

Filesharing

Möglichkeiten und Grenzen des digitalen Datenaustausches mit dem Medium Internet

Eingereicht von

Michael Linhart

Kennzahl J151

Matrikel-Nr.: 9850116

am Institut für Informationswirtschaft

an der WIRTSCHAFTSUNIVERSITÄT WIEN

Studienrichtung: Betriebswirtschaft

Begutachter: Priv.Doz. Dr. Michael Hahsler

Wien, im Juni 2007

WIRTSCHAFTSUNIVERSITÄT WIEN

DIPLOMARBEIT

Titel der Diplomarbeit:

Filesharing
Möglichkeiten und Grenzen des digitalen Datenaustausches
mit dem Medium Internet

Verfasserin/Verfasser: Michael Linhart

Matrikel-Nr.: 9850116

Studienrichtung: Betriebswirtschaftslehre

Beurteilerin/Beurteiler: Priv.Doz. Dr. Michael Hahsler

Ich versichere:

dass ich die Diplomarbeit selbstständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfe bedient habe.

dass ich dieses Diplomarbeitsthema bisher weder im In- noch im Ausland (einer Beurteilerin/ einem Beurteiler zur Begutachtung) in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

dass diese Arbeit mit der vom Begutachter beurteilten Arbeit übereinstimmt.

Datum

Unterschrift

Zusammenfassung

Die vorliegende Arbeit ist eine ausführliche, kritische und wissenschaftliche Darstellung und Analyse aller wesentlichen Bereiche des Filesharings. Es werden die unterschiedlichen Möglichkeiten aufgezeigt, die der komplexe Bereich des Filesharings bieten kann. Beleuchtet werden jedoch auch die Grenzen, welche man mit diesem Vorgang nicht überschreiten sollte. Definitionen, Funktionen und Technologien, Recht und Ökonomie werden dabei anhand von Sekundärliteratur aus dem Bereich DRM und den beteiligten Fachgebieten, wie der Informatik (z.B. Kryptographie), Recht, Volkswirtschaftslehre usw. dargestellt und auf den Bereich Filesharing übertragen. Es sollen aber auch Fragen beantwortet werden, warum sich diese Art von Netzwerk bei so vielen Personen weltweit einer so großen Beliebtheit erfreut. Der Leser soll durch sein erworbenes Wissen in die Lage versetzt werden, die Probleme des Datenaustausches beim Namen zu nennen und dadurch das Unrechtbewusstsein für illegale Aktivitäten zu stärken.

Schlüsselwörter:

Peer-to-Peer, Internet, Tauschbörsen, Raubkopien, Urheberrecht, Cracker, Release, Warez, Filesharing, Verschlüsselung, Copyright

Abstract

This diploma thesis is a detailed, critical and scientific representation and analysis of all essential areas of Filesharing. It shows the different possibilities the complex area of Filesharing can offer for everyone. However, the limits, which should not be exceeded with this medium, are also examined. Definitions, functions and technologies, law and economy are represented and transferred to the area of Filesharing by using secondary literature from the area of DRM and the branches involved such as computer science (e.g. cryptography), law, political economy etc. Furthermore the question why this kind of network enjoys such a big popularity worldwide should be answered. Through gaining adequate knowledge the reader should be able to recognize the problems of data exchange and to strengthen awareness towards illegal activities in that field.

Keywords:

Peer-to-peer, internet, exchanges, pirate-copies, copyright, cracker, release, warez, file-sharing, coding, copyright

Inhaltsverzeichnis

1	EINLEITUNG	1
1.1	Ziele der Arbeit	2
1.2	Gang der Untersuchung	2
1.3	Zur Verwendung englischer Begriffe.....	3
2	DIE THEMATIK DES INTERNETS UND VON RAUBKOPIEN	5
2.1	Das Internet.....	5
2.2	Digitale Kopie.....	14
2.3	Der Begriff Raubkopie	14
2.4	Die ersten Cracker	15
2.5	Der Ursprung und der Verteilungsweg von Raubkopien.....	20
3	FILESHARING – TECHNISCHE GRUNDLAGEN UND VORAUS- SETZUNGEN.....	27
3.1	Datenkomprimierung und schnelle Internetzugänge	28
3.2	Arten von Filesharing-Systemen	33
3.3	Peer Typologien	38
3.4	Technische Infrastruktur des Filesharings.....	42
3.5	Kryptografie.....	47
3.6	Technischer Ablauf beim Filesharing	50
3.7	Verwendete Programme und deren Funktion.....	52
3.8	Anonymität beim Filesharing	55
3.9	Wie kommen die Dateien in die Tauschbörsen?	57
4	URHEBERRECHT	59
4.1	Internationale Verträge und Copyright in den USA	60
4.2	Urheberrecht in Europa	64
4.3	Urheberrecht in Österreich.....	65
4.4	Aktuelle Probleme im Urheberrecht.....	66
4.5	Ausblick Urheberrecht.....	69

5	RECHTLICHE GRUNDLAGEN ZUR VERVIELFÄLTIGUNG UND BEWERTUNG DES FILESHARINGS AUS URHEBERRECHTLICHER SICHT	71
5.1	Der Eigentumsbegriff	72
5.2	Schutzprinzipien im Internet.....	73
5.3	Abruf eines digitalen Werkes.....	75
5.4	Anbieterseite.....	76
5.5	Abnehmerseite.....	79
5.6	Haftung des Anbieters der Filesharingsoftware.....	84
5.7	Ergebnis	86
5.8	Ist ein Verbot der digitalen Privatkopie angezeigt?.....	87
5.9	Rechtliche Grundlagen der Vervielfältigung zum privaten Gebrauch.....	93
5.10	Das Vervielfältigungsrecht des Urhebers	93
5.11	Die Schranke der Vervielfältigung zum privaten Gebrauch als Einschränkung des Vervielfältigungsrechts	94
5.12	Zuständigkeit österreichischer Gerichte.....	97
5.13	Handlungsoptionen des Gesetzgebers in Urheberrecht aus rechtsökonomischer Sicht .	99
5.14	Zusammenfassung	101
6	INTERNATIONALE GESETZE, ABKOMMEN UND ORGANISATIONEN, WELCHE SICH MIT DER THEMATIK DES FILESHARINGS AUSEINANDERSETZEN	103
6.1	Internationale Entwicklungen	103
6.2	Organisationen.....	106
7	SCHUTZMÖGLICHKEITEN GEGEN UNGEWOLLTE VERVIELFÄLTIGUNG.....	110
7.1	Digital Right Management.....	110
7.2	Problematik und Gründe der Entstehung.....	112
7.3	Definitionen	115
7.4	Funktion-Technologie-Matrix	121
7.5	Das Problem der Standardisierung.....	121
7.6	Wirtschaftliche Aspekte des DRM	122
7.7	Zusammenfassung	123

8	WIRTSCHAFTLICHE, ÖKONOMISCHE UND SOZIOLOGISCHE BETRACHTUNGSWEISEN DES FILESHARINGS.....	126
8.1	Das ökonomische Problem virtueller Waren.....	126
8.2	Ökonomische Aspekte des Filesharings.....	127
8.3	Rechtliche Schutzmöglichkeiten.....	132
8.4	Kampagne: Raubkopierer sind Verbrecher!	136
9	ANALYSE DES FILESHARINGS	140
9.1	Philosophie und Psychologie des Kopierens.....	140
9.2	Raubkopieren.....	143
9.3	Kosten des Anbietens von Dateien.....	150
9.4	Nutzen des Anbieters von Dateien.....	152
9.5	Maßnahmen gegen Freerider	154
9.6	Legal oder Illegal	156
10	SCHÄTZUNG FÜR DEN VERURSACHTEN MARKTSCHADEN	159
11	ZUSAMMENFASSUNG UND FAZIT	169
	LITERATURVERZEICHNIS.....	175
	ABBILDUNGSVERZEICHNIS	196
	TABELLENVERZEICHNIS	196

1 Einleitung

Filesharing ist seit dem Aufkommen der Internettauschbörse „Napster“ kontinuierlich in den Medien präsent. Das Interesse an dieser „Musiktauschbörse“ ist nicht verwunderlich, da sich kaum an einem anderen Angebot, wie Napster & Co, der rasante Fortschritt digitaler Vervielfältigungs- und Verbreitungstechniken aufzeigen lassen. Während früher die Bedeutung des Kopierens und Tauschens von Schallplatten oder Videokassetten durch die zum Teil schlechte Qualität der Kopie eher begrenzt war, findet sich eine solche Einschränkung im digitalen Zeitalter nicht mehr. Digitale Vervielfältigungstücke entsprechen nicht nur dem Original wie ein Ebenbild, sondern lassen sich auch mit wenig Aufwand beliebig über das Medium Internet verbreiten. Dabei spielen Entfernungen, wie sie in der analogen Ära relevant waren, keine Rolle mehr. Filesharingnetzwerke im Internet potenzieren diesen Effekt, indem sie Angebot und Nachfrage gezielt weltweit zusammenführen. Die Handhabung dieser Software lässt sich in kürzester Zeit ohne größere Schwierigkeiten aneignen. Danach stehen für den Benutzer durch die Lokalisierung der gesamten Inhalte selbst ungewöhnlichste Dateien zum Download bereit. So interessant und aufregend diese Möglichkeiten für jeden einzelnen sind, so problematisch ist die Entwicklung dieser neuartigen Strukturen für die Rechtswissenschaft, denn diese moderne Kommunikationsform lässt sich nicht problemlos in das bisherige Rechtssystem einordnen.

Die Informationsindustrie ist ein in sich international ausgerichteter Wirtschaftssektor. Informationen sind ihrer Natur nach ubiquitär, d.h. überall verbreitet. Sie können ohne hohen Kostenaufwand reproduziert und, zum Beispiel über internationale Datennetze, in wenigen Sekunden transferiert werden. Gerade technische Innovationen wie die Satellitenübertragung oder das Internet zeigen deutlich, dass nationale Grenzen keine besondere Bedeutung mehr haben.

Wir sind fast immer und überall erreichbar, erhalten rund um die Uhr Informationen zu allen erdenklichen Themen oder können sie, wenn erforderlich, jederzeit abrufen. Das Informationszeitalter kennt weder nationale, noch kulturelle, noch ethnische, noch ökonomische Grenzen. Weltweite Vernetzung und Verfügbarkeit aller Informationen öffnet die Märkte, schärfere Konkurrenz treibt technologische Innovationen und Produktivität voran. In dieser Welt räumlich und zeitlich unbegrenzter

Informationsmöglichkeiten wird die Rangfolge ganzer Staaten und Gesellschaften neu bestimmt.

1.1 Ziele der Arbeit

Ziel dieser Arbeit ist es, eine ausführliche, kritische und wissenschaftliche Darstellung und Analyse aller wesentlichen Bereiche des Filesharings zu liefern. Dabei werden die verschiedenen Möglichkeiten aufgezeigt, welche der komplexe Bereich des Filesharings für jeden einzelnen bieten kann. Des Weiteren werden jedoch auch die Grenzen beleuchtet, welche man mit diesem Medium nicht überschreiten sollte. Definitionen, Funktionen und Technologien, Recht und Ökonomie werden dabei anhand von Sekundärliteratur aus dem Bereich DRM und den beteiligten Fachgebieten, wie der Informatik (z.B. Kryptographie), Recht, Volkswirtschaftslehre usw. dargestellt und auf den Bereich Filesharing übertragen. Weiters sollen Fragen beantwortet werden, warum sich diese Art von Netzwerk bei so vielen Personen weltweit einer so großen Beliebtheit erfreut.

1.2 Gang der Untersuchung

In *Kapitel 2* soll zunächst kurz eine Vorstellung des Mediums Internet erfolgen, sodass die Eigenart dieses Netzwerkes und die damit verbundenen Probleme verständlich werden. Es wird weiters versucht, eine Grundlage zu schaffen, auf welcher sich die spezifische Problematik erläutern lässt.

Kapitel 3 befasst sich mit den technischen Grundlagen und Voraussetzungen, welche benötigt werden, um an einem gewöhnlichen Tauschvorgang im Internet teilnehmen zu können. Dabei wird - soweit es der Umfang dieser Arbeit erlaubt - auf die technische Infrastruktur des Filesharings eingegangen.

Kapitel 4 behandelt die Thematik des Urheberrechtes der verschiedenen Länder und geht dabei auch auf die geschichtlichen Hintergründe ein.

In *Kapitel 5* werden die rechtlichen Grundlagen zur Vervielfältigung und Bewertung des Filesharings aus urheberrechtlicher Sicht näher erläutert. Dabei wird auf die in der Praxis rasant zunehmende Zahl der Urheberrechtsverletzungen hingewiesen.

Kapitel 6 erläutert Internationale Gesetze, Abkommen und Organisationen, welche sich mit dem Thema Filesharing auseinandersetzen.

Kapitel 7 setzt den Schwerpunkt in der Darstellung von rechtlichen und vor allem auch technischen Schutzmöglichkeiten, durch die Industrie ihre Produkte vor einer missbräuchlichen Vervielfältigung schützen kann. Im weiteren Verlauf dieses Kapitels werden die rechtlichen Implikationen von DRMS in Bezug auf das Urheberrecht herausgearbeitet.

In *Kapitel 8* werden die wirtschaftlichen, ökonomischen und soziologischen Betrachtungsweisen des Filesharing analysiert. Auch hier ist die Zielsetzung, die bestehenden Zusammenhänge zu analysieren sowie die wesentlichen Informationen für den einzelnen Benutzer herauszuarbeiten. Daran schließt sich noch ein kurzer Abriss der österreichischen Zuständigkeit solcher Vorgänge im Internet an. Denn durch die weltweiten Auswirkungen, die jede einzelne Datenübermittlung haben kann, könnte eine konkurrierende Zuständigkeit mehrerer Staaten gegeben sein.

Kapitel 9 beschäftigt sich mit einer Analyse des Filesharings. Dabei soll ein Problembereich, der derzeit in der Öffentlichkeit besonders diskutiert wird, nämlich „das Raubkopieren“, und zwar mit Hauptaugenmerk auf die Hintergründe für diese Verhaltensweise, näher untersucht werden. Nach einer Bestandsaufnahme von Art und Umfang des vorhandenen Missbrauchs wird nach Gründen und Erklärungen gesucht.

Kapitel 10 versucht eine Schätzung für den verursachten Marktschaden, welchen die Industrie jährlich erleidet, zu liefern.

Eine Zusammenfassung der Ergebnisse in *Kapitel 11* beschließt diese Arbeit.

1.3 Zur Verwendung englischer Begriffe

Da sich diese Diplomarbeit mit der Thematik von neuen Medien auseinandersetzt, welche meistens einen großen Bezug zur englischen Sprache aufweisen, wurden die meisten englischen Begriffe synonym für deutsche Wörter verwendet. Es wurde daher im Folgenden weitgehend darauf verzichtet, englische Fachbegriffe in die deutsche Sprache zu übersetzen. Auf der einen Seite ist der Großteil der zu diesem Thema veröffentlichten Literatur englischsprachig, die Verwendung von Übersetzungen könnte daher den Rückgriff auf vertiefende Literatur erschweren, auf der anderen Seite werden in den deutschsprachigen Veröffentlichungen zumeist ebenfalls die englischen

Originalbegriffe verwendet. Deshalb würden die übersetzten Begriffe, sofern eine sinnvolle Übersetzung überhaupt möglich ist, meist sehr ungewohnt klingen.

2 Die Thematik des Internets und von Raubkopien

2.1 Das Internet

Um bestimmte Entwicklungen und Risiken des Internets besser verstehen zu können, hilft ein kurzer Blick in die Geschichte.

2.1.1 Die Geschichte des Internets

Das Internet verselbständigte sich nicht einfach von gestern auf heute. Vielmehr wurde es vorsätzlich als freies Medium geschaffen. In einer Gemeinschaftsarbeit des Verteidigungsministeriums und der Universität MIT wurde 1962 der Vorläufer des heutigen Internets mit dem Namen ARPANET (Advanced Research Project Agency Network) gestartet. [KrSe06, 146-147]. Mit diesem Projekt wollte man ein ausfallsicheres Computerkonglomerat schaffen, das auch im militärischen Ernstfall noch benutzbar ist. Das perfekte Kommunikationssystem sollte dezentral aufgebaut sein, um keinen zentralen Knotenpunkt als Schwachstelle zu bieten. Durch diesen Grundgedanken angeregt, wurde ein neues System entwickelt, welches aus mehreren verbundenen Stützpunkten bestand. Dabei erhielt keine der Einheiten des Netzwerkes eine zentrale Autorität oder Steuerungsaufgabe, jede sollte eigenständig funktionieren [Wiki06r].

Das Endresultat war das erste dezentrale Computernetzwerk der Welt. Es bestand aus den vier Universitäten: University of Utah, University of California in Santa Barbara, University of California in Los Angeles und dem Stanford Research Institute. Durch die vorhandene dezentrale Struktur des ARPANET war eine schnelle und effiziente Ausdehnung gewährleistet. Nachdem ursprünglich nur vier Computer über dieses Netzwerk verbunden waren, vermehrte sich die Zahl, als das Netz auch im universitären Bereich genutzt wurde. Dort sollte der Zugriff auf eine große Menge an Rechenleistung durch den Zusammenschluss mehrerer Großrechner die Lösung wissenschaftlicher Probleme erleichtern. Im Jahr 1972 waren aus den vier Knotenpunkten bereits 37 geworden. Zwölf Jahre später bestand das Netzwerk schon aus über 1.000 Knoten, und am Anfang der 90er Jahre wurde die magische Grenze von einer Million Knotenpunkten überschritten. Inzwischen ist die tatsächliche Anzahl der Knotenpunkte auf mehr als 500 Millionen angewachsen [Wiki06s].

Am Anfang kannte man lediglich die Dienste Telnet und FTP, erst später kam auch das heute am meisten genutzte Service, E-Mail, hinzu. Zu Beginn der 80er Jahre beschloss das Verteidigungsministerium schließlich, die militärischen Bereiche abzukoppeln, daraus wurde das Milnet, die restlichen Teile verblieben der Forschung und Lehre. Im Jahre 1986 wurden die fünf größten Computer der USA der damaligen Zeit im NSFNet (National Science Foundation Network) verbunden, die Leistungsfähigkeit der Verbindungen wurde sukzessive gesteigert. Immer mehr Netzwerke schlossen sich diesem Verbund an, schließlich auch europäische Länder, bis das Internet heute eine Teilnehmerzahl von vielen Millionen erreicht hat. Aber erst in letzter Zeit wird versucht, die ungeahnten Möglichkeiten, welche das Netz bietet, auch kommerziell zu nutzen. *“The web is the most important innovation in mass media since the Gutenberg printing press, because it puts mass media into everyones hands”* [Pere05, 123-124]. Das heutige Internet eröffnet daher nicht abschätzbare Optionen, welche es in dieser einzigartigen Form noch nie gegeben hatte. Es ermöglicht es den Menschen, sich mit anderen Personen zu vernetzen. Dadurch wird der Austausch von Informationen und Wissen gefördert, ohne dabei räumlich begrenzt zu sein.

2.1.2 Was ist das Internet?

„Es gilt als der Inbegriff der Modernität, hat visionären Charme und haucht den Odem der Weltläufigkeit: das Internet.“ [Lorz99, 247].

Wie die Entstehungsgeschichte schon zeigt, wurde das Internet durch den Zusammenschluss vieler kleiner und größerer Netzwerke gebildet. Auf der untersten Ebene sind firmeneigene oder universitäre Computerverbunde zu nennen. Diese werden wiederum zu einem etwas größeren Netzwerk verbunden. Dieser Vorgang wiederholt sich, bis schließlich alle Teilnetze zu einem Ganzen zusammengefügt sind. Die obersten Verbindungen werden „Backbones“ (engl. für Rückgrat) genannt, in Europa verbindet etwa das „Ebone“ die größten Metropolen miteinander. Jedes dieser Netze stellt Ressourcen an die Netzgemeinde zur Verfügung und wird von der jeweiligen betreibenden Institution gewartet. Aufgrund dieser Tatsache besitzt das Internet auch keine zentrale Administration oder gar einen Eigentümer. Infolgedessen gibt es auch

keine zentrale Aufsicht, die etwa die Inhalte der transportierten Mitteilungen auf Konformität mit geltenden Rechtsvorschriften überprüfen könnte.

Es ist nochmals festzuhalten, dass mit dem Begriff „Internet“ die Vernetzung der Computer an sich bezeichnet wird und nicht eine der Anwendungen, welche dieses Netzwerk schließlich nutzen, wie etwa WWW. Dieser Irrtum ist oftmals anzutreffen, soll aber im Rahmen dieser Arbeit vermieden werden. Da das Internet nun nicht organisiert ist, sondern einen offenen Verbund darstellt, ist es nicht einfach, alle Computer festzustellen, die dazuzuzählen sind. Die einzige gemeinsame Basis, die alle Rechner des Internets verbindet, besteht darin, dass sie sich untereinander mittels so genannten TCP/IP Protokollen verständigen. Unter dieser Bezeichnung wird eine ganze Familie von Protokollen zusammengefasst, deren wichtigste, das transmission control protocol (TCP) und das Internet protocol (IP), als Namensgeber herangezogen wurden. Das Internet ist, anders als der Name suggeriert, kein festes abgeschlossenes Netzgebilde, sondern vielmehr ein Zusammenschluss vieler Netze, die wiederum aus einer großen Anzahl von Computern bestehen können. Es ist aus dem privaten und wirtschaftlichen Leben mittlerweile kaum mehr wegzudenken. Gerade in jüngeren Bevölkerungsschichten ist die Kommunikation über das digitale Netz alltäglich geworden. Internet bedeutet eine bis dato unbekannte Informationsmöglichkeit. Durch den dezentralen Aufbau des Internets ist eine Inhaltskontrolle kaum möglich, das Prinzip der Meinungsfreiheit wird in der Reinkultur praktiziert. Wissen wird ohne Zeitverlust weltweit verfügbar, wobei die urheberrechtliche Missbrauchsgefahr schon offensichtlich wird. Informationen sind nicht mehr ortsgebunden, können daher jederzeit und überall aus fast unendlich vielen Quellen abgerufen werden. *„Diese Offenheit, einerseits einer der großen Vorteile des Internets, lässt sich andererseits kaum kontrollieren und birgt viele Risiken für die Wirtschaft.“* [Hart01, 24]

Das Potential des Internets ist noch lange nicht erschöpft, wichtige Einsatzmöglichkeiten befinden sich noch in den ersten Entwicklungsstufen. Der Einblick in die Forschungs- und Versuchsprojekte lässt den Umfang der Weiterentwicklung des Datennetzes zu einem allumfassenden Multiservicenet mit vereinter Sprach-, Daten- und Videoübertragung ansatzweise erahnen. Sicher ist jedoch schon jetzt, dass sich die Lebens- und Kommunikationsverhältnisse von immer mehr Menschen dadurch nachhaltig verändern werden.

„Das Internet ist bei näherem Hinsehen ein virtuelles Spiegelbild der Realität – mit allen Absonderlichkeiten eben dieser. Im Unterschied zur Realität geschehen die Dinge

dort viel anonym, dadurch ungehemmt. In der Realität ist unser Leben durch Regeln des Zusammenlebens geschützt – oder beschränkt, je nach Sichtweise. Da es eine junge Gesellschaftsform ist, fehlen diese Regelnwerke in der virtuellen Realität fast völlig. ... Gefahrenpotenziale entstehen überall dort, wo Fachwissen und Sicherheitslücken auf kriminelle Energie treffen. Gelegenheit macht Diebe.“ [Hart01, 109]

2.1.3 Die Grundlagen - TCP/IP/UDP

Unter dem Schlagwort TCP/IP fasst man also alle Protokolle zusammen, mit Hilfe derer sich die Computer untereinander im Internet verständigen. Die Architektur in TCP/IP-Netzen besteht aus vier Schichten. Zuunterst befindet sich der Netzzugang, der nicht weiter spezifiziert ist. Dieser behandelt die physikalische Übertragung von Informationen zwischen den einzelnen Computern. Darauf baut die Internet-Protocol-(IP)-Schicht auf. Diese kümmert sich um die Aufteilung der Daten in die Pakete und versieht diese mit der Empfangsadresse. Das IP fungiert dabei also als Routingprotokoll, kennzeichnet Absender (Quell-IP-Adresse) und Adressat (Ziel-IP-Adresse) und leitet die Daten über die verschiedenen Router durch das Netz. Jede einzelne IP-Adresse besteht aus vier durch Punkte getrennten dreistelligen Zahlen (zwischen 001 und 255), d.h. jede Adresse ist 32 Bit groß und bezeichnet exakt einen im Internet angeschlossenen Personalcomputer. Theoretisch sind somit heute bis zu 4 Milliarden Computer eindeutig identifizierbar. Da die 32 Bit großen IP-Adressen für den alltäglichen Gebrauch recht unhandlich und vor allem schwer zu merken sind, wurde 1986 ein System entwickelt, durch welches einfache Buchstaben- und Zahlenkombinationen auf routenfähigen IP-Adressen abgebildet werden, um eine höhere Kundenfreundlichkeit für den Nutzer zu erreichen. Diese Zeichenkombinationen werden Second-Level-Domains oder auch nur kurz Domainnamen genannt und bestehen aus fast beliebig wählbaren Namen. Im Zuge des rasanten Wachstums des Internets wird jedoch über eine Ausweitung des Schemas auf ein Ipv6-System mit 128 Bitadressen nachgedacht, womit theoretisch 667 Milliarden Adressen pro Quadratmillimeter Erdoberfläche bzw. $6,5 \times 10^{28}$ Adressen pro Mensch möglich werden [Wiki06h; Wiki06i].

Auf diesem Fundament wiederum baut das Transport Control Protocol (TCP) auf. Dieses übernimmt die Funktion, die einzelnen Pakete durchnummerieren, sie mit einem Fehlercode zu versehen, beziehungsweise sie auf der gegenüberliegenden Seite wieder entsprechend ihrer Reihenfolge nach Überprüfung der Fehlercodes zusammensetzen und etwaige abgängige Pakete nachzufordern oder doppelte Pakete auszuscheiden. Auf diesen Aufbau setzt nun das Protokoll der jeweiligen Anwendung auf. Das User Datagram Protocol (Abk. UDP) ist ein minimales, verbindungsloses Netzprotokoll, das ebenfalls wie TCP zur Transportschicht der Internetprotokollfamilie gehört. Die Aufgabe von UDP ist es, Daten, welche über das Internet übertragen werden, der richtigen Anwendung zukommen zu lassen [Wiki07a].

2.1.4 Anschluss an das Internet

Nachdem die Grundzüge der Struktur des Internet verdeutlicht wurden, stellt sich die Frage, wie der einzelne Nutzer dieses Netz verwenden kann. Zunächst einmal bedarf es eines Anschlusses an das Internet. Solche werden mittlerweile in vielen Firmen, deren internes Netzwerk Teil des Internet geworden ist, angeboten, ebenso sind viele Universitäten vernetzt und bieten den Studenten und Lehrenden eine Auffahrt auf den Datenhighway.

Für den Privaten bieten so genannte „Provider“ gegen Entgelt den Zugang zum Internet sowie gewisse Unterstützung im Umgang mit diesem an. Exemplarisch für die verschiedenen Anschlüsse an das Internet wird die Verbindung mit einem gewöhnlichen Modem kurz beschrieben. In den Anfängen des Internets benötigte man dazu außer eines PC, einer Telefonleitung und eines Modems nur noch die notwendige Kommunikationssoftware. Das Modem wurde einerseits an den Computer angeschlossen, andererseits mit der Telefonleitung verbunden. Die Kommunikationssoftware wählte nun die Telefonnummer des Providers. Am anderen Ende meldete sich das dortige Modem des Providers, welches wiederum an dessen Computer angeschlossen war, und diese beiden Rechner standen nun in Kontakt. Der Computer des Providers war durch die Verbindung über ein leistungsstarkes Kabel Teil eines Netzwerkes, das wiederum Teil des Internets war. War der Kunde nun mit dem Provider verbunden, so war er auch schon mitten im Internet. Heutzutage gibt es jedoch bereits mehrere Möglichkeiten, um ins World Wide Web zu gelangen, welche jedoch

einzelnen erklärt, den Rahmen dieser Arbeit sprengen würden und deshalb zusammenfassend dargestellt werden können:

- per Glasfaserkabel
- per Satellit
- per Stromleitung
- per Funk (z.B.: Wireless Lan)
- per Telefonleitung
- per Koax-TV Kabel

Der Anschluss aller Nutzer an Glasfaser-Netze ist zwar eine Vision, welche seit Bestehen dieser Technik immer wieder als „ultima ratio“ auftaucht, aber dennoch aus Kostengründen immer wieder verworfen wird.

2.1.5 Welche Möglichkeiten bietet das Internet?

Das Internet ermöglicht einerseits, auf die Rechenleistung angeschlossener Großcomputer zuzugreifen, andererseits die unüberschaubare Menge der darauf gespeicherten Daten und Informationen zu nutzen. Die komplexe Steuerung des Datenverkehrs im Internet übernehmen dabei, wie bereits erwähnt, das Internet Protocol (IP) und das Transport Control Protocol (TCP). Diese Vorgänge erfolgen unabhängig von geografischen Entfernungen und in einer Geschwindigkeit, die herkömmliche Informationskanäle weit hinter sich lässt. Dieser Informationsaustausch erfolgt unter Zuhilfenahme verschiedener Werkzeuge, der einzelnen Internetdienste, wie etwa Peer-to-Peer oder World Wide Web.

„Die Computerkultur nähert sich dem Punkt, an dem die vollberechtigte Mitgliedschaft keine Programmierfertigkeiten mehr erfordert, sondern Personen gewährt wird, die Software von der Stange benutzen.“ [Turk98, 95]

Waren sie am Anfang des Internets noch kommandozeilenorientiert und somit fast nur für Insider verständlich, so hat durch die Entwicklung des WWW letztlich eine graphische Benutzeroberfläche Einzug gehalten und damit diesen Siegeszug des Internets rund um den Erdball erst eingeleitet. Neben den Anwendungen des World Wide Web (WWW) und den Peer-to-Peer Netzwerken (P2P) existieren noch einige

andere, meist ältere Internetdienste, welche allerdings mangels graphischer Oberfläche weniger bedienungsfreundlich, für den durchschnittlichen Anwender kaum interessant und der prozentualen Bedeutung des Internets stark rückläufig sind. Eine Ausnahme bildet der E-Mail Dienst, der durch übersichtliche Mailprogramme und graphisch aufbereitete Internetseiten mit weiteren Features einiger Mail-Anbieter den Anschluss an das WWW-Zeitalter finden konnte. Vollständigkeitshalber sollen „FTP“ (File Transfer Protocol), ein Dienst zur Datenübertragung, „Telnet“, zur Herstellung einer Terminal-Sitzung direkt auf einem entfernt stehenden PC, „Secure Shell oder SSH“ ist sowohl ein Programm als auch ein Netzwerkprotokoll, mit dessen Hilfe man sich über eine verschlüsselte Netzwerkverbindung auf einem entfernten Computer einloggen und dort Programme ausführen kann, „IRC“ (Internet Relay Chat), bezeichnet ein etabliertes, rein textbasiertes Chat-System und „Usenet Newsgroups“, Pinnwände zum Austausch von Nachrichten mit einer Vielzahl möglicher Benutzer, kurz erwähnt werden.

Nochmals sei darauf hingewiesen, dass die Dienste jeweils die oberste Schicht des demonstrierten Modells repräsentieren. Der eigentliche Datentransport erfolgt immer auf die gleiche Art und Weise.

2.1.6 Wer regiert das Internet?

Seit Ende der 90er Jahre hat die ICANN (Internet Corporation for Assigned Names and Numbers) die Oberaufsicht über das Netz – eine privatrechtliche Stiftung, formal unabhängig, tatsächlich aber von Washington kontrolliert. ICANN legt Adressendungen wie .com fest und verknüpft einprägsame Adressen mit computerlesbaren Zahlencodes. Die anderen Staaten wollen jedoch eine Internetverwaltung und –kontrolle durch eine UNO-Behörde, in der zugleich alle Staaten auch über die Kernfragen und die großen Probleme des Internets beraten und entscheiden sollen.

2.1.7 Peer-2-Peer (P2P)

Dieses Kapitel gibt einen kurzen Überblick über die Geschichte des Ausdruckes „Peer-to-Peer“ und beschreibt seine Definition in seiner derzeitigen Verwendung. Peer-to-Peer

wurde ursprünglich dazu verwendet, die Kommunikation zwischen zwei Anwendern zu beschreiben, vergleichbar mit einer Telefonunterhaltung. Eine Telefonunterhaltung benötigt zwei Personen (Peers) mit gleichen Status, also eine Kommunikation zwischen einer Point-to-Point Verbindung. Einfach ausgedrückt, entspricht es dem, was eine P2P Kommunikation ist, eine Verbindung zwischen zwei gleichwertigen Teilnehmern. Das Internet startete damals als ein Peer-to-Peer System. Das Ziel vom originalen ARPANET war die Rechenleistung innerhalb der USA zu verteilen.

Mit dem Aufkommen neuer Technologien in den späten 90er Jahren tauchte auch eine neue Definition für Peer-to-Peer auf.

“P2P is a class of application that takes advantage of resources e.g. storage, cycles, content, human presence, available at the edges of the Internet”. [Tayl05, 26].

Es besteht kein Zweifel daran, dass die kürzliche Entwicklung, welche im Bereich P2P stattgefunden hat, d.h.: der massive Datenaustausch zwischen den einzelnen Teilnehmern des Internets weltweit, die Augen von vielen Personen in den unterschiedlichsten Disziplinen geöffnet hat. Besonders im Kontext mit dem Verteilen von urheberrechtlich geschützten Materialien gab es unterschiedlichste Reaktionen und Argumente für und gegen die Ausbreitung solcher Technologien.

Die meisten Internetservices verwenden die traditionelle zentralisierte Architektur, um ihre Daten zu verteilen. Leider weist diese Architektur einen wesentlichen Nachteil auf, wenn nämlich die Anzahl der Teilnehmer steigt, wird der Server zum Flaschenhals in diesem System, das kann soweit führen, dass neue Anfragen von Teilnehmern nicht mehr beantwortet werden können, d.h. der Server ist überlastet.

Es gibt daher viele Gründe, welche für eine Peer-to-Peer Übertragung sprechen. P2P ist eine einfache Möglichkeit die Leistungsfähigkeit eines Computers zu steigern. Der große Vorteil dieses Client/Server Modells ist, dass auf der Client Seite wenig Computerleistung beansprucht wird. Wie bereits erwähnt wurde ist es in einer Welt, in welcher die Rechenleistung der Enduser ständig steigt und der Großteil davon verschwendet wird, Zeit über neue Möglichkeiten der Datenübertragung nachzudenken. Genau hier kommen die Vorteile von Peer-to-Peer zum Tragen, da sie die entstehende Rechenlast, welche bei einer Datenübertragung auftritt, untereinander gleichmäßig

verteilt. Weiters kann durch diese Variante der Datenübertragung die Fehlertoleranz verbessert werden, da der Ausfall eines Rechners nicht gleich zum Stillstand des ganzen Systems führt, wie es bei einer Client/Server Übertragung der Fall wäre.

„Since the emergence of peer-to-peer (P2P) networking in the late '90s, P2P applications have multiplied, evolved and established themselves as the leading 'growth app' of the Internet traffic workload.” [KaBF04, 121]

P2P kann sinnvollere und robustere Lösungen zur Verfügung stellen, als es derzeitige Technologien in vielen Situationen je im Stande wären. Als Beispiel können derzeitige Suchmaschinen angeführt werden, die ihre Ergebnisse zentral zur Verfügung stellen. Google, zum Beispiel, verlässt sich auf eine Datenbank, welche täglich aktualisiert wird, indem sie das Internet nach neuen Informationen durchsucht. Durch die enorme Größe dieser Datenbank (derzeit mehr als 1,8 Milliarden Einträge) ist es verständlich, dass nicht jeder Eintrag täglich aktualisiert wird. Durch diesen Umstand sind viele Informationen, welche abgefragt werden können, nicht mehr aktuell. Weiters ist es aus der Kostenperspektive unpraktisch, dass eine solche Methode für das ständig wachsende Internet eine Zukunft hat.

“For example, even though Google, at the time of writing, runs a cluster of 10,000 machines to provide its service, it only searches a subset of available Web pages (about 1.3×10^8) to create its database. Furthermore, the world produces two exabytes (2×10^{18} bytes) each year but only publishes about 300 terabytes (3×10^{12} bytes) i.e. for every megabyte of information produced, one byte gets published. Therefore, finding useful information in real-time is becoming increasingly difficult.” [Tay105, 30-31].

2.1.8 Exkurs: Deep Web

Nach einer Studie des amerikanischen Marktforschungsinstitutes Cyveillance [Cyve06] umfasste das Internet im Juli 2006 rund 17,5 Milliarden statische Webseiten. Jeden Tag kommen weitere sieben Millionen hinzu. Daneben gibt es jedoch einen viel größeren Datenbestand, häufig als „deep“, „invisible“ oder „hidden“ Web [Brig00; Looh01; Webl01] bezeichnet. Hierbei handelt es sich um Datenbanken, welche an das Internet angeschlossen sind, die erst auf eine konkrete Anfrage eines Benutzers hin die

Ergebnisse der Datenbankabfrage als dynamische Webseite darstellen. Informationen aus diesen Datenbanken werden durch eine Web-Suche, etwa mit Google, nicht gefunden.

Die verfügbaren Suchmaschinen decken nur das statische Web, und auch davon nur 10-30% [AT06], ab. Eine Studie von BrightPlanet [Brig00] geht davon aus, dass das „invisible Web“ fünfhundert Mal größer ist als die sichtbare Oberfläche des World Wide Web. Danach handelt es sich um ungefähr 6 Billionen Dokumente (Stand Juli 2006) mit einer Qualität der Informationen, die den Durchschnitt der statischen Seiten im Internet bei Weitem übersteigt. Es ist daher fast schon ein Paradoxon, dass die vielen Informationen dazu führen, dass es dem Nutzer immer schwerer fällt, für ihn relevante Informationen zu finden. Nach einer Studie von [LyVa00] werden in den nächsten drei Jahren weltweit mehr Informationen (12 Exabytes = 12 Milliarden Gigabytes) erzeugt als in den letzten 300.000 Jahren [Garb01, 511].

2.2 Digitale Kopie

Das Geschehen der digitalen Kopie begann mit Enthusiasten, welche Wissen als freies Gut ansahen. Dabei war der Begriff „der Kopie“ in den Anfangszeiten der Computerindustrie ein fortschrittlicher, positiver Gedanke. Es waren Erfinder, Studenten und Wissenschaftler, welche mit ihrem Wissensdurst einen Mehrwert für die Gesellschaft und die Menschheit schaffen wollten. Mit ihren damaligen Ideen ebneten sie den Weg in eine digitale Zukunft, in welcher wir heute leben. Noch bevor die Industrie ihr entgegengesetztes Modell definierte, war bereits längst eine Computerkultur entstanden, welche sich zu ihrem Ziel gesetzt hatte, Informationen für alle Menschen frei verfügbar zu machen [KrSe06, 11].

2.3 Der Begriff Raubkopie

„Früher waren Piraten nur auf den Weltmeeren anzutreffen, heute lauern sie digital und on-line in allen Erdteilen.“ [Herb98].

Im Jahr 1975 gründete William (Bill) Henry Gates III zusammen mit Paul Allen das Unternehmen „Micro-Soft“, was heute unter den Namen Microsoft bekannt ist. Die

revolutionäre Vision von Bill Gates war es, nicht die Hardware für einen PC, sondern die Software dafür zu verkaufen. Das Neuartige an dieser Ansicht war, dass damals die Vorstellung für Software Geld zu verlangen, der Anschauung vom Computer widersprach. Es war nämlich selbstverständlich Wissen und Erfahrungen frei mit anderen auszutauschen, also zu teilen. Diese Idee, eines neuen Marktes für Software, von Bill Gates platzte mitten in die idealistische Welt der Hacker. Sie waren schließlich der Meinung, dass jeder Programmierer sein Wissen durch andere haben und nur ein offener Austausch eine Weiterentwicklung gewährleisten könne. Bill Gates wollte jedoch sein erworbenes Wissen weder mit anderen Hackern teilen, noch sah er es ein, dass seine entwickelte Software von anderen ohne Bezahlung kopiert oder verändert werden durfte [KrSe06, 24-25].

Verärgert schrieb er am 3. Februar 1976 einen offenen Brief, den so genannten „Open Letter“, an den Homebrew Computer Club [o.V.06h]. Darin bezichtigt er jene des Diebstahls, welche seine Software ohne Bezahlung benutzen und frei kopierten. Der neue Gedanke einer „illegalen Kopie“ sorgte damals für Verwirrung und Antipathie gegenüber Bill Gates. Doch durch seine sture Haltung und seinen ausgezeichneten Geschäftssinn wurde die Software von Microsoft erfolgreicher, als man es sich je hätte vorstellen können und machte Bill Gates zum reichsten Mann der Welt. In den darauf folgenden Jahren eroberte die Firma Microsoft den Softwaremarkt zunächst mit dem Betriebssystem MS-DOS (Microsoft Disk Operation System), später mit Microsoft Windows (95, 98, 2000, XP, Vista). Mit wachsendem Marktanteil von der Firma Microsoft setzte sich in den Köpfen der Verbraucher ein neues Verständnis durch. Das Produkt Software konnte auch ein kommerzielles Produkt sein, für welches man zu zahlen hat. Bill Gates Prophezeiung, dass der Computermarkt einmal von Software beherrscht werden würde, ging in Erfüllung. So sehr sich auch Softwarebenutzer und Computerfreaks weltweit gegen die Vermarktung von Software und Informationen wehrten, eine Begrifflichkeit ist erst durch den Open Letter entstanden, nämlich der Begriff „Raubkopie“ [KrSe06, 25-27].

2.4 Die ersten Cracker

Während in der Industrie und Wissenschaft der Umgang mit Computern immer wichtiger wurde, war damals für den Enduser vor allem der Faktor Unterhaltung ein

entscheidendes Kaufkriterium. Merkmale wie Speicherkapazität oder Prozessorgeschwindigkeit spielten dabei keine Rolle. Disketten und Festplatten waren für den Homeuser eigentlich gar nicht geplant. Die Software wurde damals auf handelsüblichen Kassetten gespeichert, welche mit speziellen Laufwerken in den PC geladen wurden. Die Kassetten zu kopieren, war für den durchschnittlich technisch interessierten Privatanwender keine große Herausforderung, da er lediglich einen Kassettenspieler und einen Kassettenrecorder benötigte. Die Gefahr, dass jedoch eine Kopie unerlaubt verteilt wurde, war jedoch sehr gering, da gerade einmal 0,4% der amerikanischen Haushalte einen Computer besaßen [o.V.83a, 42]. Zudem wies jede Kopie einen deutlichen Qualitätsverlust auf, ähnlich bei Kopien von Musikkassetten. Es konnte daher leicht passieren, dass durch einen Kopiervorgang die Software nicht mehr einwandfrei funktionierte [KrSe06, 28-30].

Auf der einen Seite waren damals die Softwarehersteller empört darüber, dass ihre entwickelte Software illegal kopiert wurde. Auf der anderen Seite reizte es die Entwickler die Herausforderung ihre selbst entwickelten Produkte unkopierbar zu machen. Im Jahr 1982 waren dann erstmals Softwareprodukte mit einem Kopierschutz versehen. Das einfache Kopieren war ab diesem Moment mit den normalen Maßnahmen nicht mehr denkbar [KrSe06, 29-30].

2.4.1 Die erste Generation

Die allerersten Cracker waren Privatanwender, welche sich der Herausforderung stellten, einen Kopierschutz zu knacken, um eine Kopie erstellen zu können. Dabei versahen diese Personen ihre gecrackte Software mit einem Pseudonym und brachten die erstellte Kopie über verschiedene Verteilungswege in Umlauf. Am meisten wurden auf den Schulhöfen zwischen den einzelnen Schülern die so kopierten Speichermedien getauscht. Dabei verteilten Schüler im Alter zwischen 12 und 18 Jahren die gecrackte Software innerhalb kürzester Zeit per Post oder von Hand zu Hand auf der ganzen Welt. Als im Jahre 1983 die ersten Diskettenlaufwerke ausgeliefert wurden, war ein direktes Kopieren von Software ohne Qualitätseinbußen möglich.

Durch die verschiedenen Möglichkeiten, um an raubkopierte Software zu gelangen, gingen immer mehr Privatanwender dazu über, sich die benötigte Software nicht mehr zu kaufen. Die Softwarehersteller, welche eigentlich ihre Software ursprünglich nur

gegen eine leicht überschaubare Anzahl von Raubkopierern schützen wollte, hatten mit der Einführung ihres Kopierschutzes eine Entwicklung ausgelöst, welcher sie nun hilflos gegenüberstanden. Es wird daher nicht ohne Grund behauptet, dass die Einführung des Kopierschutzes der größte Fehler der Softwareindustrie war. Das Problem war, dass die Privatanwender kaum ein Unrechtsbewusstsein hatten, wenn sie sich eine 1:1 Kopie des Originals erstellten. Das Kopieren von Softwareprogrammen wurde, sozusagen wie das Kopieren von Schallplatten auf Musikkassetten als selbstverständlich empfunden.

Im Laufe der Zeit schlossen sich die einzeln agierenden Cracker zu Gruppen zusammen, welche unter dem Namen „Cracking Groups“ bekannt wurden. Der damalige Distributionsweg beschränkte sich noch immer, wie bereits oben erwähnt, auf den Postweg und die persönliche Weitergabe untereinander. Erst viele Jahre später weitete sich die Übertragung der einzelnen Daten auf die Telefonleitungen aus. Da das heutige Breitbandinternet noch nicht vorhanden war, benutzte die Szene intern Modems, um die Software untereinander weltweit zu verteilen [KrSe06, 31-41].

2.4.2 Das Aufkommen einer neuen Generation

Durch die Entstehung des Internets Anfang der 90er Jahre veränderte sich die Welt der Szene abrupt. Immer mehr Normalverbraucher erhielten dadurch die Möglichkeit an Software zu gelangen, welche für sie niemals vorgesehen war. Jeder Gelegenheitskopierer hatte ab nun die Möglichkeit von der Arbeit der Cracker zu profitieren, ohne einen Beitrag für die „Szene“ zu leisten. Das Medium Internet ermöglicht nämlich jeder Person, selber gecrackte Software zu tauschen, was viele Jahre nur ein Privileg der Szenenmitglieder war. Die geheime Welt der Cracker, in welcher sie sich bewegten, wurde mit einem Schlag für alle zugänglich [KrSe06, 42-43].

Eine weitere Entwicklung, durch welche viele Szenenmitglieder aufhörten, der „Szene“ weiterhin anzugehören, war das Aufkommen des „Webwarez“. Darunter versteht man Raubkopien, welche auf verschiedenen Websites zum Download angeboten werden. Dabei brauchte man weder ein spezielles Wissen oder Passwörter oder Zugangscodes, um an die Daten zu gelangen, sondern sind für jeden frei verfügbar. Ein simpler Mausklick genügt, um die gecrackte Software auf den eigenen PC zu speichern. Der Software- und Musikindustrie sowie den Strafverfolgungsbehörden blieb diese neue

Form der Kriminalität im Internet jedoch nicht lange verborgen. Die allerersten Diskussionen, dass das Internet nicht länger ein rechtsfreier Raum sein dürfte, kamen in sämtlichen Medien etwa ab dem Jahr 1996 auf [Rütt96].

Obwohl den meisten klar war, dass Websites nicht dauerhaft der ideale Ort für Raubkopien sind, hatte das Internet dafür gesorgt, dass sich jeder beliebige Gelegenheitskopierer etwas Neues in den Kopf setzte: die weltweite Verbreitung und Beschaffung von Raubkopien [KrSe06, 42-45].

2.4.3 Die zweite Generation

Durch das Internet wurde der Wirkungskreis der Cracker als auch der Szene enorm erweitert. Alle bisherigen Methoden, durch welche die gecrackte Software verteilt wurde, waren mit einem Schlag überholt. Viele Szenenmitglieder, welche fast zwanzig Jahre aktiv in der Crackerszene waren und mit dem Internet nicht viel anfangen konnten, sahen sich ausrangiert. Doch gleichzeitig, als der Großteil der ersten Generation den Niedergang einer Ära beklagten, fingen sich die verbliebenen Mitglieder der Szene an zu reorganisieren. Es bildete sich eine neue Generation an Crackern, wodurch die Szene allgemein noch größer und mächtiger wurde [KrSe06, 49-50].

Während, wie bereits erwähnt, die gecrackte Software früher noch über lahme Modemverbindungen übermittelt wurde, gab es durch die Einführung des Internets bislang ungeahnte Varianten, Kinofilme, Software und Musikalben und mehr über schnelle Internetanschlüsse zu tauschen. Es wurde nun nicht mehr nur Software, sondern alles getauscht, was man digitalisieren konnte. Im Fachjargon der Szene allgemein wurden alle digitalisierten Tauschobjekte weiterhin unter dem Begriff „Warez“ zusammengefasst. Deshalb wird eine szeneninterne Gruppe, welche „Warez“ veröffentlicht, als „Release Group“ bezeichnet [KrSe06, 49-50].

2.4.4 Kopierschutz und Cracker

Maßnahmen, um digitale Werke vor dem Kopieren zu schützen, gibt es in verschiedenen Variationen. Viele Hersteller von digitalem Content nutzen dabei eigens entwickelte Mechanismen, andere wiederum bedienen sich wiederum bereits beliebter

Methoden. Jedoch auch die verschiedenen Vorgehensweisen, welcher sich die Cracker bedienen können, um den Kopierschutz zu entfernen, sind vielfältig. Einzelne Cracker, welche sich in diesem Zusammenhang fast tagtäglich mit dem Knacken neuer digitaler Werke beschäftigen, haben dabei individuelle Techniken entwickelt. Dabei lässt er sich von vielen Softwareprodukten unterstützen, welche speziell für diesen Zweck programmiert wurden. Oft wird noch immer fälschlicherweise angenommen, dass der Kopierschutz den Cracker vor dem Kopieren abhalten soll. Er ist jedoch nicht in erster Linie als Schutzmechanismus vor den Crackern zu verstehen, sondern es soll damit dem Gelegenheitskopierer die Möglichkeit genommen werden, das Original kopieren zu können, anstatt es sich legal zu erwerben. Der Kopierschutz ist daher als Schutz vor Heimanwendern gedacht. Die lange Geschichte des Kopierschutzes hat aber vorgezeigt, dass es bislang keinen Kopierschutz gegeben hat, welcher unknackbar gewesen wäre: Denn jeder Kopierschutz weist bestimmte Schwachstellen auf, welche ein erfahrener Cracker lediglich aufspüren muss, um ihn aushebeln zu können. Die Filmindustrie musste diese Tatsache bei ihrem angeblich unknackbaren Kopierschutz „Content Scrambling System“ (CSS) erfahren, welcher wie bereits erwähnt, Ende der 90er Jahre das neue Medium DVD vor dem unerlaubten Kopieren schützen sollte. Im Herbst 1999 tauchte bereits ein Programm namens DeCSS im Internet auf, welches den Inhalt einer gesamten DVD unverschlüsselt auf der Festplatte eines Computers speichern konnte.

Der Hauptgrund, weshalb es bis heute keinen perfekten Kopierschutz gibt, liegt in der Art der Daten, wie sie in einem Computer gespeichert werden. Wenn man nämlich annehmen würde, es gäbe wirklich den ultimativen Kopierschutz, müssten die einzelnen digitalen Daten so aufgebaut sein, dass sie ein gewöhnlicher Computer nicht mehr lesen kann. Daten, welche durch diese Weise geschützt würden, könnten auch mit erheblichem Aufwand nicht mehr manipuliert werden. Das Problem ist jedoch, dass Daten zwangsläufig kopierbar sein müssen, um mit herkömmlichen Computern verarbeitet werden zu können. Da jedoch jede Datei aus binären Zahlenfolgen besteht, welche jeder Computer lesen kann, ist es auch möglich, sie zu verändern. Ein perfekter Kopierschutz ist daher aus heutiger Sicht nicht möglich [KrSe06, 121-129].

2.4.5 Open Source und Filesharing

Ebenfalls werden auch im Bereich des Filesharing Open-Source-Lösungen immer bevorzugter. Viele Anbieter von Filesharingclients sehen in ihnen den Ausweg aus den Klagen der Musikindustrie. Die RIAA forderte im September 2005 mehrere Tauschbörsenanbieter auf, den Datenaustausch von urheberrechtlich geschützten Musikstücken zu unterbinden [McBr05]. Daraufhin reagierten die Betreiber der Tauschbörse Limewire recht originell indem sie kurzerhand das Programm als Open-Source-Software veröffentlichten. Ab diesen Zeitpunkt war es jedermann erlaubt, die Software zu verändern und weiterzuverbreiten. So wurde es ermöglicht, dass das Programm selbst weiterentwickelt und verbreitet wurde, obwohl der Hersteller selbst rechtliche Probleme hatte. Die beiden beliebtesten Filesharingprogramme eMule und BitTorrent sind ohnehin seit jeher frei erhältlich. Deshalb wird ihre Weiterentwicklung trotz diverser Klagen der RIAA nicht wirklich gestoppt werden können [KrSe06, 144].

2.5 Der Ursprung und der Verteilungsweg von Raubkopien

Laut einer Studie des Kopierschutzproduzenten Macrovision verwenden mehr als 50% aller Computerspieler regelmäßig „Warez“, dabei wissen nur wenige von ihnen, woher diese ursprünglich stammt [ByMC04].

Dabei hat jede erstellte Kopie, welche unter Freunden ausgetauscht oder aus dem Internet besorgt wurde, unabwendbar einen Ursprung. Es gibt von jeder Kopie immer ein Original, von welchem erstmals eine Kopie angefertigt wurde. Diese erstellte Kopie wird dann wieder von zahlreichen Personen vervielfältigt, welche sie ihrerseits weiterkopieren. Aufgrund der digitalen Vervielfältigungstechnik entspricht dabei jede weitere Kopie zu 100% dem Original. Die Raubkopie, welche schließlich auf der Festplatte des Gelegenheitskopierers gespeichert wird, ist bereits ein Exemplar, das schon vielfach kopiert wurde.

Wenn man in den Medien Artikel über „die Raubkopierer“ wieder findet, werden meistens damit Gelegenheitskopierer gemeint, welche sich über das Medium Internet mit „Warez“ versorgen. Obwohl die Filesharingbörsen zu den beliebtesten Umschlagplätzen für „Warez“ zählen, sind sie meistens nicht der Ursprung der jeweiligen Raubkopie. Bis zum Beispiel ein bestimmtes Computerprogramm in der

Tauschbörse gehandelt wird, hat es meistens bereits einen langen Weg hinter sich. Für eine Raubkopie sind nämlich die Tauschbörsen oder das WWW nur die Endstation einer langen Reise, welche meistens in der Releaseszene beginnt, der Geburtsstätte des „Warez“. Fast alle illegalen Kopien von Softwareprogrammen, Filmen oder Musikalben entstehen in dieser verschlossenen, geheimen Welt und folgen danach einem effizienten Verbreitungsweg. Innerhalb dieses steigt die Anzahl der Nutzer, welche sich den „Warez“ herunterladen und weiterkopieren, exponentiell an. Die einzelnen Release Groups setzen durch die Bereitstellung der Raubkopien eine Lawine in Gang, welche nicht mehr zu stoppen ist.

An der Spitze der Pyramide stehen, wie bereits erwähnt, die Release Groups, welche täglich einen neuen „Warez“ veröffentlichen. Das Interesse der Gruppen gilt dabei jedoch nicht der globalen Verbreitung der Raubkopien, sondern wie bereits früher in der ersten Generation dem Wettstreit untereinander. So zirkuliert eine Raubkopie vorerst nur innerhalb dieser abgeschotteten Releaseszene. Die komplette Abschottung in die Außenwelt gelingt jedoch den Releasegroups nicht. So erreicht der „Warez“ die nächste Stufe der Verbreitung, bis er von jedem Internetnutzer mit relativ geringem Aufwand beschafft werden kann [KrSe06, 50-51].

2.5.1 Release-Szene

Der enorme Zeitdruck, den der Wettbewerb mit neuen Veröffentlichungen mit sich bringt, führte dazu, dass man nahezu jede neue Software, jeden Film und einen Großteil der Musikveröffentlichungen spätestens am Tag ihrer Erstveröffentlichung in der Releaseszene verbreitet werden. Diese „0-Day-Releases“, welche vom Erscheinungsdatum des Originals nicht älter als 24 Stunden alt sind, werden von Jahr zu Jahr immer mehr. Jeden Tag werden somit Tausende von Schwarzkopien von „Release Groups“ in Umlauf gebracht. Um bei dieser enormen Vielfalt von Veröffentlichungen den Überblick zu behalten, werden von der Szene intern eigene Online-Datenbanken geführt, wo man jedes einzeln veröffentlichte Release wieder findet.

Durch diese enorme Datenvielfalt von „Warez“ in der Szene, haben sich im Laufe der Zeit bestimmte Verbreitungswege der Daten etabliert. In den 80er Jahren wurden noch die meisten Releases über so genannte Boards getauscht, heutzutage werden die meisten Releases über FTP-Server der Szene ausgetauscht. Diese Server sind leistungsstarke

Computer, welche von heimischen Rechnern weltweit mit digitalen Daten gefüllt werden. Das Angebot reicht von Filmen, Spielen und Musik bis zu digitalen Textdokumenten, Bildern und vielem mehr. Bei Topsites findet die Übertragung der digitalen Daten meistens über moderne Lichtwellenkabel statt. Dabei ist die Übertragungsgeschwindigkeit 100 bis 1.000mal höher als dies bei handelsüblichen DSL-Internetanschlüssen der Fall ist. Das Kopieren eines kompletten Films von einer Topsite zur anderen dauert daher nur mehr einige Sekunden. Weiters haben solche Topsites riesige Speicherkapazitäten. Während zum Beispiel ein durchschnittlicher Rechner eines Endusers mit einer 250GB Festplatte bestückt ist, sind Topsites mit einer Kapazität von über 10 Terabytes ausgestattet, was mehr als 10.000 Gigabytes Speicherkapazität entspricht [KrSe06, 52-66; O.V.04a].

2.5.2 Filesharingszene

Der mit Abstand größte Teil der Raubkopierer ist aber nicht in der Releaseszene aktiv; die meisten von ihnen sind Gelegenheitskopierer, welche „Warez“ von Kollegen in der Arbeit oder Freunden erhalten oder ihn aus dem Netz herunterladen. Während man in der Szene nur über eigene Kanäle und mit ausgefallenen Methoden den „Warez“ austauschen kann, haben durch die Einführung des Filesharings auch weniger technisch versierte Nutzer die Möglichkeit, an Raubkopien aller Art zu gelangen. Bei diesem technischen Konzept wird das Nehmen und Geben von digitalen Dateien vereinfacht. Jeder Nutzer des Filesharingprogramms stellt die ausgewählten Dateien auf seiner Festplatte allen anderen Benutzern der Tauschbörse über das Internet zur Verfügung. Dabei ist der ausschlaggebende Vorteil gegenüber FTP-Servern die Option, Daten direkt von Nutzer zu Nutzer auszutauschen. Es gibt somit keine zentrale Sammelstelle mehr, wo der „Warez“ liegen müsste.

Kommt irgendeine Kopie eines digitalen Werkes in ein Filesharingnetz, sorgt die Filesharingszene dafür, dass dieses Werk innerhalb kurzer Zeit in allen bekannten Tauschbörsen wieder zu finden ist. Was also von den einzelnen Releasegroups hinter verschlossenen Türen veröffentlicht wurde, findet sich einige Zeit später auf den Festplatten von Millionen Computernutzern weltweit.

Das Geniale dabei ist, je mehr Nutzer ein Filesharingprogramm verwenden, desto mehr digitale Werke stehen allen Beteiligten zur Verfügung. Durch diese Verteilungsmethode

kann ein einzelner Benutzer im Idealfall auf die digitalen Daten von mehreren Millionen anderer Benutzer zugreifen. Einzige Voraussetzung dabei ist lediglich ein Breitbandinternetzugang und das Filesharingprogramm, welches in der Regel gratis im Netz zum Download bereitsteht. Dabei ist der Nutzer durch die Teilnahme am Filesharing zugleich Sender und Empfänger von digitalen Daten. Bereits in den 70er Jahren war die kollektive Nutzung von Ressourcen in Computernetzwerken prinzipiell bekannt. Die Netzbetreiber von damals nannten diese Form der Verteilung Peer-to-Peer (P2P), weil dabei Gleiche mit Gleichen vernetzt werden. Heutzutage wird der Begriff „P2P“ sehr oft synonym mit „Filesharing“ gebraucht.

In der gesamten Geschichte der Raubkopie wurde niemals soviel getauscht wie mit der jetzigen Filesharingtechnologie. Durch sie bildete sich eine weltweite Gemeinschaft, welche den Tausch von Raubkopien nicht mehr ausschließlich im Geheimen betreibt. In dieser weltumspannenden Gemeinschaft kann jeder Internetteilnehmer am Datenaustausch von „Warez“ teilhaben. Dabei besteht diese Gemeinschaft aus einer sehr großen Anzahl von Einzelgängern. Diese Personen benutzten die jeweilige Tauschbörse nur, um sich einen bestimmten „Warez“ herunterzuladen, eine charakteristische Benutzergruppe ist dabei nicht auszumachen. Ob Schüler oder Lehrer, Student oder Professor, Arbeiter, Angestellter oder Arzt, die Klientel ist bunt durcheinander gemischt. Ein szenenähnlicher Aufbau oder Engagement liegt ihnen zumeist beileibe nicht am Herzen [KrSe06, 79-97].

Aber warum stellen Benutzer Files für andere zur Verfügung - trotz des Wissens der Illegalität dieser Handlung. Sie tun dies laut einer Studie deshalb, weil der Großteil der Nutzer befürchtet, dass das System nicht funktionieren würde, wenn sie es nicht täten. [BKKM03, 52]. Dies sei eben der Hauptgrund, was zum Erfolg von P2P Systemen führe.

2.5.3 Was wird alles getauscht!

„Since their first appearance, P2P file-sharing network have evolved from music swapping only applications (such as Napster) to multi-functional systems that not only enable sharing variety of types of digital content but also support different classes of users ...” [THVW05, 302]

Inzwischen kann nahezu jedes digitale Produkt, welches es auch käuflich zu erwerben gibt, als Raubkopie heruntergeladen werden. Von Software, Filmen, Musik, Spielen oder digitalen Büchern, die zur Verfügung stehende Auswahl scheint grenzenlos. Für viele Internetuser ist das WWW zu einem unermesslichen Büffet geworden, an welchem sie sich reichlich bedienen. Die meisten der erhältlichen Kopien werden dabei von den einzelnen Releasegroups in den Umlauf gebracht, wobei sich die meisten von ihnen auf ein bestimmtes Medium konzentrieren. Zumeist spezialisieren sich die einzelnen Gruppen noch weiter. So gibt es Releasegroups, welche nur PC-Spiele für Spielekonsolen, Pop-Alben oder Zeichentrickfilme aus Japan releasen. Doch einige Raubkopien, werden wie bereits erwähnt, von einzelnen Personen außerhalb der Szene erstellt, wie zum Beispiel außergewöhnliche Fernsehsendungen oder seltene Hörspiele. Diese Personen bieten dann ihre Kopien in der Regel direkt über eines der Filesharingnetzwerke oder über Freehoster, wie zum Beispiel Rapidshare an. Dabei lassen sich vier Hauptgruppen von Raubkopien unterscheiden: „Warez“, „Moviez“, „MP3z“ und „EBookz“. Wobei unter den Begriff „Warez“ früher die Szene ausschließlich Raubkopien von Software verstanden hat. Mittlerweile wird dieser Begriff jedoch auch synonym für die oben beschriebenen Bereiche gebraucht.

„Die Angebotsvielfalt und Menge der Daten, die über das Internet distribuiert werden, ist beeindruckend.“ [BeCl03, 261].

2.5.4 Legale Filesharingdateien

Nicht die Tauschbörsen selbst sind illegal, sondern die Art und Weise, wie viele sie nutzen. Anstatt illegal zu tauschen, können Musiker dort ja auch selbst gemachte Musik legal anbieten. Oder junge, unbekannte Bands stellen ihre Titel kostenlos zur Verfügung, um sich eine Fangemeinde aufzubauen.

Neben illegalen Dateien gibt es daher auch eine Menge legale digitale Inhalte zum Download. Insbesondere BitTorrent und eMule eignen sich hervorragend um große Dateien, ohne viel Servertraffic zu verursachen, zu verteilen. Da sich Bit-Torrent-Dateien in erster Linie für große Dateien eignen, finden sich häufiger Linux-Distributionen oder Datenschergewichte wie die Wikipedia-DVD oder die Microsoft Office-Alternative OpenOffice.org als Torrent-Downloads auf den Servern der

Anbieter. Aber auch viele Sänger und Filmemacher bieten ihre Downloads über dezentrale Filesharingnetzwerke an. Probleme mit großen Downloads haben auch Spielehersteller. Mit der Betaversion von „World of Warcraft“ hat der Spieleproduzent Blizzard seiner Zeit die Verteilung der Datei via BitTorrent getestet. Völlig legale Filme, Musikalben und Bücher bietet die Webseite Legaltorrents.com. Hier finden sich Alben von Netlabels neben der WiredCD und DivX-Filmen von Indie-Filmern. Dabei kann die Seite auf beachtliche Downloadzahlen verweisen. Die Heft-CD von Wired wurde beispielsweise über 30.000 Mal heruntergeladen [Hott05b, 1-2]. Neben den eben erwähnten Angeboten kann auch jeder beliebige User seine privaten Urlaubsfotos und Filme der Netzgemeinde zur Verfügung stellen.

2.5.5 Exkurs: Moviez

Da „Moviez“ den meisten Speicherplatz auf der Festplatte benötigen, möchte ich anhand dieses Beispiels zeigen, wie solche Daten in Tauschbörsen gelangen. So ähnlich wie früher bei Musik-CDs war es lange für die Szene allgemein undenkbar, Filme zu kopieren und über das Medium Internet auszutauschen. Für die damaligen Internetverbindungen, welche über Modems aufgebaut wurden, waren die Dateien einfach viel zu groß. Zusätzlich hatten die damaligen Computer nicht die nötige Rechenleistungen, welche benötigt werden, um einen Film komplett zu digitalisieren. Erst am Ende der 90er Jahre gelang der Durchbruch für kopierte Filme im Netz. Im September 1999 analysierten der französische Filmeliebhaber und Hacker Jérôme Rota alias Gej gemeinsam mit seinem Hackerkollegen Max Morice das damals bekannte MPEG4-Verfahren von der Firma Microsoft. Durch dieses Verfahren konnte der Speicherplatz, welcher durch die Filme benötigt wurde, deutlich verringert werden, ähnlich dem MP3 Verfahren bei Liedern. Die beiden Hacker studierten dabei die Komprimiermethode des MPEG4-Verfahrens und verbesserten es nach eigenen Vorstellungen. Das endgültige Ergebnis dieser Experimente war das heute weit verbreitete DivX Komprimierungsverfahren. Hatte ein normaler DVD-Film bislang eine effektive Größe von fünf bis acht Gigabytes, ließ er sich durch dieses Verfahren bis auf das Zehnfache verkleinern [o.V.06i].

Trotz dieser erheblichen Verkleinerung blieb dabei die Filmqualität, so hoch wie beim MP3-Verfahren bei Musik. Heutzutage kann bereits fast jeder handelsübliche DVD-

Spieler Filme im DivX-Format abspielen. Die einzelnen Videodateien auf einer DVD sind dabei mit dem Content Scrambling System (CSS) verschlüsselt. Bereits einen Monat nach der Veröffentlichung des DivX-Verfahrens wurde im Oktober 1999 erstmals die CSS-Verschlüsselung von DVDs gehackt. Diese beiden Techniken miteinander sollten sich schon bald als das „Schreckgespenst“ der Filmindustrie erweisen. Es verging nämlich nicht viel Zeit, bis Release Groups anfangen, sich der neuen Möglichkeit des Filmekopierens zu widmen [Neuh06].

Heute ist die Auswahl im WWW an Filmkopien unüberschaubar geworden. Es gibt fast keinen Film mehr, welcher nicht im Internet zum Download bereitsteht. Dabei werden nicht nur DVDs und Kinofilme digitalisiert und verbreitet. Ebenso können oft TV-Sendungen bereits einen Tag nach ihrer Ausstrahlung im Internet heruntergeladen werden. Dabei stammen jedoch längst nicht mehr alle raubkopierten Filme aus der Releaseszene. Denn vor allem die Übertragungen von TV-Serien oder Sportveranstaltungen werden sehr oft außerhalb der Szene allgemein erstellt und über das Netz verbreitet. Die Releasegroups haben sich indessen auf die Verbreitung von Kinofilmen und DVD-Neuerscheinungen spezialisiert. [KrSe06, 106].

Die erreichte Qualität und die vielen Extras, welche durch DVDs angeboten werden, bleiben jedoch noch lange unübertroffen. Denn die im Internet illegal erhältlichen DivX-Filme und auch jene Filme, welche von manchen kostenpflichtigen Streaminganbietern über das Netz vertrieben werden, erreichen meistens nicht einmal VHS-Qualität. Doch der Trend geht dazu über, dass bereits komplette 1:1 Kopien von DVDs angeboten werden, welche eine Größe von bis zu 9 GB erreichen.

3 Filesharing – technische Grundlagen und Voraussetzungen

Heute leben wir in einer Informationsgesellschaft, welche sich in rasantem Tempo global weiterentwickelt. Durch die Revolution der Kommunikationstechnologie wird es möglich, Informationen mit Lichtgeschwindigkeit um den Globus zu schicken. Bisher bestehende räumliche und zeitliche Beschränkungen verschwinden. Jeder kann mit jedem auf weltweiten Datenautobahnen in Wort, Bild und Ton kommunizieren. Die Welt wird zu einem elektronischen Dorf. Unendliches hält die Welt, hält das Internet für den bereit, welcher sie mit den modernen Medien durchforschen kann. Nahezu unbegrenzt sind angebotenen Erkenntnissen und Anregungen.

Die Idee von Filesharing ist es, lokal gespeicherte Dateien, wie beispielsweise Filmdateien zwischen ad-hoc gebildeten Nutzergruppen auszutauschen. Die Aufgabe einer Filesharingplattform ist es dabei, diesen Austausch durch die Bereitstellung von Suchoperationen, Verzeichnisdiensten oder auch Caching-Techniken zu unterstützen. Dabei kommen die Vorteile einer verteilten Speicherung zum Tragen: es wird nämlich weitgehend der Flaschenhals bzw. der „Single Point of Failure“ vermieden und die Last bzw. Kosten (hier im Wesentlichen der Speicherplatzbedarf) werden auf viele Teilnehmer verteilt.

„Due to the widespread appearance of filesharing systems like Napster, the peer-to-peer concept has recently become well known.” [GeSc03, 218]. Während der Betrieb von Napster, der „Mutter aller Börsen“, nach einer Klage des amerikanischen Musikindustrieverbandes RIAA eingestellt wurde, steigen die Nutzerzahlen neu gegründeter Tauschbörsen und mit ihnen der Datentransfer stetig an. Dabei sind die meisten Tauschbörsen nicht auf Audiodateien beschränkt. Es werden neben Musik auch Software, Filme, Spiele, E-books und Bilder getauscht, eben alle Daten, welche sich digitalisieren lassen. Angesicht dieser Tatsachen schlugen die Interessenverbände der betroffenen Unterhaltungsindustrieweige Alarm. [o.V.01a]. Während man damals in fast jeder PC-Zeitschriften nachlesen konnte, wo man am besten Musik und Co herunterladen kann. Hat sich inzwischen diesbezüglich schon einiges geändert.

Doch bevor eine solche rechtliche Bewertung erfolgt, soll zunächst die technische Seite des Filesharing näher erläutert werden, denn der Erfolg der Filesharingnetzwerke seit dem Start von Napster im Jahre 1999 wird nur dann verständlich, wenn man die

Entwicklung zweier Techniken näher betrachtet: zum einen die Entwicklung digitaler Komprimierungstechniken, zum anderen der Einzug der Breitbandtechnologie in die einzelnen Haushalte.

3.1 Datenkomprimierung und schnelle Internetzugänge

Würde man versuchen, die Datenmenge einer herkömmlichen Film-DVD über eine ISDN-Leitung über das Medium Internet auf einen Heimcomputer zu überspielen, so würde dieses Vorhaben auch unter optimalen Bedingungen der Übertragungsgeschwindigkeit rund 176 Stunden, d.h. mehr als eine Woche Zeit in Anspruch nehmen, wobei für die gleiche Zeit entsprechende Kosten für die Verbindung anfallen würden [o.V.05c]. Dazu wären wohl selbst geduldige Computerbenutzer kaum bereit. Die Entwicklung verlustfreier bzw. verlustarmer Komprimierungstechniken war demnach eine wesentliche Voraussetzung für den heutigen Erfolg von Tauschbörsen im Internet. In Verbindung mit der starken Verbreitung der Breitbandinternetzugänge wurde das Thema Filesharing auch für die breite Öffentlichkeit interessant. Denn durch die starke Komprimierung und die hohe Geschwindigkeit der Datenübertragung kann jeder, welcher sich diese Technologien leisten möchte, große Mengen an Daten mit anderen Personen weltweit austauschen.

3.1.1 Audio und Videokomprimierung

Im Audibereich hat sich zur Komprimierung das 1992 vom Fraunhoferinstitut für Integrierte Schaltungen in Erlangen veröffentlichte Audio Layer 3-Verfahren, bekannt unter dem Namen „MP3“, als Quasi-Standard etabliert [o.V.05a].

Während auf herkömmlichen Audio-CDs pro Sekunde Spielzeit eine Datenmenge von etwa 1400 KBit gespeichert ist, dies entspricht rund 10 MB Daten pro Minute, sind MP3-Dateien wesentlich kleiner: je nach Komprimierungsgrad um den Faktor 7 bis 14.

Wie alle anderen verlustbehafteten Kompressionsformate für Musik nutzt MP3 so genannte psychoakustische Effekte der Wahrnehmung aus, z.B. dass der Mensch zwei Töne erst ab einem gewissen Mindestunterschied der Frequenz voneinander unterscheiden kann oder dass man vor und nach sehr lauten Geräuschen für kurze Zeit leisere Geräusche schlechter oder gar nicht wahrnimmt. Es ist daher nicht notwendig,

das gesamte Ursprungssignal exakt abzuspeichern, sondern es reichen die Signalanteile, welche das menschliche Gehör auch wahrnehmen kann [o.V.05b].

Ein durchschnittlicher Pop-Song im MP3-Format hat infolge der Komprimierung eine Größe von 3 bis 4 MB, gegenüber 30 bis 40 MB bei herkömmlichen Audio CDs.

Neben dem MP3-Verfahren finden sich auf dem Markt inzwischen weitere Komprimierungstechniken, wie z.B.: OGG oder WMA, die zum Teil bessere Klangqualität bei gleicher Komprimiertrate aufweisen. Trotz dieser Vorteile ist das MP3 Format das meistverwendete Musikformat in Tauschbörsen. Im weiteren Verlauf der Arbeit wird das MP3-Format daher exemplarisch für alle Audio-Komprimierungen angeführt.

Um MP3-Dateien herzustellen, werden ein handelsüblicher Computer mit CD-Laufwerk oder DVD-Laufwerk und eine Software, in welcher ein „Audioencoder“ integriert ist, benötigt. Der Arbeitsschritt, in welchem die Daten mittels dieser Software von der Musik-CD auf die Festplatte ausgelesen und dabei komprimiert werden, wird als „Grabben“ bezeichnet. Die Dauer dieses Vorganges hängt sehr stark von der Rechenleistung des verwendeten Computers ab.

Zur Erstellung von MP3-Dateien ist aber ohnehin nicht zwangsläufig eine Audio-CD als Ausgangsdatenträger erforderlich. Auch Audio-Dateien, die bereits in einem computerspezifischen Format, wie z.B. Wav-Dateien vorliegen, lassen sich nachträglich komprimieren. Die erstellten MP3-Dateien können im Anschluss durch entsprechende Hardware (Soundkarte im Computer, DVD-Spieler, MP3-Player etc.) abgespielt werden. MP3-Dateien lassen sich durch entsprechende Software, in welcher ein „Audidecoder“ integriert ist, in unkomprimierte Audiodateien zurückverwandeln, sodass eine Wiedergabe über herkömmliche CD-Spieler ermöglicht wird.

Seit etwa Mitte des Jahres 2001 versucht die Musikindustrie dies bei zahlreichen veröffentlichten Audio-CDs durch entsprechende Kopierschutzsysteme zu unterbinden. Bislang ohne nennenswerten Erfolg. Auf die einzelnen Kopierschutztechniken kann leider nicht näher eingegangen werden, da dies den Umfang der vorliegenden Arbeit sprengen würde.

Techniken für die Komprimierung stehen nicht nur für Audio-Daten zur Verfügung, sondern es gibt auch entsprechende Algorithmen für Filme. Die Vorgehensweise, um zu einem komprimierten Film zu gelangen, sind dabei weitgehend mit dem Audio-Bereich identisch. Die größte Nachfrage in Filesharingbörsen besteht nach Filmen, welche von einer DVD „gerippt“ sind. Bei dieser Vorgehensweise wird eine komplette DVD

(Größenordnung: ab ca. 3GB bis 9,4GB) zumeist mit Hilfe der Komprimierungsmethode DivX oder Mpeg auf wenige hundert Megabyte, in den meisten Fällen auf 700 Megabyte reduziert. Diese Größe ist ideal, um auf einen CD-Rohling Platz zu finden. Der große Nachteil dieses Verfahrens ist, dass das komplette Menü, welches sich auf der DVD befindet, entfernt wird und nur mehr die reinen Filme mit einer Sprache abgespielt werden können. Doch heute gibt es bereits neuere Verfahren, wie z.B.: RATDVD, welche es ermöglichen, das Menü mit seinen vielen Auswahlmechanismen ebenfalls zu komprimieren. Die dabei entstehende Größenordnung entspricht meistens 1GB, um den Film in einer ähnlichen Qualität wie bei DivX und Co. zu erhalten. Dies ist wahrscheinlich auch der Grund, warum sich dieses Verfahren in der breiten Öffentlichkeit noch nicht etabliert hat, da der große Vorteil des CD-Brennens entfällt. Die Bedienerfreundlichkeit für solche Softwareprogramme hat sich dabei zunehmend verbessert. Computersoftware, welche zum Rippen von DVDs geeignet ist, wird größtenteils als so genannte Freeware, d.h. gratis, zum Downloaden angeboten.

Mit diesem Verfahren auf CD-Rohlinge übertragene Filme lassen sich nicht nur in den entsprechenden Computerlaufwerken wiedergeben, sondern auch auf handelsüblichen DVD-Playern, welche heutzutage meistens diese Formate unterstützen.

In dieser Kompatibilität zwischen On- und Offlinemedien dürfte der Schlüssel für die große Akzeptanz dieser Technik liegen. In der Zukunft werden daher immer schnellere und bessere Komprimierungsverfahren für immer kleinere Datenpakete sorgen, welche sich über das Medium Internet unkompliziert auf den heimischen Computer übertragen lassen.

3.1.2 Breitbandinternetzugänge: DSL & Co.

Neben der voranschreitenden Komprimierungstechnik ist vor allem das zunehmende Angebot an schnellen und kostengünstigen Internetanschlüssen für den „Boom“ des Datenaustausches via Internet verantwortlich. Während bis vor einigen Jahren mit herkömmlichen Modem- oder ISDN-Verbindungen lediglich Datenübertragungen von 56 bzw. 64KBit/s möglich waren, haben sich in jüngster Zeit so genannte DSL-Anschlüsse für den Zugang ins Internet durchgesetzt. Die überwiegende Anzahl derartiger Angebote ermöglicht eine Datenübertragung von bis zu 6MBit/s, also

sechshundertfacher ISDN Geschwindigkeit. Ein durchschnittlicher Popsong von dreieinhalb Minuten Länge lässt sich bei optimalem Datendurchsatz damit in weniger als 6 Sekunden übertragen, eine komprimierte Videodatei von 700MB theoretisch in gut 20 Minuten. Das solche Theoriewerte in der Praxis kaum erreicht werden, ist darauf zurückzuführen, dass andere Personen ihren Upload meist drosseln, um höhere Downloadraten zu erzielen. Seit neustem sind bereits DSL 2 Anschlüsse, welche eine Datenübertragung von 24 MBit/s ermöglichen, zu haben, wodurch sich die Übertragungsgeschwindigkeit weiter verringert.

Neben DSL über das Telefonkabel sind weitere Internetzugangstechniken mit ähnlichen Übertragungsgeschwindigkeiten am Markt verfügbar. Zu nennen sind Angebote via TV-Kabel, über das Stromnetz („Powerline Communication“) oder via Satellit.

Mit voranschreitender Technik ist auch in diesen Segmenten zu erwarten, dass sie neben DSL den Massenmarkt erobern werden.

Als schnelle Internetzugänge sind außerdem sog. Standleitungen, also permanente Verbindungen zum Internet zu erwähnen. Diese finden sich meistens in gewerblichen Bereichen, etwa zur Anbindung gesamer Unternehmen an das Internet, zunehmend auch im universitären Sektor.

Weltweit hat man sich zum Ziel gesetzt, breitbandige, schnelle Zugänge zum Internet in den nächsten Jahren flächendeckend zur Verfügung zu stellen. Die Digital Subscriber Line (DSL-) Techniken erlauben es heute bereits auf herkömmlichen Telefonleitungen – je nach Technologiestufe – bis zu mehreren Mbit/s zu übertragen. Andererseits werden die breitbandigen TV-Kabel zunehmend nicht nur für digitale Fernsehverteilung, sondern auch für die schnelle Datenübertragung genutzt. Nicht zuletzt bieten verschiedene drahtlose Zugangstechniken ergänzende Lösungen und Alternativen für die mobilen Teilnehmer. In Zukunft stehen der breiten Bevölkerung in den weltweiten Glasfasernetzen Transportraten von Giga- und bald Terabit pro Sekunde zur Verfügung, welche die Nutzungsmöglichkeiten des heutigen Internets revolutionieren werden. Das heutige Breitbandinternet ist daher das Schmalband von morgen.

Zusammenfassend kann festgehalten werden, dass auf der technischen Seite die Voraussetzungen für einen ungebremsen Datenaustausch beständig optimiert werden. Dies geschieht zum einen durch bessere Komprimierungstechniken, zum anderen sorgt die zunehmende Verbreitung schneller Internetzugänge dafür, dass immer mehr Privatleute über die Möglichkeit verfügen, digitalisierte Werke mit wenig Zeitaufwand

und damit kostengünstig über das Medium Internet auszutauschen. An der Schnittstelle dieser beiden Entwicklungen setzen Filesharingnetzwerke an.

3.1.3 Zusammenfassung

Die vorliegende Untersuchung hat bislang gezeigt, dass neue technologische Möglichkeiten wie die Weitergabe von urheberrechtlich geschützten Werken über Filesharingnetze zu einer erheblich gesteigerten Werknutzung führen. Im digitalen und vernetzten Kontext entfallen Begrenzungen wie die Notwendigkeit eines physisch-realen Austausches oder die dürftige Qualität von Kopien. Digitale Vervielfältigungsstücke entsprechen nicht nur qualitativ dem Ausgangsstück, sie lassen sich auch mit wenig Aufwand mit Hilfe des Internets über beliebige Entfernungen verteilen. Filesharingnetzwerke potenzieren diesen Effekt zusätzlich, indem sie Angebot und Nachfrage gezielt und ohne Streuverluste zusammenführen. Schwierigkeiten bei der Lokalisierung der Inhalte oder mit der Handhabung komplizierter Technik müssen nicht überwunden werden. Aus derzeitiger Sicht ist die technische Entwicklung noch nicht einmal abgeschlossen. Mit der Entwicklung neuerer, besserer Komprimierungstechniken können immer größere Datenmengen für den elektronischen Austausch aufbereitet werden; die steigende Verfügbarkeit schnellerer Internetzugänge für eine breite Masse tut ein Übriges. Künftig ist damit zu rechnen, dass schnelle Internetzugänge in größerem Rahmen auch mobil zur Verfügung stehen werden. Internetanwendungen wie Filesharing sind damit in absehbarer Zeit nicht nur auf den heimischen beziehungsweise stationären PCs problemlos verfügbar, sondern an jedem beliebigen Ort. Marktforscher erwarten daher insgesamt ein weiteres Ansteigen der Zahl der über Filesharingbörsen getauschten Werke [Heis02b]. Es liegt auf der Hand, dass das Voranschreiten der Technik damit nicht nur zu einer noch größeren Bedeutung der Schrankenregelungen und hier – wie für das Filesharing gezeigt – speziell der Schranke der individuellen Vervielfältigung zum privaten Gebrauch führen wird. Insoweit schreitet auch die digitale Kopiertechnik zur endgültigen Festlegung heruntergeladener Werke stetig voran. Mit der „Blue-ray Disc“ ist unlängst von einem Firmenkonsortium ein Speichermedium vorgestellt worden, das etwa 13 Stunden Film in DVD-Qualität (entsprechend 23 GB) aufzeichnen kann.

3.2 Arten von Filesharing-Systemen

Derzeit interagieren User typischerweise mit dem Medium Internet durch die Verwendung eines Webbrowsers und einer Client/Server basierenden Software.

Dieses Kapitel soll einen kurzen Überblick über Client/Server und Peer-to-peer Anwendungen geben.

Ein Client ist ein Empfänger von Informationen wie zum Beispiel ein Webbrowser, ein Server hingegen ist ein Lieferant von Informationen wie zum Beispiel ein Webserver oder ein Peer, der Dateien zum Tausch anbietet. Ein Peer ist demnach eine Vorrichtung, welche sowohl als Empfänger als auch als Sender von Informationen interagiert [Tayl05, 4].

3.2.1 Zentralisierte und dezentralisierte Systeme

Auf einer Seite des Spektrums haben wir zentralisierte Systeme, wie zum Beispiel typischerweise Client/Server basierende Architekturen und andererseits gibt es dezentralisierte Systeme, die oft als P2P bezeichnet werden. Dazwischen gibt es einen Mix von beiden extremen Ausprägungsformen, der als hybrides System bekannt ist.

Laut Tayler [Tayl05] gibt es drei Hauptkriterien, die ein System als zentralisiert oder dezentralisiert beschreiben.

1. Resource Discovery
2. Resource Availabilitiy
3. Resource Communication

3.2.1.1 Resource Discovery

Innerhalb eines Verbundsystemes muss es einen Mechanismus geben, welcher die Zusammenhänge der einzelnen Ressourcen kennt. Dabei kann „resource discovery“ entweder zentralisiert (z.B.: DNS) oder dezentralisiert (z.B.: Gnutella) sein. Discovery ist dabei typischerweise ein zweistufiger Prozess. Zuerst werden die notwendigen Services lokalisiert; danach werden alle relevanten Informationen herangezogen.

Ein gutes Beispiel, um diesen Begriff zu erklären, ist die Internetseite Google. Diese ist hauptsächlich ein zentralisierter Server, welcher über die Adresse <http://www.google.com> aufgerufen werden kann. Dabei wird von den meisten Benutzern jedoch angenommen, dass sich hinter dieser Adresse nur ein einziger Server verbirgt. Wenn man den Domännamensdienst (DNS) kontaktiert, erhält man die IP Adresse 168.127.47.8, mit der man den Hauptserver von Google direkt adressieren kann. Wie auch immer ist Google eine Suchmaschine, die von mehreren Millionen Personen täglich verwendet wird und derzeit um die 1.6 Milliarden Einträge verwaltet. Um diese Informationen liefern zu können, wird jedoch auf eine Datenbank zugegriffen, welche aus einem Cluster von 10,000 parallelen Linux Rechnern (zum Zeitpunkt des Schreibens) besteht. Aus der Sicht des Endkunden arbeitet diese Suchmaschine zentralisiert, aber von der Betreiberseite betrachtet, wird dieser Service von einer Vielzahl von Rechnern zur Verfügung gestellt [Tayl05, 6-7].

3.2.1.2 Resource Availability

Ein anderer wichtiger Faktor ist die Verfügbarkeit der Ressourcen. Webserver werden unter diesem Gesichtspunkt als zentralisiert betrachtet, da sie nur eine IP Adresse besitzen. Wenn man den Server abschaltet, kann die Webseite nicht mehr erreicht werden. Hingegen wird ein Dienst dezentralisiert betrieben, führt das Abschalten eines Rechners noch nicht zum Stillstand des gesamten Systems. Es kann daher ohne Probleme weiterhin auf die Daten zugegriffen werden, da ein anderer Rechner die Aufgaben des abgeschalteten Rechners übernimmt. Daher ist ein dezentralisiertes System viel zuverlässiger gegen Ausfälle einzelner Rechner. Eine Mischform zwischen diesen beiden extremen Ausformungen war die Filesharingsoftware Napster. Bei ihr wurde die Suchanfrage zwar zentralisiert abgewickelt, jedoch der eigentliche Datentransfer lief dezentralisiert ab. Fand also bereits eine Datenübertragung zwischen zwei Rechnern statt, konnte sie auch nach einem Ausfall des „Suchservers“ ohne Probleme beendet werden [Tayl05, 7-9].

3.2.1.3 Resource Communication

Der letzte Faktor ist, wie die einzelnen Rechner miteinander kommunizieren. Es werden dabei zwei unterschiedliche Arten der Kommunikation unterschieden:

1. Brokered Communication: bei dieser Kommunikationsvariante findet die Kommunikation immer über einen zentralen Server statt. Dabei muss der Rechner nicht direkt über die eigene Adresse angesprochen werden. Es kann daher ein Proxy-Server dazwischengeschaltet werden. Ein gutes Beispiel für ein mit Hilfe eines Vermittlers geregeltes System ist die Filesharingsoftware Napster. Sie speichert Informationen über den Aufenthaltsort der Teilnehmer und Musikfiles zentralisiert ab, danach lässt sie aber die Teilnehmer direkt miteinander kommunizieren, wenn sie untereinander die Daten transferieren.
2. Point-to-Point (or Peer-to-Peer) Communication: bei dieser Variante besteht eine direkte Verbindung zwischen dem Sender und Empfänger. In diesem Fall weiß der Sender Bescheid, wo sich die gegenüberliegende Ressource befindet. Es ist daher nicht möglich, über einen Proxyserver zu kommunizieren. Als Beispiel kann jede P2P-Software angeführt werden, die komplett dezentralisiert organisiert ist, wie zum Beispiel die beiden beliebten Programme Limewire (<http://www.limewire.com>) und Bearshare (<http://www.bearshare.com>).

Im ersten Fall wird von einer zentralisierten Kommunikation gesprochen, im zweiten von einer dezentralisierten [Tayl05, 9-10].

3.2.2 Peer-2-Peer Systeme

„Das Filesharing ist zweifelsohne der populärste Anwendungsbereich des P2P-Computing. Erst durch den medial stark beachteten Auf- und Abstieg der Internettauschbörse Napster erlangte neben dem Filesharing selbst auch das P2P breite Aufmerksamkeit. Daher werden von vielen Benutzern die Begriffe P2P und Filesharing synonym verwendet.“ [GrSV03, 337]

„Peer-to-Peer ist Vision und Hoffnung für die Informatik und wird zum Schrecken für die Medienindustrie. Die Bezeichnung Peer-to-Peer (P2P) umschreibt eine Klasse von Anwendungen und Systemen, die die Ressourcen mehrerer Rechner einsetzt, um eine Aufgabe in einer verteilten Weise zu lösen.“ [Müll03, 643]

Bezogen auf Netzwerke kann ein P2P-System als Netz angesehen werden, welches auf spezielle Server verzichtet und in dem Clients direkt miteinander kommunizieren. Die P2P-Idee lässt sich so an einigen wesentlichen Eigenschaften charakterisieren [SaHS05, 756]:

- Die Knoten (so genannte Peers) im Netzwerk sind gleichberechtigt, d.h. jeder Peer kann sowohl als Client als auch als Server agieren und prinzipiell auf die Ressourcen aller anderen Peers zugreifen.
- Jeder Peer „zahlt“ für seine Teilnahme am Netz und die Inanspruchnahme von Diensten, indem er anderen Peers Zugriff auf einen Teil seiner Ressourcen gewährt.
- Es gibt weder eine zentrale Koordination noch eine zentrale Datenbasis.
- Kein Peer hat eine globale Sicht auf das gesamte System, d.h., es gibt kein „globales Wissen“.
- Das globale Verhalten des gesamten Systems ist ein Ergebnis der lokalen Interaktion von Peers.

Weiterhin wird den einzelnen Peers eine gewisse Autonomie zugestanden, sodass „unzuverlässige“ Peers und Verbindungen zu berücksichtigen sind.

Aus der Sicht eines verteilten Datenmanagements in P2P-Systemen bestehen zwei wichtige Aufgaben [SaHS05, 757]:

1. die vorhandenen Daten müssen in geeigneter Weise organisiert werden und
2. einzelne Anfragen zum Auffinden und eventuell auch Verknüpfungen bestimmter Daten sind zu beantworten.

Laut Wolff [Wolf04], kann P2P zum einen als allgemeines Kommunikationsmodell zwischen gleichberechtigten Partnern verstanden werden, zum anderen als logisches, dynamisches Netz im Internet, bei dem Computer direkten Zugriff auf Ressourcen anderer im P2P-Netz befindlichen Rechner besitzen.

Zur Einordnung der verschiedenen P2P-Techniken wurden einige Klassifikationen vorgeschlagen. So wird zwischen zentralisierten, dezentralisierten und hierarchischen Modellen unterschieden, je nachdem, ob ein zentraler Index (ein Server), nur dezentrale Indices (nur gleichberechtigte Peers) oder eine Kombination aus beiden existieren.

Jeder Anwender, der an das Internet angeschlossen ist, besitzt heutzutage einen Prozessor mit ein oder mehreren Kernen, der eine Rechenleistung aufweist, welche 100-mal stärker ist, oder bereits noch schneller, als Supercomputer in den frühen neunziger Jahren waren. Dabei fand die GardnerGroup bei einer Studie heraus, dass 95% dieser Rechenleistung weltweit verschwendet wird [o.V.05d].

3.2.3 NAT Systeme

Um mit einem Computer am Internet teilnehmen zu können, muss er eine IP Adresse besitzen. Diese ist eine einmalige 32-bit Nummer, die es ermöglicht, den Standort des Computers exakt festzustellen. In der Theorie existieren 2^{32} (4,294.967.296) einzigartige Adressen, doch die verfügbare Anzahl ist viel kleiner, nämlich zwischen 3,2 und 3,3 Milliarden. Das ist deshalb so, weil die IP Adressen in einzelne Klassen eingeteilt werden und andere für Multicasting (Übertragung einer Nachricht oder Information von einem zentralen Computer zu vielen Computern des Netzwerkes), Testzwecke oder spezielle Teilnehmer reserviert werden. Durch die explosionsartige Vergrößerung des Internets sind die durch diese Variante verfügbaren IP Adressen bei weitem nicht mehr ausreichend. Daher wird das Adressformat von IPv4 auf IPv6 geändert, was eine theoretische Anzahl von 2^{128} (entspricht ~340 Sextillionen Adressen) einzigartigen IP Adressen ermöglicht. Doch bevor dieses Adressformat eingeführt werden kann, vergeht sicher noch einige Zeit, da die gesamte Infrastruktur des Internets modifiziert werden muss [Wiki06u].

„Gnutella defined and popularised modern P2P technology through its truly decentralized design and implementation.” [Tay105, 101]

Das Gnutella Netzwerk besteht aus Tausenden von Informationsteilnehmern, die nicht auf einem zentralen Ort aufgelistet werden.

Gnutella wurde das erste Mal im März 2000 veröffentlicht. Laut seinem Entwickler Tom Pepper, wurde es geschaffen, um Kochrezepte unter den Leuten zu verteilen [Tay105, 101]. Gnutella ist ein Protokoll für eine verteilte Suche in einem Netzwerk. In diesem Modell ist jeder Teilnehmer im Netzwerk ein Client und ein Server gleichzeitig.

Um in diesem Netzwerk ein File zu lokalisieren, sendet ein „Server“ eine Anfrage zu all seinen direkten Nachbarn, welche wiederum eine Anfrage an ihre direkten Nachbarn weiterreichen und dieser Prozess wiederholt sich. [Tayl05, 106-107]

P2P führte zu einer erneuten Steigerung des Interesses an dezentralen Systemen. Obwohl das basierende Internet seinerseits das größte dezentrale Computersystem in der Welt darstellt, setzen die meisten Systeme eine zentrale Topologie ein.

3.2.4 Exkurs: Grid Computing

„Der Begriff Grid-Computing stammt von der englischen Bezeichnung für das Stromnetz, dem Power Grid. Die Idee des Grid Computings ist dabei, die Rechenleistung - ähnlich wie elektrischen Strom - "aus der Steckdose" vom Grid beziehen zu können. Der User übergibt seinen Auftrag über genormte Schnittstellen ans Grid, woraufhin die Ressourcenallokation automatisch erfolgt.“ [Wiki06j]

Unter Grid-Computing wird daher die Allgegenwärtigkeit von Rechenleistung, Speicherplatz und computergestützten Diensten bei optimaler Nutzung von existierenden Ressourcen verstanden. Dies soll über die Vernetzung zahlreicher Einzelressourcen mittels P2P-Technologie und eines uniformen Zugangs zu dem resultierenden Gesamtnetz realisiert werden.

3.3 Peer Typologien

Dieser Teil der Diplomarbeit basiert auf einem Online-Artikel [Mina01] und zeigt eine Vielzahl von Varianten, welche ein P2P-Netzwerk verwenden kann. Hauptsächlich wird in der Literatur zwischen zentralisierten und dezentralisierten Netzwerken unterschieden, d.h. wie die einzelnen Knotenpunkte im System verbunden sind. Für P2P Netzwerke wird der Informationsfluss zwischen diesen Knotenpunkten in Betracht gezogen. Knotenpunkte in den Graphiken sind Peers und Verbindungen zwischen Peers sind Hinweise auf einen Informationsaustausch zwischen den einzelnen Knotenpunkten.

Nachstehend werden nun die vier häufigsten Typologien beschrieben und drei hybride Typologien kurz angesprochen. Diese sind:

1. zentralisiert
2. Ring
3. hierarchisch
4. dezentralisiert
5. zentralisiert/Ring
6. zentralisiert/zentralisiert
7. zentralisiert/dezentralisiert

Die wichtigsten Formen für das Filesharing sind dabei zentralisierte, dezentralisierte und hybride Topologien. Die sieben Topologien werden in den folgenden Unterkapiteln näher beschrieben, wobei jedoch nur die drei wichtigsten Formen durch eine grafische Darstellung untermauert werden.

3.3.1 Die vier Grundtypologien

3.3.1.1 Zentralisiert

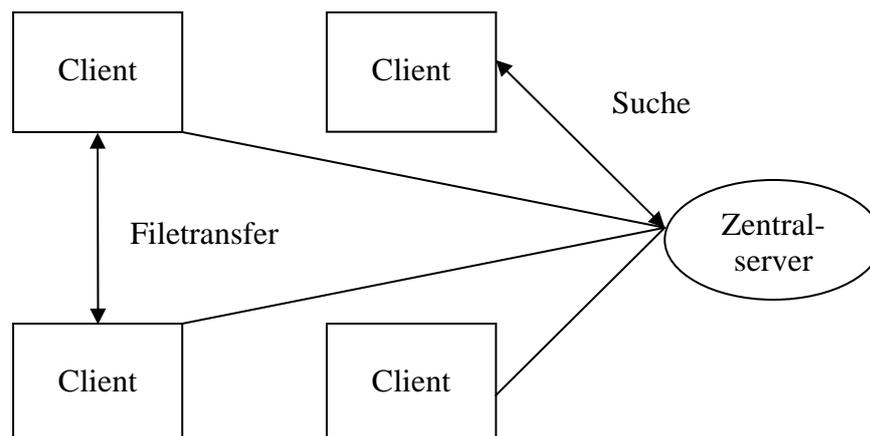


Abbildung 1: Zentralisiertes P2P (Napster, OpenNap)

Zentralisierte Client/Server Systeme sind die am häufigsten vorkommende Typologieform. Die Kommunikation ist dabei komplett zentralisiert mit vielen Clients, welche

direkt mit dem Server verbunden sind. Beispiele für diese Variante sind Client/Server, Webserver, Datenbanken, Suchfunktion in der Filesharingsoftware Napster etc.

3.3.1.2 Ring

Die Ring Topologie ist eine physikalisch geschlossene Schleife, welche aus Point-to-Point Verbindungen besteht. Diese Variante ist die übliche Methode, um zentralisierte Dienste anbieten zu können. Die Kommunikation zwischen den einzelnen Servern gewährleistet, dass der Ring für Außenstehende wie eine Einheit agiert. Typischerweise werden Ringsysteme bestehend aus Rechnern, die an das gleiche Netzwerk angeschlossen sind (z.B. Intranet), also firmeninterne Netzwerke verwendet.

3.3.1.3 Hierarchisch

Hierarchisch angeordnete Topologien haben eine baumstammähnliche Struktur und gewährleisten daher eine extrem schnelle Beantwortung von Suchanfragen in einer hierarchisch geordneten Informationsdatenbank. Das bekannteste hierarchische System im Internet ist der Domain Name Service (DNS), wobei Webseitenamen über mehrere hierarchische Ebenen in ihre numerische Adresse umgewandelt werden. Das Usenet ist ebenfalls ein großes hierarchisch gegliedertes System, das eine baumstammähnliche Struktur verwendet, um binäre Artikel zwischen den einzelnen Servern zu kopieren.

Dezentralisiert

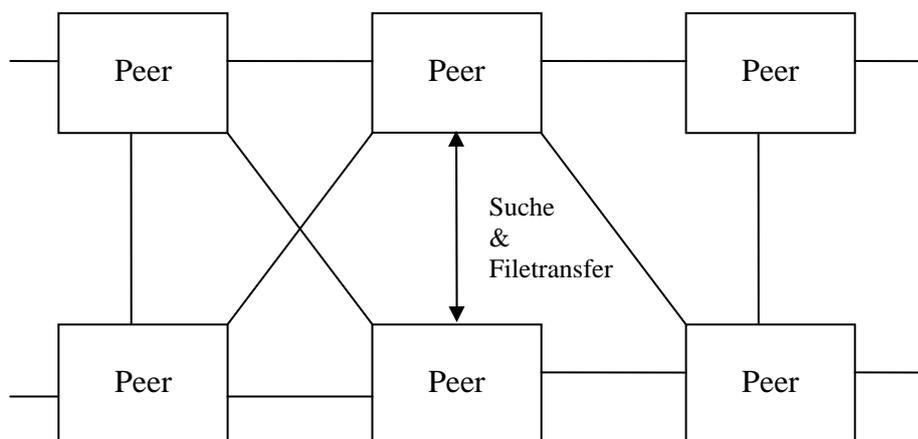


Abbildung 2: Dezentralisiertes P2P (Gnutella, Freenet)

In einem komplett dezentralisierten System gibt es keinen einzelnen Punkt, der alles kontrolliert. Die einzelnen Peers kommunizieren symmetrisch und haben einen äquivalenten Status. Ein gutes Beispiel für dezentralisierte Netzwerke ist das von Gnutella. Rein dezentralisierte Netzwerke weisen eine extrem hohe Fehlertoleranz auf, da eine gewisse Anzahl an Knoten ausfallen kann, ohne Daten im Netzwerk zu verlieren. Jedoch geschieht dies um den Preis, dass eine enorme Bandbreite benötigt wird, um Daten in jenen Netzwerk zu finden, da es keinen zentralen Ansprechpartner gibt.

3.3.2 Hybride Typologien

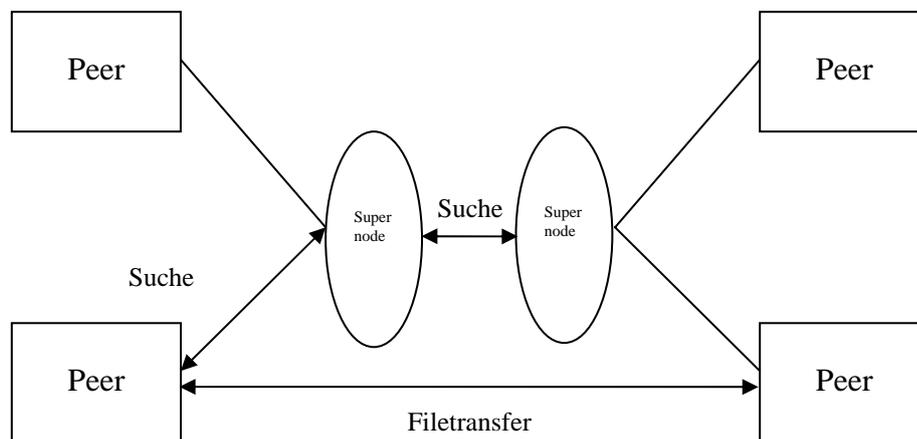


Abbildung 3: Hybrid P2P (FastTrack, eDonkey, WinMX)

Heutzutage stellen jedoch die meisten Systeme eine Kombination zwischen mehreren Topologien dar und machen sie daher komplizierter als einfache Netzwerktopologien. Wenn also Systeme zwei oder drei Grundtopologien miteinander vereinen, werden sie als hybride Topologien bezeichnet.

3.3.2.1 Zentralisiert/ Ring

Wie bereits oben erwähnt, haben robuste Webserver häufig einen Ring von mehreren Servern, um einen Lastenausgleich und eine höhere Ausfalltoleranz zu gewährleisten. Dabei wird der Server selbst als Ring betrieben, jedoch das System als ganzes

(inklusive der Clients) ist eine hybride Typologie: ein zentralisiertes System, in dem die Server selbst einen Ring bilden. Das Resultat ist daher vereinfacht ein zentrales System (von der Sicht des Clients) mit der Robustheit eines Ringes. Als Beispiel können seriöse Webanwendungen und Server genannt werden, welche eine hohe Verfügbarkeit aufweisen müssen.

3.3.2.2 Zentralisiert/ Zentralisiert

Bei dieser Variante gibt es einen zentralen Punkt der Kontrolle, jedoch bei näherer Betrachtung greift dieser Server auf Informationen von einem weiteren oder mehreren Servern zu, die ebenfalls zentralisiert angeordnet sind. Ein Beispiel wären Webanwendungen, bei denen ein Webbrowser einen Server kontaktiert, um eine Anfrage zu beantworten, und dabei dieser Server einige weitere Knotenpunkte kontaktiert, um eine Antwort auf diese Anfrage zu erhalten. Ein bekanntes Beispiel dafür sind Datenbanken großer Systeme (Google), sowie n-stufige Anwendungen etc.

3.3.2.3 Zentralisiert/Dezentralisiert

Eine neue Generation von Peer-to-Peer Systemen verwendet eine Architektur von zentralisierten Systemen, welche in dezentralisierte Systeme eingebettet werden. Diese hybride Typologie wird mit Hunderttausenden von Teilnehmern im Fasttracknetzwerk verwirklicht, das ebenfalls in KaZaA und Morpheus benutzt wurde. Die meisten Teilnehmer in diesem Netzwerk haben eine zentralisierte Beziehung zu einem so genannten „Supernode“, welcher alle Anfragen von den herumliegenden Clients beantwortet (vergleichbar, wenn ein Napsterclient eine Anfrage an den Napsterserver stellt). Das heißt, dass ein Client das gesamte Netzwerk durchsuchen kann, ohne eine große Bandbreite in Anspruch zu nehmen. Diese Topologie findet heutzutage am meisten Verwendung in Filesharingprogrammen.

3.4 Technische Infrastruktur des Filesharings

Alle Filesharingnetze beruhen auf einem Protokoll, welches es den Teilnehmern erlaubt, in direkten Kontakt miteinander zu treten und über das Internet Daten auszutauschen.

Diese Möglichkeit besteht weltweit, völlig ungeachtet des tatsächlichen Aufenthaltsortes des einzelnen Teilnehmers. Durch die Verwendung eines gemeinsamen Protokolls werden die Teilnehmer zu einem eigenen, gegenüber dem Internet zumindest virtuell abgegrenzten Netzwerk verbunden. Der Zugang zu sämtlichen Filesharingnetzwerken mittels der entsprechenden Software ist kostenlos möglich und an keine weiteren Voraussetzungen gebunden.

Die Zugangssoftware kann man sich meistens über die Homepage der Initiatoren des jeweiligen Filesharingsnetzwerkes herunterladen, sie wird aber ebenfalls auf verschiedenen Marktplätzen angeboten, welche sich mit dem Thema Filesharing auseinandersetzen. Wenn die Software einmal installiert ist und der Rechner mit dem Internet verbunden wurde, genügt es, die Software zu starten, welche sich innerhalb kurzer Zeit mit dem Netzwerk verbindet. Danach ist es dem Benutzer möglich, gezielt nach bestimmten Dateien zu suchen. Durchsucht werden dabei die Datenbestände der Nutzer, welche ebenfalls zu diesem Zeitpunkt mit dem Netzwerk verbunden sind. Ähnlich zu herkömmlichen Internetsuchmaschinen, wie etwa Google, wird dem Nutzer das Ergebnis seiner Anfrage in einer überblicksartigen Liste präsentiert, die regelmäßig weitere Auskünfte über die gefundenen Ergebnisse preisgibt. Welche Arten von Dateien gesucht werden können, ist von der jeweiligen Tauschbörse abhängig. Jedoch kann man davon ausgehen, dass man alle gängigen Dateiformate in den jeweiligen Tauschbörsen vorfindet, da die überwiegende Mehrzahl von Filesharingnetzen keine Beschränkung auf ein bestimmtes Dateiformat vorsieht.

Aufgrund der relativ hohen Teilnehmerzahlen, bei populären Tauschbörsen in Spitzenzeiten bis zu einigen Millionen gleichzeitig, ist die Trefferquote von Suchanfragen zumindest bei beliebten Files recht hoch.

Die Anzahl und Auswahl der herunterladbaren Stücke ist dabei stark abhängig von der Bereitschaft der Teilnehmer, selbst entsprechende Dateien im Netzwerk bereitzustellen. Nachdem das Programm auf der Festplatte installiert ist, wird ein bestimmter Speicherbereich für den Zugriff von außen freigegeben. Alle Dateien, welche in diesem Teil gespeichert sind, werden den anderen Teilnehmern zur Verfügung gestellt. Zu beachten ist auch, dass alle Dateien, die man gerade herunterladet, ebenfalls anderen Personen im Netzwerk zur Verfügung gestellt werden. Ob ein Teilnehmer Inhalte zur Verfügung stellen muss, unter Umständen sogar eine bestimmte Menge, bevor er selbst berechtigt ist, von anderen Teilnehmern Dateien herunterzuladen, ist abhängig von der jeweiligen Tauschbörse. Jede Datei, die freigegeben wurde, ist für die anderen

Teilnehmer nur solange verfügbar, wie der Teilnehmer mit dem Netzwerk verbunden ist.

Der große Vorteil bei diesem Verfahren ist, dass der meist teure Betrieb eines gesonderten Servers, auf welchen die Daten permanent gespeichert sind, entfällt.

Das Angebot von Inhalten durch die Teilnehmer bedeutet demnach auch, dass Menge und Attraktivität der verfügbaren Dateien in solch einem Netzwerk vollständig von seinen Teilnehmern abhängt.

Eine Tauschbörse kann sich am Markt nur dann behaupten, wenn eine möglichst große Anzahl von Teilnehmern möglichst viele attraktive Dateien zur Verfügung stellt. Um einen Download nicht zu zerstören, wenn der Anbieter während des Herunterladens das Tauschnetzwerk verlässt, verfügen die meisten Tauschbörsen inzwischen über eine Funktion, die es erlaubt, eine Datei von mehreren Teilnehmern gleichzeitig in kleinen Stücken herunterzuladen, und die es zudem gestattet, im Falle des Ausscheidens des Tauschpartners auf einen anderen Teilnehmer zu wechseln, der die betreffende Datei ebenfalls im Netzwerk anbietet.

Wie die Suche nach bestimmten Dateien und deren Austausch zwischen den einzelnen Teilnehmern erfolgt, ist vom technischen Aufbau des Filesharingnetzwerkes abhängig.

3.4.1 Zentralisierte Filesharingnetze

Den Prototypen des zentralen Netzwerkes stellt die Tauschbörse Napster dar. Solche Systeme beruhen auf einem zentralen Server (sog. Indexserver), welcher die angeschlossenen Computer der einzelnen Filesharingteilnehmer und die von diesem angebotenen Daten verwaltet. Hierzu meldet sich der einzelne Teilnehmer durch Aufruf der Filesharingsoftware beim zentralen Server an. Dieser fragt Informationen über den Teilnehmer selbst ab, etwa dessen IP-Adresse, und Daten in welchem Verzeichnis freigegeben worden sind. Diese Informationen werden danach zentral gespeichert und in regelmäßigen Abständen neu abgefragt, um immer aktuelle Daten zur Verfügung zu stellen. Dabei werden auf dem Server keine Inhalte, also etwa Musik- oder Filmwerke gespeichert, sondern ausschließlich die Daten der einzelnen Teilnehmer im Netzwerk verwaltet. Sucht ein Teilnehmer eine Datei, so vergleicht der Zentralserver diese Suchanfrage mit dem aktuellen Datenbestand. Die Ergebnisse werden danach dem Teilnehmer in einer Übersichtsliste präsentiert. Der Suchende hat jetzt die Möglichkeit

aus jener Liste sich die Dateien auszusuchen, welche er downloaden möchte. Dazu stellt die Filesharingsoftware eine direkte Verbindung zwischen den einzelnen Teilnehmern her. Danach werden die Daten zwischen den verbundenen Teilnehmern transferiert. Ab diesem Zeitpunkt hat der Zentralserver keinen Einfluss mehr auf diesen Transfer.

Der technische Vorteil einer solchen Netzwerkstruktur liegt im zentralen Verzeichnis, das ständig aktualisiert wird und daher immer die neusten Fakten den einzelnen Teilnehmern schnell und zuverlässig übermittelt. Dabei wird der gesamte Datenbestand von allen Teilnehmern des Netzwerkes erfasst, was die Zahl der Treffer bei einer Suchanfrage deutlich erhöht.

Diesen Umstand konnten sich die Kläger in den US-amerikanischen Gerichtsverfahren gegen Napster zunutze machen, da es nur einen Zugangspunkt zum Netzwerk gab, dessen Ausfall das gesamte Netzwerk lahm legt. Die Tauschbörse konnte durch das Abschalten dieses Serverparks das gesamte Netzwerk stilllegen.

3.4.2 Dezentralisierte Filesharingnetze

Die überwiegende Zahl der heutigen Filesharingnetze ist mittlerweile sicherlich auch wegen der Erkenntnisse im Falle Napster nach einer dezentralen Struktur aufgebaut. Als Prototyp eines solchen Netzwerkes wird meistens Gnutella genannt, das in seiner originalen Form heute zwar keine Rolle mehr spielt, jedoch immer noch als Grundlage für auf seiner Struktur weiterentwickelte Tauschbörsen wie etwa „Limewire“ oder „Bearshare“ herangezogen wird.

Dezentrale Netzwerke kommen völlig ohne zentralen Server aus und bestehen vielmehr aus einem Netz miteinander verbundener, gleichberechtigter Computer. Jeder Teilnehmer in diesem Netzwerk ist zugleich Server und Client, d.h. vereinfacht gesagt, er stellt Anfragen an das Netzwerk und beantwortet auch solche von anderen Teilnehmern. Man spricht in diesem Zusammenhang auch von „Servants“; aus der Gleichberechtigung folgt die englische Bezeichnung des „Peer-to-Peer“- Netzwerkes.

Um Teilnehmer an einem solchen Netzwerk zu werden, ist lediglich eine Verbindung auf Grundlage des entsprechenden Softwareprotokolls mit nur einem beliebigen aktiven Teilnehmer des Netzwerkes erforderlich. Das Netzwerk nutzt dabei ebenfalls die physische Struktur des Internets, d.h. die Leitungen, sind jedoch von jenem abzugrenzen, da es unabhängig von diesem existiert. Eine Suchanfrage nach einer

bestimmten Datei wird zunächst an den oder die Rechner der Teilnehmer weitergeleitet, mit denen der eigene Computer direkt verbunden ist. Diese Computer geben die Anfrage wiederum in einer Art Schnellballsystem an diejenigen Computer weiter, mit denen sie selbst verbunden sind, usw. Ein unendliches Kreisen einer Suchanfrage im Netzwerk wird durch einen so genannten „Time to Live“-Befehl (TTL) verhindert. Jeder Rechner, der die Suchanfrage empfängt, prüft, ob die gesuchte Datei lokal vorhanden ist und meldet Treffer über den gleichen Weg zurück, über den die Anfrage gegangen ist. Da jeder Rechner bei diesem Vorgang seine IP-Adresse mitschickt, werden bei einem gültigen Treffer die jeweiligen Rechner miteinander verbunden und der Datentransfer wird begonnen. Das dezentrale Netzwerk spielt bei dieser Verbindung keine Rolle mehr.

Bei diesem Netzwerk gibt es keinen zentralen, vor allem realen Angriffspunkt in Form eines abschaltbaren Indexservers, sondern nur ein virtuelles Netz, das auf einem häufig massenhaft verbreiteten Softwareprotokoll beruht. Würde die Herstellerunternehmen entsprechender Software geschlossen, könnten die Nutzer weiter ungehindert Dateien tauschen. Als Beispiel dafür kann die Tauschbörse EDonkey2000 genannt werden, welche im 3.Quartal 2006 geschlossen wurde und bis heute noch für seine Benutzer weiterhin verfügbar ist.

3.4.3 Mischsysteme

In der Praxis spielen auch Tauschnetzwerke eine bedeutende Rolle, welche die technischen Vorzüge beider Systeme, zentral und dezentral, auf sich vereinen.

Bei Mischformen verstärken besonders leistungsfähige Computer mit permanenter Internetverbindung, so genannte „Superpeers“, die Netzstruktur.

Das zentrale Element der Netzwerkstruktur ist das Verwalten der Suchanfrage der einfachen Nutzer durch die „Superpeers“. Da dieser Rechner typischerweise nicht der Kontrolle des Initiators des Tauschnetzwerkes, also dem Anbieter der Tauschsoftware, unterliegt, existiert auch bei derartigen Mischformen von Tauschnetzen kein wirklicher Angriffspunkt aus juristischer Sicht [Rött01].

Teilweise wird vom Anbieter der Tauschsoftware ein so genannter „Loginserver“ betrieben, der die Benutzerverwaltung und Statistikfunktionen erledigt und dem einfachen Nutzer gegebenenfalls die Adressen eines zur Verfügung stehenden

„Superpeers“ mitteilt. Das Tauschnetzwerk funktioniert jedoch auch ohne jenen Server, der mehr oder weniger nur einen komfortableren Zugang ins Netzwerk ermöglicht.

3.5 Kryptografie

Kryptografie ist eine grundlegende Maßnahme, um Daten sicher von einem Ort zu einem anderen zu transferieren. Dabei wird eine Nachricht vor dem Verschicken verschlüsselt, damit sie nicht von anderen gelesen werden kann. Bevor sie der Empfänger wieder lesen kann, wird sie wieder entschlüsselt. Diese Verschlüsselung wird durch die Verwendung eines Keys gewährleistet. Alle zu diesem Zwecke verwendeten Systeme haben zwei grundlegende Eigenschaften:

- der Algorithmus ist öffentlich bekannt und
- der Schlüssel wird geheim gehalten.

Verschlüsselung sichert das verschlüsselte File vor zwei Arten von äußeren Attacken:

1. Abhören: wird dadurch extrem schwierig. Obwohl es zwar möglich ist, die gesamte Nachricht mitzulesen, sieht man nur eine Aneinanderreihung von Daten, welche in dieser Form unbrauchbar sind. Um den unverschlüsselten Inhalt anzeigen zu können, wird der private Schlüssel benötigt.
2. Veränderungen an den Daten sind noch schwieriger durchzuführen, da hierzu der verwendete Schlüssel sowie die gebrauchte Verschlüsselungsmethode bekannt sein muss, um die Daten so manipulieren zu können, dass der Empfänger mit seinem privaten Schlüssel die Datei wieder entschlüsseln kann.
[Tayl05, 138-140]

3.5.1 Arten von Verschlüsselungen

Ein Kryptographiesystem wird also verwendet, um Daten sicher von einer Person zu einer anderen schicken zu können. Dabei werden hauptsächlich drei Arten von Verschlüsselungssystemen unterschieden:

1. Secret Key (symmetrische Verschlüsselung)

Ein einzelner Schlüssel wird verwendet, um die Daten verschlüsseln und entschlüsseln zu können.

2. Public/Private Key (asymmetrische Verschlüsselung)

Hierzu werden zwei Schlüssel benötigt: einer für die Verschlüsselung (public key) und der andere für die Entschlüsselung (private key).

3. One-Way Function (Hashfunktion)

Dabei werden digitale Informationen so verschlüsselt, um eine Prüfsumme mit bestimmter Länge zu erhalten (Kontrollwert), mit welchem die Authentizität des originalen Files festgestellt werden kann.

3.5.1.1 Symmetrische Verschlüsselung

Bei dieser Methode wird derselbe Schlüssel für die Verschlüsselung sowie für die Entschlüsselung der Daten verwendet. Ein gutes Beispiel für eine symmetrische Verschlüsselung ist der Data Encryption Standard (DES).

Der Datenverschlüsselungsstandard (DES) war eine weit verbreitete Methode, um Daten sicher zu verschlüsseln. Dabei gibt es bei einer Schlüssellänge von 56 Bits 72.000.000.000.000.000 (72 Quadrillionen) oder mehr möglicher Schlüsselvarianten, die verwendet werden können. Heute wird jedoch DES aufgrund seiner geringen Schlüssellänge für viele Anwendungen als nicht mehr sicher genug betrachtet [Tayl05, 142-143].

3.5.1.2 Asymmetrische Verschlüsselung

In asymmetrischen Verschlüsselungen (besser bekannt als public-key systems) sind die Schlüssel für die Ver- und Entschlüsselung der Datei verschieden, doch bilden sie

zusammen ein einzigartiges Paar. Diese beiden Schlüssel sind zwar nahe verwandt, jedoch ist es theoretisch nicht möglich, durch den Besitz eines Schlüssels den anderen herauszufinden. Dieses Schlüsselpaar wird als private key und public key bezeichnet. Wie der Name bereits preisgibt, kann der public key öffentlich zugänglich sein, da er nur ermöglicht, die Daten zu verschlüsseln. Einzig allein dem Besitzer des private keys ist es nun möglich, die mit dem public key verschlüsselten Daten zu entschlüsseln. Das Wichtigste bei diesem Verfahren ist die Geheimhaltung des private keys [Tayl05, 143-144].

3.5.1.3 Kryptografische Hashfunktion

Alle bekannten digitalen Signaturverfahren außer der symmetrischen Verschlüsselung sind recht langsam in ihrer Verarbeitung. Da jedoch die Größe einer zu signierenden Datei oft die Megabyte-Grenze überschreitet, müsste ein zu signierendes Dokument in den meisten Fällen in Tausende kleiner Einheiten zerstückelt werden. Um dieses Problem zu lösen, haben sich Kryptologen in den achtziger Jahren das Prinzip der kryptografischen Hashfunktion einfallen lassen. Dabei handelt sich um ein Verfahren, das zu einer gegebenen Nachricht beliebiger Länge eine spezielle Prüfsumme (Hashwert) bildet. Die Anforderungen an eine kryptografische Hashfunktion sind jedoch alles andere als trivial. Die Wichtigste davon ist, dass es sehr unwahrscheinlich sein muss, zwei unterschiedliche Nachrichten mit dem gleichen Hashwert zu finden – ansonsten würde nämlich eine digitale Signatur zu beiden Nachrichten passen. Da es stets deutlich mehr mögliche Nachrichten als mögliche Hashwerte gibt, ist diese Anforderung nicht einfach zu erfüllen, denn die Existenz mehrerer Nachrichten mit gleichem Hashwert ist nicht zu verhindern. Eine kryptografische Hashfunktion muss daher so konstruiert werden, dass es mit vertretbarem Aufwand nicht möglich ist, die vorhandenen Duplikate zu finden. Die Anforderungen, welche Kryptologen an eine kryptografische Hashfunktion stellen, gehen jedoch einen Schritt weiter. Es soll nicht nur unmöglich sein, zu einer gegebenen Nachricht eine zweite mit gleichen Hashwerten zu finden – vielmehr soll es generell nicht machbar sein, zwei Nachrichten mit gleichem Hashwert (eine so genannte Kollision) zu finden. Da sich RIPE-MD-160 bisher gegenüber allen Versuchen Kollisionen zu finden, behauptet hat, ist das Verfahren zur

zweitwichtigsten kryptografischen Hashfunktion neben SHA-1 geworden. [Schm04, 274-279]

Beide Verfahren finden sich bei modernen Filesharingprogrammen wieder, um Dateien im Netzwerk eindeutig identifizieren zu können. Mittels des „Hash Wertes“ lässt sich jedoch auch bei einigen Tauschbörsen der Download einer bestimmten Datei durch Direct- oder Quicklinks starten, welche auf speziellen Webseiten, die täglich aktualisiert werden, übersichtlich zusammengestellt sind.

Eine Hash Funktion ist also eine Abbildung einer Datei, die von jeder Inputdatei, egal welcher Größe, gebildet werden kann und immer einen fix definierten hash key mit gleicher Länge ergibt. Ein kryptografischer Hashschlüssel muss folgende Eigenschaften besitzen:

- Er darf nicht umkehrbar sein: Es darf daher keine Möglichkeit bestehen, die Originaldatei aus den Hashschlüssel zu erhalten.
- Er muss sehr sensibel auf die Eingangsdatei reagieren: Der Hashwert muss sich bei jeder kleinsten Änderung der Eingangsdaten, sogar wenn sich nur ein Bit ändert, einen anderen Wert ergeben. Dieses Phänomen ist auch als „Avalanche- oder Lawineneffekt“ bekannt, d.h. eine kleine Veränderung am Eingang bewirkt eine große Veränderung am Ausgang.
- Er soll immun gegen Kollisionen sein: Es soll unmöglich sein, mit zwei unterschiedlichen Eingangswerten den gleichen Hashwert zu erhalten.

Der Hashwert hat also immer die gleiche Größe (z.B.: 128 Bit) und der Eingangswert kann dabei jede beliebige Größe annehmen (z.B.: 32 MB). Weiters kann man mit Hashfunktionen die Integrität von Daten feststellen, dabei ist der Hashwert viel verlässlicher als Checksummen oder andere Methoden, die zur Verifizierung von Daten Verwendung finden [Tayl05, 145-146].

3.6 Technischer Ablauf beim Filesharing

Technisch gesehen, wird beim zentralisierten Filesharing ein zentraler Verzeichnisserver verwendet, welcher einen Index aller angebotenen Dateien verwaltet

und die Peers (die Clientprogramme) miteinander verbindet. Der Index selbst enthält zum Beispiel einen einfachen MD5-Hashschlüssel, die Dateiinformationen (ID3-Tags wie Titel, Interpret, Album etc. bei MP3-Files) sowie IP-Adresse und Verbindungsgeschwindigkeit des Clients. Eine Suchabfrage läuft nun immer über diesen zentralen Index: Anhand von Suchbegriffen für die Attribute wie bei MP3-Files Titel oder Interpret werden die Treffer ermittelt und an den anfragenden Client zurück geschickt. Dort kann der Nutzer eine Auswahl vornehmen, und durch eine weitere Anfrage beim Server wird die Adresse des anbietenden Peers (konkret IP-Adresse und Port) ermittelt. Mit diesen Informationen kann nun eine direkte Verbindung zwischen den beiden Peers aufgebaut werden und der Download der Datei erfolgen. Anhand der Beschreibung wird deutlich, dass ein zentraler Index nicht nur technisch, sondern auch rechtlich einen Flaschenhals bzw. Angriffspunkt bildet. Ein bekanntes Beispiel für diese Filesharingvariante war Napster.

In der zweiten Generation von Filesharing Systemen wurde daher versucht, weitgehend auf zentrale Komponenten zu verzichten. Jedes dieser dezentralisierten Programme ist sowohl Client als auch Server. Darüber hinaus gibt es keine zentralen Komponenten. Da es jedoch somit auch keinen festen Ansprechpartner gibt, erfordert die Teilnahme an einem solchen Netzwerk die Kenntnis mindestens eines Peers, was wiederum zum Austausch von Peerlisten führt. Somit kennt jeder Peer nur einige Nachbarn, nicht jedoch alle Knoten des Systems. Suchanfragen werden durch Fluten (engl. Flooding) bearbeitet, d.h. ein Peer sendet seine Anfrage an seine Nachbarn, diese antworten und leiten die Anfrage gleichzeitig an ihre Nachbarn weiter usw. Anhand der Ergebnisse kann schließlich ein Download initiiert werden, welcher dann direkt zwischen dem anfragenden und dem bereitgestellten Peer abläuft. Es ist offensichtlich, dass eine derartige Suchstrategie schnell zu einer sehr hohen Netzlast führen kann. Daher wurden einige Maßnahmen getroffen, welche diese Last reduzieren sollen. So nutzt ein Peer nur eine kleine Zahl an Nachbarn (meist 5), Nachrichten werden über eine Zufallszahl (quasi-) eindeutig identifiziert, womit ein Peer bereits weitergeleitete Nachrichten erkennen und verwerfen kann. Schließlich wird jede Nachricht mit einem so genannten Time to Live (TTL)-Wert versehen, welcher bei jedem Weiterleiten dekrementiert wird. Wird dieser Wert 0, so wird die Nachricht verworfen und somit nicht mehr weitergeleitet. Daraus ergibt sich ein „Horizont“ im Netzwerk, über den ein Peer nicht hinaus kommt. Trotz dieser Maßnahmen gibt es bei dieser Variante einige Probleme. Hierzu zählen aus technischer Sicht die durch das Fluten generierte hohe Bandbreite

und die „Fragmentierung“ des Netzes durch die TTL-basierte Beschränkung der Weiterleitung von Nachrichten [Wiki06g]. Ein Beispiel für dieses System ist Gnutella.

3.7 Verwendete Programme und deren Funktion

Um einen kurzen Einblick in die Tauschbörsenvielfalt zu geben, werden zwei häufig genutzte Vertreter kurz vorgestellt, nämlich Bit Torrent und E-Mule.

3.7.1 E-Mule

E-Mule ist die Open-Source Variante des Filmtauschnetzes von E-Donkey2000, welches durch das Einschreiten der Filmindustrie geschlossen wurde, und greift auf dessen Netz zu. Dieses beruht noch auf einer Client-Server-Architektur mit vielen zentralen Servern, bei denen man sich anmelden muss. Es ist somit anfälliger gegen strafrechtliche Verfolgungsmaßnahmen. Statt des zusätzlichen „Overnet“ nutzt sie das so genannte Kademila-Netz. Dabei findet der Datentausch ohne einen zentralen Server, also direkt unter den Anwendern, statt. In diesem Netz werden einige PCs selbst zum Server, an die weitere Nutzer als Clients angeschlossen sind. Die Server enthalten Verzeichnisse mit den freigegebenen Ordnern der einzelnen Nutzer. Eine Datei ist so auf mehrere Server verteilt, wobei ihre Bestandteile von den einzelnen Rechnern heruntergeladen und anschließend zusammengesetzt werden. Dies geschieht deshalb, um die Downloadgeschwindigkeit zu erhöhen. Dadurch ist gewährleistet, dass, wenn einer der angeschlossenen Rechner vom Netz gehen sollte, die verbliebenen Rechner die Daten noch komplett liefern können. Weiters besitzt dieser Client eine übersichtliche Suche, bei der alle Dateien zur jeweiligen Suchanfrage aufgelistet werden, welche zum Download im Netzwerk bereitstehen. Wie E-Donkey2000 lädt auch E-Mule die Dateien von mehreren Computern gleichzeitig. Fehlerhafte heruntergeladene Dateien werden erkannt und der Download wird nur mit den benötigten Teilen fortgesetzt. Wie bei E-Donkey2000 werden auf den Servern die Verzeichnisse aller freigegebenen Ordner der verbundenen Rechner gesammelt. Der Link zur gewünschten Datei nennt sich „ed2k“, er basiert auf dem E-Donkey2000-Netz [Wiki06k].

3.7.2 Bit Torrent

„The excitement about P2P systems has been encouraged by recent innovations that foster easier sharing of files, such as downloading simultaneously from multiple sources, and the sharing of many different file types, as well as improvements to the usability of these clients.”[GoKr03, 137]

Das Außergewöhnliche an BitTorrent ist seine extrem hohe Geschwindigkeit. Durch die spezielle Technik, die bei diesem Netzwerk verwendet wird, können die digitalen Daten viel schneller heruntergeladen werden als mit anderen Filesharingprogrammen. Um das zu bewerkstelligen, werden die einzelnen Dateien in viele kleine Fragmente zerlegt, welche zwischen den jeweiligen Nutzern übertragen werden. Nachdem der Download beendet wurde, können anhand des Übertragungsprotokolls die einzelnen Teile automatisch wieder zu einer vollständigen Datei zusammengesetzt werden. Ein Nutzer, welcher dieses Protokoll verwendet, muss daher nicht über die gesamte Datei verfügen, um nicht schon einzelne Teile anderen Nutzern anbieten zu können. Während das Programm beispielsweise noch einen Film herunterlädt, können andere BitTorrentnutzer einzelne Fragmente jenes Films erhalten. Desto mehr Benutzer sich in ein solch aufgebautes Netzwerk einwählen, desto schneller kann die Datei untereinander verteilt werden.

Auf das BitTorrentnetzwerk greift man anders zu, als man es von den anderen P2P-Programmen gewohnt ist. Um Dateien zu tauschen, bilden die Nutzer für jede einzelne Datei ein eigenes Netzwerk. Je mehr Nutzer gleichzeitig dieselbe Datei herunterladen, desto schneller wird die Verbindung. Durch diese Technik entstehen keine Wartezeiten auf einzelne Files. Im Vergleich zu anderen P2P-Programmen ist dabei die Downloadgeschwindigkeit sehr hoch. Daher eignet sich Bit Torrent vorzüglich für große Datenmengen, wie dies z.B.: bei Videos gegeben ist.

Anders als die sonstigen P2P-Clients besitzt das Programm jedoch keine Suchfunktion. Man geht stattdessen im Internet auf spezielle BitTorrentseiten oder Suchmaschinen. Dort sind die gerade zur Verfügung stehenden Dateien aufgelistet. Mit einem Klick auf die gewünschte Datei lädt sich der Anwender eine Art Infodatei herunter, den so genannten „Torrent“ (englisch für „reißender Strom“). Diese Datei aktiviert dann das BitTorrentprogramm. Anschließend fragt das Programm den Benutzer, wo die Datei auf seiner Festplatte gespeichert werden soll. Danach startet der Download [Wiki06I].

BitTorrent hat zwar selbst einen Erfinder, jedoch nicht einen Betreiber. Die Tauschbörse funktioniert dabei völlig dezentral und existiert allein durch die aktive Beteiligung ihrer Nutzer. Es gibt somit keine zentrale Instanz, welche man mit einer Klage zu einer Einstellung zwingen könnte.

3.7.3 Services von Filesharingclients

„In practise, more and more P2P software vendors are implementing such mechanisms, like providing peers with incentives for opening more shares in exchange for faster download speed, and offered the accounting functions in the software to protect against malicious users.“ [XuWT05, 209]

Filesharingdienste wie Bit Torrent oder eMule stellen einem Nutzer im Wesentlichen vier Services zur Verfügung:

1. Serversoftware und Netzwerk: Mit der Installation einer Filesharingsoftware kann ein Nutzer seinen PC zu einem Server innerhalb des Filesharingnetzwerkes definieren. Dabei kann ein Nutzer 0 bis n Dateien bereitstellen. Zumeist werden die Daten, welche ein Nutzer herunter lädt, automatisch in diesem Verzeichnis abgelegt, so dass das Download- dem Uploadverzeichnis entspricht.
2. Indexierung: Inhalte, die ein Anbieter auf seiner Festplatte zum Upload bereitstellt, werden indexiert und in einem Index abgelegt, der zentral oder dezentral geführt wird.
3. Download: Filesharingnetzwerke bieten eine Peer-to-Peer Verbindung an, welche einen Download der über den Index gefundenen Dateien bei einem oder mehreren Nutzern ermöglicht.
4. Verbunddienstleistungen: Neben dem Download von Dateien bieten die meisten Filesharingdienste zudem Community-Features, wie z.B. Instant Message, Hotlists, einen Player und andere Services an.

3.7.4 Sicherheit einer Peer-to-Peer Software

Laut Definition einer Studie ist eine Peer-to-Peer Filesharingsoftware sicher und brauchbar, wenn der Benutzer: [GoKr03, 139-142]

1. eindeutig weiß, welche Dateien für die anderen Nutzer zum Download bereitgehalten werden,
2. in der Lage ist zu bestimmen, wie man Files mit anderen Nutzern teilt und jederzeit erfolgreich aufhören kann, Dateien mit anderen zu tauschen,
3. keine schwerwiegenden Fehler begeht, die dazu führen können, unabsichtlich private Dateien mit anderen Filesharingteilnehmern zu teilen und
4. sicher darüber Bescheid weiß, was mit anderen ausgetauscht wird und zuversichtlich ist, dass das System die vorgenommenen Einstellungen richtig ausführt.

3.8 Anonymität beim Filesharing

Um Dateien auch weiterhin zu tauschen, ohne von IFPI, RIAA und Co angezeigt zu werden, gibt es einige Methoden, um im Internet unerkant zu bleiben. Damit es nämlich überhaupt zu einer Klage gegen einen Filesharer kommen kann, muss erst dessen Name und Adresse ermittelt werden. Die wichtigsten Methoden, wie sich dabei Filesharer vor Klagen der Industrie schützen können, werden hier kurz vorgestellt:

1. **IP-Adresse über Proxy verstecken:** Eine der einfachsten und sichersten Möglichkeiten, um im Internet unerkant zu surfen oder Dateien zu tauschen, ist das Verschleiern der eigenen IP-Adresse. Wer nämlich seine eigene IP-Adresse nicht preisgeben möchte, kann diese mit Hilfe eines so genannten Proxyserver verstecken. Ein Proxy ist in diesem Fall ein Server, welcher als eine Art „Zwischenstation“ beim Datenverkehr im Internet eingesetzt wird. Der große Vorteil bei dieser Methode ist, dass ausschließlich der Proxyserver erfährt, welche IP-Adresse der Internetuser besitzt. Der Webserver, welcher die eigentliche Anfrage des Internetnutzers bekommt, erhält dabei nur die IP-Adresse des Proxyserver. Der Nachteil dieser Variante ist jedoch eine beträchtliche Geschwindigkeitseinbuße, da alle Daten zusätzlich über den Proxyserver übermittelt werden. [Scho05a, 1-3]
2. **IP-Adressen blocken:** Dabei werden Programme eingesetzt, ähnlich einer Firewall, welche bestimmte IP-Adressen blocken. Der große Vorteil dabei ist, dass, wenn eine IP-Adresse von einem solchen Programm geblockt wird, der

dazu gehörige P2P-Client nicht mehr auf den eigenen Rechner zugreifen kann. Hierzu werden so genannte „Blacklists“ verwendet, in denen die entsprechenden IPs aufgelistet sind. Der Nachteil bei dieser Variante ist, dass solche Listen auch der Industrie bekannt, und daher nie ganz aktuell sind. Ist eine Blockfunktion dabei nicht schon im Filesharingprogramm enthalten (wie zum Beispiel in Kazaa Lite oder eMule), kann man auch ein externes Tool zum Blocken der IP-Adressen benutzen [Scho05b, 1-2].

- 3. Verschlüsselung des Datentransfers:** Hierbei werden die übermittelten Daten so verschlüsselt, dass für einen Außenstehenden nicht mehr ersichtlich ist, wer welche Daten wen zur Verfügung stellt. Weiters wird mittels spezieller Techniken die IP-Adresse verschleiert und eine Auflistung aller angebotenen Dateien unterdrückt. Vertreter dieser Methode sind Filetopia, Freenet oder Mute. Im Gegensatz zu anderen Filesharingclients werden hierbei jedoch keine Proxy-Server eingesetzt, sondern so genannte IP-Bouncer. Bei dieser Übertragungstechnik wird der gesamte Datenverkehr über einen anderen Rechner umgeleitet. Hierdurch erfahren daher weder Anbieter noch Downloader die echte IP ihres Gegenübers. Neben den bereits oben beschriebenen Varianten ist dieses Verfahren sicherlich das sicherste von allen. Jedoch hat diese Sicherheit der vorgestellten Netze seinen Preis. Sie sind längst nicht so bekannt und beliebt, wie zum Beispiel eMule. Das wirkt sich vor allem auf die Userzahlen, und damit auf die Anzahl der angebotenen Dateien aus. Weiters ist die Geschwindigkeit dieser Datenübertragung gering und sie weisen eine schlechte Performance auf. [Scho05c, 1-3].

3.8.1 Wenn Tauschbörsen Privates liefern

Neben dem Risiko erwischt zu werden, gibt es eine zweite, wesentlich größere Gefahr, nämlich das versehentliche Freigeben von Dateien. Fast alle Filesharingclients haben nach der Standardinstallation ein Verzeichnis, welches für den freien Tausch freigegeben ist. Alle Dateien, die sich also dort befinden, sind für die anderen Tauschbörsennutzer zum Abruf freigegeben. Dabei ist jedoch die Gefahr nicht sehr groß private Daten für andere zur Verfügung zu stellen, weil sich dort meistens nur die bereits heruntergeladenen Dateien befinden. Viele Filesharingclients bieten jedoch die Option an, dieses Verzeichnis mit einigen Mausklicks beliebig zu erweitern. Eine

falsche Einstellung führt daher schnell dazu, dass die gesamte Festplatte für den Datenaustausch im Internet freigegeben wird. Die Folgen sind dabei dramatisch, da nach einer solchen Freigabe alle privaten Daten für alle anderen Filesharinguser zum Download bereitstehen. Einen Schutz gegen diese „Komplettfreigaben“ gibt es nicht, nur das Verantwortungsbewusstsein des Anwenders kann ihn selbst vor weiteren Schäden schützen. [Rent05].

3.9 Wie kommen die Dateien in die Tauschbörsen?

Diese Frage wird stellvertretend für alle in Tauschbörsen verfügbaren Dateien anhand eines Filmreleases erörtert. Nach kurzer Zeit, als der letzte Teil der „Star Wars Saga“ im Kino präsentiert wurde, war der Film bereits auch schon im Filesharingnetzen verfügbar. Es gibt viele Wege, wie Filme wie „Star Wars“ in die Tauschbörsen gelangen können. *„In die Tauschbörsen kommen die Files über die verschiedensten Wege –DVD- und CD-Rips von Usern, aus anderen Tauschbörsen gezogenes Material, Stuff von FxPlern oder Releasegroups“* [Hott05a, 1]. Als FxPlern werden Personen bezeichnet, welche die digitalen Daten der Releasegroups der Öffentlichkeit zur Verfügung stellen. Sie sind daher hierarchisch betrachtet unterhalb der Releasegroups und oberhalb der Filesharinggroups einzuordnen. Am chancenreichsten sind jedoch Tauschbörsenreleases, wenn sie über eine entsprechende Community gestartet werden. Die Communities versuchen gezielt, einen Release schnell auf zahlreichen Rechnern in Netzwerk anzubieten, entsprechend sind die so gestarteten Tauschbörsenreleases in der Regel besser verteilt und länger für die User verfügbar. Verantwortlich für das Erscheinen von Filmen wie „Star Wars“ in den Tauschbörsen sind häufiger jedoch organisierte Gruppen, so genannte Release Groups. Von diesen gelangen die Dateien schließlich auch zu den Tauschbörsenreleasern, welche sich häufig in den entsprechenden Boards organisieren. An die Originale kommen die Releasegroups auf unterschiedliche Weise – eigene Rips, Quellen in der Releaseszene, Kontakte ins Kino – qualitativ gute Releases können beispielsweise auch an der entsprechenden Schnittstelle eines digitalen Projektors abgegriffen werden. Ist der Film erstmal in den Händen der Releasergroups, geht die Verteilung ganz schnell. *„Zuerst wird die Datei an die Gruppenmitglieder verteilt. Der Hash-, Torrent-, Esel- oder Applejuicelink wird in den entsprechenden Boards bzw. Seiten veröffentlicht, und dann wird die Datei auch*

gezogen werden – und entsprechend von den Leechern auch wiederum angeboten. Angesichts der zahlreichen Multi-Netzwerkclients kann man davon ausgehen, dass eine gut verteilte Datei dann auch zügig in andere Tauschbörsen auftaucht“ [Hott05a, 2].

Als „Leecher“ werden Benutzer in Tauschbörsen bezeichnet, welche nur Daten herunterladen möchten und nicht bereit sind, eigene als Gegenleistung hochzuladen oder anderen Benutzern eigene Dateien zum Download zur Verfügung zu stellen. Eine völlig andere Bedeutung kann der Begriff 'leechen' allerdings innerhalb des BitTorrent-Netzwerkes haben. Dabei sind „Seeder“ die Personen, die die Datei bereits vollständig geladen haben, und „Leecher“ die Personen, die gerade die Datei herunterladen – und normalerweise auch gleichzeitig hochladen [Wiki07b]. Genauso wie für Filme gibt es Releasegroups, welche sich nur auf Software, Musik oder andere digitale Formate spezialisiert haben. Es besteht jedoch auch die Möglichkeit, dass einzelne User selbst Dateien digitalisieren und anschließend für andere zum Download bereitstellen.

4 Urheberrecht

Das Urheberrecht stellt auf den Schutz des Herstellers eines Werkes ab und entstand mit der Entwicklung des Buchdrucks Ende des 15. Jahrhunderts. Damals stand zwar noch der Schutz der Verlage vor dem Schutz der Autoren, was sich mit der Entwicklung der Theorie vom geistigen Eigentum um 1700 jedoch änderte. Seit dieser Zeit wird auch der volkswirtschaftliche Aspekt des Urheberrechts anerkannt, wonach der Urheber durch Anreize zur weiteren Schaffung von Werken gebracht werden sollte.

Das heutige Urheberrecht ist Teil des Kulturrechts. Es hat dabei zwei Aufgaben zu erfüllen: erstens schützt es bestimmte kulturelle Geistesschöpfungen, was als objektive Aufgabe des Urheberrechtes verstanden werden kann, zweitens sichert es, als subjektive Aufgabe, dem Urheber gewisse Rechte an seinem Werk [Wiki06t].

Diese Rechte stehen dem Urheber unmittelbar nach Schöpfung des Werkes zu und es bedarf nicht, wie z.B. bei Patenten, Marken bzw. Trademarks der Eintragung in ein Register. Meistens hält das Urheberrecht seit dem 16. Jahrhundert am Grundsatz des Territorialitätsprinzips (beschäftigt sich mit der Frage, welches Recht auf welche Personen wann und an welchem Ort anwendbar ist. Generell sagt das Territorialitätsprinzip, dass alle Personen der Oberhoheit und den Gesetzen des Staates unterworfen sind) fest, es gibt jedoch auch einige internationale Abkommen, die für das Urheberrecht von Bedeutung sind.

Zu bedenken ist aber, dass das Urheberrecht nur die Form eines Werkes schützt, d.h. die Art und Weise seiner Zusammenstellung, Strukturierung und Präsentation. Die Idee, welche einem Werk zugrunde liegt, ist nicht geschützt. Je konkreter einzelne Gestaltungselemente übernommen worden sind, desto näher ist man an einer Urheberrechtsverletzung. Schwierig, ja fast unmöglich scheint aber die Grenzziehung zwischen Idee und Form.

4.1 Internationale Verträge und Copyright in den USA

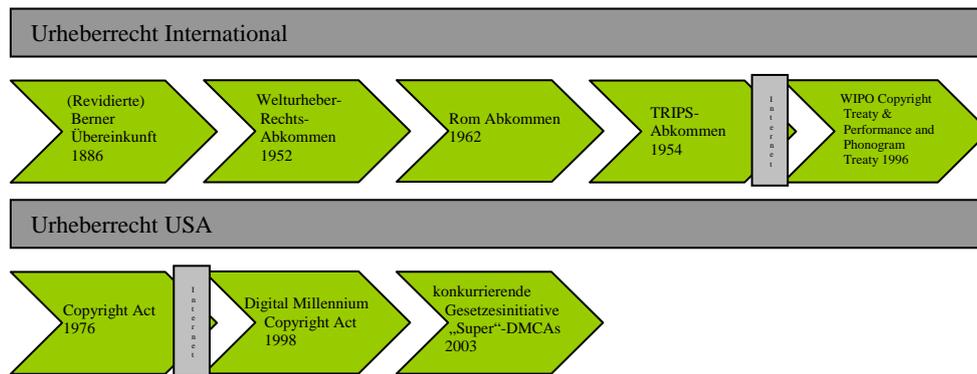


Abbildung 4: Übersicht Urheberrecht International und USA, nach [FrKa04, 58]

4.1.1 Revidierte Berner Übereinkunft

Die „Revidierte Berner Übereinkunft zum Schutz von Literatur und Kunst“ vom 09.09.1886 ist das wichtigste internationale Abkommen, welches sich mit Fragen zum geistigen Eigentum beschäftigt. An diesem Abkommen, welches zum ersten Mal die Anerkennung des Urheberrechts zwischen souveränen Staaten begründet und bereits siebenmal revidiert wurde, nehmen mittlerweile 150 Staaten teil [Wiki06v].

Mit diesem Abkommen werden jedem Urheber eines Mitgliedsstaates die gleichen Rechte wie einem inländischen Urheber zugesichert. Weiters sichert die Revidierte Berner Übereinkunft den Urhebern gewisse Mindestrechte zu, auf welche sie sich auch dann berufen können, wenn das inländische Recht weniger Schutz bieten würde. Seit der Gründung der World Intellectual Property Organisation (WIPO) 1967 wird die Revidierte Berner Übereinkunft von dieser verwaltet [FrKa04, 58-59].

4.1.2 Welturheberrechtsabkommen

Nach dem Beitritt der USA 1989 zur Revidierten Berner Übereinkunft verlor das von der UNESCO initiierte Welturheberrechtsabkommen, welches von 36 Staaten unterzeichnet wurde, seine Bedeutung, auf Grund der wesentlich weniger strengen Vorschriften [FrKa04, 58-59]

4.1.3 Rom-Abkommen

Dieses Abkommen von mehr als 56 Staaten unterzeichnet, regelt Probleme, welche sich mit der Angleichung und gegenseitigen Anerkennung von Leistungsschutzrechten der ausübenden Künstler, Tonträgerhersteller sowie Sendeunternehmen zwischen den einzelnen Mitgliedsstaaten befassen [FrKa04, 59].

4.1.4 TRIPS-Abkommen

Das „Trade Related Aspects of Intellectual Property Rights“- Abkommen entstand 1994 als Eckpfeiler des Gründungsvertrages der World Trade Organisation (WTO). Mit diesem Abkommen finden erstmals alle Aspekte des geistigen Eigentums Einzug in einen multilateralen Vertrag und ermöglichen härtere Sanktionen gegen Vertragsstaaten [TRIP06]. Da bei diesem Abkommen zum ersten Mal auch Computerprogramme und Datenzusammenstellungen besonders geschützt werden, können diese Teile des TRIPS-Abkommen als erste internationale Regelungen des Urheberrechts angesehen werden, welche einen Bezug auf das digitale Zeitalter aufweisen.

4.1.5 WIPO

Da man sich einig darüber war, dass die Probleme des digitalen Zeitalters das bestehende Recht überforderten, wurden 1996 zwei weitere bedeutende internationale Verträge geschlossen; der WIPO Copyright Treaty (WCT) und der WIPO Performance and Phonograms Treaty (WPPT). Diese sehr allgemein gehaltenen Regelungen schreiben erstmals vor, Urheber und andere Rechteinhaber vor Umgehung technischer Schutzmaßnahmen sowie vor Manipulation von elektronischen Rechtmanagementinformationen zu schützen.

4.1.6 USA

Das Copyright in den Vereinigten Staaten von Amerika basiert auf Art. I, Section 8 der US-Verfassung, worin es heißt: *“The Congress shall have power to lay and collect taxes, duties, imposts and excises, to pay the debts and provide for the common defense*

and general welfare of the United States; but all duties, imposts and excises shall be uniform throughout the United States; (...) to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Investors the exclusive Right to their respective Writings and Discoveries“ [USCON06].

4.1.7 Copyright Act

Aufgrund der Ermächtigung in der US-Verfassung erließ der Kongress 1976 den bis heute gültigen Copyright Act. Die einzelnen Urheber erhalten demnach das exklusive Recht, ihre Werke zu vervielfältigen, zu reproduzieren sowie zu verteilen, darzustellen und auszustellen [USC06]. Zu den wichtigsten Ausnahmen der exklusiven Verfügungsgewalt der Urheber gehören die

- „First-Sale-Doktrin“
- „Public domain“ und die
- „Fair-use Doktrin“.

Die First-Sale-Doktrin regelt, dass der Käufer einer rechtmäßigen Kopie urheberrechtlich geschützter Werke diese Kopie weiter verkaufen kann, ohne dabei Gebühren an den Urheber abgeben zu müssen. Ein Werk wird dann als „public domain“ bezeichnet, wenn es nach dem 1.1.1978 entstanden und älter als 70 Jahre ist. Treffen diese Tatbestände zu, kann das Werk ohne Erlaubnis des Urhebers verwendet werden. Als „Fair-use“ bezeichnet man eine Rechtsdoktrin dann, wenn man Personen eine bestimmte Nutzung eines Werkes ohne die Zustimmung des Urhebers zugesteht, sofern sie der öffentlichen Bildung und der Anregung geistiger Produktionen dient. Sie wird dort eingesetzt, wo zu hohe Transaktionskosten die Vereinbarung von Lizenzen verhindern würde und erfüllt damit eine vergleichbare Funktion wie die Schrankenbestimmungen des kontinentaleuropäischen Urheberrechts [Wiki06m].

4.1.8 Digital Millenium Copyright Act

Der Digital Millenium Copyright Act (DMCA), welcher im Jahr 1998 verabschiedet wurde, setzt die Vorgaben der WIPO-Verträge um. Der Digital Millenium Copyright

Act versucht die Gegebenheiten, welche sich durch die digitale Reproduktion von „perfekten Kopien“ ergeben, zu regeln [Wiki06n].

Dabei führen die nicht genau festgelegten Schranken der „Fair-use-Doktrin“ zu heftigen Diskussionen, da der DMCA das vollständige Verbot der Umgehung von technischen Schutzmaßnahmen vorschreibt. Dies bedeutet, dass User, selbst wenn eine Umgehung des Kopierschutzes im Sinne des „fair-use“ in Frage käme, dieses Recht nicht ausnutzen dürfen, weil sie ohne die Umgehung von technologischen Schutzmaßnahmen keine Kopie des Werkes erstellen können [FrKa04, 61-62].

4.1.9 Konkurrierende Gesetzesinitiativen „Super“ DMCAs

Viele Bundesstaaten in den USA, gerieten unter den Druck der Motion Picture Association of America (MPAA), da sie vorschrieben, strengere Gesetze einzuführen, welche Copyright Sünder härter bestrafen sollten. Im Gegensatz zum Digital Millennium Copyright Act regeln die "Super-DMCAs" urheberrechtliche Fragen nicht auf Ebene des Bundes, sondern auf Ebene der einzelnen Bundesstaaten [EFF06].

4.1.10 Exkurs: Copyright

Programmieren von Software kann mit dem Komponieren von Musik verglichen werden, es ist nämlich kreative geistige Arbeit. Komponierte Lieder kann jeder nachspielen, welcher die Fähigkeit besitzt, Noten zu lesen, programmierte Software kann technisch beliebig oft kopiert werden. Deswegen gibt es für Computerprogramme wie für Musik ein Copyright. Der Komponist oder der Programmierer kann selbst entscheiden, wer sein Werk wann und wie benutzen darf. Ein Softwareentwickler hat hierzu mehrere Möglichkeiten zur Auswahl. Erstens kann er die Nutzung seiner Software freigeben, wie dies bei Freeware der Fall ist. Zweitens kann er alle Details seiner Programmierung offen legen, also den Quellcode anderen zur Verfügung stellen, damit andere sein Programm weiterentwickeln können, wie bei Open Source Software. Drittens kann er die Software, aber auch gegen Lizenz allen Interessenten zur Verfügung stellen, die Details seiner Programme jedoch für sich behalten. Wer jedoch ein Softwareprogramm kauft, erwirbt damit nicht, wie die meisten glauben, die Eigentumsrechte an den Programmen, sondern ausschließlich das Nutzungsrecht über

eine Lizenz. Das Urheberrecht und damit das Eigentumsrecht hat weiterhin nur der Programmierer.

Laut dem Wissenschaftler Lawrence Lessing haben Gesetze und Regulierungen im Gebiet des Copyrights derartige Ausmaße angenommen, dass sogar große Unternehmen zum Teil davor zurückschrecken, innovativ zu handeln: Dabei wird die gewohnte Art und Weise, in welcher Menschen Kultur erschaffen und teilen, durch gesetzliche Beschränkungen eingeengt, deren Kontrolle sich dann weiters auf die Kreativität und Kultur ausdehnt, wie dies nie zuvor der Fall war [Less03, 8].

4.2 Urheberrecht in Europa

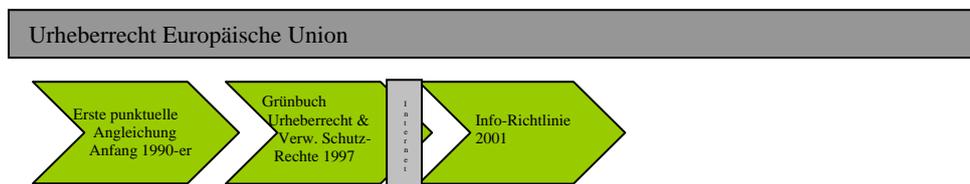


Abbildung 5: Übersicht Urheberrecht Europa, nach [FrKa04, 62]

Da das Urheberrecht im EG-Vertrag nicht erwähnt wird, beschäftigt sich das Europäische Recht erst spät mit dieser Thematik. Das Hauptproblem in Europa ist, dass der Schutz der Urheber meistens auf nationales Urheberrecht beruht, trotz der vielen internationalen Verträge an denen viele Beitrittsländer beteiligt sind. So wird das geistige Eigentum, das in ganz Europa einheitlich behandelt werden sollte, in jedem einzelnen Mitgliedsland unterschiedlich gehandhabt. Die Folgen, welche sich aus der Vielfalt der einzelnen Urheberrechte ergeben, sind zum einen, dass der Schutz der Urheber nicht in allen Mitgliedsstaaten gleichermaßen gewährleistet ist und zum anderen, dass durch die unterschiedliche Rechtsauffassung der Binnenhandel in Europa behindert wird.

Aus dieser Problematik entstand 1988 das Grünbuch über Urheberrechte, welches das erste Dokument der Kommission darstellte, das sich mit der Notwendigkeit einer Harmonisierung im Bereich Urheberrecht und verwandte Schutzrechte in einem konzeptionellen Rahmen befasste. Die Grundlage dieses Grünbuches war stets der Art. 94 EG-Vertrag, welcher die Schaffung eines gemeinsamen Marktes vorsieht, der durch einen Abbau der nationalen Urhebergesetze eine allmähliche Angleichung des

Urheberrecht vorsieht [o.V.06c]. Trotz dieser Bemühungen konnte kein einheitliches europäisches Urheberrecht erzielt werden.

Einige Jahre später im Jahr 1995 entstand als Grundlage eines neuen Ansatzes der EG zur Harmonisierung und nicht zum Abbau von nationalen Gesetzen ein „Grünbuch für Urheberrecht und verwandte Schutzrechte“. Aufbauend auf dieses wurde 1997 ein Richtlinienvorschlag der EG-Kommission entwickelt, welcher die Harmonisierung bestimmter Aspekte des Urheberrechtes und verwandter Schutzrechte in der Informations-Gesellschaft behandelte.

Die endgültige Richtlinie (Info-RL) trat erst am 22. Juni 2001 in Kraft. Die Grundlage für die Info-RL waren die WIPO-Verträge, welchen man kurz zuvor am 16. März 2001 beigetreten ist. Dabei sind die einheitlichen Vervielfältigungsrechte sowie das Exklusivrecht der Urheber, die öffentliche Wiedergabe oder das öffentliche Zugänglichmachen zu erlauben oder zu verbieten, inhaltlich hervorzuheben. Weiters bestehen bestimmte Ausnahmefälle, wie die private Kopie, welche von den einzelnen Mitgliedsstaaten selbst geregelt werden können. Es werden aber auch Bestimmungen zum Schutz von technischen Maßnahmen und von Informationen zur Rechtewahrnehmung umgesetzt. Die Info-RL bildet somit das Fundament ähnlich dem DMCA in den USA für die Verwendung von DRMS in Europa [o.V.06d].

Dabei ist festzuhalten, dass bei der Europäischen Gemeinschaft im Gegensatz zur US-amerikanischen Auffassung nicht das copyright law im Mittelpunkt steht, sondern die Beziehung des Urhebers zu seinem Werk.

4.3 Urheberrecht in Österreich

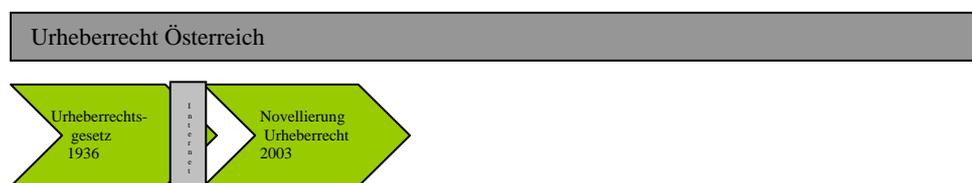


Abbildung 6: Übersicht Urheberrecht Österreich

Das Urheberrechtsgesetz aus dem Jahr 1936 ist eines der ältesten in ganz Europa. Auch das Österreichische Urheberrecht ist im Gegensatz zum US-amerikanischen von der Beziehung des Urhebers zu seinem Werk geprägt. Dieser Urheberpersönlichkeitsschutz

hebt die künstlerischen und ästhetischen Interessen des Urhebers an seinem Werk in den Vordergrund und lässt die wirtschaftliche Komponente des Urheberrechts verblassen. Durch die Sicherung einer angemessenen Vergütung und durch die starke Eigentümerstellung des Urhebers bezüglich seiner Schöpfung soll ein Anreiz für den Urheber geschaffen werden, damit er weiter Werke herstellt. Im Gegensatz zum US-amerikanischen Recht können in Österreich aber nur natürliche Personen und nicht juristische Schöpfer eines Werkes sein.

Das Urheberrecht schützt den Urheber in zwei Bereichen. Es gewährt im einerseits den Urheberpersönlichkeitsschutz, der eine Ausweitung des grundrechtlich festgelegten allgemeinen Persönlichkeitsschutzes darstellt. Andererseits gewährt es ihm gem. §14-25 UrhG Verwertungsrechte bzgl. seines Werks, die ähnlich denen des §106, 17 U.S.C sind [UrhG06, USC06]

Die Novellierung des Urheberrechtes im Jahr 2003 setzt die Richtlinie umfassend um und geht teilweise sogar einen Schritt weiter. Für digitale Medien und das Internet ist besonders das Vervielfältigungsrecht sehr bedeutend. Es gewährt dem Urheber das exklusive Recht, ob und wie oft sein Werk vervielfältigt werden darf oder nicht. Eine Besonderheit stellt die Vervielfältigung zum eigenen und zum privaten Gebrauch dar, die in § 42 UrhG geregelt wird. Demnach darf jedermann von einem Werk einzelne Vervielfältigungsstücke auf Papier oder einem ähnlichen Träger zum eigenen Gebrauch herstellen. Weiters darf er Vervielfältigungsstücke auf anderen Trägern zum eigenen Gebrauch zu Zwecken der Forschung herstellen, soweit dies zur Verfolgung nicht kommerzieller Zwecke gerechtfertigt ist [UrhG06].

Der Schutz des Urhebers endet laut § 60, wie auch in den meisten anderen Ländern, 70 Jahre nach dem Tod des letzten Miturhebers [UrhG06].

4.4 Aktuelle Probleme im Urheberrecht

„Die explosionsartige Vervielfältigung der technisch erreichbaren Informationsmöglichkeiten verlangt vom Mediennutzer ein viel größeres Maß an souveräner Entscheidungskompetenz.“ [Berg99, 261]

Mit der immer steigenden Bandbreite und höheren Datendurchsatz erhöht sich auch die Bedeutung des Internets für die Distribution und Nutzung geistigen Eigentums. Durch

immer niedrigere Online-Kosten auf Anbieter- und Nutzerseite, d.h. billiger großer Speichermedien und kostengeringer breitbandiger Internetanbindungen gewinnt der multimediale Datenaustausch weiter an Attraktivität. Das österreichische Urheberrecht ist von 1936 und die Gesetzeslage stellt sich erst langsam auf diese Neuheiten ein. Gesetzesvielfalt und –umfang hat mittlerweile ein Ausmaß angenommen, bei welchem die Legislative mit Anpassungen und Modernisierungen kaum noch hinterherkommt.

„..., the decentralized and anonymous characteristics of P2P environments make the task of controlling access to sharing information more difficult, which cannot be done by traditional access control methods.“ [THVW05, 302]

Das Hauptproblem, welches sich für den Gesetzgeber ergibt, ist zweifelsfrei das illegale Kopieren von digitalen Medien über das Medium Internet. Obwohl es diesen Missstand bereits Anfang der 90er Jahre gab, war er damals durch die niedrigen Bandbreiten und kaum verwendeten Kompressionsverfahren hauptsächlich auf Text- und Grafikdateien beschränkt. Die enorme wirtschaftliche Auswirkung des illegalen Kopierens wurde erst Ende der 90er Jahre deutlich, als es technisch für jeden User möglich wurde über das Internet Audio- und Filmdateien zu vertreiben. Die bekannteste Peer-to-Peer-Filesharingsystem, welches vor allem durch die Verbreitung von Audiodateien bekannt wurde, war Napster, welche im Juli 2001 ihren unkommerziellen Dienst nach zahlreichen gerichtlichen Revisionen einstellen musste. Jedoch entstanden nach Napster eine Vielzahl anderer Peer-to-Peer Systeme, wie zum Beispiel Bit Torrent, Emule, Limewire oder Morpheus, die seither gegen die rechtlich herrschende Meinung eine Daseinsberechtigung zu erlangen versuchen. Nach österreichischem Recht verstoßen Onlinetauschbörsen dieser Art zweifellos gegen das Urheberrecht, da sie zur Verbreitung von illegalen Kopien verwendet werden.

Diese Entwicklung führt zu zwei folgeschweren Problemen. Erstens muss die Frage beantwortet werden, inwieweit Vervielfältigungen von digitalen Werken erlaubt sein sollen und ab wann jegliche Art von Vervielfältigung bestraft werden muss. Zweitens muss ein gerechter Ausgleich zwischen den Urheber- und Nutzerinteressen gefunden werden [Ruiz03, 1-2].

Die erste Frage, ob man rein technisch bedingte Vervielfältigung, welche keine ökonomischen Auswirkungen hat, wie zum Beispiel das Zwischenspeichern von Daten im Hauptspeicher eines Computers als gesetzwidrig einstufen sollte, wurde bereits bei

den Verhandlungen zu den WIPO-Verträgen 1996 diskutiert. Da es jedoch verschiedene Auffassungen zu diesem Problem gab, wurde auf eine explizite rechtliche Regelung verzichtet. Allerdings haben einige europäische Staaten diese Frage durch die Umsetzung der Info-RL in nationales Recht geregelt und schlossen vorübergehende Vervielfältigung aufgrund eines technischen Verfahrens vom urheberrechtlichen Schutz aus. In der Europäischen Union und in Österreich wurde diese Problematik jedoch zunächst ignoriert. Die exakte Auslegung, was den Umgehungsschutz technischer Schutzmaßnahmen zu Lasten der Nutzer betraf, wurde sogar durch die Urheberrechtsnovellierung im Jahr 2003 erweitert und wird im § 90c ausführlich angeführt [UrhG06]. Die Musikindustrie sieht diese harte Haltung zugunsten der Urheber als gerechtfertigt an, da sie Raubkopien aus dem Internet als Hauptgrund für ihren Umsatzrückgang in den letzten Jahren ansieht.

Das zweite Anliegen, der Ausgleich zwischen den einzelnen Interessen, konnte bis heute nicht zufrieden stellend gelöst werden.

Das Problem liegt jedoch nicht an den fehlenden rechtlichen Regelungen im Gesetz, sondern vielmehr an dem Problem, dieses in der Realität durchzusetzen. Die konkrete Durchsetzung scheitert dabei an der hohen Anzahl von Delikten, deren lückenlosen Erfassung sowie an den dadurch entstehenden hohen Kosten. Da das Herunterladen von Kopien aus dem Internet gesellschaftlich von vielen Personen bereits nur noch als Kavaliersdelikt abgetan wird, sprechen einige schon vom Tod des Urheberrechtes [Barl06].

Eine Lösung für dieses Dilemma könnte die Einführung von modernen DRMS bringen. Die rechtliche Basis für solche Systeme sind die strengen Regelungen in Bezug auf technische Schutzmaßnahmen. Da jedoch durch die in Europa erfolgte Erlaubnis der digitalen Privatkopie durch die einzelnen Gesetzgeber in Verbindung mit der Vorschrift der Info-RL, dass technische Schutzmaßnahmen nicht umgangen werden dürfen, können auch in diesen Bereich Probleme mit der Umsetzung in DRMS entstehen. Um jene Barrieren zu beseitigen, müsste ein DRMS entwickelt werden, welches private Kopien erlaubt, ohne dass es umgangen werden muss. Eine Möglichkeit dieses Vorhaben umzusetzen, wäre eine individuelle vertragliche Vereinbarung zwischen Urheber und Nutzer [Bech02, 154-178].

4.5 Ausblick Urheberrecht

„Ohne ein funktionierendes Urheberrecht, welches den modernen digitalen und globalen Gegebenheiten angepasst wird und in das Bewusstsein der gesamten Bevölkerung eindringt, verlieren Künstler und Kulturwissenschaft die wirtschaftliche Basis.“ [Gutm03, 33-34]

Ob das Urheberrecht jetzigen Typs generell bestehen bleiben wird oder wie es sich weiter entwickelt, ist derzeit noch offen. Dass jedoch das Urheberrecht komplett abgeschafft wird, was einige befürchten, erscheint unrealistisch, da das Urheberrecht, wenn auch nicht in der derzeitigen Form, grundsätzlich bestehen bleibt. Dies ergibt sich aus der Notwendigkeit von Schrankenbestimmungen, ohne welche ein Interessensgleichgewicht zwischen Urhebern und Konsumenten nicht zu erreichen wäre.

Die Schrankenregelungen müssen insgesamt in rechtsvergleichender Perspektive neu eingeordnet werden. Es kann nämlich einfach nicht richtig sein, dass die Nutzung von Werken in einigen Ländern frei, in anderen wiederum nur gegen Vergütung oder sogar nur mit der Zustimmung der Rechteinhaber zulässig ist. Deshalb ist vor allem im Interesse der Rechtesicherheit und des Verkehrschutzes eine transnationale Angleichung der Schranken geboten [Hoer03, 56].

Im digitalen Zeitalter ist dieses Gleichgewicht zwischen den einzelnen Interessen nur schwer zu erzielen und daher ist das bestehende Urheberrecht in vielen Fällen nicht mehr durchsetzbar. Auf lange Sicht muss sich daher das Urheberrecht auf die gegebene Situation anpassen, was nur mittels eines starken Wandels erreicht werden kann. Das Hauptproblem mit dem dabei der Gesetzgeber konfrontiert wird, ist, dass illegales Kopieren von digitalen Werken gesellschaftlich nicht mehr als Vergehen angesehen wird und daher der Sinn und Wert von urheberrechtlichen Schutzmechanismen nicht erkannt und akzeptiert wird. Eine Option, um eine gesellschaftliche Akzeptanz zu erreichen, wäre es, das Urheberrecht als exklusives wirtschaftliches Verwertungsrecht zu definieren [Litm01, 180]. Dadurch würde das Urheberrecht für die breite Masse wesentlich leichter durchschaubar, was zur Folge hätte, dass es auch von mehr Personen akzeptiert wird.

Eine andere Möglichkeit besteht darin, dass der Urheber durch DRMS mittels Zwang seine Interessen auch gegen eine grundsätzliche gesellschaftliche Nichtakzeptanz

durchsetzt. Dadurch werden individuelle Nutzungsverträge zunächst durch technische Schutzmaßnahmen gesichert und diese wiederum von Umgehungsverboten. Das Urheberrecht würde erst als letzte Instanz als schwächster Schutzmechanismus eingreifen [Bech02, 371-373]. Als gerechter Interessenausgleich kann man in diesem Zusammenhang nicht sprechen, da der Konsument durch solche Systeme in seinen Rechten, das digitale Werk zu nutzen, beschnitten wird.

„Es sind ganz neue Wege zur Lösung der Copyright-/Urheberrechtsfrage im digitalen Medium nötig, die dem Rechnung tragen können, dass einerseits mit Informationsprodukten Geld verdient werden kann, andererseits die freie Nutzung von Information unter fairen Bedingungen weiterhin gestattet wird“ [Kuhl03, 131].

Den Einwand, dass man nicht objektiv und messbar festlegen kann, was denn „fair“ sei, kann man nicht gelten lassen. Anders als das europäische Urheberrecht kannte das amerikanische System sehr wohl einen „fair use“ –Begriff, mit dem man, gerade weil er nicht definiert war, bislang gut zurechtkam. Auch im Sport weiß jeder, was „fair play“ ist. Man einigt sich übereinstimmig, was jeweils darunter zu verstehen ist. Es kommt also auf die Balance des freizügigen Umgangs mit Wissen und Information an.

Es besteht daher ein dringender Handlungsbedarf, das Urheberrecht in Bezug auf digitale Medien anzupassen. Dass sich jedoch die urheberrechtlichen Gesetze fundamental ändern werden, ist jedoch nicht anzunehmen. Denn zum einen werden analoge Vorgänge weiterhin auch in Zukunft bestehen bleiben, und zum anderen ist das bestehende Urheberrecht mit Hilfe der juristischen Auslegungsmethoden auf viele Probleme der heutigen Zeit anwendbar.

5 Rechtliche Grundlagen zur Vervielfältigung und Bewertung des Filesharings aus urheberrechtlicher Sicht

Die Übermittlung von Texten, Bildern, Grafiken, Computerprogrammen, Tonaufnahmen und Videofilmen, modern auch zusammenfassend „content“ oder „Inhalt“ genannt, über das Internet betreffen das Urheberrecht direkt und werfen eine Vielzahl neuer Fragen auf.

Der Hauptunterschied zwischen klassischer und Online-Nutzung liegt zunächst im digitalen Dateiformat. Es stellt sich im Zusammenhang mit digitalen Medien die Frage der urheberrechtlichen Behandlung von digitaler Schöpfung und Digitalisierung analog vorhandenen Materials. Während in traditionellen Medien schon äußerlich wahrnehmbare Unterschiede vorliegen, verschwimmen alle Werkarten im Onlinebereich im digitalen Format. Ein Bild im Internet besteht genauso wie ein Text oder ein Musikstück aus binären Informationen, d.h. Nullen und Einsen. Durch die netzaufbaubedingte Datenübermittlung des Internets liegen bei der Datenübermittlung im Internet nur einzelne Teilstücke vor. Ein übermittelter Datenblock kann sowohl den Teil eines Bildes als auch eine Musiksequenz enthalten. Kommt noch eine Komprimierung oder eine Verschlüsselung hinzu, ist eine Zuordnung unmöglich.

Auch die neuen Dienste bewegen sich nicht in einem rechtsfreien Raum. Was offline strafbar ist, bleibt auch online strafbar. Die grenzüberschreitende Vernetzung lässt es jedoch zumindest als problematisch, in der Regel sogar als unmöglich erscheinen, die Verursacher etwaiger Rechtsverstöße zu fassen. Der einzelne Staat als Ordnungsmacht und Sanktionskraft stößt daher bei Rechtsverstößen sehr schnell an seine Grenzen.

Im Folgenden soll ein typischer Tauschvorgang, wie er jeden Tag millionenfach zwischen Nutzern von Filesharingnetzen stattfindet, urheberrechtlich untersucht werden. Zum einen wird die Seite des Anbieters betrachtet, welcher ein urheberrechtlich geschütztes Werk in ein Filesharingnetzwerk für die anderen Nutzer bereitstellt. Zum anderen wird die Seite des Abnehmers untersucht, also diejenigen Personen, welche aus dem Filesharingnetzwerk urheberrechtlich geschützte Werke auf ihren Rechner herunterladen. Dabei wurden ausschließlich rechtliche Interpretationen des deutschen Rechtes verwendet und es wurde versucht, diese analog auf die österreichische

Gesetzeslage anzuwenden. Die jeweiligen Vorgänge werden anhand einer MP3-Datei, also einer komprimierten, digitalen Fassung eines Musikstückes untersucht. Die Beschränkung auf ein MP3-File geschieht dabei vornehmlich aus Gründen der Übersichtlichkeit. Die einzelnen Ausführungen gelten jedoch insoweit auch für andere urheberrechtlich geschützte Werke, wie beispielsweise Filmwerke oder literarische Werke. Auch diese kommen, sofern sie über Filesharingnetze angeboten werden, größtenteils in einem komprimierten oder zumindest sonstigen digitalisierten Format vor (Filmwerke z.B.: mittels DivX-Codec komprimiert, literarische Werke zumeist im PDF-Format der Firma Adobe). Die Betrachtung erfolgt auf Grundlage des österreichischen Urheberrechts, wie es sich nach Umsetzung der EU-Richtlinien zum Urheberrecht in der Informationsgesellschaft darstellt.

5.1 Der Eigentumsbegriff

Unser historisch gewachsenes und gesellschaftlich etabliertes Verständnis von Eigentum stammt aus dem Zeitalter der Aufklärung. Dieser Eigentumsbegriff bezieht sich auf Gegenstände bzw. Sachen und vermittelt dem Einzelnen ausreichende Anhaltspunkte für die Verhaltensregeln. Abgesehen von wenigen Ausnahmesituationen sind wir in unserer Gesellschaft jederzeit in der Lage zu erkennen, mit welcher Eigentumssituation wir es zu tun haben und wie wir uns in dieser Situation verhalten sollen. Fälschlich wird nun dieses historisch gewachsene Eigentumsverständnis auf Gegenstände übertragen, deren Inhalte urheberrechtlich geschützt sind. Denn bei einem Kauf einer DVD zum Beispiel erwirbt man nicht das Eigentum der Inhalte, welche sich auf diesem Medium befinden, sondern nur eingeschränkte Verfügungs- oder Nutzungsrechte. Jedoch auch in einem zweiten Fall scheitert die Übertragung unseres intuitiven Rechtsverständnisses auf den urheberrechtlich geschützten Inhalt. Denn während wir eine Tat, bei der ein Gegenstand seinem Besitzer weggenommen wird, intuitiv als unrechtmäßig verurteilen, fehlt uns dieses Verständnis bei der Kopie, weil das Tatbestandsmerkmal der Wegnahme fehlt und damit die Figur des „Wegnehmens“, die unserem historisch gewachsenen Bewusstsein von Eigentum und Diebstahl zu Grunde liegt, nicht mehr greift. Zwar ist durch vielfältige Aufklärung über das Urheberrecht und den korrekten Umgang mit urheberrechtlich geschützten Werken erreicht worden, dass kaum noch jemand entschuldigend auf fehlende Kenntnisse

verweisen kann, was jedoch immer noch bei den allermeisten Menschen fehlt, ist ein intuitives Rechtsempfinden, das mit den Regelungen des Urheberrechts übereinstimmt. *„An diesem Punkt wird es helfen, wenn sich mit der Zeit mehr und mehr der Begriff der Verfügungsrechte in den Köpfen der Verbraucher etabliert.“* [Wöbk04, 30]. Es sollte daher in Zukunft beim Kauf digitaler urheberrechtlich geschützter Inhalte nicht von Eigentum gesprochen werden, sondern nur noch von einem Erwerb eingeschränkter Verfügungsrechte. Dieser Erwerb von Verfügungsrechten sagt aus, dass der Nutzer im Gegensatz zu einem Eigentum die geschützten digitalen Inhalte nur in ganz bestimmten Zusammenhängen sich zunutze machen darf, welche durch die jeweiligen Lizenzbestimmungen eindeutig geregelt werden. Ein weiterer förderlicher Ansatz liegt in der Strategie, dem einzelnen Verbraucher keine physischen Gegenstände mehr in seine Hand zu geben, welche ihm nahe legen, sich als wahrhafter Eigentümer jener Gegenstände zu fühlen. Auf diesem Weg stellt sich dann nämlich die Frage nach dem rechtmäßigen Umgang mit den auf dem Datenträger vorhandenen urheberrechtlichen geschützten Inhalten gar nicht mehr. Beide Ansätze, die Änderung der sprachlichen Regelung ebenso wie die Vermeidung von physischen Gegenständen, wird in Zukunft der Gesellschaft helfen, eine Kultur des Umgangs mit geistigem Eigentum in der digitalen Welt zu etablieren [Wöbk04, 30-31].

5.2 Schutzprinzipien im Internet

„Wenn Sie sich vorstellen, dass wir mit dem Internet ein globales Medium haben, bei dem eine einzige Oase das gesamte Rechtssystem zu Fall bringen kann, ahnen Sie, welche Pandoradose wir mit dem Internet aufgemacht haben“ [Pico03, 140].

„Alles, was man braucht, ist ein Server in einem Land, in dem es keine Gesetze gegen den Diebstahl von Urheberrechten gibt, und davon gibt es reichlich“, erläutert Martin Smith [McCa01, 7].

Bedingt durch den Aufbau des Internets kann unabhängig vom eigenen Standort weltweit auf jeden an das Internet angeschlossenen Rechner zugegriffen werden. Aufgrund der oftmals unterschiedlichen Rechtsordnung der potentiellen Zielländer treten zwangsläufig Probleme bei der Rechtsanwendbarkeit auf. Für das Urheberrecht

ergibt sich somit das Problem, welche nationale Rechtsordnung Anwendung findet, wenn in einem Land urheberrechtliche Werke auf einem Server angeboten und in verschiedenen anderen Ländern abgerufen werden.

Bisher wurden hierzu verschiedene Lösungsansätze in der Literatur entwickelt. Die hauptsächlich verbreiteten Ansatzpunkte sind das [EnBV02, 406-437]:

- Schutzlandprinzip
- Abruflandprinzip
- Ursprungslandprinzip.

5.2.1 Das Schutzlandsprinzip

Das Schutzlandprinzip besagt, dass immer das Recht des Landes anzuwenden ist, für dessen Gebiet Schutz begehrt wird. In der Praxis ist demnach zumeist maßgeblich, in welchem Land die Urheberrechtsverletzung stattgefunden hat. Die Anwendung des Schutzlandprinzips kann dazu führen, dass mehrere nationale Rechtsordnungen parallel betroffen sind [EnBV02, 407].

5.2.2 Das Abruflandprinzip

Das Abruflandprinzip vereinfacht dagegen und sieht das Recht des Staates für anwendbar, von dem aus das Werk angeboten wird, d.h. der Server steht. Das Problem dieses Ansatzes liegt in der Möglichkeit desjenigen, welcher ein Werk ohne Erlaubnis nutzen möchte, einfach und beliebig einen Staat mit geringer Urheberrechtsbestimmung auszuwählen und dort die Verwertungshandlung vorzunehmen, etwa ein digitales Werk auf einem Server zum Abruf anzubieten [EnBV02, 428].

5.2.3 Das Ursprungslandprinzip

Folgt man dem Ursprungslandprinzip, ist ausschließlich das Urheberrecht des Landes heranzuziehen, in welchem das Werk erstmalig veröffentlicht wurde oder bei unveröffentlichten Werken das Recht des Heimatstaates des Urhebers. Für den Nutzer

würde dies jedoch bedeuten, dass er vor jedem Abruf eines Inhaltes zunächst den Urheber ausfindig machen und anschließend das unter Umständen ausländische Recht auf Zulässigkeit seiner beabsichtigten Nutzungshandlung prüfen müsste. Gerade im Internet ist dies fast unmöglich [EnBV02, 437].

Keiner der theoretischen Ansätze hat bisher zu einer umfassenden befriedigenden Lösung für die Urheber und Rechteinhaber sowie für die Nutzer geführt. Derzeit neigen die Rechtsprechung und auch die Literatur dazu, dem Schutzlandprinzip den Vorzug zu geben [EnBV02, 437].

5.3 Abruf eines digitalen Werkes

Der Abruf eines digitalen Werkes durch den Nutzer stellt aus technischer Sicht notwendigerweise das Auslösen einer Reihe von Kopiervorgängen dar. Die Daten werden hierzu von der Festplatte in den Arbeitsspeicher (RAM) des Servers geladen, von dort über das digitale Netzwerk „Internet“ verschickt, hierbei in Speichern von unzähligen Routern und eventuell Proxy-Servern zwischengespeichert. Danach in den Arbeitsspeicher des Hostcomputers kopiert, meist vom Browserprogramm im Cache zwischengelagert und anschließend auf der Festplatte des Nutzercomputers zum Verbleib abgespeichert bzw. auf dem Monitor angezeigt oder eventuell auf einem Drucker ausgegeben. Es werden daher bei jedem Vorgang des Herunterladens oder auch nur Betrachtens von digitalen Inhalten im Internet eine Vielzahl von Speichervorgängen ausgelöst. Es stellt sich in diesem Zusammenhang die Frage, ob hier jeweils die Verwertungsrechte des Schöpfers, im Besonderen das Vervielfältigungsrecht, betroffen ist und wem diese Handlungen zuzurechnen sind. Nach den allgemeinen Grundsätzen ist eine Handlung demjenigen zuzurechnen, der das Geschehen beherrscht, d.h. steuernd in Händen hält. Im obigen Kopiervorgang ist dies der Nutzer, welcher durch das Herunterladen eine Reihe von Kopiervorgängen auslöst. Eine Ausnahme ist der Proxy-Caching-Vorgang, bei dem der Datenvermittler aktiv in den Kopiervorgang eingreifen kann, d.h. diese Kopiervorgänge sind dem Vermittler des Proxy-Servers zuzurechnen.

5.3.1 Download

Unter den Begriff Download versteht man das gezielte Herunterladen von Dateien eines Servers auf den eigenen Rechner, um diese dann auf der eigenen Festplatte abzuspeichern. Im Gegensatz zum Aufrufen von Internetseiten, was eigentlich auch nur ein Abruf, d.h. Herunterladen von einzelnen Daten bedeutet, geht es dem Nutzer beim Download gerade darum, die entsprechende Datei auffindbar zur weiteren Verwendung abzuspeichern und nicht nur kurzfristig für den Augenblick des Ansehens im Internetbrowser zur Verfügung zu haben. Der Download etwa von Programmen, Bildern oder Musikstücken mit anschließender Speicherung auf einem Datenträger ist zweifelsohne eine Vervielfältigung im Sinne des Urheberrechts. Aber auch schon das Zwischenstadium der Speicherung in den verschiedenen Arbeitsspeichern stellt jeweils eine urheberrechtliche relevante Vervielfältigung dar.

5.4 Anbieterseite

Zunächst wird die Seite des Anbieters betrachtet, welcher ein urheberrechtlich geschütztes Werk in ein Filesharingnetzwerk für die anderen Nutzer bereitstellt. Der jeweilige Vorgang wird anhand einer MP3-Datei, also einer komprimierten, digitalen Fassung eines Musikstückes untersucht.

5.4.1 Herstellen einer komprimierten MP3-Datei

Wie bereits erwähnt ist es allgemein üblich, ein Musikstück vor der Weitergabe in ein komprimiertes, digitales Dateiformat zu verwandeln. Eine solche Umwandlung (typischerweise) in das MP3-Format könnte als Vervielfältigung im Sinne des §15 UrhG zu werten sein und damit ein ausschließliches Verwertungsrecht des Urhebers betreffen. Vervielfältigung ist in diesem Zusammenhang die Herstellung einer oder mehrerer Festlegungen, die geeignet sind, das Werk den menschlichen Sinnen auf irgendeine Weise wiederholt unmittelbar oder mittelbar wahrnehmbar zu machen. Bei der Umwandlung in das MP3-Format erfolgt eine endgültige Festlegung typischerweise auf der Festplatte des Benutzers oder einem entsprechenden Speichermedium. Diese Form der Festlegung ermöglicht zwar dem Benutzer nicht den unmittelbaren

Werkgenuss, wie etwa das Lesen eines Buches oder das Betrachten einer Photographie. Jedoch ist der mittelbare Werkgenuss über entsprechende Wiedergabegeräte möglich, etwa mittels entsprechender Software, am Computer angeschlossenen Lautsprecherboxen oder mittels eines so genannten MP3-Players [MöNA00].

Wie bereits dargestellt, wird bei der Herstellung einer MP3-Datei die vorhandene Datenmenge auf durchschnittlich etwa ein Zwölftel ihrer ursprünglichen Größe komprimiert. Daher hat die so entstandene MP3-Datei hinsichtlich Größe, Form und Datenstruktur laut technischer Ansicht nichts mehr mit den ursprünglichen Musikinformaten der Originalmusik CD gemeinsam. Doch es werden dabei weder das individuelle Tongefüge als Ganzes, also die konkrete Kombination musikalischer „Bausteine“, wie der Aufbau der Tonfolgen, der Rhythmus, die Instrumente und/ oder Stimmen noch die Melodie durch die Datenkompression berührt. Typisch für das MP3-Verfahren ist allenfalls eine gewisse minimale Klangeinbuße aufgrund der Begrenzung der Bandbreite des Frequenzganges.

Die Frage der Wahrnehmbarkeit im Sinne des Vervielfältigungsbegriffes ist somit keine Frage des technischen Formates, in welchem das Werk vorliegt. Auch die digitale Festlegung als MP3-Datei erfüllt daher grundsätzlich alle Merkmale einer Vervielfältigung im Sinne des §15 UrhG. Sofern die so erstellte MP3-Datei ein weiteres Mal abgespeichert wird, etwa auf einem anderen Bereich der Festplatte, z.B. in einem für den Tausch von Dateien vorbestimmten Ordner, liegt in der erneuten, digitalen Fassung der Sachverhalt einer weiteren Vervielfältigung im Sinne des §15 UrhG vor [Schr99; FrNo98].

5.4.2 Bereithalten eines Werkes zum Abruf

Die Frage, wie das Zugänglich- bzw. Verfügbarmachen eines (urheberrechtlichen geschützten) Werkes auf einem Server rechtlich zu bewerten ist, wurde in jüngster Vergangenheit lebhaft diskutiert. Es muss jedoch bereits an dieser Stelle erwähnt werden, dass Meinungsäußerungen zu dieser Frage im Regelfall davon ausgehen, dass Werke auf einem fremden Server (zumeist dem eines Freehosters wie Rapidshare) dauerhaft abgelegt werden, also nach diesem „Upload“-Vorgang typischerweise dem unmittelbaren Zugriff des „Anbieters“ entzogen wird. Er behält zwar prinzipiell die Kontrolle über die Werke bei, da er sie jederzeit wieder löschen kann, doch dazu ist ein

aktives Handeln erforderlich. Nimmt er solche Änderungen nicht vor, nachdem das Werk einmal auf dem Server abgelegt worden ist, so besteht für Dritte unabhängig von einem weiteren Willen des „Anbieters“ jederzeit die Möglichkeit, das auf dem Server abgespeicherte Werk auf seinen eigenen Rechner herunterzuladen. Dies gilt solange, wie der Server technisch erreichbar ist, also keine Störungen auftreten [MöNA00].

Beim Filesharing stellt sich die Sachlage dagegen etwas anders dar. Der Austausch von Daten ist nämlich nur möglich, solange der „Anbieter“ der Datei seine Onlineverbindung zum Internet aufrechterhält. Dies liegt daran, dass keine Zwischenspeicherung der Dateien auf einem Server eines Filesharingdienstes stattfindet, sondern ein Austausch von Daten stets zwischen zwei Nutzern direkt erfolgt. Das gilt sowohl für zentralisierte wie auch für dezentral aufgebaute Filesharingnetzwerke. Für die Praxis bedeutet dies, dass unter Umständen nur für wenige Minuten die Möglichkeit für einen Interessenten einer Datei besteht, diese von der Festplatte des Anbieters herunterzuladen. Natürlich ist auch das gegenteilige Extrem denkbar, dass zum Beispiel der Anbieter einer Datei über eine Standleitung verfügt und daher 24 Stunden täglich erreichbar ist. Letzterer Fall ist daher vergleichbar mit der Variante des Ablegens eines Werkes auf einem fremden Server. Jedoch behält beim Filesharing der „Anbieter“ zumindest theoretisch die stete und jederzeit durchsetzbare Kontrolle darüber, ob er Zugriffe auf seinen persönlichen Datenbestand erlaubt oder nicht. Er kann zumeist bestimmen, ob und in welchem Umfang er Daten überhaupt für andere Benutzer freigibt oder er hat die Möglichkeit, jederzeit die Verbindung zum Filesharingnetzwerk zu trennen. Wie das Verfügbarmachen einer Datei beim Filesharing urheberrechtlich zu bewerten ist, wird im folgenden Text näher betrachtet.

Vor der Novellierung des Urheberrechts 2003 war es umstritten, wie das Bereithalten eines Werkes zum Online-Abruf rechtlich erfasst werden sollte. Es war bereits umstritten, ob es sich hierbei um eine Verwertung des Werkes in körperlicher oder in unkörperlicher Form handelte. Der Gesetzgeber hat den Streit schließlich durch die Einführung des neuen §18 a UrhG beendet. Er konnte dabei auf internationale und europarechtliche Vorgaben zurückgreifen. Seither wird den Urhebern das Recht gewährt, die öffentliche Zugänglichmachung der Werke in der Weise, dass sie Mitgliedern der Öffentlichkeit von Orten und zu Zeiten ihrer Wahl zugänglich sind, zu erlauben oder zu verbieten [Schr99; FrNo98].

5.4.3 Zwischenergebnis

Als Zwischenergebnis ist festzuhalten, dass beim Anbieten von geschützten Werken in einem Filesharingssystem Verwertungsrechte des Urhebers betroffen sind: Das Herstellen einer komprimierten digitalisierten Fassung des Werkes ist eine Vervielfältigung im Sinne des §15 UrhG. Das Verfügbarmachen dieser Werkfassung zum Abruf unterfällt dem Recht der öffentlichen Zugänglichmachung nach §18a UrhG. Fraglich ist im Folgenden, ob diese Eingriffe durch eine Schrankenregelung in den §§42 ff. gedeckt sind [Schr99; FrNo98; MöNA00].

5.4.4 Eingreifen von Schrankenregelungen

Somit muss die Frage beantwortet werden, ob die Herstellung einer komprimierten Datei eines Musikwerkes, das in einem Filesharingnetz angeboten werden soll, noch als Vervielfältigung zum privaten Gebrauch gemäß §42a UrhG privilegiert ist. Privater Gebrauch war als Gebrauch in der Privatsphäre zur Befriedigung rein persönlicher Bedürfnisse durch die eigene Person oder die mit ihr durch ein persönliches Band verbundenen Personen definiert worden. Damit gehört jedenfalls nicht mehr zum privaten Gebrauch, was sich an die Öffentlichkeit richtet. Diese Eingriffe werden nach neuem Recht daher nicht von einer Schrankenregelung gedeckt [Schr99; FrNo98].

5.5 Abnehmerseite

Nun wird der gleiche Vorgang von der Seite des Abnehmers untersucht, also diejenigen Personen, welche aus dem Filesharingnetzwerk urheberrechtlich geschützte Werke auf ihren Rechner herunterladen. Der jeweilige Vorgang wird ebenso anhand einer MP3-Datei, also einer komprimierten digitalen Fassung eines Musikstückes untersucht.

5.5.1 Download als Vervielfältigung

Lädt sich ein Teilnehmer eines Filesharingnetzes eine MP3-Datei auf seine Festplatte herunter, so bedeutet dies im Ergebnis eine erneute Vervielfältigung des Werkes (§15 UrhG) in digitaler Form. Bis jedoch eine endgültige Festlegung einer solchen

Werkskopie auf der Festplatte des Abnehmers stattfinden kann, sind weitere Vervielfältigungen unvermeidbar: Trotz einer Direktverbindung zwischen Anbieter und Abnehmer wird eine Datei nicht als Ganzes übermittelt, sondern in kleine und kleinste Datenpakete zerlegt, die getrennt über verschiedene Rechner und auf unterschiedlichen Routen übermittelt werden (so genanntes „Routing“). Die Datenpakete werden dabei in der Regel auf den zwischengeschalteten Rechnern („Routern“) kurzfristig zwischengespeichert und erst an ihrem endgültigen Ziel, dem Computer des Empfängers, gemäß den Vorgaben des Übertragungsprotokolls wieder zusammengefügt. Rein technisch gesehen, kommt es auf dem Weg zum Abnehmer also zu weiteren Vervielfältigungen. Die übertragenen Datenpakete sind jedoch in aller Regel so klein, dass ihnen per se kein urheberrechtlicher Schutz mehr zukommen wird. Die einzelnen zwischengespeicherten Datenpakete sind mangels schöpferischer Eigenart, individueller Prägung und ohne einen mit menschlichen Sinnen wahrnehmbaren Inhalt keine selbständigen Werke oder geschützte Werkteile [UrhG06]. Das so genannte „Routing“ stellt folglich keinen Eingriff in das Vervielfältigungsrecht des Urhebers dar [MöNA00].

5.5.2 Download als Privatkopie nach §42 UrhG

Im Hinblick auf die Festlegung des Werkes auf die Festplatte des Abnehmers stellt sich die Frage, ob diese Vervielfältigung als Privatkopie im Sinne des §§42 ff. UrhG zulässig ist oder ein ungerechtfertigter Eingriff in das Vervielfältigungsrecht des Urhebers aus §15 UrhG vorliegt [Schr99; FrNo98].

Umstritten ist bei diesem Sachverhalt bereits, wer bei dem Abruf einer Datei als Vervielfältigender anzusehen ist. Denn dies muss nicht unbedingt zwangsläufig der Abrufende allein sein, sondern zumindest auch teilweise der Anbieter. Wie bereits oben festgestellt, verlässt der Anbieter beim Filesharing bereits durch das Bereithalten zum Abruf einer Datei die von §42 ff. UrhG gezogenen Grenze des privaten Nutzungszweck. Im Hinblick auf das Herunterladen einer konkreten Datei aus dem Filesharingnetz entscheidet alleine der interessierte Abnehmer, was und zu welchem Zeitpunkt er sich vom Computer des Anbieters etwas auf seinen eigenen Rechner herunterlädt. Zwar übt der Anbieter die Sachherrschaft über den Download-Vorgang aus, indem er ihn jederzeit nach seinem Willen abrechnen kann. Es lässt sich jedoch die grundsätzliche

Absicht des Anbieters in Filesharingnetzen dahingehend definieren, lediglich den Zugang zu einer bestimmten Datei zu ermöglichen, während der Wille des Nutzers entscheidend dafür ist, ob eine Vervielfältigung stattfindet oder nicht. Daher ist auch der Herunterladende Vervielfältiger im rechtlichen Sinne. Die teilweise vertretene Ansicht, auch der Anbieter einer Datei sei im Falle eines Downloads als ihr Vervielfältiger anzusehen, ist daher im Falle des Filesharings abzulehnen. Vervielfältiger im Sinne des §42 UrhG ist allein derjenige, der die angebotene Datei abrufen [Schr99; FrNo98].

§42 ff. UrhG wäre weiterhin nur dann anwendbar, wenn ein privater Gebrauch des Vervielfältigungsstückes beabsichtigt ist. Dieser scheidet jedenfalls dann aus, wenn der Abnehmer seinerseits beabsichtigt, die heruntergeladene Datei zum Abrufen anzubieten, da er dadurch selbst in das dem Urheber vorbehaltene Recht der öffentlichen Zugänglichmachung nach §18a UrhG eingreifen würde. Nicht ganz unproblematisch ist in dieser Hinsicht beim Filesharing, an welchem Ort die heruntergeladene Datei auf der Festplatte gespeichert wird. Typischerweise geschieht dies, abhängig von der jeweiligen Software, welche hierzu verwendet wird, in einem Ordner, auf den in der Standardeinstellung der meisten Börsen, Dritte zugreifen können. Dies entspricht einem der Grundgedanken des Filesharing: Was heruntergeladen wurde, steht unmittelbar wieder für den Tausch bereit. Allein die Existenz einer Datei in einem solchen Tauschordner ist ein deutliches Indiz gegen eine beabsichtigte Nutzung allein zu privaten Zwecken [FrNo98; MöNA00].

Die überwiegende Zahl der Tauschbörsen gestattet es ihren Nutzern, nur Dateien herunterzuladen, nicht aber selbst als Anbieter aufzutreten, auch wenn dieses Verhalten als „Leeching“ in Tauschbörsenkreisen offenbar verpönt ist. In diesem Fall ergibt sich der außerprivate Nutzungszweck nicht schon aus dem Vorhandensein einer heruntergeladenen Datei im Tauschordner, wenn der Teilnehmer die Zugriffsmöglichkeit Dritter auf diesen Ordner deaktiviert hat.

5.5.3 Keine private Vervielfältigung von einer „offensichtlich rechtswidrigen“ Vorlage

Es ist sehr umstritten, ob §42 UrhG voraussetzt, dass für die Vervielfältigung ein legales Werkstück benutzt wird. Nach Ansicht der Mehrheit sollte eine Privatkopie dann nicht rechtmäßig sein, wenn ein Piraterieprodukt als Ausgangsstück verwendet worden ist. Im

Bereich des Filesharing war diese Fragestellung von erheblicher Relevanz, da durch das Angebot zum Download eine etwaige auf Anbieterseite bestehende Privilegierung im Sinne des §42 UrhG zumindest rückwirkend entfällt und die zum Download bereitgehaltene Datei folglich ein unter Verletzung des Vervielfältigungsrechts des Urhebers (§15 UrhG) hergestelltes Vervielfältigungsstück darstellt. Die Interessenvertreter der Musik- und Filmindustrie lesen die Rechtmäßigkeit der Kopiervorlage als zwingendes Kriterium aus dem Gesetz heraus. Eine derartige Einschränkung lässt sich jedoch nicht entnehmen. In Deutschland, wo es eine ähnliche Diskussion über den § 53 UrhG gab, der die private Vervielfältigung regelt, wurde durch die Novellierung des UrhG 2003 der §53 UrhG durch eine Einschränkung des Wortlautes ergänzt. Seither sind Vervielfältigungen für den privaten Gebrauch künftig nur zulässig, „soweit nicht zur Vervielfältigung eine offensichtlich rechtswidrige hergestellte Vorlage verwendet wird“. Weitere Streitigkeiten sind mit dieser schwammigen Formulierung jedoch bereits vorprogrammiert. So wird künftig bei deutschen Verhandlungen im Mittelpunkt der Diskussion stehen, wann eine Vervielfältigungsvorlage „offensichtlich rechtswidrig“ ist oder nicht [Schr99; FrNo98]. Der österreichische Gesetzgeber hat sich hingegen noch nicht entschlossen eine ähnliche Einschränkung in den Gesetzestext aufzunehmen. Es wäre jedoch sicherlich nicht angemessen, dies durch eine folgende Novellierung dem deutschen Gesetzgeber nachzuempfinden, weil eine solche Einschränkung nur zu weiteren Streitigkeiten führt. Es müssen daher neue Wege gefunden werden, um diese offenen Fragen in der rechtlichen Auslegung zu beseitigen, da dies die Problematik in jenem Sachbereich erheblich vereinfachen würde.

5.5.4 Offensichtliche Rechtswidrigkeit bei Filesharingbörsen

Für die vorliegende Untersuchung bleibt jedoch zu erörtern, ob der Download von Werken über Filesharingbörsen immer als „offensichtlich rechtswidrig“ anzusehen ist. Die meisten Personen sind der Meinung, dass es dem einzelnen Nutzer einer Filesharingbörse unmittelbar einleuchten müsse, dass das massenhafte Angebot von urheberrechtlich geschützten Werken nur rechtswidrig sein kann.

Gegen eine „offensichtliche Rechtswidrigkeit“ beim Download aus Filesharingnetzwerken sprechen demgegenüber zwei Aspekte. Zum einen setzen

Künstler wie Plattenfirmen MP3s mittlerweile gezielt zu Marketingzwecken ein. Es ist daher nicht ungewöhnlich, dass bestimmte Stücke einer bekannten Musikgruppe als MP3 von offizieller Seite im Internet bereitgestellt werden, um zum Beispiel für eine neue Veröffentlichung des Künstlers zu werben. Es nutzen jedoch auch unbekannte Bands das Internet, um mit dem Angebot von MP3-Dateien zum kostenlosen Download auf sich aufmerksam zu machen. Ob es sich bei einer angebotenen Datei letztlich um eine rechtmäßige oder rechtswidrige handelt, ist dieser damit in vielen Fällen nicht anzusehen, zumindest wird eine Rechtswidrigkeit in den meisten Fällen nicht „offensichtlich“ sein [MöNA00].

Über die Verfügbarkeit rechtmäßiger Dateien in Filesharing-Börsen hinaus, dürfte es zum anderen für den Nutzer derartiger Dienste in vielen Fällen schwierig sein, richtig einzuschätzen, ob der Anbieter einer Datei mit deren öffentlicher Zugänglichmachung rechtmäßig oder rechtswidrig handelt. Insoweit ist weiters zu berücksichtigen, dass Filesharingnetze, wie das Internet selbst, grundsätzlich grenzenlos sind. Das Angebot einer bestimmten Datei kann wie auch der Download an jedem beliebigen Ort der Welt erfolgen. Für das beim Bereithalten eines Werkes in Filesharingnetzen einschlägige Recht der öffentlichen Zugänglichmachung ist aber in diesem Fall bereits materiellrechtlich umstritten, an welchem Ort die Verwertungshandlung überhaupt stattfindet. Angesichts der aufgezeigten Problematik erscheint es im Ergebnis somit nicht ohne weiteres vertretbar, beim Download aus Filesharingnetzen immer von einer „offensichtlichen Rechtswidrigkeit“ der Vorlage auszugehen. Insoweit ist nicht einmal „offensichtlich“ österreichisches Recht anwendbar. Soweit nämlich die Anwendung ausländischen Rechts in Frage steht, wird der Vervielfältigende kaum sicher die Rechtswidrigkeit einer Vorlage beurteilen können. Von einer „offensichtlichen Rechtswidrigkeit“ wird man daher im Ergebnis nur in wenigen Fällen sprechen können, nämlich dann, wenn ohne weiteres ersichtlich ist, dass es sich um ein österreichisches Angebot handelt, bei dem es vernünftigerweise nicht in Betracht kommt, dass der Urheber mit einer Zugänglichmachung einverstanden ist. Im Übrigen wird man daher jeweils sehr genau die Umstände des Einzelfalls zu werten haben [FrNo98; MöNA00].

5.5.5 Offensichtliche Rechtswidrigkeit und die Umgehung technischer Schutzmaßnahmen §90 c UrhG

In diesem Zusammenhang ist die Frage zu stellen, ob sich der Vervielfältigende auf das Privileg des §42 UrhG berufen kann, wenn er bei der Herstellung der Privatkopie technische Schutzmaßnahmen umgeht und damit entgegen dem Verbot des §90 c UrhG handelt. Ferner ist bislang ungeklärt, ob eine unter Missachtung des §90 c UrhG hergestellte Kopie ihrerseits eine „offensichtlich rechtswidrige“ Vorlage darstellt. Ersteres wird man bejahen müssen, da §42 UrhG selbst in dieser Hinsicht keine Einschränkungen im Hinblick auf die Art und Weise der Herstellung der Privatkopie enthält. Auch wird keine „offensichtlich rechtswidrige“ Vorlage benutzt, wenn ein kopiergeschützter Original-Datenträger vervielfältigt wird. Das führt zu dem durchaus kuriosen Ergebnis, dass das Vervielfältigungsstück selbst privilegiert, seine Herstellung unter Umgehung technischer Schutzmaßnahmen aber verboten ist. Nach seinem Zweck ist §90 c UrhG eine reine Schutznorm zugunsten technischer Schutzmechanismen. Unter welchen Voraussetzungen eine Kopie als private Vervielfältigung anzusehen ist, regelt §90 c UrhG dagegen nicht. Da beispielsweise nicht alle in Österreich vertriebenen CDs (oder DVDs) einen Kopierschutz enthalten und somit hiervon nicht zwangsläufig auszugehen ist, wird es praktisch in erster Linie darauf ankommen, ob der Kopierschutz auch auf der Kopie noch enthalten und erkennbar ist, denn bestimmte Kopierschutzprogramme, wie etwa „CloneCD“ kopieren den „Kopierschutz“ vieler Firmen schlichtweg mit [VoBä03; MöNA00].

5.6 Haftung des Anbieters der Filesharingsoftware

Ergänzend soll noch im Überblick auf die Frage eingegangen werden, ob der Anbieter der Filesharingsoftware urheberrechtlich haftet. Wie bereits erörtert, erfolgt die Übertragung der einzelnen Dateien systemunabhängig ausschließlich zwischen den am Tauschvorgang unmittelbar Beteiligten. Der Anbieter der Filesharingsoftware selbst hält weder die Werke zum Abruf bereit, noch vervielfältigt er sie oder greift sonst direkt in ein Verwertungsrecht ein. In Betracht kommt dagegen eine mittelbare Haftung für Urheberrechtsverletzungen der einzelnen Teilnehmer, namentlich für das nicht von

einer entsprechenden Schranke gedeckte Bereithalten eines Werkes zum Abruf [FrNo98].

Das Eröffnen des bloßen technischen Zugangs zum Tauschnetz durch die entsprechende Software dürfte in haftungsrechtlicher Hinsicht nicht relevant sein. Insoweit wird bei Tauschbörsen lediglich der Zugang zu einem Datennetz vermittelt sowie der Datenaustausch innerhalb dieses Netzes ermöglicht. Dies ist von der Funktion her vergleichbar mit üblicher Browsersoftware wie dem Internet Explorer von Microsoft, der den Zugang zum World Wide Web (WWW) ermöglicht. Das bloße Anbieten von Filesharingsoftware ist somit unproblematisch [MöNA00].

Anders könnte im Hinblick auf die weitergehenden Funktionen der Filesharingsoftware bzw. der Filesharingdienste zu urteilen sein. Eine ausschlaggebende Tätigkeit wird man dann bejahen können, wenn der Dienstanbieter den einzelnen Tauschvorgang zwischen Anbieter und Abnehmer in erheblichen Umfang steuert. Ob eine solche Einflussnahme vorliegt, hängt im Wesentlichen davon ab, ob es sich um ein zentrales oder dezentrales Tauschsystem handelt. Bei zentralen Tauschsystemen sammelt der Filesharingdienst die Angaben der Nutzer, welche Dateien zum Tausch bereit stehen. Im Falle einer konkreten Anfrage werden die passenden Angaben dem Nutzer in aufbereiteter Form präsentiert. Der Tauschbörsenbetreiber fungiert in diesem Fall als unverzichtbarer Mittler zwischen den Tauschwilligen und ist als solcher am Tauschvorgang beteiligt. Dies rechtfertigt es, von einer ausschlaggebenden Tätigkeit zu sprechen und die Betreiber von zentralen Filesharingplätzen haftungsrechtlich als (Mit-) Veranstalter nach §71 UrhG einzuordnen [Schr99; FrNo98].

Bei dezentralen Tauschbörsen hingegen wird die Suche dagegen praktisch von den Nutzern selbst organisiert. Suchanfragen werden von Nutzer zu Nutzer weitergereicht. Bei diesen Systemen erfolgt keine explizite Suchunterstützung durch den Anbieter der Filesharingsoftware über die reine technische Funktion der Software hinaus. Eine Beteiligung am Tauschvorgang, bzw. ein unmittelbares Fördern des öffentlichen Angebotes des Werks ist damit nicht gegeben. Die Anbieter von Softwareprotokollen für dezentral aufgebaute Tauschbörsen sind demnach haftungsrechtlich nicht als „Veranstalter“ nach §71 UrhG zu qualifizieren. Nach den dargestellten Maßstäben der Rechtssprechung kann damit das Angebot dezentraler Filesharingdienste, also das bloße Zurverfügungstellen entsprechender Software zwar als adäquat kausal für die Urheberrechtsverletzung der Teilnehmer angesehen werden, aber es folgt hieraus jedoch lediglich die Verpflichtung, die Teilnehmer zu Beachtung fremder Urheberrechte

anzuhalten. Bei zentralen Tauschbörsen wird jedoch eine solche Maßnahme nicht genügen, da sie den Tausch geschützten Materials organisieren und (mit-) veranstalten. Deshalb können sie sich nicht durch einen schlichten Warnhinweis einer weitergehenden Haftung entziehen [Schr99; MöNA00].

5.7 Ergebnis

Ein typischer Filesharingvorgang, wie er täglich millionenfach vorkommt, bei dem zunächst ein Musikwerk digital komprimiert, im Anschluss zum Abruf bereitgehalten und schließlich von einem Dritten auf den eigenen Computer heruntergeladen wird, ist danach im Gesamtergebnis wie folgt zu bewerten: Das Komprimieren eines Musikstückes ist eine Vervielfältigung nach §15 UrhG. Soll die komprimierte Datei in einem Filesharingnetzwerk zum Abruf durch Dritte bereitgehalten werden, ist diese Vervielfältigung nicht durch eine Schrankenregelung gedeckt und daher rechtswidrig. Das Bereithalten der komprimierten Datei zum Abruf unterfällt dem §18 a UrhG als Recht der öffentlichen Zugänglichmachung. Schrankenregelungen, welche das Bereithalten erlauben könnten, bestehen nicht [Schr99; FrNo98].

Beim Herunterladen eines digitalisierten Werkes findet eine weitere Vervielfältigung im Sinne des §15 UrhG statt; hierbei ist allein der Abrufende der Datei als Vervielfältigender anzusehen. Sofern die Vervielfältigung zu privaten Zwecken erfolgt, also insbesondere die heruntergeladene Datei nicht wiederum in einem Filesharingnetz der Öffentlichkeit angeboten wird, kann sich der Herunterladende auf die Privilegierung des §42 UrhG berufen, wenn die Vervielfältigung nicht von einer „offensichtlich rechtswidrigen“ Vorlage erfolgt ist. Dieses Tatbestandsmerkmal ist auch in Tauschbörsen nicht immer erfüllt, sondern muss in der Regel im Einzelfall festgestellt werden [Schr99; FrNo98; MöNA00].

Der vorgesehene Rechtsschutz gegen die Umgehung von technischen Schutzmöglichkeiten greift jedoch nur dann ein, wenn diese technischen Schutzmöglichkeiten wirksam sind. *„Wirksame technische Schutzmaßnahmen sind zu definieren als Technologien, Vorrichtungen und Bestandteile, die im normalen Betrieb dazu bestimmt sind, mittels Zugangskontrolle, Verschlüsselung, Verzerrung, Umwandlung oder sonstiger Schutzgegenstände oder Kontrollmechanismen eine vom Rechteinhaber vorgegebene Nutzungsbeschränkung zu sichern.“* [Gutm03, 171]. Bei

einer engen Betrachtung ist diese Regelung jedoch unanwendbar. Wenn nämlich die Schutzmöglichkeiten wirksam sind, können sie nicht umgangen werden. Es gibt also auch niemanden, gegen den sich der Rechtsschutz wenden kann. Diese Regelung wäre unnötig. Ist die Schutzmöglichkeit allerdings unwirksam und kann umgangen werden, greift der Rechtsschutz nicht ein, da der technische Schutz eben nicht wirksam ist. Eine Lösung in diesem Fall bietet sich in der weiter gefassten Auslegung des Begriffes „wirksam“ unter der Betrachtung im Zusammenhang mit dem Wortlaut des Art. 6 Abs. 3 S. 1 Info-RL „im normalen Betrieb“ an. Wirksam ist hiernach so zu verstehen, dass der Schutzmechanismus einen Durchschnittsnutzer an der Vornahme von Nutzungshandlungen hindert, zu denen eine entsprechende Erlaubnis des Berechtigten nicht vorliegt [Schr99; FrNo98; MöNA00].

5.8 Ist ein Verbot der digitalen Privatkopie angezeigt?

5.8.1 Tendenzen in der Rechtsprechung zur Einschränkung von Schrankenbestimmungen im digitalen Kontext

Es ist zu klären, ob die Anwendbarkeit des §42 UrhG auf digitale Vervielfältigungen und damit auf Downloadvorgänge in Filesharingnetzen immer untersagt werden sollte, weil hierhin eine urheberrechtsrelevante Nutzung in einem Ausmaß und einer Intensität erschlossen wird, die sich mit den eine Privilegierung rechtfertigenden Erwägung nicht mehr so vereinbaren lässt.

In der Rechtsprechung ist die Tendenz erkennbar, die urheberrechtlichen Schrankenregelungen bei digitalen Technologien angesichts der mit diesen verbundenen Gefahren für den Urheber und die Durchsetzung seiner Verwertungsrechte wesentlich restriktiver zu handhaben als bei analogen Medien [Krög00, 662-663].

Auch im Rahmen des Filesharings sind die Auswirkungen der Digitaltechnik, nämlich die einfache und kostengünstige Weitergabe von Werken und deren intensive Nutzung deutlich geworden. Somit ist es fraglich, ob eine entsprechende Ausnahme der digitalen Privatkopie von §42 UrhG zumindest immer angezeigt ist [MöNA00].

5.8.2 Argumente gegen ein Verbot der privaten digitalen Vervielfältigung

Dafür sprechen mehrere Gesichtspunkte. Zum einen dürfte, betrachtet man einen Filesharingvorgang insgesamt, die größere Gefährdung der Urheberinteressen weniger im einzelnen tatsächlichen Download als Vervielfältigung für den privaten Gebrauch liegen, der keine weitergehende wirtschaftliche Auswertung des Werkes nach sich zieht, sondern im Bereithalten des Werkes zum Abruf, das einen größeren potenziellen Nutzerkreis erst erschließt. Das Bereithalten zum Onlineabruf wird dem Urheber aber bereits als Recht der öffentlichen Zugänglichmachung vorbehalten und als solches auch von der relevanten Ausnahmvorschrift des §42 UrhG ausgenommen. Selbst wenn man die Trennung zwischen Angebot und Abruf nicht nachvollziehen möchte und den Filesharingvorgang als einheitliches Geschehen begreift, fällt doch auf, dass jenseits des privaten Nutzungsinteresses auf der Seite des Herunterladenden keine wirtschaftliche Weiterverwendung des Werkes erfolgt. Insbesondere ist bisher am Beispiel des Musiksektors auch kein exklusiver Ursachenzusammenhang zwischen Filesharing, privatem Brennen und Umsatzrückgängen bei CD-Verkäufen nachgewiesen worden. Selbst wenn man in der digitalen Privatkopie eine Beeinträchtigung der Absatzchancen auf dem Primärmarkt sehen möchte, sprechen weitere Argumente gegen ein generelles Verbot der Privatkopie. Das Hauptargument dagegen ist jedoch nach wie vor, dass sich der private Bereich einer, beispielsweise aus dem öffentlichen Angebot folgenden, urheberrechtlichen Kontrollmöglichkeit entzieht. Was 1965 für die damals ebenso „revolutionäre“ private Tonbandaufnahme galt, gilt heute für das CD-Brennen am heimischen Personal Computer: Ein Verbot wäre nicht durchsetzbar. Zwar geben die Teilnehmer beim Filesharing ihre Identität über ihre IP-Adresse bekannt und verlassen damit den Bereich der Anonymität. Angesichts der Masse der ausgetauschten Daten ist eine effektive Kontrolle jedoch kaum vorstellbar, wollte man nicht eine intensive Überwachung des gesamten Datenverkehrs jedes Internetbenutzers durchführen. Für die Beschaffung der Kopiervorlage im Wege des Filesharing gilt nichts anderes als für den eigentlichen heimischen Kopiervorgang selbst: Die breite Masse dieser Vorgänge ist einer Kontrolle entzogen und Übertretungen könnten nur durch intensivste Überwachung, Zufall oder durch Denunziation bekannt werden. Als Zwischenstand lässt sich festhalten, dass ein Verbot der digitalen Privatkopie wegen fehlender

Kontrollmöglichkeiten nach wie vor grundsätzlich nicht angezeigt ist [Schr99; MöNA00].

Dem Argument der fehlenden Kontrollmöglichkeit wird aber entgegengehalten, dass künftig technische Systeme in der Lage sein werden, entsprechende Verbote auch tatsächlich durchzusetzen. In der Sache geht es hierbei insbesondere um Kopierschutzsysteme, die das Vervielfältigen von Werken verhindern sollen und auch um das so genannte Digital Rights Management (DRM) siehe Kapitel 7.

5.8.3 Die Grenzen technischer Schutzmaßnahmen

Um künftig DRM und Kopierschutzsysteme als Allheilmittel aller urheberrechtlichen Probleme im digitalen, vernetzen Kontext zu sehen, sprechen jedoch drei wesentliche Punkte dagegen. Zum einen erfassen diese Systeme nachträglich keine Werke mehr, die vor dem Einsatz entsprechender Schutzmaßnahmen auf den Markt gekommen sind. Was einmal ungeschützt in einem Filesharingnetzwerk zirkuliert, oder zum jetzigen Zeitpunkt nur auf einem beliebigen ungeschützten digitalen Datenträger vorhanden ist oder auch nur in digitalisierbarer analogen Form ist unwiderruflich verloren.

Zum anderen müssen Kopierschutz- und DRM-Systeme erst tatsächlich in der Praxis beweisen, was sie theoretisch versprechen. Bislang ist nämlich kein einziges System bekannt geworden, das einen Schutz über eine längere Zeitdauer effektiv gesichert hätte. Wo technische Schutzmaßnahmen vorhanden sind, ist der nächste Hacker nicht fern, welcher die Aufforderung zur technischen Auseinandersetzung annimmt. DRM und Kopierschutzsysteme sind möglicherweise dazu geeignet, einen überwiegenden Teil der Konsumenten, der „breiten Masse“, die Lust auf das private Kopieren zu nehmen, wenn dieses Kopieren technisch nur mit Mühen zu realisieren ist. Mit Filesharingnetzen stehen im Anschluss neuerdings Instrumente bereit, die für eine schnelle, unkomplizierte horizontale Verteilung der von ihrem technischen Schutz befreiten Werke sorgen können. Dabei reicht es theoretisch, dass eine einzige Person weltweit in der Lage ist, den Schutz zu umgehen und den digitalen Content der breiten Masse zur Verfügung zu stellen. Auf der anderen Seite wird es natürlich auch Nutzer geben, vermutlich sogar die Mehrzahl, welche die technischen Schutzmaßnahmen und deren Umgehungsverbot akzeptieren. Hieraus folgt dennoch nicht, dass Kopierschutz- und DRM-Systeme das Urheberrecht vollständig ersetzen können.

Schließlich ist auch zu bedenken, dass der Einsatz von DRM- und Kopierschutz-Systemen mit erheblichen Kosten verbunden ist. Entsprechende Systeme müssen von den Herstellern ständig weiterentwickelt werden, um überhaupt einen gewissen Schutz garantieren zu können. Vor allem wird es großen Unternehmen der Unterhaltungsindustrie vorbehalten sein sich solche Systeme zu leisten, denn nicht jeder Urheber wird in der Lage sein, diese beträchtlichen zusätzlichen Kosten zum Schutze seines geistigen Eigentums zu tragen. Gerade deshalb ist es erforderlich, gegenüber dem einzelnen Urheber eine rechtlich abgesicherte Vergütung beispielsweise für private Vervielfältigung seiner Werke zu gewährleisten und ihn nicht lediglich auf technische Lösungen zu verweisen.

5.8.4 Erfassung von Internet und Filesharing auf Vergütungsebene

Es ist bereits vorgeschlagen worden, den Zugang ins Internet vergütungspflichtig zu machen, und zwar über eine Betreiberabgabe, der so genannten Access Provider, also der Zugangsvermittler ins Internet [Dust01, 234–236].

Diese Überlegung beruht auf der Annahme, dass der Access Provider die entscheidenden Voraussetzungen für alle über das Browsen hinausgehenden privaten Vervielfältigungsvorgänge schaffe. Je länger ein Kunde im Internet surfe, desto größer sei die Wahrscheinlichkeit, dass es zum Abruf und zur dauerhaften Vervielfältigung urheberrechtlich geschützter Werke komme [Dust01, 235-240].

Es dürfte jedoch fraglich sein, ob eine derartige Betreiberabgabe tatsächlich ein „zielgenaues Mittel“ darstellt, um die dem Urheber für die bei Onlinenutzungen erfolgten privaten Vervielfältigungen zustehende Vergütung zu realisieren. Überdenkenswert an diesem Ansatz erscheint jedoch, für private Vervielfältigung, die durch das Internet und Filesharingnetze erst ermöglicht werden, auch eine online-spezifische Vergütung festzulegen. Speziell im Bezug auf Filesharingbörsen erscheinen daher zwei Ansatzpunkte für eine Vergütungsregelung grundsätzlich erwägenswert:

Einmal wäre es denkbar, nur den spezifischen Datenverkehr zu erfassen, der über ein Filesharingnetz abgewickelt wird. Dies könnte über eine volumenmäßige Vergütungsregelung geschehen. Diese Variante stieße allerdings auf erhebliche technische und auch rechtliche Probleme. Wollte man den spezifischen Filesharing-Datenverkehr erfassen, so müsste man sich den Umstand zu nutze machen, dass solcher

Datenverkehr über bestimmte „Ports“, also bestimmte Übergabestellen zwischen Sender und Empfänger abgewickelt wird, welche sich von übrigen Internetanwendungen unterscheiden lassen [Schw06]. Hierin liegt jedoch keine endgültige, technisch sichere Lösung, da sich grundsätzlich frei konfigurieren lässt, über welche der 65.536 möglichen Schnittstellen ein spezifischer Datenverkehr erfolgen soll. Um daher definitiv sagen zu können, um welchen spezifischen Datenverkehr es sich handelt, müsste der komplette Datenverkehr des Nutzers analysiert werden. Diese Variante wäre zwar technisch zu realisieren, stößt aber, da sie einer Überwachung sämtlicher Online-Kommunikation gleichkommt, auf erhebliche verfassungsrechtliche Bedenken. Sie ist daher abzulehnen.

Zweitens bestünde die Möglichkeit, die Anbieter von Filesharingsoftware mit einer entsprechenden Abgabe pro abgerufener Tauschsoftware zu belegen. Dabei wäre aber problematisch, dass der Tauschvorgang als solcher, welchen die Software ermöglicht, nach österreichischem Recht zumindest teilweise rechtswidrig ist, nämlich jedenfalls auf Anbieterseite wegen eines nicht gerechtfertigten Eingriffs in das Recht der öffentlichen Zugänglichmachung. Darüber hinaus ist eine nationale Abgabenregelung bei einer international über das Internet verfügbaren Software eines ausländischen Anbieters realistischlicherweise praktisch ohnehin nicht durchsetzbar.

Will man also eine online-spezifische Vergütung erreichen, müsste mangels sonstiger praktikabler Alternativen tatsächlich der Zugang ins Internet insgesamt mit einer pauschalen Urheberrechtsabgabe belastet werden.

5.8.5 Verhältnis von technischen Schutzmaßnahmen und pauschaler Vergütung

Es hat sicherlich mehr Sinn, eine Vergütung für Einzelkomponenten zu erheben, die zweifelsfrei als Vervielfältigungsgeräte identifiziert werden können, nicht zuletzt auch, weil der einzelne Nutzer entscheidet, welche dieser Komponenten er in seinem Computer benötigt und welche nicht. Auf den tatsächlichen Umfang der urheberrechtlichen relevanten Nutzung komme es für die Frage der Vergütungspflicht nicht an, solange die Vermutung nicht zu entkräften ist, dass die Geräte ihrer Zweckbestimmung nach zumindest auch für urheberrechtlich relevante Vervielfältigung genutzt werden können. Eine pauschale Abgabe auf „den PC“, den es im Zeitalter

zweck- und einsatzoptimierter Rechner ohnehin nicht gibt, ist daher nicht gerechtfertigt. Es wäre auch darüber nachzudenken, nicht nur die Hersteller von Kopiergeräten und Leermedien mit einer Vergütungspflicht zu belegen, sondern auch die Hersteller von entsprechender Vervielfältigungssoftware, welche den Vervielfältigungsvorgang zwischen den einzelnen Computerbauteilen steuert [MöNA00].

Da pauschale Vergütungsmodelle wie gezeigt auch in der Zukunft von Bedeutung sein werden, gleichzeitig aber zu erwarten ist, dass verstärkt Kopierschutz- und DRM-Systeme zum Einsatz kommen, bleibt die Frage zu lösen, wie diese beiden Mechanismen in Einklang gebracht werden können. Technische Schutzsysteme werden künftig zumindest bei einer größeren Zahl von Nutzern, die derartige Systeme und ihr Umgehungsverbot akzeptieren, dafür sorgen, dass eine private digitale Vervielfältigung technisch nicht mehr möglich ist oder vom Rechteinhaber nur noch gegen eine individuelle Vergütung gestattet wird. In diesen Fällen stellt sich nach dem ersten Eindruck die Frage, warum für Vervielfältigungsgeräte und entsprechende Medien weiterhin eine pauschale Abgabe gezahlt werden sollte, wenn der Nutzer solche Geräte und Speichermedien nicht mehr für entsprechende private Vervielfältigungen gebrauchen kann. Das Problem einer derartigen „Doppelbezahlung“, nämlich pauschale Abgaben auf Vervielfältigungsmedien einerseits sowie individuelle Zahlungen für die Nutzung andererseits, hat auch in der InfoRL seine Erwähnung gefunden. Die Hoffnung des EU-Gesetzgebers bestand darin, dass Vergütungsregelungen für digitale Privatkopien im Ergebnis letztlich überflüssig werden könnten, wenn der Schutz auf technischem Wege und über individuelle Vergütungen möglich ist. In der Praxis hat sich jedoch gezeigt, dass ein Ausschlussverhältnis zwischen technischen Schutzmaßnahmen und pauschalen Vergütungsregelungen nicht realisierbar ist, wodurch zukünftig beide Systeme nebeneinander bestehen müssen. Erforderlich ist daher eine differenzierte Regelung, welche beide Systeme bestmöglich aufeinander abstimmt [MöNA00].

Neue, intensive Nutzungsformen von Werken im digitalen vernetzten Kontext wie das Filesharing führen nach geltendem Recht zu einer massenhaften Anwendbarkeit von Schrankenregelungen, namentlich der Schranke der Vervielfältigung zum privaten Gebrauch. Obwohl in der Rechtsprechung die Tendenz erkennbar ist, bestimmte digitale Nutzungsformen von einem privilegierten Gebrauch auszunehmen, empfiehlt es sich im Ergebnis nicht, die digitale Privatkopie immer zu untersagen. Insoweit hat sich gezeigt, dass ein solches Verbot auf absehbare Zeit nicht wirksam durchgesetzt werden kann,

auch nicht durch technische Schutzmaßnahmen und deren rechtliche Absicherung. Erforderlich ist es in diesem Zusammenhang, die derzeitigen Vergütungssätze für digitale Vervielfältigungen deutlich zu erhöhen sowie die Vergütungspflicht auf online-spezifische Nutzungsformen auszudehnen.

5.9 Rechtliche Grundlagen der Vervielfältigung zum privaten Gebrauch

Das vom Urheber erstellte Werk und die darin verkörperte geistige Leistung sind Eigentum des Urhebers. Die Herrschaft des Urhebers über sein Werk wird ihm hiernach nicht erst durch den Gesetzgeber verliehen, sondern folgt bereits aus dem „geistigen Eigentum“ am Werk [Riga01, 8].

Im Umfang der Verwertungsrechte hat der Urheber das alleinige Recht, sein Werk zu nutzen und Dritte von der Benutzung des Werkes auszuschließen.

Neben der Anerkennung des Urheberrechts als „geistiges Eigentum“ entwickelte sich die Erkenntnis, dass dieses Eigentum, wie Sacheigentum auch, im Interesse der Allgemeinheit einer Sozialbindung unterliegt [Pahu01, 15].

So ist das Interesse der Allgemeinheit darauf ausgerichtet, die Werke der Kunst möglichst uneingeschränkt zu genießen. Insofern besteht ein gesamtgesellschaftliches Interesse an einem reichen, lebendigen, sich entwickelnden Kultur- und Geistesleben. Geistiges Eigentum sollte daher prinzipiell frei sein, d.h. sie dürfen nur in beschränktem Maße monopolisiert werden. Der Zugang zu den einzelnen Geistesschöpfungen soll jedermann möglichst einfach gewährleistet sein, da andernfalls die geistige Entwicklung behindert wäre [Pahu01, 33].

5.10 Das Vervielfältigungsrecht des Urhebers

Das Vervielfältigungsrecht stellt zusammen mit dem Verbreitungsrecht die Hauptanwendung der Verwertung des Werkes in körperlicher Form dar. Durch das Vervielfältigungsrecht soll dem Urheber ein Entgelt für diejenigen Nutzungshandlungen zugesichert werden, welche darin bestehen, dass ein Werkgenuss nicht durch das Original selbst, sondern durch Vervielfältigungen des Originals erfolgt. Durch diesen Vervielfältigungsprozess des Werkes tritt ein Multiplikatoreffekt ein, welcher es

ermöglicht, dass einem sehr viel größeren Personenkreis, unabhängig von der Benutzung des Originals, der Werkgenuss ermöglicht wird [UrhG06].

Auch nach heutigem Verständnis der Materie ist von einem weiten, umfassenden Vervielfältigungsbegriff auszugehen. Vervielfältigung ist demnach jede körperliche Festlegung eines Werkes, welche geeignet ist, das Werk auf irgendeine Weise unmittelbar oder mittelbar den menschlichen Sinnen wahrnehmbar zu machen. Auf welche Art und Weise und in welcher Anzahl die Vervielfältigung erfolgt, ist dabei ohne Belang. Dadurch ist auch die so genannte Digitalisierung eines Werkes als Vervielfältigung zu bezeichnen. Dies gilt jedenfalls dann, wenn mit der Digitalisierung eine Festlegung der digitalen Fassung auf einen beliebigen Datenträger einhergeht. Ein gesondertes Recht an der Digitalisierung eines Werkes ist nach alledem nicht erforderlich. Fraglich war bislang dagegen, ob eine Digitalisierung auch dann eine Vervielfältigung im Sinne des §15 UrhG darstellt, wenn keine dauerhafte Festlegung der digitalisierten Form erfolgt, es zum Beispiel bei einer Zwischenspeicherung im Arbeitsspeicher verbleibt. Nach den neuen EU-Richtlinien zum Urheberrecht fallen auch vorübergehende Vervielfältigungen von kürzester Dauer grundsätzlich unter das Vervielfältigungsrecht des Urhebers, ausgenommen hiervon sind jedoch flüchtige Vervielfältigungen wie sie beispielsweise beim „Routing“, also bei der Datenübertragung im Internet, vorkommen [Schr99; FrNo98].

5.11 Die Schranke der Vervielfältigung zum privaten Gebrauch als Einschränkung des Vervielfältigungsrechts

Schrankenregelungen, die das Vervielfältigungsrecht betreffen, finden sich in sämtlichen Vorschriften der §§42 ff. UrhG. Unter der Schranke der Vervielfältigung zum privaten Gebrauch wird der Verwendungszweck in der Privatsphäre zur Befriedigung rein persönlicher Bedürfnisse durch die eigene Person oder mit ihr durch ein persönliches Band verbundene Person verstanden [UrhG06]. Der entsprechend Befugte darf das Werk auf beliebige Weise vervielfältigen, wenn die Vervielfältigung lediglich der Befriedigung persönlicher, also weder beruflicher noch erwerbswirtschaftlicher Bedürfnisse seiner selbst oder seines engeren Freundes- und Familienkreises dient [FrNo98; MöNA00].

Schon beim Entwurf zum UrhG 1965 sah der Gesetzgeber „einschneidende Änderungen“ durch neue Erfindungen auf dem Gebiet der Vervielfältigungsverfahren und hieraus resultierende Probleme, welche für das Urheberrecht „von weittragender Bedeutung seien“. So wies das Gericht vorausschauend schon damals im Hinblick auf das Vervielfältigungsrecht darauf hin, dass der Urheber im Falle einer freigestellten Privatsphäre bei allen Werken, die vorwiegend für den Werkgenuss im privaten Bereich geschaffen werden, kaum noch wirtschaftliche Früchte aus der Arbeit ziehen könne, sobald die Technik es jeder einzelnen Person ermöglicht, ohne besondere Kosten und Mühen Werkstücke im häuslichen Bereich selbst herzustellen. Besonders dann, wenn sie einen einwandfreien Werkgenuss vermitteln und den gewerblich hergestellten Vervielfältigungsstücken gleichwertig seien, sah der Gesetzgeber eine angemessene Vergütung vor[Schr99].

Ein komplettes Verbot der privaten Vervielfältigung wurde jedoch weiter mit der Überlegung abgelehnt, dass dieses Verbot in der Praxis nicht hätte durchgesetzt werden können. Eine wirksame Überprüfung könne nur dann durchgeführt werden, so die Begründung, wenn es den Kontrolleuren der privaten Verwertungsgesellschaften gestattet werden würde, die Wohnung jedes einzelnen Staatsbürger daraufhin zu überprüfen, ob dieser ein Gerät besitzt, mit welchem man urheberrechtlich geschützte Werke vervielfältigen könnte und für alle vervielfältigten Werke eine Genehmigung des jeweiligen Urhebers nachweisen kann [Schu03, 159]. Ein solch massenhaftes Ausforschen, ob gesetzliche Bestimmungen eingehalten werden oder nicht, hätte auch für den Fall einer entsprechenden gesetzlichen Regelung die Frage der Verhältnismäßigkeit der Mittel herausgefordert.

Dies lässt darauf schließen, dass der Gesetzgeber insoweit eher auf den appellativen Charakter eines Verbotes speziell in den genannten Fällen hoffte [MöNA00].

5.11.1 EU-Richtlinie zum Urheberrecht in der Informations-Gesellschaft

Mit der Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22.05.2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (im folgenden InfoRL) dringt der europäische Gesetzgeber erstmals in den Kernbereich des Urheberrechts vor. Die

InfoRL befasst sich dabei entgegen ihres Titels nicht ausschließlich mit Fragen des Urheberrechts in der Informationsgesellschaft, also mit Fragen, die durch die Digitalisierung und Vernetzung an das Urheberrecht herangetragen werden. Es geht vielmehr um nicht weniger als die horizontale Harmonisierung der Kernvorschriften des Urheberrechts insgesamt, indem Verwertungsrechte und Schrankenregelungen festgeschrieben werden. Ziel der InfoRL ist es, gemeinsame Regeln für den Schutz des Urheberrechts und der Leistungsschutzrechte im Rahmen des freien Waren- und Dienstleistungsverkehrs im europäischen Binnenmarkt zu schaffen [o.V.06d].

Durch Art.2 InfoRL ist das Recht der Vervielfältigung geregelt. Danach ist dem Urheber das ausschließliche Recht vorbehalten, die unmittelbare oder mittelbare, vorübergehende oder dauerhafte Vervielfältigung seiner Werke auf jede Art und Weise und in jeder Form ganz oder teilweise zu erlauben oder zu verbieten. Insbesondere wird nicht zwischen analoger und digitaler Vervielfältigung unterschieden.

In Art. 5 Abs. 2 lit. b InfoRL findet sich die spezifische Schrankenregelung für die private Vervielfältigung. Demnach können die Mitgliedsstaaten Ausnahmen vom Vervielfältigungsrecht vorsehen in Bezug auf Vervielfältigungen auf beliebigen Datenträgern durch eine natürliche Person zum privaten Gebrauch, wenn die Vervielfältigung weder direkt noch indirekt kommerziellen Zwecken dient und die Rechteinhaber einen „gerechten Ausgleich“ erhalten [o.V.06d].

Wie bereits oben erwähnt, unterscheidet die InfoRL in ihrer endgültigen Fassung in Art. 5 Abs. 2 lit. b nicht zwischen digitalen und analogen Privatkopien. Gleichwohl enthalten die Erwägungsgründe Hinweise auf eine Forderung nach einer Differenzierung zwischen diesen beiden Varianten, besonders im Hinblick auf die Höhe der Vergütung. Aus seinem Wortlaut wird man dagegen noch nicht folgern können, dass dem nationalen Gesetzgeber bei der Umsetzung der Richtlinie Differenzierungen dahingehend gestattet sind, dass digitale private Vervielfältigungen als solche für unzulässig erklärt werden können [o.V.06d].

Weiters stellt sich die Frage, ob ein Verbot der digitalen Privatkopie trotz der Einführung „wirksamer technischer Maßnahmen“ erlaubt ist oder nicht. Gemeint sind hiermit insbesondere Kopierschutzsysteme, welche die Vervielfältigung von Werken verhindern sollen, im Weiteren aber auch das umfassendere so genannte Digitale Rights Management (DRM). Die InfoRL regelt entsprechende Maßnahmen in Art. 6 und 7 in Umsetzung zum Teil recht allgemein gehaltener Vorgaben aus den WIPO Verträgen WCT und WPPT. Solche Maßnahmen basieren auf der Überlegung, dass der Schutz des

Urheberrechts im digitalen Umfeld größtenteils auf der Anwendung technischer Schutzvorrichtungen basieren wird, die von den Rechteinhabern zu diesem Zweck eingesetzt werden. Zwar wird der Zusammenhang zwischen zulässiger Vervielfältigung, Vergütung und technischer Schutzmaßnahmen an mehreren Stellen der InfoRL angesprochen, aber eine genaue Verhaltensweise für den einzelnen Gesetzgeber kann jedoch daraus nicht abgeleitet werden [o.V.06d].

Zusammenfassend kann gesagt werden, dass ein generelles Verbot der Privatkopie laut der Auffassung des Gesetzgebers im häuslichen Bereich nicht durchzusetzen ist. Das Aufkommen von digitalen Vervielfältigungsmöglichkeiten änderte in diesem Sinne nichts an der grundsätzlichen Entscheidung des Gesetzgebers für die private Vervielfältigung. Der nationale Gesetzgeber zog demgemäß die mehrfach vorhandene Möglichkeit, bei Urheberrechtsreformen die private Vervielfältigung insgesamt zu untersagen, nicht in Betracht. Dem liegt zum einem die Erkenntnis zu Grunde, dass die Privatkopie nach wie vor nicht kontrollierbar ist, zum anderen ist durch die Rechtssprechung der Umstand bekannt, dass für die Privatkopie Interessen der Allgemeinheit angeführt werden können und über das Mittel der Vergütungspflicht insoweit ein adäquater Ausgleich geschaffen werden kann. Auch die InfoRL von 2001, die erstmals Kernbereiche des Urheberrechts regelt, enthält sich einer abschließenden Stellungnahme zur Zulässigkeit der digitalen Privatkopie. Dem ist der österreichische Gesetzgeber mit dem Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft inhaltlich gefolgt.

5.12 Zuständigkeit österreichischer Gerichte

Das Internet ist ein Datennetz, in dem Informationen rund um den Globus versendet werden. Mit der Nutzung von Diensten wie vor allem dem World Wide Web und Peer-to-Peer Systemen werden die Auswirkungen jeder einzelnen dort vorgenommen Handlung auf der ganzen Welt sichtbar. Dieser transnationale Aspekt führt dazu, dass Vorkommnisse, welche eigentlich weit ab von Österreich erfolgen, auch hierzulande einen Effekt zeigen. Doch kann nicht jede im Netzwerk gesetzte strafrechtlich bedenkliche Handlung gleichsam automatisch der österreichischen Jurisdiktion unterstellt werden. Vielmehr ist in jedem Einzelfall zu überprüfen, ob ein ausreichender Anhaltspunkt besteht, diesen vor ein inländisches Gericht zu bringen.

Alle hier besprochenen Handlungen sind Formaldelikte, daher ist lediglich der Ort der Handlung maßgeblich. Somit beschränkt sich die österreichische Zuständigkeit auf all jene Handlungen, die ihren Ausgangspunkt innerhalb der österreichischen Grenzen genommen haben. Eine gegenteilige Auffassung würde bedeuten, dass Österreich für alle auf dieser Welt im Internet begangenen Delikte zuständig wäre. Das würde eine schier unerträgliche Situation für Österreich darstellen. Es kann daher lediglich auf den Ort ankommen, von dem aus der Täter gehandelt hat. Es ist daher irrelevant, ob die Information auf ihrem Weg irgendwo über österreichisches Territorium gelangt ist oder ob sie schließlich aus dem Inland abrufbar ist.

Ein internationales Computernetzwerk kann niemals nur im Hinblick auf eine einzelne Rechtsordnung betrachtet werden; die Auswirkungen, die eine Handlung hat, welche in einem solchen Netzverbund gesetzt wird, sind weltweit zu bemerken. Daher ist nur ein internationales Vorgehen zielführend. Bisher sind solche Bemühungen noch nicht sehr weit gediehen, in erster Linie liegt das daran, dass das Internet bzw. seine weltweite und nicht immer harmlose Nutzung für die gesetzgebenden Gremien ein noch relativ neues Phänomen ist und es so noch einiger Zeit bedarf, um entsprechende und passende Regelungen auszuarbeiten. Andererseits ist es gerade in globaler Sicht nicht einfach, einen gemeinsamen Konsens darüber zu finden, welche Einschränkungen des Informationsaustausches im Internet vorgenommen werden sollen. Die Einstellungsunterschiede, welche durch die unterschiedlichen Kulturen gegeben sind, gleichzeitig aber auch die verschieden hohe Bewertung der Freiheit der Meinungsäußerung sowie des Austausches von Ideen und Informationen machen eine weltweite Einigung, welche Inhalte im Internet verboten sein sollen, fast unmöglich.

Ein gänzlich anderes Problem, welches nicht in dieser Arbeit erfasst ist, besteht darin, die Identität von Personen festzustellen, bzw. ihrer habhaft zu werden, um sie zur Verantwortung zu ziehen. Ganz besonders gilt dies für den Fall, dass aus dem Ausland operiert wird. Vor allem durch den Einsatz kryptographischer Verfahren kommt die Schwierigkeit der Feststellung hinzu, ob eine übermittelte Information überhaupt unter den Straftatbestand fällt. Hierbei handelt es sich aber nicht um strafrechtlich-wissenschaftliche Probleme, sondern „lediglich“ um Beweisschwierigkeiten in konkreten Einzelfällen.

5.13 Handlungsoptionen des Gesetzgebers in Urheberrecht aus rechtsökonomischer Sicht

Bei der Erstellung neuer Gesetze sollte sich der Gesetzgeber sowohl an der Effizienz der neuen Vorhaben als auch an deren Beitrag zur Maximierung der gesamtwirtschaftlichen Wohlfahrt orientieren. Im Folgenden werden fünf mögliche Handlungsoptionen des Gesetzgebers angeführt und kurz bewertet.

Die Allgegenwart des Internets und der damit überall mögliche Zugang zu digitalen Medien eröffnet einen weiteren Problembereich, mit welchem sich die Gesetzgeber in Zukunft verstärkt zu befassen haben. Es handelt sich hierbei um das internationale Urheberrecht, das bisher nur in sehr wenigen Staaten geregelt ist. Die große Frage ist wie der Urheberschutz grenzüberschreitend gewährleistet werden soll [BoNe01].

Derzeit folgt das Urheberrecht dem Territorialitätsprinzip, wonach jedes Land ein eigenes nationales Urheberrecht hat, welches nur innerhalb der Grenzen des jeweiligen Staates anwendbar ist. Dem folgt auch das österreichische Schutzlandprinzip, nach dem die Rechteinhaber ihre Rechte nur im jeweiligen Schutzland geltend machen dürfen. In diesen Kontext ergeben sich jedoch Schutzlücken für die Rechteinhaber, welche auch durch die internationalen Verträge nicht völlig ausgeräumt werden können [BoNe01, 139]. Jenes Problem führte zur Idee, den jeweiligen Schutz eines digitalen Werkes an seine Herkunft zu knüpfen (Herkunftslandprinzip). Dabei wird jedoch die Rechtsunsicherheit nicht behoben, sondern verschiebt sich nur vom Rechteinhaber auf den Rechtenutzer. Zusätzlich ergibt sich auch für den Urheber eine große Gefahr: Durch die Möglichkeit, die Erstveröffentlichung eines digitalen Werkes auf einen beliebigen Server zu transferieren, indem man diesen in einem Land mit möglichst wenig Restriktionen aufstellt, löst ein Wettrennen nach dem Land mit dem geringsten Schutzniveau aus [HoSi00, Kap 7.10].

Aufbauend auf den bisherigen internationalen Verträgen, muss es daher das Ziel sein, eine globale konsensuale Lösung zu finden, die, Rechteinhaber wie Rechtenutzer gleichermaßen schützt. Handlungsoptionen des Gesetzgebers im Urheberrecht nach Fränkl aus rechtsökonomischer Sicht können daher sein:

- moralische Appelle;
- Erweiterung des Pauschalabgabemodells;

- Verschärfung der Gesetzgebung und
- Selbstregulierung durch DRMS [Frän03].

5.13.1 Handlungsoption: Moralische Appelle

Durch moralische Appelle könnte ein Mittel gefunden werden, um Probleme wie das illegale Kopieren von digitalen Medien zu lösen, indem der Versuch unternommen wird, die Kunden in eine vorbestimmte Richtung zu lenken. Dabei ist es wichtig den Kunden klar zu machen, welche Auswirkungen ihr Verhalten für das Schaffen zukünftiger Werke darstellt. Weiters sollte eine Basis gefunden werden, in der eine ethnisch-moralische Akzeptanz der Konsumenten für die Verwertung von urheberrechtlichen Werken vorherrscht. Derzeit ist jene Akzeptanz nur bei wenigen Endverbrauchern vorzufinden. Die meisten Endnutzer werten Urheberrechtsverletzungen als Kavaliersdelikte und sehen das veränderte hohe Preisniveau aufgrund fallender Transaktionskosten als ungerechtfertigt an [Kuhl02].

5.13.2 Handlungsoption: Erweiterung des Pauschalabgabemodells

Seit 1. April 1996 ist die Betreibervergütung (Reprografieabgabe) Inhalt des österreichischen UrhG [UrhG06, §42]. Durch diese Regelung wird der Urheber für die legale Kopie seines Werkes entschädigt, indem der Anbieter von Geräten, welche zur Vervielfältigung von urheberrechtlich geschützten Werken bestimmt sind, eine Pauschalabgabe zahlt. Verwertungsgesellschaften nehmen in diesem Zusammenhang die Abwicklung jener Abgaben wahr.

Neben der Abgabe auf analoge Geräte gibt es bereits auch Pauschalabgaben auf DVD- und CD-Brenner sowie auf Scanner. Seit 1. Jänner 2006 sind auch in Österreich Urheberrechtsabgaben auf Computer und Drucker vorgesehen. Dazu haben sich die Literar Mechana, Wahrnehmungsgesellschaft für Urheberrechte, und die Verwertungsgesellschaft bildender Künstler im Dezember 2005 geeinigt [Futu06a].

5.13.3 Handlungsoption: Verschärfung der Gesetzgebung

Eine weitere Möglichkeit für den Gesetzgeber besteht darin, die Gesetze generell zu verschärfen. Das bisherige Problem an der Gesetzeslage ist, dass die Kosten der Verfolgung von Urheberrechtsverletzungen an digitalen Werken um ein Vielfaches höher sind, als der Nutzungswert, welcher aus einer ungerechtfertigten Verwendung entsteht. Durch diesen Umstand entwickelt sich das Prinzip der „eingeschränkten Piraterieverfolgung“. Meistens handelt es sich dabei um Personen mit niedriger Zahlungsbereitschaft für digitale Werke, da Nutzer mit hoher Zahlungsbereitschaft auch bei niedrigen Strafen das Risiko einer Verfolgung nicht eingehen [Dete01].

5.13.4 Handlungsoption: Selbstregulierung durch DRMS

Der Gesetzgeber hat auch die Option des Laissez-Faire. Jenes Element, welches aus dem Liberalismus stammt und auf die selbständige Regulierung des Marktes aufbaut, ohne die Eingriffe des Staates. Durch die ständige Weiterentwicklung von DRMS könnte sich diese Handlungsmöglichkeit als eine bedeutende Alternative zu Regulierungs- und Abgabemodellen herausstellen, denn DRMS bieten die Möglichkeit der Selbstregulierung durch individuell ausgehandelte Verträge zwischen Konsument und Urheber.

5.14 Zusammenfassung

Aus der Sicht der Problematik der zunehmenden Anzahl an Urheberrechtsverletzungen stellen DRMS eine technische Lösung dar, die Zugangs- und Nutzungskontrolle und Abrechnung von physikalischen und digitalen Inhalten zu unterstützen.

Derzeit kann der Weltmarkt als globaler, dynamischer Markt charakterisiert werden, der sich noch in der Entwicklung befindet. Aus der Perspektive von Medienunternehmen sind zentrale Erfolgsfaktoren von DRMS vor allem durch ihre einfache Bedienbarkeit, ihre auf Fair-Use basierende Konzeption sowie ihre hohe Standardisierung gekennzeichnet. Weiters muss erwähnt werden, dass nur dann, wenn der Nutzer ein DRMS leicht bedienen kann und sich fair behandelt fühlt, auch DRMS akzeptieren wird. Am Beispiel von Liquid Audio und Apple iTunes kann man deutlich erkennen,

dass einfache Bedienung und faire Preisgestaltung regelrechte Erfolgsgaranten darstellen.

Seit es Computerprogramme gibt, ist das Problem der illegalen Kopie vorhanden. Die Contentindustrie wehrt sich durch die Verwendung eines Kopierschutzes gegen die unrechtmäßige Nutzung ihrer Produkte. Im Laufe der Jahre wurden diese Verfahren immer mehr verfeinert. Unter anderem deshalb, weil Cracker die Kopierschutzverfahren immer wieder geknackt und damit die Software- oder Audio-CDs kopierbar gemacht haben. Dabei gibt es zwei grundsätzliche Möglichkeiten, eine CD vor dem Kopieren zu schützen: Entweder verhindert der Schutz, dass sich eine CD überhaupt kopieren lässt, oder er sorgt dafür, dass sich die Kopien hinterher nicht verwenden lassen. Mittlerweile hat auch der Gesetzgeber auf diese Problematik reagiert und die Umgehung jeglicher Kopierschutzverfahren unter Strafe gestellt.

Aus der Sicht der Medienunternehmen ist ein hohes Problembewusstsein vorhanden, jedoch herrscht gleichzeitig eine große Unsicherheit, insbesondere durch die unklare Linie der Gesetzgeber. Die Gesetzgebung hat wie bereits früher, besonders im Urheberrecht, eine abwartende Haltung gegenüber neue Entwicklungen wie etwa DRMS, und reagieren daher erst spät auf solche Trends.

Es muss jedoch die Illusion aufgegeben werden, dass mittels DRMS die Verbreitung von digitalem Content total kontrolliert werden kann, denn die analoge Lücke werden DRMS ebenso wenig gänzlich schließen können wie die organisierte Kriminalität. Andersherum werden zu stark geschützte digitale Inhalte als minderwertig eingestuft und finden daher ebenfalls keine Abnehmer.

Die vorliegende Untersuchung hat auch gezeigt, dass sich der einzelne trotz des Massencharakters des Phänomens Filesharing insgesamt nach wie vor grundsätzlich auf die Anwendbarkeit individueller urheberrechtlicher Schrankenregelungen berufen kann. Es stellt sich in diesem Zusammenhang die Frage, ob dieses Ergebnis die widerstreitenden Interessen der Urheber und der Allgemeinheit tatsächlich noch in einem ausgewogenen Verhältnis zeigt oder ob insoweit eine Korrektur des Gesetzes erforderlich ist.

Zusammenfassend muss daher ein Gleichgewicht zwischen den technologischen Möglichkeiten, den erforderlichen und möglichen Funktionen, rechtlichen und rechtsökonomischen Aspekten sowie sozialen und gesellschaftlichen Betrachtungen gefunden werden.

6 Internationale Gesetze, Abkommen und Organisationen, welche sich mit der Thematik des Filesharings auseinandersetzen

6.1 Internationale Entwicklungen

6.1.1 Revidierende Berner Übereinkunft (RBÜ)

Die Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst vom 09.09.1886 ist der älteste multinationale Vertrag auf dem Gebiet des Urheberrechts. Sie wurde entsprechend der Vorgaben in Art.27 Abs. 1 RBÜ im Sinne einer kontinuierlichen Verbesserung des Urheberrechtsschutzes mehrfach vervollständigt und revidiert, zuletzt am 24.07.1971 in Paris. Im Vergleich mit allen anderen Urheberrechtsabkommen gewährleistet die RBÜ das höchste Schutzniveau. So erwähnt die Übereinkunft in Art. 5 das Prinzip der Inländerbehandlung, sie gewährt ausländischen Urhebern also annähernd dieselbe Rechtsstellung wie inländischen. Darüber hinaus gewährt die RBÜ zahlreiche Rechte, auf die sich jeder Urheber eines anderen Mitgliedstaates der RBÜ im jeweiligen Schutzland als mindestens zustehend berufen kann. Das bestehende Schutzniveau wird dabei durch Art. 20 RBÜ gesichert. Danach können die Verbandsstaaten zwar weitere Abkommen treffen, aber nur sofern ein weiterreichender Schutz vereinbart wird oder sofern die Bestimmungen solcher Abkommen den durch die RBÜ gewährten Rechten nicht zuwiderlaufen[o.V.06e].

6.1.2 Welturheberrechtsabkommen (WUA)

Am 06.09.1952 wurde in Genf das von der UNESCO initiierte Welturheberrechtsabkommen (WUA) als zweites großes multilaterales Abkommen unterzeichnet. Mit der Einführung des WUA wurde das Ziel verfolgt, einzelne Staaten, welche das hohe Schutzniveau der RBÜ auf absehbare Zeit nicht erreichen konnten, in ein internationales Schutzsystem einzubinden. Das Schutzniveau ist daher nicht so hoch einzustufen als in der RBÜ. Ebenso sind die Mindestrechte der Urheber, welche das WUA gewährt, deutlich schwächer ausgeprägt als in der RBÜ.

Die Bedeutung des WUA ist inzwischen recht gering, insbesondere deshalb, weil das WUA nicht zur Anwendung kommt, wenn zwischen zwei Staaten die RBÜ Anwendung findet. Die praktische Bedeutung des WUA beschränkt sich im Wesentlichen auf die urheberrechtlichen Beziehungen zu kleineren Staaten, welche nur dem WUA, nicht aber der RBÜ angehören.

6.1.3 ROM-Abkommen

Das am 26.10.1961 unterzeichnete internationale Abkommen über den Schutz der ausübenden Künstler, der Hersteller von Tonträgern und der Sendeunternehmen, kurz Rom- Abkommen (RA) genannt, betrifft die verwandten Schutzrechte. Es ist das erste und wichtigste Übereinkommen auf dem Gebiet des internationalen Leistungsschutzrechts. In dem von 1961 geschlossenen Abkommen finden naturgemäß keine Aspekte des digitalen Zeitalters Berücksichtigung.

6.1.4 TRIPs-Übereinkommen

Das Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums (Österreich: Abkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums) bezeichnet als TRIPs-Übereinkommen oder auch nur als TRIPs („Agreement on Trade-Related Aspects of Intellectual Property Rights“) ist am 01.01.1995 in Kraft getreten. Gegenstand des TRIPs –Schutzes sind unter anderem das Urheberrecht und bestimmte verwandte Schutzrechte, Art.1 Abs.2, Art.9 -14 TRIPs. Das TRIPs- Übereinkommen ist als Bestandteil des WTO-Übereinkommen für alle seine Mitglieder verbindlich [Wiki06o]. Zum 03.09.2006 waren dies insgesamt 149 Staaten [o.V.06f], darunter die Europäische Gemeinschaft als eigenständiges Mitglied neben den einzelnen Mitgliedsstaaten der Gemeinschaft. Auf die Hintergründe des Abschlusses des TRIPs Abkommen soll hier im Detail nicht eingegangen werden.

Der durch das TRIPs Abkommen gewährte Schutz ist ein Mindestschutz. Die Mitglieder können jedoch weiter reichende Maßnahmen vorsehen, sofern diese den TRIPs-Zielen nicht zuwider laufen. Das TRIPs- Abkommen befasst sich auch mit Gegenständen, welche bislang von der RBÜ nicht ausdrücklich geregelt wurden, wie zum Beispiel Computerprogramme und Datensammlungen (Art.10 TRIPs). Daraus

kann geschlossen werden, dass eine Modernisierung des internationalen Urheberrechtsschutzes im Hinblick auf die Herausforderungen der Informationsgesellschaft an das Urheberrecht stattgefunden hat.

6.1.5 WIPO-Verträge

Auf der Konferenz der Weltorganisation für geistiges Eigentum (WIPO) in Genf wurden zwei internationale Verträge über das Urheberrecht und über verwandte Schutzrechte am 20.12.1996 geschlossen. Zum einen der WIPO-Urheberrechtsvertrag (WIPO Copyright Treaty, kurz WCT), zum anderen der WIPO-Vertrag über Darbietungen und Tonträger (WIPO Performances and Phonograms Treaty, kurz WPPT). Die Europäische Union hatte damals erklärt, den beiden WIPO-Verträgen zusammen mit den Mitgliedsstaaten erst dann beizutreten, wenn die Richtlinie zum Urheberrecht in der Informationsgesellschaft, welche die Bestimmungen der WIPO-Verträge aufgreift, von allen Mitgliedsstaaten in nationales Recht und soweit wie möglich auch auf Gemeinschaftsebene umgesetzt worden ist.

6.1.5.1 WIPO Copyright Treaty (WCT)

Der WCT ist das Ergebnis der Bemühungen der WIPO, das internationale Urheberrecht auf der Grundlage der seit 1971 nicht mehr revidierten RBÜ fortzuentwickeln. Im Vergleich zu den TRIPs zeichnen sich WCT und WPPT durch einen traditionelleren Ansatz aus. Die beiden Verträge sind nicht mit konkreten handelspolitischen Maßnahmen verknüpft und verzichten auf das Schutzprinzip der Meistbegünstigung (vgl. Art.4 TRIPs). Im Gegensatz dazu tragen sie jedoch bereits den neueren Entwicklungen der Informationstechnik Rechnung. Neu sind auch die in Art. 11 und 12 WCT enthaltenen Schutzverpflichtungen in Bezug auf technische Schutzmaßnahmen und kodierte Informationen über die Rechteverwaltung („rights management information“). Aus Art 10 Abs. 2 WCT kann man entnehmen, dass Ausnahmen und Beschränkungen der nationalen Gesetze, die bislang als den Bestimmungen der RBÜ entsprechend angesehen worden sind, künftig auch auf den digitalen Bereich ausgedehnt werden dürfen.

6.1.5.2 WIPO Performances and Phonograms Treaty (WPPT)

Der WPPT steht nach Art. 1 Abs. 3 WPPT mit keinen anderen internationalen Abkommen in rechtlicher Verbindung; Rechte oder Pflichten der Vertragsparteien aus anderen internationalen Verträgen werden dabei nicht berührt.

6.2 Organisationen

Der Großteil der Raubkopierer weiß inzwischen, dass er durch seine Handlungen nicht gesetzeskonform agiert. Doch die konkreten Strafen, welche er bekommen könnte, sind ihm meistens nicht bewusst. Es gibt nur wenige Menschen, welche bereits verklagt wurden oder jemanden kennen, der bereits belangt wurde. Dabei handelt es sich nicht um eine Ordnungswidrigkeit, wie es zum Beispiel beim Falschparken der Fall wäre, sondern um ein strafrechtliches Delikt. Raubkopierer können also durch die Polizei festgenommen und strafrechtlich durch die Staatsanwaltschaft verfolgt werden. Die Sanktionen, welche sich aus einem solchen Verfahren ergeben können, reichen von Geld- bis Freiheitsstrafen. Es besteht jedoch auch die Möglichkeit, dass die Rechteinhaber zivilrechtlich gegen einen Raubkopierer vorgehen können, was beträchtliche Schadenersatzforderungen mit sich bringen kann.

Theoretisch kann jeder beliebige Filesharingnutzer, welcher illegal urheberrechtlich geschützte Dateien downloadet und dabei keine Verschleierungsmethode benutzt, identifiziert und angeklagt werden. Das Problem ist jedoch, dass es weltweit Millionen von Raubkopierern gibt, welche sich täglich im Internet mit dem neusten „Warez“ versorgen. Die Verfolgung jedes einzelnen Straftäters ist aufgrund der Anzahl an Vorfällen nicht möglich. Das schien zuerst nicht tragisch zu sein, da die Industrie nicht das Ziel verfolgte einzelne Nutzer zu verfolgen. Vielmehr wurden die Betreiber der so genannten Tauschbörsen bekämpft, was jedoch mit wenig Erfolg gekrönt war. Als dann später noch die Umsätze der Unterhaltungsindustrie sanken und die tatsächliche Anzahl der aktiven Filesharinguser immer weiter stieg, entschloss man sich dann doch zu härteren Maßnahmen gegen die einzelnen Nutzer. In der Praxis werden jedoch nur die wenigsten Vergehen straf- oder zivilrechtlich verfolgt. Dem einzelnen Tauschbörsennutzer droht am meisten Gefahr durch die Urheber selbst, da sie sich in zahlreiche Verbände zusammengeschlossen haben und dabei die Raubkopierer oft auf

eigene Faust verfolgen. Die wichtigsten und größten werden im folgenden Abschnitt kurz vorgestellt [KrSe06, 201-202].

6.2.1 Business Software Alliance (BSA)

Die Business Software Alliance ist ein globaler Interessenverband, welcher sich für den Schutz von Software und deren legale Verwendung einsetzt. Führende Softwarehersteller, wie zum Beispiel Microsoft, Apple oder IBM engagieren sich dabei für das Durchsetzen von Urheberrechten und die Erhaltung der Sicherheit im Internet. Das Hauptanliegen der BSA ist es dabei, sowohl mit zivil- und strafrechtlicher Verfolgung wie auch durch den Einsatz von Aufklärungsprogrammen die hohe Raubkopiererrate zu reduzieren. Des Weiteren setzt sich der Verband auch für die strikte Einhaltung der Urheberrechtsgesetze ein [Wiki06a].

In einem Kinospot im Jahr 2000 führte der deutsche Zweig der BSA jeden einzelnen Kinobesucher vor, welche Strafen Raubkopierern drohen [BSA05]. Jedoch auch das medienwirksame Zerstören von Raubkopien gehört neben solchen Spots zu den Aktivitäten der BSA. Es wurden bereits Tausende Schwarzkopien in Schreddern zerhäckselt, verbrannt [Schu04] oder raubkopierte CDs von Dampfwalzen überfahren [Faiß00].

Weiters bietet sie die Möglichkeit über ihre jeweiligen länderspezifischen Webseiten oder über eine kostenlose Telefonhotline mutmaßliche Strafdaten zu melden. Neben der BSA gibt es weitere Industrieverbände, welche Lobbyarbeit für eine strengere Gesetzgebung betreiben und Klagen gegen Raubkopierer in die Wege leiten. Für die Musikbranche sind dies zum Beispiel der Verband der US-Musikindustrie RIAA sowie der Weltverband der Phonoindustrie IFPI [KrSe06, 202-203].

6.2.2 Verband der US-Musikindustrie (RIAA) und Weltverband der Phonoindustrie (IFPI)

Die Recording Industry Association of America (RIAA – Verband der Musikindustrie in den USA) ist eine Interessensgemeinschaft, welche die Anliegen der Unternehmen aus der Musikindustrie in den USA vertritt. Die RIAA ist durch ihr vehementes Vorgehen gegen die Tauschbörsen in die Medien gekommen. Sie tritt unter anderem für

die Rechte der vier größten Plattenfirmen (SonyBMG, Universal Music, EMI und Warner) ein, und damit aus ihrer Sichtweise auch für deren Künstler [Wiki06b]. Im Jahr 2002 hat die RIAA erstmals auch begonnen gegen Enduser mit juristischen Mitteln vorzugehen [Scho02].

Die RIAA arbeitet dabei sehr eng mit dem in Deutschland und weltweit aktiven Verband International Federation of the Phonographic Industry (IFPI) zusammen. Die Hauptaufgabe der IFPI besteht unter anderem in der Wahrung der Urheberrechte auf der ganzen Welt, wobei die einzelnen Mitglieder national wie international die Interessensvertreter der Phonoindustrie gegenüber der Politik darstellen. Ein weiterer wichtiger Aufgabenbereich der IFPI ist in den letzten Jahren die Bekämpfung der Musikpiraterie. Besondere Bedeutung hat darüber hinaus die technische und rechtliche Umsetzung des weltweiten Musikhandels über das Internet und andere digitale Medien bekommen [Wiki06c]. Nicht zuletzt ist für die Filmbranche die MPAA im Kampf gegen die Raubkopierer im Einsatz [KrSe06, 202-203].

6.2.3 Motion Picture Association of America (MPAA)

Die Motion Picture Association of America (MPAA) ist eine US-amerikanische Organisation, welche ihren Hauptsitz in Encino, Kalifornien hat. Die Hauptaufgabe der MPAA besteht darin, Filme zu bewerten und danach zu entscheiden, für welche Ziel- und Altersgruppe der jeweilige Film geeignet ist. Vor allem große Filmgesellschaften lassen zurzeit ihre Filme von der MPAA überprüfen und sind gleichzeitig Mitglieder dieser Organisation. Die bekanntesten von ihnen sind: The Walt Disney Company, Sony Pictures Entertainment (mit den Labels Columbia Pictures, TriStar Pictures, Metro-Goldwyn-Mayer und United Artists), Paramount Pictures, Twentieth Century Fox, Universal Studios und Warner Bros [Wiki06d].

Die deutsche und österreichische Filmbranche und Unterhaltungssoftwareindustrie arbeitet mit der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU) zusammen, welche ein Tochterunternehmen von der MPAA ist. Sie trägt im Netzwerk der internationalen Antipiraterie-Organisationen der MPA (Motion Picture Association) dazu bei, geistiges Eigentum zu schützen, die Verbreitung von Raubkopien einzudämmen und den durch sie entstehenden wirtschaftlichen Schaden so gut wie möglich zu begrenzen [Wiki06e]. Sie agiert dabei wie eine Art Privatpolizei der

Branche, da sie die Behörden bei der Strafverfolgung unterstützt, indem sie eigene Ermittlungen durchführt [ScVe06, 42].

Trotz der zahlreichen Klagen in den letzten Jahren ist die Gefahr relativ gering, dass man auf die Anklagebank wandern muss.

Das Internetmagazin Slick errechnete, dass es angesichts der großen Nutzerzahl wahrscheinlicher wäre, durch einen Flugzeugabsturz, Autounfall oder Mord ums Leben zu kommen, als von der RIAA verklagt zu werden [Menn05a; KrSe06, 202-203].

6.2.4 Gesellschaft zur Verhinderung von Urheberrechtsverletzungen

Die Gesellschaft zur Verhinderung von Urheberrechtsverletzungen (GVU) zeigt, welchen Weg Raubkopien nehmen. Die „Release Groups“, welche an der Spitze der Verteilung stehen, besorgen sich Filme aus unterschiedlichen Quellen, kopieren sie und verteilen sie laut GVU weiter an assoziierte Gruppen. Die GVU hemmt die Vervielfältigung von urheberrechtlich geschützten Werken an entscheidender Stelle, nämlich dort, wo der Verteilungsprozess in Gang gesetzt wird.

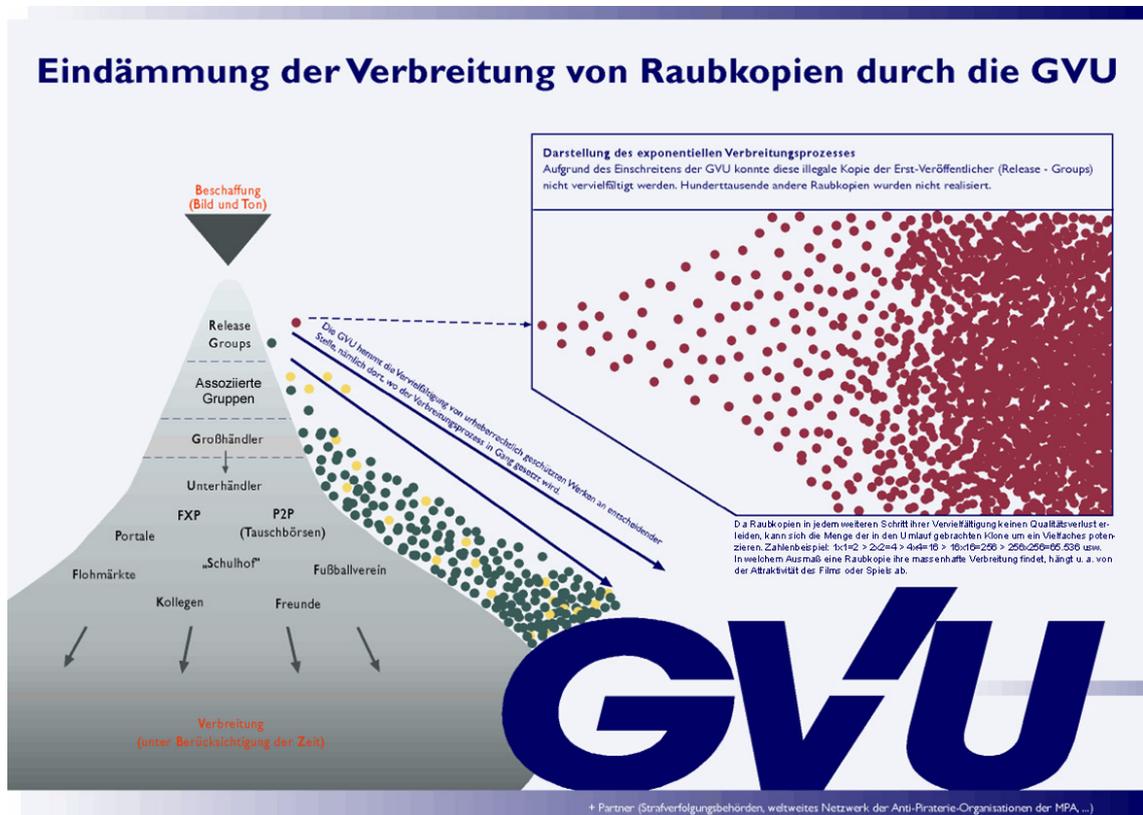


Abbildung 7: Der Weg von Raubkopien nach GVU

7 Schutzmöglichkeiten gegen ungewollte Vervielfältigung

7.1 Digital Right Management

Dr. Grisebach hält zum Beispiel die Idee des freien Inhaltes für alle für einen Irrweg: *„...warum soll gerade das Erstellen, Sammeln und Verbreiten von Informationen umsonst sein, wenn es doch angeblich die wichtigste Ressource der Zukunft ist, auch gerade in unseren Breitengraden“* [PiTh05, 99-100].

Das Recht, die Inhalte der Urheber kontrolliert zu benutzen, zu kopieren, zu verteilen und damit Geschäfte zu machen, ist durch Computer und Internet aus den Fugen geraten. Es wird nämlich milliardenfach kopiert und vermarktet, ohne dass die, denen die einzelnen Rechte gehören, einen Cent sehen. Diesem Trend soll durch die Einführung des DRM begegnet werden. Die mit der Erzeugung und dem Handel digitaler Inhalte beschäftigte Wirtschaft ist daher bestrebt, Urheberrecht und DRM zu nutzen, um auch langfristig eine Geschäftsgrundlage zu erhalten. Das „Gesetz zur Regelung des Urheberrechtes in der Informationsgesellschaft“ soll bis spätestens 2007 evaluiert und gegebenenfalls nachgebessert werden. Digital Right Management wird dabei technisch, wirtschaftlich und gesellschaftlich eine zentrale Rolle spielen.

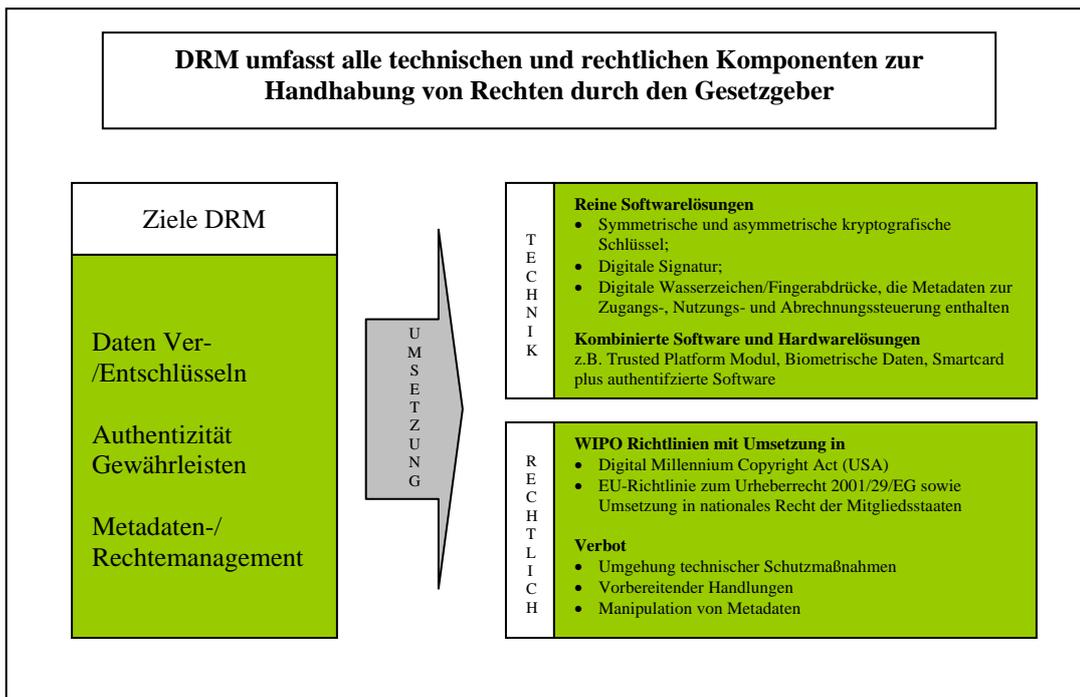


Abbildung 8: Übersicht DRM technische und rechtliche Komponenten, nach [Pico05, 3]

Digital Right Management Systeme zielen darauf ab, für digitalisierbare Inhaltsprodukte die Voraussetzung zu schaffen, damit auch in der digitalen Welt die Rechte, welche jemand mit solchen Produkten geltend machen kann, definiert und durchgesetzt werden können.

Auf der technischen Seite kennt man reine Softwarelösungen, welche auf die Verschlüsselung, auf die digitale Signatur und auf andere Kennzeichnungssysteme (Wasserzeichen, Metadaten) bis hin zur Abrechnungssteuerung zielen. Auf der Softwareebene angesiedelte Ansätze sind jedoch prinzipiell immer angreifbar und manipulierbar. Daher appellieren die meisten für kombinierte Software-Hardwarelösungen (Trusted Plattform-Chips, biometrische Daten oder Smartcard-Ansätze), weil Hardwarekomponenten schwerer veränderbar und angreifbar sind.

Medienunternehmen stehen durch die unkontrollierte Vervielfältigung von werthaltigen Inhalten vor existenziellen Bedrohungen. Digital Rights Management Systeme (DRMS) versprechen bei dieser Problematik eine Eindämmung durch die Implementierung technischer Schutzmaßnahmen.

In diesen Zusammenhang ist es problematisch, dass weder die Begriffe DRM und DRMS noch die spezifischen technischen und funktionalen Komponenten klar definiert sind.

Wenn Rechte an digitalen Gütern kostenlos definierbar und durchsetzbar wären, gäbe es kein Problem. In der Realität ist jedoch das Durchsetzen von Rechten aufwändig. Deswegen ist die Suche nach gesellschaftlich und individuell günstigen Lösungen eine sehr notwendige und auch schwierige Herausforderung. Die Urheberrechte und ähnliche Rechte versuchten bislang ein Gleichgewicht zwischen dem Interesse der Allgemeinheit und dem Interesse des Schöpfers an einer Verwertung seines Werkes zu schaffen. Die weite Verbreitung des Internets verschiebt jedoch dieses Gleichgewicht, indem sowohl Kopien als auch der Zugangsschutz in einem völlig neuen Maßstab möglich sind. Produktion und Verbreitung von Kopien sind nun zu extrem niedrigen Kosten möglich, so dass die Situation, die das alte Recht unterstellt hat, so nicht mehr existiert. Oberstes Ziel von DRM-Systemen ist es daher, die unkontrollierte Weitergabe von Inhalten zu unterbinden. Als Kombination aus Soft- und Hardware verfolgen DRMS daher eine vollständige Kontrolle über Verbreitung und Nutzung sowie eine individuelle und differenzierte Abrechnung von digitalen Inhalten [Pico05, 6-14; Hess05, 15].

Unter „digitalen Rechten“ versteht man Rechte an geistigem Eigentum in digitalisierter Form, wie zum Beispiel Filmen in WMV Format. Rechte werden von den einzelnen Anbietern in Form von Nutzungsregeln in einer „Digitale Rechtesprache“ formuliert, in den Inhalt einkodiert und auf diesem Wege in die Endgeräte hineingetragen. In den Endgeräten gibt es dann Regelinterpreten, welche diese Regeln lesen und umsetzen. Jede Nutzungsregel stellt dabei eine Einschränkung der Nutzungsmöglichkeiten für den Kunden dar.

Prof. Kuhlen findet „...dass die Digital-Rights-Regelungen (DRM) sehr weit in den Privatbereich, in den Wirtschaftsbereich, in den Politikbereich, in den Medienbereich, kurz: in sämtliche gesellschaftliche Bereiche eingreift“ [PiTh05, 128].

7.2 Problematik und Gründe der Entstehung

Wie bereits oben erwähnt, verlangt die verlustfreie Kopierbarkeit von Medieninhalten, besonders durch die Digitalisierung der Daten neue legislative, technische sowie ökonomische Strategien, solche Inhalte zu verteilen. Früher waren private Kopiervorgänge aufgrund hoher Qualitätsverluste nur eingeschränkt praktikabel und konnten pauschal vergütet werden.

Durch die starke Verbreitung von digitalisiertem Content dehnt sich diese Problematik nun auch auf die Bereiche Video, Print und Software aus.

Gründe für die Entstehung der Digital Rights Problematik aus technischer Sicht
• Verlustfreie Kopierbarkeit digitaler Medien
• Leistungsfähige Kompressionsalgorithmen
• Breitbandige Kommunikationsnetzwerke
• Preiswerte Massendatenträger
• Leistungsfähige Hardwareausstattung
• Nutzerfreundliche Peer-to-Peer-Software

Tabelle 1: Gründe für die Entstehung der Digital Rights Problematik aus technischer Sicht, nach [o.V.06b]

Vor allem Faktoren wie die verlustfreie Kopierbarkeit, das Vorhandensein von leistungsfähigen Kompressionsalgorithmen, die leichte und kostengünstige Verfügbarkeit von Breitbandinternet tragen zur Entstehung dieser Problematik bei. Weiters kann auch die Verfügbarkeit von preiswerten Massendatenträgern angeführt werden. So können z.B.: USB-Sticks mit 2 GB, Festplatten über 400 GB etc. für unter 100 Euro erworben werden. CD- und DVD-Rohlinge kosten ebenfalls nur noch einen Bruchteil von dem, was sie noch vor einigen Jahren gekostet haben. [o.V.06a].

Die verlustfreie Kopierbarkeit ist in diesem Zusammenhang ein primäres Charakteristikum digitaler Medien.

Bei DRM werden Rechteverletzungen von vornherein verhindert, anstatt erst nachträglich verfolgt. *„DRM kann Rechtsicherheit und Klarheit schaffen und letztlich auch Interessen von Rechteinhabern und Nutzern ausgleichen ... DRM bietet auch Schutz vor Raubkopien, d.h. der Nutzer kann sich auf die Rechtmäßigkeit des Werkes verlassen, weil das Werk technisch dann entsprechend abgesichert ist“* [PiTh05, 134].

Digital Rights Management Systeme werden als Lösungsansatz für die Eindämmung von Urheberrechtsverletzungen diskutiert und auch schon in der Praxis eingesetzt. Doch wird es mit DRMS nicht gelingen, alle analogen Abspielgeräte durch digitale zu ersetzen. Deshalb wird stets die Möglichkeit bestehen, dieses analoge Signal abzugreifen und gegebenenfalls mit entsprechenden Filtern wieder zu digitalisieren. Damit wird DRMS niemals diese Problematik vollständig beseitigen können.

Der ursprüngliche Begriff Digital Rights Management (DRM) entstand erst vor wenigen Jahren, jedoch ist die Thematik bereits Anfang der neunziger Jahre aufgetreten. Der Begriff „Electronic Copyright Management“ [PiVä00], der dabei anfangs verwendet wurde, macht die Ursprünge im Urheberrecht deutlich. Die damaligen Lösungen scheiterten hauptsächlich an der mangelnden Akzeptanz der Benutzer, diese wurde durch die hohe Komplexität der Materie verursacht.

Häufig wird Digital Rights Management mit dem Begriff des Kopierschutzes gleichgestellt, was jedoch sachlich falsch ist. Beim Kopierschutz wird meistens der Datenträger vor unrechtmäßigem Zugriff geschützt und nicht der Inhalt wie beim Digitalen Rights Management.

7.2.1 Digitale Mauern

In diesem Zusammenhang geht es neben der gesellschaftlichen Akzeptanz von Urheberrechten besonders um den Schutz von Eigentum. Um diesen Zweck zu erfüllen, werden Mauern gebaut, Zäune gezogen, Alarmanlagen installiert und Tresore aufgestellt. Freilich können Softwareunternehmen bei ihren Produkten keine gewöhnlichen Mauern bauen, jedoch ähnlich wirkungsvolle Schutzmechanismen, beispielsweise in Form eines Digital Rights Management etablieren. Bei sehr vielen Softwareprodukten hat sich die Produktaktivierung bewährt, nicht weil mit dieser Lösung letztlich kein Missbrauch mehr möglich wäre, sondern weil damit das Grundprinzip der Limitierung des Zuganges erfolgreich integriert wird [Wöbk04, 10-11]. Die meisten Menschen sind nämlich nicht in der Lage, solche Schutzmaßnahmen zu umgehen. Jedoch ermöglicht der digitale Fortschritt die Defizite aus der Sichtweise des einzelnen Individuums zu kompensieren. Denn eine einzige Person, welche diesen Schutzmechanismus zu umgehen beherrscht, kann über das Medium Internet allen anderen dieses „Mehrwissen“ zu Verfügung stellen. Das Ergebnis dieser Herausforderung steht dann in Form von „Loadern“, „Cracks“, „Patches“, „Serials“ und „Keygens“ allen anderen Gruppen von Raubkopierern zum Herunterladen zur Verfügung

7.2.2 Anreiz für die Nutzer

In diesen Zusammenhang stellt sich die Frage, welchen Anreiz es für die Nutzer gibt, sich an der Rechteprüfung zu beteiligen. Technisch wird es nämlich immer Möglichkeiten geben, die Rechteprüfung zu umgehen. Ab dem Zeitpunkt, wo ein digitaler Content frei im Netz zur Verfügung steht, kann dieser auch frei weiterverteilt werden. Einmal entschlüsselt und im Netz verteilt, wäre ein freies Format nicht mehr rückverfolgbar. Zunächst sollte man das gemeinsame Interesse der Anbieter und ihrer Nutzer herausfinden. Dieses besteht interessanterweise in der Weitergabe der digitalen Ware. Erstens kann man jene Situationen identifizieren, in welchen die Anbieter die unentgeltliche Weitergabe von Waren wünschen. Das ist etwa in der Werbung der Fall. Zweitens kann man jene Situationen herausfinden, in welchen die Nutzer an der Bezahlung weitergegebener Waren Interesse haben. Das ist etwa der Fall, wenn Nutzer eine Provisionszahlung bekommen.

Das Ziel muss es daher sein, diese zwei Sichtweisen in einem gemeinsamen Verkaufsmodell zu vereinigen [Grim03, 103].

7.3 Definitionen

7.3.1 Definition Digital Rights Management (DRM)

Derzeit gibt es keine einheitliche Definition von Digital Right Management. Weder in der Wissenschaft noch in der Praxis konnte sich eine weitgehend einheitliche Definition des Digital Rights Management durchsetzen. Die Definitionen unterscheiden sich hinsichtlich ihres Anwendungszwecks, ihrer Funktion sowie ihres Umfangs. Es wurde bereits eingangs die Problematik der Analogkopie angesprochen, welche nochmals an dieser Stelle zur Veranschaulichung dienen kann. Wäre zum Beispiel eine Datei komplett digital verwaltet, beim Abspielen auf analoge Medienträgern aber nicht mehr, ist die Sinnhaftigkeit von DRM sehr stark eingeschränkt.

Eine sehr gute, theoretisch fundierte und zugleich vergleichsweise praxisnahe Definition formuliert Iannella:

„Digital Rights Management (DRM) involves the description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and

intangible assets – both in physical and digital form – including management of Rights Holders relationships.“ [Iann01]

Iannella beschreibt mit seiner Definition alle aus derzeitiger Sicht möglichen Aufgaben im DRM. Ausdrücklich wird betont, dass keine Beschränkung auf digitale Inhalte erfolgt. Weiters wird auch die Beziehung der beteiligten Personen (und Institution) berücksichtigt.

7.3.2 Definition Digital Rights Management Systeme (DRMS)

Versucht man, die Kernessenz des DRM auf DRMS zu übertragen, kann DRMS folgendermaßen definiert werden:

Digital Rights Management Systeme sind technische Lösungen zur sicheren zugangs- und nutzungskontrollierten Verteilung, Abrechnung und Verwaltung von digitalem und physischem Inhalten. [Frän03, 26]

Zentrales Ziel ist es, den Zugang und Nutzung in dem erwünschten Umfang so einfach wie möglich zu gewährleisten und gleichzeitig den unerwünschten Zugang und Nutzung zuverlässig zu verhindern.

Die einzelnen Elemente, aus denen DRMS bestehen, werden im Folgenden unter den Begriff Komponenten zusammengefasst. Dabei wird zwischen Funktionen und Technologien unterschieden.

Funktionen	Technologien
<ul style="list-style-type: none"> • Zugangskontrolle • Nutzungskontrolle • Abrechnung • Management Rechtsverletzungen <ul style="list-style-type: none"> - Integrität - Authentizität - Strafverfolgung • Weitere funktionale Anforderungen 	<ul style="list-style-type: none"> • Wasserzeichen (incl. Digitalen Fingerabdrücken) • Verschlüsselung (incl. Digitaler Signatur) • Rechtedefinitionssprachen • Weitere Technologien

Tabelle 2: Komponenten eines Digital Rights Management System, nach [o.V.06b]

7.3.3 Funktionen eines Digital Rights Management Systems

Die Kernfunktion eines DRMS ist, den Zugang und die Nutzung für einen digitalen Content entsprechend den Vorgaben des Rechteinhabers zu gewährleisten. Der digitale Inhalt muss dabei authentisch und integer sein, ebenso sollten die Nutzung abgerechnet werden können und Rechtsverletzungen verfolgbar sein.

7.3.3.1 Zugangskontrolle

Das Ziel einer Zugangskontrolle ist sicherzustellen, dass nur Berechtigte Zugang zu den digitalen Inhalten haben. Dies können Personen, Institutionen und Systeme sein. Die Berechtigung wird durch den Urheber festgelegt. Dabei handelt es sich um ein qualitatives Kriterium hinsichtlich des Benutzers und beantwortet die Frage nach dem „Wer“. Zugangskontrolle beinhaltet auch die Tatsache, Unberechtigten sicher den Zugang zu verweigern.

7.3.3.2 Nutzungskontrolle

Die Aufgabe der Nutzungskontrolle ist eine Kombination qualitativer (Nutzungsart, weitere Variable) und quantitativer (Nutzungshäufigkeit) Kriterien hinsichtlich der Inhaltsnutzung. Sie beantwortet die Frage nach dem „Wie“ der Nutzung. Der Begriff Kopierschutz wird sehr oft fälschlicherweise synonym für Nutzungskontrolle verwendet. Kopierschutz ist jedoch nur eine von vielen Möglichkeiten der Nutzungskontrolle [CEN03].

Das primäre Ziel von Nutzungskontrolle ist nicht Kopieren im Sinne eines Speicherschutzes zu verhindern, sondern Kopiervorgänge steuern zu können, also Kopierkontrolle.

7.3.3.3 Abrechnung

Es sollten, wenn die Möglichkeit besteht, alle Arten an Erlösformen unterstützt werden. Dabei müssen die DRMS grundsätzlich eine Offenheit gegenüber neuen Geschäftsmodellen aufweisen. Als Beispiel könnte pro Öffnungsvorgang eines Dokumentes ein bestimmter Betrag abgerechnet werden. Bei pauschalvergüteten

Abonnementmodellen wird anstatt der Abrechnung eines Betrages, das Vorhandensein eines Abonnements überprüft.

7.3.3.4 Management von Rechtsverletzungen

Rechtsverletzungen sollten bei DRMS weitestgehend verhindert und deren Folgen minimiert werden. Tritt trotz dieser Vorkehrungen eine Rechtsverletzung auf, so müssen DRMS diese eruieren können und eine Strafverfolgung unterstützen.

Weiters muss die Integrität sichergestellt werden, d.h. dass die digitalisierten Daten nicht von Unbefugten modifiziert werden können, sie also integer bleiben [PffK02, 13].

Es sollte auch die Zurechenbarkeit von Informationen zum jeweiligen Urheber gewährleistet sein, was man unter Sicherstellung der Authentizität beschreiben könnte.

DRMS sollen es ermöglichen, dass derjenige, der eine Urheberrechtsverletzung begeht, eindeutig und im juristischen Sinn zweifelsfrei ermittelt werden kann.

7.3.3.5 Weitere funktionale Anforderungen

Der Schutz der gesamten Wertkette muss gewährleistet sein. Ganz wesentlich ist es dabei, alle Verwertungsstufen des digitalen Content zu erfassen. Um eine möglichst hohe Marktpenetration zu erhalten, müssen DRM-Lösungen, insbesondere für den Endnutzer einfach zu bedienen sein. Weiters sollten DRM-Lösungen einen hohen Standardisierungsgrad aufweisen, d.h. dass sie Clients unterstützen, welche auf einer möglichst hohen Zahl verschiedenartiger Plattformen lauffähig sind und so auch eine möglichst breite Auswahl an Endgeräten unterstützen. DRMS müssen in der Lage sein verschiedenste Medientypen und Contentformate verarbeiten zu können.

7.3.4 Technologien eines Digital Rights Management Systems

Die einzelnen vorgestellten Funktionen werden mittels DRMS-Technologien realisiert. Sie bestehen aus mehreren eigenständigen Technologien, welche intelligent kombiniert werden, um das breite Funktionsspektrum abzudecken. Im Wesentlichen sind dies die beiden Technologien Wasserzeichen und Verschlüsselung einschließlich deren

Sonderformen sowie für die digitale Welt neu entwickelte Technologien Rechtsdefinitionssprachen und weitere Technologien.

7.3.4.1 Digitale Wasserzeichen

Das Einbringen von Wasserzeichen bedeutet, beliebige Informationen über ein mediales Werk in diesem selbst zu verbergen. Dies sind meistens Informationen über den Urheber, den Content selbst (Metadaten) oder auch über Nutzungsrechte. Das Ziel von Wasserzeichen im Zusammenhang mit DRMS ist es hauptsächlich, die Authentizität und die Integrität von digitalen Inhalten sicherzustellen [Ditt00, 13]. Wasserzeichen sind dabei untrennbar in das digitale Werk integriert und dadurch den gleichen Belastungen unterworfen wie das Werk selbst. Jedes derzeitige Verschlüsselungssystem kann einmal entschlüsselt werden. Wasserzeichen werden in diesen Zusammenhang benötigt, um zu erfahren, wer es getan hat.

Zu den Anforderungen an Wasserzeichen zählen Robustheit und Nicht-Wahrnehmbarkeit für Menschen und Maschine. Bei normaler Nutzung sollten Wasserzeichen Belastungen wie Verschlüsselung, Entschlüsselung, Kompression, Digital-Analog-Wandlung und Änderung des Dateiformates überstehen [CoMB02, 10]. Wasserzeichen müssen daneben auch „böartige“ Angriffe überstehen. Dazu gehören speziell Spatial Filtering, verlustbehaftete Kompression, Ausdrucken und Einscannen ebenso wie geometrische Störversuche wie Drehen und Skalieren, die auch dann erfolglos sein müssen, wenn die Algorithmen, welche dem Werk zugrunde liegen, bekannt sind [CoMB02, 30]. Derzeit ist es jedoch technisch noch nicht machbar, ein solches Wasserzeichen in ein digitales Werk einzubringen.

Die wichtigste Sonderform von Wasserzeichen stellen digitale Fingerabdrücke dar, in welchen Informationen über den Käufer in den Originalinhalt mittels Wasserzeichen integriert werden, um Rechtsverletzungen nachvollziehbar zu machen.

7.3.4.2 Verschlüsselung

Um digitale Inhalte nutzen zu können, muss der Content die geschützte Umgebung des Contentanbieters verlassen. Dabei entsteht die Gefahr, dass die digitalen Daten Unberechtigten in die Hände fallen. An dieser Stelle setzt die Verschlüsselung an, die

Unberechtigten den Zugang verwehren und unerlaubte Nutzung verhindern soll. Die digitalen Daten werden hierfür mit einem Key verschlüsselt und danach verschickt. Vor der Nutzung muss der Endnutzer die digitalen Daten mittels eines Keys wieder entschlüsseln, um sie nutzen zu können. Die Verschlüsselung kann mittels Software oder Hardware durchgeführt werden. Ein hoher Sicherheitsgrad für DRMS kann dadurch erreicht werden, dass die Systeme später auf andere Verschlüsselungsverfahren und Schlüssellängen umgestellt werden können [Smit98, 69].

Fachleute können heutzutage selbst gelöschte Bits wieder lesbar machen. Dazu analysieren sie die Festplatten oder andere Speichermedien in staubfreien Räumen mit besonders empfindlichen Messinstrumenten, welche selbst geringste Restspuren einer vorherigen Magnetisierung erkennen können. Bei sensiblen Daten sollte daher der kritische Festplattenteil oder die gesamte Festplatte verschlüsselt werden.

Natürlich kann auch die beste Verschlüsselung nicht verhindern, dass zum Beispiel ein Premiere-Kunde einen Film auf Video aufnimmt. Dies zeigt einmal mehr, dass es im digitalen Rechtemanagement keine perfekten Lösungen gibt. So verwundert es auch nicht, dass es bereits zahlreiche Lösungen gegeben hat, welche geknackt worden sind. Das bekannteste Beispiel ist die Software „Acrobat Reader“ der Firma Adobe. Nähere Details über Verschlüsselung finden sie in Kapitel 3.5.1.

7.3.4.3 Rechtedefinitionssprachen

Unter Rechtedefinitionssprachen wird die Art und der Umfang der Rechte verstanden, die den einzelnen Nutzer eingeräumt werden. Das können verschiedene Zugangs- und Nutzungsrechte wie auch spezifische Abrechnungsinformationen über die digitalen Daten sein. Es kann zum Beispiel ein Dokument nur unter einem bestimmten Betriebssystem geöffnet werden oder jede Seite, welche ausgedruckt wird, kostet 20 Cent.

Durch festgelegte Attribute wird eine sehr genaue Steuerung der Nutzungsrechte gewährleistet, sehr viel exakter als das bei analogen Medien der Fall ist. Die einzelnen Attribute legen beispielsweise fest, wie oft oder an welchen Tagen eine bestimmte Datei geöffnet werden kann.

Die Rechteinformation kann dabei entweder mittels Wasserzeichen im Content selbst oder separat abgespeichert werden. Ein sehr wichtiges Kriterium ist dabei, dass alle

denkbaren Rechtsformen und Abrechnungsmodifikationen in der Rechtedefinitionssprache abgebildet werden können.

7.4 Funktion-Technologie-Matrix

Die folgende Tabelle fasst die einzelnen Technologien und Funktionen in einer Matrix zusammen und zeigt, wie gut welche Funktionen durch welche Technologien geleistet werden können.

Digital Right Management Systeme				
	Zugangskontrolle	Nutzungskontrolle	Mgmt. von Rechtsverletzungen	Abrechnung
Digitale Wasserzeichen	bedingt	bedingt	sehr gut	-
Digitale Fingerabdrücke	bedingt	bedingt	sehr gut, Primärzweck	bedingt – gut
Verschlüsselung	sehr gut, Primärzweck	sehr gut, Sekundärzweck	gut – sehr gut	bedingt – gut
Rechtedefinitionssprachen	sehr gut	sehr gut	kaum	sehr gut, Primärzweck

Tabelle 3: Funktionen-Technologien-Matrix eines DRMS, nach [o.V.06b]

Wenn ein vollständiges DRMS erstellt wird, müssen die einzelnen Technologien sinnvoll kombiniert werden, um ihrem jeweiligen Einsatzzweck zu entsprechen.

7.5 Das Problem der Standardisierung

Die Formulierung, Verteilung und Durchsetzung von Rechten erfordert eine Standardisierung. Um jedoch von einer globalen Standardisierung sprechen zu können, erfordert es eine weltweite Kooperation so unterschiedlicher und zum Teil untereinander konkurrierender Institutionen wie Autoren/Komponisten und ihrer Interessensverbände (GEMA), Inhaltsanbieter (Filmverleihe, Musikverlage, Buchverlage, Spieleverlage usw.), Betriebssystem- und Gerätehersteller, Konsumgeräteindustrie, Netzbetreiber sowie der mächtigen Verbraucherverbände. Diese Standardisierungsversuche sind jedoch bisher gescheitert. Dabei muss nicht jedes Detail standardisiert sein. Endgeräte, Rechteinterpret, ja sogar digitale Wasserzeichen

können getrost einzigartig sein. Aber Kommunikationsprotokolle, Dateiformate, Metadaten (etwa über Rechte) und Sicherungskomponenten wie Signaturen und Verschlüsselung müssen überregional und anwendungsübergreifend standardisiert sein [Gloc05, 86-88].

Gleichzeitig hinkt die Nutzungsfreundlichkeit DRM-geschützter Inhalte aber auch dem „Free Content“, d.h. dem im Internet kostenfrei verfügbaren Inhalten hinterher. Jeder, welcher sich schon einmal die Mühe gemacht hat, solchen „Free Content“ zu beziehen, wird festgestellt haben, dass dies technisch ganz problemlos ist. Egal auf welcher technischen Plattform man agiert, egal an welchem Ort man sich befindet – der Bezug, der meist illegal ins Netz gestellten Medieninhalte klappt vorzüglich. Ganz anders stellt sich dies dar, wenn man versucht, ein DRM-geschütztes Medienprodukt zu beziehen. Oftmals wird man hier an einer Firewall scheitern, an der Inkompatibilität des Betriebssystems oder des Internet Browsers. Es gibt eine Fülle technischer Probleme, welche DRM-geschützte Medienprodukte heute zu einer echten technischen Herausforderung für den Enduser machen.

Die klassische DRM-Technik erfordert immer die Durchsetzung der Rechte in den Endgeräten. Sie richtet sich also gegen ihre eigenen Nutzer. Damit wird eine alte Regel der IT-Sicherheit verletzt: jener Partner, welcher gegenüber dem anderen ein Interesse an einer Sache hat, muss auch die Mittel an ihrer Durchsetzung in der Hand halten. Beim klassischen DRM ist es jedoch umgekehrt: die Mittel zur Durchsetzung der Rechte der Anbieter liegen in der Hand der Nutzer, daher darf man sich nicht wundern, wenn sie dort ausgehebelt werden. Bald wird es jedoch Modelle geben, welche dieses Problem beseitigen. Das klassische DRM mit seinem Kopierschutz wird nicht aussterben, aber seine dominante Rolle einbüßen. Die unsinnige Kriminalisierung der Internetnutzer muss ein Ende haben. Das Ziel muss es sein, dass es sich für den einzelnen Nutzer lohnt, für digitale Waren zu bezahlen, weil man etwas Wertvolles dafür erhält.

7.6 Wirtschaftliche Aspekte des DRM

Laut der Studie „Datenschutzverträgliches und nutzungsfreundliches Digital Right Management – Privacy4DRM“ nutzen heutzutage Digital-Right-Management Systeme

die wirtschaftlichen Potentiale nur zu einem sehr geringen Teil. Die Hauptgründe sieht die Studie darin, dass die Systeme wechselseitig inkompatibel sind, umfassend Benutzerdaten generiert werden und insgesamt keinen angemessenen Kundennutzen darstellen [Schu05, 1].

Die Bedingungen, welche die Zahlungsbereitschaft fördern, sind für die Nutzer sehr unattraktiv: *„Die vorhanden DRM-Mechanismen sind unhandlich, intransparent, bedrohlich und isolieren die legalen Kunden auf zersplitterten Marktinseln“* fasst die Studie *„Datenschutzverträgliches und nutzungsfreundliches Digital Right Management – Privacy4DRM“* zusammen [Schu05, 1].

Die Brennerstudie 2006, welche von der International Federation of Phonographic Industry (IFPI), einer hartnäckigen Verfechterin von DRM, erstellt wurde, kam zu dem Ergebnis, dass von den 512 Millionen Musikdownloads im Jahr 2005 nur 24 Prozent legal waren. Auch Apples Online Shop iTunes nimmt die Studie genauer ins Visier und stellte dabei fest, dass das reine Downloadgeschäft von iTunes kaum zum Gewinn beiträgt, denn Apple meldet die Umsatzzahlen von iTunes nur in Verbindung mit den Verkäufen des iPod.

7.7 Zusammenfassung

„Statt mit stark eingeschränkten Nutzungsrechten verbundene Musiktitel im Internet zu kaufen, ziehen die Konsumenten es vor, sich die Dateien weiterhin kostenlos und frei von technischen Restriktionen im Internet zu beschaffen“ [WaHe03, 543]

Wie kompliziert und auch nicht unumstritten DRM sein kann, sei am Beispiel des TCG-Ansatzes angedeutet, der Ansatz der Trusted Computing Group, der Unternehmen angehören, wie zum Beispiel Microsoft, Intel, HP, Compac, IBM um nur einige zu nennen. Dieser Ansatz zielt darauf ab, eine spezifische Hardware-Software-Kombination zu installieren und als Quasi Standard im Bereich der Rechnertechnik zu verbreiten. Dadurch dass es eine Kombination aus Hard- und Software ist, besteht eine viel geringere Möglichkeit einer Manipulation von außen. Deshalb ist auch eine höhere Sicherheit für den Nutzer gewährleistet. Jedoch verliert durch eine solche Umsetzung in die Praxis der Nutzer die Kontrolle über seinen Rechner, weil er nicht mehr selbst bestimmen kann, welche Art von Software er im Einzelnen laufen lässt [Pico05, 5].

Dass legale Distributionen von Musikinhalten es so schwer haben, sich am Markt zu etablieren, liegt zum Teil daran, dass die legal betriebenen Plattformen nur einen Bruchteil des Repertoires anbieten, das bei nicht legalen Quellen zu finden ist. Zudem sind die Nutzungsrechte der legal erworbenen Musik meist stark eingeschränkt. So ist es oft nicht erlaubt, die Musikdateien beliebig oft auf CD zu brennen oder auf andere Medien zu speichern. So sehr jedoch der Umstand der Datenpiraterie aus der Sicht der Rechteinhaber zu beklagen ist, so zeigt er doch auch die enorme Nachfrage der Konsumenten nach solchen digitalen Produkten. Der bereits vor Jahren angekündigte Siegeszug der Breitbandnetze ist nun Wirklichkeit geworden. Mit Übertragungsraten im Mbit/Sekunde Bereich ist das Tauschen von Musikdateien und Filmdateien kein technisches Problem mehr. Digitale Mehrfachverwertung nimmt in allen Medienkategorien zu, allerdings in unterschiedlicher Geschwindigkeit. Die digitale Nutzung ist heutzutage technisch möglich, vom Kunden erwünscht und lässt sich daher nicht mehr aufhalten. Medienunternehmen müssen daher auf die Wünsche der Kunden mit neuen Geschäftsmodellen eingehen und digitale Produkte mit entsprechender Rechtesicherung anbieten. Die meisten Menschen werden sich an ein DRMS halten und werden eher den Nutzen erkennen, als zu versuchen, es zu umgehen.

“Mass market acceptance of DRM will only happen when ease of use equals current practices” [Luij, 74]. Die DRM Systeme der Zukunft müssen daher nicht gegen die Nutzer, sondern auf den Nutzer und seine Interessen zugeschnitten werden.

„Consumers want to enjoy their content anywhere, anytime, with the device of their choice“[Luij, 67]. DRMS können daher keinesfalls die Lösung für das Problem der Medienindustrie sein, sondern können nur einen Baustein in einem Gesamtkonzept darstellen.

Wichtig sind in diesem Zusammenhang auch die Überlegungen der World Intellectual Property Organization (WIPO) zur Einführung eines weltweiten Identifizierungscodes. Mit Hilfe eines solchen Codes wäre es möglich, jedes digitale Werk sofort zu erkennen und gegen die Übernahme des Werkes vorzugehen. Besonders viel versprechend sind in diesem Zusammenhang digitale Wasserzeichen, welche das Werk untrennbar mit einem Urheber- und Lizenzierungshinweis verknüpfen und auch das Auffinden von Werken im Internet über Suchmaschinen ermöglichen können. Welche Lösungen sich jedoch letztlich durchsetzen werden, bleibt vorerst abzuwarten.

Der auf Musik-CDs enthaltene Kopierschutz zum Beispiel verärgert viele Kunden, weil sich diese „Fast-CDs“ in PC-Laufwerken, einigen Autoradios und CD-Playern nicht

abspielen lassen. Hinweise auf den entsprechenden CDs, welche den festgelegten Industrie-Standard der Audio-CD („Redbook“) nicht mehr erfüllen, fehlen. Die Rückgabe der digital geschützten CDs ist oft von der Kulanz des Verkäufers abhängig. Das Hauptziel muss es daher sein, dass geschützte digitale Inhalte, welche dem Endkunden zur Verfügung gestellt werden, genau so genutzt werden können wie die klassische Audio CD heute. Dies betrifft jedoch nicht die Nutzungsszenarien, welche P2P Netzwerke und illegale Nutzung anbelangen. Jedoch alle Szenarien, welche der Kunde gewohnt ist, müssen auch in der „Digital Rights Welt“ abgebildet werden können [Gloc05, 75].

8 Wirtschaftliche, ökonomische und soziologische Betrachtungsweisen des Filesharings

Es gibt drei Bereiche, in denen man gegen Tauschbörsen und ihre Nutzer vorgehen kann:

- **rechtliche Schritte** gegen Betreiber und Nutzer von Tauschbörsen;
- **ökonomische Schritte** wie zum Beispiel die Nutzung des Internets als weiteren Absatzkanal für Musik oder der Aufkauf illegaler Tauschbörsen und
- **technische Schritte** in Form von Digital Rights Management Systemen oder dem Einschleusen von fehlerhaften Dateien in die Tauschbörse. [Hess04, 112-115]

8.1 Das ökonomische Problem virtueller Waren

Das Hauptproblem virtueller Waren kann man an einem allgemeinen Lebenszyklus von Waren darstellen, welcher beim Menschen beginnt und endet. Der Anfang und das Ende des Lebensweges liegt subjektiv im menschlichen Kopf: er beginnt mit der Erfindung einer schöpferischen Kreation und endet im Genuss des Konsums. Dazwischen liegt der Weg über Produktion, Reproduktion, Verteilung und Wiedergabe: das sind Prozesse, welche technisch unterstützt werden und die im Falle digitaler Waren überwiegend computer- und internetgesteuert stattfinden. Bei virtuellen Waren gibt es jedoch eine Besonderheit: Unter virtuellen Waren versteht man solche Waren, welche sich leicht und ohne wesentlichen Qualitätsverlust kopieren und weitergeben lassen, wie das etwa bei digitalisierter Musik der Fall ist. Für diese gibt es eine drastische Kostenreduktion im mittleren Teil: bei der Reproduktion, bei der Wiederherstellung und der weiteren Verteilung. Denn Bits und Bytes lassen sich im Computer mit nur wenigen Maus-Klicks kopieren, vervielfältigen und im Internet weiterverteilen. Das ist das wesentliche Merkmal einer virtuellen Ware, denn wenn sie einmal digitalisiert ist, lässt sie sich ohne Qualitätsverlust reproduzieren und verteilen [Vari00; VaSa98].

8.2 Ökonomische Aspekte des Filesharings

8.2.1 Filesharing und CD oder DVD-Brennen als Ursache für die rückläufigen Umsätze

Die Gründe für den Rückgang der Verkaufszahlen sieht die Musikindustrie vor allem im zunehmenden so genannten privaten „Brennen“ von Musikstücken. Dabei werden Audiodaten mithilfe eines CD oder DVD Brenners, welcher im Computerhandel schon ab ca. 25 Euro erhältlich ist, auf einen entsprechenden Rohling übertragen, im üblichen Sprachgebrauch „gebrannt“. Die Herkunft der einzelnen Audiodaten ist dabei grundsätzlich nicht von Relevanz. Es ist mittels entsprechender Software möglich, komplette (Original-) Audio-CDs oder auch nur einzelne Musikstücke von diesen zu vervielfältigen; ebenso können über Filesharingbörsen oder einschlägige Webseiten heruntergeladene MP3-Dateien auf CD oder DVD Rohlinge gebrannt werden. MP3 Dateien lassen sich dabei vor dem eigentlichen Brennvorgang, dem Vervielfältigen, in das WAV- Format zurückübertragen, welches auch von herkömmlichen CD-Spielern gelesen werden kann. Heutige CD und DVD-Player können jedoch meistens bereits MP3-Dateien direkt abspielen, was dazu führt, dass eine digitale Umwandlung in ein anderes Format überflüssig ist.

Nach einer GfK-Studie im Auftrag der Deutschen Phonoverbände wurden 10.000 Personen im Rahmen Ihres Konsumentenpanels zu ihrem Brenn-/ Downloadverhalten befragt. Diese Stichprobe ist repräsentativ für 64 Mio. Deutsche ab dem 10 Lebensjahr. Diese Zahlen lassen erkennen, dass aus juristischer Sicht die Zahl von 439 Millionen musikbespielter Rohlingen nicht gleich mit den 315,3 Millionen Raubkopien in Zusammenhang gebracht werden kann. Ein Großteil der Überspielungen dürfte vielmehr von der Regelung des § 53 Abs. 1 UrhG, welche die Vervielfältigung zum privaten Gebrauch gestattet, gedeckt sein.

Dabei wird nicht nur die Vervielfältigung für den eigenen Gebrauch gestattet, sondern in gewissem Umfang auch Vervielfältigungen für Personen, welche mit dem Vervielfältigenden durch ein persönliches Band verbunden sind.

Aus der Sicht der Musikindustrie ist Filesharing zunächst einmal ein Multiplikator für das Brennen von Audio-CDs, weil es dem Kopierenden weiteres digitales Material verschafft, an das er womöglich nicht so einfach herangekommen wäre. Gleichzeitig unterstellt die Musikindustrie, dass durch das Filesharing der Absatz von Audio-CDs

insgesamt kontinuierlich vermindert wird, weil der potentielle Käufer von Musik CDs sein Interesse zunehmend nicht mehr mit Musik CDs aus dem Plattengeschäft, sondern anderweitig befriedigt.

Außer den freien Tauschbörsen führen nach Einschätzung der Musikindustrie auch illegale Kopien physischer Tonträger zu erheblichen Umsatzeinbußen. [BUPW04, 8-12]. Entsprechend intensiv sind die Bemühungen der Phonobranche, Maßnahmen gegen die unberechtigte Weitergabe von Musik und zum Schutz der Urheberrechte zu entwickeln. Hierzu gehört insbesondere der Einbau von Kopierschutzmechanismen. Doch selbst auf herkömmlichen Wiedergabegeräten gibt es immer wieder Probleme mit der Abspielbarkeit. Aus diesem Grund werden kopiergeschützte Tonträger geringwertiger eingestuft als solche, bei denen auf derartige Maßnahmen verzichtet wird.

Der Wunsch der Konsumenten ist jedoch eine uneingeschränkte Weiterverwendbarkeit gekaufter Musiktitel, insbesondere hinsichtlich des Brennens auf CD.

Eine weitere Maßnahme der Musikindustrie besteht in der juristischen Verfolgung von Betreibern und Anwendern freier Tauschbörsen. Hinsichtlich der Wirksamkeit solcher Schritte gibt es unterschiedliche Einschätzungen. Eine Umfrage des Pew Internet Projects unter 1.300 amerikanischen Online-Anwendern ergab, dass 14% jener Nutzer, die schon einmal Musik über eine freie Tauschbörse bezogen haben, dies zukünftig unterlassen wollen [RaMa04, 1]. Aus Angst vor juristischer Verfolgung erklären aber immerhin 60% der Befragten, die noch nie eine Tauschbörse benutzt haben, dies auch in Zukunft nicht zu tun [RaMa04, 2]. Insofern könnte die Androhung rechtlicher Schritte zumindest im Hinblick auf diese potenzielle Kundengruppe eine wirkungsvolle Maßnahme sein. Wie sich jedoch die juristischen Schritte in den Nutzerzahlen freier Tauschbörsen bisher niedergeschlagen haben, muss in diesen Zusammenhang ebenfalls beachtet werden. Zwar ist im Erhebungszeitraum der Studie zwischen Februar und März 2004 die Anzahl der Nutzer der populären Tauschbörse KaZaA gesunken [RaMa04, 3]; alternative Angebote, wie BitTorrent, iMesh oder eMule, verzeichneten allerdings gleichzeitig Zuwachsraten [RaMa04, 4].

Darüber hinaus ist bei der Diskussion der Wirksamkeit einer juristischen Verfolgung von Tauschbörsennutzern zu berücksichtigen, dass Filesharingprogramme zunehmend mit Anonymisierungsfunktionen ausgerüstet werden. Vermutlich glaubt auch aus diesem Grund eine große Mehrheit der Befragten (84,5%), dass eine strafrechtliche Verfolgung die zukünftige Existenz von freien Tauschbörsen nicht verhindern wird.

In diesem Kontext sollte auch noch eine Harvard-Studie aus dem März 2004 Beachtung finden, welche zu dem Ergebnis kommt, dass der Schaden, welcher durch derartige Tauschbörsen entstanden ist, gegen Null tendiert. [ObSt04]

8.2.2 Andere Ursachen für den Umsatzrückgang

Die Hauptgründe für den Rückgang der Umsätze in der Musikindustrie sind weltweit die gleichen: „*Starke Substitution legaler Verkäufe durch nicht autorisiertes CD-Brennen, starker Wettbewerb um die knapper werdenden Freizeitbudgets sowie generell unsichere wirtschaftliche Rahmenbedingungen*“ [Jaco05, 24].

Dass jedoch das Filesharing und das Brennen von Rohlingen alleinige oder zumindest Hauptursache des beklagten Umsatzrückgangs sind, erscheint allerdings anzweifelbar. Zum einen scheinen die Probleme der Musikindustrie zumindest teilweise hausgemacht zu sein, da sie nicht auf die Wandlung der Bedürfnisse der Kunden eingegangen ist; zum anderen müssen die Umsatzeinbrüche beim Absatz von CDs und DVDs im Gesamtzusammenhang mit den Ausgaben für andere Medienformen gesehen werden. Eine detaillierte wirtschaftliche Analyse des Filesharings kann die vorliegende Arbeit nicht leisten. Hinzuweisen ist jedoch auf folgende Faktoren:

1.) Die GfK-„Brennerstudie“ 2006 zeigt, dass die Medienausgaben in der Gruppe der „Brenner/Downloader“ insgesamt konstant geblieben sind. Erkennbar ist dabei ein Trend hin zu neueren, derzeit noch recht teuren Medien wie der HD-DVD und Blu-ray Disk. Der Umsatzrückgang bei der CD ist also zumindest teilweise auf eine höhere Konkurrenz durch andere Unterhaltungsmedien zurückzuführen; insoweit ist eher von einer Umsatzverlagerung zu sprechen.

2.) Umsatzrückgänge bei den CD- und DVD- Verkäufen werden zunehmend auch als Resultat einer verfehlten Geschäftspolitik der großen Plattenfirmen gedeutet. Diese setzen trotz zunehmender Individualisierung von Musiktrends nach wie vor auf wenige Superstars (deren Veröffentlichung nur bescheidene Erfolge erzielten) oder Schnellschussprojekte von künstlerisch zweifelhafter Qualität („Deutschland sucht den Superstar“ oder „Starmania“) statt auf eine ernsthafte Nachwuchsförderung und den gezielten Aufbau junger Talente [Witt00, 161]. Dies rächt sich nun in sinkenden Absatzzahlen. Beklagt werden auch überteuerte Preise bei Audio-CDs, die dazu beitragen, dass immer weniger Konsumenten sich Original Audio-CDs leisten wollen.

3.) Die Phonoindustrie hat den Absatzmarkt Internet zu lange unterschätzt und es verabsäumt, durch ein eigenes Online-Angebot von Musik potentielle Käuferschichten an sich zu binden [Witt00, 143]. Diese müssen nun mühsam von den kostenlosen Tauschbörsen zurückgewonnen werden. Die nun angebotene Musik von Online-Portalen kostet momentan trotz relativ weniger verfügbarer Stücke verhältnismäßig viel und erlaubt die Nutzung der Musik zumeist nur in eingeschränktem Umfang. (näheres über DRM siehe Kapitel 7).

Bewegung kam allerdings durch die Computerfirma Apple in den Markt. Deren in April 2003 vorgestelltes Bezahlangebot iTunes, bei dem Apple-Nutzer Songs aller großen Major-Plattenfirmen für 99 Cent pro Stück herunterladen können, wurde wider Erwarten gut angenommen [Dern03]. Die Bereitschaft für den Download von Musik aus dem Internet zu bezahlen, scheint daher durchaus vorhanden zu sein.

Die Situation bei Filmen stellt sich vergleichbar dar. Während über Filesharingtauschbörsen neueste „Blockbuster“ aus Hollywood noch vor der offiziellen Veröffentlichung zu bekommen sind, stoßen kommerzielle Anbieter von downloadbaren Filmen (sog. „Online-Videotheken“) bislang auf wenig Interesse. Schuld daran dürfte das magere Angebot von Filmen und deren restriktiven Abspielkonditionen sein.

4.) Nach einer Untersuchung von Forrester Research seien Tauschbörsen nicht Schuld an der Krise der Musikindustrie. Ursachen hierfür seien eher die allgemein schlechte wirtschaftliche Lage der letzten Jahre sowie die aufkommende Konkurrenz durch Video-Spiele und DVDs. Nach Nielsen/Netratings seien sogar Tauschbörsenbesucher „eifrige CD-Käufer“ [Heis02a].

Es ist ebenfalls nicht gerechtfertigt, eine bestimmte Zahl von privaten digitalen Vervielfältigungen auf der Sekundärebene ohne weiteres mit einem entsprechenden Verlust auf dem Primärmarkt gleichzustellen. So werden zum Beispiel die wirtschaftlichen Interessen eines Komponisten nicht dadurch beeinträchtigt, dass ein Sammler von einer eigenen Original-Audio CD ein Duplikat für den privaten Gebrauch im Auto herstellen darf.

Eine tatsächliche Beeinträchtigung des Primärmarktes können damit nur solche privaten Vervielfältigungen bewirken, welche eine alternative Nutzungsmöglichkeit parallel zur Nutzung des Originals schaffen, die also geeignet sind, das Original zu ersetzen. Dies liegt beispielsweise immer dann nahe, wenn Kopiervorlage und Vervielfältigungsstück von verschiedenen Personen, obgleich privilegierten Personen getrennt voneinander

benutzt werden. Jedoch fehlt auch in diesen Fällen der Nachweis, dass das Vervielfältigungsstück das Original auch wirtschaftlich substituiert. Von der Musikindustrie wird dies ohne weiteres angenommen und teilweise sogar auch in der juristischen Literatur vorausgesetzt. Ein solcher Zusammenhang ist zwar nicht ganz fern liegend. Dass die digitale Privatkopie jedoch für den sinkenden Absatz der Musikindustrie auch tatsächlich eine entscheidende Beeinträchtigung darstellt und dem Urheber signifikante wirtschaftliche Vorteile entzieht, konnte bisher in dieser Konsequenz noch nicht festgestellt werden. Unterschiedliche Studien hierzu kommen zu unterschiedlichen Ergebnissen.

Weiters muss bei der privaten Vervielfältigung als sekundäre Nutzungsform von einer primären Verwertung des Werkes und hierdurch erzielte Einnahmen unterschieden werden muss. Es ist dabei auch zu berücksichtigen, dass die private Vervielfältigung derzeit nicht effektiv genug kontrolliert werden kann und wirkungsvolle Kopierschutzmechanismen oder Systeme zur digitalen Rechteverwaltung nicht auf dem Markt sind.

Es lässt sich daher festhalten, dass die Umsatzeinbußen der Musikindustrie in den vergangenen Jahren nicht ohne weiteres und nicht ausschließlich auf das Aufkommen von Filesharingbörsen im Internet zurückgeführt werden können. Jene sind allenfalls ein Faktor von vielen, welche es in den letzten Jahren gegeben hat.

8.2.3 Reaktionen und Maßnahmen der Musikindustrie

„...the record labels and publishing companies do not own the rights to music from the most popular artists, it might be difficult to provide a library nearly as complete as the current free system.“ [BKKM03, 53].

Die Musikbranche sieht sich durch Online-Tauschbörsen auf Basis so genannter Peer-to-Peer Systeme fundamental bedroht. Dem Computerhersteller Apple Inc. ist es nun gelungen, mit dem iTunes Music Store das erste erfolgreiche kommerzielle Onlineangebot für digitale Musikdateien zu etablieren. Erstmals finden sich liberale DRMS, wobei die Integration von Peer-to-Peer-Elementen hervorzuheben ist. Der technologische Mittelweg ist Ausdruck eines strategischen Kalküls. Apple integriert die Bedürfnisse der Musikverlage nach monetärer Kompensation mit den neuen Ansprüchen der Kunden auf freizügigere Nutzungsbedingungen zu einer innovativen

Dienstleistung. Ökonomisch betrachtet muss die bislang nahe liegende Vermutung, dass die Zahlungsbereitschaft für Musik im Internet gegen Null tendiert, relativiert werden. Der Erfolg des Musicstores legt vielmehr nahe, dass die Zahlungsbereitschaft zielgruppenspezifisch variiert. Die Konsumenten signalisieren durch die Akzeptanz des Apple-Modells, dass sie im Ausgleich für die Berücksichtigung ihrer Wünsche (Tausch und Kopieren von Dateien) auch bereit sind, die Bedürfnisse der Musikbranche (Durchsetzung der Property-Rights) zu respektieren. Weiters lässt das Modell erkennen, dass das Internetpublikum innovative Dienstleistungen nicht nur gerne nutzt, sondern auch bereit ist, dafür einen als angemessen empfundenen Preis zu bezahlen. Die Musikindustrie muss sich jedoch wahrscheinlich daran gewöhnen, dass sich zukünftig ihr Erlösmodell online wie offline viel mehr an dem von den Nutzern empfundenen Werten zu orientieren haben wird.

Die Musikverlage versuchen nun seit geraumer Zeit selbst, das Internet als weiteren Absatzkanal für Musik zu nutzen, wobei die meisten Angebote mit strikten Digital-Rights-Management-Systemen verbunden werden. Daneben gibt es Bestrebungen, die Attraktivität von klassischen Musik-CDs zu erhöhen (z.B. durch aufwändige Booklets) oder vermehrt Konzerttourneen als Einnahmequelle zu erschließen [DrHa03, 19-20].

Laut einer empirischen Studie mit 2.260 Teilnehmern, welche über das Internet durchgeführt wurde, kam man zum Ergebnis, dass weder der Einbau von Kopierschutzmechanismen noch die juristische Verfolgung von Tauschbörsennutzern wirksame Mittel sind, um den Verkauf von Tonträgern und Online-Musik zu steigern. Weiters fand sie heraus, dass eine Preissenkung bei Musikdownloads zu einer Umsatzerhöhung und damit zu einem Vorteil für Anbieter und Konsumenten führen könnte, da sich die derzeitige Zahlungsbereitschaft potenzieller Käufer von Onlinemusik deutlich unter den Preisen aktiver Downloadshops befindet [BPJS05, 118].

8.3 Rechtliche Schutzmöglichkeiten

„Der Tausch von Musik über Filesharing-Netzwerke ist die größte Massenstraftat, die es je in Deutschland gegeben hat.“ [Solm06, 3]

In letzter Zeit häufen sich die Fälle, in denen österreichische User von Tauschbörsen seitens der Verwertungsgesellschaften wegen Eingriffen in Urheberrechte

Abmahnungen bekommen. Darin wird ein pauschaler Schadenersatz von rund 3.000 Euro und mehr gefordert.

„Sowohl im Strafverfahren als auch in den darauf folgenden Zivilverfahren muss die Uploadmöglichkeit positiv nachgewiesen werden. Der Täter muss einwandfrei identifiziert werden. Allein die IP-Adresse verrät nur den Anschlussinhaber. In Familien nutzen meist mehrere Menschen gleichzeitig einen Rechner. Wohngemeinschaften nutzen oft einen gemeinsamen Internetanschluss, W-LAN Anschlüsse können leicht manipuliert werden.“ [Solm06, 3]

Um die derzeitige Rechtslage verstehen zu können, muss zwischen zwei Vorgängen unterschieden werden. Erstens dem Herunterladen von digitalisierten Werken („Download“) und zweitens dem Bereithalten von digitalisierten Werken zur weiteren Verbreitung im Internet an andere User („Upload“). Grundsätzlich ist der Vorgang des Downloadens zum eigenen Gebrauch (Privatkopie) nicht strafbar. Ob der alleinige „Download“ zulässig ist, hängt jedoch zum einen davon ab, ob es sich überhaupt um ein urheberrechtlich geschütztes Werk handelt und allenfalls, welche Rechte die Quelle an dem Werk hat. Dagegen ist das Bereitstellen zum „Upload“ jedenfalls strafbar und auch zivilrechtlich verboten. [HOrf06]. *„Allein das Vorhandensein der Daten auf der Festplatte und die Möglichkeit, von außen auf die Festplatte „blicken“ zu können, heißt aber noch nicht, dass in diesen Fällen auch ein Upload möglich ist.“ [Solm06, 2-3]*

Das Werk als geistiges Eigentum ist eine anerkannte Rechtsposition. Das Urheberrecht kennt sowohl zivilrechtliche als auch strafrechtliche Maßnahmen, welche sich gegen eine Verletzung der absoluten Urheberpersönlichkeitsrechte und der ausschließlichen Verwertungsrechte richten.

8.3.1 Zivilrechtliche Ansprüche in Österreich

Die zivilrechtlichen Sanktionen des Urheberrechts dienen der Abwehr bestehender und drohender Urheberrechtsverletzungen und der Wiedergutmachung des durch Verletzungen erlittenen Schadens. Anspruchsinhaber ist grundsätzlich der Urheber. Neben den ausdrücklich im Urheberrechtsgesetz geregelten Ansprüchen kommen auch die allgemeinen zivilrechtlichen Vorschriften des ABGB in Betracht.

8.3.1.1 Unterlassungsansprüche

Eine drohende künftige fortgesetzte, erneute oder erstmalige Verletzung in einem urheberrechtlichen Ausschließlichkeitsrecht oder auch Urheberpersönlichkeitsrecht berechtigt zu einer Unterlassungsklage nach §81 UrhG [Cire97, 193]. Die Verletzungshandlung muss lediglich widerrechtlich, nicht jedoch verschuldet sein. Häufigster Anwendungsfall ist das Bestehen einer Wiederholungsgefahr nach bereits erfolgter Verletzung.

8.3.1.2 Beseitigungsansprüche

Besteht ein widerrechtlicher noch fortbestehender Zustand, der durch einen rechtswidrigen Eingriff verursacht wurde, kann der Berechtigte die Beseitigung nach §82 UrhG verlangen [Cire97, 196]. Der Anspruch kann nach Wahl des Verletzten in Form der Zustandsbeseitigung und bei körperlichen Vervielfältigungsstücken auch in Form der Vernichtung oder Überlassung an den Berechtigten erfolgen. Der Beseitigungsanspruch richtet sich nach österreichischem Recht grundsätzlich gegen den Eigentümer der beeinträchtigenden Sache siehe §82 Abs. 6 UrhG.

8.3.1.3 Schadenersatzansprüche

Bei schuldhafter, d.h. fahrlässiger oder vorsätzlicher Verletzung der urheberrechtlichen geschützten Rechte – Verwertungsrechte wie auch Persönlichkeitsrechte – kann der Verletzte von dem Verletzer Schadenersatz nach §87 UrhG fordern [Cire97, 201]. Der Schadenersatzanspruch besteht aufgrund der weitgehenden Unmöglichkeit der Naturalrestitution zumeist aus einer Entschädigung in Geld und berechnet sich nach der Differenztheorie in Höhe des erlittenen Vermögensschadens. Ausdrücklich ist auch die Forderung des dem Verletzten durch die Verletzungshandlung entgangenem Gewinn zulässig, §87 Abs.1 UrhG.

8.3.1.4 Anspruch auf verschuldensunabhängiges Entgelt

Das österreichische Urheberrecht kennt in einigen genau aufgezählten Fällen auch bei verschuldensunabhängiger Verletzungshandlung einen Anspruch auf angemessenes Entgelt laut §86 UrhG.

8.3.1.5 Anspruch auf Auskunft und Rechnungslegung

Der Verletzer hat nach §87a UrhG auf Verlangen des Berechtigten über den mit der Verletzungshandlung erzielten Gewinn Rechnung zu legen und soweit die Verletzungshandlung in einer Verbreitung vorliegt, umfassend Auskunft über Dritte zu geben.

8.3.2 Strafrechtliche Konsequenzen in Österreich

Im Gegensatz zu den zivilrechtlichen Ansprüchen ist eine Analogie im Strafrecht ausgeschlossen, die strafrechtlichen Konsequenzen des Urheberrechts sind abschließend, soweit nicht einschlägige Normen aus anderen Gesetzen, etwa dem StGB in Betracht kommen.

Nach österreichischem Urheberrecht wird ein widerrechtlicher Eingriff in die Verwertungsrechte des Urhebers nach §91 Abs.1 UrhG mit bis zu sechs Monaten oder mit Geldstrafen bis zu 360 Tagessätzen bestraft. Bei gewerbsmäßiger Begehung beträgt der Strafraum laut §91 IIa UrhG bis zu zwei Jahren. Eine Geldstrafe ist dann nicht vorgesehen. Strafrechtliche Maßnahmen setzen jedenfalls ein vorsätzliches Handeln voraus, §7 Abs.1 StGB [KoRe03, 177].

8.3.3 Exkurs: Rechtssicherheit

Ein Raubkopierer muss für seine begangenen Straftaten nicht einmal seinen Schreibtisch verlassen. Jedoch auch wenn er sich in seiner Wohnung meist sicher und unbeobachtet fühlt, befindet er sich niemals in einem rechtsfreien Raum. Nutzer und Verbreiter von Raubkopien stehen daher zwei sehr wichtige Instanzen gegenüber. Auf der einen Seite gibt es das Gesetz, welches freies Kopieren von Musik, Software oder

Filmen meistens verbietet. Auf der anderen Seite gibt es die einzelnen Urheber, wie Filmstudios, Plattenfirmen und Softwareunternehmen, welche den Raubkopien schon vor vielen Jahren den Krieg erklärt haben.

8.4 Kampagne: Raubkopierer sind Verbrecher!

„Während die Verbände nicht müde werden, Filesharer zu kriminalisieren und über Raubkopier-Metaphern und zweifelhaften Kampagnen mit Gewalttätern gleichzusetzen, ist die rechtliche Einschätzung nach wie vor unklar. Angefangen mit Ermittlungsmethoden über die Beweisführung bis hin zur Bezifferung verursachter Schäden besteht trotz jahrelanger Debatte keine einheitliche Meinung.“ [Joos06]

Viele Kinobesucher in Deutschland und Österreich bekamen im Jahr 2004 noch vor dem Hauptfilm unfreiwillig ein Propagandavideo zu sehen. In diesem wurden zwei junge Männer gezeigt, welche gerade in ein Gefängnis eingeliefert werden. Dabei beobachten Altinsassen, wie die zwei Neuankömmlinge von den Gefängniswärtern zu ihren Zellen gebracht werden und erklären mit „hämischem Grinsen“, dass sie sich schon sehr auf die „knackigen Ärsche“ der beiden „Raubkopierer“ freuen. Angesichts derartiger Kinowerbung waren nicht nur die Zuschauer fassungslos. Auch der Geschäftsführer Volkler Nickel des Zentralverbandes der deutschen Werbewirtschaft (ZAW) hielt die Art und Weise, wie diese Kampagne umgesetzt wurde, in höchstem Maße für fragwürdig [Krem03]. Diese umstrittene Reklame war ein Teil einer sehr groß angelegten Werbekampagne der deutschen Filmwirtschaft unter der Mithilfe der Zukunft Kino Marketing GmbH (ZKM). In Plakatmotiven und Kinospots sollte dabei auf das illegale Raubkopieren hingewiesen werden. Der Leitsatz dieser Aktion: „Raubkopierer sind Verbrecher“ erklärte mit einem Schlag Millionen Computeranwender pauschal zu Kriminellen. Dabei ist schon die Aussage juristisch gar nicht haltbar. Denn im strafrechtlichen Sinn handelt es sich hier nicht um ein „Verbrechen“, sondern um ein „Vergehen“. Ohnedies erzielte diese Kampagne bei den vielen Kinobesuchern nicht die von den Verantwortlichen erhoffte Wirkung. Die Besucher im Kino, welche noch nie eine Raubkopie benutzt haben, fühlten sich von diesem Spot nicht angesprochen. Empört hingegen waren viele Kinobesucher, als Verbrecher bezeichnet zu werden, obgleich sie soeben für den Kinofilm einen Eintritt

bezahlt hatten. Im Jahr 2005 startete eine Neuauflage der Kampagne der ZKM, dieses Mal ohne unterschwellige Gewaltandrohung. Der Idee blieb jedoch die Gleiche: „Raubkopierer sind keine Kunden, sondern Kriminelle“.

Den starken Wandel, welchen sich die Musikindustrie in den letzten Jahren unterzogen hat, muss sich die Filmwirtschaft noch unterziehen. Denn bereits heute kann man einen Film in sehr guter Qualität herunterladen und danach selbst auf eine leere DVD brennen. Tag für Tag bedienen sich Millionen von Filmfans in den zahlreich verfügbaren Tauschbörsen. Jedoch ist eine Filmdatei weitaus voluminöser als es zum Beispiel ein digitales Musikstück ist. Deshalb nimmt ein Download eines Filmes im Durchschnitt mehrere Stunden in Anspruch. Nicht jeder Internetnutzer ist bereit, eine solche Wartezeit dafür in Kauf zu nehmen.

Indes steigt die flächendeckende Versorgung mit schnellen Internetanschlüssen stetig. Schon jetzt benutzen in vielen europäischen Staaten mehr private Internetnutzer einen Breitbandanschluss als klassische ISDN Anschlüsse [Otte05]. Die technische Voraussetzung, welche für einen raschen Download von sehr großen digitalen Dateien benötigt wird, ist bereits für viele Kunden keine Zukunftsvision mehr und tendenziell deutlich auf dem Vormarsch. In nicht so ferner Zukunft wird sogar ein kompletter Download eines Filmes in DVD-Qualität nur noch so viel Zeit benötigen, wie es heutzutage dauert, eine MP3-Datei downzuloaden. Deshalb sind die heutigen Probleme, mit welchen sich die Filmwirtschaft auseinandersetzen muss, erst der Anfang eines großen Wandlungsprozesses. Der Enduser, welcher das Grundprinzip des kostenlosen Downloads am Beispiel von Musikfiles bereits längst verinnerlicht hat, wird sicherlich auch im Filmbereich dieser Versuchung nicht widerstehen können. Daher ist es der Filmwirtschaft aus wirtschaftlicher Sicht zu wünschen, dass sie aus den begangenen Fehlern der Musikindustrie lernen kann. Doch die oben erwähnten Kampagnen wie „Raubkopierer sind Verbrecher“ lassen eher darauf schließen, dass auch die Filmwirtschaft den falschen Weg eingeschlagen hat.

Raubkopien aller Art sind heute mehr verbreitet als jemals zuvor. Sogar die immer härteren Maßnahmen, welche die einzelnen Rechteinhaber gegen die Raubkopierer unternehmen, werden das illegale Kopieren von Originalen nicht eindämmen können. Eher das Gegenteil ist eingetreten, denn was vor vielen Jahren als Hobby von einzelnen Computerfreaks und Hackern betrieben wurde, ist heutzutage zu einem Massenphänomen geworden. Viele Millionen Personen auf der ganzen Welt laden sich

urheberrechtlich geschützte digitale Daten herunter und brennen diese Raubkopien auf CDs und DVDs.

Doch die einzelnen Rechteinhaber zeigten sich vorerst von derartigen Entwicklungstendenzen nahezu unbeeindruckt. Erst als sich ihre klassischen Vertriebsmethoden als ineffizient erwiesen, gab man den Raubkopierern die Hauptschuld für die anhaltenden Umsatzrückgänge. Als Ersatz für neue Geschäftsmodelle und Erschließung von Märkten überließ die angeschlagene Industrie dieses Problem einfach ihren Anwälten. Seit diesem Zeitpunkt werden Downloader von urheberrechtlich geschützten Material strafrechtlich verfolgt, die Rechte von den Käufern immer mehr eingeschränkt und die vollzogenen Strafen für Raubkopierer kontinuierlich verschärft.

Die Szene mit ihren eigens aufgestellten Werten und Regeln abseits von Gerichtsurteilen und Gesetzen fühlt sich durch die strafrechtliche Verfolgung nur noch mehr herausgefordert. Desto heftiger sich daher die Contentindustrie mit ihren Rechtsmitteln gegen die Verbraucher wehrt, umso größer wird der digitale Widerstand gegen sie. Dabei wird immer unklarer, wer gegen die Gesetze verstößt und wer noch das geltende Recht vertritt.

Wie von der Industrie erhofft, führen die Anstrengungen nicht zu einem stärkeren Unrechtbewusstsein der Leute. Umso mehr beklagen die betroffenen Menschen den ständig stärker werdenden Verlust ihrer individuellen Freiheit und die anwachsende Kontrolle der einzelnen Urheber auf ihre digitalen Werke. Viele Dinge, welche bis vor kurzem noch selbstverständlich waren, werden durch diese Vorgehensweise in Frage gestellt. Die Arbeit einer anderen Person zu verbessern, fortzusetzen oder aus ihr eine eigene Schöpfung zu gestalten, wird immer schwieriger. Daher werden viele Künstler heutzutage durch das strenge Urheberrecht in ihrer Kreativität stark eingeschränkt. Unter den gegebenen Umständen fällt es daher für viele sehr schwer, die digitalen Werke der Unterhaltungsindustrie, seien es Filme oder Musikstücke, noch als Kulturgut zu bezeichnen. Sie sind vielmehr Produkte einer Industrie, welche für sie allein als Einnahmequelle fungiert [KrSe06, 256-259].

Einige Studien von renommierten Universitäten belegen, dass Raubkopierer nicht alleine für die Umsatzeinbrüche verantwortlich gemacht werden können, welche die Industrie in den vergangenen Jahren hinnehmen musste. Mit Sicherheit wird auch künftig ein funktionierendes Urheberrecht von ungeheurer Bedeutung für unsere Gesellschaft sein. Doch in diesem Zusammenhang stellt sich die Frage, wie das derzeitige

Urheberrecht noch förderlich sein kann, wenn es nicht mehr für die Gesellschaft von Nutzern ist, sondern nur unter Einfluss der Unterhaltungsindustrie steht? Denn die einzelnen Konsumenten werden daher keinen überzeugenden Grund sehen, sich an die Gesetze des Urheberrechtes zu halten, solange ihnen das Copyright wie eine Einschränkung von einigen mächtigen Rechteinhabern vorkommt. So gesehen schaden die bisherigen Anstrengungen der Unterhaltungsindustrie gegen Raubkopierer nicht nur der Kultur, sondern nutzen nicht einmal der Industrie selbst. Trotz des scharfen Vorgehens von Seiten der Industrie gegen Raubkopierer steigen nämlich die Umsätze der Industrie nicht wie von ihr prophezeit wurde wieder an. Daher kann man einfach sagen: Solange eine Nachfrage nach digitalen Werken existiert, wird es auch immer ein entsprechendes Angebot verfügbar sein. Die Frage ist dabei lediglich, wo und von wem sie angeboten werden.

9 Analyse des Filesharings

Laut einer Studie zum Thema digitale Mentalität wurde von 66 Prozent der Teilnehmer privates Raubkopieren als weniger gravierend im Vergleich zu Ladendiebstahl empfunden. Immerhin 30 Prozent beurteilten es als ebenso gravierend und etwa 3 Prozent stuften Raubkopieren als gravierender im Vergleich zu Ladendiebstahl ein. Gründe für diese Aussage liegen vor allem in der Anonymität beim Raubkopieren sowie in der Tatsache, dass beim Raubkopieren der Geschädigte nicht ins Bewusstsein tritt. Die Umfrage unterstützt auch die Vermutung, dass beim privaten Einsatz von Raubkopien keine Strafverfolgung befürchtet wird. 60 Prozent der Nutzer von Raubkopien hatten keine Sorge, erwischt zu werden. [Wöbk04, 15]

9.1 Philosophie und Psychologie des Kopierens

„Verkaufe ich jemandem ein materielles Gut, sagen wir, ein Auto, so hat nach dem Geschäft der Käufer das Auto, ich habe es nicht mehr. Verkaufe ich jedoch jemanden eine Information, so hat nach dem Geschäft natürlich der Käufer die Information, ich habe sie aber auch noch.“ [Stock04]

Das digitale Zeitalter brach so schnell in die privaten Haushalte ein, dass sich der Gesetzgeber nicht an die neuen Technologien anpassen konnte. Es gibt nämlich meistens eine Übergangsphase, welche der Gesetzgeber benötigt, bis die rechtlichen Bestimmungen die neue Technik eingeholt haben. Bis zu diesem Zeitpunkt sieht sich der Gesetzgeber mit der Problematik einer digitalen Gesellschaft gegenübergestellt, mit welcher er versucht mittels herkömmlicher Gesetze gerecht zu werden. Die neue Informationstechnologie ist die kommende Herausforderung, welcher sich die heutige Gesellschaft und daher auch die Gesetzgebung zu stellen haben [KrSe06, 169-172].

Wie bereits damals Bill Gates der „Community“ 1976 in seinen offenen Brief mitteilte, könne er keinen Sinn darin erkennen, mit sehr viel Mühe und Geld Software zu entwickeln, um nachher zusehen zu müssen, wie jede Person sie kopiert [Gate76]. Aus wirtschaftlicher Sichtweise entwickeln die Unternehmen ihre Produkte zum Zwecke der Gewinnmaximierung und möchten dementsprechend für deren Herstellung vergütet

werden. Jedoch wenn es um den Preis von Software oder Informationen allgemein geht, ist es sehr schwierig, dafür einen gerechten Preis festzulegen. Vergleicht man die Ware Information mit einem physischen Produkt, entstehen für dessen Entwicklung ebenfalls Kosten. Jedoch gehen die Herstellungskosten nahezu gegen Null, wenn die Software jene Kosten eingespielt hat. Die Software kann, wie bereits erwähnt, ohne allzu großen Aufwand beliebig oft kopiert werden, schließlich besteht sie ja lediglich aus digitalen Daten, welche man vervielfältigen kann. Deshalb sind bei einem Kauf von Software fast keine Materialkosten zu bezahlen. Der Nutzer erwirbt schließlich nur eine Kopie des Originals. Tatsächlich ist daher der Wert einer Software der Verkaufspreis, welchen das Softwareunternehmen für ihr Produkt festsetzt. Das Erzeugnis, welches der Nutzer erwirbt, kann daher also nicht am Rohmaterial gemessen werden. Es ist demgemäß sehr schwierig für den einzelnen Kunden, den realen Wert des Softwareproduktes nachzuvollziehen. Der Benutzer der Software muss deswegen dem Hersteller glauben, dass der Nutzen des Produktes dem veranschlagten Preis entspricht. Sich aus diesem Sachverhalt resultierende Widersprüche und umstrittene Urteile, können als direkte Auswirkungen von einer Panik machenden Industrie charakterisiert werden. Diese führt einen Streit gegen die heutige digitale Gesellschaft, in welcher das Umdenken bereits längst eingesetzt hat. Zwar tut die Contentindustrie ihr Bestmöglichstes, um darauf hinzuweisen, dass Raubkopien und die Weitergabe von urheberrechtlich geschützten Daten in Tauschbörsen illegal sind; trotzdem werden sie von einigen Millionen Menschen auf der Welt genutzt. Was veranlasst jedoch diese Menschen, sich digitalen Content aus dem Netz herunterzuladen, anstatt sich die Produkte in einem Geschäft zu kaufen?

Raubkopierer haben gänzlich unterschiedliche Gründe, weshalb sie auf den Erwerb von Originalsoftware verzichten. Nur einigen von ihnen ist bei ihrem Handeln nicht bewusst, dass es illegal ist. Die meisten Raubkopierer sind Gewohnheitstauscher oder folgen einem Sammeltrieb, weil sie mit dem Vorhandensein von Tauschbörsen aufgewachsen sind.

Doch weitaus verbreiteter sind Motive, welche sich auf rein wirtschaftliche Tatsachen begründen lassen. Auf der einen Seite kopieren Raubkopierer, weil sie sich den Originalcontent nicht leisten können, auf der anderen Seite kann man sich durch das Kopieren das Geld für das Original einfach sparen.

Laut eines Modells der Wirtschaftswissenschaften kann der Mensch als „Homo oeconomicus“ verstanden werden. Danach versucht jeder Mensch so zu handeln, dass er

daraus einen möglichst großen Nutzen zieht. Wenn man das Verhalten eines Raubkopierers aus dieser Perspektive betrachtet, kommt man zu der Schlussfolgerung, dass, wenn ein Mensch vor die Alternative gestellt wird, ein digitales Produkt zu erwerben oder es sich zu kopieren, dass sich der „Homo oeconomicus“ letztlich für die Option entscheiden wird, welche ihm den größten Nutzen bringt: nämlich die Kopie.

Andere Personen kopieren wiederum wirklich nur aus ideologischen Motiven und benutzen tatsächlich nur Raubkopien. Solche vertreten meistens die Meinung, dass Musik, Software und Filme völlig frei erhältlich sein sollten, nach dem Prinzip „Freie Information für alle“. Andere wiederum sehen die Benutzung von illegalen Kopien als einen Protest gegen die Hersteller von digitalen Produkten wegen aus ihrer Sichtweise überzogenen Preises. Auch die Produkte der Firma Microsoft werden daher zum Teil aus einer Protesthaltung gegen die Monopolstellung des Softwaregiganten kopiert. Doch es muss festgehalten werden, dass die Idealisten weltweit betrachtet nur für einen Bruchteil der Raubkopien verantwortlich sind.

Vor allem darf der soziale Druck nicht unterschätzt werden, welcher vom privaten Umfeld der einzelnen Raubkopierer ausgeht. Denn in sozialen Gruppen, in welchen die Mitglieder in einem engen Kontakt zueinander stehen, ist das Teilen untereinander gewisser Maßen eine Selbstverständlichkeit. Ein Mitglied einer solchen Gruppe, welches sich weigern würde, Sachen für andere zu kopieren, könnte dabei rasch als Außenseiter bezeichnet werden.

Dennoch kann diese Tatsache nicht erklären, warum Millionen Computernutzer Musik, Software, Filme und Bücher weltweit mit unzähligen Fremden in Tauschbörsen teilen. Es muss daher auch untersucht werden, warum so viele Personen, welche sich normalerweise gesetzestreu verhalten, im Bereich Urheberrecht das Gesetz so häufig übertreten.

Als Grund kann jedoch nicht das fehlende Unrechtbewusstsein genannt werden. Denn eine Untersuchung der Gesellschaft für Konsumforschung (GfK) aus dem Jahre 2004 hat ergeben, dass in Deutschland zum Beispiel 74% der Personen wissen, dass fast alle Musikangebote die in Tauschbörsen angeboten werden, illegal sind [Fiut04]. Eine andere Studie der Universität Witten/Herdecke kam im gleichen Jahr zum Ergebnis, dass sogar 98% der befragten Personen der Meinung waren, Software sei kein freies Gut [o.V.04a, 16]. Es werden jedoch trotz dieses hohen Rechtsempfindens, welches man bei Umfragen nachweisen konnte, massenhaft Raubkopien benutzt.

Schon lange befassen sich Kriminalwissenschaftler weltweit mit der Frage, weshalb Personen illegale Handlungen begehen. Eine noch sehr junge Kriminalitätstheorie stammt von Travis Hirschi und Michael Gottfredson [GoHi90]. In ihrer veröffentlichten General Theory of Crime gehen die beiden Forscher von der Annahme aus, dass Personen generell rational handeln und dabei vor jeder Handlung etwaige Vor- und Nachteile ihrer Taten abwägen. Für die beiden Wissenschaftler entstehen nämlich Strafdaten zur Befriedigung von Bedürfnissen und aus Eigeninteresse. Je geringer bei dieser Tat die Gefahr ist, entdeckt und bestraft zu werden, um so eher werden Personen ein Gesetz übertreten. Legt man dieses Wissen auf das Filesharing um, sind rechtliche Sanktionen sehr unwahrscheinlich. Dass man bei illegalen Filesharingaktivitäten erwischt wird, ist laut Univ. Prof. Markus Giesler quasi gleich Null [Baue04]. Umso größer dabei die Anzahl der aktiven Nutzer in einer solchen Tauschbörse ist, desto niedriger ist dabei das Risiko des einzelnen Users. Die durchgeführte Studie der Universität Witten/Herdecke kam in diesen Zusammenhang folgerichtig zum Ergebnis, dass die Mehrzahl der aktiven Nutzer von Raubkopien keine Angst davor hat, jemals überführt zu werden [o.V.04a, 15]. Die scheinbare Anonymität, in welcher sich die meisten Nutzer des Internets fälschlicherweise glauben zu befinden, ist dabei ein sehr wichtiger Faktor. Die einzelnen Internetnutzer fühlen sich sicher und unbeobachtet, wenn sie das Medium Internet benutzen. Des Weiteren verleiht diese scheinbare Anonymität Selbstvertrauen und ermöglicht so den User Hemmungen abzubauen [Dona01]. So handeln viele Benutzer in einer Art, welche sie niemals im realen Leben an den Tag legen würden. Wenn man sich also als Teil einer großen anonymen Masse fühlt und sich daher nicht für sein Verhalten verantworten muss, wird ein unsoziales Verhalten begünstigt [Dori03, 135].

Dabei ist diese Anonymität, in welcher man sich wiegt, nur eine vermeintliche Sicherheit. Denn prinzipiell kann jeder Internetnutzer zurückverfolgt und daher seine tatsächliche Identität ausfindig gemacht werden.

9.2 Raubkopieren

Stellen sie sich vor, bei ihnen um die Ecke macht ein Geschäft auf. Mit stets dem Neuesten an Büchern, Filmen, Software und Musik-CDs. Das volle Sortiment, immer gefüllte Regale, nur keine Kassen. Das Geschäft wäre jeden Tag voll mit Menschen

aller Altersschichten, welche sich streng ökonomisch verhalten und das bestmögliche Produkt zum günstigsten Preis haben wollen – oder umsonst. Nach dem gleichen Prinzip funktionieren Tauschbörsen und Peer-to-Peer-Netze im Internet: Hier gibt es alle Inhalte, welche digitalisierbar sind und sich über das Netz verschicken lassen. Es wird alles gratis angeboten, was sonst viel Geld kostet. Das Risiko, etwas Illegales zu tun, nehmen viele dabei in Kauf.

Die Ausgangssituation dabei ist die Verbreitung einer Verhaltensweise, welche heutzutage unter dem Begriff „Raubkopieren“ zu einem Phänomen geworden ist, das auf der ganzen Welt bekannt ist. Die Tatsache, dass die Verbreitung von urheberrechtlich geschützten digitalen Daten eine Straftat ist, scheint den meisten Menschen keine große Rolle zu spielen.

„Wir befinden uns in einer Situation, in der sich ein erheblicher Teil unserer Gesellschaft wissentlich oder unwissentlich über geltendes Recht hinwegsetzt, ohne dass sich dieses Verhalten auf bestimmte Gruppen innerhalb der Gesellschaft einschränken ließe.“ [Wöbk04, 3]

Allein die Bezeichnung „Phänomen“ enthält bereits einen Hinweis darauf, dass die Erwartung an die Wirklichkeit nicht der Erfahrung entspricht: Raubkopieren verstanden als eine Straftat müsste in dieser Erwartung „eigentlich“ die Ausnahme und dürfte nicht die Regel sein, wie wir sie erleben. Tatsächlich kann man jedoch beobachten, dass Raubkopieren für viele Personen zum normalen, alltäglichen Leben gehört.

„Im Falle der Urheberrechtsverletzung, die durch digitale Vervielfältigung begangen wird, bleibt ein intuitives Verständnis für das damit verbundene Unrecht aus, weil das Tatbestandsmerkmal der Wegnahme fehlt, das unseren historisch gewachsenen Vorstellungen von Diebstahl zu Grunde liegt.“ [Wöbk04; 4]

Tausende von Tauschbörsen bieten geknackte Software, Newsgroups im Usenet liefern Terabyte an raubkopierten Filmen Wochen vor dem Kinostart und Musik ohne Kopier- und Abspielschutz. Hackertools, Seriennummern, verbotene Kopierprogramme und geknackte Software lassen sich mit jeder Suchmaschine finden. Jedoch nicht alles, was im Netz zu finden ist, ist auch legal. Diese Tatsache ist so alt wie das Internet selbst. Zumindest über die Illegalität von einigen Inhalten bestehen heute kaum noch Zweifel: so fanden Wissenschaftler der Universität Witten im Auftrag von Microsoft heraus: 90 Prozent aller Nutzer wissen, dass sie sich mit Raubkopien strafbar machen. 66 Prozent hält dieses Wissen jedoch nicht davon ab, Kopien anzufertigen oder sie zu nutzen [Wöbk04, 15].

9.2.1 Typen von Raubkopierern

Das bereits beschriebene Phänomen des Raubkopierens ist durch eine genaue Analyse der verschiedenen Einstellungen unterschiedlicher Typen von Raubkopierern zu erklären. Da sich nämlich die Gesamtheit der Raubkopierer nicht auf einen gemeinsamen Nenner bringen lässt, erlaubt eine Aufteilung in verschiedene Gruppen eine genauere Beschreibung spezifischer Denkmuster und Verhaltensweisen. Zur Untersuchung der verschiedenen Ausprägungen einer digitalen Mentalität bei unterschiedlichen Softwarenutzerguppen musste diese Nutzergruppe erst einmal intern voneinander unterschieden werden. Dazu werden zwei Größen als Unterscheidungskriterium herangezogen. Zum einen die Beurteilung der individuellen Computerexpertise, welche die Auseinandersetzung, Begeisterung und Kenntnisse einer Gruppe für das Medium Computer beschreibt, zum anderen die Raubkopierintensität im privaten Bereich, welche die Verbreitung und den Besitz von Raubkopien zusammenfasst. In diesen Zusammenhang wird unter vier verschiedenen Personenkreisen unterschieden [Wöbk04, 18-20]:

- PC-Freaks
- Hobby-User
- Pragmatiker und
- PC-Profis.

Bildet man die soeben beschriebenen Dimensionen (Computer-Expertise, Raubkopierintensität privat) auf einer Matrix ab, lassen sich vier unterschiedliche überschneidungsfreie digitale Typen identifizieren.

		Computer-Expertise	
		hoch	niedrig
Raubkopierintensität privat	hoch	PC-Freaks	Hobby-User
	niedrig	PC-Profis	Pragmatiker

Abbildung 9: Vier-Feld-Matrix der digitalen Typen nach [Wöbk04, 18]

Die Gruppe der PC-Freaks, welche 10% der digitalen Typen repräsentiert, zeichnet sich durch eine hohe Raubkopierintensität sowie durch eine hohe Computerexpertise aus. Dabei können sie in Bezug auf ihr Raubkopierverhalten als echte „Sammler und Jäger“ gelten, welche sich sämtliche digitale Daten besorgen, welche sie irgendwo vielleicht einmal benötigen könnten. Deshalb fungieren die PC-Freaks als beachtliche Knoten im Tauschnetzwerk für Raubkopien. Die Hobbyuser hingegen, welche 34% der digitalen Typen abbilden, zeichnen sich durch eine geringe Leidenschaft gegenüber ihrem Computer aus, ihr Raubkopierverhalten ist jedoch ähnlich den PC-Freaks. Die Pragmatiker, welche 49% der digitalen Typen ausmachen, setzen den PC meistens schlicht als ein Arbeitsgerät ein, dazu werden Raubkopien nur im vergleichsweise geringen Maße benutzt. Die große Gruppe der Pragmatiker ist innerhalb der durchgeführten Umfrage am stärksten vertreten. Der Altersdurchschnitt liegt nebenbei erwähnt bei 34 Jahren. Die PC-Profis, welche 7% der digitalen Typen repräsentieren, stellen die letzte Gruppe der identifizierten digitalen Typen dar. Sie nutzen den Computer in einer professionellen Weise und setzen hierzu nur legal erworbene Software ein. Diese vier beschriebenen Nutzergruppen dienen im weiteren Verlauf der Arbeit als Einheiten der weiteren Analyse [Wöbk04, 5].

Die Anzahl der ideologisch motivierten Raubkopierer, welche Kopien zum Beispiel als wirtschaftlichen Boykott der Preispolitik eines Softwaremonopolisten legitimieren, ist vergleichsweise gering und reicht nicht aus, um als eine eigene abgrenzbare Gruppe innerhalb der Masse der Raubkopierer wahrgenommen zu werden.

Um im weiteren Verlauf ein präziseres Bild von Raubkopierern zu erhalten, wurden noch zwei weitere Größen eingeführt, mit denen sich die exakte Einstellung der Softwarenutzer zu Raubkopien treffend beschreiben lässt. Diese Größen sind das Rechtsbewusstsein und die Raubkopiermentalität. Das Rechtsbewusstsein zeigt dabei, inwieweit sich das klassisch vorhandene Rechtsempfinden auf die digitale Welt überträgt. Mit dem festgestellten Ausmaß des Rechtsbewusstseins lässt sich feststellen, inwieweit einzelne Verletzungen von Urheberrechten, wie beispielsweise eine physische Eigentumsverletzung wahrgenommen werden. Außerdem benennt die Größe das Ausmaß an Ehrlichkeit und drückt dadurch den gewissenhaften Zahlungswillen für in Anspruch genommene Leistungen aus. Die Raubkopiermentalität hingegen misst, in welchem Maß das Raubkopieren von Software eine Sonderrolle im Vergleich zum Kopieren von CDs, MP3-Dateien oder DVDs einnimmt.

Entlang der beiden extrahierten Dimensionen lassen sich nun die verschiedenen Einstellungen der vier digitalen Typen zum Thema Software-Raubkopieren genauer charakterisieren.

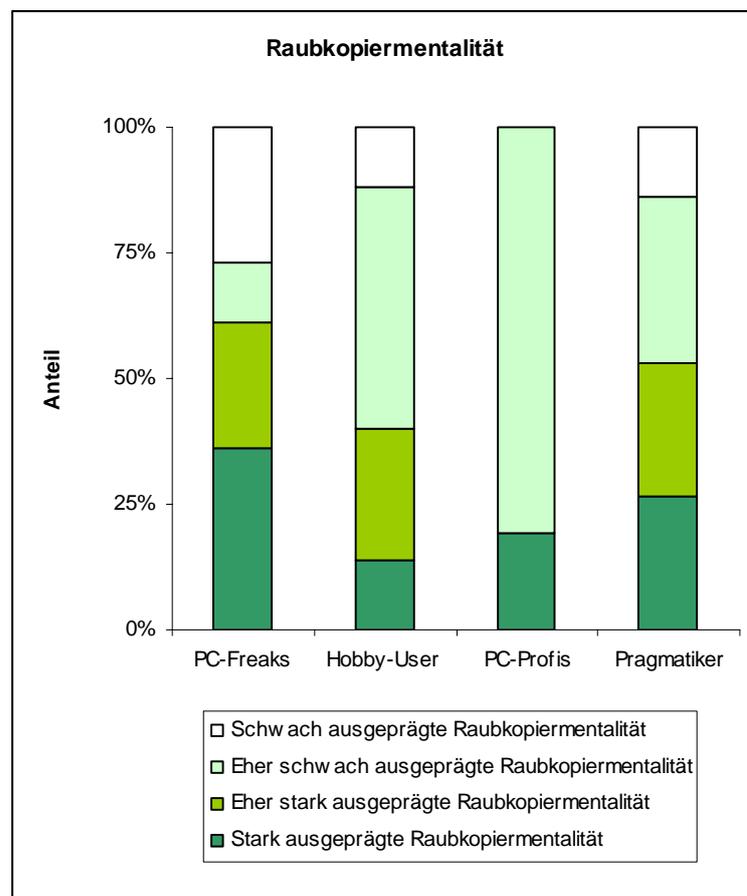


Abbildung 10: Ausprägung der Raubkopiermentalität nach [Wöbk04, 22]

Dabei lassen sich überraschende Werte der Ausprägung der Raubkopiermentalität bei der Gruppe der PC-Freaks finden. Nahezu 65 Prozent dieser Gruppe geben an, dass sie eine stark bis eher stark ausgeprägte Raubkopiermentalität besitzen. Diese Ausprägungsform kann im ersten Augenblick überraschen, da sie bedeutet, dass Software-Raubkopien im Vergleich zu anderen Copyrightverletzungen als sehr gravierend eingestuft werden. Der Grund für dieses ermittelte Ergebnis liegt vermutlich daran, dass die Gruppe der PC-Freaks gerade wegen dieser Einstellung Anreize für das Raubkopieren hat. Die Selbstwahrnehmung als Überwinder der Kopierschutzmechanismen und als Verbrecher motiviert wahrscheinlich einen Teil dieser Gruppe dazu, sich ständig aufs Neue den Herausforderungen des Raubkopierens zu stellen.

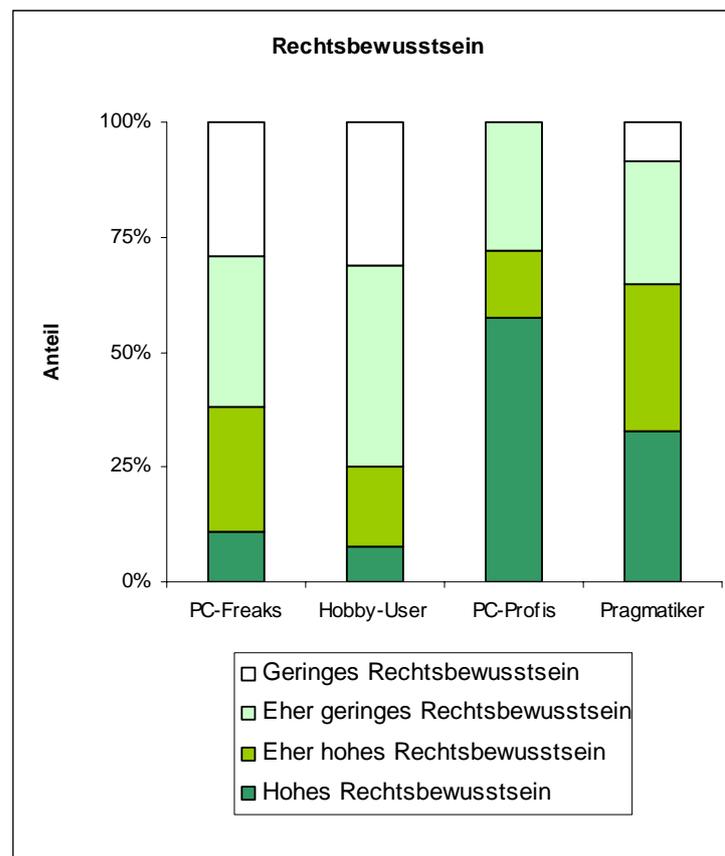


Abbildung 11: Ausprägung des Rechtsbewusstseins nach [Wöbk04, 23]

Die Abbildung 15 zeigt deutlich, welchen Einfluss ein dementsprechend ausgeprägtes Rechtsempfinden auf das Raubkopierverhalten hat. Das gesamte Ausmaß des Rechtsbewusstseins der Vielkopierer (PC-Freaks, Hobby-User) bleibt deutlich hinter dem der Wenigkopierer (PC-Profis, Pragmatiker). In der Gruppe der PC-Profis weist

der Anteil von 75% an eher hohem Rechtsbewusstsein darauf hin, dass diese Gruppe sehr bewusst auf Raubkopien verzichtet, um sich gesetzeskonform zu verhalten.

Die Unterscheidung der anonymen Masse der Raubkopierer in die jeweiligen Gruppen erlaubt weithin eine Differenzierung, welche in Kombination mit den Möglichkeiten des DRM neben einer generellen Senkung der Raubkopiererrate auch neue Möglichkeiten der Kundenbindung verspricht.

9.2.2 Zusammenfassung

Die Ergebnisse zeigen recht deutlich, dass in der Frage nach dem Rechts- und Unrechtsbewusstsein im digitalen Medium eine weit verbreitete Klarheit herrscht. Es fällt der überwiegenden Mehrheit der Internetnutzer nämlich nicht schwer, ihr eigenes Handeln im Bezug auf Raubkopien als Unrecht zu bewerten.

Faktum in diesem Zusammenhang ist jedoch, dass dieses Rechtsbewusstsein nur einen geringfügigen Einfluss auf das vorherrschende Raubkopierverhalten hat. Es lässt sich beispielsweise beobachten, dass besonders der Anreiz, Familie und Freunde mit Raubkopien zu versorgen, eine Eigendynamik entwickelt. Die dabei entstehenden Kräfte und die Eigendynamik dieses Kopierens im Freundeskreis überwiegen den möglichen Einfluss einer rechtlichen Regelung bei weitem. Im Folgenden wird kurz aufgezeigt, welche prinzipiellen Bedingungen erfüllt sein müssen, damit Menschen sich an geltendes Recht halten [Wöbk04, 27]:

1. Optimalerweise stimmt eine Verordnung oder ein Gesetz mit dem intuitiven Rechtsempfinden des Einzelnen überein. In diesem besonderen Fall entspricht das rechtskonforme Verhalten der Verhaltensweise, welche die jeweilige Person auch ohne die entsprechend gesetzlichen Regelungen gezeigt hätte.
2. Wo jedoch diese Übereinstimmung von geltendem Recht und intuitivem Rechtsempfinden nicht gegeben ist, braucht es Aufklärung. Die gesetzlichen Regelungen müssen so begründet und aufbereitet werden, dass es jedem möglich ist, sie zu kennen und nachzuvollziehen. Sobald beides, Nachvollziehbarkeit und Kenntnis, vorhanden ist, wird sich das Individuum im Idealfall gesetzeskonform verhalten. Wird jedoch trotz umfassender Aufklärungsarbeit die rechtliche Regelung nur zur Kenntnis genommen, bleibt nur noch die

3. Sanktionierung gesetzwidrigen Verhaltens. In diesem Fall muss jedoch die Höhe der Strafe ausreichend sein, um die geforderte Verhaltensänderung zu rechtfertigen, und zweitens muss die Wahrscheinlichkeit, dass gesetzeswidriges Verhalten im Einzelfall auch tatsächlich sanktioniert wird, hinreichend hoch sein.

Die Unterhaltungsindustrie sollte daher die identifizierten Gruppen so ansprechen, dass sich die jeweils anderen Gruppen nicht dadurch angegriffen fühlen. So gleichen sich beispielsweise die PC-Profis und PC-Freaks in ihrem professionellen Umgang mit dem PC, deshalb könnten die PC-Freaks zum Teil zu PC-Profis werden, wenn sie in ihrer Ehre als Spezialisten als gleichwertige Partner angesprochen werden. Die Gruppe der Hobby-User wird wie keine andere über DRM-Systeme gebunden werden können. Am wenigsten Zahlungsbereitschaft für Software ist bei den Pragmatikern zu erwarten. Hier kann man sich die Frage stellen, ob nicht jene Gruppe durch kleinere und noch billigere Versionen oder Freewarelösungen entkriminalisiert werden sollte. Neben den PC-Profis kann auch die Gruppe der PC-Freaks als Meinungsführer gelten, welche durch eine hohe Qualität der Produkte überzeugt werden kann. Alles in allem wird jeder der gezeigten Ansätze seine Zeit benötigen, denn ein digitales Selbstverständnis muss kulturell wachsen.

9.3 Kosten des Anbietens von Dateien

Das rationale Kalkül eines Nutzers, Dateien (z.B.: Filme) in Filesharingdiensten anzubieten, erfordert eine Analyse der Angebotskosten. Es ist dabei zu unterscheiden, ob der Teilnehmer eine Datei anbietet, welche erstmalig in das Netzwerk eingefügt wird (Initialanbieter), bislang kaum im Netzwerk enthalten ist (Diffusionsinitiator) oder bereits eine starke Verbreitung im Netzwerk erfahren hat (Diffusionshelfer).

9.3.1 Initialangebot

Bevor ein Nutzer einen Film oder Song erstmals im Internet anbieten kann, muss er die Mediendatei digitalisieren. Nachdem die erste geeignete Kopie für die Onlinedistribution erstellt wurde, muss der Anbieter sie in das entsprechende

Uploadverzeichnis des Filesharingservices kopieren. Damit belegt er bei einem mit DivX codierten 90 Minuten Film in der Regel 700MB Speicherplatz. So trägt ein Nutzer neben den Wertschöpfungskosten zur Erstellung der Mastercopy für die Online-Distribution auch die Opportunitätskosten der Speicherplatzbelegung auf seinem Rechner.

Nutzer, welche eine Kopie erstmalig und womöglich vor dem offiziellen Verkaufsstart anbieten, werden zudem von der Medienindustrie als Schlüsselfiguren angesehen und laufen erhöhte Gefahr, juristische Konsequenzen für ihr Verhalten tragen zu müssen.

Weiterhin muss ein Anbieter die Distributionskosten in sein Kalkül mit einbeziehen. Diese setzen sich aus den Online- und den Opportunitätskosten für durch Nachfrager beanspruchte Bandbreite zusammen.

Die Kosten für das erstmalige Anbieten eines stark nachgefragten Films, wie zum Beispiel „Starwars“ sind demnach hoch.

9.3.2 Frühe Anbieter – Diffusionsinitiatoren

Einige Teilnehmer sind nicht auf der Suche nach einer unmittelbaren Gegenleistung des Downloaders und bieten den Film frei an – koste es, was es wolle. Häufig reicht es aus, wenn ein oder zwei Initialanbieter die Datei ohne Gegenleistung anbieten, um eine rasche Diffusion zu erreichen. Nutzer, welche die hohen Kosten des Initialangebotes vermindern können, sind eher bereit, die Dateien auch wieder anzubieten, da dadurch die Kosten sinken.

9.3.3 Später Anbieter – Diffusionshelfer

Wenn ein Film stark nachgefragt wird und die kritische Masse der Diffusionsinitiatoren erreicht wurde, können Nutzer von Filesharingnetzwerken, welche ein „Intelligent Download“ von Segmenten einer Datei bei mehreren Anbietern zulassen, erhebliche Kostenersparnisse realisieren. Dadurch, dass oftmals nur noch Segmente einer Datei bei einem Nutzer herunter geladen werden, reduzieren sich die Distributionskosten. Bei zunehmender Anzahl von Anbietern verringert sich dann die Anzahl der Nachfrager pro Anbieter. Die Kosten des Anbietens reduzieren sich somit im Laufe des Diffusionsprozesses erheblich.

Die Kosten des Angebotes nehmen wieder zu, wenn der Lebenszyklus eines Filmes über die Hitphase hinaus betrachtet wird. Nachdem viele Nutzer den Film gesehen haben, werden einige ihn aus dem Archiv löschen und das Angebot damit vermindern. Dies ist bei Musik nicht so wahrscheinlich, da dort die Kosten für Speicherplatz geringer sind und Musik häufiger wiederholt konsumiert wird.

9.4 Nutzen des Anbieters von Dateien

Legt man dem Angebot in Filesharingnetzen die dargestellten Kosten zugrunde, fällt es schwer, die schiere Menge an angebotenen Dateien in der Realität rational zu erklären. Da mit einem großen Angebot die Downloadmöglichkeiten über Multiple-Source-Downloadmechanismen steigen und zudem ein schnellerer Download ermöglicht wird, ist davon auszugehen, dass die Anzahl der Nutzer umso größer wird, je größer die Anzahl der Teilnehmer an einer Datei ist. Dabei steigt die Zahl der Nutzer, wenn Dateien verschiedener Art und Inhalt angeboten werden, also das Sortiment breiter ist. Ein positiver Nutzen wird demnach in erster Linie durch eine breite Auswahl und eine hohe Verfügbarkeit von Mediendateien generiert.

Da ein Angebot den individuellen Nutzer jedoch nicht erhöht, bei einem Teilnehmer aber Kosten verursacht, ergibt sich als dominante Strategie eines jeden rationalen Nutzers, möglichst viel Dateien nachzufragen und selbst keine Dateien anzubieten. Dies gilt umso mehr, da sich die mit einem Angebot verbundenen Kosten durch Freeriding vermindern lassen. Dem individuellen rationalen Kalkül steht dann allerdings ein gesellschaftlich irrationales Ergebnis gegenüber. Da sich der Nutzer jedoch ebenfalls aus Größe und Vielfältigkeit des Angebots zusammensetzt, ergibt sich für sämtliche Teilnehmer der jeweils größte Nutzen in dem Fall, wenn alle Beteiligten die Strategie eines möglichst breiten Angebots verfolgen. Unterteilt man die Teilnehmerentwicklung eines Filesharingnetzes in eine Einführungsphase sowie eine Wachstums- bzw. Reifephase, werden die verschiedenen Einflüsse auf die Nutzerstruktur erkennbar.

9.4.1 Angebotsverhalten in der Einführungsphase

In dieser Phase ist der absolute Nutzen eines Angebots relativ hoch und der Nutzen des Freeriding noch gering. Denn ausgehend von der geringen Größe des Netzwerkes

müssen die Teilnehmer befürchten, dass das öffentliche Gut Filesharing nicht zustande kommt, wenn nicht jeder seinen Beitrag leistet und die Datei anbietet. Verfolgen die Teilnehmer eine langfristige Strategie, in der ihnen an dem Erhalt des Netzes gelegen ist, werden sie ihre Strategie anpassen und unabhängig von der Entscheidung der anderen Teilnehmer selbst anbieten. So wissen die Teilnehmer des Filesharingnetzes in der Einführungsphase, dass der Tausch von Dateien auf dem Konzept des beiderseitigen Gebens und Nehmens der Nutzer basiert.

9.4.2 Angebotsverhalten in der Wachstumsphase

In der Wachstumsphase verändert sich die Einstellung der Teilnehmer, so dass sie durch ein defensives Verhalten das Netzwerk gefährden. Denn in dieser Phase besteht eine negative Beziehung zwischen der Gruppengröße und der Wahrnehmung des eigenen Beitrages, der zum Erhalt des Netzwerkes beiträgt. Der Grenznutzen nicht-kooperativer Teilnehmer ist hier höher als bei den kooperativen. Während in der Einführungsphase noch der Nutzen der Kooperation überwiegt, dominiert mit zunehmender Netzwerkgröße der Nutzen des Nicht-Kooperierens.

9.4.3 Angebotsverhalten in der Reifephase

Durch die höheren Teilnehmerzahlen in den Filesharingnetzen steigt der Nutzen Dateien anzubieten nur mäßig, während der Nutzen des Freeridings zunimmt. In der Reifephase verschärft sich dieser Trend. Jetzt drohen selbst die überzeugten Teilnehmer ihr Angebot einzustellen und das Netz läuft theoretisch Gefahr zu kollabieren. Je größer und anonym er dabei ein Netzwerk ist, desto geringer sind die Möglichkeiten der Beobachtung und zugleich größer die Wahrscheinlichkeit als Freerider nicht entlarvt zu werden. Jedoch sollte beachtet werden, dass nur die Strategie beiderseitigen Anbietens optimal ist. Sie führt zu den individuell höchsten Auszahlungen und sollte daher eigentlich von den Teilnehmern bevorzugt werden. Denn ein reduziertes Angebot führt zu eingeschränkten Nachfragemöglichkeiten, die als Konsequenz der gesunkenen Attraktivität des Netzes die weitere Abwanderung der Nutzer und Anbieter zur Folge haben. Da Filesharingnetzwerke „Kritische-Masse-Systeme“ sind, kann das

Unterschreiten der kritischen Masse zu einem Zusammenbruch des Tauschsystems führen.

9.5 Maßnahmen gegen Freerider

Solange die Wachstumsraten bei den Filesharingnetzwerken weiterhin so hoch sind, werden die Netze kaum an einem Angebotsmangel leiden. Dennoch könnte eine zunehmende Verbreitung von Freeriding negative Folgen auf das Filesharingnetz haben. Eine Netzwerkanalyse ergab, dass 70% der Peer-to-Peer User nur Files downloaden, ohne andere Files für andere Benutzer bereitzustellen. Diese „free rider“ oder „free loaders“, wie sie in diesem Zusammenhang bezeichnet werden, sind dafür verantwortlich, dass viele P2P Systeme unter langsamen Downloadgeschwindigkeiten leiden. [BKKM03, 50].

Während im Konzept des Filesharingpioniers Napster zu Beginn kaum Vorkehrungen gegen Freeriding vorhanden waren, tragen die neu entwickelten Filesharingdienste dem Freeriding und der Heterogenität der Nutzer teilweise schon Rechnung. Grundsätzlich weisen die Nutzer einen hohen Grad an Heterogenität auf. So unterscheiden sie sich insbesondere durch die Internetzugangsgeschwindigkeit, die Latenzzeiten, die Zeit, die sie online sind und schließlich durch die Anzahl und Qualität der angebotenen Dateien. Die meisten Filesharingnetze nutzen ein intelligentes Downloadmanagement. Die Aufteilung einer Datei in Einzelteile (Chunks) erlaubt, dass Teile einer Datei, welche gerade herunter geladen werden, bereits wieder von Dritten nachgefragt werden. Da die Datei erst nach dem vollständigen Download aus dem Upload-Verzeichnis in ein anderes Verzeichnis geschoben werden kann, wird so von den meisten Filesharingsoftwareprodukten sichergestellt, dass Nachfrager auch zu Anbietern werden, auch wenn es nur Teile einer Datei sind.

Ebenfalls könnten technische Verzögerungen dazu führen, dass gegen Ende des Downloads die Downloadgeschwindigkeit bei dem Nutzer reguliert und verlangsamt wird: So könnte ein Nutzer möglichst lange online gehalten werden, so dass andere Nutzer bereits die ersten Chunks wieder herunter geladen haben. Nutzer, welche viele Daten anbieten, würden dieser technischen Verlangsamung nicht oder in geringem Maße unterliegen.

Ebenso bieten die meisten Filesharingdienste einen Instant-Message-Service an. Dieser erlaubt es den Nutzern, untereinander zu kommunizieren und auf diese Weise die Community-Effekte zu verstärken.

Durch die Mitgliedschaft bei so genannten Privaten – Trackern, das sind private Personen, welche für das Bit-Torrent Netzwerk einen Server zur Verfügung stellen, wird das Verantwortungsbewusstsein gegenüber den anderen Filesharingteilnehmern erhöht.

Das geschieht durch Communityeffekte, wie auch durch die Einführung von so genannten Ratios. Diese zeigen das Verhältnis von Upload zu Downloadmenge an. Je höher dabei die Ratio ist, desto höher ist die Reputation in der Community. Weiters erhält man durch eine hohe Ratio Zugang zu mehr Dateien, kann Anfragen nach bestimmten Dateien stellen, hat Zugang zu mehr Informationen (NFO Dateien; welche in der Warez-Szene sehr beliebt sind, können gelesen werden: Darin werden üblicherweise Informationen über die Qualität des Releases, Seriennummern zum Entsperrern der mitgelieferten Software oder ähnliches aufgeführt) [Wiki07c], oder genießt das Privileg, dass keine Wartezeiten beim Download entstehen und dadurch meistens schnellere Downloadraten für den Nutzer bereitstehen.

Alle Maßnahmen, welche Freerider als solche erkennen lassen, erweitern demnach die Angebotsmenge, da Communities opportunistisches Verhalten nur begrenzt dulden.

9.5.1 Zusammenfassung (Kosten & Nutzen)

Trotz der Kosten, welche ein Anbieter in Abhängigkeit des bereits realisierten Diffusionsgrades einer Mediendatei internalisiert, kommt es zu einem enormen Angebot von Dateien im Internet. Jedoch kann ein Nutzer auch in den Genuss des Gesamtangebotes kommen, wenn er selbst nichts zu dem System beiträgt – also Freeriding betreibt.

Die Motive der Anbieter in Filesharingnetzwerken sind dabei vielfältig. Es wurde gezeigt, dass das individuelle Angebotsverhalten davon abhängt, in welchem Stadium sich das Netzwerk befindet. In der Einführungsphase befürchten die Teilnehmer vor allem negative Einflüsse, die durch unkooperatives Verhalten entstehen können, während in späteren Phasen zunehmend weniger Anreize bestehen, Daten anzubieten. Um die Zwangsläufigkeit zu verhindern, dass sich immer mehr Freerider in einem Netz

tummeln und sich dadurch der Anreiz zum Anbieten stark verringert, müssen Filesharingnetzwerke zunehmend Mechanismen implementieren, um dieser Gefahr entgegen zu wirken.

9.6 Legal oder Illegal

„Peer-to-Peer-(P2P)Technologien versprechen durch die weitgehende Loslösung von zentralen Institutionen neue Dimensionen des Informationsmanagements: Die Beschleunigung von Kommunikationsprozessen, die hohe Austauschfähigkeit aktueller, dezentral generierter Informationen, die bessere Auslastung „brachliegender“ Ressourcen oder die effiziente Bewirtschaftung von knappen Ressourcen, sind attraktive Anwendungsbeispiele.“ [ScWe03, 257].

Aus rechtlicher Sicht ist dem Tauschen von digitalen Daten mit Tauschbörsen nur sehr schwer beizukommen. Die Filesharingprogramme selbst sind jedoch juristisch betrachtet nicht mehr als eine normale Software. Denn die Tauschbörsen bieten selbst keine Raubkopien an, sondern stellen lediglich eine Technologie zur Verfügung, welche einen Austausch von digitalen Daten ermöglicht. Mit solchen Filesharingclients können nämlich durchaus auch urheberrechtlich nicht geschützte Daten, wie zum Beispiel selbst gemachte Musik untereinander getauscht werden. Die sehr bekannte Tauschbörse BitTorrent ist dafür extra entwickelt worden, große vor allem legale Dateien, wie beispielweise das frei erhältliche Betriebssystem Linux rasch zwischen den Nutzern verteilen zu können.

Geräte, wie zum Beispiel Videorecorder sind auch nicht illegal, nur weil sie es technisch ermöglichen, mit ihnen Urheberrechtsverletzungen zu begehen. Eine Zeit lang stand es unstrittig fest, dass der Austausch urheberrechtlich geschützter Dateien in der Eigenverantwortung der einzelnen Nutzer liegt. Erst durch ein Urteil des Obersten Gerichtshofes in den USA brachte diese Sichtweise ins Schwanken. Nach einem Jahr des andauernden Rechtsstreits der Unterhaltungsindustrie in Amerika gegen die Tauschbörsen Morpheus und Grokster wurde im Juni 2005 entschieden, dass die einzelnen Betreiber von solchen Filesharingclients durchaus zur Verantwortung gezogen werden können, wenn Verstöße gegen das Urheberrecht nachweisbar sind. Wenn man jedoch dieses Urteil näher betrachtet, war es weniger ausschlaggebend, als

zunächst von den meisten Betroffenen angenommen wurde. Das Höchstgericht nannte nämlich als notwendige Voraussetzung für eine gesetzliche Klage gegen die Betreiber von Tauschbörsen, dass die Clients explizit für Zwecke entworfen sein müssen, welche illegal sind. Die Software von Tauschbörsen wurde demnach nicht generell für illegal erklärt. Es muss daher vielmehr bei jeder einzelnen Klage, welche vor dem Gericht ausgetragen wird, geklärt werden, ob eine grundsätzliche Verletzung des Urheberrechtes von den Softwareprogrammierern der Entwicklungsfirmen vorgesehen war oder nicht. Obwohl jedoch die derzeit genutzte Filesharingtechnik an sich völlig legal ist, kann sie sich, da sie hauptsächlich illegal benutzt wird, sehr schwer als ein rechtmäßiger Teil des Mediums Internet behaupten. Beispielweise hielt der spanische Professor Jorge Cortell einen Vortrag über Filesharing an der Universität Valencia, welcher sich mit den legalen Nutzungsmöglichkeiten dieser neuen Technik befasste. Die Universität zwang ihn daraufhin nach starkem Druck der spanischen Verwertungsgesellschaft im Mai 2005 schließlich zur Kündigung [Kott05].

Da Filesharing zumeist illegal genutzt wird oder gerade deswegen, ist es inzwischen zum Allgemeingut geworden. Millionen von Menschen weltweit laden sich Software, Musik, Bücher und Filme aus dem Internet herunter. Die einzelnen Filesharingnutzer sind wohl nur halbwegs vor Klagen der Industrie geschützt, weil es so eine gigantische Anzahl an aktiven Nutzern gibt. Das Verklagen und Rückverfolgen von Millionen Filesharingnutzern ist schlichtweg unmöglich. Deshalb werden eher aus Gründen der Abschreckung immer wieder Prozesse von der Film- und Musikindustrie ausgetragen, in welchen an einzelnen Filesharingnutzern ein Exempel statuiert wird. Trotz aller Anstrengungen der Contentindustrie steigen die Nutzerzahlen von Tauschbörsen kontinuierlich an. Laut einer Internetanalyse des Magazines Slick hat sich die Anzahl von Filesharingnutzern in den Zeitraum von 2003 bis 2005 fast verdoppelt [Menn05]. Wobei bei diesen Statistiken nur die größten Filesharingnetze berücksichtigt worden sind. Jedoch ist die sehr populäre Tauschbörse BitTorrent ebenfalls in dieser Studie nicht berücksichtigt worden, da es aus heutiger Sicht technisch nicht möglich ist die genaue Anzahl der aktiven Nutzer zu ermitteln. Eine Studie des Unternehmens CacheLogic aus Großbritannien kam zu dem Ergebnis, dass mehr als ein Drittel des gesamten Internettraffics durch das BitTorrentnetzwerk verursacht wird [Wire04]. Insgesamt betrachtet, soll Filesharing sogar für bis zu 80% des totalen Datenverkehrs im Medium Internet verantwortlich sein [Cache04]. Die bisherige Geschichte des

Filesharings hat vor allem eines gezeigt: Noch bevor die Unterhaltungsindustrie ein vorhandenes Problem lösen kann, sind bereits neue Problematiken entstanden.

10 Schätzung für den verursachten Marktschaden

Fernsehzuschauer und Zeitungsleser erfahren sehr oft vom Schaden, welchen „die Raubkopierer“ verursachen. Dabei stützten sich solche Berichte sehr oft auf konkrete Zahlen. Der herbeigeführte Schaden, welchen die Raubkopierer anrichten, bewegt sich anhand diesen Berichterstattungen wiederholt im Milliardenbereich. Dabei wird angenommen, dass diese exorbitanten Summen den einzelnen Unternehmen Jahr für Jahr verloren gehen. Wenn man jedoch diese Berichterstattungen etwas näher betrachtet, lässt sich rasch feststellen, dass diese Zahlen von den jeweiligen Vertretern der Rechteinhaber publiziert werden.

Wenn man jedoch versucht, eine genaue Berechnung eines konkreten Schadens, welcher durch die Raubkopierer verursacht wird, zu ermitteln, erkennt man schnell, dass dies keine leichte Aufgabe ist. Denn anders als bei einem bestimmten Gut, welches man mit der Hand angreifen kann, ist der Schaden, welcher durch die Verwendung einer Software entsteht, nur sehr ungenau zu ermitteln. Bei Software handelt es sich schließlich um ein Gut mit außergewöhnlichen Eigenschaften. Man kann nämlich Software nicht anfassen wie etwa ein materielles Objekt, wie beispielsweise einen Fotoapparat oder ein Auto. Deshalb begibt man sich oft in kontroverse Diskussionen, wenn man vom „Diebstahl einer Software“ spricht. Beim Diebstahl eines gewöhnlich materiellen Gutes besitzt der Dieb den entwendeten Gegenstand, der Bestohlene hat ihn jedoch nicht mehr. Wird hingegen eine digitale Datei kopiert, besitzt diese der Urheber nach diesem Vorgang weiterhin. Das Außergewöhnliche beim Herunterladen digitaler Daten ist, dass dabei gar nichts verloren geht, denn digitale Daten lassen sich endlos reproduzieren. Wenn man daher einen Schaden ermitteln möchte, gilt es zu klären, ob durch das widerrechtliche Kopieren von digitalen Daten, dem Urheber ein finanzieller Verlust entstanden ist. Von einem tatsächlichen Einnahmeverlust kann jedoch nur dann ausgegangen werden, wenn sich der User, welcher sich eine Kopie besorgt hat, die digitalen Daten auch tatsächlich gekauft hätte. Der reale Schaden, von welchem in Beziehung mit Raubkopieren immer gesprochen wird, ist daher eher als Gewinnausfall zu bezeichnen. Sehr oft sind es beliebte Programme, wie beispielsweise das populäre Programm Photoshop der Firma Adobe, welches massenweise raubkopiert wird. Diese Software kostet zirka um die 1499 Euro (derzeit Photoshop CS3 Extended Version), wenn sie neu auf den Markt kommt. Worüber die meisten jedoch ungern sprechen, ist

die belegte Tatsache, dass sich die meisten der illegalen Kopierer es sich nicht leisten könnten, derart teure Programme zu erwerben. In vielen Fällen handelt es sich nämlich um Studenten, welche sich zu Studienzwecken Software kopieren, da sie noch nicht über die nötigen finanziellen Mittel verfügen, um sich solche Produkte leisten zu können [Doub03].

Einige Computeranwender gehen wiederum nur einem digitalen Sammeltrieb nach. Diese Nutzer kopieren Tausende von Filmen und Musikalben aus dem Netz, ohne jemals alle digitalen Daten konsumieren zu können. Bei dieser Art von notorischen Sammlern würde keinesfalls jede downgeladete digitale Datei einem realen Kauf gleichkommen. Vor allem viele Schüler lagern oft unzählige illegal kopierte Filme und MP3-Dateien auf ihren Festplatten. Der reale Kaufpreis dieser gesammelten digitalen Daten übersteigt dabei ein Vielfaches ihres Taschengeldbudgets. Das sehr oft verwendete Argument, dass ein kleines Budget oder ein extremer Sammeltrieb keinen Raub rechtfertigen können, ist im Bereich von digitalen Daten umstritten. Denn in der digitalen Welt kann ein realer Schaden nur dann entstehen, wenn potentielle Käufer verloren gehen, welche durch eine Raubkopie auf den tatsächlichen Kauf der Daten verzichten.

Die dabei angewandten Berechnungsmethoden eines tatsächlichen Verlustes durch das Ausbleiben von Verkäufen gleichen meistens einem Ratespiel. Die meistzitierten Zahlen, welche von den Medien veröffentlicht werden, kommen vom weltweiten Industrieverband BSA. Dieser veröffentlicht Jahr für Jahr die so genannte „Piracy Study“, in welcher Angaben über die weltweite Verbreitung illegaler Softwarekopien und den daraus folgenden Gewinneinbussen für die weltweite Contentindustrie gemacht werden. Die aktuellen Werte für das Jahr 2005 wurden vom Marktforschungsinstitut IDC (International Data Corporation) ermittelt, welches jährlich von der BSA damit beauftragt wird [BSAS05].

Die Aufgabe der IDC war dabei, den kompletten Schaden für das Jahr 2005 zu ermitteln, welcher der Softwareindustrie durch Raubkopien entstanden war. Um dies zu bewerkstelligen, versuchte die IDC zu ermitteln, wie viel Software von den Menschen auf der ganzen Welt im Jahr 2005 eingesetzt worden war. Hierzu bediente sich das Marktforschungsinstitut Studien und Interviews, um den durchschnittlichen Softwarebedarf eines normalen PCs zu ermitteln. Dabei stellt sich die Frage, ob es überhaupt möglich ist, durch die verwendeten Mittel solche Zahlen zu bestimmen. Weiters ermittelte die IDC, wie viel Software im Jahr 2005 legal verkauft wurde. Wenn

nun im Einzelfall der Softwarebedarf eines normalen PCs höher war als die Verkaufszahlen, so musste nach Logik der IDC raubkopierte Software benutzt worden sein. Es sei ja mehr Software verwendet worden, als im selbigen Jahr verkauft wurde. Die Anzahl der nach diesem Rechenschema nicht verkauften Softwareprodukte ergab die Menge der Schwarzkopien. Des Weiteren wurde angenommen, dass jede Raubkopie einen wirtschaftlichen Schaden in der Höhe ihres tatsächlichen Verkaufspreises verursachen würde. Dieses Zahlenspiel der BSA wurde im Mai des Jahres 2006 als offizielle Statistik veröffentlicht. Laut dieser Publikation wurden 35% illegale Softwareprodukte auf PCs verwendet, was demzufolge einen realen Schaden in der Höhe von 34 Milliarden US-Dollar für die Softwareindustrie im Jahr 2005 entspricht [BSAS05, 1-11].

Bei dieser Datenerhebung bemängeln Kritiker, dass bei der Schätzung des Gesamtbedarfs von Software keine Open-Source-Produkte einkalkuliert worden waren, welche bekannter Weise kein Geld kosten. Es sollen beispielsweise der frei erhältliche Internetbrowser Firefox und das ebenso kostenlos beziehbare Open-Office-Paket mit einem Geldwert in den Gesamtschaden eingerechnet worden sein [Joos05]. Weiters wurde nicht berücksichtigt, dass viele Softwarenutzer auch ältere Versionen eines bestimmten Softwareproduktes verwenden. Wenn daher ein Softwareanwender ein Grafikprogramm im Jahr 2004 erworben, im Jahr darauf jedoch kein neues Update gekauft hatte, war diese Tatsache für das Marktforschungsinstitut Anlass genug, anzunehmen, dass der Kunde seinem Gesamtbedarf an Software nicht nachgekommen sei. Die Untersuchung schlussfolgerte somit, dass der Softwareanwender im Jahr 2005 eine Raubkopie benutzt hatte. In Prozenten ausgedrückt, ergab die so berechnete Anzahl an Raubkopien die „Piraterierate“. Auf Basis dieser Berechnungen gibt die BSA ebenfalls den Schaden an, welcher durch Raubkopierer in den untersuchten Ländern verursacht wurde. Dazu multiplizierte das Marktforschungsinstitut einfach die berechnete Anzahl an Raubkopien mit einem durchschnittlich ermittelten Verkaufspreis. Das Ergebnis dieser Berechnungsmethode sind astronomische Summen, welche der Softwareindustrie jährlich verloren gehen. Laut dem Wissenschaftler Steve Lohr stellen jedoch nur rund ein Zehntel der Raubkopien einen tatsächlich verlorenen Kauf und somit einen konkreten Umsatzverlust dar [Lohr04, 8].

Die BSA nutzt ihre so ermittelten Daten indessen zur politischen Einflussnahme. So werden derzeitige Diskussionen über härtere Strafen für Raubkopierer nicht unmaßgeblich von den BSA-Studien beeinflusst. Auf der ganzen Welt betreibt die BSA

schon seit längerer Zeit aktive Lobbyarbeit und verwendet ihre imposanten Zahlen, um Verfahren oder Gesetzesanträge zu untermauern. Da solche konkreten Angaben über Raubkopien beinahe ausschließlich von der BSA vorgestellt werden, bestimmen diese Berechnungen, so kurios sie auch sein mögen, fast ausnahmslos die öffentliche Berichterstattung.

Softwarehersteller, Filmverleiher und Plattenfirmen beklagen seit vielen Jahren sehr hohe Umsatzeinbußen, welche ihnen angeblich durch Raubkopierer entstehen. Im Besonderen geriet die Musikindustrie fast gleichzeitig mit dem Aufkommen des Internets in eine gewaltige Umsatzkrise. Im Jahr 1996 verzeichnete die Musikindustrie noch weltweit einen Umsatz von 39 Milliarden US-Dollar, im Jahr 2004 lag dieser Wert nur noch bei 32 Milliarden Dollar [Benj03, 72-78; Chip05]. Infolgedessen wurden Tausende von Mitarbeitern der Plattenfirmen entlassen, um diese Umsatzeinbußen zumindest teilweise kompensieren zu können.

Häufig betonen die einzelnen Vertreter der Industrieverbände den Einfluss der Raubkopien, welcher sich angeblich verheerend auf ihre Umsatzzahlen auswirken soll. Im Besonderen durch die Entstehung des Internets, welches all seinen Benutzern die Gelegenheit bietet, illegal Kopien zu tauschen, soll der Hauptgrund für die Krise der Unterhaltungsindustrie sein. Wenn man sich die nackten Zahlen vor Augen hält, erscheinen sie auf den ersten Blick tatsächlich bedrohlich. Die Brennerstudie aus dem Jahr 2006 der Gesellschaft für Konsumentenforschung (GfK) zeigt, dass allein in Deutschland die Zahl der mit Musik bespielten Leer-CDs in den Jahren 1999 bis 2005 von 58 auf 275 Millionen stieg. Demzufolge wurden im Jahr 2005 mehr als 275 Millionen CD-Rohlinge und 21 Millionen DVD-Rohlinge mit Musik bespielt. Dies entspricht unter der Annahme, dass man auf eine DVD die 7,8-Fache Datenmenge speichern kann, insgesamt 439 Millionen CD-Äquivalenten. Im gleichen Zeitraum ging die Anzahl der verkauften Musikalben von 198 auf 123,7 Millionen zurück. Daher wurden laut der GfK im Jahr 2005 alleine in Deutschland 882 Millionen bespielbare CDs von Computeranwendern gebrannt. Außerdem stellte die GfK Studie bei ihren Befragungen einen eindeutigen Einfluss des Raubkopierens auf die Verkaufszahlen fest. Die Downloader und Brenner von Musik im Jahr 2005 zeigten einen stärkeren Rückgang ihrer gesamten Ausgaben für Musik, als dies insgesamt am Markt festzustellen war. Immerhin geben rund 20% aller befragten Personen an, ihren Gesamtbedarf an Musik durch das Herunterladen und anschließende Brennen von Musik zu befriedigen [GfK06, 1-59]. Aus der Perspektive der Contentindustrie sind

solche exorbitanten Zahlen Grund genug, fast die vollständige Schuld an ihren Umsatzeinbußen den Raubkopierern zu geben.

Wirtschaftlich betrachtet ist es jedoch mehr als fraglich, ob tatsächlich Raubkopien alleine für das vollständige Ausmaß der Krise verantwortlich sind. In Fachkreisen ist es nämlich umstritten, inwieweit illegale Kopien aus Filesharingnetzwerken die Anzahl der legalen Käufe negativ beeinflussen.

Die beiden Wirtschaftsprofessoren Patrick Waelbroeck und Martin Peitz veröffentlichten im Jahr 2004 eine Studie, in welcher sie die tatsächlichen Auswirkungen von Internetdownloads auf Musikalbenverkäufe untersuchten. Sie kamen bei ihrer Studie zu dem Schluss, dass die einzelnen Downloads zwar für einen Großteil der Umsatzeinbußen des Jahres 2001 verantwortlich gemacht werden können, nicht jedoch für den Rückgang der Musikalbenverkäufe im Jahr 2002. Dafür sind laut ihnen andere Ursachen verantwortlich. Beispielsweise kann angenommen werden, dass mit der stärkeren Nutzung des Mediums Internet der gesamte Musikkonsum zurückgegangen sei. Infolgedessen wurden vermehrt Onlineaktivitäten nachgegangen, wie dem Anschauen von Videoclips, dem Chatten oder dem ungezielten Internetsurfen [PeWa04].

In diesem Zeitraum untersuchte ebenfalls Felix Oberholzer-Gee von der Harvard Business School und sein Kollege Koleman Strumpf von der University of North Carolina die Auswirkungen von Filesharing auf den Verkauf von Musik. In ihrer Analyse verglichen sie den Verkauf von Musik-CDs in den Vereinigten Staaten im Jahr 2002 mit der Anzahl der heruntergeladenen Musikdateien in Filesharingnetzen. Laut ihrer Studie hatten selbst hohe Downloadraten kaum einen Einfluss auf die Verkaufszahlen. Der größte Teil der Internetnutzer hätte sich die entsprechenden Musikalben ohnehin nicht gekauft. Selbst bei pessimistischer Schätzung ergäben erst 5.000 Downloads einer Musikdatei nach Meinung der Wirtschaftswissenschaftler den Verlust einer real gekauften Musik-CD [ObSt04]. Im direkten Vergleich zu diesen Zahlen weist die „Brennerstudie 2006“ der GfK für Deutschland etwa 512 Millionen Musikdownloads im Jahr 2005 aus. Laut der Behauptung der beiden Professoren würde das einen realen Verlust von nur 102.400 Musikalben bedeuten.

In der Studie stellte man sogar fest, dass sich Filesharing für die Musikalben, welche sich im Untersuchungszeitraum am meisten verkauften, sogar positiv auswirkt. In diesen Fällen erhöhten bereits 150 Downloads eines einzelnen Musikstückes die realen Verkäufe des jeweiligen Musikalbums um ein Exemplar. Für die populärsten

Musikalben wirkte daher die Nutzung von Filesharing wie eine Art Verstärker für die tatsächlich verkauften Musik-CDs. Lediglich für die Verkäufe der weniger beliebten Musikalben konnte nachgewiesen werden, dass durch Downloads die Verkaufszahlen negativ beeinflusst wurden. Aufgrund der Ergebnisse ihrer Studie kamen die beiden Wissenschaftler zu dem Schluss, dass die Nutzung von Filesharingbörsen höchstens für einen geringen Teil der Umsatzeinbußen der Musikindustrie verantwortlich sind [ObSt04].

Im Juni des Jahres 2005 bestätigte selbst die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) diese Bewertungen. Sie kam in einer aufwendigen Analyse des Onlinemusikhandels zu dem Ergebnis, dass ein ursächlicher Zusammenhang zwischen dem Anstieg der Tauschbörsennutzung und den Umsatzeinbußen der Musikindustrie nicht nachweisbar sei. Eher kommen sie zu dem Resultat, dass andere Ursachen für den Umsatzeinbruch verantwortlich sind. Diese wären beispielsweise die mangelhafte Qualität und Verfügbarkeit der legal geführten Downloadportale sowie eine wachsende Konkurrenz von anderen Formen der Unterhaltung, wie DVD-Filme oder Computerspiele [WuVi05].

Ausgerechnet von Bill Gates wird die Äußerung aus den 90er Jahren überliefert, dass Raubkopien Microsoft bei dem Einstieg in den chinesischen Markt geholfen hätten. Nachdem die Menschen in China sich langsam mit der Software vertraut machten und so auf den Geschmack gekommen waren, konnte man Wege finden, um diesen Trend auch in ertragreiche Erlöse umzuwandeln [Econ05].

Inzwischen wird jedoch die positive Sichtweise auf Raubkopien bei dem Softwaremonopolisten verschwiegen. Unter bestimmten Umständen kann die Softwareindustrie tatsächlich von illegal gemachten Kopien profitieren, da diese unter Umständen auch solche Computeranwender an ein Softwareprogramm heranzuführt, welche nicht zur potentiellen Käuferschicht zählen. Viele der großen Softwareunternehmen verkaufen auch ihre Produkte an Studenten zu verhältnismäßig günstigen Preisen. Die einzelnen Unternehmen gehen dabei von der Annahme aus, dass manche von den Studenten nach ihrem Universitätsabschluss Entscheidungsträger in größeren Unternehmen werden. Die Manager entscheiden erfahrungsgemäß über den massenhaften Erwerb von Lizenzen meistens aufgrund ihrer persönlichen Erfahrung mit den Produkten. Ebenso könnte es auch durchaus sein, dass ein Student viele Jahre die Raubkopie einer teuren Software benutzt, da er sich die Originalversion nicht leisten kann. Viele Jahre später, wenn er dann im Berufsleben ist, kauft er sich dann die

aktuelle Version der Software, weil er nun über die erforderlichen finanziellen Mittel verfügt. Für ein bestimmtes Unternehmen muss es nicht zwangsläufig schlecht sein, wenn eine hohe Anzahl von Raubkopien ihrer Software im Umlauf ist. Denn durch diesen Umstand erhöht sich der Bekanntheitsgrad ihres Produktes, was bei einer Marktdurchdringung des jeweiligen Programms behilflich sein kann.

Selbst die angeschlagene Musikindustrie kann von solchen Effekten profitieren. Zwar können auf der einen Seite durch den massenhaften illegalen Download von Musikfiles Umsätze verloren gehen. Auf der anderen Seite werden jedoch auch viel mehr Menschen auf die jeweiligen Musikalben aufmerksam. Dies kann soweit führen, dass sich diese Personen möglicherweise das Nachfolgealbum erwerben oder nachträglich das Konzert des Künstlers besuchen.

Aus den USA, dem größten Musikmarkt auf der Welt, werden inzwischen wieder steigende Verkaufszahlen gemeldet, obwohl die Filesharingnutzung weiter steigt [StHH05]. Doch auch in anderen Kontinenten werden wieder mehr Musikalben abgesetzt. In jenen Ländern, welche weiter mit rückläufigen Umsätzen zu kämpfen haben, scheinen sich zumindest die Umsatzverluste zu verlangsamen.

Während einerseits die Verkaufszahlen wieder ansteigen, steigt andererseits die Anzahl der illegalen Downloads rasant an. Diese neuen Zahlen widersprechen daher der gängigen These der einzelnen Plattenfirmen, dass vor allem das Medium Internet mit seinen Filesharingnetzen für ihre enormen Umsatzrückgänge verantwortlich sei. Deshalb befindet sich die Musikindustrie aufgrund dieser neuen Fakten in Erklärungsnot.

Jedoch auch der Filmindustrie geht es ungeachtet der steigenden Filesharingnutzung wieder besser. Die Kinos in Deutschland verzeichneten sogar im Jahr 2005 rund fünf Millionen Kinobesucher mehr als im Jahr zuvor, was in etwa einem Umsatzplus von 8,9% entspricht [FFAi06]. Im Jahr 2004 sind in der EU zum zweiten Mal in der Geschichte seit 1990 über eine Milliarde Besucher in die Kinos gegangen [EuAV05].

In den vergangenen Jahren stiegen jedoch vor allem die DVD-Verkäufe drastisch an. In Deutschland hat sich dank des neuen Mediums DVD sogar der gesamte Umsatz der Heimvideobranche innerhalb weniger Jahre in etwa verdoppelt [Spät05]. Durch die Verkäufe von DVDs verdient die Filmbranche zwei bis dreimal so viel, wie sie an den Kinokassen einnimmt [BeSWO5, 128]. Auch der Computer- und Videospieleindustrie ergeht es nicht viel schlechter. Ihre Umsätze steigen ungeachtet der steigenden Anzahl

von illegalen Raubkopien seit Jahren kontinuierlich an und liegen inzwischen bereits betragsmäßig über denen der Filmindustrie [Spät05].

Die immer vorgebrachte Behauptung vom großen Schaden, welcher durch das illegale Kopieren beim Filesharing jedes Jahr verursacht wird, scheint daher nicht gerechtfertigt zu sein. Produktionsfälschungen und professionelle Kopien, welche auf Schwarzmärkten weltweit vertrieben werden, stellen nämlich eine weitaus größere Bedrohung dar als die täglichen Internetdownloads. Wie groß aber der tatsächliche Einfluss der digitalen Raubkopierer ist und inwieweit er sich wirklich auf die Umsätze der Industrie auswirkt, wird sicherlich noch weiterhin ein Bestandteil von kontroversen Diskussionen bleiben.

Wenn man die Geschichte der Musikindustrie näher betrachtet, brachen die erwirtschafteten Umsätze schon früher einmal stark ein. Dies war in den 20er Jahren der Fall, als zum ersten Mal Radios Einzug in die einzelnen Haushalte fanden, wodurch es den Menschen ermöglicht wurde, Musik nicht mehr zwangsläufig kaufen zu müssen, da sie kostenlos über Radiowellen zu ihnen nach Hause kam. Die Musikindustrie hat daher schon einige Erfahrungen sammeln können, inwieweit man auf erstmalige technische Innovationen reagieren sollte. Um daher mit den Musiktäuschbörsen im Internet konkurrieren zu können, hätte man daher rechtzeitig neue Verkaufsstrategien entwickeln müssen. Das renommierte Marktforschungsinstitut Forrester Research machte bereits im Jahr 2000 auf dieses Problem in einem Bericht über die einzelnen Auswirkungen des Medium Internets auf die Musikindustrie aufmerksam. Der Forrester Analyst Eric Scheirer fand damals schon heraus, dass das Bedürfnis, Musik zu sammeln und zu organisieren, individuelle CDs und Playlisten zu erstellen und die eigenen Lieblingsstücke tausende Male abzuspielen, den größten Teil der Faszination von Filesharing ausmacht. Bereits damals hielt es Scheirer für notwendig, dass die einzelnen Musiklabels die Wünsche der einzelnen Kunden akzeptieren und dementsprechend auf sie eingehen [OutL05]. Wenn man eine Raubkopie rein wirtschaftlich betrachtet, ist es mit dem Original ein identisches Produkt zu einem wesentlich günstigeren Preis. Da es jedoch auch in der Zukunft kaum möglich sein wird, das Raubkopieren technisch oder rechtlich ganz zu unterbinden, müssen sich die einzelnen Unternehmen mit marktwirtschaftlichen Maßnahmen den Kampf gegen die Raubkopierer aufnehmen. Dies kann jedoch im Bereich der Musik nur dann tatsächlich gelingen, wenn rechtmäßig erworbene MP3-Dateien einen klaren Mehrwert aufweisen. Eine riesige Auswahl an angebotenen Musikstücken und eine für den Endverbraucher einfache Bedienbarkeit

sind unabdingbar für ein legales Angebot, welches Filesharing Konkurrenz machen soll. Es dürfen vor allem keine Einschränkungen, wie es zum Beispiel mittels DRM gemacht wird, die Nutzer davor abschrecken, dieses Angebot in Anspruch zu nehmen.

Selbst als die bekannte Tauschbörse Napster im Internet Millionen von Usern in kürzester Zeit anlockte und es offensichtlich wurde, dass eine enorme Nachfrage nach Musikfiles im MP3-Format bestand, gaben die Musiklabels ihre ablehnende Haltung gegenüber diesen Formates nicht auf. Stattdessen überzog sie Napster mit Urheberrechtsklagen, ohne jedoch den aktiven Nutzern eine legale Alternative anzubieten. Die Musikindustrie hatte jedoch damals eine andere Meinung. Anstatt sich mit den neuen Technologien anzufreunden und darauf aufbauend ganz neue Geschäftsmodelle zu entwickeln, hielt sie an der alten Technologie fest. Die Musikindustrie versuchte stattdessen, sich der Internetrevolution zu entziehen und wurde aufgrund dieser Tatsache von ihr überrollt. Daraufhin brachen die Umsätze ein und die Musik-CD, welche jahrelang so erfolgreich vermarktet wurde, war von einem Moment auf den anderen nicht mehr von so großer Bedeutung.

Wie den großen Plattenfirmen langsam klar wurde, dass sie den bisher geführten Kampf gegen die Masse der Filesharer nicht mit klassischen Methoden gewinnen konnten, begingen sie einen weiteren, schwerwiegenden Fehler. Sie erklärten dem illegalen Download von Musikfiles den Krieg. In diesem Zusammenhang übersahen sie jedoch völlig die Tatsache, dass 80% der Filesharer trotz des Mediums Internet auch weiterhin Musik-CD-Käufer waren [GfK06]. Die Musikindustrie hatte durch diese Maßnahmen den Kampf gegen ihre eigenen Kunden angesagt. Das Hauptproblem dabei ist, dass man in jenem Augenblick, in welchen man die Verkaufsmechanik am Dieb ausrichtet und nicht an dem Kunden, macht man es den Kunden ziemlich ungemütlich, da er wie ein gewöhnlicher Dieb behandelt wird [Renn05].

Ob sich die beträchtlichen Umsatzrückgänge der großen Musiklabels mit wenigen Fakten erklären lassen, bleibt weiterhin offen. Zu den Fehlentscheidungen der Musikwirtschaft kam ein zunehmender Wettkampf mit anderen Unterhaltungsformen (DVD-Filme, Mobiltelefone, Videospiele) und eine generell schlechte wirtschaftliche Lage. Es bleibt daher weiterhin offen, ob es überhaupt jemals einen kausalen Zusammenhang zwischen der massenhaften Verbreitung von Raubkopien durch Filesharing und den großen Umsatzeinbußen der Unterhaltungsindustrie überhaupt gegeben hat. In welchem Ausmaß ein eventuell verursachter Schaden durch Raubkopierer entsteht, wird wohl kaum jemals geklärt werden können. Doch angesichts

der entsetzlichen Fehler, welche die Unterhaltungsindustrie in den letzten Jahren begangen hat, ist jedoch stark anzunehmen, dass Raubkopien, welche über Filesharingnetzwerke getauscht werden, nur einen geringen Teil der Umsatzeinbußen erklären können.

11 Zusammenfassung und Fazit

„Aber all diese neuen Technologien, Verschlüsselungen und Gesetze werden die Datenpiraterie nicht beenden. Die Schlacht wird einfach weitergehen. Es liegt in der Natur des Internets, dass es keine Gesetze kennt. Das Netz ist auf den freien Austausch von Information ausgerichtet – wobei hier die Betonung auf „frei“ liegt. So lange es einen Markt gibt, wird es daneben auch einen Schwarzmarkt geben.“ [McCa01, 11].

„..., wie alle aktuellen Erhebungen (GfK, W3B, @Facts) belegen: 50% der Internet-Nutzer sind grundsätzlich bereit, für den Inhalt und Services im Internet auch etwas zu zahlen.“ [Pico03, 171].

Die derzeit am Markt vertretenen Filesharingnetzwerke führen Angebot und Nachfrage von beliebigen Daten, gleich ob urheberrechtlich geschützt oder nicht, millionenfach zusammen. Durch die ständige technische Entwicklung bei Peer-to-Peer Systemen, welche den Tausch von Daten noch einfacher und schneller machen sollen, ist der Datenaustausch unkompliziert und in kürzester Zeit möglich geworden. Weder die Rechteinhaber, sonstige Organisationen oder offizielle Stellen sind derzeit in der Lage, den Datenaustausch von urheberrechtlich geschütztem Material effektiv zu überwachen. Die zunehmend dezentrale Struktur, welche die Tauschbörsen aufweisen, bietet juristisch wenig Angriffsflächen; der Trend weist auch dahin, dass der einzelne Nutzer weitgehend anonym Daten tauscht. *„Entscheidend für die Zukunft von P2P wird sich wohl die Frage nach Sicherheit und Privatsphäre herausstellen. Der freie Austausch widerspricht nicht nur dem wirtschaftlichen Gewinnerzielungsprinzip, sondern ist auch gegenläufig zum Wunsch nach Sicherheit.“ [Müll03, 644].*

Die Industrie entwickelt bereits heute zuverlässige DRM-Systeme, welche zum Teil schon eingesetzt werden. In Zukunft werden daher wohl immer mehr digitale Werke mit solchen technischen Schutz- und eventuell auch Individualabrechnungssystemen versehen werden. Die Computertechnologie eröffnet heute nahezu unbegrenzte Möglichkeiten, digitale Inhalte zu nutzen. Autoren und Urheber erwarten jedoch, dass die Computertechnologie auch hilft, ihre entwickelten Inhalte zu schützen. Digital Rights Management (DRM) ist in diesem Zusammenhang die Zukunft in punkto sicherer Verwaltung digitaler Nutzungsrechte.

Durch die explosionsartige Verbreitung des Mediums Internet und der anwachsenden Bedeutung digitaler Medien, wird das bestehende Urheberrecht an den Rand seiner Existenzberechtigung gedrängt. Auf der einen Seite wird in der heutigen Informationsgesellschaft das Gut „Information“ immer wichtiger. Auf der anderen Seite wird das Vervielfältigen der Information immer unkomplizierter. Um mit dieser Problematik fertig zu werden, enthält das bestehende Urheberrecht eine Fülle von Ausnahmen. Die einzelnen Details sind für die meisten Privatanwender nicht bekannt oder nur schwer durchschaubar.

Ob es sich bei einer erstellten Kopie um eine legale oder rechtswidrige Raubkopie handelt, hängt immer von der Art der Herstellung und von deren Nutzung ab. Daher muss jeder einzelne Sachverhalt separat betrachtet werden, um eine objektive Aussage tätigen zu können. Denn eine legal kopierte Kopie eines Musikalbums für private Zwecke, wird zum Beispiel zu einer Raubkopie, wenn man sie auf einem Flohmarkt verkaufen würde. Seit der letzten Urheberrechtsreform im Jahre 2003 ist laut den §90b UrhG und §90c UrhG das Umgehen eines Kopierschutzes verboten. Weiters sind ab diesem Zeitpunkt Kopierprogramme, welche das Herstellen solcher Kopien ermöglichen, nicht mehr für den Verkauf oder die legale Verbreitung zugelassen. Selbst das Publizieren von Anleitungen, in welchen der Vorgang des Umgehens eines Kopierschutzes beschrieben wurde, war ab dieser Novellierung illegal. Streng genommen ist daher das Verschenken einer älteren Computerzeitschrift strafbar, wenn sie solche Anleitungen enthalten sollte. Ein Großteil der Anbieter solcher Software musste daraufhin ihre Geschäfte aufgeben oder in ein Land verlagern, in welchem die Gesetzeslage eine Umgehung des Kopierschutzes nicht verbietet: Ein bekanntes Beispiel ist die Firma „Slysoft“, welche ihre in Deutschland illegal gewordene Software seither von der Karibikinsel Antigua aus verkauft.

Die Reformierung des aktuellen Urheberrechtsgesetzes ist durch solche Maßnahmen noch lange nicht abgeschlossen. Im Jahr 2003 wurden nämlich nur jene Paragraphen der EU-Richtlinie umgesetzt, welche für die einzelnen EU-Mitglieder zwingend vorgeschrieben waren. Es werden auch weiterhin die unterschiedlichen Ansichten der jeweiligen Interessensverbände aufeinanderprallen. Die Privatanwender werden auch in Zukunft gegen eine Kriminalisierung von Filesharingprogrammen und sich für eine Erstellung einer Privatkopie einsetzen. Die Contentindustrie hingegen fordert noch schärfere Gesetze und ein noch effektiveres Vorgehen gegen Tauschbörsenbenutzer,

welche illegale Inhalte downloaden. Weiters würde sie eine völlige Abschaffung der Privatkopie begrüßen.

Aufgabe der nationalen und europäischen Gesetzgeber ist es dann, vor allem die Ausgleichsfunktion des Urheberrechtes weiterhin zu garantieren und neben den Interessen der Rechteinhaber und Verwerter auch die Schranken, besonders die Schranke der privaten Kopie effizient zu bewahren.

Aufgrund der obigen Erörterungen steht daher fest, dass auch die Einführung technischer Schutzmaßnahmen wie Kopierschutz oder DRM-Systeme kein vollständiges Verbot der digitalen Privatkopie rechtfertigen kann. Da ein Verbot der digitalen Vervielfältigung im Ergebnis nicht angezeigt ist, stellt sich die Frage, ob und gegebenenfalls in welcher Form die geschilderten Auswirkungen der Digitaltechnik sonst berücksichtigt werden sollten. Dabei muss eine Lösung gefunden werden, welche einen gerechten Ausgleich der Interessen gewährleistet, gleich ob zukünftig bestimmte Werke wirksam technisch geschützt sind oder nicht. Es bietet sich an, eine solche Lösung über das bereits bestehende Vergütungssystem bei Privatkopien zu suchen.

Gesetzliche Regelungen können nicht mit dem raschen technischen Fortschritt, welcher in diesem Bereich stattfindet, mithalten. Es müssen daher Regelungen und Wege gefunden werden, welche es den Gesetzgebern ermöglichen rasch auf solche Ereignisse reagieren zu können, ohne durch die bürokratischen Hürden ausgebremst zu werden.

Die internationalen Bestrebungen, denen gerade in einem so stark grenzüberschreitenden Netzwerk überragende Bedeutung zukommt, sind dagegen noch weit von einer Harmonisierung der Gesetze entfernt. So beschäftigt sich etwa die EU intensiv mit der Thematik, kann aber derzeit außer Empfehlungen an die Mitgliedsstaaten, enger zusammenzuarbeiten und die Kooperation stärker zu koordinieren, noch nichts in Richtung bindender Regelungen vorweisen. Auch die UNO und der Europarat beschäftigen sich in Expertenkomitees mit der Problematik, bis jetzt hat sich daraus aber noch nichts Umsetzbares entwickelt. Gerade in diesem Bereich der internationalen Zusammenarbeit ist aber die zentrale Entwicklung zu erhoffen. Ohne internationales Instrumentarium wird eine Bekämpfung unerwünschter Inhalte im Internet auch in weiterer Zukunft ineffizient bleiben. Es wäre daher sehr erstrebenswert, an den wichtigsten internationalen Bemühungen teilzunehmen, um eine grenzüberschreitende Verfolgung der „Internet-Delikte“ zu gewährleisten.

Mit Werbekampagnen wie „Raubkopierer sind Verbrecher“ versucht die Filmindustrie bereits seit Jahren, die einzelnen Verbraucher für das Thema der illegalen Kopie zu sensibilisieren. Anstatt jedoch Aufklärung zu betreiben, erntete die Kampagne größtenteils Unverständnis bei der Bevölkerung. In Anbetracht immer neuer Meldungen und Medienberichten von angeblichen Milliarden Schäden, welche die Industrie Jahr für Jahr erleidet, gerät auch das Wort „Raubkopie“ zunehmend in die Kritik. Aber nicht nur im allgemeinen Sprachgebrauch, sondern auch im juristischen Sinne ist mit dem Wort „Raub“ eine Form des Diebstahles gemeint, bei dem ein Gegenstand mit Gewalt entwendet wird. Beim illegalen Kopieren von Software, Musik oder Filmen kann hiervon jedoch keine Rede sein. Außerdem wird bei einem Diebstahl von der Tatsache ausgegangen, dass die beraubte Person den Gegenstand, welcher ihr entwendet wurde, nicht mehr besitzt. Bei einer digitalen Kopie bleibt jedoch das Original komplett erhalten [KrSe06, 10]. *„Analog zu den Vergehen des Schwarzfahrens und der Schwarzarbeit, die auch nicht »Raubfahren« oder »Raubarbeit« genannt werden, erscheint der Begriff »Schwarzkopie« weniger wertend als Bezeichnung für illegale Kopien.“* [KrSe06, 10]

Wie bereits öfters erwähnt, können ohne fachspezifisches Wissen heutzutage Musik, Software oder Filme aus dem Internet heruntergeladen werden. Breitbandinternet und DVDs perfektionieren das Kopieren von Filmen. Musikdateien lassen sich heute in 45 Sekunden und Kinofilme in weniger als zwei Stunden aus dem Internet ziehen. Neue Kompressionsverfahren und schnellere Internetzugänge werden diese Zeiten weiter verkürzen. Das Herunterladen von digitalen Daten geschieht dabei meist nicht aus kriminellen Motiven, sondern eher aus Unwissenheit und „weil es ja ohnehin jeder macht“. In diesem Bereich muss daher noch sehr viel Aufklärungsarbeit geleistet werden, um Internetnutzer nicht nur für neue Medien zu gewinnen, sondern sie auch für einen verantwortungsvollen und bewussten Umgang mit digitalen Daten zu sensibilisieren. Es ist daher sehr wichtig, ihnen ein Rechtsbewusstsein gegenüber den komplexen Themen des Urheberrechts und Copyrights zu vermitteln. Die einzelnen Nutzer sollen einsehen, dass illegale Kopien den Unternehmen, Künstlern und letztlich auch ihnen selbst schadet. Weiters sollten sie die rechtlichen Grundlagen zum Thema Urheberrecht kennen und den Zusammenhang zwischen neuen technologischen Entwicklungen und der Entstehung von neuem Regelungsbedarf verstehen. Das Endziel sollte daher sein, dass jeder Internetnutzer in der Lage ist, zwischen Recht und Unrecht

unterscheiden zu können. Dies soll ihm dabei helfen, ein Bewusstsein für die Notwendigkeit moralischen Verhaltens zu entwickeln, welches ihn dazu befähigt sein eigenes Fehlverhalten zu erkennen und die Bereitschaft aufzubringen, es notfalls auch zu korrigieren.

Was sich hier schon in den letzten drei Jahren bemerkbar gemacht hat, ist ein gewisser Bewusstseinswandel und ein Wirken der entsprechenden Wissensmodelle um Recht und Unrecht, die natürlich auch ein Umdenken bewirken. Das Entscheidende ist, dass alle Maßnahmen ineinander greifen. Nur, wenn rechtliche Rahmenbedingungen inklusive der effektiven Verfolgung kapitaler Delikte, technische Standards, realistische Businessmodelle und Maßnahmen zur Stärkung des Unrechtsbewusstseins, sinnvoll ineinander greifen, wird es spürbare Erfolge geben.

Der Preis einer Software zum Beispiel sollte so angesetzt werden, dass sich die Zielgruppe, für welche das Programm geschrieben wurde, diese auch leisten kann. Denn Raubkopierern sollte man dabei nicht so viel Beachtung schenken, denn sie machen die Software, ohne die Entstehung von zusätzlichen Kosten, mehr publik und erweitern so indirekt den Kundenstamm für das Produkt. Weiters sollte man viel mehr den Support der Software Beachtung schenken. Auf hochwertige Schulungen, Hotlines und Hilfen sollte dabei besonders geachtet werden, denn sie bringen einen zusätzlichen Profit für die Software ein. So könnte ein gutes Modell ausschauen. Mit Open Source und Linux funktioniert das bereits sehr gut, und dieses Marktsegment wächst ständig. Eine Software braucht daher einen ausgezeichneten Support. Personen, welche sich verpflichtet fühlen, sich die Software illegal zu beschaffen, müssen dann eben auf diesen verzichten.

Als Hauptursachen für den Schaden der Industrie werden die hohe Anzahl unrechtmäßiger Kopien physischer Tonträger sowie der umfangreiche Download über die freien Tauschbörsen angeführt. Allerdings sind auf dem Musikmarkt auch positive Signale zu erkennen. Die DVD gewinnt als Medium sowohl für Audio als auch Video immer mehr Abnehmer. Wenn man in diesem Zusammenhang von Schaden spricht, dann sollte nicht von dem Schaden, welcher durch die Verbände berechnet wird, gesprochen werden. Es ist nämlich sowieso sehr fragwürdig in diesem Bereich über Schaden zu sprechen, denn im kriminologischen Sinne ist es ein Kontrolldelikt. Jene

Zahlen, welche daher oft publiziert werden, können daher nicht zur Beurteilung der Lage herangezogen werden.

Immer mehr Bereiche unseres Lebens spielen sich in der digitalen Welt ab, werden von ihr berührt oder verlagern sich komplett in diese Welt. Der Erfolg dieser Entwicklung hängt direkt von der Frage ab, welchen Stellenwert diese digitale Welt in unserer Gesellschaft hat und haben wird. Es muss daher der Umgang mit geistigem Eigentum in der Erziehung einen festen Platz bekommen, sodass der Begriff des geistigen Eigentums seine Abstraktheit verliert und angreifbar wird.

Das Katz-und-Maus-Spiel von Hackern, Crackern und der Industrie wird weiter gehen. Ein Sieg der Industrie ist dabei nicht in Sicht, dazu ist die Anzahl der Downloadangebote, die Vielfalt der Inhalte und die Menge der aktiven Cracker viel zu groß, und die Signalwirkung der getroffenen Maßnahmen ist zu gering.

„All of our estimates of real Internet traffic, even based on simplistic port number analysis, confirm our hypothesis that P2P traffic is growing in volume and will continue to grow unabatedly in the future.“ [KaBF04, 134]. Das Interesse der Nutzer an einem Datenaustausch ist tendenziell steigend, da weltweit immer mehr Haushalte an das Internet angeschlossen werden. Die Datenmenge des getauschten, urheberrechtlichen geschützten Materials steigt kontinuierlich an. Ein Abflauen des Interesses an einem Tausch von digitalen Daten ist nicht in Sicht.

Ein Ende des Filesharings ist deshalb aus heutigen Gesichtspunkten nicht zu erwarten. Die Menschen teilen nämlich digitale Inhalte, weil das eine höhere Ebene darstellt, um ein bestimmtes Medium zu konsumieren.

Literaturverzeichnis

- [Alf199] Alflen, Manfred: Die Anforderungen des Informationszeitalters an (Aus)Bildung. In: Rutz, Michael: Die Byte-Gesellschaft – Informationstechnologien verändern unser Leben, Olzog Verlag München, 1999, S. 16-27.
- [AT06] @-WEB: Suchmaschinenindex, 2006.
<http://www.at-web.de/informationen/suchmaschinenindex.htm>
Abruf am 2006-11-15
- [Barl06] Perry, Barlow; Selling Wine Without Bottles. The Economy of Ideas, 2006,
<http://homes.eff.org/~barlow/EconomyOfIdeas.html>
Abruf am 2006-03-17
- [Baue04] Bauer, Wilhelm: Risiko beim Datenklau gleich null, Presstext.de, 23.04.2004,
<http://www.pressetext.at/pte.mc?pte=040423016>
Abruf am 2006-09-18
- [Bech02] Bechtold, Stefan: Vom Urheber- zum Informationsrecht – Implikation des Digital Rights Management. In: Thomas Hoeren et al. (Hrsg.): Information und Recht, Band. 33, München 2002
- [BeCl03] Becker, Jan U.; Clement, Michel.: Generation Napster – Das ökonomische Kalkül eines Anbieters von Medien-Dateien bei Filesharing-Diensten, In: Wirtschaftsinformatik 45 (2003) 3, S.261-271.
http://www.wirtschaftsinformatik.de/wi_artikel.php?sid=1207
Abruf am 2005-11-14
- [Benj03] Benjamin, Walter: Alles nur geklaut, Der Spiegel, 01.09.2003, S.72-78.
- [Berg99] Bergsdorf, Wolfgang: Medienethik in der Informationsgesellschaft. In: Rutz, Michael: Die Byte-Gesellschaft – Informationstechnologien verändern unser Leben, Olzog Verlag München, 1999, S. 261-277.
- [BeSW05] Beier, Lars-Olav; Schulz, Thomas; Wolf, Martin: Goldrausch mit Silberlingen, Der Spiegel, 13.06.2005, S.128

- [BKKM03] Balakrishnan, Hari; Kaashoek, M. Frans; Karger, David; Morris, Robert, Stoica, Ion.: An end-user perspective on file-sharing systems, In: Communication of the ACM, Publication Date: February 2003, p49-53.
<http://doi.acm.org/10.1145/606272.606300>
Abruf am 2006-11-11
- [BoNe01] Boehme-Neßler, Volker: Internetrecht, München, DTV-Beck Verlag, 2001,
- [BPJS05] Buxmann, Peter; Pohl, Gerrit; Johnscher, Patrick, Strube, Jochen.: Strategien für den digitalen Musikmarkt – Preissetzung und Effektivität von Maßnahmen gegen Raubkopien, In: Wirtschaftsinformatik 47 (2005) 2, S. 118-125.
http://www.wirtschaftsinformatik.de/wi_artikel.php?sid=1579
Abruf am 2005-11-15
- [Brig00] BrightPlanet: The Deep Web: surfacing hidden value, Study, 2000.
<http://www.completeplanet.com/tutorials/deepweb/summary03.asp>
Abruf am 2006-11-15
- [BSA05] Herrnleben, Georg: Business Software Alliance, Regional Manager Central Europe, München, 2005
<http://www.bsa.org/germany/presse/upload/Zum-Spot.mpa>
Abruf am 2006-09-21
- [BSAS05] O.V.: Second Annual BSA and IDC Global Software Piracy Study, 2005
<http://www.bsa.org/globalstudy/upload/2005-Global-Study-English.pdf>
Abruf am 2006-09-22
- [BUPW04] O.V.: Bundesverband der Phonographischen Wirtschaft: Phonowirtschaft verbucht mit -2,9% im 1.Halbjahr 2004 den geringsten Absatzrückgang seit 2000.
<http://www.ifpi.de/news/news-411.htm>
Abruf am 2006-11-15
- [ByMC04] Byron, Simon; Mehlman, Simon; Chuang, Miao: 52 Per Cent of Gamers Admit to Piracy, London, Macrovision.com, 11.06.2004,
<http://www.macrovision.com/company/news/press/newsdetail.jsp?id=Fri%20Jun%2011%2010:18:05%20PDT%202004>
Abruf am 2006-09-14

- [Cach06] O.V.: The True Picture of Peer-to-Peer Filesharing, Cachelogic.com, Juli 2004,
<http://www.cachelogic.com/home/pages/research/index.php>
Abruf am 2006-09-14
- [CEN03] O.V.: Draft Report Digital Rights Management, 2003
<http://www.cenorm.be/cenorm/businessdomains/businessdomains/iss/ activity/cenissdrmareportfinal30october2003.zip>
Abruf am 2006-02-12
- [Chip05] O.V.: Musikbranche: Online-Umsatz dammt Verluste ein, CHIP Online, 19.01.2005,
http://archiv.chip.de/news/c1_archiv_news_17190009.html
Abruf am 2006-09-25
- [Cire97] Ciresa, Meinhard: Urheberrecht aktuell, Wirtschaftsverlag C. Ueberreuter, 1997
- [CoMB02] Cox, Ingemar; Miller, Matthew; Bloom, Jeffrey: Digital Watermarking, Morgan Kaufmann Publisher, San Francisco, 2002
- [Cyve06] O.V.: Cyveillance: Cyveillance Web Study, 2006.
http://www.cyveillance.com/web/us/forms/request.asp?form=type=download_wp&wp=study
Abruf am 2006-11-15
- [Dern03] Dernbach, Christoph: Erfolg von Apples Online-Musikshop uberrascht die Musikindustrie. Heise Zeitschriften Verlag, 2003-05-06,
<http://www.heise.de/newsticker/meldung/36633>
Abruf am 2006-09-01
- [Dete01] Detering, Dieter: Okonomie der Medieninhalte. Allokative Effizienz und Soziale Chancengleichheit in den neuen Medien
<http://www.medieninhalte.de>
Abruf am 2006-04-12
- [Ditt00] Dittmann, Jana; Digitale Wasserzeichen – Grundlage, Verfahren, Anwendungsgebiete, Springer Berlin 2000

- [Dona01] Donath, Andreas: Studie zum Thema „Internet als Kontaktbörse“,
golem.de, 26.01.2001,
<http://golem.de/0101/11947.html>
Abruf am 2006-09-18
- [Döri03] Döring, Nicola: Sozialpsychologie des Internet, Die Bedeutung des
Internet für Kommunikationsprozesse, Identitäten, soziale Beziehungen
und Gruppen, 2. Auflage, Ilmenau, 2003,
- [Doub03] Douban, Basma: Targum, Daily: Rutgers students react to piracy issues,
threats, U-Wire, New Brunswick, New York, 02.10.2003
- [DrHa03] Drösser, Christoph; Hamann, Götz: Die Jobs-Maschine. In: Die Zeit,
15.05.2003, S.19-20.
- [Dust01] Dustmann, Andreas: Die privilegierten Provider, Baden-Baden, 2001
- [EbQu04] Eberspächer, Jörg; Quadt Hans-Peter: Breitband- Perspektiven, Springer
Verlag Berlin Heidelberg, Münchner Kreis, 2004.
- [Econ05] BSA or just BS, The Economist print edition, 19.05.2005
http://www.economist.com/business/displayStory.cfm?story_id=3993427
Abruf am 2006-09-26
- [EFF06] O.V.: State-Level "Super DMCA" Initiatives Archive, Electronic Frontier
Foundation, 2006,
<http://www.eff.org/IP/DMCA/states/>
Abruf am 2006-03-07
- [EnBV02] Ensthaler, Jürgen; Bosch, Wolfgang; Völker, Stefan.: Handbuch
Urheberrecht und Internet, Verlag Recht und Wirtschaft GmbH,
Heidelberg, 2002.
- [EuAV05] O.V.: Über eine Milliarde Kinobesuche belegen lebhaftere Entwicklung der
großen Märkte in der Europäischen Union, Europäische Audiovisuelle
Informationsstelle, 04.05.2005,
www.obs.coe.int/about/oea/pr/mif2005pdf.pdf.de
Abruf am 2006-09-27

- [Faiß00] Faißnerl, Klaus: 1,3 Mrd. Schilling Schaden durch Raubkopien in Österreich, Presstext Austria, 28.11.2000
<http://www.pte.at/pte.mc?pte=001128050>
Abruf am 2006-09-21
- [FFAi06] O.V.: Das offizielle Kino-Ergebnis 2005, FFA info Nr. 2/06, 09.02.2005,
http://www.filmfoerderungsanstalt.de/downloads/publikationen/ffa_intern/FFA_info_2_2006.pdf
Abruf am 2006-09-27
- [Fiut04] Fiutak, Martin: Studie: Deutsche Surfer tauschen MP3s trotz Unrechtsbewusstseins, ZDNET, 23.01.2004,
<http://www.zdnet.de/news/tkomm/0,39023151,39119167,00.htm>
Abruf am 2006-09-18
- [Frän03] Fränkl, Gerald.: DRMS. Pg-Verlag Fränkl u. Karpf GbR, 2006,
<http://www.digital-rights-management.info/einfuehrung-in-drm/einleitung.html>
Abruf am 2006-02-01
- [FrKa04] Fränkl, Gerald.; Karpf, Philipp.: Digital Rights Management Systeme. Pg-Verlag, München 2004
- [FrNo98] Fromm, Friedrich-Karl; Nordemann, Wilhelm: Urheberrecht, 9. Auflage, Stuttgart 1998
- [Futu06a] O.V.: Urheberrechtsabgabe auf Drucker und PC, Homepage des Österreichischen Rundfunkanstalt, 2006
<http://futurezone.orf.at/it/stories/83740/>
Abruf am 2006-04-11
- [Garb01] Garbe, Wolf: BINGOOO – Die Transformation des World Wide Web zur virtuellen Datenbank. In: Wirtschaftsinformatik 43 (2001) 5, S. 511-516.
http://www.wirtschaftsinformatik.de/wi_artikel.php?sid=823
Abruf am 2005-11-15
- [Gate76] Gates, Bill: An Open Letter to Hobbyists, 1976
<http://cryptnet.net/mirrors/texts/gates1976.html>
Abruf am 2006-09-13

- [GeSc03] Gehrke, Nick; Schumann Matthias: Constructing Electronic Marketplaces using Peer-to-Peer Technology, In: 36th Annual Hawaii International Conference on System Sciences (HICSS'03) – Track 7, Publication Date: January 2003, p218-228.
<http://doi.ieeecomputersociety.org/10.1109/HICSS.2003.1174579>
Abruf am 2006-11-11
- [GfK06] O.V.: Brennerstudie 2006, Gesellschaft für Konsumentenforschung, 01.06.2006,
<http://www.ifpi.de/wirtschaft/brennerstudie2006.pdf>
Abruf am 2006-09-26
- [Gloc05] Glockner, Cyrill: DRM im vernetzten Haushalt – der PC als Medienzentrale. In: Picot Arnold; Thielmann, Heinz (Hrsg.): Distribution und Schutz digitaler Medien durch Digital Rights Management, Springer Verlag Berlin Heidelberg 2005, S. 75-84.
- [GoHi90] Gottfredson, Michael; Hirschi, Travis: A general theory of crime, Stanford, 1990;
- [GoKr03] Good, Nathaniel S.; Krekelberg, Aaron.: Usability and privacy: a study of KaZaA P2P file-sharing, In: Proceedings of the SIGCHI conference on Human factors in computing systems, Volume No.5, Issue No.1, April 2003, p137-144.
<http://doi.acm.org/10.1145/642611.642636>
Abruf am 2006-11-11
- [Grim03] Grimm, Rüdiger: Digital Rights Management: Technisch-organisatorische Lösungsansätze. In: Picot, Arnold (Hrsg.): Digital Rights Management, Springer Verlag Berlin Heidelberg 2003, S. 93-106.
- [Grim05] Grimm, Rüdiger: DRM – Techniken und ihre Grenzen. In: Picot Arnold; Thielmann, Heinz (Hrsg.): Distribution und Schutz digitaler Medien durch Digital Rights Management, Springer Verlag Berlin Heidelberg 2005, S. 85-96.

- [GrSV03] Grasmugg, Stefan; Schmitt, Christian; Veit, Daniel.: Internetquellen zu Peer-to-Peer-Systemen, In: Wirtschaftsinformatik 45 (2003) 3, S. 335-344.
http://www.wirtschaftsinformatik.de/wi_artikel.php?sid=1242
Abruf am 2005-11-14
- [Gutm03] Gutman, Daniel: Urheberrecht im Internet in Österreich, Deutschland und der EU, Missbrauch, technische Schutzmöglichkeiten und rechtliche Flankierungen, Berliner Wissenschaftsverlag, 2003.
- [Hart01] Hartmann, Frank: Wirtschaftskriminalität im Internet, Geschäftsrisiken durch Computermissbrauch und Datenspionage, Deutscher Wirtschaftsdienst, 2001.
- [Heis02a] O.V.: Marktforscher: Tauschbörsen nicht Schuld an Krise der Musikindustrie. Heise Zeitschriften Verlag, 2002-08-14,
<http://www.heise.de/newsticker/meldung/29960>
Abruf am 2006-09-01
- [Heis02b] O.V.: Marktforscher lesen der Musikbranche die Leviten. Heise Zeitschriften Verlag, 15.08.2002,
<http://www.heise.de/newsticker/meldung/29972>
Abruf am 2006-09-08
- [Herb98] Herberger, Maximilian: Engagement für den Schutz der kulturellen Vielfalt, Grußwort des Bundespräsidenten Roman Herzog.
<http://www.jurpc.de/aufsatz/19980155.htm>
Abruf am 2006-11-08
- [Hess04] Hess, Thomas: Neue Dienste für Geschäft und Unterhaltung, Peer-to-Peer: Chancen und Risiken in Breitbandnetzen. In: Eberspächer, Jörg; Quadt Hans-Peter: Breitband- Perspektiven, Springer Verlag Berlin Heidelberg, Münchner Kreis, 2004, S. 107-117.
- [Hess05] Hess, Thomas: Digital Rights Management Systeme: eine Technologie und ihre Wirkungen. In: Picot Arnold; Thielmann, Heinz (Hrsg.): Distribution und Schutz digitaler Medien durch Digital Rights Management, Springer Verlag Berlin Heidelberg 2005, S. 15-22.

- [Hoer03] Hoeren, Thomas: Welche Chancen hat das Urheberrecht im Internet-Zeitalter. In: Picot, Arnold (Hrsg): Digital Rights Management, Springer Verlag Berlin Heidelberg 2003, S. 5-92.
- [HOrf06] O.V.: VKI: Rechtslage bei Musik-Downloads, Verein für Konsumenteninformation, 23.10.2006,
<http://help.orf.at/?story=5342>
Abruf am 2006-10-24
- [HoSi00] Hoeren, Thomas, Sieber, Ulrich: Handbuch Multimedia-Recht – Rechtsfragen des elektronischen Geschäftsverkehrs, München, Verlag C.H. Beck, 2000,
- [Hott05a] Hottes, Sascha: Nachgefragt: Wie kommen die Dateien in die Tauschbörsen?, H² media factory GmbH, 5.Juni 2005.
<http://www.netzwelt.de/news/71372-nachgefragt-wie-kommen-die-dateien.html>
Abruf am 2006-12-07
- [Hott05b] Hottes, Sascha: P2P mal anders: Legale Filesharing-Dateien, H² media factory GmbH, 12.Juni 2005.
<http://www.netzwelt.de/news/71500-p2p-mal-anders-legale-filesharingdateien.html>
Abruf am 2006-12-07
- [Iann01] Iannella, Renato.; Digital Rights Management Architectures, D-Lib Magazine, Volume 7 Number 6, Juni 2001,
<http://www.dlib.org/dlib/june01/iannella/06iannella.html>
Abruf am 2006-02-01
- [Jaco05] Jacob, Hubert: Musik – eine Wachstumsindustrie im Winterschlaf. In: Picot Arnold; Thielmann, Heinz (Hrsg.): Distribution und Schutz digitaler Medien durch Digital Rights Management, Springer Verlag Berlin Heidelberg 2005, S. 23-42.
- [Joos05] Joos, Richard: BSA sei von den Reaktionen auf ihren Pirateriebericht angeekelt, Gulli.com, 15.06.2005
<http://www.gulli.com/news/bsa-sei-von-den-reaktionen-auf-2005-06-15/>
Abruf am 2006-09-24

- [Joos06] Joos, Richard: Straf- und zivilrechtliche Konsequenzen, Gulli.com, 19.07.2006
<http://www.gulli.com/news/filesharing-straft-und-2006-07-19/>
Abruf am 2006-11-16
- [KaBF04] Karagiannis, Thomas; Broido, Andre; Faloutsos, Michalis.: Transport layer identification of P2P traffic, In: Proceedings of the 4th ACM SIGCOMM conference on Internet measurement, October 2004, p121-134.
<http://doi.acm.org/10.1145/1028788.1028804>
Abruf am 2006-11-11
- [KoRe03] Kolba, Peter; Resetarits Peter.: Mein großer Rechts-Berater, Linde Populär Verlag, 2003.
- [Kott05] Kottmair, Daniel: Medienlobbyisten zensieren freie Rede – Spanischer Uni-Dozent verliert Job, Macwelt.de, 15.06.2005
<http://www.macwelt.de/index.cfm?pid=4&pk=331962>
Abruf am 2006-09-14
- [Krem03] Krempl, Stefan: Werbeverband hält Kampagne gegen Raubkopierer für äußerst fragwürdig, Heise Online, 03.12.2003,
<http://www.heise.de/newsticker/meldung/42578>
Abruf am 2006-09-27
- [Krög00] Kröger, Detlef: Anmerkungen zu OLG Hamburg CR 2000, 658 – Elektronischer Pressespiegel und Urheberrecht, CR 2000, S.662-663.
- [KrSe06] Krömer, Jan; Sen, Evrim: No Copy – Die Welt der digitalen Raubkopie, Tropen Verlag, Köln 2006,
- [Kuhl02] Kuhlen, Rainer: Digitales Urheberrecht - Zwischen "Information Sharing" und "Information Control" - Spielräume für das öffentliche Interesse an Wissen,
<http://www.wissensgesellschaft.org/themen/publicdomain/informationsethik.html>
Abruf am 2006-04-10
- [Kuhl03] Kuhlen, Rainer: Medienprodukte im Netz – Zwischen Kommerzialisierung und freien Zugang. In: Picot, Arnold (Hrsg): Digital Rights Management, Springer Verlag Berlin Heidelberg 2003, S.107-132.

- [Less03] Lessing, Lawrence: Free culture: how big media uses technology and the law to lock down culture and control creativity, New York 2003, S 8
- [Litm01] Litman, Jessica: Digital Copyright, Prometheus Books, New York, 2001,
- [Lohr04] Lohr, Steve: Software Group Enters Fray Over Proposed Piracy Law, New York Times, 19.07.2004, S C8.
- [LooH01] Loohaus, J.: The hidden 'deep Web' holds treasures. In: Inquirer 2001-05-31.
http://inq.philly.com/content/inquirer/2001/05/31/tech_life/DEEP31.htm
Abruf am 2006-11-15
- [Lorz99] Lorz, Stephan: Wirtschaftspolitik in der digitalen Ökonomie. In: Rutz, Michael: Die Byte-Gesellschaft – Informationstechnologien verändern unser Leben, Olzog Verlag München, 1999, S. 247-260.
- [Luij05] Alty van Luijt: Beyond DRM: Balancing of Interest. In: Picot Arnold; Thielmann, Heinz (Hrsg.): Distribution und Schutz digitaler Medien durch Digital Rights Management, Springer Verlag Berlin Heidelberg 2005, S. 61-74.
- [LyVa00] Lyman, P; Varian, H.: How Much Information? Studie; School of Information Management and Systems (SIMS), University of California, Berkeley 2000.
- [McBr05] McBride, Sarah: File-Sharing Firms are urged to protect Music-Industries Rights, The Wall Street Journal, 15.09.2005.
- [McCa01] McCandless, David: Warez World, Heise Zeitschriften Verlag, 26.07.2001,
<http://www.heise.de/tp/r4/artikel/9/9171/1.html>
Abruf am 2006-10-24
- [Menn05a] Mennecke, Thomas: RIAA's Grand Total: 10,037 – What are Your Odds?, Slyck, 02.05.2005
<http://www.slyck.com/news.php?story=769>
Abruf am 2006-09-21
- [Menn05b] Mennecke, Thomas: Interest in File-Sharing at All Time High, Slyck, 27.04.2005,
<http://www.slyck.com/news.php?story=763>
Abruf am 2006-09-14

- [Mina01] Minar, Nelsen: Distributed Systems Topologies: Part 1, 2001-12-14;
http://www.openp2p.com/pub/a/p2p/2001/12/14/topologies_one.html
Abruf am 2005-12-06
- [MöNA00] Möhring, Philip; Nicolini, Käte; Ahlberg, Hartwig: UrhG, Urheberrechtsgesetz, Kommentar, Verlag Franz Vahlen, 2. Auflage, 2000,
- [Müll03] Müller, Günter: An End-User Perspective on File-Sharing Systems. In Wirtschaftsinformatik 45 (2003) 6, S. 643-657
- [Neuh06] Neuhold, Michael: Kopierschutz und Ländercodes, 2006
http://members.aon.at/neuhold/dvd/dvd_kopierschutz.html
Abruf am 2006-09-15
- [o.V.01a] O.V.: Musikindustrie: Internet ist ein Piratenmedium. Klab & Ihlenfeld Verlag GmbH, 2001-06-13,
<http://golem.de/0106/14339.html>
Abruf am 2005-12-02
- [o.V.04a] O.V.: PIRATES OF THE INTERNET, International Law Enforcement Sails After Criminal Warez Groups, fbi.gov, 17.05.2004
<http://www.fbi.gov/page2/may04/051704piracy.htm>
Abruf am 2006-09-14
- [o.V.05a] O.V.: Audio & Multimedia MPEG Audio Layer-3 . Fraunhofer-Gesellschaft, 2005,
<http://www.iis.fraunhofer.de/amm/techinf/layer3/index.html>
Abruf am 2005-12-02
- [o.V.05b] O.V.: MP3. Wikimedia Foundation Inc, 2005,
<http://de.wikipedia.org/wiki/Mp3>
Abruf am 2005-12-02
- [o.V.05c] O.V.: Integrated Services Digital Network. Wikimedia Foundation Inc, 2005,
<http://de.wikipedia.org/wiki/ISDN>
Abruf am 2005-12-02
- [o.V.05d] O.V.: What is PC grid computing? Entropia, Inc, 2005,
http://www.entropia.com/what_is_pc_grid.asp
Abruf am 2005-12-05

- [o.V.06a]. O.V.: Datenträger. Amazon.com Int'l Sales, Inc. und Amazon Services Europe S.a.r.l, 2006,
<http://www.amazon.de>
 Abruf am 2006-02-01
- [o.V.06b] O.V.: DRMS. Pg-Verlag Fränkl u. Karpf GbR, 2006,
<http://www.digital-rights-management.info/>
 Abruf am 2006-02-01
- [o.V.06c] O.V.:Art. 94 EG-Vertrag. dejure.org Rechtsinformationssysteme GbR, 2006
<http://dejure.org/gesetze/EG/94.html>
 Abruf am 2006-03-15
- [o.V.06d] O.V.: Info-RL 2001, TU-Wien, 2006
<http://www.is.tuwien.ac.at/bbr/Urheberrecht-RH.pdf>
 Abruf am 2006-03-15
- [o.V.06e] O.V.: Berner Übereinkommen zum Schutz von Werken der Literatur und Kunst, 2006,
http://www.uni-muenster.de/Jura.itm/hoeren/material/berner_uebereinkommen.htm
 Abruf am 2006-09-03
- [o.V.06f] O.V.: Understanding the WTO - Members and Observers, 2006
http://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm
 Abruf am 2006-09-04
- [o.V.83a] O.V.: Home Computer Market, Discount Store News, Vol.22, No 12,13, 13.07.1983, S42, in: Predicasts Inc., Cleveland,
- [ObSt04] Oberholzer, Felix; Koleman, Strumpf.: The Effect of File Sharing on Record Sales – An Empirical Analysis, Harvard Business School 2004,
http://www.unc.edu/~cigar/papers/FileSharing_March2004.pdf
 Abruf am 2006-11-16
- [Otte05] Ottens, Morag: Statistik kurz gefasst, Industrie, Handel und Dienstleistungen – Bevölkerung und soziale Bedingungen, Wissenschaft und Technologie, Europäische Gemeinschaften, 18/2005, 02.05.2005

- [OutL05] O.V.: Research company says music and book industrie will lose billions, OUT-LAW News, 21.09.2000,
<http://www.out-law.com/page-1011>
 Abruf am 2005-11-02
- [Pahu01] Pahud, Eric: Die Sozialbindung des Urheberrechts, Bern, 2000,
- [Pere05] Perens, Bruce: Social Aspects. In: Picot Arnold; Thielmann, Heinz (Hrsg.): Distribution und Schutz digitaler Medien durch Digital Rights Management, Springer Verlag Berlin Heidelberg 2005, S. 119-126.
- [PeWa04] Peitz, Martin; Waelbroeck, Patrick: The Effect of Internet Piracy on CD Sales: Crosssection Evidence, CESinfo Working Paper Series No.1122, 01.01.2004,
- [PffK02] Pfitzmann, Andreas; Federrath, Hannes; Kuhn, Markus: Anforderungen an die gesetzlichen Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität technischer Schutzmechanismen – Technischer Teil, 2002
<http://www.cl.cam.ac.uk/~mgk25/dmmv-gutachten.pdf>
 Abruf am 2006-02-17
- [Pico03] Picot, Arnold: Digital Rights Management, Springer Verlag Berlin Heidelberg 2003.
- [Pico05] Picot, Arnold: Digital Rights Management – ein einführender Überblick. In: Picot Arnold; Thielmann, Heinz (Hrsg.): Distribution und Schutz digitaler Medien durch Digital Rights Management, Springer Verlag Berlin Heidelberg 2005, S. 1-14.
- [PiTh05] Picot Arnold; Thielmann, Heinz: Distribution und Schutz digitaler Medien durch Digital Rights Management, Springer Verlag Berlin Heidelberg 2005.
- [PiVä00] Pitkänen, Olli.; Välimäki, Mikko.: Towards a Framework for Digital Rights Management, 2000,
http://www.hiit.fi/de/drm_framework_iec2000.pdf
 Abruf am 2006-02-01

- [RaMa04] Rainie, Harrison; Madden, Mary: The state of music downloading and file-sharing online, 25.04.2004.
http://www.pewinternet.org/pdfs/PIP_Filessharing_April_04.pdf
 Abruf am 2006-11-15
- [Renn05] Renner, Tim: Raus aus dem Horror-Kreislauf, Netzeitung, 27.09.2004,
<http://www.netzeitung.de/entertainment/music/305001.html>
 Abruf am 2006-09-27
- [Rent05] Rentrop, Christian: Filesharing-Falle: Wenn Tauschbörsen Privates liefern, H² media factory GmbH, 8.Juli 2005.
<http://www.netzwelt.de/news/71852-filessharingfalle-wenn-tauschboersen-privates-liefern.html>
 Abruf am 2006-12-06
- [Riga01] Rigamonti, Cyrill P: Geistiges Eigentum als Begriff und Theorie des Urheberrechts, Baden-Baden, 2001,
- [Rött01] Röttgers, Janko: Morpheus im Fadenkreuz. Heise Zeitschriften Verlag, 2001-10-04,
<http://www.heise.de/tp/r4/artikel/9/9713/1.html>
 Abruf am 2005-12-02
- [Ruiz03] Ruiz, Blanca; After Napster. Cyberspace and the Future of Copyright. In: Computer Law Review International. Jahrgang. 2003, Heft 1, 2003, Köln, S. 1-5.
- [Rütt96] Rüttgers, Jürgen: Netzbeschmutzern muss das Handwerk gelegt werden. Das Internet darf kein rechtsfreier Raum sein, Frankfurter Rundschau, 07.1996,
- [SaHS05] Saake, Gunter; Heuer, Andreas; Sattler, Kai-Uwe.: Datenbanken, mitp-Verlag/Bonn, 2005.
- [Schm04] Schmeh, Klaus: Die Welt der geheimen Zeichen, Die faszinierende Geschichte der Verschlüsselung, Wissenschaft verständlich & spannend, W3L GmbH, 2004.
- [Scho02] Schotzger, Erwin: Musikindustrie will nun einzelne User verklagen, Presstext Austria, 03.07.2002,
<http://www.presstext.at/pte.mc?pte=020703025>
 Abruf am 2006-09-21

- [Scho05a] Scholl, Christoph: Anonymes Filesharing: IP-Adresse über Proxy verstecken, H² media factory GmbH, 19.Juli 2005.
<http://www.netzwelt.de/news/71942-anonymes-filesharing-ipadresse-ueber-proxy.html>
Abruf am 2006-12-06
- [Scho05b] Scholl, Christoph: Anonymes Filesharing: IPs blocken, H² media factory GmbH, 21.Juli 2005.
<http://www.netzwelt.de/news/71960-anonymes-filesharing-ips-blocken.html>
Abruf am 2006-12-06
- [Scho05c] Scholl, Christoph: Anonymes Filesharing: Sichere P2P-Netze, H² media factory GmbH, 24.Juli 2005.
<http://www.netzwelt.de/news/71979-anonymes-filesharing-sichere-p2pnetze.html>
Abruf am 2006-12-06
- [Schr99] Schricker, Gerhard: Urheberrecht Kommentar, Verlag C.H.Beck, München 1999
- [Schu03] Schulze, Marcel: Materialien zum Urheberrechtsgesetz: Texte – Begriffe – Begründungen, Weinheim, 2003,
- [Schu04] Schumy, Barbara: Piraterie-Jäger äschern Raubkopien ein, Wirtschaftsblatt Online, 07.04.2004,
<http://www.wirtschaftsblatt.at/cgi-bin/page.pl?id=342297>
Abruf am 2006-09-21
- [Schu05] Schulzki-Haddouli, Christiane: Studie für Forschungsministerium fordert nutzerzentriertes DRM, Heise Online, 16.11.2005,
<http://www.heise.de/newsticker/meldung/66257>
Abruf am 2006-10-13
- [Schw06] Schwarz, Patrick: Was sind Ports? Hamburg, 2006,
<http://www.netzadmin.org/theorie/ports.htm>
Abruf am 2006-09-12
- [ScVe06] Schmidt, Caroline; Verbeet, Markus: Fluch der Silberlinge, Spiegel, Heft 4/2006, S42.

- [ScWe03] Schoder, Detlef; Weinhardt, Christof.: Peer-to-Peer – Technologien, Architekturen und Anwendungen, In: Wirtschaftsinformatik 45 (2003) 3, S.257.
http://www.wirtschaftsinformatik.de/wi_artikel.php?sid=1244
Abruf am 2005-11-15
- [SeKr06] Sen, Evrim; Krömer Jan: Was ist eine Schwarzkopie?, Köln, 2006
<http://www.schwarzkopien.de/was-ist-eine-schwarzkopie.htm>
Abruf am 2006-09-13
- [Smit98] Smith, Richard: Internet-Kryptographie, Addison-Wesley, Bonn, 1998
- [Solm06] Solmecke, Christian: Straf- und zivilrechtliche Konsequenzen. In: Zeitschrift Multimedia und Recht (MMR) 2006 Heft 7 XXIII, 2006.
<http://www.rae-michael.de/news/it-recht/mmr-aufsatz-filesharing-straft-und-zivilrechtliche-konsequenzen-267/>
Abruf am 2006-11-16
- [Spät05] Späth, Nikos: Hoffen auf den weißen Ritter, Welt am Sonntag, 20.02.2005,
<http://www.wams.de/data/2005/01/09/385478.html>
Abruf am 2006-09-27
- [StHH05] Strain, Adrian; Harari, Julie; Harley, Fiona: Global music retail sales, including digital, flat in 2004, Ifpi.org, London, 22.03.2005
<http://www.ifpi.org/site-content/press/20050322.html>
Abruf am 2006-09-26
- [Stock04] Stock, Wolfgang; Zitat von Prof.Dr.Wolfgang G.Stock, Universität Düsseldorf, 2004,
- [Tay105] Taylor, Ian.J: From P2P to Web Services and Grids. Springer, London 2005.
- [THVW05] Tran, Huu; Hitchens, Michael; Varadharajan, Vijay; Watters, Paul: A Trusted based Access Control Framework for P2P File-Sharing Systems, In: Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05) – Track 9, Publication Date: January 2005, p302-312.
<http://doi.ieeecomputersociety.org/10.1109/HICSS.2005.58>
Abruf am 2006-11-11

- [TRIP06] O.V.: WTO/TRIPS, Eidgenössisches Institut für geistiges Eigentum, 2006,
<http://www.ige.ch/D/jurinfo/j1101.shtm>
 Abruf am 2006-03-07
- [Turk98] Turkle, Sherry: Leben im Netz der Identität in Zeiten des Internet,
 Reinbek b.Hamburg, Rohwohlt Verlag, 1998.
- [UrhG06] O.V.: Urheberrechtsgesetz, 2006
http://www.i4j.at/gesetze/bg_urhg2a.htm
 Abruf am 2006-03-16
- [USC06] O.V.: 17 USC 106 Exclusive rights in copyrighted works, 2006
<http://www.bitlaw.com/source/17usc/106.html>
 Abruf am 2006-03-07
- [USCON06] O.V.: U.S. Constitution Article I, 2006
<http://www.law.cornell.edu/constitution/constitution.articlei.html>
 Abruf am 2006-03-07
- [Vari00] Varian, Hal R.: Variants in Economic Theory: Selected Work of Hal R.
 Varian in Economists of the Twentieth Century, August 2000,
- [VaSa98] Varian, Hal R.; Saphiro, Carl: Information Rules: A Strategic Guide to
 the Network Economy; Harvard Business School Press; 1998
- [VoBä03]. Volpe Francesco, Bär Christian: Zum Erkennen von
 Kopierschutzmechanismen. In: C'T Magazin für Computertechnik
 Ausgabe 07/2003, S.144-151.
- [WaHe03] Benedikt von Walter; Hess, Thomas.: iTunes Music Store – Eine
 innovative Dienstleistung zur Durchsetzung von Property-Rights im
 Internet, In: Wirtschaftsinformatik 45 (2003) 5, S. 541-546.
http://www.wirtschaftsinformatik.de/wi_artikel.php?sid=1316
 Abruf am 2005-11-15
- [Webl01] Weblens: The Invisible Web.
<http://www.weblens.org/invisible.html>
 Abruf am 2006-11-15
- [Wiki06a] O.V.: Business Software Alliance BSA. Wikimedia Foundation Inc, 2006
http://de.wikipedia.org/wiki/Business_Software_Alliance
 Abruf am 2006-09-21

- [Wiki06b] O.V.: Recording Industry Association of America (RIAA). Wikimedia Foundation Inc, 2006
<http://de.wikipedia.org/wiki/RIAA>
Abruf am 2006-09-21
- [Wiki06c] O.V.: International Federation of the Phonographic Industry (IFPI). Wikimedia Foundation Inc, 2006
<http://de.wikipedia.org/wiki/IFPI>
Abruf am 2006-09-21
- [Wiki06d] O.V.: Motion Picture Association of America (MPAA), Wikimedia Foundation Inc, 2006
<http://de.wikipedia.org/wiki/MPAA>
Abruf am 2006-09-21
- [Wiki06e] O.V.: Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e.V. (BVU), WikimediaFoundation Inc, 2006
http://de.wikipedia.org/wiki/Gesellschaft_zur_Verfolgung_von_Urheberrechtsverletzungen_e.V.
Abruf am 2006-09-21
- [Wiki06f] O.V.: No Electronic Theft Act (NET Act), Wikimedia Foundation Inc, 2006
http://en.wikipedia.org/wiki/NET_Act
Abruf am 2006-09-21
- [Wiki06g] O.V.: Time-to-live, Wikimedia Foundation Inc, 2006
<http://de.wikipedia.org/wiki/Time-to-live>
Abruf am 2006-11-01
- [Wiki06h] O.V.: Transmission Control Protocol, Wikimedia Foundation Inc, 2006
http://de.wikipedia.org/wiki/Transmission_Control_Protocol
Abruf am 2006-11-06
- [Wiki06i] O.V.: IP Adresse, Wikimedia Foundation Inc, 2006
<http://de.wikipedia.org/wiki/IP-Adresse>
Abruf am 2006-11-06
- [Wiki06j] O.V.: Grid-Computing, Wikimedia Foundation Inc, 2006
<http://de.wikipedia.org/wiki/Grid-Computing>
Abruf am 2006-11-14

- [Wiki06k] O.V.: E-Mule, Wikimedia Foundation Inc, 2006.
<http://de.wikipedia.org/wiki/E-Mule>
Abruf am 2006-11-29
- [Wiki06l] O.V.: Bit Torrent, Wikimedia Foundation Inc, 2006.
http://de.wikipedia.org/wiki/Bit_Torrent
Abruf am 2006-11-29
- [Wiki06m] O.V.: Fair-Use. Wikimedia Foundation Inc, 2006
http://de.wikipedia.org/wiki/Fair_Use
Abruf am 2006-03-07
- [Wiki06n] O.V.: Digital Millennium Copyright Acts. Wikimedia Foundation Inc, 2006
http://de.wikipedia.org/wiki/Digital_Millennium_Copyright_Act
Abruf am 2006-03-08
- [Wiki06o] O.V.: Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums. Wikimedia Foundation Inc, 2006,
<http://de.wikipedia.org/wiki/TRIPS>
Abruf am 2006-09-04
- [Wiki06p] O.V.: Homebrew Computer Club, Wikimedia Foundation Inc, 2006,
http://en.wikipedia.org/wiki/Homebrew_Computer_Club
Abruf am 2006-09-13
- [Wiki06q] O.V.: DivX. Wikimedia Foundation Inc, 2006
<http://de.wikipedia.org/wiki/DivX>
Abruf am 2006-09-15
- [Wiki06r] O.V.: ARPANET. Wikimedia Foundation Inc, 2006
<http://de.wikipedia.org/wiki/ARPANET>
Abruf am 2006-09-17
- [Wiki06s] O.V.: Internetknoten. Wikimedia Foundation Inc, 2006
<http://de.wikipedia.org/wiki/Internetknoten>
Abruf am 2006-09-17
- [Wiki06t] O.V.: Urheberrecht. Wikimedia Foundation Inc, 2006,
<http://de.wikipedia.org/wiki/Urheberrecht>
Abruf am 2006-03-06

- [Wiki06u] O.V.: IPv6, das Internet Protocol Version 6. Wikimedia Foundation Inc, 2006,
<http://de.wikipedia.org/wiki/IPv6>
Abruf am 2006-12-05
- [Wiki06v] O.V.: Berner Übereinkunft. Wikimedia Foundation Inc, 2006,
http://de.wikipedia.org/wiki/Berner_%C3%9Cbereinkunft_zum_Schutz_von_Werken_der_Literatur_und_Kunst
Abruf am 2006-03-07
- [Wiki07a] O.V.: User Datagram Protocol. Wikimedia Foundation Inc, 2007,
http://de.wikipedia.org/wiki/User_Datagram_Protocol
Abruf am 2007-05-23
- [Wiki07b] O.V.: Leechen. Wikimedia Foundation Inc, 2007,
<http://de.wikipedia.org/wiki/Leechen>
Abruf am 2007-05-23
- [Wiki07c] O.V.: NFO. Wikimedia Foundation Inc, 2007,
<http://de.wikipedia.org/wiki/NFO>
Abruf am 2007-05-24
- [Wire04] O.V.: File-Sharing Thrives Under Radar, Wired News, 06.11.2004
<http://www.wired.com/news/digiwood/0,1412,65625,00.html?tw=rss.TOP%20>
Abruf am 2006-09-14
- [Witt00] Wittgenstein, Philipp: Die digitale Agenda der neuen WIPO-Verträge – Umsetzung in den USA und der EU unter besonderer Berücksichtigung der Musikindustrie, Bern, 2000
- [Wöbk04] Wöbken, Hergen: Digitale Mentalität, Institut für Strategieentwicklung März – Juni 2004 in Kooperation mit der Universität Witten/Herdecke.
http://download.microsoft.com/download/D/2/B/D2B7FE98-CA92-4E18-ACD6-94A915B4CAFF/Digitale_Mentalitaet.pdf
Abruf am 2006-11-22
- [Wolf04] Wolff, Donna: What is peer-to-peer, Techtarget.com, 22.02.2004
http://searchnetworking.techtarget.com/sDefinition/0,290660_sid7_gci212769,00.html
Abruf am 2006-11-14

- [WuVi05] Wunsch-Vincent, Sacha; Vichery, Graham: Digital Broadband Content: Music, 08.06.2005,
<http://www.oecd.org/dataoecd/13/2/34995041.pdf>
Abruf am 2006-09-26
- [XuWT05] Xu, Heng; Wang, Hao; Teo, Hock-Hai.: Predicting the Usage of P2P Sharing Software: The Role of Trust and Perceived Risk, In: Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05) – Track 9, Publication Date: January 2005, p201-211.
<http://doi.ieeecomputersociety.org/10.1109/HICSS.2005.500>
Abruf am 2006-11-11

Abbildungsverzeichnis

Abbildung 1: Zentralisiertes P2P (Napster, OpenNap)	39
Abbildung 2: Dezentralisiertes P2P (Gnutella, Freenet)	40
Abbildung 3: Hybrid P2P (FastTrack, eDonkey, WinMX)	41
Abbildung 6: Übersicht Urheberrecht Österreich	65
Abbildung 7: Der Weg von Raubkopien nach GVU	109
Abbildung 8: Übersicht DRM technische und rechtliche Komponenten, nach [Pico05, 3]	111
Abbildung 9: Vier-Feld-Matrix der digitalen Typen nach [Wöbk04, 18]	146
Abbildung 10: Ausprägung der Raubkopiermentalität nach [Wöbk04, 22]	147
Abbildung 11: Ausprägung des Rechtsbewusstseins nach [Wöbk04, 23]	148

Tabellenverzeichnis

Tabelle 1: Gründe für die Entstehung der Digital Rights Problematik aus technischer Sicht, nach [o.V.06b]	113
Tabelle 2: Komponenten eines Digital Rights Management System, nach [o.V.06b]	116
Tabelle 3: Funktionen-Technologien-Matrix eines DRMS, nach [o.V.06b]	121