

## Filme im Internet: Zwischen Urheberrechten und redlicher Nutzung

Vor weniger als zwei Jahren brachte unser *IRIS Focus* einen Artikel über eine erste Welle von Prozessen um online angebotene Audiodateien (siehe IRIS 2000-8: 14, „MP3: Redliche oder unredliche Nutzung?“). Schon damals war es nur eine Frage der Zeit, wann die digitale Technologie so weit sein würde, dass es ebenso attraktiv ist, audiovisuelle Dateien im Internet anzubieten.

Mittlerweile sind Filme im Internet zu haben, und zwar, wie zu erwarten war, meist ohne Zustimmung der Urheberrechtsinhaber. Darüber hinaus werden sie unter Umgehung technischer Maßnahmen zum Schutz des Urheberrechts angeboten. Die Filmangebote im Internet werfen also bekannte und auch neue rechtliche Fragen auf. Wie in den MP3-Prozessen setzt sich die US-Industrie auch hier mit Klagen an die Spitze der juristischen Auseinandersetzung. Doch die rechtlichen Probleme rund um die Online-Filmangebote sind wahrhaft global.

Dieses *IRIS plus* ergänzt unseren früheren Artikel mit Betrachtungen zu den neuen Rechtsfragen und ihren sachlichen Hintergründen. Wir hoffen, damit Ihrem Bedarf an rechtlichen Informationen und an Wissen über die zugrunde liegenden technischen Entwicklungen gerecht zu werden.

*Straßburg, April 2002*

**Susanne Nikoltchev**

*IRIS Koordinatorin*

*Rechtsexpertin der Europäischen Audiovisuellen Informationsstelle*

**IRIS plus** erscheint als Redaktionsbeilage von **IRIS**, *Rechtliche Rundschau der Europäischen Audiovisuellen Informationsstelle*, Ausgabe 2002-4



OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL  
EUROPEAN AUDIOVISUAL OBSERVATORY  
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSTELLE

76 ALLEE DE LA ROBERTSAU • F-67000 STRASBOURG  
TEL. +33 (0)3 88 14 44 00 • FAX +33 (0)3 88 14 44 19  
<http://www.obs.coe.int>  
e-mail: [obs@obs.coe.int](mailto:obs@obs.coe.int)

 **Nomos**  
Verlagsgesellschaft

WALDSEESTRASSE 3-5 - D-76530 BADEN-BADEN  
TEL. +49 (0)7221 2104-0 • FAX +49 (0)7221 2104-27  
e-mail: [nomos@nomos.de](mailto:nomos@nomos.de)



# Filme im Internet: Zwischen Urheberrechten und redlicher Nutzung

von **Susanne Nikoltchev und Francisco Javier Cabrera Blázquez**  
Europäische Audiovisuelle Informationsstelle

## Einführung

Die DVD (*Digital Versatile Disc*) ist das digitale Standardmedium für den Vertrieb von Filmen an private Haushalte, auf das sich alle großen Filmstudios geeinigt haben. Eine DVD hat einen Durchmesser von 12 cm und kann ein Datenvolumen von mehreren Gigabytes speichern – genug für audiovisuelle Dateien mit Spielfilmen in Kinoqualität. Abgespielt werden können DVDs auf DVD-Playern oder auf PCs mit DVD-ROM-Laufwerk und zusätzlichen Hardware- oder Software-Modulen (Media-Playern).

Technisch versierte Benutzer können heute in der Regel eine Filmdatei von der Original-DVD auslesen. Sie können also identische Kopien erstellen, indem sie die digitalen Informationen einfach auf der Festplatte des eigenen Rechners speichern. Danach kann der Film wie jede andere Datei von der PC-Festplatte gelesen und elektronisch weiterverbreitet werden. Wenn die Filmdatei im Internet angeboten wird, kann jeder beliebige Nutzer eine eigene Kopie anlegen. Dieser Vorgang, der nur mit geringfügigen Kosten oder Aufwand verbunden ist, wirkt rechtliche Fragen bezüglich der geistigen Eigentumsrechte der Film- und der DVD-Industrie auf. Der DVD-Markt steckt zwar noch in den Kinderschuhen, gewinnt aber immer mehr an Bedeutung,<sup>1</sup> und die großen Anbieter kämpfen mit allen – auch rechtlichen – Mitteln gegen die Piraterie.

In unserer früheren Publikation „MP3: Redliche oder unredliche Nutzung?“<sup>2</sup> haben wir uns bereits mit entscheidenden rechtlichen Fragen auseinandergesetzt, etwa ob das Kopieren einer Datei von einer CD auf einen elektronischen Datenträger einen Verstoß gegen Urheberrechtsgesetze darstellt, in welchen Fällen das Kopieren zulässig sein könnte und welche juristischen Implikationen sich aus den bestehenden Verbreitungsmechanismen ergeben. Die faktischen und rechtlichen Probleme der rechtswidrigen Vervielfältigung und Verbreitung digitaler Filmdateien sind weitgehend dieselben wie bei CDs, da MP3- und Filmdateien grundsätzlich dieselbe Technologie zugrunde liegt. Insbesondere ist es (wie bereits bei CD-Aufnahmen) für Privatpersonen möglich, auf der eigenen Website digitale Kopien von DVD-Filmen direkt anzubieten oder Links zu anderswo gespeicherten Kopien zu setzen. Hierbei können spezielle Verbreitungsmechanismen bereitgestellt<sup>4</sup> oder Links zu solchen Mechanismen auf anderen Websites gesetzt werden.

Eine neue Entwicklung, die in dem MP3-Artikel lediglich in ihrer Anfangsphase erfasst wurde, ist der Dateiaustausch zwischen Privatleuten über Peer-to-Peer-Netze („P2P“)-, durch den einige der relevanten rechtlichen Überlegungen erschüttert werden. Peer-to-Peer-Systeme funktionieren nach dem Schneeballprinzip: Ein Benutzer stellt zunächst eine Verbindung zu einem oder mehreren anderen Benutzern her, um seine Anfrage nach einem bestimmten Film durchzugeben. Die Empfänger leiten diese Anfrage dann an alle Benutzer weiter, mit denen sie ihrerseits verbunden sind, bis die entsprechende Datei im Netz gefunden ist. Die eigentliche Dateiübertragung findet dann zwischen zwei Privatpersonen statt und bleibt anonym.<sup>5</sup> Neuerdings wird der Austausch von Filmdateien per Internet durch das System FastTrack erleichtert und beschleunigt. FastTrack basiert auf einer neuen Variante der P2P-Software für den Dateiaustausch und wird kostenlos im Internet angeboten. Der aus diesem Austausch entstandene Rechtsstreit (siehe *infra*, MGM gegen Grokster) verdeutlicht, dass der Streit um MP3 jetzt bei den P2P-Verbreitungsmechanismen für Filme seine Fortsetzung findet.

Allerdings wirft der Austausch von Filmdateien per Internet rechtliche Fragen auf, die über die gerichtlich erörterten Fragen zu MP3 und auch über die durch FastTrack hinzugekommenen Probleme hinausgehen. Dies liegt vor allem daran, dass die Industrie einen technischen Sicherungsmechanismus namens *Content Scramble System* (CSS) gegen das Raubkopieren von DVDs entwickelt hat, der im MP3-Beispiel noch

nicht relevant war.<sup>6</sup> Die Antwort einiger Programmierungsexperten erfolgte umgehend in Form von DeCSS, einer Software zum Dekodieren (*unscrambling*) von CSS.

Die Mischung aus bereits bekannten und neuen Aspekten der Verbreitung audiovisueller Dateien gibt die Gliederung dieses Artikels vor. Er beginnt mit den MP3 Rechtsfällen unter besonderer Berücksichtigung jener Fragen, die auch bei der Verbreitung von Filmdateien eine Rolle spielen. Anschließend behandelt er den Rechtsstreit um FastTrack, beschreibt dann die CSS/DeCSS-Technologie mit ihren rechtlichen Implikationen und zieht zum Abschluss ein kurzes Fazit.

## Lehren aus den Rechtsstreitigkeiten über Audiodateien

Wenn Audio- oder Audio-Video-Dateien ohne Zustimmung des Rechtsinhabers übertragen werden, ist meist ein Rechtsstreit die Folge. So war es bei der Verbreitung von MP3-Dateien im Internet, und so ist es nun auch bei der elektronischen Übertragung von Filmdateien. Nach der bisherigen Rechtsprechung zu MP3 ist es illegal, nicht spezifizierten Kunden nicht autorisierte Audiodateien anzubieten, wobei es unerheblich ist, ob dies über Links zu diesen Dateien direkt oder über Datelisten oder andere Websites erfolgt, die direkte Links oder Listen bereitstellen. Darüber hinaus riskieren zumindest in einigen Ländern auch Internet-Diensteanbieter, deren Dienste für den Online-Austausch von MP3-Dateien und das Hosting von Websites erforderlich sind, dass sie für indirekte Urheberrechtsverletzungen haftbar gemacht werden.<sup>7</sup>

In den MP3-Fällen ging es auch um den Urheberrechtsschutz bei bestimmten Verbreitungsmechanismen wie My.MP3.com<sup>8</sup> und Napster.<sup>9</sup> Bei My.MP3.com konnten Abonnenten den Inhalt ihrer eigenen CDs speichern, bearbeiten und von jedem Ort der Welt aus anhören, solange sie Zugang zum Internet hatten. Die für den Kunden bereitgestellten digitalen Kopien wurden von dem Unternehmen, das diesen Dienst anbot, angefertigt und archiviert und waren zumeist nicht autorisiert. Napster hingegen war eine reine Plattform für den Austausch von MP3-Kopien zwischen den Kunden. Abgesehen von dem Index der verfügbaren Dateien, den Napster bereitstellte, handelte es sich im Grunde um ein P2P-System. Die Angebote von My.MP3.com und Napster wurden in den USA verboten, wenn auch im Fall Napster nur durch ein Vorabentscheidungsverfahren, wobei die Entscheidung in der Hauptsache noch aussteht.

Unabhängig vom jeweils geltend gemachten Anspruch mussten die Gerichte zunächst eine direkte Urheberrechtsverletzung feststellen. Keine Mühe schien die Feststellung der notwendigen Fakten zu machen, wenn die im Internet angebotenen Dateien größtenteils oder insgesamt ohne Zustimmung des Rechtsinhabers kopiert worden waren.<sup>10</sup>

Schwieriger war die Frage, ob das Up- oder Downloaden als privater Gebrauch bzw. redliche Nutzung oder im Rahmen einer anderen Ausnahmeregelung zu rechtfertigen sei. In einem Fall berief man sich (erfolglos) auf das Recht auf freie Meinungsäußerung, da ein Verbot von Links auf MP3-Dateien eine unzulässige Einschränkung darstelle.<sup>11</sup> In eine ähnliche Richtung weist das Argument von Napster, die Kläger hätten insgeheim verabredet, „ihre Urheberrechte zu nutzen, um ihre Kontrolle auf die Online-Verbreitung auszudehnen“.<sup>12</sup>

Der Ausgleich zwischen absoluten Urheberrechten und dem öffentlichen Interesse an einem gewissen Maß privaten Gebrauchs – oder in US-Terminologie: an einer redlichen Nutzung (*fair use*) – stand nicht nur im Mittelpunkt der MP3-Kontroversen, sondern war bereits bei der Ersten Diplomatischen Konferenz der WIPO im Jahr 1884 thematisiert worden.<sup>13</sup> Seither werden Ausnahmen von den absoluten Urheberrechten in internationale Verträge und nationale Gesetze hineingeschrie-



ben. Die jüngste Erweiterung der einschlägigen europäischen Gesetzgebung ist die Richtlinie zum Urheberrecht in der Informationsgesellschaft (die „Richtlinie“).<sup>14</sup> Artikel 5 der Richtlinie zählt alle Ausnahmen und Beschränkungen der Urheberrechte auf, die die nationale Gesetzgebung vorsehen kann, aber nicht muss.<sup>15</sup> Die Ausnahme des privaten Gebrauchs ist für das Vervielfältigungsrecht ausdrücklich in Artikel 5 Absatz 2b) vorgesehen, sofern keine kommerziellen Ziele verfolgt werden. Auf diese Ausnahme wird in Zusammenhang mit dem Verbreitungsrecht in Artikel 5 Absatz 4 Bezug genommen. Privater Gebrauch betrifft auch digitale Träger und deckt daher das private Kopieren auf Festplatten ab. Hierbei ist unerheblich, ob derjenige, der eine private Kopie anfertigt, dies für den Eigengebrauch oder für einen Dritten tut.<sup>16</sup> Die Ausnahme für den privaten Gebrauch – wie auch alle anderen urheberrechtlichen Ausnahmen nach EG-Recht – darf ferner „nur in bestimmten Sonderfällen angewandt werden, in denen die normale Verwertung des Werks oder des sonstigen Schutzgegenstands nicht beeinträchtigt wird und die berechtigten Interessen des Rechtsinhabers nicht ungebührlich verletzt werden“. Anders als bei anderen Ausnahmen und bei der redlichen Nutzung setzt der private Gebrauch generell voraus, dass der Rechtsinhaber einen gerechten Ausgleich erhält.

Bei der Beurteilung des Verhaltens der Nutzer von My.MP3.com und Napster stand die redliche Nutzung im Vordergrund. Im Gegensatz zum europäischen Ansatz, bei dem der private Gebrauch durch bestimmte Schlüsselemente definiert ist, die dann im nationalen Recht genauer ausgeführt und festgelegt werden, ist die redliche Nutzung dynamisch und auf den Einzelfall bezogen festzustellen. Nach 17 U.S.C. § 107 sind vier spezifische Kriterien zu berücksichtigen, doch auch andere können zusätzlich herangezogen werden. Dies ist ein weiterer Unterschied zum EG-Recht.

In den MP3-Fällen war keines dieser Kriterien erfüllt. Im Fall Napster allerdings ist dies bislang nur ein vorläufiges Ergebnis, und insofern sind die Grenzen der „redlichen Nutzung“ in den USA noch nicht endgültig geklärt.

Die Untersuchung von Urheberrechtsverletzungen bei den jeweiligen Verbreitungsmechanismen endet nicht damit, dass Kunden gefunden werden, die für das Up- oder Downloaden elektronischer Dateien primär haftbar sind. Die nächste Frage lautet, ob auch der Anbieter der betreffenden Dienste haftbar gemacht werden kann. Der Anbieter von Napster haftet dem Gericht zufolge sekundär für direkte Urheberrechtsverletzungen gemäß den Theorien von der mittelbaren und der stellvertretenden Urheberrechtsverletzung (*contributory and vicarious copyright infringement*).<sup>17</sup>

Napster hat die Feststellung der sekundären Haftbarkeit unter Berufung auf § 512 (a) des *Digital Millennium Copyright Act* (Urheberrechtsgesetz für das digitale Jahrtausend – DMCA) angefochten.<sup>18</sup> Diese Schutzbestimmung beschränkt die Haftung der Anbieter von Onlinediensten für die über ihre Dienste ausgetauschten Informationen, wenn der Anbieter technische Maßnahmen zum Schutz der Urheberrechte, wie zum Beispiel Verschlüsselungssysteme, unterstützt. Sie greift jedoch nicht, wenn der Anbieter von (wiederholten) Verstößen wusste oder wissen musste. Die Wahrscheinlichkeit dieses Wissens machte die Einrede von Napster im Vorverfahren zunichte, wo allerdings die vorgelagerte Frage offen blieb, ob es sich bei Napster überhaupt um einen Internet-Diensteanbieter handelt. Es hat den Anschein, dass Mechanismen zur Verbreitung von Dateien im Internet unter die Schutzbestimmungen des DMCA fallen könnten. Wenn sie die Anforderungen noch nicht erfüllen sollten, könnten einige Änderungen ihres technischen Aufbaus die Anwendbarkeit zu ihren Gunsten herbei führen. Dies könnte bereits bei der P2P-Konstellation der Fall sein.

Mit diesem Ergebnis deckt sich auch die Richtlinie. Einerseits hat sie das Exklusivrecht auf Zugänglichmachung eingeführt, das die Mitgliedstaaten den Herstellern erstmaliger Aufzeichnungen von Filmen in Bezug auf das Original und auf Vervielfältigungsstücke ihrer Filme einräumen müssen. Zentralisierte Verbreitungsmechanismen, wie sie für MP3 genutzt werden, bieten Dienste an, die „Mitgliedern der Öffentlichkeit von Orten und zu Zeiten ihrer Wahl zugänglich sind“.<sup>19</sup> Daher werden sie wahrscheinlich als interaktive Übertragungen auf Abruf eingestuft. Wenn der Gebrauch nicht vom Rechtsinhaber genehmigt wird, könnten diese Dienste folglich mit dem Recht auf Zugänglichmachung kollidieren. Andererseits heißt es in Erwägung 27 der Richtlinie: „Die

bloße Bereitstellung der Einrichtungen, die eine Wiedergabe ermöglichen oder bewirken, stellt selbst keine Wiedergabe im Sinne dieser Richtlinie dar.“ Dies deutet darauf hin, dass zumindest der „traditionelle“ Internet-Diensteanbieter vor einer Haftung für die Erbringung seiner Dienste sicher ist. Wie Napster hier zu beurteilen wäre, ist ungewiss, da P2P-Netze wohl eine interessante Zwittererscheinung sind.

### Das FastTrack-System: MGM gegen Grokster

Das erfolgreichste dieser P2P-Netze entstand durch das FastTrack-System, eine proprietäre P2P-Filesharing-Software. Mit FastTrack kann jeder Benutzer bei jedem anderen Benutzer Dateien aller Art finden und durch eine individuelle Übertragung direkt von Benutzer zu Benutzer (ohne Zentralserver) auf den eigenen Rechner kopieren. Die Firma Consumer Empowerment BV (auch unter dem Namen „Kazaa“ bekannt) hat die FastTrack-Software entwickelt, kostenlos im Internet verbreitet und Lizenzen an Grokster und MusicCity vergeben. Daraufhin haben diese beide Firmen FastTrack ebenfalls kostenlos im Internet angeboten. Alle drei Firmen bieten FastTrack mit einer eigenen Oberfläche an, in der sie Mitteilungen und Werbung einblenden. Durch FastTrack können Kazaa, Grokster und MusicCity gemeinsam dasselbe Benutzernetz ansprechen.

FastTrack funktioniert ähnlich wie andere P2P-Systeme, ist aber im Gegensatz zu ihnen nicht vollkommen dezentralisiert. In vollkommen dezentralen P2P-Filesharing-Netzen (wie Gnutella) müssen Suchanfragen oft das gesamte Netz durchlaufen, weil jeder Computer nach der gewünschten Datei gefragt wird. Dies erzeugt nicht nur einen enormen Datenverkehr im Internet, sondern es bremst auch den Suchprozess erheblich (oder verhindert ihn gelegentlich sogar ganz).

Zur Ausschaltung dieses Problems haben die Entwickler von FastTrack das SuperNode-Prinzip erdacht. SuperNodes sind eine zufällige Auswahl von Benutzerrechnern, die als Drehscheibe für andere FastTrack-Benutzer in einem bestimmten geographischen Bereich dienen. Offenbar wählt das System einzelne Rechner automatisch als SuperNodes aus und wechselt sie laufend je nach den Anforderungen des Netzes. Die Benutzer müssen der Inanspruchnahme als SuperNodes zustimmen.

Jeder Benutzer ist mit einem bestimmten SuperNode verbunden, der eine Reihe von Benutzern verwaltet und einen Index der Dateien führt, die sie zum Download bereithalten. Alle SuperNodes sind zudem untereinander verbunden und haben somit Zugriff auf den Index jedes anderen. Als Netz verwalten die SuperNodes eine Gesamtliste aller Dateien, die bei allen FastTrack-Benutzern verfügbar sind. Ein System wie Napster dagegen würde einen Index der Dateien auf einem oder mehreren Zentralservern vorhalten. Wenn ein FastTrack-Benutzer eine Suchanfrage an seinen „lokalen“ SuperNode richtet, werden automatisch die Listen sämtlicher SuperNodes durchsucht.

Am 2. Oktober 2001 verklagten mehrere Kläger, die die Tonträger- und die Filmindustrie vertreten, die Firmen Grokster, Ltd., MusicCity.Com, Inc., MusicCity Networks, Inc. und Kazaa auf Schadenersatz wegen Urheberrechtsverletzung und beantragten eine einstweilige Verfügung.<sup>20</sup> Der Fall soll am 1. Oktober 2002 vor einem Schwurgericht verhandelt werden.<sup>21</sup> Die Kläger wollen mit dieser Klage „verhindern, dass die Beklagten weiterhin massive Verletzungen ihrer urheberrechtlich geschützten Werke im Internet fördern, ermöglichen und davon profitieren“.<sup>22</sup> Den Beklagten wurde vorsätzliches Handeln unter Missachtung der Rechte der Kläger vorgeworfen. Den Klägern zufolge sind die meisten Dateien im Netz der Beklagten illegale Kopien, darunter befinden sich auch kürzlich veröffentlichte Filme, von denen einige noch in den Kinos laufen und noch nicht auf dem Video/DVD- oder Fernsehmarkt verfügbar sind.

Die Beklagten räumen ein, dass die Benutzer ihres Netzes urheberrechtlich geschützte Werke unberechtigt verbreitet haben. Es geht daher in diesem Fall ausschließlich um die sekundäre Haftung der Beklagten für direkte Verstöße gemäß den Theorien von der mittelbaren und der stellvertretenden Urheberrechtsverletzung.

### Mittelbare Urheberrechtsverletzung

Nach der Theorie von der mittelbaren Urheberrechtsverletzung (*contributory copyright infringement*) kann jeder, der wissentlich das rechtsverletzende Verhalten eines anderen veranlasst, bewirkt oder wesentlich dazu beiträgt, als „mittelbarer Rechtsverletzer“ haftbar gemacht wer-



den.<sup>23</sup> Den Klägern zufolge bieten die Beklagten die Software, Unterstützung und Dienste für die Rechtsverletzungen an, fördern und erleichtern diese dadurch und ermuntern die Benutzer zu solchem Verhalten.

Im Fall Napster hatte der *Court of Appeals* (Berufungsgericht) festgestellt, dass den Benutzern die unberechtigte Vervielfältigung von urheberrechtlich geschütztem Material über das Netz ohne die unterstützenden Dienste von Napster nicht möglich gewesen wäre. Allerdings hätte dem Gericht zufolge die bloße Bereitstellung der Mittel für die rechtsverletzende Tätigkeit keine mittelbare Urheberrechtsverletzung dargestellt. Da die Zentralserver von Napster jedoch den Index der Dateien verwaltet hätten, habe Napster tatsächliche Kenntnis von den rechtsverletzenden Aktivitäten in seinem Netz gehabt und es gleichwohl versäumt, das unberechtigte Kopieren von Musikdateien zu verhindern. Daher kam das Gericht zu dem Schluss, Napster habe zu den rechtsverletzenden Aktivitäten wesentlich beigetragen.

Im Gegensatz zu Napster bringen die Beklagten nun jedoch vor, dass sie (bei der Lieferung) keine tatsächliche Kenntnis davon haben, wie die Kunden ihre Software nutzen werden. Sie behaupten, nicht an dem Vorgang der Dateisuche und des Dateiaustauschs im Netz beteiligt zu sein, weil der Dateiindex gemeinsam von den SuperNodes verwaltet wird. Darüber hinaus erhielten sie keine Informationen über Suchaktivitäten und hätten auch keine Kenntnis davon.

Die Kläger entgegnen darauf, dass sie die Beklagten über rechtsverletzende Dateien informiert hätten. Außerdem unterhielten sich die Benutzer in einem von den Beklagten überwachten Chatroom frei über ihre rechtsverletzenden Aktivitäten.

Die Beklagten berufen sich auch auf das Sony-Betamax-Urteil,<sup>24</sup> in dem es hieß: „Der Verkauf von Kopiergeräten stellt, ebenso wie der Verkauf anderer Handelswaren, keine mittelbare Rechtsverletzung dar, wenn das Produkt weithin zu rechtmäßigen, einwandfreien Zwecken eingesetzt wird. Sie müssen lediglich zu wesentlichen nicht rechtsverletzenden Verwendungszwecken in der Lage sein.“ Nach Auffassung der Beklagten ist die FastTrack-Software, genau wie der Sony-Betamax-Videorekorder, zu wesentlichen nicht rechtsverletzenden Verwendungszwecken in der Lage.

Die Kläger bestreiten diese Einrede, weil die Beklagten ihre Software für den rechtsverletzenden Gebrauch entwickelt hätten und das Sony-Betamax-Urteil weder die unberechtigte Verbreitung urheberrechtlich geschützter Werke rechtfertige noch für Fälle gelte, in denen die rechtsverletzende Aktivität unterbunden werden kann, während nicht rechtsverletzende Verwendungen weiter möglich bleiben. Den Klägern zufolge haben die Beklagten die wesentlichen nicht rechtsverletzenden Verwendungen nicht belegt.

#### Stellvertretende Urheberrechtsverletzung

Bei der stellvertretenden Urheberrechtsverletzung (*vicarious copyright infringement*) hat der Rechtsverletzer „das Recht und die Fähigkeit, die rechtsverletzenden Aktivitäten zu überwachen, und darüber hinaus ein direktes finanzielles Interesse an solchen Aktivitäten“.<sup>25</sup> Er muss sich der tatsächlichen Rechtsverletzung nicht bewusst sein. Den Klägern zufolge haben sich die Beklagten stellvertretend haftbar gemacht, weil sie Kontrolle über die Mittel ausübten, mit denen die direkte Rechtsverletzung begangen wurde. Sie profitierten von diesen rechtswidrigen Handlungen, indem sie Benutzer in ihr Netz lockten, und erzielten finanzielle Vorteile, indem sie in ihre Software-Oberfläche Werbung einblendeten.

Dem Fall Napster zufolge besteht der finanzielle Vorteil darin, dass durch das Verfügbarmachen von rechtsverletzendem Material Kunden angelockt werden.<sup>26</sup> Im vorliegenden Fall scheint der finanzielle Vorteil sogar besonders ausgeprägt zu sein, weil die Beklagten mit dem Einblenden von Werbung Einnahmen erzielen. Ihre Gebühren richten sich hierbei nach der Zahl der Benutzer im Netz.

Statt auf das Sony-Betamax-Urteil, das sich nur auf die mittelbare Urheberrechtsverletzung bezieht, berufen sich die Beklagten darauf, dass sie nach der Auslieferung der P2P-Software die Aktivitäten der Benutzer nicht mehr überwachen und/oder kontrollieren können. Selbst wenn sie ihre Zentralserver stilllegten, würde das gesamte System weiter funktionieren. Lediglich die Benutzernamen würden in der Oberfläche nicht richtig angezeigt, außerdem würden die Grafiken und die Werbung nicht am Bildschirm erscheinen. Die Kläger bestreiten dies mit

Hinweis auf die Bemühungen der Beklagten, die Software zu aktualisieren und zu pflegen und ihre Beziehungen zu den Kunden zu fördern.

„Nach der Napster-Entscheidung scheint das Urheberrecht den P2P-Entwicklern eine Entscheidung zwischen zwei gegensätzlichen Möglichkeiten aufgezwungen zu haben: Sie können entweder ein System entwickeln, das eine genaue Beobachtung und Kontrolle der Benutzeraktivitäten ermöglicht, oder aber ein System, das eine solche Beobachtung und Kontrolle völlig unmöglich macht“.<sup>27</sup> Kazaa, Grokster und MusicCity scheinen dies begriffen zu haben, als sie ein Geschäftsmodell entwickelten, das sich auf ein sich selbsterzeugendes, von SuperNodes verwaltetes Netz stützt, das sie möglicherweise vor einer sekundären Haftung für Urheberrechtsverletzungen bewahrt. Allerdings müssen die Attacken der Kläger gegen dieses System erst abgewehrt werden. Die entscheidende Frage für die Geschworenen wird lauten, ob die Beklagten tatsächliche Kenntnis von den rechtsverletzenden Aktivitäten hatten und ob sie sie wirksam hätten beobachten oder kontrollieren können.

Die Ähnlichkeiten zwischen den Verbreitungsmechanismen von Napster und FastTrack dürfen uns nicht den Blick auf die Unterschiede zwischen Audiodateien und audiovisuellen Dateien verstellen. Insbesondere DVDs waren von Anfang an stärker durch technische Maßnahmen geschützt. Die Filmgesellschaften haben gegen illegales Kopieren ein Zugangskontroll- und Kopierschutzsystem entwickelt und eingeführt. Dieses System hat dem Rechtsstreit um Urheberrechte eine neue Dimension verliehen.

#### **CSS und DeCSS**

Das *Content Scramble System* (CSS) kontrolliert den Zugriff auf Filmdateien und verhindert das Kopieren dieser Dateien. Es handelt sich um ein zweistufiges Schutzsystem. Es arbeitet mit einer Reihe von Schlüsseln, die auf der DVD und dem DVD-Player gespeichert sind, um die Authentizität von beiden zu überprüfen.

Zunächst verschlüsselt CSS die Audio- und Grafikdateien. Hierzu ist jede DVD auf dem Markt mit einem verschlüsselten Disc-Schlüssel kodiert, der sie eindeutig identifiziert. Außerdem ist die Hardware (DVD-Player oder Computer mit DVD-Laufwerk) mit einer passenden Konfiguration ausgestattet, sodass sie die verschlüsselten Informationen entschlüsseln und wiedergeben kann. Wenn ein DVD-Player eine DVD zu lesen versucht, geht er mit seinem Player-Schlüssel die Liste der verschlüsselten Disc-Schlüssel auf der DVD durch und versucht, einen zu entschlüsseln, der zu dem auf der DVD passt. Der Player-Schlüssel wird validiert, sobald ein korrekter Disc-Schlüssel gefunden ist, und ein weiterer Schlüssel für die DVD wird verfügbar. Dieser Schlüssel dient dann dazu, den eigentlichen DVD-Inhalt zu entschlüsseln.

CSS erlaubt den Wiedergabegeräten das Entschlüsseln und Abspielen, aber nicht das Kopieren der Filme. Die *DVD Copy Control Association* (DVDCCA) stellt die CSS-Schlüssel bereit und lizenziert sie unter strengen Sicherheitsanforderungen an die Hersteller von Discs und Playern weiter. Die Lizenz verbietet auch die Herstellung von Geräten mit einem digitalen Ausgang, der zum Kopieren geschützter DVDs verwendet werden könnte.

Vorerst ist CSS nur mit Computern kompatibel, die als Betriebssystem Windows (nicht aber beispielsweise Linux) einsetzen.

Im 21. Jahrhundert erscheint es beinahe unausweichlich, dass ein Verschlüsselungssystem von findigen Köpfen geknackt wird. Erst recht gilt dies, wenn der Anreiz für die Entschlüsselung von der Bewältigung der „wissenschaftlichen Herausforderung“ bis zum kostenlosen Zugriff auf Hollywoodfilme reicht. Im Jahr 1999 knackte der Teenager Jon Johansen das CSS-System durch *reverse engineering* (Rückentwicklung) eines lizenzierten DVD-Players. Anhand des aufgedeckten CSS-Verschlüsselungsalgorithmus und der Schlüssel entwickelte er ein Computerprogramm namens DeCSS, das das CSS entschlüsselt und es dem Benutzer ermöglicht, DVD-Filme auf nicht lizenzierten Playern abzuspielen und digital zu kopieren. Dadurch können die Filmdateien wie beliebige andere Dateien per Internet weitergegeben werden. Johansen bot DeCSS kostenlos auf seiner Website an. Von dort wurde es heruntergeladen und zahlreiche andere Websites stellten Kopien bereit.

In Verbindung mit weiterer Software bietet DeCSS jedem Benutzer die Möglichkeit, eine digitale Kopie von einer mit CSS verschlüsselten

DVD anzufertigen. Die gesamte für die Decodierung erforderliche Software ist kostenlos im Internet zu haben.

Der erste Schritt beim Kopieren einer CSS-verschlüsselten Datei auf die Festplatte eines nicht kompatiblen Computers besteht im „Rippen“ (Extrahieren und Decodieren) der Originaldatei (VOB-Datei) auf der DVD. Anschließend kann die VOB-Datei in ein Dateiformat komprimiert werden, das mit den meisten Wiedergabeprogrammen (Media-Playern) auf dem Computer abgespielt werden kann. Danach kann die komprimierte Datei durch zusätzliche Komprimierungsschritte weiter verkleinert werden, sodass die Dateiübertragung im Internet beschleunigt wird. Die Bildqualität dieses Endprodukts ist zwar geringer als die der Original-DVD, reicht aber zum Ansehen des Films auf dem Computerbildschirm immer noch aus.

### Rechtliche Implikationen von DeCSS

Am 9. Januar 2002 klagte ØKOKRIM (die norwegische Strafverfolgungsbehörde für Wirtschaftskriminalität) Johansen an, weil er in den abgeschlossenen Besitz eines anderen eingebrochen sei, um sich unberechtigten Zugriff auf Daten zu verschaffen.<sup>28</sup> Bei einer Verurteilung drohen Johansen nach dem norwegischen Strafgesetzbuch bis zu zwei Jahre Haft.<sup>29</sup> Die Anklage stützt sich auf § 145, dessen relevanter Teil wie folgt lautet:<sup>30</sup>

„2. Dieselbe Strafe gilt für jede Person, die sich durch Aufbrechen einer Schutzvorrichtung oder auf ähnliche Weise rechtswidrig Zugriff auf Daten oder Software verschafft, die mit elektronischen oder anderen technischen Mitteln gespeichert oder übertragen werden.“

Die Anklage ist eine positive Reaktion auf die von der DVDCCA und der Motion Picture Association geführten Klage.<sup>31</sup> Folgende Fragen, für die es im norwegischen Recht keinen Präzedenzfall gibt, werden über den Ausgang des Prozesses entscheiden: Erstens: Umfasst der Begriff „Daten“ auch den CSS-Code oder nur Filmdateien? Zweitens: Erstreckt sich die Bestimmung auch auf das Brechen des Codes zum Zugriff auf Material auf einer DVD, wenn diese der Person, die die Schutzvorrichtung umgeht, selbst gehört? Drittens: Erfüllt das *reverse engineering* die Kriterien für kriminelles Verhalten? Viertens: Ist überhaupt ein vertraglicher Verzicht auf das nach norwegischem Recht ausdrücklich garantierte Recht auf *reverse engineering* möglich, insbesondere wenn die entsprechende vertragliche Verpflichtung im Rahmen einer über das Internet zustande gekommenen Lizenzvereinbarung eingegangen wird (vgl. die Ausführungen zu dem kalifornischen Prozess)?<sup>32</sup>

Bevor diese Fragen beantwortet werden können, muss zunächst ein Prozesstermin anberaumt werden.

In den USA hat die DVDCCA mehrere Klagen gegen das Anbieten von DeCSS und von Links auf Websites mit DeCSS eingereicht. Einige dieser Fälle sind mittlerweile abgeschlossen. Andere führten zu einer einstweiligen oder endgültigen Verfügung.

Am 20. Januar 2000 erließ ein kalifornisches Gericht der ersten Instanz eine einstweilige Verfügung gegen Andrew Bunner, die es ihm untersagt, DeCSS durch Wiederveröffentlichung auf seiner Website oder anderswo weiterzugeben. Das Gericht verbot es ihm jedoch nicht, Links auf andere Websites zu setzen, die DeCSS anbieten.<sup>33</sup> Am 1. November 2001 wurde die Verfügung von der Berufungsinstanz aufgehoben.<sup>34</sup> Wie am 22. Februar 2002 gemeldet wurde, will der California Supreme Court nun über den Fall verhandeln.<sup>35</sup>

Am 23. August 2000 verbot der *United States District Court for the Southern District of New York* (US Bezirksgericht für den Südlichen Bezirk New Yorks) den Beklagten die Veröffentlichung von DeCSS auf ihrer Website und das wissentliche Setzen von Links von ihrer Website zu anderen Websites, die DeCSS anbieten.<sup>36</sup> Zwei der Beklagten, Eric Corley und seine Firma 2600 Enterprises, Inc., gingen am 28. November 2001 in Revision, verloren aber vor dem *United States Court of Appeals for the Second Circuit* (US Berufungsgericht für den Zweiten Gerichtsbezirk).<sup>37</sup>

Während es bei dem kalifornischen Prozess um die Bestimmungen der kalifornischen Version des *Uniform Trade Secrets Act* (Einheitliches Gesetz über Geschäftsgeheimnisse) geht, stützt sich die New Yorker Klage auf den DMCA und damit auf Bundesrecht. Gemeinsam ist beiden Fällen, dass auch die verfassungsrechtliche Dimension der Erstellung, Verwendung und Verfügbarmachung von DeCSS erörtert wird. In beiden Fällen richtete sich die Klage nicht gegen Johansen, aber dennoch waren seine Taten implizit zu bewerten.

### Der kalifornische Fall (DVDCCA gegen Bunner)

Gegen Bunner trug die DVDCCA das Argument vor, DeCSS enthalte, verwende und/oder sei eine wesentliche Ableitung ihrer vertraulichen proprietären Informationen. Angeblich enthält DeCSS den Hauptschlüssel eines zugelassenen CSS-Lizenznehmers. Dieser Lizenznehmer biete CSS-Software ausschließlich im Rahmen einer Lizenzvereinbarung an, die *reverse engineering* untersagt. Jeder Benutzer, der den Prozess der Software-Installation durchlaufe, stimme dem Vertrag zu, weil bei der Installation die Endbenutzer-Lizenzvereinbarung am Bildschirm erscheine, in der es heiße, das „Produkt in Form von Quellcode“<sup>38</sup> sei „vertraulich“ und ein „Geschäftsgeheimnis“ und der Benutzer dürfe „nicht versuchen, irgendeinen Teil des Produkts zurückzuentwickeln“.

Bei der Beurteilung dieser Sachverhalte kam das Gericht zu dem Schluss, dass die DVDCCA CSS mit Recht als Geschäftsgeheimnis bezeichnen könne und angemessene Anstrengungen zu seinem Schutz unternommen habe. Dieses Geheimnis sei durch *reverse engineering* gelüftet worden. Der kalifornische *Uniform Trade Secrets Act* (*Civil Code Section* § 3426 – 3426.11, kalifornisches Zivilgesetz)<sup>39</sup> bestimmt, dass eine Person, die ein Geschäftsgeheimnis verrät oder nutzt, von dem sie wusste oder hätte wissen müssen, dass eine andere Person es durch „unlautere Mittel“ oder unter Verstoß gegen eine Vertraulichkeitsverpflichtung erlangt hat, dieses Geschäftsgeheimnis widerrechtlich verwendet. Das Gericht ging davon aus, dass Bunner DeCSS weitergegeben hat, obwohl er zumindest hätte wissen müssen, dass DeCSS durch die unberechtigte Nutzung proprietärer CSS-Informationen, die durch das rechtswidrige Brechen des Codes durch Johansen erlangt worden waren, entstanden war. Die Rechtswidrigkeit von Johansens Tat ergab sich jedoch aus seinem Verstoß gegen die Lizenzvereinbarung, die *reverse engineering* verbot, und nicht aus dem *reverse engineering* als solchem, da dieses ausdrücklich nicht zu den unlauteren Mitteln gezählt wird (*Civil Code*, § 3426.1 Unterabschnitt (a)).

Das Gericht sprach kein Verbot von Links zu anderen Websites aus, da ein Website-Eigentümer nicht für den Inhalt anderer Websites hafte. Außerdem betrachtete es Links als unverzichtbar für den Zugriff auf das Internet.

Der Hauptaspekt, der dem *California Court of Appeals* in der zweiten Instanz zur Prüfung blieb, war die Beurteilung der Frage der freien Meinungsäußerung nach dem *First Amendment* (verfassungsrechtliche Norm zum Schutz der freien Meinungsäußerung) durch die Vorinstanz. Dieser Aspekt wird weiter unten gemeinsam mit den Fragen erörtert, die durch den New Yorker Fall aufgeworfen wurden.

### Der New Yorker Fall (DVDCCA gegen Corley)

Im Fall Corley ging es vor allem um die Frage, ob DeCSS ein nach dem DMCA verbotenes Umgehungsinstrument ist. Der DMCA setzt unter anderem die nach Artikel 11 des WIPO-Urheberrechtsvertrags (WCT) und Artikel 18 des WIPO-Vertrags über Darbietungen und Tonträger (WPPT) bestehende Verpflichtung zur Gewährung eines ausreichenden und wirksamen Schutzes vor der Umgehung technischer Maßnahmen, mit denen Urheberrechtshaber ihre Werke schützen, in US-Recht um. Hierbei unterscheidet er zwischen technischen Maßnahmen, (i) die den unberechtigten „Zugriff“ auf ein urheberrechtlich geschütztes Werk verhindern (§ 1201 (a)(2)) und (ii) die das unberechtigte „Kopieren“ eines urheberrechtlich geschützten Werks verhindern (§ 1201 (b)(1)).<sup>40</sup> Die Weitergabe ist zwar in beiden Fällen verboten, die Umgehung an sich jedoch nur bei den Maßnahmen der ersten Kategorie.<sup>41</sup>

Der District Court stuft CSS als Zugangskontrollmaßnahme gemäß § 1201 (a)(2) ein, weil die Software verschiedene Schlüssel verlange, bevor sie das Lesen eines CSS-geschützten Werkes auf einer DVD zulasse. Der Zugriff zu diesen Schlüsseln werde ausschließlich durch Lizenzvereinbarungen oder durch den Kauf von DVD-Playern oder -Laufwerken, die die Schlüssel gemäß einer solchen Lizenz enthalten, gewährt. Durch die Entwicklung von DeCSS habe Johansen diese technische Maßnahme umgangen, da DeCSS ein verschlüsseltes Werk, nämlich die geschützte Filmdatei, ohne Genehmigung des Urheberrechtshabers entschlüssele (§ 1201 (a)(1)(A)).<sup>42</sup>

Als nächstes erwog der District Court, ob Johansen sich mit Erfolg auf das später als Linux-Einrede bekannt gewordene Argument hätte

berufen können. Die Beklagten brachten vor, Johansen habe DeCSS nur geschaffen, um die Entwicklung eines DVD-Players, der unter dem Betriebssystem Linux lief, zu fördern. (Einen solchen gab es damals nicht.) Nach § 1201 (f) DMCA haftet nicht, wer eine Umgehungstechnologie allein dazu entwickelt oder nutzt, Elemente des Programms zu identifizieren und zu analysieren, die zur Erzielung der Interoperabilität von Computerprogrammen durch *reverse engineering* erforderlich sind, sofern er berechtigt ist, eine Kopie des Computerprogramms zu diesem Zweck zu nutzen. DeCSS sei zugestandenermaßen unter Windows entwickelt worden und laufe nur unter Windows, sodass die entschlüsselten Dateien natürlich wie jede andere ungeschützte Datei mit Linux oder Windows kopiert werden könnten. Darüber hinaus kam der *District Court* zu der Auffassung, das Knacken von CSS sei für Johansen ein Selbstzweck gewesen und habe ihm dazu gedient, sein Talent unter Beweis zu stellen. Außerstenfalls habe zu seinen Zielen auch die Entwicklung eines DVD-Players auf Linux-Basis gehört. Für die Beklagten, die DeCSS nicht geschrieben hatten, wäre die Absicht, Linux zu fördern, in jedem Fall unwesentlich gewesen, weil grundsätzlich nur derjenige, der Informationen durch *reverse engineering* gewonnen habe, diese Informationen auch verfügbar machen dürfe.

Ferner beurteilte der *District Court* die Bereitstellung von DeCSS durch die Beklagten auf deren Websites als Verstoß gegen die Weitergabeverbote in § 1201 (a)(2) und § 1201 (b)(1). Während er sich also hauptsächlich auf die „Zugriffs“-Alternative konzentrierte, berücksichtigte später der *Appellate Court* vor allem die technische Frage, ob das CSS-Verfahren auch unberechtigtes Kopieren verhindern würde. Er kam zu dem Ergebnis, dass „die Unterlagen wenig Aufschluss darüber geben, wie CSS eine DVD nicht nur vor dem Abspielen auf einem nicht lizenzierten Player, sondern auch vor dem Kopieren schützt“, dass jedoch „das Programm DeCSS den wie auch immer gearteten Mechanismus umgeht, der das Kopieren der Datei blockiert“. Daher greife auch das Weitergabeverbot, das am Schutz vor rechtswidrigem Kopieren ansetze.

Für die Zugriffs- und die Kopieralternative verbietet das Gesetz die Weitergabe von Vorrichtungen, die (i) primär zur Umgehung von Schutzmechanismen entwickelt oder hergestellt werden, (ii) außer der Umgehung von Schutzmechanismen keinen nennenswerten wirtschaftlichen Zweck erfüllen oder (iii) für den Einsatz bei der Umgehung von Schutzmechanismen vermarktet werden.<sup>43</sup> Der *District Court* sah alle drei Bedingungen erfüllt, weil das Anbieten oder Bereitstellen die verbotene Handlung sei. Dieses Verbot bestehe – sofern keine gesetzliche Ausnahme greife – unabhängig von dem Grund, warum das Programm geschrieben wurde.

Anschließend prüfte der *District Court*, ob der DMCA gegen den *Copyright Act* verstößt, wenn er so auszulegen sei, dass er die in § 107 des *Copyright Act* festgelegte Ausnahme der redlichen Nutzung „eliminieren“. Tatsächlich mache (das durch den DMCA geschützte) CSS einige Nutzungen unmöglich, die möglicherweise die Ausnahmekriterien erfüllten, insbesondere weil es das exakte Kopieren der gesamten Datei oder auch nur von Teilen davon verhindere. Dem *District Court* zufolge ist die redliche Nutzung eine Einrede gegen Urheberrechtsverletzungen (und als solche nach § 1201 (c)(1) DMCA ausdrücklich nicht betroffen), während der DMCA lediglich das Anbieten und Bereitstellen von Technologien verbiete, die zur Umgehung technischer Maßnahmen bestimmt seien, die den Zugriff auf urheberrechtlich geschützte Werke kontrollierten. Darüber hinaus verbiete der DMCA nur den Akt der Umgehung und nicht das Kopieren, nachdem der unberechtigte Zugriff erst einmal erfolgt sei. Ferner nenne er konkret sechs Ausnahmen, die das Konzept der redlichen Nutzung abdecken, darunter *reverse engineering*, Verschlüsselungsforschung und Sicherheitsprüfung.<sup>44</sup> Die Entstehungsgeschichte des DMCA zeige, dass der Kongress diese Liste zusammengestellt habe, um einen Ausgleich zwischen den widerstreitenden Interessen zu schaffen, und bewusst auf die Aufnahme einer weiter reichenden Einrede der redlichen Nutzung verzichtet habe.

Der *US Appellate Court* bestätigte diese Feststellungen und fügte hinzu, der *US Supreme Court* habe die Einrede der redlichen Nutzung niemals für verfassungsrechtlich erforderlich befunden.<sup>45</sup> Außerdem hätten sich die Beklagten niemals auf redliche Nutzung berufen, und die Verfügung habe eine redliche Nutzung auch nicht ausgeschlossen.

Grundsätzlich bleibe das Kopieren von CSS-geschütztem Material (zum Beispiel mit Hilfe einer Videokamera) möglich, zumal redliche Nutzung kein Recht auf Kopieren mit der optimalen Methode oder im selben Format wie das Original garantiere.

Der *District Court* musste auch zu den Links auf andere Websites, die DeCSS anbieten, Stellung nehmen. Hierzu ging er der Frage nach, ob das Linken als öffentliches Anbieten von DeCSS oder als Bereitstellung oder sonstige Weitergabe der Software im Sinne von § 1201 (a)(2) DMCA zu beurteilen sei. Seine Schlussfolgerung lautete: „Das Weitergabeverbot des DMCA greift, wenn jemand eine Umgehungstechnologie oder -vorrichtung in Kenntnis ihres Wesens präsentiert, in Aussicht stellt oder verfügbar macht, damit andere sie sich aneignen können.“ Das Gericht wandte diese Definition auf die verschiedenen Arten der Bereitstellung von Links an und gelangte zu folgendem gestaffelten Ansatz: Wenn der Link den Download von DeCSS automatisch starte, komme seine Bereitstellung der Übertragung des DeCSS-Codes zum Benutzer gleich. Dasselbe gelte auch, wenn der Link auf eine Webseite führt, die im Wesentlichen nur die Möglichkeit zum Downloaden bietet. Nur wenn der Link zu einer Seite führe, die neben einem Link zum Downloaden oder einem Link auf eine Seite zum Downloaden „noch allerlei Inhalte außer DeCSS“ enthält, sei die Sache fraglich. Da sich die Beklagten nicht auf die letztgenannte Alternative berufen hätten, verstießen die Links gegen den DMCA. Dieses Ergebnis wurde vom *US Appellate Court* bestätigt.

#### Die verfassungsrechtliche Dimension

Die Aktivitäten von Bunner und Corley wurden auch im Hinblick auf ihre vorgetragene verfassungsrechtliche Dimension überprüft. Im Grundsatz waren sich beide Berufungsgerichte einig, dass DeCSS selbst unter dem Schutz des *First Amendment* stehe. Unterschiedlich beantworteten sie jedoch die Frage, wie viel Schutz erforderlich sei und ob der Schutz der freien Meinungsäußerung sich auch auf die Bereitstellung von Links auf andere Websites erstreckte, die DeCSS anbieten.

In einem ersten Schritt von zentraler Bedeutung hatten die Berufungsgerichte zu entscheiden, ob die gerichtlichen Verfügungen, die sich auf den DMCA bzw. auf den *Uniform Trade Secrets Act* stützten, die Verbreitung von DeCSS - verstanden als Meinungsäußerung (*speech*) - verfassungswidrig eingeschränkt haben. Grundsätzlich kann ein Gesetz Beschränkungen der freien Meinungsäußerung nur anordnen, wenn bestimmte Bedingungen erfüllt sind. Diese richten sich nach der Art der betreffenden Meinungsäußerung und nach der Intensität der Prüfung, der die Ziele und Mittel der Beschränkung unterzogen werden.

Beide Berufungsgerichte befanden, es handele sich bei DeCSS um eine Meinungsäußerung, weil damit Informationen übermittelt würden, nämlich der Software-Code. Der *California Court of Appeals* stellte sogar ausdrücklich fest, es mache keinen Unterschied, dass der Beklagte ein Zweitveröffentlicher und nicht der ursprüngliche Autor von DeCSS sei. Ferner waren sich die Gerichte einig, dass DeCSS auch ein „Funktionselement“ enthalte, das keine Meinungsäußerung darstelle. Ansonsten jedoch wichen die Auffassungen und Argumentationen der beiden Gerichte voneinander ab.

Der *California Court of Appeals* engte das Element der Meinungsäußerung ganz auf den Quellcode ein, den er als die bevorzugte Sprache für die Kommunikation unter Programmierern und somit als „reine Meinungsäußerung“ bezeichnete. Er deutete an, dass der anderen Funktion des Quellcodes, nämlich der Erstellung von Objektcodes, diese Qualität fehle, weil sie keine Ideen hervorbringe. Dennoch, und trotz des fragwürdigen sozialen Wertes von DeCSS, kam er zu dem Schluss, dass das gegen Bunner verhängte Verbot der Weitergabe von DeCSS im Quellcode-Format ein Verbot der reinen Meinungsäußerung darstelle.

Der *California Court of Appeals* weigerte sich zudem, Präzedenzfälle anzuwenden, in denen Verfügungen gegen die widerrechtliche Verwendung von Geschäftsgeheimnissen bestätigt worden waren, weil in diesen Fällen durch freiwillige Vereinbarungen zur Nichtweitergabe eines Geschäftsgeheimnisses auf den Schutz des *First Amendment* verzichtet worden sei. Im Fall Bunner hingegen sei der verfassungsmäßige Schutz nicht durch eine vertragliche Nichtweitergabeverpflichtung, sondern durch das Gesetz selbst außer Kraft gesetzt worden. Auch eine Berufung auf urheberrechtliche Präzedenzfälle sei nicht möglich, weil

der *Uniform Trade Secrets Act* nicht dieselbe verfassungsrechtliche Basis wie der *Copyright Act* habe.

Der *California Court of Appeals* kam zu dem Schluss, das Verbot der Weitergabe des DeCSS-Quellcodes stelle eine apriorische Beschränkung der freien Meinungsäußerung dar, da sie bereits eingreife, bevor die Kommunikation stattfindet. Er betonte, dass die Rechtsprechung auf Einzelstaats- und Bundesebene apriorische Beschränkungen sehr negativ sehe und ihnen Verfassungswidrigkeit unterstelle. Eine apriorische Beschränkung könne nur dann aufrechterhalten werden, wenn das geschützte Interesse grundlegender sei als das *First Amendment* selbst. Dem *California Appellate Court* zufolge ist dies jedoch noch nie der Fall gewesen und trifft auch im Fall *Bunner* nicht zu.

Der *US Appellate Court* hingegen betrachtete DeCSS als gemischte Meinungsäußerung, wobei das Funktionselement die Konsequenz seiner Verwendung sei, und zwar unabhängig davon, ob DeCSS im Quell- oder im Objektcode dargestellt werde. Zudem verwies er darauf, dass ein einfacher Mausklick den DeCSS-Mechanismus, der eine verschlüsselte Videodatei automatisch entschlüsselt, in Gang setze. Er war der Auffassung, die Bestimmungen des DMCA, auf die sich das Verbot der Verwendung und Verbreitung von DeCSS stütze, zielten auf das inhaltsneutrale Element, das keine Meinungsäußerung darstelle. Sie dienten einem Zweck, der nichts mit dem Inhalt der Äußerung zu tun habe, auch wenn sie möglicherweise einen ungewollten Nebeneffekt auf einige Botschaften oder deren Verkünder hätten.

Eine Regelung kann als inhaltsneutral gelten, wenn sie (i) einem wichtigen staatlichen Anliegen dient, (ii) nicht mit der Unterdrückung der Informationsfreiheit zusammenhängt und (iii) dem Grundsatz der Verhältnismäßigkeit genügt, indem sie nicht wesentlich mehr die Meinungsäußerungsfreiheit belastet, als zur Förderung dieses Anliegens erforderlich ist.<sup>46</sup> Der *US Appellate Court* stellte fest, die Verhinderung eines unberechtigten Zugriffs auf verschlüsseltes urheberrechtlich geschütztes Material sei ein wesentliches Interesse, dem das Verbot diene. Am Rande merkte er an, der Kongress könne schließlich auch Regelungen zu Sicherheitsvorrichtungen für Waren erlassen. CSS unterscheide sich hiervon nur in der Form der Kommunikation, nicht aber im Ziel der Regelung. Außerdem bestätigte er, dass das dritte und das zweite Kriterium für eine inhaltsneutrale Regelung erfüllt seien. Insbesondere habe der *District Court* nicht das am wenigsten restriktive Mittel wählen müssen, sondern es reiche aus, dass er die Meinungsäußerungsfreiheit nicht wesentlich mehr belastet habe, als erforderlich gewesen sei. Eine interessante Fußnote (Nr. 29) zu dem Urteil deutet darauf hin, dass dieser letztgenannte Punkt unter Umständen neu bewertet werden muss, wenn die Technik in Zukunft Vorrichtungen hervorbringt, die das Anfertigen einzelner Kopien zulassen, nicht aber das Kopieren in Serie.

Der *US Appellate Court* stimmte dem *District Court* zu, dass auch die Bereitstellung von Links eine Meinungsäußerung ist, und unterstrich, dass es sich um eine gemischte Meinungsäußerung handele. Ein Link (Hyperlink) teilt die Adresse einer verknüpften Website mit (Informationsaspekt) und ruft diese Seite auch auf dem Bildschirm des Benutzers auf, wenn sie angeklickt wird (Funktionsaspekt). Der DMCA habe auch insoweit die Anforderungen an eine inhaltsneutrale Regelung erfüllt, als er das Verbot der Bereitstellung von Links autorisiere.

Der *US Appellate Court* räumte mögliche Beeinträchtigungen der freien Meinungsäußerung durch das Verbot von Links ein. So würden möglicherweise Website-Betreiber mit der Befürchtung, dass eine andere Website DeCSS anbietet, keinen Link auf diese Site setzen, sodass auch andere Informationen auf dieser Website unzugänglich blieben. Dennoch ist nach Auffassung des Gerichts die Anforderung der Verhältnismäßigkeit erfüllt. Insbesondere lehnte das Gericht es ab, die Absicht zur Schadensverursachung zur Voraussetzung zu machen, oder die Elemente anzuwenden, die ein Verbot von Printmedien erlauben. Auch schloss es sich nicht dem vom *District Court* vorgeschlagenen erhöhten Standard an. Vielmehr gelangte es zu dem Schluss, dass eine Entscheidung zwischen einer gewissen Beeinträchtigung der Kommunikation und der Duldung der Entschlüsselung getroffen werden müsse, bei der es sich aber um eine politische Entscheidung handele, die dem Kongress überlassen werden müsse. Der Kongress habe sich jedoch durch die Verabschiedung des DMCA für den Schutz der Verschlüsselung entschieden.

## Fazit

Die Rechtsprechung zu Peer-to-Peer-Systemen zeigt, dass die Innovationen bei der Software und der Technologie, die zum Austausch von Dateien über das Internet verwendet werden, in Bezug zu juristischen Konzepten zur Bekämpfung von Urheberrechtspiraterie zu setzen sind. Softwareentwickler haben versucht, den Online-Tausch von Audio- und audiovisuellen Dateien gegen juristische Überprüfungen abzusichern, indem sie Systeme wie Napster und Grokster konzipiert haben. Die audiovisuelle Industrie, die die Kontrolle über urheberrechtlich geschützte Werke wiedererlangen wollte, wehrte sich mit der Einführung von CSS als Ergänzung des angeblich unvollständigen rechtlichen Schutzes. Als Antwort der Softwareprogrammierer folgte postwendend DeCSS. Ein Waffenstillstand ist nicht in Sicht. So haben weitere Beteiligte (die Schöpfer von CSS und DeCSS) dem Rechtsstreit um die Verbreitung von Filmen im Internet neue Nahrung gegeben.

Auch neue rechtliche Instrumente kamen hinzu. Die WIPO-Vertragsparteien haben sich verpflichtet, die rechtliche Stellung von Urheberrechtssinhabern zu stärken, indem sie einen ausreichenden Schutz für technische Maßnahmen gewährleisten. Die entsprechenden Bestimmungen des DMCA wurden bereits erörtert. Das europäische Gegenstück, Kapitel III der Richtlinie, verpflichtet die Mitgliedstaaten, einen angemessenen Rechtsschutz gegen die Umgehung technischer Maßnahmen und die Herstellung oder Weitergabe solcher Umgehungswerkzeuge vorzusehen (Art. 6). Die objektiven und subjektiven Elemente, die durch die nationale Gesetzgebung abgedeckt werden müssen, entsprechen weitgehend jenen, die auch das US-Recht vorsieht, und dies ist ein guter Grund, den Rechtsstreit um DeCSS genau zu verfolgen.

Würde der DeCSS-Prozess jedoch in Europa stattfinden, hätte er eine ganz eigene Charakteristik. Dies ist unvermeidlich, weil die WIPO-Instrumente den Interessen aller Vertragsparteien Rechnung zu tragen hatten und daher sehr allgemein formuliert sind. Außerdem versucht auch die Richtlinie selbst, die nationalen Gesetze zu harmonisieren. Ganz besonders gilt dies für Art. 6 Absatz 4, in dem sieben Beschränkungen der Urheberrechte angesprochen werden, die für die Begünstigten zugänglich bleiben müssen, vorausgesetzt, dass sie von einem Mitgliedstaat gewährt werden.<sup>47</sup> Anders als der DMCA gilt diese verbindliche Vorschrift nur für den Akt der Umgehung und lässt den Schutz gegen die Weitergabe von Zugangs- oder Kontrollvorrichtungen intakt.<sup>48</sup> Die Richtlinie überlässt es dem Ermessen der nationalen Gesetzgeber, bestimmte Formen des privaten Gebrauchs zu erlauben. In den USA dagegen liegt die weitere Feststellung der redlichen Nutzung bei den Gerichten.

Die Ausnahme des privaten Gebrauchs bzw. der redlichen Nutzung ist vermutlich das wichtigste Hilfsmittel bei der Abwägung zwischen den Interessen, die dem gegenwärtigen Rechtsstreit zugrunde liegen, nämlich jenen des Urheberrechtssinhabers und jenen der Öffentlichkeit an einigen Formen des vom Urheberrechtsschutz ausgenommenen Gebrauchs. Besonders wichtig ist das Interesse der Öffentlichkeit, wenn die freie Meinungsäußerung, eine anerkannte Säule der Demokratie, berührt ist. Koelman hat argumentiert, dass „das Urheberrecht eine Form von Informationspolitik darstellt und dem öffentlichen Interesse dient, weil es die Verfügbarkeit von Informationsprodukten maximiert, indem es einerseits ein ausschließliches Recht gewährt und damit einen Schöpfungsanreiz schafft und andererseits die Reichweite des Monopols begrenzt, welches das Urheberrecht gewährt, damit Informationen weithin verfügbar und nutzbar sind.“ Er kommt zu dem Schluss, dass „technische Schutzmaßnahmen die Kontrolle der Rechtsinhaber erweitern und das Gleichgewicht potenziell stören“.<sup>49</sup> Den Rechtsinhabern zufolge war indes ein Ungleichgewicht bereits durch das unberechtigte Kopieren audiovisueller Werke entstanden.

Das Ringen um das „richtige“ Gleichgewicht geht weiter. In den USA wurde gerade erst der *Consumer Broadband and Digital Television Act* von 2002 im Senat eingebracht. Dieses Gesetz würde die Industrie zwingen, sich über die Integration eines Kopierschutzsystems in alle Vorrichtungen für digitale Medien (Hardware und Software) zu einigen.<sup>50</sup> Das System soll unberechtigtes Kopieren verhindern, aber den rechtmäßigen Gebrauch zulassen. Noch ist das Gesetz nicht verabschiedet, doch schon heute steht unverrückbar fest, woran sich sein Erfolg messen lassen muss: Die Frage lautet schlicht, ob das Gesetz die nächste Generation von Umgehungsvorrichtungen überflüssig machen kann.

- 1) Die weltweite Herstellung von Film-DVDs beispielsweise stieg von 194 Millionen Kopien im Jahr 1999 auf 474 Millionen im Jahr 2000 und 905 Millionen im Jahr 2001 an. Siehe Statistisches Jahrbuch 2001 der Europäischen Audiovisuellen Informationsstelle, Seite 125.
- 2) Susanne Nikoltschew und Francisco Javier Cabrera Blázquez, „MP3: Redliche oder unredliche Nutzung?“, in IRIS Fokus: Urheberrechte im digitalen Zeitalter, abrufbar unter [http://www.obs.coe.int/oea\\_publ/iris/iris\\_plus/focus8\\_2000](http://www.obs.coe.int/oea_publ/iris/iris_plus/focus8_2000)
- 3) MP3 ist ein Dateiformat für komprimierte Audiodateien.
- 4) Ein Beispiel aus jüngster Zeit war die Website Movie88.com, wo eine komplette Auswahl urheberrechtlich geschützter Filme jeweils drei Tage lang für 1 USD per Streaming abgerufen werden konnte. Mittlerweile hat der Provider diese Site geschlossen.
- 5) Das System Gnutella ist in Abschnitt E des MP3-Artikels beschrieben.
- 6) Die Tonträgerindustrie hat erst vor kurzem CDs mit Kopierschutz auf den Markt gebracht. Diese CDs lassen sich auf (den meisten) normalen CD-Playern abspielen, nicht aber auf den CD-ROM-Laufwerken von Computern.
- 7) Beispiele finden sich in Abschnitt A und B des MP3-Artikels.
- 8) UMG Recordings, Inc. et al. gegen MP3.Com, Inc, Case 00 Civ. 0472 (S.D.N.Y. 2000). Eine inoffizielle Version des Urteils vom 6. September 2000 ist abrufbar unter: [http://news.findlaw.com/cnn/docs/mp3/0906\\_mp3\\_unoffruling.html](http://news.findlaw.com/cnn/docs/mp3/0906_mp3_unoffruling.html)
- 9) A&M Records, Inc. gegen Napster, Inc., 239 F.3d 1004 (9<sup>th</sup> Cir. 2001) vom 12. Februar 2001, abrufbar unter: <http://www.ce9.uscourts.gov/web/new-opinions.nsf/4bc2cbe0ce5be94e88256927007a37b9/c4f204f69c2538f6882569f100616b06?OpenDocument>. Für eine Zusammenfassung der Entscheidung siehe IRIS 2001-4: 13.
- 10) Im Fall Napster war das Berufungsgericht der Auffassung, dass die Nutzer beim Upload der Dateien das Verbreitungsrecht und beim Download das Vervielfältigungsrecht (17 U.S.C. § 106 (1) bzw. (3)) verletzt hätten.
- 11) Erinstanzliches Gericht antworten in Sachen IFPI Belgium gegen Werner Guido Beckers (ARK Nr. 99/594/C), Beschluss vom 21. Dezember 1999.
- 12) Siehe den Napster-Fall, *ibid.*, unter VII. C. Im Vorabverfahren war diese Einrede des Urheberrechtsmissbrauchs zurückgewiesen worden, weil sie gegen eine einstweilige Verfügung nicht wirksam ist. Unterdessen hat der *District Court* (Bezirksgericht) weitere Ermittlungen zu der Frage angeordnet, ob die Kläger ihre Urheberrechte missbraucht haben, um den digitalen Distributionsmarkt zu monopolisieren. Der Beschluss vom 21. Februar 2002 ist abrufbar unter: <http://www.cand.uscourts.gov/cand/tentrule.nsf/4f9d4c4a03b0cf70882567980073b2e4/31e0b537993cd73288256b6800673c73?OpenDocument>
- 13) Siehe die historische Abhandlung mit weiteren Literaturangaben von Hermann Cohen Jehoram, „Einige Grundsätze zu den Ausnahmen im Urheberrecht“, in GRUR Int 2001, S. 807.
- 14) Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABL. L 167 vom 22. Juni 2001 S. 10-19. <http://europa.eu.int/cgi-bin/eur-lex/udl.pl?REQUEST=Seek-Deliver&COLLECTION=oj&SERVICE=eurl&LANGUAGE=en&DOCID=20011167p0010>
- 15) Für die Entstehungsgeschichte und eine detaillierte Beschreibung von Art. 5 siehe Jörg Rheinbothe, „Die EG-Richtlinie zum Urheberrecht in der Informationsgesellschaft“, GRUR Int 2001, S. 733 (739-740).
- 16) Rheinbothe, *ibid.*, S. 739.
- 17) Diese beiden Theorien werden weiter unten am Fall MGM gegen Grokster erörtert.
- 18) Pub.L.No. 105-304, 112 Stat. 2860 (1998).
- 19) Siehe Erwägung 25 der Richtlinie.
- 20) *United States District Court Central District of California* (US Bezirksgericht für den Distrikt Kalifornien), Western Division, Metro-Goldwyn-Mayer Studios Inc., et al. gegen Grokster, Ltd., et al., Case No. CV 01-08541 Svw (Rnbx). Alle Gerichtsdokumente, die diesen Fall betreffen, sind zu finden unter: [http://www.eff.org/IP/P2P/MGM\\_v\\_Grokster/](http://www.eff.org/IP/P2P/MGM_v_Grokster/)
- 21) Am 4. März lehnte der *U.S. District Court* den Antrag der Beklagten auf ein Teilurteil im vorläufigen Verfahren als verfrüht ab. Das Verhandlungsprotokoll ist abrufbar unter: [http://www.eff.org/IP/P2P/MGM\\_v\\_Grokster/20020304\\_mgm\\_hearing\\_transcript.html](http://www.eff.org/IP/P2P/MGM_v_Grokster/20020304_mgm_hearing_transcript.html). Unabhängig von diesem Fall wies das Bezirksgericht Amsterdam die Firma Kazaa am 29. November 2001 an, Maßnahmen zur Beendigung der Urheberrechtsverletzungen durch nicht autorisierte Musikdateien in ihrem Netz zu ergreifen (siehe IRIS 2002-1: 13). Am 28. März 2002 wurde diese Entscheidung in der nächsten Instanz aufgehoben. Siehe [http://story.news.yahoo.com/news?tmpl=story&cid=581&u=/nm/20020328/tc\\_nm/tech\\_entertainment\\_dc\\_2](http://story.news.yahoo.com/news?tmpl=story&cid=581&u=/nm/20020328/tc_nm/tech_entertainment_dc_2)
- 22) Am 4. März 2002 wurde diese Klage mit einer ähnlichen Klage von Musikautoren und -verlegern gegen dieselben Beklagten verbunden. Alle Gerichtsdokumente, die letzteren Fall betreffen, sind zu finden unter: [http://www.eff.org/IP/P2P/NMPA\\_v\\_MusicCity/](http://www.eff.org/IP/P2P/NMPA_v_MusicCity/)
- 23) Siehe Gershwin Publ'g Corp. gegen Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971).
- 24) Sony Corporation of America gegen Universal City Studios, Inc., 464 U.S. 417, 104 S. Ct. 774, 78 L. Ed. 2d 574 (1984), vom 17. Januar 1984, abrufbar unter: [http://www.eff.org/Legal/Cases/sony\\_v\\_universal\\_decision.html](http://www.eff.org/Legal/Cases/sony_v_universal_decision.html)
- 25) Siehe Gershwin Publ'g Corp. gegen Columbia Artists Mgmt., Inc.
- 26) Der *Court of Appeals* zitiert hier das Urteil im Fall Fonovisa, Inc. gegen Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996), abrufbar unter: [http://www.law.cornell.edu/copyright/cases/76\\_F3d\\_259.htm](http://www.law.cornell.edu/copyright/cases/76_F3d_259.htm)
- 27) Fred von Lohmann, *Sharing and Copyright Law after Napster*, abrufbar unter: [http://www.eff.org/IP/P2P/Napster/20010227\\_p2p\\_copyright\\_white\\_paper.html](http://www.eff.org/IP/P2P/Napster/20010227_p2p_copyright_white_paper.html)
- 28) Näheres hierzu siehe unter [http://www.eff.org/IP/Video/DeCSS\\_prosecutions/Johansen\\_DeCSS\\_case/20020110\\_eff\\_pr.html](http://www.eff.org/IP/Video/DeCSS_prosecutions/Johansen_DeCSS_case/20020110_eff_pr.html).
- 29) Gesetz vom 22. Mai 1902 Nr. 10, geändert durch die Gesetze vom 16. Februar 1979 Nr. 3 und vom 12. Juni 1987 Nr. 54.
- 30) Der norwegische Originaltext und eine englische Übersetzung finden sich in der Erklärung Jon Bings vom 18. Januar 2000, abrufbar unter: [http://www.eff.org/IP/Video/DVCCA\\_case/20000118\\_bing\\_norway\\_law\\_decl.html](http://www.eff.org/IP/Video/DVCCA_case/20000118_bing_norway_law_decl.html)
- 31) Siehe die englische Übersetzung des Schreibens ihres Anwalts an ØKOKRIM unter: [http://www.eff.org/IP/DeCSS\\_prosecutions/Johansen\\_DeCSS\\_case/20000104\\_dvdcca\\_no\\_prosecutor\\_letter.en.html](http://www.eff.org/IP/DeCSS_prosecutions/Johansen_DeCSS_case/20000104_dvdcca_no_prosecutor_letter.en.html).
- 32) Zu weiteren Details der rechtlichen Fragen siehe die Erklärung Jon Bings; Endnote 30.
- 33) *Santa Clara County Superior Court* (erstinstanzliches Gericht), Anordnung einer vorläufigen Verfügung für den Kläger gegen die Beklagten, in DVCCA gegen McLaughlin, Bunner et al., abrufbar unter: [http://www.eff.org/IP/Video/DVCCA\\_case/20000120-pi-order.html](http://www.eff.org/IP/Video/DVCCA_case/20000120-pi-order.html).
- 34) *Court of Appeal of the State of California Sixth Appellate District* (Berufungsgericht für den Sechsten Bezirk des Staates Kalifornien), Beschluss zur Aufhebung der Verfügung im Fall DVCCA gegen Bunner, abrufbar unter [http://www.eff.org/IP/Video/DVCCA\\_case/20011101\\_bunner\\_appellate\\_decision.pdf](http://www.eff.org/IP/Video/DVCCA_case/20011101_bunner_appellate_decision.pdf)
- 35) Siehe Newsbytes.com unter <http://www.newsbytes.com/news/02/174688.html>.
- 36) Universal City Studios, Inc. gegen Reimerdes, 111 F. Supp. 2d 346 (S.D.N.Y. 2000).
- 37) *United States Court of Appeals for the Second Circuit*, Docket No. 00-9185, Universal City Studios, Inc. gegen Reimerdes.
- 38) Quellcode ist der Text eines Computerprogramms in einer Programmiersprache. Damit dieser Code für den Computer verständlich ist, muss er in maschinenlesbare Folgen von Nullen und Einsen, den sogenannten Objektcode, übersetzt werden.
- 39) Der Originaltext des Gesetzes ist abrufbar unter <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=03001-04000&file=3426-3426.11>
- 40) Siehe die Zusammenfassung der US-Urheberrechtsbehörde: *US Copyright Office Summary, The Digital Millennium Copyright Act of 1998*, Dezember 1998, S. 4 ff.
- 41) Siehe § 1201 (a)(1)(A).
- 42) Zur Definition der Umgehung siehe § 1201 (a)(3).
- 43) Siehe § 1201 (a)(2) und § 1201 (b)(1).
- 44) Das Gericht lehnte die Aussage ab, dass die Bereitstellung von DeCSS als Verschlüsselungsforschung oder als Sicherheitsprüfung zu betrachten und somit gerechtfertigt sei. Zu den anderen Ausnahmen siehe § 1201 (d) bis (j).
- 45) Der *California Appellate Court* dagegen, obwohl im Grunde nicht mit Urheberrechten sondern mit Geschäftsgeheimnissen befasst, hat hervor, die Theorie von der redlichen Nutzung habe im Hinblick auf ihre *First-Amendment*-Implikationen dazu gedient, Unterlassungsverfügungen in Prozessen wegen Urheberrechtsverletzung (freie Meinungsäußerung) zu bestätigen, und stellte in diesem Zusammenhang fest, Art. I § 8 cl. 8 der US-Verfassung verleihe dem *Copyright Act* verfassungsrechtliche Autorität.
- 46) Turner Broadcasting System, Inc. gegen FCC, 512 U.S. 622, 662 (1994), Zitat aus Ward gegen Rock Against Racism, 491 U.S. 781, 799 (1989).
- 47) Diese Ausnahmen sind Reprographien, öffentliche Einrichtungen und Archive, ephemere Aufzeichnungen, nicht kommerzielle soziale Einrichtungen, Lehre und Forschung, die Nutzung durch behinderte Menschen sowie die Nutzung zu Zwecken der öffentlichen Sicherheit und der Sicherstellung von Verfahren.
- 48) Die Ausnahmen des DMCA richten sich nach der Unterscheidung zwischen „Zugriffs“- und „Kopier“-Kontrolle. Die meisten gelten auch für das Weitergabeverbot. Näheres hierzu siehe § 1201 (d) bis (j) DMCA.
- 49) Siehe Kamil J. Koelman, *A Hard Nut to Crack: The Protection of Technological Measures*, EIPR 2000, S. 272-280 (279).
- 50) Der Entwurf ist abrufbar unter: <http://www.politechbot.com/docs/cbdtpa/hollings.s2048.032102.html>