„Neue Medien“

Stand der Technik - Stand des Rechts

Seminar im Urheberrecht

21. – 24. Juni 2002 in Amsterdam

bei Prof. Dr. M. Rehbinder

und Prof. Dr. R. Hilty

vorgelegt als Gruppenarbeit von:

Beat Hangartner	Lukas Hohl	Tobias Koch	Till Quack
Birmensdorferstrasse 38	Zürichstrasse 75	Chilenholzstrasse 28	Regensbergstrasse 81
8004 Zürich	8700 Küsnacht	8907 Wettswil	8050 Zürich
bhangart@ee.ethz.ch	lhohl@freesurf.ch	tkoch@ee.ethz.ch	till@quack.ch

Inhaltsverzeichnis

Literaturverzeichnis

[1] Shirky, Clay: How did the Web grow so quickly?, http://www.shirky.com/OpenSource/view_source.html (besucht im Mai 2002)

[2] Tedeschi, Bob: Ticketmaster and Microsoft Settle Linking Dispute, The New York Times On The Web, http://www.nytimes.com/library/tech/99/02/cyber/articles/15tick.html (besucht am 10.6.2002)

[3] Tedeschi, Bob: Ticketmaster Sues Again Over Links, The New York Times On The Web, http://www.nytimes.com/library/tech/99/08/cyber/articles/10tickets.html (besucht am 10.6.2002)

[4] Kaplan, Carl S.: Legality of 'Deep Linking' Remains Deeply Complicated, The New York Times On The Web, http://www.nytimes.com/library/tech/00/04/cyber/cyberlaw/07law.html (besucht am 10.6.2002)

[5] Weinknecht, Jürgen: Grundlagen des nationalen und internationalen Urheberrechts, http://www.weinknecht.de/uii02.html/Urheberrecht_International (besucht am 10.6.2002).

[6] Massenansturm auf Napster, Phoenix Online, http://www.phoenix.de/old/themen/topt/022001/01414/ (besucht am 11.6.2002)

[7] Napster.com engagiert Microsoft-Ankläger, Neue Studie verunsichert Musikindustrie, University of Phoenix online, http://wolpertinger.hypermart.net/newspro/arc2.html (besucht am 11.6.2002)

[8] Gillespie, Thom: Rip, Mix & Burn, http://www.indiana.edu/~slizzard/p2p/index.html (besucht am 11.6.2002)

[9] Tarantella: Das WinPhone Peer-to-Peer Suchsystem, http://www.megasoft.co.at/german/tarantella.htm (besucht am 11.6.2002)

[10] Ding, Oliver: Datentausch-Dienste-Mini-FAQ, http://www.sockenseite.de/datentausch-minifaq.txt (besucht am 11.6.2002)

[11] Murkherjee, Patrick; Kelm, Hans-Jürgen; Prüfert, Holger: Informatik und Gesellschaft, Technische Universität Berlin, http://ig.cs.tu-berlin.de/w2000/ir1/referate2/k-3b/ (besucht im April 2002)

[12] Zoier, Markus: Peer-to-Peer Tauschbörsen, Technische Universität Graz, www.iicm.edu/research/seminars/ ws_01/zoier-peer2peer.pdf (besucht am 11.6.2002)

[13] Pedrazzini, Mario/von Büren, Roland/Marbach, Eugen: Immaterialgüer- und Wettbewerbsrecht, Bern 1998

[14] McCannell, Steve: A Pressplay Test Drive, Openp2p.com, http://www.openp2p.com/pub/a/p2p/2002/03/07/pressplay.html (besucht am 11.6.2002)

[15] McFadden, Andy: CD-Recordable FAQ http://www.cdrfaq.org/faq02.html (besucht am 10.6.2002)

[16] Zota, Volker: Klonverbot, c't 02/2002, 90

[17] Amman, Daniel: Mafia gegen Microsoft, Weltwoche Nr. 19 2002, 46

[18] Cherry, Steven M.: Making Music Pay, IEEE Spectrum Oktober 2001, 41

[19] ders.: Getting Copyright Right, IEEE Spectrum Februar 2002

[20] Cherry, Steven M./ Siang, Sanyin: Digital Millennium Copyright Act Faces Court Tests, IEEE Spectrum Oktober 2001

[21] Krempl, Stefan: Geschützte Kopiersperren, c't 08/2002, 18

[22] Mulholland, Judie: Digital Rights (mis)Management www.w3.org/2000/12/drm-ws/pp/Overview.html (besucht am 10.6.2002)

[23] Kuhn, Kelin J.: Audio Compact Disc – Writing and Reading http://www.ee.washington.edu/conselec/CE/kuhn/cdaudio2/95x7.htm (besucht am 10.6.2002)

[24] DRM Features http://www.giantstepsmts.com/drmarticle.htm (besucht am 10.6.2002)

Abkürzungsverzeichnis

ADSL	Asymmetric Digital Subscriber Line
CD	Compact Disc
CAD	Computer Aided Design
CAE	Computer Aided Engineering
DIVX	Digital Video Express
DRM	Digital Rights Management
DVD	Digital Versatile Disc
EFM	Eight to Fourteen Modulation
ECC	Error Correction Code
HTML	Hyper Text Markup Language
HTTP	Hypertext Transfer Protocol
ISP	Internet Service Provider
MP3	MPEG Audio Layer 3
P2P	Peer-to-Peer
RIIA	Recording Industry Institute of America
WWW	World Wide Web

Einleitung

Der technische Fortschritt hat in den letzten Jahrzehnten grossartige Errungenschaften hervorgebracht. Darunter fallen auch unsere nun alltäglichen digitalen Medien. Gerade weil das Internet und die Compact Disc, welche die mächtigsten Vertreter der neuen Medien sind, in unserer Gesellschaft eine überaus weite Verbreitung gefunden haben, sind die Gesetze gefordert, klare Regeln aufzustellen. Bekanntermeise sind diese noch nicht vorhanden und die vorliegende Gegenüberstellung *Stand der Technik – Stand des Rechts* wird zeigen, dass es nicht einfach ist, klare Regeln aufzustellen.

Der Reiz und die Problematik der neuen Medien liegen in der einfachen und komfortablen Handhabung der transportierten Inhalte. Seit man Lösungen gefunden hat, wie man z.B. Texte, Musikstücke, Bilder und vielleicht bald Gerüche digitalisieren kann, lassen sie sich in hoher Geschwindigkeit ohne Qualitätsverluste und ohne nennenswerten Aufwand verteilen, vervielfältigen und verarbeiten. Die Digitalisierung und deren Vorzüge trennen den Inhalt und die durch das Medium bestimmte Form von Werken geistigen Eigentums in zunehmenden Masse. Das heisst, die Form ist sehr wandelbar geworden und verliert an Bedeutung. Aber gerade die Form wie z.B. ein gedrucktes Buch ermöglicht es Urhebern ihre Werke zu verwerten.

Wir sind bei einem Interessenskonflikt angelangt, dessen Lösung primär im Immaterialgüterrecht gesucht wird. Die vorliegende Arbeit beschränkt sich auf urheberrechtliche Aspekte der neuen Medien und lässt Betrachtungen im Patent- und Markenrecht weg. Die Autoren behandeln die vier aktuellen Themen *Peer to Peer, Urheberrecht und Software, Urheberrecht und WWW* sowie den *Rechtsschutz technischer Schutzmassnahmen* unter dem Aspekt *Stand der Technik – Stand des Rechts*.[1]

[1] Diese Arbeit ist als Gruppenarbeit in Zusammenhang mit der MTU-Veranstaltung *Management und Recht* des Departements ITET an der ETH Zürich entstanden. Die Autoren bringen einen technischen Hintergrund mit und haben sich aus dieser Perspektive an das Urheberrecht herangetastet.

A. Peer to Peer

Bekannt geworden ist die Peer-to-Peer-Technologie (P2P) durch die Musiktauschbörse Napster. Aufgrund der einfachen Handhabung und des grossen Angebots an Musiktiteln, die im MP3-Format[2] zu finden waren, erfreute sich Napster bald einer grossen Beliebtheit.
Der Verband der US-Musikindustrie (RIAA) jedoch beklagte Verluste von mehr als 300 Mio. Dollar[3], und verklagte 1999 die Musiktauschbörse wegen Verletzung von Urheberrechten. Die Gerichte entschieden zu Ungunsten von Napster, was zur Folge hatte, dass bis zu 200'000 Musikdateien geblockt werden mussten. Aus diesem Grund haben viele Benutzer[4] auf eine andere P2P-Software gewechselt. Mittlerweile hat der Bertelsmann-Konzern Napster übernommen und will die Software in ein kommerziell nutzbares Modell umwandeln.
Es hat sich jedoch gezeigt, dass Napster nur den Anfang gemacht hat und weitere (dezentrale) P2P-Progarmme dessen Funktion übernommen haben. Hinzu kommt, dass mit der wachsenden Zahl von Breitbandanschlüssen (Kabelmodem, ADSL) immer grössere Datenmengen relativ rasch heruntergeladen werden können. So sind Kino-Filme im DIVX-Format[5] zu finden, welche in Europa noch gar nicht in den Kinos laufen. Zusätzlich wird auch immer mehr Software getauscht.
Da die heutige Gesetzgebung den technischen Möglichkeiten „hinterherhinkt“, ist es unumgänglich, wenigstens im Nachhinhein die Gesetzte so anzupassen, dass die Rechtsinhaber auf mögliche Urheberrechtsverletzungen reagieren können. Darüber hinaus ist aber auch zu untersuchen, ob es Möglichkeiten gibt, Rechtsverletzungen im voraus zu verhindern.

Dieser Teil der Arbeit befasst sich mit den urheberrechtlichen Aspekten der P2P-Technologie. Wichtige Kernfragen sind:

---

[2] Mit Hilfe des MP3-Formates kann die Grösse eines Musik-Files ohne hörbare Verluste auf einen Bruchteil der ursprünglichen Grösse reduziert werden. Auf die technischen Details wird hier nicht eingegangen, das Format hat aber insofern eine wichtige Bedeutung, dass erst dank diesem Format das Herunterladen von Musik-Titeln über eine langsame Internetverbindung attraktiv wurde.

[3] www.phoenix.de. Dies ist allerdings mehr als fraglich ist, denn laut einer Umfrage des Marktforschungsunternehmens Yankelovich haben 59% von 16.000 befragten US-Bürgern angegeben, dass sie zuerst im Internet gehörte Musikstücke später auf CD gekauft haben (wolpertinger.hypermart.net).

[4] Die männliche Form bezieht sich in der ganzen Arbeit auf beide Geschlechter

[5] DIVX stellt etwa das Pendant zu MP3 dar. Während ein Film normalerweise nur auf einer DVD Platz findet, kann man Filme im DIVX-Format auf einer CDROM abspeichern.

- Tritt bei P2P-Systemen wirklich eine Verletzung des Urheberrechts auf?
- Hätte Napster auch in der Schweiz aufgrund Urheberrechtsverletzung verurteilt werden können?
- Wie könnte eine Kontrolle von P2P-Systemen zur Verhinderung von Urheberrechtsverletzungen aussehen?

I. Was ist Peer-to-Peer?

Die P2P-Technologie unterscheidet sich von anderen Internet-Technologien vor allem dadurch, dass sie nicht Client-Server-basiert ist. Client-Server-basiert bedeutet, dass der eine Teilnehmer mehrheitlich Daten liefert (Server) und der andere v.a. Daten fordert (Client). Wenn man sich z.B. die Webseite der ETH anschauen möchte, so sendet man eine Anfrage an die gewünschte Adresse (www.ethz.ch) und erhält die Seite. Die ETH ist also der Server und die Person, welche sich die Seite anschaut, ist der Client.
Das Prinzip der P2P-Technologie beruht darauf, dass jeder Teilnehmer zugleich Server und Client ist, das heisst man sucht nicht nur nach Daten, sondern man bietet auch welche an. Während bei Client-Server-basierten Systemen die Anzahl der Nutzer nur einen Einfluss auf die Belastung des Servers hat (bei zu vielen Nutzern ist der Server überlastet), hängt bei P2P-Systemen das Angebot stark von der Menge der zur Verfügung gestellten Daten ab, d.h. die Attraktivität eines P2P-Netzes hängt auch stark von der Anzahl Nutzer ab. Im Folgenden sind drei wesentliche Varianten dieser Technologie beschrieben:

1. Modell Napster[6]

Napster unterhält eine zentrale Datenbank, welche eine Liste der zur Zeit verfügbaren Daten enthält. Als verfügbar gelten sämtliche Daten, welche von den Benutzern, die gerade online sind, mittels Filesharing zur Verfügung gestellt werden (wobei der Nutzer selbst wählen kann, welche Teile seiner Festplatte allgemein zugänglich sind). Es sei jedoch erwähnt, dass auch zentral geführte P2P-Netze wie z.B. *Audiogalaxy* existieren, die zusätzlich auf Daten von Nutzern, welche nicht mehr online sind, verweisen. Diese Daten können dann erst heruntergeladen werden, wenn der Besitzer sich wieder im Netz angemeldet hat. Der Funktionsablauf eines solchen Systems sieht wie folgt aus: Der Benutzer meldet sich auf der Homepage von Napster an und teilt dort mit, welche Daten er selbst zur Verfügung stellen will. Bei der Suche nach einem bestimmen Musiktitel kann man mit Hilfe der Datenbank ermitteln, wer dieses File anbietet. Der Download der Daten geschieht dann ohne Umweg über Napster, das heisst es wird direkt eine Verbindung zum betreffenden Benutzer aufgebaut und das File heruntergeladen (siehe Abbildung 1).

---

[6] Z.B. Napster, Audiogalaxy.

Eigentlich benutzt Napster nicht klassische P2P-Technologie, denn sämtliche Anfragen werden zentral bearbeitet. Aufgrund der von Napster geführten Datenbank ist bekannt, welche Titel gerade angeboten werden, weshalb Napster als Drehscheibe des Systems ein relativ einfaches Ziel für die Attacken der Musikindustrie darstellt.

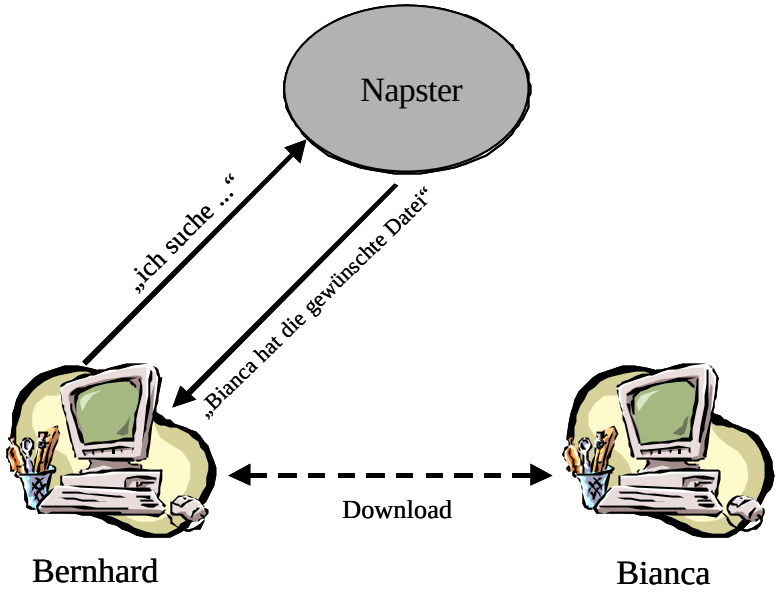

Abbildung 1: Modell Napster

2. Modell Gnutella[7]

Gnutella bezeichnet eigentlich nur ein Kommunikationsprotokoll. Das heisst, eine Software, die das Gnutella-Protokoll verwendet, kann mit einer anderen Gnutella-Software kommunizieren.

Im Gegensatz zu Napster arbeitet Gnutella völlig dezentral. Wenn sich ein Benutzer anmeldet, so schickt er einfach eine Meldung an „benachbarte“ Benutzer. Sucht man nun eine Datei, so „fragt“ man zuerst beim „Nachbarn“ nach. Dieser schickt die Meldung, ob er im Besitz der gewünschten Datei ist, zurück und sendet die Anfrage an seine „Nachbarn“ weiter, welche gleich vorgehen (*Schneeballprinzip*). Nach einer Weile sollte man eine Liste von Benutzern haben, welche die gesuchte Datei besitzen, und kann die Daten direkt herunterladen (siehe Abbildung 2).

Aufgrund der dezentralen Struktur ist es praktisch unmöglich, ein Gnutella-Netzwerk auszuschalten, wie das bei Napster noch möglich war.

[7] Z.B. Bearshare, Limewire

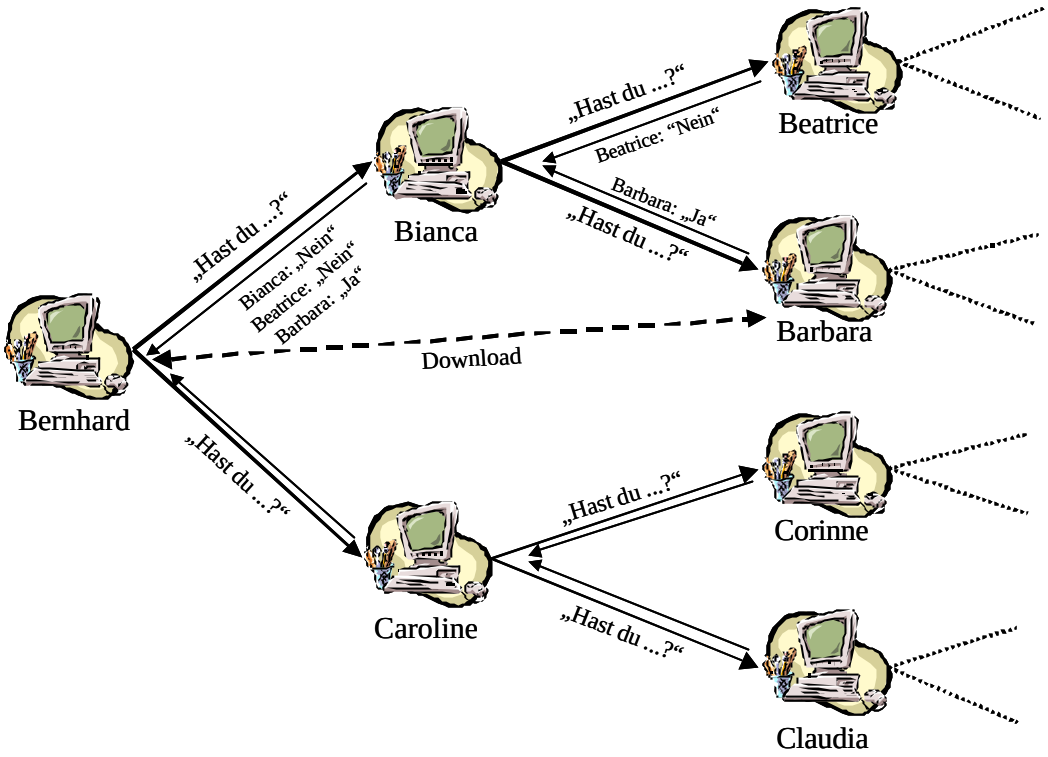

Abbildung 2: Modell Gnutella

3. Modell Fasttrack[8]

Fasttrack arbeitet nach einem ähnlichen Prinzip wie Gnutella. Beide Technologien arbeiten dezentral. Während bei Gnutella alle Benutzer sowohl als Server wie auch als Client fungieren, wird das Netz bei Fasttrack in sogenannte *Nodes* und *Superpeers* unterteilt. Als *Nodes* gelten alle Benutzer, welche zwar nach Daten suchen und Daten anbieten, die aber keine Suchanfragen weiterleiten (im Gegensatz zu den *Superpeers*, welche zusätzlich Suchanfragen weiterleiten; siehe dazu Abbildung 3). Beim einloggen meldet sich der Benutzer bei einem zentralen Server an, welcher bestimmt, ob man als *Node* oder *Superpeer* fungiert (abhängig davon, wie leistungsfähig der Rechner in punkto Rechenleistung und Netzwerkanbindung ist), und den Nutzern die Adressen der „benachbarten“ Teilnehmer mitteilt.

Damit eine Suche möglich ist, muss jeder *Node* eine Liste mit den zur Verfügung gestellten Daten an den *Superpeer* schicken, so dass dieser bei einer Anfrage weiss, ob die an ihn angeschlossenen *Nodes* die gesuchten Daten besitzen. Bei der Suche nach Daten schickt man die Anfrage an den *Superpeer*, welcher die Suche an die anderen *Superpeers* weiterleitet. Das Herunterladen funktioniert gleich wie bei anderen P2P-Varianten: das File wird direkt vom einen *Node* zum anderen transferiert. Durch diese Aufteilung in *Node* und *Superpeer* ist ein Fasttrack-Netzwerk v.a. bei einer grossen Anzahl Nutzern leistungsfähiger

[8] Z.B. KaZaA

als ein Gnutella-Netzwerk, denn die Suchanfragen, welche abhängig von der Zahl der Benutzer viel Bandbreite benötigen können, gehen nur noch über die „schnellen“ *Superpeers*, wodurch ein Benutzer mit einer “langsamen“ Internetanbindung nicht das ganze Netz lahmlegen kann.

Noch zu erwähnen sei, dass der einzige zentrale Teil der Login-Server darstellt. Dieser koordiniert nur den Anmeldeprozess und ist für ein weiteres Funktionieren des Netzes nicht nötig. Enfernt man den Server, so muss jeder Nutzer selbst ermitteln, welches die „benachbarten“ Teilnehmer sind. Gelingt dies, so kann das Netz in gleicher Weise wie vorher genutzt werden. Aus diesem Grund kann man Fasttrack-Netzwerke nicht auf dieselbe Art ausschalten wie zentrale P2P-Systeme nach dem Modell von Napster.

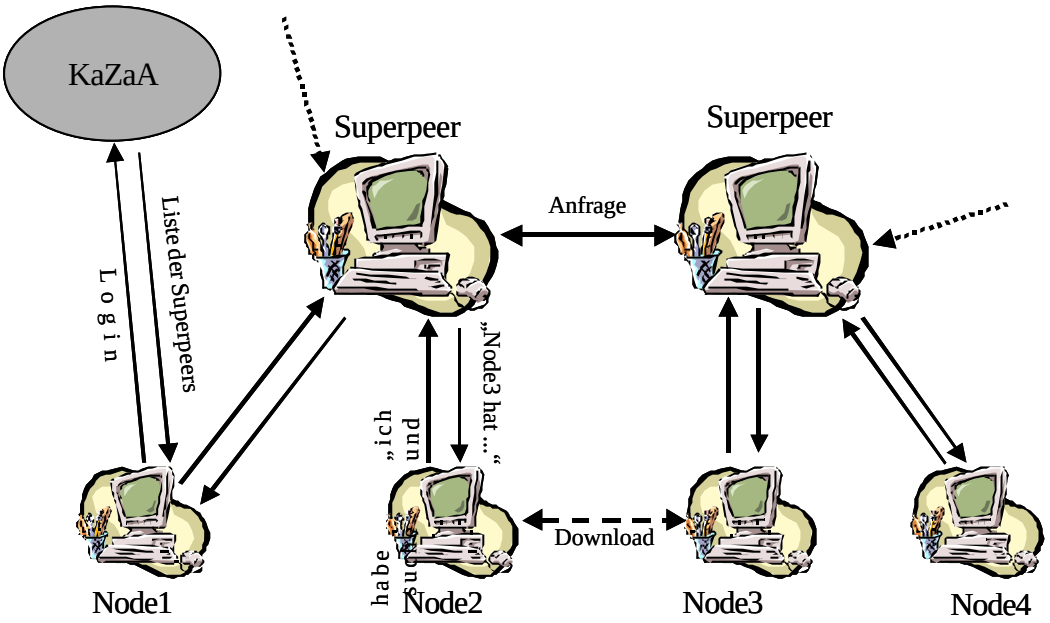

Abbildung 3: Fasttrack

4. Zusammenfassung P2P

Während P2P-Modelle, welche durch einen zentralen Server verwaltet werden, noch relativ einfach kontrolliert werden können, ist dies bei dezentralen Systemen praktisch unmöglich, denn solche Netze funktionieren auch ohne zentrale Elemente. Für die Rechtsinhaber bedeutet dies, dass man innovativere Lösungen zur Kontrolle eines P2P-Systems finden muss.

Im Kapitel Kontrolle von P2P-Systemen wird genauer auf verschiedene Kontrollmöglichkeiten eingegangen, es sollte aber bereits erwähnt werden, dass eine totale Kontrolle aufgrund der dezentralen Struktur praktisch unmöglich ist.

II. Rechtliche Aspekte

1. Urheberrechtsgesetz der Schweiz

a) Anwendung auf einzelne P2P-Nutzer

Laut Urheberrechtsgesetz hat jede Person das Recht, ein veröffentlichtes Werk wie z.B. eine CD, welche man im Laden gekauft hat, für den Eigengebrauch zu verwenden. Als Eigengebrauch gilt:

1. *„Jede Werkverwendung im persönlichen Bereich und im Kreis von Personen, die unter sich eng verbunden sind, wie Verwandte und Freunde.*
2. *Jede Werkverwendung der Lehrperson für den Unterricht in der Klasse.*
3. *Das Vervielfältigen von Werkexemplaren in Betrieben, öffentlichen Verwaltungen, Instituten, Kommissionen und ähnlichen Einrichtungen für die interne Information oder Dokumentation"* (Art. 19 URG)

Die Werkverwendung im persönlichen Bereich ist vergütungsfrei (Art. 20 URG).

Wie im vorherigen Kapitel beschrieben, funktioniert die P2P-Technologie so, dass die Teilnehmer einen Teil ihrer Festplatte allen anderen zur Verfügung stellen (Filesharing) und die anderen mittels Anfrage herausfinden, wer gerade die gesuchte Datei „im Angebot" hat. Es stellt sich nun die Frage, ob durch den für jedermann ermöglichten Zugriff auf eine Festplatte Urheberrechte verletzt werden.

These: Jede Person hat das Recht, erworbene Werke auf ihrer Festplatte abzuspeichern, da dies als Eigengebrauch gilt (Art. 19 URG). Da die Festplatte nicht der Allgemeinheit zugänglich ist, sondern nur vereinzelten Personen (solche, welche dieselbe P2P-Software benützen), wird das Vervielfältigungsrecht nicht verletzt, denn die Handlung beschränkt sich auf einen privaten Kreis (und gilt daher als Eigengebrauch). Ausserdem werden keine urheberrechtlich geschützten Daten angeboten, denn Filesharing ermöglicht anderen Netzteilnehmern zwar den Zugriff auf die Festplatte, es wird aber nicht öffentlich bekannt gegeben, welche Daten angeboten werden (der Nutzer muss von sich aus eine Anfrage stellen, ob jemand im Besitz der gesuchten Daten ist). In dieser Hinsicht unterscheidet sich Filesharing vom Anbieten von Daten über eine Website, wo ein Teilnehmer nicht gezielt suchen muss, um die gewünschten Files zu finden. Der „Täter" ist also derjenige, welcher nach (urheberrechtlich geschützten) Daten sucht, demzufolge verletzt jemand, welcher geschützte Daten auf seiner Festplatte abspeichert und sie anderen Personen zugänglich macht, keine Urheberrechte.

Antithese: Das Kopieren von Daten auf Festplatte gilt als Reproduktionsverfahren, d.h. ohne Vervielfältigungsrecht ist dies nicht erlaubt[9]. Da man bei veröffentlichten Werken bei Eigengebrauch zu jeder Werkverwendung berechtigt ist, dürfen jegliche Daten auf die Festplatte gespeichert werden. Speichert man allerdings auf einen Datenträger, der der Allgemeinheit zugänglich ist, so handelt es sich nicht mehr um Eigengebrauch (kein privater Kreis). Das heisst, wenn eine Person einen Teil ihrer Festplatte Leuten zugänglich macht, welche nicht zum privaten Kreis gehören, so muss dafür gesorgt werden, dass auf diesem Teil keine urheberrechtlich geschützten Daten vorhanden sind. Dass die Daten auf der eigenen Festplatte abgespeichert werden spielt keine Rolle, denn wenn diese jedermann zugänglich ist, kann man nicht mehr von Eigengebrauch sprechen. Ausserdem zählen die Personen, welche dieselbe P2P-Software benutzen, nicht zum privaten Kreis, denn es kann sich jeder diese Software herunterladen, wodurch jeder die Möglichkeit hätte, zum privaten Kreis eines anderen zu gehören, ohne dass es dieser weiss.

Stellungnahme: Da das Kopieren von Daten auf Festplatte als Vervielfältigung gilt, ist dies nur für den Eigengebrauch erlaubt. Ist die Festplatte aber einer grösseren Anzahl Personen zugänglich, so handelt es sich nicht mehr um Eigengebrauch und man verletzt unter Umständen Urheberrechte. Jede Person, welche Teile ihrer Festplatte anderen zur Verfügung stellt, muss also dafür sorgen, dass sich auf dieser Festplatte keine urheberrechtlich geschützten Daten befinden. Ansonsten hat der Urheber das Recht, gegen diese Person juristisch vorzugehen.

b) Anwendung auf P2P-Anbieter

P2P-Software bietet eine gute Infrastruktur zum Tauschen von Daten. Dass diese Daten urheberrechtlich geschützt sein können, bestreitet niemand. Allerdings gilt die Vermittlung von urheberrechtlich geschützten Daten in der Schweiz nicht als Verletzung der Urheberrechte, wodurch rechtliche Schritte gegen P2P-Anbieter nicht möglich sind[10]. Nachfolgend werden wir auf den Fall Napster sowie die rechtliche Lage bei dezentralen P2P-Varianten (siehe Modell Gnutella und Modell Fasttrack) eingehen.

Napster unterhält eine zentrale Datenbank, auf welcher gespeichert ist, welcher Nutzer welche Daten auf seiner Festplatte zur Verfügung stellt. Dies stellt keine Verletzung der Urheberrechte dar, denn man bietet keine urheberrechtlich geschützten Daten an, sondern zeigt nur, wo diese zu finden sind (vergleichbar mit einer Suchmaschine im Internet). Daher hätte Napster in der Schweiz nicht verurteilt werden können. Allerdings wäre es möglich

---

[9] M. Pedrazzini, R. von Büren, E. Marbach: *Immaterialgüter- und Wettbewerbsrecht* s.72.

[10] Anders sieht die Situation bei Websites aus, welche MP3's anbieten wie z.B. www.mp3.com

gewesen, mit Hilfe der in der zentralen Datenbank gespeicherten Informationen gegen einzelne Nutzer vorzugehen, welche die Urheberrechte verletzt haben.

Bei Anbietern, welche dezentrale P2P-Software anbieten (siehe Modell Gnutella und Modell Fasttrack) sieht die Rechtslage gleich wie beim Fall Napster aus, denn auch hier werden keine urheberrechtlich geschützten Daten angeboten. Zusätzlich kann nur schwer gezeigt werden, dass geschützte Daten getauscht werden, denn es gibt keinen zentralen Server, welcher Informationen über die gerade verfügbaren Daten speichert. Aus diesem Grund ist es praktisch unmöglich, gegen Nutzer vorzugehen, welche urheberrechtliche Daten anderen zur Verfügung stellen.

2. Internationale Normen und Richtlinien der EU in Bezug auf das Urheberrecht

a) Anwendung auf P2P-Nutzer

Nach der Berner Übereinkunft geniesst der Urheber das ausschliessliche Recht, die Vervielfältigung seiner Werke zu erlauben. Den Verbandsländern bleibt aber vorbehalten, *„die Vervielfältigung in gewissen Sonderfällen unter der Vorraussetzung zu gestatten, dass eine solche Vervielfältigung weder die normale Auswertung des Werkes beeinträchtigt noch die berechtigten Interessen des Urhebers unzumutbar verletzt."* (Art. 9 Berner Übereinkunft)

In Bezug auf den P2P-Nutzer sieht die Rechtslage auf internationaler Ebene also gleich aus wie in der Schweiz. Da laut WIPO-Urheberrechtsvertrag *„die elektronische Speicherung eines geschützten Werks in digitaler Form als Vervielfältigung gilt"* (Art. 1 WTC), verletzt ein Nutzer, welcher urheberrechtlich geschützte Daten auf seiner Festplatte speichert und diese anderen Personen zugänglich macht, Urheberrechte.

In der EU ist die Rechtslage mit derjenigen auf internationaler Ebene vergleichbar. Nach der Richtlinie 2001/29/EG des europäischen Parlaments und des Rates vom 22. Mai 2001 sehen die Mitgliedstaaten *„für die folgenden Personen das ausschliessliche Recht vor, die unmittelbare oder mittelbare, vorübergehende oder dauerhafte Vervielfältigung auf jede Art und Weise und in jeder Form ganz oder teilweise zu erlauben oder zu verbieten:*

1) *Für die Urheber in Bezug auf ihre Werke,*
2) *Für die ausübenden Künstler in Bezug auf die Aufzeichnung ihrer Darbietung,*
3) *Für die Tonträgerhersteller in Bezug auf ihre Tonträger (...)* „ (Art. 2 Richtlinie 2001/29/EG)

Auch hier bleibt den Mitgliedsstaaten die Möglichkeit vorbehalten, Ausnahmen oder Beschränkungen *„in Bezug auf Vervielfältigung auf beliebigen Trägern durch eine natürliche Person zum privaten Gebrauch“* (Art. 5 Richtlinie 2001/29/EG) vorzusehen. Das Speichern von Daten auf einer Festplatte gilt als Vervielfältigung und ist nicht erlaubt, wenn die Festplatte der Allgemeinheit zugänglich ist (in diesem Fall kann man nicht von privatem Gebrauch sprechen). Deshalb verletzt ein Nutzer, welcher mittels Filesharing urheberrechtlich geschützte Daten anbietet, Urheberrechte.

b) Anwendung auf P2P-Anbieter

Die Vermittlung von urheberrechtlich geschützten Daten wird in der Berner Übereinkunft und dem WIPO-Urheberrechtsvertrag nicht behandelt und gilt daher nicht als Verletzung der Urheberrechte. Rechtliche Schritte gegen Anbieter von (zentraler oder dezentraler) P2P-Software sind daher auf internationaler Ebene nicht möglich.

Anders sieht die Rechtslage in der EU aus: Nach der Richtlinie 2001/29/EG des europäischen Parlaments und des Rates vom 22. Mai 2001 haben die Rechtsinhaber die Möglichkeit, gerichtliche Anordnung gegen einen Vermittler zu beantragen, welcher urheberrechtlich geschützte Daten in einem Netz überträgt:
„*Die Mitgliedstaaten stellen sicher, dass die Rechtsinhaber gerichtliche Anordnungen gegen Vermittler beantragen können, deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandter Schutzrechte genutzt werden*.“ (Art. 8 Richtlinie 2001/29/EG)
Wie die Realität zeigt, können sämtliche im Netz angebotenen P2P-Programme genutzt werden, um Urheberrechte zu verletzten. Es ist aber nur bei zentralen P2P-Systemen nachweisbar (z.B. Napster), dass Urheberrechte auch wirklich verletzt wurden. Bei allen dezentralen Systemen (siehe Modell Gnutella und Modell Fasttrack) kann dies nicht nachgewiesen werden. Im Folgenden wird auf diese beiden Fälle etwas genauer eingegangen.

Da Napster eine zentrale Datenbank unterhält, kann nachgewiesen werden, dass urheberrechtlich geschützte zum Tausch angeboten wurden, d.h. die Dienste der Musiktauschbörse können von den Nutzern zur Verletzung eines Urheberrechts genutzt werden. Nach der vorher genannten Richtlinie haben die Rechtsinhaber also die Möglichkeit gegen den Anbieter vorzugehen. Das bedeutet, dass Napster in Mitgliedstaaten, in welchen diese Richtlinien bereits umgesetzt wurden, hätte verurteilt werden können.

Bei dezentralen P2P-Systemen kann die Verletzung von Urheberrechten nicht so leicht nachgewiesen werden, da keine Informationen über die angebotenen Daten gespeichert

werden. Es lässt sich aber leicht feststellen, ob geschützte Daten angeboten werden, indem man sich ebenfalls in diesem Netz einloggt und nach urheberrechtlich geschützten Daten sucht. Findet man geschützte Daten, so haben die Rechtsinhaber auch hier die Möglichkeit, rechtliche Schritte gegen die Anbieter zu unternehmen.

Die Richtlinien der EU ermöglichen also den Rechtsinhabern, Druck auf die P2P-Anbieter auszuüben und diese so zum Einbau von Kontrollmechanismen, welche Urheberrechtsverletzungen verhindern sollen, in ihre Software zu bewegen.

III. Kontrolle von P2P-Systemen

Eine Kontrolle ist nur dann sinnvoll, wenn sie zum einen durchführbar ist und zum anderen Urheberrechtsrechtsverletzungen verhindern kann. Eine Lösung wie im Fall Napster macht nur wenig Sinn, da die durch die Musiktauschbörse begangenen Verstösse gegen das Urheberrecht zwar verhindert werden konnten, die Nutzer aber mit Hilfe einer anderen P2P-Software weiterhin urheberrechtlich geschützte Daten austauschen. Um einen Software-Wechsel zu verhindern, müssen einerseits die Kontrollen möglichst flächendeckend eingeführt werden, andererseits sollten die Programme mit eingebauter Kontrolle in punkto Auswahl, Bedienerfreundlichkeit und Preis möglichst nahe an die bisherigen Programme herankommen. Im folgenden werden einige Varianten zur Verhinderung von Urheberrechtsverletzungen aufgezeigt.

1. Mögliche Varianten zur Kontrolle von P2P-Systemen

Variante 1: Man versucht mit Hilfe eines Filters das Suchen oder den Transfer von urheberrechtlich geschützten Daten zu verhindern (das Abspeichern auf dem eigenen Computer ist also immer noch möglich). Da bei gewissen P2P-Programmen die Suchanfragen verschlüsselt werden und beim Download das HTTP-Protokoll verwendet wird, ist es nicht möglich, den Transfer von geschützten Daten durch Blockieren von einzelnen Protokollen zu unterbinden (würden die P2P-Programme ein proprietäres Protokoll verwenden, so wäre dies möglich). Aus diesem Grund muss das Filter in die Software eingebaut werden. Während bei dezentral aufgebauten P2P-Systemen in jede Software ein solches Filter integriert werden muss, genügt es bei zentralen Systemen, die Suchanfragen nach geschützten Daten im Server zu unterbinden. Da jede Datei spezifische Informationen zu den Daten enthält (MP3-Files besitzen z.B. einen Tag, welcher Interpret und Titel der Datei angibt), könnte das Filter anhand dieser Informationen entscheiden, welche Daten urheberrechtlich geschützt sind und welche nicht. Allerdings können diese Informationen leicht in ähnlich klingende Informationen geändert werden, wodurch die

Nutzer die Daten immer noch erkennen, das Filter jedoch versagt[11]. Besser ist es, sogenannte Wasserzeichen in die Files einzufügen, welche urheberrechtlich geschützte Daten markieren[12] (da diese Markierungen nicht entfernt werden können, ist es möglich, dass sie unter Umständen auch in den Files enthalten bleiben, wenn die Schutzfrist schon abgelaufen ist). Dadurch können urheberrechtlich geschützte Daten nicht mehr als ungeschützte „getarnt" werden. Es ist jedoch fraglich, ob diese Lösung die nötige Akzeptanz unter den Nutzern finden wird, denn sie schränkt die Auswahl der verfügbaren Daten stark ein (denn meist sind die interessanten Daten urheberrechtlich geschützt).

Variante 2: Die Produzenten (Musik-, Filmindustrie etc.) entwickeln ein eigenes System und bieten darüber ihre Daten an. Dadurch können auch andere Formate als MP3 verwendet werden, welche einen Kopierschutz beinhalten. Der Nutzer kann zwischen verschiedenen Abonnementen auswählen, je nachdem, wie seine Ansprüche sind. Mit dieser Variante kann der Urheber entschädigt werden und Urheberrechtsverletzungen werden so verhindert. Es existieren bereits Varianten, zum einen von Sony Music, Universal Music und EMI (*Pressplay*), zum anderen von AOL Time Warner, Bertelsmann und EMI (*Musicnet*). *Musicnet* verwendet das sogenannte RealAudio-Format. Der Nutzer kann sich die gewünschten Titel direkt herunterladen und anhören. Allerdings ist das Brennen auf CD's sowie das kopieren auf einen MP3-Player nicht möglich und nach einer gewissen Zeit werden die Titel wieder gelöscht. *Pressplay* verwendet das WMA-Format, welches auch von *Windows Media Player* genutzt wird. Hier ist das Brennen einer beschränkten Anzahl CD's erlaubt (wenn auch nur zwei Titel pro Interpret pro Monat), auch bleiben die Stücke erhalten[13]. Beide Lösungen verwenden ein Format mit Kopierschutz und verhindern so die unrechtmässige Vervielfältigung von Daten. Die Nachteile sind jedoch offensichtlich: Da jedes Netz nur etwa die Hälfte der gesuchten Daten anbieten kann (nur EMI ist an beiden Netzten beteiligt), müsste man *Musicnet* und *Pressplay* zusammen benutzen, was aber den meisten Nutzern zu teuer sein wird. Zudem sind die Angebote nicht besonders attraktiv, da sie den Benutzer zu sehr einschränken. Aus diesen Gründen wird es schwierig sein, eine breite Masse für *Musicnet* oder *Pressplay* zu gewinnen, v.a. wenn man mit den momentan erhältlichen P2P-Programmen ein besseres Angebot gratis bekommen kann.

---

[11] Wären z.B. alle Titel von ‚Pink Floyd' gesperrt, so könnte man seine MP3's einfach unter ‚Pink Flod' abspeichern, wodurch das Filter keine Urheberrechtsverletzungen entdecken kann, routinierte Nutzer den gewünschten Titel aber ohne weiteres finden.

[12] Auf die technischen Details wird hier nicht genauer eingegangen. Die Wasserzeichen sind so konzipiert, dass sie auch durch Komprimierungsvorgänge, Filterung oder Zerstörungsversuche nicht entfernt werden können.

[13] www.openp2p.com.

Variante 3: Der Anbieter von P2P-Software zeigt sich für eine rechtmässige Entschädigung des Urhebers verantwortlich, darf dafür aber eine Gebühr für die Suche und den Transfer von urheberrechtlich geschützten Daten verlangen. Die Software zeichnet auf, wie viele geschützte Daten transferiert wurden[14] und schickt diese Information in regelmässigen Zeitabständen (z.B. jeden Monat) an ein zentrales Abrechnungssystem, welches das Geld vom Nutzer einfordert[15]. Ein Vorteil dieser Lösung stellt die saubere Abrechnung dar. Der Nutzer bezahlt nur Gebühren für den Transfer von Daten, welche urheberrechtlich geschützt sind. Er kann aber weiterhin (urheberrechtlich geschützte) Daten für den privaten Gebrauch auf seiner Festplatte abspeichern. Ein weiterer Vorteil ist, dass die Auswahl an Daten nicht verringert wird (falls man davon ausgeht, dass die Anzahl Nutzer trotz Gebühr gleich bleibt). Allerdings ist diese Variante für die Anbieter nicht besonders attraktiv, weil das dazu benötige Abrechnungssystem doch einen hohen Aufwand nach sich zieht.

Variante 4: Wie bei **Variante 3** zeigt sich der Anbieter für eine rechtmässige Entschädigung des Urhebers verantwortlich. Der aufwändige Betrieb eines Abrechnungssystems wird nun aber vermieden, indem man Software, welche nur eine beschränkte Anzahl von Transfers zulässt, an die Nutzer verkauft. Ein integrierter Zähler ermittelt die Anzahl Transfers geschützter Daten und sperrt die Software beim Erreichen einer vorbestimmten Limite. Der Nutzer kann die Software nicht mehr nutzen, es sei denn, er bezahlt für eine weitere Anzahl Transfers. Diese Variante beinhaltet die Vorteile von **Variante 3**, ist aber weniger aufwändig und daher einfacher zu implementieren.

Variante 5: Produzenten (z.B. Musik-, Filmindustrie etc) gehen Allianzen mit Internet Service Providers (ISP, z.B. Swisscom, Cablecom,...) ein, wodurch mit einem Teil der Gebühren, welcher der Nutzer für den Internetanschluss bezahlt, die Urheber entschädigt werden. Die ISP können im Gegenzug ihren Kunden Zugriff auf Dienste der Produktionsfirmen[16] anbieten und damit Werbung machen. Ein Beispiel hierfür wäre eine Allianz zwischen *Pressplay* und *Cablecom*, wo in der Miete für den Internetanschluss die Benützung von *Pressplay* inbegriffen ist. Solche Allianzen machen durchaus Sinn, denn das Herunterladen von grossen Daten wie z.B. Filme ist nur mit genügend grosser Bandbreite

---

[14] Die Erkennung von urheberrechtlich geschützten Daten mittels eines Filters wurde bereits in Variante 1 behandelt.

[15] Für die Bezahlung gibt es verschiedene Varianten: Der Nutzer muss beim Bezug der Software eine Kreditkarten-Nummer angeben oder er hinterlässt eine Adresse, an die der Anbieter einen Vertrag schickt, welcher unterzeichnet zurückgesandt werden muss, damit die Software benutzt werden kann.

[16] Wie das Herunterladen von Musik,Filmen, Programmen etc. Siehe dazu Variante 2.

attraktiv. Der Vorteil dieser Lösung ist, dass der Preis für die Dienste der Verwertungsgesellschaften geringer sein werden als die Gebühren für den Breitbandanschluss, wodurch sich der Nutzer nicht zu sehr an den zusätzlichen Ausgaben stört. Ist das Angebot attraktiv genug, so verlieren P2P-Programme vielleicht ihren Reiz. Allerdings mangelt es im Moment an angebotenen Diensten. Es ist also mit grossem Aufwand seitens der Produktionsfirmen zu rechnen, will man mit dieser Variante Erfolg haben.

Variante 6: Die einfachste Möglichkeit ist das Erlassen einer Gebühr auf Festplatten. Sie ist allerdings nicht besonders elegant, da die meisten Daten auf einer Festplatte privat sind und anderen Benutzern freigegeben werden dürfen. Zudem bezahlt man damit auch Gebühren für Daten, welche nicht anderen Benutzern zugänglich sind.

2. Umgehungsmöglichkeiten

Alle sechs aufgeführten Varianten sind nach dem heutigen Stand der Technik machbar und verhindern Urheberrechtsverletzungen. Allerdings wurde bisher die Frage der Umgehung obiger Kontrollmechanismen noch nicht behandelt. Dies soll nun in zwei Teilen getan werden. Zum einen soll auf die technischen Umgehungsmöglichkeiten hingewiesen werden und zum anderen auf Möglichkeiten, welche kein technisches Fachwissen erfordern (wie z.B. das Wechseln der Software).

a) Technische Umgehungsmöglichkeiten

Die technischen Umgehungsmöglichkeiten beinhalten einerseits das Beseitigen der Kontrollmechanismen in der Software, andererseits das Benutzen eines P2P-Netzes mit einer „fremden“ Software, welche keine Kontrollmechanismen enthält.

Grundsätzlich kann davon ausgegangen werden, dass jeder Kontroll- und Schutzmechanismus beseitigt oder umgangen werden kann. Deshalb gilt es, diese Mechanismen so in die Software einzubauen, dass der Aufwand für einen „Hacker“ zu gross wird.
Während die Umgehung von Kontrollmechanismen der Varianten 1, 2 und 5 stark von der Wahl des Formates abhängt (wie gut lässt sich ein Wasserzeichen oder ein Kopierschutz entfernen?), hat man rein theoretisch bei den Varianten 3 und 4 unabhängig vom Format die Möglichkeit, die Kontrollmechanismen wirkungslos zu machen. Durch Manipulation der internen Methoden, welche zu Abrechnungszwecken benötigt werden, kann man dem System vermitteln, dass man gar keine urheberrechtlich geschützten Daten transferiert hat, und muss daher auch nichts bezahlen. Diese Methoden können aber beim Programmieren

geschickt in das Programm eingebaut werden, so dass es schwierig ist, die relevanten Stellen im Code ausfindig zu machen.

Des weiteren muss verhindert werden, dass mit Hilfe eines fremden Programms (welches keine Kontrollmechanismen enthält) auf ein Netz zugegriffen wird, ohne dass es der Anbieter bemerkt und daher Urheberrechtsverletzungen nicht verhindern kann. Dieses Problem sollte aber durch eine Verschlüsselung der Kontrollinformationen (z.B. Adressen der anderen Benutzer, Suchanfragen etc.) gelöst werden können, wobei verhindert werden muss, dass der „Hacker" in den Besitz des geheimen Schlüssels kommt (weiss er diesen Schlüssel, so kann er sämtliche Informationen entziffern und hat Zugriff auf das Netz). Auf die Details der Verschlüsselung soll hier nicht genauer eingegangen werden, es sei jedoch gesagt, dass aufgrund der grossen Bedeutung von kryptographischen Methoden zum Schutz von Datentransfer (z.B. eBanking) die heutigen Verschlüsselungsmethoden schon ziemlich ausgereift sind und ständig verbessert werden.

Da eine technische Umgehung von Schutzmechanismen in Software schon seit längerem ein Problem darstellt, sind laufend Bestrebungen im Gange, immer noch ausgeklügeltere Methoden zu entwickeln, welche eine solche Umgehung verhindern.
Aufgrund der dezentralen Struktur des Internets ist es aber unter Umständen gar nicht nötig, Schutzmechanismen zu umgehen, weil eine vergleichbare Software zu finden ist, welche diese Mechanismen gar nicht enthält. Auf diese Problematik soll im nächsten Kapitel eingegangen werden.

b) Umgehungsmöglichkeiten für den „technischen Laien"

Die von der EU erlassene Richtlinie (Art. 8 Richtlinie 2001/29/EG) stellt ein wichtiges Hilfsmittel dar um Urheberrechtsverletzungen zu verhindern, da die Rechtsinhaber die Möglichkeit haben, Druck auf die Anbieter von P2P-Software auszuüben, damit diese Kontrollmechanismen in ihre Programme integrieren. Ob dies den gewünschten Erfolg erzielt, hängt allerdings stark davon ab, wie viele der Anbieter zu einer solchen Massnahme bewegt werden können. Enthalten nur vereinzelte Programme Kontrollmechanismen, so werden die meisten Nutzer die Software wechseln, denn die Annahme, dass die Benutzer aus schlechtem Gewissen gegenüber dem Urheber zu einem Anbieter wechseln, welcher den legalen Tausch von Daten ermöglicht, trifft wohl nur bei den wenigsten zu.
Ein weiteres Problem stellt sich beim Austausch von Filmen über das Internet, denn selbst wenn der Austausch auf legalem Weg stattgefunden hat, so hat man immer noch die Möglichkeit, einen Film herunterzuladen, bevor die DVD im eigenen Land zum Verkauf angeboten wird. Um dies zu verhindern, müsste weltweit am gleichen Tag mit dem Verkauf von DVD's eines bestimmten Films begonnen werden.

Um den unrechtmässigen Austausch von urheberrechtlich geschützten Daten über das Internet zu verhindern, ist jedenfalls mit einem grossen Aufwand für die Rechtsinhaber zu rechnen, und selbst dann ist nicht sicher, ob die durchgeführten Massnahmen nicht bloss „ein Schuss in den heissen Ofen“ sind. Es wird jedenfalls interessant zu beobachten sein, wie sich die Situation in Zukunft entwickelt.

B. Urheberrecht und Software

Jährlich gehen Milliarden von Dollar durch Softwarepiraterie verloren. Darunter versteht man die illegale Verbreitung und/oder das Raubkopieren von Software für private sowie für geschäftliche Zwecke. Der unmittelbar auf Raubkopien zurückzuführende Schaden für die Softwareindustrie betrug so zum Beispiel 1996 weltweit mehr als 15 Milliarden US Dollar[17].

Während der Hersteller das Raubkopieren der Software sicher trifft, ist der letztendlich Leidtragende dieser kriminellen Handlungen der Verbraucher.
Unautorisiertes Kopieren von Software bringt ihre Entwickler um den gerechten Lohn ihrer Arbeit, erhöht damit den Preis (weil dieses Raubkopieren einkalkuliert wird) und folglich mangelt es an Qualität und behindert die Entwicklung von neuen Softwareprodukten.

Technischer Fortschritt ist natürlich nicht umsonst zu haben. Der Aufwand der Softwareentwicklung wird nur dann betrieben, wenn es sich für den Entwickler oder die Firma lohnt. Und dass es sich lohnt, sieht das Recht bestimmte Schutzrechte vor. Es stellt sich daher nicht die Frage, ob Software geschützt werden muss. Diese Frage wird fast jeder mit einem „Ja“ beantworten. Die Frage ist vielmehr wie, d.h. mit welchem Rechtsinstrument Software angemessen geschützt werden kann, sowie ob und welche technischen Massnahmen es gibt, um Software zu schützen.

Ohne, dass nun eindeutig geklärt ist, was Software eigentlich ist, wird sie analog zu Literatur zum Gegenstand des Urheberrechts gemacht, weil sie sich der "Sprache als Ausdrucksmittel" bedient. Software wird in einer von Menschen lesbaren Programmiersprache geschrieben und dann mit einem "Compiler" (eine Art Übersetzer) in eine lange Folge von „0“ und „1“ übersetzt, die wiederum für den Computer eine Art Sprache darstellt, die festlegt, was er genau machen soll. Den menschenlesbaren Teil davon bezeichnet man als Source-Code[18].

Software ist leicht kopierbar, weil sie immer digital vorliegt. Das bedeutet, dass jede Kopie nicht mehr vom Original unterscheidbar und genauso nutzbar ist. Bei analogen Medien, wie Schallplatten oder Büchern, ist das Kopieren immer mit einem Verlust an Qualität verbunden. Die Digitalisierung auch dieser Bereiche durch CDs, ebooks usw. führt dazu, dass das (unerlaubte) Kopieren auch hier immer einfacher wird. Als Kopierwerkzeug dient

---

[17] Geschätzter Wert der Business Software Alliance (BSA)

[18] Auch Quellcode genannt

einfach das Allround-Werkzeug, der PC. Deshalb geht auch bei "Multimedia" der Trend in Richtung eines die Nutzung stark einschränkenden Urheberrechts[19].

Software ist also als geistiges Gut geschützt, unabhängig davon, ob sie als Source-Code, in Papierform, auf einer Diskette usw. existiert. Damit wird Software eigentlich auch nicht verkauft, sondern "zur Nutzung überlassen". Wie diese Nutzung aussieht, ist von Programm zu Programm verschieden und in den jeweiligen Nutzungsbedingungen, den Lizenzen, vertraglich festgelegt. Gekaufter Software liegt normalerweise eine solche Lizenz bei, ob in gedruckter oder elektronischer Form. Häufig wird sie beim Installieren von Programmen in einem Fenster angezeigt, bis man mit einem Mausklick bestätigt, sie anzuerkennen. Oft legen die Lizenzen auch inhaltliche Bedingungen für die Nutzung fest, wie z.B. die Beschränkung auf private Nutzung und auf nur einen Computer.

Um den rechtlichen Status von Software genauer analysieren zu können, ist es notwendig, zwischen verschiedenen Softwaretypen zu differenzieren, denn es ist bei weitem nicht so, dass jede Software gekauft werden muss und der Source-Code nicht jedem frei zur Verfügung steht. Deshalb werden im folgenden Abschnitt die oft zu Verwirrung führenden Fachausdrücke definiert und erklärt.

I. Definition und Differenzierung von Software

1. Kommerzielle Software und ihr rechtlicher Status

Kommerzielle Software ist Software, die von einer Firma mit dem Ziel entwickelt wird, aus der Benutzung dieser Software Geld zu machen. Dazu gehören Produkte wie Microsoft's Word, Excel, PowerPoint oder auch Photoshop oder Pagemaker von Adobe. In den Source-Codes dieser Programme darf nur bedingt Einsicht genommen werden, so z.B. zu Sicherstellung der Funktionalität mit einem anderen Programmen (Interoperabilität)[20].
Heute unterliegt kommerzielle Software automatisch dem Urheberschutz[21], zum Teil ist bestimmte Software auch patentierbar[22]. Das Copyright (unter Copyright verstehen wir eigentlich Urheberrecht, auch wenn das ausser Juristen kaum jemand sagt), das ursprünglich zum Schutz von schriftstellerischen und künstlerischen Werken geschaffen wurde, schützt allerdings nicht die Idee, die hinter einer bestimmten Software steckt. Es schützt „nur" den

[19] siehe Kapitel A. Peer to Peer

[20] Urheberrechtsgesetz (URG), Kapitel 5, Art. 21, Abschnitt 1,2

[21] Urheberrechtsgesetz (URG), Kapitel 2, Art.2, Abschnitt 3

[22] siehe Kapitel B. II. Vom Urheberrecht zur Patentierung von Software

Wortlaut des jeweiligen Programms. Der Begriff „Urheberrecht" bezeichnet zwei Dinge: einmal die Sammlung von Gesetzen, die Rechte rund um geistige Schöpfungen regeln, zum anderen ist es das Recht selbst, das dem Schöpfer oder der Schöpferin zusteht, über das Werk nach eigenen Vorstellungen zu verfügen.
Das Kopieren und die Weitergabe (falls nicht vertraglich ausgeschlossen) von kommerzieller Software ist gemäss dem allgemeinen Urheberrecht verboten (bzw. dem Rechtsinhaber vorbehalten). Hier sind die Vorschriften mittlerweile strenger als beispielsweise bei Audio-CDs. Bei Audio-CDs ist immer noch eine sogenannte private Kopie erlaubt, genauso wie das Kopieren von Büchern in einem gewissen Umfang. Ein gewisser Anteil der Einnahmen für Papierkopien in Copyshops und Büros und den Verkauf von leeren Kassetten fliesst über die Verwertungsgesellschaften an die Urheber zurück, um den möglicherweise dabei erlittenen finanziellen Nachteil wieder auszugleichen. Bei Software gibt es so etwas nicht (Kopie für den Eigengebrauch ist unzulässig), weil sich die zum Teil erheblich voneinander abweichenden Preise und damit mutmasslichen Verluste nicht über eine solche Pauschalabgabe abdecken liessen. Die Anfertigung einer Sicherheitskopie ist jedoch erlaubt.

Die Anwendung des Urheberrechts auf kommerzielle Software ist auch von wirtschaftlicher Natur. Während früher der Persönlichkeitsschutz der künstlerisch-geistig Schaffenden im Vordergrund stand, dient das Urheberrecht heute mehr der Wahrung von wirtschaftlichen Interessen. Das Urheberrecht ist ein Fundament ganzer Wirtschaftszweige wie Verlage, Plattenfirmen, Radio und Fernsehen geworden. Das Urheberrecht hat sich vom Kulturrecht zum Wirtschaftsrecht gewandelt. Dabei sollte man sich wirklich fragen, ob das Urheberrecht das richtige Mittel ist, um um kommerzielle Software zu schützen. Steht nicht gerade das traditionelle Urheberrecht etwas quer zur Idee des Softwareschutzes ?

Was jetzt, nach einem Jahrhundert, übrig bleibt, sind von der Industrie vorgegebene Gesetze, die festlegen, wie man mit Urheberrecht Geld macht.
(Mike Godwin in einer Rezension des Buches Copywrong)

Mit der weiten Verbreitung von Computern entstand der Bedarf, auch in diesem Bereich das Urheberrecht gesetzlich zu regeln - vor allem als kommerzielle Software mit der Einführung des Personal Computers (PC) anfing, zu einem Massenprodukt zu werden. Eine zur kommerziellen Software parallel ablaufende und komplett verschiedene Entwicklung beschreibt jedoch die sogenannte Open-Source Software.

2. Open-Source Software (Free Software)[23]

GNU[24], BSD[25], Mozilla[26], Apache[27] und viele mehr sind die Bezeichnungen für Software, welche in den letzten Jahren eine neue Ära im Umgang mit Softwareprodukten und Software-Know-how einläuteten. Geheimhaltungsvereinbarungen betreffend Softwarecodes sind vorbei. Am Markt gewinnt nicht der Eigentümer eines Produktes (Inhaber der Urheberrechte), sondern derjenige, welcher mit dem Softwareprodukt und den Marktbedürfnissen entsprechend umgehen kann. Wer den Source-Code seiner Software öffentlich zugänglich macht (sein Softwareprodukt als Open-Source deklariert), beschreitet neue Wege. Er macht über Internet jedermann das sogenannte Engineering seiner Software möglich und stellt sich den Diskussionen der News-Gruppen[28]. Zudem schafft er dem Produkt die Möglichkeit, dass es weltweit eingesetzt und weiter entwickelt werden kann, sowie dass es sich gegenüber anderer, insbesondere kommerzieller Software am Markt behauptet und vielleicht sogar durchsetzen kann.

a) Geschichte und Motivation der Open-Source Bewegung

„Linux übernimmt die Weltherrschaft", „Linux hat den Durchbruch geschafft", „Linux - mit Volldampf voraus!" - das Betriebssystem Linux[29], das als Open-Source Software jedem frei zugänglich ist, sorgt für Schlagzeilen, und das nicht nur in der Fachpresse. Ausgelöst wurde der Pressewirbel durch die Ankündigungen der grossen Computerhersteller wie IBM, Hewlett Packard und Compaq, ihre Hardware mit Linux auszustatten. Damit erhält das Microsoft-Betriebssystem Windows, mit dem die Mehrzahl der PCs ausgestattet ist, nichtkommerzielle Konkurrenz. Dass bereits rund 10 Millionen Computer unter Linux laufen und 1998 etwa 750000 Server mit diesem Betriebssystem bestückt wurden, zeigt die Entwicklung von Linux zu einer ernstzunehmenden Alternative mit Bedeutung für die gesamte Computerindustrie. Allerdings macht nicht Linux allein den Erfolg der Open

---

[23] Open-Source und Free Software ist per Definition gleich

[24] Das GNU Projekt wurde 1983 begonnen, um ein vollständiges Unix-artiges Betriebssystem zu entwickeln, das freie Software ist – das GNU System. (GNU ist eine rekursive Abkürzung von „GNU's Not Unix!" (http://www.gnu.org)

[25] BSD steht für Berkeley Software Distribution, die Weiterentwicklung von UNIX durch die Computer Systems Research Group (CSRG) an der University of California, Berkeley (UCB)

[26] Mozilla ist ein Open-Source Web Browser, der hauptsächlich für Web-Entwickler geschrieben wird (http://www.mozilla.org)

[27] Apache ist ein kostenloser Open-Source Webserver (weltweit am meisten verbreitet, da er sehr leistungsfähig und stabil ist)

[28] News-Gruppen sind Kommunikationskanäle im Internet zum Austausch von Interessen und Wissen

[29] Linux ist ein Betriebssystem für verschiedene Hardware-Plattformen (http://www.linux.org)

Source Software aus; zahlreiche weitere Computerprogramme werden auf diese Weise verbreitet.

Die Idee von „freier Software“ entwickelte sich aus dem Bedürfnis vieler Programmierer, vorhandene Software nach den eigenen Anforderungen weiterentwickeln zu können. Dazu fehlte aber bei der kommerziellen Software der Quellcode, der zur Änderung und Weiterentwicklung von bestehender Software erforderlich ist, und rechtlich die Erlaubnis der Rechtsinhaber, die erworbene Software zu verändern.

Richard Stallmann gründete 1983 in den USA die „Free Software Foundation“ (FSF)[30] mit dem Ziel, ein System freier, UNIX-kompatibler[31] Software zu entwickeln. Der Kerngedanke dieses GNU-Systems besteht darin, Software jedermann kostenlos mit dem Quellcode verfügbar zu machen, wobei alle Nutzer von der Weiterentwicklung anderer profitieren, weil eben diese Änderungen wieder kostenfrei zur Verfügung gestellt werden.

Praktisch funktionieren kann dieses System nur, weil zahlreiche Programmierer an der Verbesserung der Software arbeiteten, ohne dafür bezahlt zu werden. Der Ansporn zur immer weiterreichenden Entwicklung der Software war, komplizierte Lösungen auf nicht triviale Probleme zu finden und dadurch bekannt zu werden. Dabei wurde eine Eigendynamik erzeugt, die zu einem guten Teil auf dem Wissensaustausch in News-Gruppen beruht, wo die Nutzer dieser Software Probleme in einem grossen Forum präsentieren können. Dadurch beschäftigt sich immer eine grosse Zahl von Spezialisten mit den praktisch auftretenden Problemen.
Herzstück in dem von der Free Software Foundation initiierten GNU-System ist das Betriebssystem Linux.

Die Entwicklung von Linux wurde vom finnischen Informatikstudenten Linus Torvalds 1991 begonnen. Torvalds wollte seinen privaten PC mit einem Betriebssystem versehen, das UNIX-Funktionalität besass. Das seit 1975 kommerziell vertriebene UNIX war ihm aber zu teuer und zu umfangreich für den eigenen PC, so dass Torvalds begann, ein eigenes UNIX-kompatibles Betriebssystem zu entwickeln. Er stellte Linux unter die „General Public License“ (GPL)[32] von GNU und bat im Internet um Mitarbeit an dem neuen System.

---

[30] (http://www.fsf.org)

[31] Unix ist ein Betriebssystem, das von den Bell-Laboratories in den 70er Jahren entwickelt wurde. Heute gibt es verschiedene Unix-Derivate wie SunOS, Solaris, HP Unix oder AIX

[32] General Public license (GPL) siehe Kapitel B. II. 2. b) Die GNU General Public License und ihr rechtlicher Status

Interessierte aus aller Welt begannen, Linux mit gewaltiger Dynamik weiterzuentwickeln. Ein „Komitee“ sichtet die jeweiligen Verbesserungen und entscheidet, was davon der jeweils neuen „offiziellen“ Versionsnummer unterstellt wird.

Besondere Merkmale von Linux sind seine im Verhältnis zu Windows grössere Stabilität und Schnelligkeit - was gerade bei Betriebssystemen von Unternehmen von Bedeutung sein kann -, aber auch eine geringere Anwenderfreundlichkeit für Laien. Daher fand das Betriebssystem zunächst Eingang in die professionellen Systeme. Die neueste Entwicklung von benutzerfreundlichen Bedieneroberflächen lässt aber auch eine Ausweitung im Bereich der PCs (Private Anwendungen) erwarten.
Ein weiterer Schub für die Verbreitung von Linux sind die zahlreichen Distributoren[33]. Distributoren sind kommerziell arbeitende Firmen, die Linux auf Datenträgern verkaufen und dazu Handbücher und einen Kundenservice anbieten.
So soll der Distributor „Red Hat“ nach eigenen Angaben innerhalb weniger Monate 5 Millionen Nutzer gewonnen haben. Auch die grossen Computerfirmen wie IBM, die jetzt Linux auf ihrer Hardware vorinstallieren wollen, arbeiten mit den Distributoren zusammen. Damit wird ein Hauptproblem für die Verbreitung von Linux gelöst, nämlich der mangelnde Kundenservice. Anders als die „Linux-Gemeinde“, die sich via Internet in Diskussionsforen und News-Gruppen informiert, ist die Mehrzahl der Nutzer von PCs auf einen Kundendienst angewiesen.

In Anbetracht der erheblichen Beachtung, die Linux und die Free Software Foundation in der Fachöffentlichkeit der Computerwelt erfahren, mag es verwundern, dass, soweit ersichtlich, Stellungsnahmen in der juristischen Öffentlichkeit bislang relativ selten sind. Dies zu Recht, denn durch die GNU General Public License entfallen die meisten Probleme bzgl. Urheberrecht wie sie etwa bei kommerzieller Software auftreten.

b) Die GNU General Public License und ihr rechtlicher Status

Die Free Software Foundation definiert Free Software als Software, die von jedermann benutzt, kopiert oder verteilt werden darf, sei es unverändert oder mit Modifikationen, kostenlos oder gegen Bezahlung, stets aber mit dem Source Code.
Die Free Software Foundation ist auch Initiant der GNU General Public License, der GNU Library General Public License und der GNU Lesser General Public License. Diese Lizenzen sollen die Verbreitung Freier Software fördern und die rechtlichen Rahmenbedingungen schaffen. Eine deutsche Übersetung der GNU General Public License (auch GPL genannt) findet man unter (http://www.tu-harburg.de/dlhp/DE-GPL.html)

[33] Es gibt verschiedene Linux Distributoren wie z.B. Red Hat, Suse, Mandrake

Die GNU Lesser General Public License ist die Nachfolgerin der "GNU Library General Public License".
Wer eine Open-Source Lizenz hat, kann gebührenfrei auf den Source-Code der Software zugreifen und hat grundsätzlich die Erlaubnis, die Software beliebig zu gebrauchen, d.h. auch zu verändern.
Der Begriff Open-Source ist klar abzugrenzen, einerseits von Freeware (siehe Kapitel 2.3), bei welcher kein Quellcode offen gelegt wird und nur eine Gratislizenz vorliegt und anderseits von der Public Domain Software, bei welcher der Urheber sein Urheberrecht aufgibt und sämtliche Rechte am Programm der Öffentlichkeit übergibt.
Auch innerhalb der Open-Source Welt gibt es noch zwei grundsätzliche Unterscheidungen, nämlich in sogenannte Copyleft-Lizenzen, bei welchen der jeweilige Lizenznehmer Änderungen und Weiterentwicklungen an einem Open-Source Programm wieder freigeben muss, d.h. der Öffentlichkeit zur Verfügung stellt und zwar unter denselben Lizenzbedingungen, wie das ursprüngliche Programm. Die bedeutendste aller Copyleft-Lizenzen ist die oben erwähnte GNU General Public License GPL.
Daneben gibt es die Non-Copyleft Open-Source Lizenzen, bei welchen es dem Programmierer, welcher eine Open-Source weiterentwickelt oder verändert, entscheiden kann, ob er den neuen Quelltext der Öffentlichkeit zugänglich machen oder geheimhalten möchte. Non-Copyleft Open-Source hat auch die Bezeichnung BSD (Berkley Software Distribution).

Selbstverständlich gibt es auch Mischformen, so beispielsweise die Netscape-Public-License. Hier muss der Software-Entwickler den neuen Quelltext der Allgemeinheit zur Verfügung stellen, Netscape selbst behält sich zudem das Recht vor, diese Weiterentwicklungen in seinen proprietären Programmen zu verwenden.

3. Freeware

Freeware hat keine allgemein akzeptierte Bedeutung. Man versteht jedoch darunter Software, die kostenlos verteilt oder vom Internet heruntergeladen werden kann, aber nicht geändert werden darf, und deren Source-Code nicht erhältlich ist.
Beispiele für solche Freeware sind der Acrobat Reader (Adobe) zum Lesen und Ausdrucken von PDF[34] Dateien oder der Flash Player (Macromedia) um Webseiten die auf Flash-Animationen aufgebaut sind anzuschauen. Der rechtliche Rahmen wird durch individuelle Lizenzbestimmungen festgelegt (am Beispiel vom Acrobat Reader: http://www.adobe.com/products/acrobat/acrreula.html) und muss z.B. beim herunterladen

[34] PDF steht für Portable Document Format und ist ein offener Standard für die weltweite Distribution von Dokumenten in elektronischer Form

durch einen Mausklick bestätigt werden. Da aber jedermann kostenlos zu Freeware kommt, sind Probleme wie unerlaubtes Kopieren, wie das bei der kommerziellen Software der Fall ist, kaum vorhanden. Zudem ist der Source-Code ein offener Standard und folglich hat niemand das Interesse, den Source-Code zu ändern und dann als neue Software (nicht mehr dem Standard entsprechend) zu verkaufen.
Dank offenen Standards wie PDF kann man nun Textdokumente auf jeglichen PDF-tauglichen elektronischen Geräten öffnen und bearbeiten. So ist es heute möglich, ein Textdokument, das auf dem PC geschrieben wurde, auf irgendeinem anderen Gerät wie z.B. einem Handheld oder Communicator, sofern diese den PDF Standard unterstützen, ohne Problem zu öffnen, unabhängig vom Betriebssystem.

4. Public Domain Software

"Public Domain" ist ein Rechtsbegriff, der vor allem in den USA gebraucht wird. Software, die "Public Domain" ist, unterliegt nicht dem Urheberrecht. Public Domain Software hat eine interessante rechtsgeschichtliche Entwicklung. In den USA wurden mit öffentlichen Mitteln Softwareprojekte an Universitäten gefördert. Die so geförderte Software durfte nicht verkauft werden, sondern gehörte der Allgemeinheit. Diese Idee fand auch Anklang im privaten Bereich. Viele Programmierer stellten ihre Software daraufhin ebenfalls als Public Domain Software zur Verfügung. Der Entwickler gibt das Copyright an seinem Programm auf und stellt es kostenlos der Allgemeinheit zur Verfügung. Jeder darf das Programm beliebig kopieren, weitergeben und sogar verändern. Allein die kommerzielle Verwertung bleibt untersagt.

5. Shareware

Shareware ist kommerzielle Software, die zunächst einmal für eine Testzeit benutzt werden darf, ohne dafür zu bezahlen. Erst wenn man sich dazu entschliesst, das Programm dauernd zu benutzen, muss man einen kleinen Betrag an den Autor oder die Autorin schicken. Nicht immer ist das Bezahlen von Shareware ganz einfach, vor allem, wenn die Software aus dem Ausland kommt und der Weg über die Kreditkarte nicht möglich (oder nicht gewollt) ist. Deshalb haben sich vereinzelt Organisationen gegründet, in denen sich Autoren, Händler und Mail-Box-Betreiber zusammentun, um sowohl den Software-Vertrieb als auch die Registrierung zu erleichtern. Die bekannteste ist wohl die Association of Shareware Professionals (ASP) - zu finden im Internet unter: http://www.asp-shareware.org.
Da Shareware rechtlich gesehen gleich zu behandeln ist wie kommerzielle Software, unterliegt auch sie den Bestimmungen des Urheberrechts, wobei je nach Lizenzvertrag gewisse Abweichungen möglich sind. So ist z.B. im Allgemeinen ein Erstellen und Weitergeben einer Kopie an einen Interessenten erlaubt.

6. Crippleware, Careware

Crippleware ist eine spezielle Form von Shareware, allerdings mit eingeschränkter Funktionalität („Verkrüppelte" Software). Zum Beispiel lässt sich ein Dokument nicht drucken oder speichern, die Dimensionierung von Feldern oder Datensätzen könnte stark reduziert sein, oder besondere Zusatzfunktionen sind nicht aktiv. Nach einer bestimmten Zeit kann die Software auch den Dienst verweigern. Das Ganze hätte dann nur Demo-Charakter und soll zum Erwerb der Vollversion animieren.

Unter Careware versteht man Shareware, bei der der Entwickler auf den Gewinn verzichtet und ihn statt dessen einer genannten gemeinnützigen Organisation zukommen lässt. Für den Anwender gelten ansonsten die gleichen Regeln wie bei normaler Shareware.

II. Vom Urheberrecht zur Patentierung von Software

Ein Trend der sich seit geraumer Zeit abzeichnet hat, ist dass kommerzielle Software nicht nur mehr dem Urheberrecht unterstellt ist, sondern in gewissen Fällen auch patentiert werden kann.

Einmal mehr eilt der technische Fortschritt den gesetzlichen Regelungen voraus. So schliesst etwa das Patentgesetz den Schutz von Computerprogrammen als solchen ausdrücklich aus. Doch neuere Entwicklungen haben die Prüfungsrichtlinien der meisten Patentämter den praktischen Erfordernissen angenähert.

Einerseits bietet das Urheberrecht, das Software-Entwicklungen automatisch schützt, aufgrund der fehlenden Eintragung und Prüfung in einem amtlichen Verfahren nur eine schwache Rechtsposition für den kreativen Programmierer. Selbst bei Kennzeichnung der Urheberschaft etwa im Programmkopf ist lediglich die unautorisierte Vervielfältigung und Nutzung durch Dritte gerichtlich angreifbar. Der eigentliche „Kern“ jeder Software, die Algorithmen, bleiben im Unterschied zum Patent ungeschützt.

Andererseits führte der wachsende Einzug mikroelektronischer Steuerungen (durch Software implementiert) in nahezu allen Bereichen des täglichen Lebens zu einem hohen wirtschaftlichen Potential der Steuerprogramme für aktive Elektronikkomponenten. Inzwischen wurden allein in Europa mehr als 30.000 Software-Patente erteilt.

Das Europäische Patentamt unterscheidet heute zwischen Software „als solcher" und Software mit „technischem Charakter". Eine Software weist nach amtlicher Auffassung dann einen „technischen Charakter"[35] auf, wenn:

- die Software selbst ein technisches Problem löst (z. B. Steuerungs- und Regelungssysteme)

- bei der Ausführung der Software ein zusätzlicher technischer Effekt auftritt, wobei physikalische Veränderungen in der Hardware (wie sie bei jeder Ausführung von Software auftreten) nicht ausreichen. Neuheit und Erfindungsgrad vorausgesetzt, erkennen die meisten Patentämter z.B. Software als patentfähig an, die höhere Datentransferraten ermöglicht, die eine höhere Auflösung etwa in der Bildverarbeitung erzielt oder effektivere Datenkompression oder -speicherung bewirkt.

Der alte Grundsatz „Software ist nicht patentfähig" gilt also nicht mehr. Inwieweit die Patentierung von Software-Produkten in der Praxis aber tatsächlich sinnvoll ist, kann letztlich nur im Einzelfall entschieden werden. Bei sehr kurzen Produktlaufzeiten ist an Stelle eines zeit- und kostenaufwendigen Patentierungsverfahren oftmals eine Geheimhaltung der Algorithmen und insbesondere des Quellcodes bei Kennzeichnung des Autors bzw. der Firma (resp. Hochschule) ausreichend.
Ein Trost bleibt den Urhebern von Software (ob patentfähig oder nicht) in jedem Falle: Das Urheberrecht erstreckt sich bis zu 50 Jahre[36] nach den Tod des Autors und kostet keinen Cent. Jedes noch so kostspielige Patent läuft spätestens 20 Jahren nach Anmeldung aus.

Die Patentierung von Software kann unter Umständen aber zum grossen Problem in der Entwicklung von Computerprogrammen führen. In den USA kann Software auch dann patentiert werden, wenn ihr lediglich ein Algorithmus, das heisst eine Rechenregel oder eine Geschäftsidee, zugrunde liegt. Die Regelung in den USA birgt die Gefahr in sich, dass auch einfache Befehlsfolgen - sofern sie die übrigen Bedingungen erfüllen - patentiert werden können. Für Einzelprogrammierer und Kleinbetriebe wird es dann immer schwieriger, bei allen verwendeten Programmbausteinen zu überprüfen, ob sie bereits dem Patentschutz unterliegen. Deshalb wird nicht zu unrecht befürchtet, dass die Ausweitung der Möglichkeit des Patentschutzes auf alle Software-Produkte zu einem Erliegen der Arbeit freier

[35] Bericht zur Technizität von Software in der NZZ vom 25.9.01 und vom 11.2.02

[36] Urheberrechtsgesetz (URG), Kapitel 6, Art. 29, Abschnitt 2a

Programmierer führt und Software-Herstellung nur noch in grossen Weltunternehmen mit entsprechenden Rechtsabteilungen möglich ist.

C. Urheberrecht und WWW

Seit der Erfindung des World Wide Web (WWW) und des ersten Browsers im Jahr 1991 hat das rasante und turbulente Wachstum dieses neuen Mediums unter anderem auch zu erheblichen Herausforderungen im Bereiche des Urheberrechtes bzw. Urheberschutzes geführt.

Ursprünglich von einigen wenigen Teilnehmern zur Publikation und zum Austausch von wissenschaftlichen Informationen genutzt, entwickelte sich das WWW rasch zu einem Netzwerk mit heute über 530 Millionen Nutzern (2001), deren Interesse sich bei weitem nicht nur auf wissenschaftliche Texte beschränkt. Ob und wie der rechtliche Schutz der Inhalte mit dieser Entwicklung Schritt halten konnte, soll im vorliegenden Abschnitt untersucht werden.

Zuvor soll jedoch eine kurze technische Definition den Begriff des WWW erklären und abgrenzen.

Das World Wide Web ist eine der Anwendungen, die auf der Plattform des Internets laufen. Wichtig ist hier zwischen den Begriffen des WWW und des Internets zu unterscheiden, die umgangssprachlich oft gleichgesetzt werden: Das Internet stellt sozusagen die technische Infrastruktur dar, das WWW ist nur eine der Applikationen (neben E-Mail, FTP, File-Sharing etc.) die von dieser Plattform Gebrauch machen.

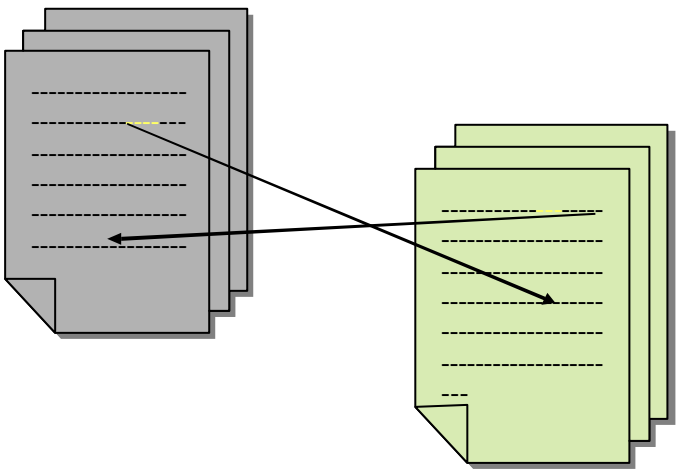

Abb 1HTML Dokumente mit Hyperlinks

Grundelement des WWW sind Hypertextdokumente. Hypertext enthält sog. Links - direkte Verweise zu anderen Hypertextdokumenten. Im WWW ist es möglich, durch anklicken dieser Links mit der Maus von einem Dokument zu einem anderen zu „springen“. Dieser Vorgang wird als „browsen“ bezeichnet und wird in der Regel mit einem der Web-Browser wie Netscape oder Internet Explorer ausgeführt. Salopp formuliert könnte man das WWW als „das, was man im Browser sieht“ definieren.

Dieser Abschnitt beschränkt sich also auf die Diskussion urheberrechtlicher Fragen im Zusammenhang mit dem WWW und geht nicht auf andere Applikationen des Internets wie E-Mail etc. ein.

I. Schutz von Inhalten

Im Zusammenhang mit dem World Wide Web haben sich eine grosse Anzahl neuer urheberrechtlicher Fragen ergeben. Eine Auswahl dieser Probleme soll hier genauer untersucht werden. Als erstes soll der Schutz von Web-Site Inhalten untersucht werden. Diese umfassen im Allgemeinen vor allem Text und Bilder, weshalb diesen beiden Punkten ein eigener Unterabschnitt gewidmet ist. Im selben Themenkreis wird auch die Frage nach dem Schutz eines grafischen Layouts einer Web-Site behandelt.

Bezug auf den Titel dieser Arbeit nehmend, lohnt es sich zuerst einen Blick auf den *Stand der Technik* zu werfen. Die Browser sind heutzutage, was den Benutzerkomfort angeht, sehr ausgereift. So lassen sich Web-Seiten mit wenigen Mausklicks speichern oder drucken, einzelne Textpassagen können markiert kopiert und direkt weiterverwendet werden, Bilder können ebenfalls einfach gespeichert oder in eigene Dokumente eingebunden werden.
Kurzum: Die Zugänglichkeit des WWW erlaubt den Zugriff auf schier unermessliche Datenmengen, die einfache Bedienung der Browser fördert das bedenkenlose Kopieren von dieser Daten. Die Frage die sich stellt, ist, ob die herkömmlichen rechtlichen Methoden ausreichen, um die Verwendung dieser Inhalte zu regeln oder ob allenfalls zusätzliche Massnahmen notwendig sind – also ob der Stand des Rechts dem der Technik entspricht.
In den folgenden Abschnitten werden die drei im WWW am häufigsten anzutreffenden Inhalte in Bezug auf urheberrechtliche Fragen untersucht: Es handelt sich im einzelnen um Texte, Bilder und Gesamtlayouts von Web-Seiten[37].

[37] Multimedia Applikationen wie Flash sollen hier nicht untersucht werden: Sie setzen sich ebenfalls aus den erwähnten Elementen zusammen (unter Umständen kommen noch Audiodaten hinzu – diese werden jedoch im Abschnitt über Peer to Peer diskutiert).

Alle drei Typen müssen den gleichen Kriterien genügen, um urheberrechtlichen Schutz beanspruchen zu können: Art. 2 Abs. 1 URG setzt voraus, dass das Werk eine *geistige Schöpfung* ist und *individuellen Charakter* hat.
Eine Kopie liegt vor, bzw. eine Verletzung des Urhebberechtes tritt gemäss Art. 19 URG dann ein, wenn ein veröffentlichtes Werk für nicht private bzw. nicht interne Zwecke kopiert wird. In Bezug auf das WWW handelt es sich in den meisten Fällen um die Veröffentlichung der übernommenen Inhalte auf einer Web-Site.

1. Texte

In der Schweiz sind „literarische, wissenschaftliche und andere Sprachwerke" nach Art. 2 lit. a URG eindeutig als Werk deklariert und somit dem Schutz des Urheberrechtes unterstellt. Unbestritten dürfte auch sein, dass auf Web-Seiten publizierte Texte dieser Werkgruppe angehören – es sei denn, es handelt sich um Texte, die laut Art. 5 Abs. 1 URG und Art. 5 Abs. 2 URG allgemein keinen Schutz geniessen.
Somit ist es nach Schweizer Recht unzulässig fremde Texte, die den oben definierten Kriterien für ein Werk genügen im WWW zu publizieren. Dabei spielt es keine Rolle, ob die Texte von einer anderen Web-Site kopiert wurden, von einem anderen digitalen Datenträger kopiert wurden oder aus anderen Medien mittels eines Scanners in digitale Form gebracht wurden.

Hat ein Autor den Verdacht, dass sein eigenes Werk auf illegale Weise im WWW veröffentlich wurde[38], so kann eine Kopie eigentlich relativ leicht gefunden werden *wenn der Text in seiner Gesamtheit, d.h. mit den gleichen Formulierungen etc.* übernommen wurde: Es genügt einen oder zwei Sätze aus dem Werk in einer der Suchmaschinen wie Google[39] einzugeben, um allfällige Kopien aufzufinden.
Diese Methode versagt natürlich, wenn der eigentliche Inhalt übernommen wurde, jedoch neu formuliert wurde, was aber auch kein urheberrechtliches Problem wäre, da das URG nicht den Inhalt sondern die Form schützt.
Verschiedene digitale Dokumentformate und Applikationen erlauben Schutzmassnahmen oder zumindest die Identifizierung der Urheber anhand beigefügter Daten. Einige Ansätze sind in Kapitel D.II *Digital Rights Management (DRM)* zu finden.

Oft ergibt sich auch die Frage, ob Texte, die unter urheberrechtlichem Schutz stehen sollen, als solche markiert werden müssen. Im WWW wird oft das Copyright Zeichen verwendet,

---

[38] Natürlich in einem Format, dass von Suchmaschinen durchsucht wird, also derzeit HTML, TXT, XML, PDF, MS Office Dokumente – aber zum Beispiel nicht ZIP Files.

[39] http://www.google.com

um eben dies anzuzeigen. Dies beruht darauf, dass früher in den USA die Angabe von Autor, Datum und Copyright Zeichen vorgeschrieben war. In anderen Teilen der Welt war dies nie vorgeschrieben, seit die USA die RBÜ (Siehe E Internationale Vereinbarungen) unterzeichnet haben, ist die Verwendung des © auch in den USA nicht mehr notwendig. Es sei aber angemerkt, dass man durch die Anzeige eines © oder einen gleichwertigen Hinweis Anwender noch mal darauf aufmerksam macht, dass die Inhalte dem urheberrechtlichen Schutz unterliegen und damit eventuell wenigstens in einigen Fällen eine Verletzung der Rechte verhindern kann.

2. Bildmaterial

Bildinhalte sind besonders einfach zu speichern und zu kopieren. In den gängigen Browsern genügt ein „rechter“ Mausklick und das Bild kann direkt auf dem eigenen PC gespeichert werden. In der neusten Version des Internet Explorers von Microsoft wurde sogar ein spezielles Tool integriert, das das speichern von Bildern noch weiter vereinfacht, siehe Abb 2.

Abb 2 Im Browser erscheint beim überfahren eines Bildes mit der Maus ein Kontextmenü.

Oft lässt dieser einfache Prozess vergessen, dass in der Regel auch alle Bildmaterialien geschützt sind, falls nicht anders deklariert. Die Kopie für den privaten Gebrauch ist in der Schweiz gemäss URG 19 erlaubt. Oft werden jedoch die Bilder kopiert, um sie auf der eigenen Web-Seite zu veröffentlichen. Es kann sich hier um kleine Icons, aber auch um Photographien handeln.

Abb 3 Bild mit sichtbarem Wasserzeichen[40]

Im Unterschied zu HTML-Texten lassen sich jedoch Bilder durch Digitale Wasserzeichen zumindest als geschützt markieren. Dies können sichtbare Wasserzeichen sein, wie sie oft bei den kostenlosen Probebildern von Bilddatenbanken zum Einsatz kommen, wie Abb 3 zeigt.

Weitaus mächtiger aber ist es, Bilddaten zusätzlich mit nicht sichtbaren digitalen Wasserzeichen zu versehen.

Dies kann zum Beispiel mit dem Tool von Digimarc[41] geschehen, das beispielsweise standardmässig in Photoshop[42] integriert ist. Wie in Abb 4 und Abb 5 ersichtlich, kann jedes Bild auf ein nicht sichtbares Wasserzeichen von Digimarc überprüft werden.

Will man seine eigenen Bilder mit Wasserzeichen versehen, so muss man sich zuerst bei Digimarc registrieren und erhält in der Folge eine ID. Diese kann dann genau so leicht auf ein Bild übertragen werden.

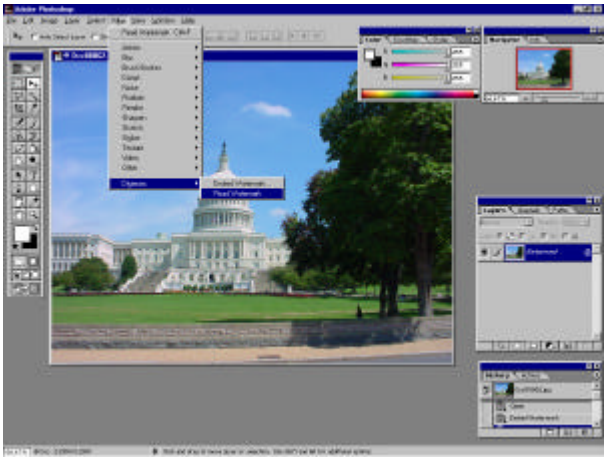

Abb 4 Auswahl des Digimarc Tools aus dem Menü...

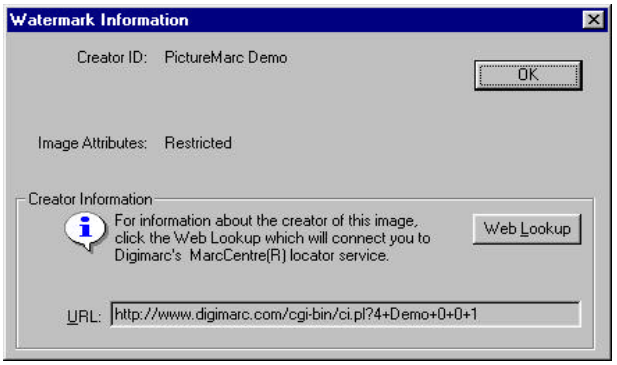

Abb 5 ... und das Tool zeig an, dass es sich um ein geschütztes Bild handelt. Ausserdem kann man durch Klick auf „Web Lookup" direkt Informationen zum Urheber bekommen.

[40] Quelle: Corbis, ww.corbis.com

[41] www.digimarc.com

[42] Photoshop ist ein weit verbreitetes Tool zur digitalen Bearbeitung von Bildern und wird von Adobe vertrieben, www.adobe.com.

Die Wasserzeichen bleiben auch erhalten, wenn die Bilder digital verändert werden, also zum Beispiel verkleinert oder vergrössert werden, mit anderen Bildern in einer Collage gruppiert etc. Firmen wie Digimarc bieten komplette Dienstleistungen, die nicht nur das versehen der Bilder mit Wasserzeichen erlauben, sondern auch das auffinden der markierten Bilder im Internet umfasst. Ein Beispielreport ist in Abb 6 gezeigt

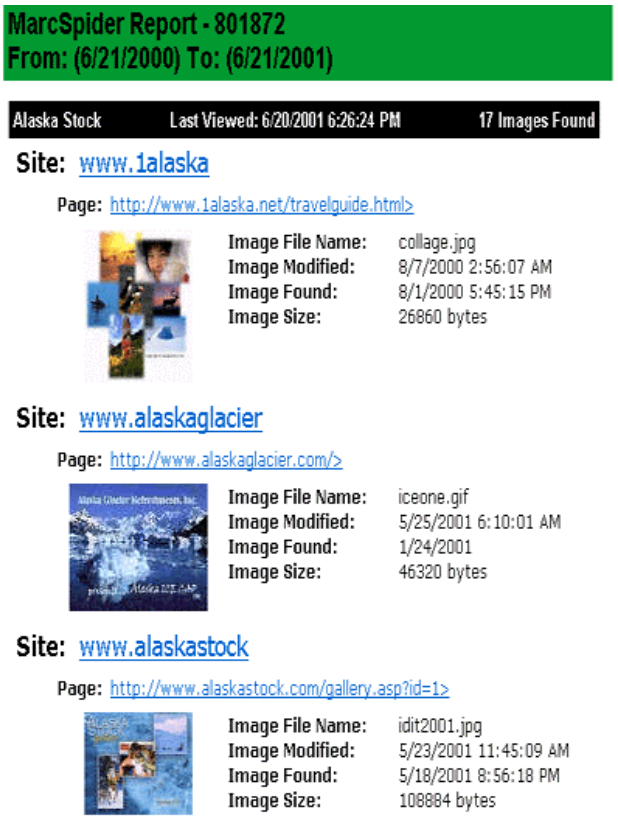

Abb 6 Beispielreport[43]

So wird zwar das Auffinden von Urheberrechtsverletzern extrem vereinfacht – die Frage nach den Möglichkeiten der Verfolgung und Ahndung der Vergehen bleibt jedoch bestehen.

3. Schutz des Layouts von Web-Sites

Neben einzelnen Texten oder Bildern, werden auch häufig komplette graphische Layouts von Web-Sites kopiert.

Um diesen Vorgang rechtlich zu beurteilen, muss zuerst definiert werden, was kopiert wird. Zum einen ist der dem Layout zugrundeliegende Code von HTML-Dokumenten frei zugänglich und kann so kopiert werden. Auf dieses Thema wird in C.II Schutz von HTML und Programmcode eingegangen. In diesem Abschnitt soll vielmehr das Übernehmen von reinen graphischen Konzepten untersucht werden. Die zugrundeliegende Technologie bzw. der Quelltext sollen dabei vorerst nicht beachtet werden.

Ein Beispiel ist in Abb 7 und Abb 8 zu sehen: Fast jeder würde das Design der in Abb 8 abgebildeten Web-Site als Kopie derjenigen in Abb 7 erkennen. (Die an dieser Stelle nicht

[43] Quelle http://www.digimarc.com/support/csspidersample.htm (besucht im Mai 2002)

abgebildeten, weiteren Seiten der beiden Sites machen dies noch deutlicher). Rechtlich gesehen ist nach dieser tatsächlichen Erkenntnis der Fall klar:

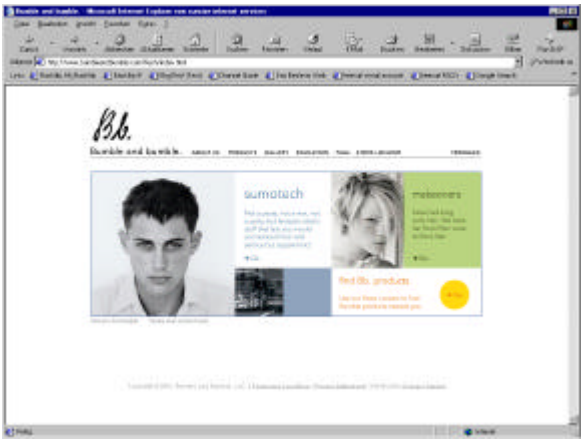

Abb 7 Original

(www.bumbleandbumble.com 20.5.2002)

Abb 8 Eine Kopie des Layouts der Web-Site aus Abb 7[44]

Nach Schweizer Urheberrecht ist das Design einer Web-Site als Werk aufzufassen und damit geschützt. Im wesentlichen kommen die Paragraphen

> URG Artikel 2 c: Werke der bildenden Kunst, insbesondere der Malerei, der Bildhauerei und der Graphik;
>
> URG Artikel 2 g: Fotografische, filmische und andere visuelle oder audiovisuelle Werke;

zur Anwendung.

Im Unterschied zu dem genannten Beispiel, ist wohl nicht immer eindeutig feststellbar, ob ein Layout wirklich kopiert wurde, d.h. es ist unter Umständen Auslegungssache wie ähnlich das Original und die vermeintliche Kopie sind. Beispielsweise ist der Gebrauch einer Navigationsleiste am linken Bildschirmrand und ein Inhaltsbereich, der den Rest des Bildschirms füllt, sehr verbreitet – hier ist die *Individualität,* wie sie nach dem zuvor genannten Art. 2 Abs. 1 URG vorausgesetzt wird, nicht mehr gegeben. Oder anders argumentiert, muss überprüft werden, ob es sich nicht um ein Konzept handelt, welches nicht geschützt wäre, sondern ob der konkrete Ausdruck der Idee übernommen wurde. (Im obigen Fall könnte die Anordnung einer horizontalen Navigationsleiste über einem Inhaltsbereich aus Text und Bildern als Konzept aufgefasst werden. Die Umsetzung mit den Farben und der Aufteilung des Inhaltes in Text und Bild ist aber ein konkreter Ausdruck des Konzepts.)

---

[44] *www.digitalresultsgroup.com/edu/ 20.5.2002, gefunden via pirated-sites.com.*

II. Schutz von HTML und Programmcode

Urheberrechtsfragen, die sich im Zusammenhang mit Software und Programmcode ergeben, wurden schon in Kapitel B Urheberrecht und Software diskutiert.
Dennoch soll hier noch einmal kurz auf das Thema eingegangen werden. Dazu werfen wir einen kurzen Blick auf den Stand der Technik im Zusammenhang mit dem WWW.
Im wesentlichen kann im WWW zwischen Serverseitigen Programmen und Clientseitigen Programmen unterschieden werden. Die Serverseitigen Programme (in Sprachen wie Java, Perl, PHP oder ASP verfasst) werden auf dem Server ausgeführt, der User bekommt nur das Resultat eines Programmaufrufes, meist in Form einer HTML Seite zu sehen. Da der User nicht ohne weiteres an den Quelltext der Serverseitigen Programme gelangen kann, ist hier die Gefahr von Urheberrechtsverletzungen geringer[45]. Am Rande sei bemerkt, dass in solchen Fällen der Schutz des produzierten HTML Codes eine untergeordnete Rolle spielt, da die wahre geistige Leistung und damit der Aufwand in den Serverseitigen Programmen liegen wird, die meist eine komplexe Datenbankabfrage o.ä. ausführen.
Anders verhält es sich bei Clientseitigen Programmen (zum Beispiel Javascript) und HTML-Dokumenten. Diese werden auf den Rechner des Users heruntergeladen und dort lokal ausgeführt bzw. dargestellt. Der gesamte Quellcode kann mit jedem Browser leicht eingesehen werden und dementsprechend auch kopiert werden.
Dem aufmerksamen Leser mag aufgefallen sein, dass HTML neben den Clientseitigen Programmen als weiterer Begriff aufgeführt wurde: HTML wird oft als Programmiersprache deklariert, in Wirklichkeit ist es aber eine sogenannte Auszeichnungssprache (engl.: Markup Language), in der vollen Länge *Hypertext Markup Language*. Bei einem HTML Dokument handelt es sich um ein spezielles Textdokument, ein Hypertext-Dokument. Ein Hypertext-Dokument enthält neben dem eigentlichen Inhalt auch Elemente, die seine Struktur definieren. Diese sogenannten Tags sind im Falle von HTML zum Beispiel <h1></h1> für eine Überschrift, für einen Absatz. Wesentliche Elemente, die eine *Programmiersprache* ausmachen und den Programmfluss definieren, zum Beispiel Schleifen (for, while: mehrfaches Ausführen einer Instruktion) oder Bedingungen (if... else: Ausführen einer Instruktion, nur falls gewisse Bedingungen zutreffen) sind jedoch nicht vorhanden.
Nach dieser Definition liegen HTML Dokumente eigentlich im Bereich von Text-Werken und unterliegen deshalb urheberrechtlichen Schutz, auch wenn ein Urheberrecht (noch) keine Regelungen für Software enthält.

---

[45] D.h. der Quelltext der auf dem Server abgelegten Programme, kann nicht eingesehen werden, ohne in das Serversystem einzudringen, bzw. es zu „hacken“.

Interessanterweise sind uns jedoch keine Fälle bekannt, in denen es zum Prozess um urheberrechtlichen Schutz von HTML Text (oder Javascript) kam, obwohl HTML so einfach kopiert werden kann und davon auch rege Gebrauch gemacht wird. Spezielle HTML-Konstruktionen wurden in der Geschichte des WWW millionenfach kopiert (zum Beispiel das positionieren von Elementen mit sog. blinden GIF's.[46] Die Möglichkeit den HTML Code anderer auf einfache Weise einzusehen und davon zu lernen ist einer der Gründe dafür, weshalb es überhaupt zu der rasanten Entwicklung des WWW[47] kam. Vermutlich dürfte hier der Grund dafür liegen, dass sich kaum jemand daran stört, dass im Bereich des HTML und Clientseitiger Programme das Kopieren an der Tagesordnung ist.

III. Links und Urheberrecht

Wie in der Einleitung zu diesem Abschnitt über das WWW erwähnt, zeichnet sich Hypertext durch die Verlinkung einzelner HTML Dokumente aus. Diese Verlinkung bringt aber auch urheberrechtliche Probleme mit sich, von denen die wichtigsten zwei *Deep-Linking* und *Framing* sind.

1. Deep Linking

Unter Deep-Linking versteht man das setzen eines Links von einer Seite in einer Domain auf eine Seite in einer anderen Domain, wobei der Link nicht auf die Hauptseite der Domain, sondern auf eine der Unterseiten zeigt. Dies ist an sich in den meisten Fällen nicht problematisch, im Gegenteil, die Idee ist ja, möglichst direkt zu der gewünschten Information zu linken.

---

[46] Bei dieser von David Siegel (http://www.dsiegel.com) Mitte der 90er erfundenen Technik, werden durchsichtige, sog. „blinde" Bilddateien im GIF Format verwendet, um als Platzhalter für Web-Seiten Layouts zu dienen.

[47] Shirky: How did the Web grow so quickly?

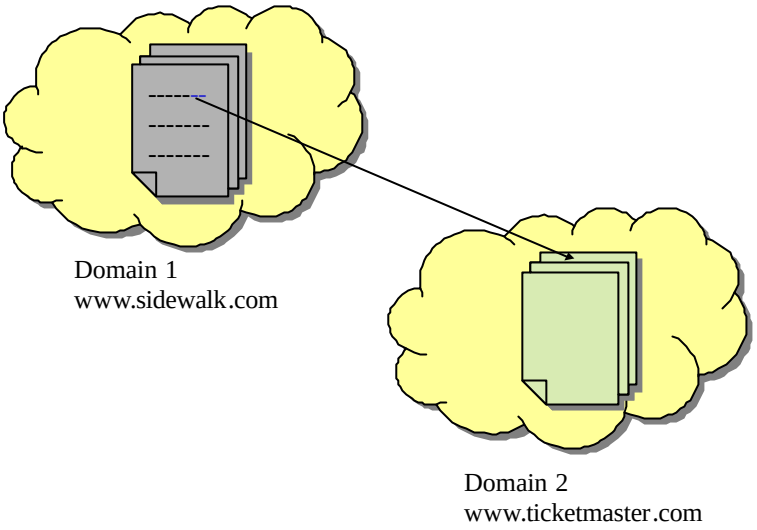

*Abb 9 Deep Linking: Verweis von einem Dokument in Domain1 auf eine **Unterseite** in Domain 2*

Anders verhält es sich jedoch, wenn so viele Links von einer Domain zu einer Informationssammlung auf einer anderen Domain erstellt werden, und so die Daten den Usern der ersten Domain mehr oder weniger direkt zur Verfügung stehen. Diese Informationssammlungen können zum Beispiel Zeitungsartikel oder Anzeigen sein. Zwei Fälle sollen an dieser Stelle als Beispiel dienen.

a) Ticketmaster vs. Microsoft[48]

Am 28. April 1997 reichte der Online Ticket-Händler *Ticketmaster* beim *U.S. District Court for the Central District of California* Klage gegen Microsoft ein. Microsoft hatte von seiner *Microsoft Sidewalk*[49] Seite, die Informationen zu verschiedenen amerikanischen Städten bietet, direkt zu den jeweiligen Event-Beschreibungen auf Unterseiten von www.ticketmaster.com gelinkt.

Ticketmaster argumentierte, dass Microsoft sich der Daten bediene, die Ticketmaster mit erheblichem Aufwand zusammenstelle:

By accessing Ticketmaster's live event information and services without Ticketmaster's approval, and by prominently offering it as a service to their users, Microsoft is feathering its own nest at Ticketmaster's expense. It is, in effect, committing electronic piracy. In this narrow corridor of cyberspace, Ticketmaster must maintain control of the manner in which others utilize and profit from its proprietary services, or face the prospect of a feeding frenzy diluting its content."[50]

---

[48] Ticketmaster Corp. v. Microsoft Inc., CV 97-3055 RAP, C.D. Cal., First Amended Complaint, Filed Apr. 28, 1997

[49] www.sidewalk.com

[50] *http://www.jmls.edu/cyber/cases/ticket1.html (besucht im Mai 2002).*

Indem die Hauptseite von Ticketmaster "umgangen" wurde, entgingen Ticketmaster ausserdem wichtige Werbeeinnahmen, die durch die Anzeige von Bannern auf der Startseite generiert werden.
Zusätzlich hatte ein Konkurrent zu Microsofts Sidewalk, CitySearch, kurz zuvor ein Abkommen mit Ticketmaster unterzeichnet, dass CitySearch *gegen Bezahlung* dasselbe zu tun, was Microsoft ohne einen Vertrag und damit auch ohne zu zahlen, tat.
Der Rechtsstreit wurde am 22. Januar 1999 durch einen Vergleich zwischen Microsoft und Ticketmaster gelöst. Microsoft's Sidewalk linkte in der Folge nicht mehr zu Ticketmaster [51].
Es wurde also kein Urteil gefällt, ob Deep-Linking legal sei oder nicht.

b) Ticketmaster vs. Tickets.com [52]

Tickets.com ist eine Firma, die wie Ticketmaster Tickets für Events verkauft. Im Unterschied zu Ticketmaster verkauft aber Tickets.com die Tickets nicht nur selber, sondern verweist für gewisse Veranstaltungen auch auf andere Anbieter – so auch auf Ticketmaster, die für einige Veranstaltungen das Exklusivrecht zum Verkauf von Karten besitzen. Gemäss den Behauptungen von Ticketmaster soll zudem Tickets.com gewisse Informationen von Ticketmaster kopiert haben - dies soll jedoch an dieser Stelle nicht weiter beachtet werden.
Ticketmaster reichte Klage gegen Tickets.com ein, wieder mit denselben Argumenten wie im Fall gegen Microsoft. Insbesondere habe Tickets.com die Gewinnung der Informationen von Ticketmaster auch automatisiert, indem Programme die Seiten von Ticketmaster automatisch absuchten.
In Bezug auf die Frage der Legalität von Deep-Links, entschied das Gericht in einem ersten Urteil vom 27.3. 2000 folgendermassen:
"Further, hyperlinking does not itself involve a violation of the Copyright Act (whatever it may do for other claims) since no copying is involved. The customer is automatically transferred to the particular genuine web page of the original author. There is no deception in what is happening. This is analogous to using a library's card index to get reference to particular items, albeit faster and more efficiently."[53]

Das Urteil bestätigt also die Legalität von Hyperlinking in jeder Form, auch Deep-Linking[54].
Im Sinne des WWW ist das aus unserer Sicht sicherlich der richtige Entscheid – ein Verbot von Deep-Linking würde die Idee des Hypertexts verbieten und damit das WWW Nutzlos machen. Es scheint, dass sich auch die rechtlichen Instanzen dieser Problematik bewusst

---

[51] Tedeschi, The New York Times On The Web.

[52] Ticketmaster Corp. v. Tickets.Com, Inc., 54 U.S.P.Q.2d 1344, C.D.Cal. 2000, March 27, 2000.

[53] http://www.gigalaw.com/library/ticketmaster-tickets-2000-03-27.html

[54] Tedeschi, The New York Times On The Web; Kaplan, The New York Times On The Web.

sind. Allerdings sind die Argumente von Ticketmaster, was das Zusammenstellen und Sammeln von Informationen angeht auch nicht haltlos. Es bleibt die Frage, ob es möglich wäre, Deep-Linking für *bestimmte Situationen* einzuschränken ohne Präzedenzfälle zu generieren, die zu unsinnigen Prozessen um Hyperlinks führen. Zumindest nach Schweizer Urheberrecht ist auch dies schwierig, denn ein Verbot würde voraussetzen, dass Kopien angefertigt würden und dies ist beim Linking nicht der Fall.
Am Rande sei angemerkt, dass es auch technische Methoden gibt, eingehenden Verkehr von bestimmten Seiten zu sperren. So hatte Ticketmaster in der Folge Verkehr von Tickets.com ausgeschlossen. Tickets.com fand aber neue Wege zu den Informationen zu linken.

2. Framing

Beim *Framing* kommt eine weitere spezielle Technik des WWW zur Anwendung. Mit HTML besteht die Möglichkeit, ein Dokument in verschiedene Bereiche aufzuteilen, in sog. Frames. In diesen Frames können dann einzelne HTML Dokumente geladen werden, siehe Abb 10.

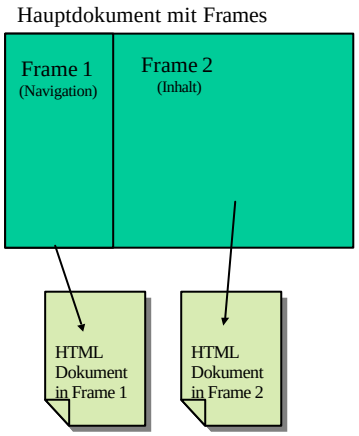

Abb 10 Anwendung von Frames

Vor einigen Jahren war diese Technik sehr gebräuchlich, um Navigationsleisten in einem Frame und den Inhalt in einem anderen anzuzeigen – mit dem Resultat, dass das Frame mit der Navigationsleiste beim Wechseln des Inhaltes nicht aktualisiert werden muss. Heute sind Frames jedoch wieder auf dem Rückzug.
Nichtsdestotrotz, besteht hier eine spezielle Gefahr für Urheberechtsverletzungen: So können beliebige Dokumente in Frames eingebunden werden, die irgendwo im Internet unter einer URL zu finden sind. Damit kann ein fremder Inhalt zu der eigenen Navigation geladen werden, ohne dass der User etwas merkt - es kann sogar ein weiteres Frame eingebunden werden, in dem Werbung angezeigt wird. Die durch die Werbung entstehenden Einnahmen werden dann mit fremden Inhalten generiert.

Auch zu diesem Thema soll ein Fallbeispiel hinzugezogen werden:

Die Betreiberin von www.derpoet.de unterhält unter der genannten Domain eine Sammlung von lyrischen Texten. Ein weiterer deutscher Anbieter stellte einige Inhalte von derpoet.de auf seiner eigenen Seite innerhalb eines Frames dar, in der oben beschriebenen Form des Framing:

„Dabei wurde die Website vollständig und unverändert abgebildet, oben links befand sich der Name der Verfügungsbeklagten mit dem Zusatz, dass es sich um einen externen Link handelt, für den Inhalt dieser Seite sei die Verfügungsbeklagte nicht verantwortlich. Daneben befand sich ein Werbefeld mit einer bei der Verfügungsbeklagten geschalteten Werbeanzeige.“[55]

Es wurde also nicht nur der Inhalt in ein Frame übernommen, sondern auch noch Werbung eingeblendet.

Das Landgericht Köln Entschied am 2. Mai 2001[56] zugunsten der Klägerin, die damit eine einstweilige Verfügung erreichte.

„Datenbank im Sinne dieser Vorschrift ist eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind und deren Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert. Diesen Anforderungen wird die von der Antragstellerin unter der Domain www.derpoet.de angebotene Textsammlung gerecht, denn die einzeln und unabhängig voneinander bestehenden Beiträge sind nach ihrem unbestrittenen Vortrag von ihr zusammengestellt und geordnet worden und sie sind mit elektronischen Mitteln einzeln zugänglich. Auch das Erfordernis der wesentlichen Investition ist vorliegend zu bejahen, denn nach dem von der Verfügungsbeklagten ebenfalls nicht bestrittenen Vortrag der Verfügungsklägerin forderte die Erstellung und die weitere Bereithaltung der Textsammlung eine Investition von erheblichem personellem und finanziellem Umfang.“

Interessant ist in diesem Fall die Hervorhebung einer Datenbank. Im Schweizer Urheberrecht sind Datenbanken nicht explizit geschützt. Es würde wohl aber genügen, die Seite als Werk im Sinne des URG zu definieren – in der Schweiz sind jedoch Datenbanken nur geschützt, wenn die Zusammenstellung bzw. Präsentation der Daten individuell ist. (Ob dies hier der Fall wäre, wäre wohl der zentrale Punkt der Argumentation bei einem Prozess. Wenn Sie diese zum Beispiel in spezielle Kategorien aufgeteilt hat (und nicht nur nach Autor geordnet), wäre dieses Argument sicher haltbar.) In der EU ist der Schutz von Datenbanken in der speziellen Richtlinie 96/9/EG festgehalten.

---

[55] *http://www.netlaw.de/urteile/lgk_19.htm (besucht im Mai 2002).*

[56] *Aktenzeichen 28 0 141/01.*

Beachtenswert ist ausserdem, dass das Urteil zugunsten der Klägerin ausfiel, auch wenn der Beklagte auf seiner Seite drauf hinwies, dass es sich um externe Daten handle.

Im Unterschied zum Deep-Linking besteht bei der Einschränkung des Framing kaum Gefahr, dass ein wesentlicher Teil der Funktionalität des WWW eingeschränkt würde. So besteht hier nicht nur aus technischer Sicht kein Grund zur Zurückhaltung, insbesondere wenn, wie im vorliegenden Fall, neben der Übernahme der Inhalte auch noch Werbung angezeigt wird, durch die möglicherweise finanzielle Einkünfte für den Urheberrechtsverletzer entstehen.

D. Rechtsschutz technischer Schutzmassnahmen

Die Kontrolle der Rechte eines Urhebers an seinem (digitalen) Werk wurde durch die rasante technologische Entwicklung der letzten zwei Jahrzehnte zusehends erschwert. So können z.B. Software- und Musik-CDs heutzutage beinahe von jedermann mit äusserst geringem Aufwand und Kosten , insbesondere ohne relevante Qualitätsverluste vervielfältigt werden.

Um die Rechte der Urheber zu wahren, wurden gleichziehend mit den neuen Vervielfältigungsmöglichkeiten auch entsprechende Massnahmen zum Schutze dieser Rechte gesucht und implementiert. Jedoch fehlt diesen technischen Einrichtungen bis dato der rechtliche Schutz[57]. Dieser rechtliche Schutzmantel wird bis Ende 2002 von den EU-Staaten aufgrund der Urheberrechtsrichtlinie[58] umgesetzt werden müssen. Es ist zudem absehbar, dass sich die Schweiz im Zuge der laufenden Urheberrechtsreform ebenfalls stark an besagter Richtlinie orientieren wird, die sich wiederum stark auf die WIPO-Verträge (WCT und WPPT) stützt, welche die Schweiz auch unterzeichnet hat und ratifizieren wird.

Im folgenden soll in einem ersten Teil ein Überblick von technischer Seite über die gebräuchlichen Schutzmechanismen – auch Kopierschutz genannt - gegeben werden. In einem weiteren Teil wird auf das Digital Rights Management (DRM) eingegangen, sowie ausgewählte rechtliche Gesichtspunkte beleuchtet.

I. Technische Schutzmassnahmen auf neuen Medien

Zwischen den Entwicklern der Schutzmechanismen und den einschlägigen Benutzerkreisen, die versuchen diese zu knacken, spielt sich ein eigentliches Katz-und-Maus Spiel ab. Dieses Spiel ist gerade auch bei der CD möglich, weil die technischen Standards dort auch gewisse Freiräume offen lassen.[59] Gründe hiefür sind: Vor 25 Jahren, als der Audio-CD Standard bei

---

[57] Abgesehen vom umstrittenen US-Amerikanischen Digital Millenium Copyright Act (DMCA).

[58] EU-Richtlinie 2001/29/EG.

[59] Der erste Standard beschrieb nur die Audio-CD. Er wurde in den Jahren 1980/81 von Philips und Sony gemeinsam entwickelt und ursprünglich in einem roten Hefter herausgegeben bzw. lizenziert. Daher auch der Übername „Red-Book“. Erst 1986 kam der „Yellow-Book“ Standard (ebenfalls von Philips und Sony) heraus, der wesentliche Aspekte der Daten-CD beschrieb. Es folgten zahlreiche weitere Standards, von denen die meisten auch einen farbigen Namen tragen, bei denen aber auch andere Firmen mitgewirkt haben. Der „Red-Book“ Standard ist ein *de facto* Standard und kein

Philips und Sony entwickelt wurde, konnte die „digitale Revolution“ nicht in vollem Umfang vorausgesehen werden. Das heisst man hat für ein Problem eine aus damaliger Sicht unproblematische Lösung gewählt und aber deren Eignung für einen Schutzmechanismus nicht erkannt. An den historischen Grund anschliessend darf auch vermutet werden, dass den damaligen Ingenieuren schlicht das Bewusstsein über die Tragweite ihrer Entwicklung fehlte, und sie sich einer urheberrechtlichen Problematik nicht bewusst waren.[60]

Es gibt aber auch technische Gründe: In den Standards wurden Fehlerkorrektursysteme implementiert, um z.B. Kratzer, Fingerabdrücke und Fertigungstoleranzen zuzulassen, was für das funktionieren aller Systeme unerlässlich ist. Wie diese Freiräume und Fehlerkorrektursysteme zu Schutzzwecken verwendet werden, wird in den folgenden Abschnitten klar.

1. Der Schutz von Musik-CDs

Hier stellt sich die Frage, wie man einer an sich toten Musik-CD „beibringt“, dass sie sich nur auf einem Musik CD-Player und nicht in einem Computer CD-ROM Laufwerk abspielen lässt (Denn dann kann man Sie digital auf den Computer auslesen, kopieren und per MP3 über Internet verbreiten). Die landläufige Meinung Player ist gleich Laufwerk trifft technisch nicht zu. Mann muss sich das dahingehend vorstellen, dass das menschliche Ohr der Musik, und damit der Wiedergabe von CDs durch CD-Player, gewisse Fehler erlaubt (psychoakustische Effekte). Hingegen ist ein Computer bei Software auf (fast) jedes einzelne Bit angewiesen ist.[61] Diese Gegebenheit wird in der Hardware berücksichtigt.

In der Folge wird eine Auswahl der gängigsten Schutzmechanismen beschrieben.

a) SafeAudio (Macrovision)[62,63]

Bei SafeAudio werden in unregelmässigen Abständen fehlerhafte Sektoren in den Musikdatenstrom eingefügt. Ein Sektor besteht aus 2352 Bytes Nutzdaten und 784 Kontrollbytes, die kontrollieren, ob die Nutzdaten keine Fehler aufweisen (genannt Error Correction Code, ECC). Dies stellt eine Redundanz dar und im Normalfall stimmen Daten

---

offener Standard. Er untersteht den Lizenzbedingen von Philips und Sony. Die Rechte sind jedoch am ablaufen.

[60] Das ist nicht als Vorwurf zu werten, und solches wird sich auch wiederholen!

[61] Dies ist bei weitem nicht der einzige Unterschied, genügt hier aber als Erklärungsansatz für die eingesetzten Fehlerkorrekturverfahren.

[62] http://www.macrovision.com (besucht am 10.6.2002)

[63] McFadden, Andy: CD-Recordable FAQ

und Kontrolldaten gemäss der ECC-Vorschrift überein. Was passiert aber, wenn die ECC-Daten eines Sektors auf der Original-CD bewusst falsch gesetzt werden und unpassende Musikdaten (Burts) geschrieben werden? CD-Player werden aufgrund des nicht übereinstimmenden ECC einen Fehler erkennen und versuchen die Musikdaten zu reparieren, das heisst, mit dem vorhergehenden und nachfolgenden Sektor zu interpolieren. CD-ROM Laufwerke hingegen tun dies nicht und melden einen Lesefehler, der die meisten (aber nicht alle) CD-Kopierprogramme zum stoppen bringt. Werden die ECC Information von den Programmen einfach ignoriert und die Daten trotzdem geschrieben, entstehen auf den Kopien oder im MP3-File hässliche Störgeräusche (Knacken, Bursts). Beim hören der CD auf einem Player werden wir nichts bemerken (da interpoliert).

b) Cactus Data Shield (Midbar Tech)[64,63]

Von diesem Kopierschutz existieren mittlerweile 3 Versionen: CDS100, CDS200 und CDS300. Der erste (und schwächste) Schutz besteht darin, dass ein bezüglich Datenformat ungültiges und damit nicht dem Standard entsprechendes Inhaltsverzeichnis auf die CD geschrieben wird (Illegal TOC)[65]. Weiter werden auch die Angaben über die Musikstücklänge gezielt falsch gesetzt. Dieses Vorgehen verwirrt eine grosse Anzahl von CD-ROM Laufwerken, wird aber von fast allen CD-Playern übergangen. Ein Symptom dieser Technik ist, dass nur die ersten 30 Sekunden der CD vom Computer abgespielt werden. Die neueren beiden Versionen setzten eine Kombination mehrerer Techniken ein, wie sie hier beschrieben werden.

c) Duolizer (Bay View Systems)[66]

Dieses System funktioniert nicht für Audio-CDs, die auf Playern abgespielt werden sollen und setzt eine Internetverbindung voraus. Die Musikdaten werden aufgetrennt, d.h. der grosse Anteil wird auf der CD geliefert und ein kleiner aber wichtiger Teil muss zeitgleich mit dem Abspielen übers Internet geladen werden. Der Sinn diese Verfahrens ist, dass die CDs vor dem offiziellen Release den Distributoren und Läden ausgeliefert werden können, ohne Gefahr zu laufen, dass die Musikstücke vor der Veröffentlichung per MP3 über Internet verteilt werden. Es geht vor allem darum, die ersten und meist lukrativsten Wochen nach dem offiziellen Release zu schützen.

---

[64] http://www.midbartech.com (besucht am 10.6.2002)

[65] Illegal Table of Content, ungültiges Inhaltsverzeichnis. CD-ROM Laufwerke lesen immer zuerst den Datentrack, erst danach den Audio-Track. Wird für den Daten-Track ein ungültiges Inhaltsverzeichnis erstellt, brechen die Laufwerke den Lesevorgang ab. CD-Player hingegen übergehen den Daten-Track.

[66] http://www.bayviewsystems.com/solutions/solutions.htm (besucht am 10.6.2002)

d) Physische Fehler

Durch absichtliches Beschädigen der CD-Oberfläche können die Daten nicht mehr sauber auf dem Computer ausgelesen werden, jedoch wird die Musik auf einem Player trotzdem wiedergegeben und die fehlenden Stellen interpoliert.[67] (siehe a)

e) SCMS

Das *Serial Copy Management System* ist von untergeordneter Bedeutung weil es nur in Komponenten der Consumer Electronic (CD-Player in Stereoanlagen etc.) und nicht auf dem Computer umgesetzt wurde. Man kann es gewissermassen als Vorläufer des *Digital Rights Management (siehe Abs. 3)* betrachten, da es etwas flexibler ist als eine absolute Kopiersperre und eine Kopie (zum Privatgebrauch) zulässt. SCMS ist auf allen Audio-CDs gemäss Red-Book Standard vorhanden.[59,68] Das Konzept wurde auch auf MiniDisc, DAT (Digital Audio Tape) und vermutlich auch auf weiteren Medien wie DCC[69] implementiert. Die Idee ist im digitalen Datenstrom ein Bit vorzusehen, das codiert, ob die Musik a) Urheberrechtlich geschützt ist b) ob es sich um ein nicht zu schützendes Werk handelt oder c) ob es sich um eine Erstkopie eines Werkexemplars im Rahmen der gesetzlich erlaubten Privatkopie handelt. Das Bit wird bei der Herstellung gemäss Angaben des Produzenten oder Urhebers gesetzt. Beim privaten Kopieren eines geschützten Werkes über eine digitale Schnittstelle (z.B. optisches Kabel wie TOSLink bei MiniDisc) wird das Bit gelöscht und somit als Erstkopie eines Werkexemplars gekennzeichnet. Die Geräte verhindern dann eine Zweitkopie; selbstverständlich können vom Original mehrere Kopien angefertigt werden.

2. Der Schutz von Software- oder Daten-CDs[70]

Diese CDs erlauben keinen Schutzmechanismus in der Art wie Audio-CDs. Hier muss der berechtigte Nutzer die Daten vollständig richtig lesen können. Dies verlangt nach anderen Schutzkonzepten, die in den Kopierschutzprodukten meistens kombiniert angewandt werden.

---

[67] Man kann das auch selber mit einer CD ausprobieren: Man durchbohre eine CD mit Löchern bis zu ca. 5mm Durchmesser und versuche sie abzuspielen. Sie sollte dies zumindest auf guten Playern ohne weiteres tun.

[68] Das relativiert das Urteil in Fussnote 60 selbstverständlich ein wenig.

[69] Digital Compact Cassette, eine von Philips entwickelte digital Musikkassette, ähnlich zu DAT. Das Produkt hat sich auf dem Markt, im Gegensatz zur MiniDisc nicht halten können.

[70] Dieser Abschnitt mag von der Ausführlichkeit nicht befriedigen. Die Recherche hat gezeigt, dass zu den technischen Hintergründen dieser Massnahmen wenig bekannt ist. Abschnitt SafeDisc ist als Spezialität und LaserLock als generelle Ansatzweise zu betrachten. Es gibt jedoch zahlreiche weitere Produkte. Siehe Zota, Volker: Klonverbot

a) SafeDisc 2 (Macrovision)[62,71]

SafeDisc 2 ist ein sehr cleverer Schutz und hat die Eigenschaft, dass die Daten wohl von der CD gelesen werden können, aber nicht auf allen CD-Brennern geschrieben werden. Bei diesen Daten handelt es sich um sogenannte „Schwache Sektoren". Mann muss dazu folgendes wissen: Die Vertiefungen (Pits), wie sie physisch auf der CD-Scheibe vorhanden sind um Informationen zu speichern entsprechen nicht 1:1 den Datenbits (also logischen Nullen und Einsen). Es besteht eine Vorschrift[72], wie die Pits mit den Bits zusammenhängen.[73] Eine grosse Anzahl von CD-Brennern kann aber durch eine Folge von regelmässigen Bitmustern verwirrt werden, weil im EFM-Decoder ein Überlauf in einem Zählerregister (Overflow) entsteht. Daraus resultiert ein Lesefehler und es entsteht eine fehlerhafte Kopie. SafeDisc 2 schreibt nun bei der CD-Herstellung im Presswerk genau solche Pitmuster auf die CD, welche nach der Demodulation (Rückwärtsanwendung der Vorschrift) gerade diese regelmässigen Bitmuster ergeben.

b) LaserLock (MLS International)[74]

LaserLock setzt drei Elemente ein: Ein spezielles CD-Herstellungsverfahren, ein Verschlüsselungsverfahren und Hindernisse, um das „reverse engineering" zu verhindern. Das Herstellungsverfahren erlaubt es, eine Signatur auf die CD-Oberfläche zu schreiben, die nicht per CD-Brenner kopiert, aber gelesen werden kann. Die auf der CD befindlichen wichtigen Softwareteile werden verschlüsselt. Beim Installieren der Software wird die Signatur auf der CD abgefragt und somit geprüft, ob das Original tatsächlich vorhanden ist. Damit diese Prüfung, die durch die Installationsroutine vorgenommen wird, nicht mit einfachen Tricks ausgeschaltet werden kann, werden Täuschungsmanöver eingesetzt, um das „reverse engineering" zu erschweren.

Aufgrund der speziellen Signatur ist es zwar nicht mehr möglich eine 100%ig funktionierende Kopie herzustellen. Jedoch kann man einen sogenannten Patch (einen Betriebssystemtreiber) installieren, welcher der Installationsroutine das Vorhandensein der Signatur vorgaukelt. Im Gegenzug, als die Kopierschutzhersteller dies erkannten, wird in neueren Versionen zuerst nach diesen Treibern gesucht. Sind sie vorhanden, wird die Installation abgebrochen.[75]

---

[71] Zota, Volker, Klonverbot

[72] Diese Vorschrift ist die *Eight to Fourteen Modulation (EFM)*. Ein entsprechender Microchip (der EFM-De/Encoder) der diese (De)Modulation vornimmt, ist in jedem CD-Laufwerk enthalten.

[73] Kuhn, Kelin J.: Audio Compact Disc – Writing and Reading

[74] http://www.laserlock.com/products.htm, (besucht am 11.6.2002)

[75] Zota, Volker, Klonverbot

c) Nicht standardkonforme Pit-Geometrien[76]

Wie bereits erwähnt, sind werden die Vertiefungen auf der CD-Scheibe *Pit* genannt. Pits können unterschiedlich lang sein, müssen aber gemäss Standard ein ganzes Vielfaches einer Pit-Einheitslänge aufweisen. Wird nun an bewusst gewählten Stellen auf der CD eine Reihe von Pits geschrieben, deren Länge beispielsweise genau 1.5 Einheitslängen entspricht, wird zufällig einmal eine Einheitslänge und ein andermal zwei Einheitslängen gelesen. Diese Zwischenlangen Pits können nur im CD-Herstellungsprozess gepresst und nicht mit CD-Brennern erzeugt werden. Auf der CD muss sich Software befinden, welche die bewusst gewählten Stellen mehrmals abfragt. Erscheinen nichtdeterministische Leseresultate, muss die Original-CD vorliegen.

3. Medienunabhängiger Schutz

a) Dongle („Kopierschutzstecker“)[77]

Dongles sind Schutzeinrichtungen auf Hardwarebasis zur Verhinderung der unerlaubten Softwarenutzung. Typischerweise besteht ein Dongle aus einem Stecker ohne Kabel, der wie ein Drucker über die parallele, serielle oder USB Schnittstelle an den Computer angeschlossen werden kann. Im Dongle sitzt ein Mikrochip auf den eine Codenummer programmiert ist. Diese Codenummer wird durch die zu schützende Software periodisch abfragt. Ist der Dongle nicht vorhanden und kann die Codenummer nicht ausgelesen werden, wird das Programm erst gar nicht aufstarten, beziehungsweise die Ausführung abbrechen. Diese Einrichtungen sind einiges älter als die oben beschriebenen CD-Schutzmechanismen und werden vorwiegend bei sehr teuren Softwarepaketen wie CAD/CAE eingesetzt. Sie verhindern in Unternehmen auch, dass die Software von mehreren Mitarbeitern gleichzeitig genutzt werden kann, lassen aber den Lizenznehmern die Möglichkeit, die Software auf mehreren Maschinen zu installieren. Nachteile dieser Dongles sind deren hohen Herstellungskosten, sowie häufige Hardwarekonflikte bei den Kunden.

b) Bongle

Ein Bongle ist eine CD, die jedes Mal bei der Softwarenutzung eingelegt werden muss und deren Code – entsprechend der Funktionsweise von Dongles - zur Validierung abgefragt wird. Ein Bongle löst die beiden erwähnten Probleme eines Dongles, muss jedoch selber mit einem Kopierschutz versehen werden.

---

[76] McFadden, Andy: CD-Recordable FAQ

[77] Seinen Namen hat der Dongle vom Software-Entwickler *Don Gall*, der, nachdem er durch Raupkopierer kein Geld mehr mit seiner Software verdienen konnte, den Dongle als Schutzmechanismus erfunden haben soll.

c) Seriennummern

Die Abfrage einer Seriennummer bei der Installation einer Software ist wohl der weitest verbreitete Mechanismus. Er kann aber sehr leicht umgangen werden. Die Seriennummern können, genauso wie sie auf der Softwareverpackung aufgedruckt sind, auch übers Internet verbreitet werden oder auf Papier aufgeschrieben werden. So bestehen in den einschlägigen Benutzerkreisen ganze Datenbanken mit diesen Informationen.[78] Eine Variation der simplen Serienummer besteht darin, dass sie durch den Softwarehersteller z.B. aus Angaben des Lizenznehmers - wie Name, Adresse, Prozessornummer (CPU-ID) oder MAC-Adresse[79] - nach einem geheimen Algorithmus generiert wird und somit persönlich ist.[80] Aber auch hierzu sind für einige Programme sogenannte *KeyGens* im Umlauf, denen der geheime Algorithmus bekannt ist.

Oft werden im Gegenzug von den Herstellern die im Internet kursierenden Seriennummern in späteren Softwareupdates explizit gesperrt. Dadurch wird der weitere Missbrauch der Seriennummern verhindert und nebenbei noch derjenige bestraft, der seine Seriennummer in Umlauf gebracht hat.[81]

d) Anmerkungen zu Schutzmechanismen

Es ist beachtlich, wie technisch ausgereift und durchdacht gewisse Massnahmen heute sind. Jedoch sind die Standards bekannt und bisher konnten alle Schutzmassnahmen geknackt werden, was oft eine Frage der Zeit ist.[82]

Um auf das Katz-und-Maus Spiel zurückzukommen: Das Wettrüsten wird dort ein Ende haben wo die „Grenzkosten“ erreicht sind. Entweder ist der Aufwand für die Hacker zu gross, einen Schutz zu umgehen. Oder die Zahl der Raubkopierer wird durch die neue Massnahme nur unverhältnismässig verringert. Die Leidtragenden, so ein Kopierschutz z.B.

---

[78] Die Datenbanken tragen Namen wie *Serials 2000* oder *Oscar*.

[79] MAC: Medium Access Code, Nummer, die jede einzelne Netzwerkkarte eindeutig identifiziert.

[80] Die Angaben werden an den Softwarehersteller gesandt, der dann die Seriennummer generiert.

[81] Wobei anzumerken ist, dass nicht alle kursierenden Seriennummern zwingend einmal verkauft worden sind. Es sind Methoden denkbar, um diese zu erraten.

[82] Warum müssen die Standards eingehalten werden? - Einerseits sind die Standards patentiert und das Audio-CD Logo darf nur verwendet werden, wenn diese Standards eingehalten werden. Andererseits ist die CD wertlos, wenn sie in den Abspielgeräten nicht läuft, da diese den Standard voraussetzen.

Qualitätseinbussen oder Inkompatibilitäten mit sich bringt, sind die nicht versierten Benutzer der grossen Masse.

Schutzmechanismen, welche die Musikqualität von Audio-CDs gezielt beeinträchtigen, sind nicht ganz so unproblematisch wie es scheint (Man könnte ja sagen: „Es tönt ja immer noch“).

- *Das* Qualitätsmerkmal der Musik-CD, nämlich die hochauflösende und rauscharme Musik, das unter anderem zum Markterfolg der CD schlechthin geführt hat, wird einfach umgestossen! Solche technologische Rückschritte sind nicht erstrebenswert.
- Weil die Fehlerkorrektur in den CD-Playern mehr ausgelastet wird und nicht mehr so viele Fehler korrigieren kann, die eigentlich von Kratzern oder Fingerabdrücken – also Gebrauchsspuren – stammen, sind die CDs anfälliger und haben eine insgesamt kürzere Lebensdauer, als herkömmliche CDs. Dies kann nicht im Interesse des Kunden liegen.

Bei vielen Kopiergeschützten Audio-CDs beobachtet man auch folgendes Phänomen:
Auf älteren CD-Playern oder speziellen Geräten wie z.B. Autoradios, Discmans oder multifunktionalen DVD Playern werden die neuen geschützten CDs nur teilweise abgespielt. Somit dürfte ein wesentlicher Mangel am Produkt vorliegen, da es seinen Hauptzweck nicht erfüllt.

Unabhängig von Audio oder Daten-CD kann auch folgendes angemerkt werden:
Das gezielte Einfügen von Fehlern kann durchaus auch so ausgelegt werden, dass die betreffende Scheibe nicht mehr dem CD-Standard entspricht und somit die Berechtigung verliert, als Compact Disc bezeichnet zu werden. Auch die Patentinhaber der CD-Standards haben sich dahingehend geäussert, dass sie mit solchen Entwicklungen nicht einverstanden seien. Da die Patente aber am auslaufen sind und lange Verhandlungen zu erwarten sind, werden sie nicht dagegen vorgehen.

Mit entsprechendem Wissen und geeigneten (und durchwegs erschwinglichen) Mitteln können (fast) alle Kopierschutzmassnahmen einfach mitkopiert werden. Bei diesen Mitteln handelt es sich um professionelle CD-Kopiersoftware und vor allem um CD-Brenner und Laufwerke, die im sogenannten RAW-Format[83] lesen und schreiben können. Dass das Mitkopieren des Schutzes als dessen Umgehung gewertet wird, ist ungerechtfertigt, da der

[83] Das lesen und schreiben im RAW-Format (Roh-Format) bedeutet, dass quasi Bit für Bit was auf der Scheibe eingebrannt ist gelesen (geschrieben) wird. Dabei wird keine Rücksicht auf Fehlformatierungen wie z.B. ein Nichtübereinstimmen von Daten und ECC-Information genommen.

Schutzmechanismus an sich ja nicht tangiert wird und eine Privatkopie auch in Zukunft erlaubt ist.[84]

An dieser Stelle sei auch angemerkt, dass das Erstellen von einzelnen Kopien zuhause nur die eine Hälfte des Übels ist. Einige Schutzmassnahmen wie Wasserzeichen und Hologramme zielen auch darauf ab, das Duplizieren (Remastering) von CDs in professionellen CD-Presswerken zu verhindern. Dies ist nicht mehr das Machwerk einzelner sondern ist dem organisierten Verbrechen (vorwiegend aus dem asiatischen Raum) zuzuschreiben. Beispielsweise wurden in Kloten und Lugano Ende 2000 Lieferungen von Fälschungen höchster Güte von Microsoft Betriebssystemen beschlagnahmt.[85]

II. Digital Rights Management (DRM)

Unter *Digital Rights Management* sind Geschäftsmodelle und technische Systeme zu verstehen, die in Zukunft die Rechte der Urheber beim Endkunden aufs genauste zu kontrollieren vermögen. Dies stellt im Grunde genommen ebenfalls einen Schutzmechanismus dar, geht aber sehr viel weiter, da differenzierter, und soll deshalb separat behandelt werden. Eine technische Umsetzung dürfte etwa so aussehen: Das zu schützende Dokument (z.B. PDF-File, eine Software, eine Musik-CD oder streaming Audio/Video[86]) wird mit Copyright Informationen versehen. Das sind sogenannte Metadaten, die die Nutzungsmöglichkeiten der Endkunden beschreiben. Sie enthalten die Information darüber, wer auf welche Art (z.B mit welchem Gerät) zu welchem Zeitpunkt wie lange zu welchen Bedingungen (z.B. „read only“, Kopiererlaubnis, Druckerlaubnis) und an welchem Ort Zugang zum Werk hat.

Ein gutes System muss auch berücksichtigen, dass Urheberrechte ablaufen. Unter der herrschenden Machtstellung und der protektionistischen Handlungsweise der Unterhaltungsindustrie könnte dies aber ein Punkt sein, der verloren geht.[87] Die grosse Herausforderung von technischen Schutzmassnahmen und DRM Systemen liegt darin, die gesetzgeberischen

---

[84] Krempl, Stefan: Geschützte Kopiersperren

[85] Amman, Daniel: Mafia gegen Microsoft

[86] Streaming ist eine Internettechnologie, die es erlaubt über eine Internetverbinung Radio oder Videoprogramme zu „empfangen“.

[87] Diese Diskussion ist vielleicht obsolet. Es ist nicht gesichert, dass eine Nutzung zum Zeitpunkt wo die Rechte auslaufen noch möglich sein wird. Gemeint ist, dass wir z.B. noch Schallplatten besitzen, aber es keine Plattenspieler mehr gibt, weil sie veraltet sind oder, dass die Vinylplatten altershalber nicht mehr abspielbar sind. Über die langfristige Haltbarkeit von CDs sind noch keine gesicherten Erkenntnisse vorhanden!

Feinheiten korrekt abzubilden. Dass dies nicht einfach ist, wird nur schon klar, wenn DRM Systeme, die global verbreitet werden, unterschiedliche nationale Gesetzgebungen berücksichtigen sollen.

1. Technische Umsetzung

Um z. B. Musikstücke auf einer CD mit DRM zu schützen, müssen neue Standards geschaffen werden, die Speicherplatz für die beschriebenen Metadaten freilassen. Ausserdem werden die Daten (Musikstücke) verschlüsselt werden, damit man ohne Metadaten nicht an die Musik herankommt. Das bedingt, dass der Konsument einen neuen CD-Player kauft, der eben auch geschützte CDs abspielen kann.[88] Bei eBooks oder Audio-Streams muss nur eine Software (z.B. Realplayer) heruntergeladen werden, die oft auch gratis angeboten wird. Spannend ist, wie solche neue Systeme dem Konsumenten verkauft werden, schliesslich hat der Kunde kein Interesse daran, dass seine Rechte eingeschränkt werden. Bei der Audio-CD z.B. müsste eine qualitative Verbesserung mit einhergehen, die aber schwer zu erzielen sein dürfte,[89] da die CD bereits sehr hochstehende Musikqualität bietet.

Was sicher entstehen wird, ist eine Differenzierung der Angebote. Das heisst, der Kunde kann für eine bestimmte CD wählen, welche Nutzung er kaufen möchte. Danach richtet sich dann auch der Preis. Ein Beispiel: CD, die ein einziges mal gehört werden kann: CHF 1.-. CD, die 10 mal gehört werden kann: CHF 10.-. CD, die immer gehört werden kann: CHF 150.-. Der Schritt, dass man seine Rechte nachträglich erweitern kann, indem man einen neuen Freischaltcode für weitere 10 mal CD-hören übers Internet kauft, dürfte nicht weit sein.

2. Marktstrukturen die mit DRM einhergehen

Es zeichnet sich ab, dass es mit DRM einen Kampf um das Vermarkten von Rechten auf verschiedenen Ebenen geben wird.[90] Auf der obersten und am stärksten wahrgenommenen Ebene wird von den Inhaltsanbietern um den Konsumenten geworben, damit sie ihre Produkte verkaufen können. Die Inhaltsanbieter sind jedoch auf die Servicedienstleistung der DRM-Anbieter angewiesen, denn ohne sie können die Produkte nicht „gefahrlos“ vermarktet werden. Hier öfffnet sich also eine zweite Ebene, in der DRM-Anbieter möglichst viele Inhaltsanbieter an Ihre Platform zu binden versuchen. Denn eine grosse

---

[88] Zur Verdeutlichung: Die Metadaten beschreiben die Nutzungsrechte nur; erst die Media-Player entscheiden aufgrund der Metadaten, ob die gewünschte Nutzung erlaubt ist.

[89] Eine Erweiterung wird in neuen Services zu finden sein. Z.B.: Liedtexte, CD-Text.

[90] Cherry, Steven M.: Making Music Pay.

Platform bringt durch ihre Angebotsvielfalt dem Kunden den besten Nutzen und dem Inhaltsanbieter gleichzeitig eine weit verbreitete Infrastruktur beim Endkunden. Somit ist der Krieg um die sogenannten „Media-Player“ (egal ob dies eine Set-Top Box für den Fernseher, eine Software wie *Realplayer* oder ein CD-Player sei), analog zum Browserkrieg, lanciert. Auf einer weiteren Ebene stehen sich die verschiedenen DRM-Standards gegenüber, die im Moment im Entstehen begriffen sind. Aus Konsumentensicht wäre ein einziger, funktionierender Standard wünschenswert. Jedoch instrumentalisieren gerade die DRM-Anbieter proprietäre Standards, um eine grosse Kundschaft (Konsumenten wie Anbieter) an sich zu binden, was zur Folge hat, dass unterschiedliche Standards entstehen.

3. Auswirkungen von DRM

Mit der Verfügbarkeit von DRM Systemen, die mit Verkaufskanälen gekoppelt sind, werden zusehends einzelne Künstler ihre Werke direkt vermarkten können. Das bedingt, und es soll auch gefordert sein, dass die Systeme allen zu fairen Preisen zugänglich sind. Das stellt für die Vielfalt der Angebote eine grosse Chance dar und wird der Gesellschaft zugute kommen. Leider wird dies von den Produzenten (nicht Urheber) als Gefahr gesehen werden, denn sie werden überflüssig. Es ist also absehbar, dass die Produzenten eigene technische Schutzsysteme entwickeln werden, auf denen kleine Anbieter nicht oder unter erhöhten Kosten zugelassen werden. In der Folge wird die Angebotsvielfalt der Werke gehemmt werden.

Schon die eigene Auseinandersetzung mit der Urheberrechtsproblematik lässt den folgenden Schluss zu: Die Bevölkerung wird für den Wert eines Werkes (re-)sensibilisiert werden, je mehr sie auf technische Schutzmassnahmen oder DRM Systeme trifft. Denn diese Wertschätzung ist vielleicht mit „gratis-Internet“ und CD-Brenner ein wenig geschwunden. Sollten z.B. mit DRM Werke mit verschiedenen Nutzungsrechten zu entsprechenden Preisen angeboten werden, wird es ebenfalls eine gewisse Zeit dauern, bis das in der Gesellschaft aufgenommen wird. Dann aber wird es (hoffentlich) schwieriger werden, qualitativ schlechte Produkte (z.B. CD mit einem Hit, der Rest ist Müll) mit gewinnbringenden sprich weitgehenden Nutzungsrechten zu vermarkten (Eine Hitsingle ist eben nur einen Monat aktuell).

III. Rechtliche Behandlung der Schutzmassnahmen

Wie gezeigt gibt es eine ganze Fülle von technischen Schutzmassnahmen, die stark von den verschiedenen Medien und deren Verwendungszweck abhängen. Die Rechtsetzung kann aber nicht auf die verschiedenen Mechanismen Rücksicht nehmen, da das Recht

technologieunabhängig sein soll. Ansonsten ist es veraltet bevor es in Kraft tritt oder kann mit neuen Methoden leicht umgangen werden. Die Schutzmechanismen werden folglich alle pauschal behandelt und definieren sich über ihre Wirksamkeit.

1. Rechtlicher Schutz der technischen Massnahmen

Dass technischen Schutzassnahmen ein rechtlicher Schutz gewährt werden wird, ist ein neues Element in den Urheberechtsgesetzen in der Schweiz und in Europa. Diese Forderung stammt aus der amerikanischen Unterhaltungsindustrie und wurde bereits 1998 im *Digital Millenium Copyright Act (DMCA)* in den Vereinigten Staaten umgesetzt. Die Europäische Union setzt dies in besagter Urheberrechtsrichtlinie[91] um. Art. 6 Abs. 1 lautet: *„Die Mitgliedstaaten sehen einen angemessenen Rechtsschutz gegen die Umgehung wirksamer technischer Massnahmen durch eine Person vor, der bekannt ist [...], dass sie dieses Ziel verfolgt.“* Auch in der Schweiz wird ein solcher Rechtsschutz umgesetzt werden, damit die WIPO-Verträge ratifiziert werden können.[92]

2. Problematische Punkte

Die Technische Schutzmassnahmen stellen Selbsthilfen der Rechtsinhaber zur Wahrung Ihrer Rechte dar. Dies ist grundsätzlich legitim, lässt aber schnell darüber hinwegsehen, dass somit die Kontrolle der Rechte vom Gesetzgeber in die Hand der Rechtsinhaber gleitet.

Das ist nur solange unproblematisch, wie der Inhaber mit den Schutzmassnahmen nur Werke schützt, die die Schutzvoraussetzungen (des Gesetzgebers) erfüllen. Denn wenn diese Vorsicht vom Inhaber nicht geboten wird und man einen Schutzmechanismus umgehen muss, um an das Werk (oder Teile eines Werkes) *ohne* Schutzanspruch zu gelangen, macht man sich strafbar! Es wäre also zumindest zu fordern, dass nur den Schutzvoraussetzungen genügende Werke und Teilwerke technisch geschützt werden dürfen. Würde eine technische Realisierung diese Differenzierung nicht erlauben, müsste der gesamte Schutz dahinfallen. Dies hätte automatisch zur Folge, dass zukünftige Implementationen von Schutzmechanismen die Gesetzesfeinheiten berücksichtigen.

Es steht ein Paradigmawechsel an, der von der Unterhaltungsindustrie getrieben wird. Sagen wir, die „Beweislast“ wird durch das Einführen technischer Massnahmen vom Urheber auf

---

[91] EU-Richtlinie 2001/29/EG.

[92] Die WIPO-Verträge treten erst in Kraft, wenn 30 Unterzeichnerstaaten diese ratifiziert haben, was bis heute rund 20 Staaten getan haben. Wenn die Mitgliederstaaten der EU die Urheberrechtsrichtlinie umgesetzt haben, dürften die Verträge also Gültigkeit erlangen.

den Konsumenten verlagert. Damit ist gemeint, dass bis anhin der Urheber zeigen musste, durch wen und wodurch seine Rechte verletzt werden. Nun aber, da technischen Sicherungen pauschal und flächendeckend eingesetzt werden, muss der Konsument zeigen, dass eigentlich gar keinen Schutzanspruch besteht. Dass diese pauschale Einführung vorangetrieben wird, kann man sogar Art. 5 Abs. 2 lit. b der Urheberrechtsrichtlinie[93] entnehmen, die - nota bene - fakultativ vorsieht, dass die Mitgliedstaaten Ausnahmen auf das vorgesehene Vervielfältigungsrecht machen können:

„[Ausnahmen] in Bezug auf Vervielfältigungen auf beliebigen Trägern durch eine natürliche Person zum privaten Gebrauch [...] unter der Bedingung, dass die Rechtsinhaber einen gerechten Ausgleich erhalten, wobei berücksichtig wird, ob technische Massnahmen [...] angewendet wurden."

Das heisst, wenn der private Gebrauch erlaubt wird, muss ein gerechter Ausgleich zu Gunsten der Urheber erfolgen. Dies ist soweit unproblematisch und kann über Verwertungsgesellschaften bzw. Leerkassettenabgaben vollzogen werden. Aber der Vergütungsanspruch der Urheber gegenüber den Verwertungsgesellschaften soll sich dann auch danach richten, ob ein technischer Schutz angewendet worden ist oder nicht. Das bedeutet, dass der Urheber mehr Geld erhalten soll, wenn er einen Schutz einsetzt![94]

3. Wirksamkeit

Gemäss Art. 6 Abs. 3 der Urheberrechtsrichtlinie[95] sind *„Technische Massnahmen als ‚wirksam' anzusehen, soweit die Nutzung eines geschützten Werkes [...] unter Kontrolle gehalten wird."* Das ist wohl dahingehend auszulegen, dass eine Massnahme dann nicht mehr wirksam ist, wenn sie von einem zu grossen Benutzerkreis auf einfache Weise umgangen werden kann.

Es wäre noch zu zeigen, ob gerade dies nicht auch ein Schlupfloch darstellen kann. Angenommen, ein technisch hochstehender und aufwändiger Schutz wird von einer weit verbreiteten und einfach zu bedienenden Software durch einen Nebeneffekt ausgehoben. Das heisst nach obiger Auslegung ist der Schutz nicht wirksam und Art. 6 Abs. 2 Urheberrechtsrichtlinie soll nicht anwendbar sein (dieser Art. verbietet Einrichtungen mit direktem Ziel der Umgehung des Schutzes). Wenn aber die Wirksamkeit nicht mehr

---

[93] EU-Richtlinie 2001/29/EG.

[94] Dass der Urheber mehr Geld erhält, wenn er keinen Schutz einsetzt ist zwar ebenfalls vorstellbar, dürfte aber nicht in die Denkweise der Urheberrechtrichtlinie passen.

[95] EU-Richtlinie 2001/29/EG.

gegeben ist, dürfte auch Art. 6 Abs. 1 Urheberrechtsrichtlinie nicht mehr greifen, folglich kann man für die Umgehung des Schutzes nicht belangt werden.

E. Internationale Vereinbarungen

Die grösste urheberrechtliche Herausforderung im Zusammenhang mit dem WWW (wie auch im Zusammenhang mit Software und Peer-to-Peer Netzen) ist unserer Meinung nach die schiere Grösse der Kommunikationsnetze und die Internationalität. Der Stand der Technik ist so fortgeschritten, dass dank Internet Landesgrenzen sozusagen keine Rolle mehr spielen. Anders verhält es sich beim Stand des Rechts: Die Urheberrechtlichen Gesetze sind an Nationalstaaten gebunden. Hat man Verletzungen des Urheberrechts, wie in den vorhergehenden Kapiteln geschildert, ausfindig gemacht, tritt die Frage der Verfolgung und Ahnung auf, die nicht trivial ist, da sich die meisten Fälle über die Staatsgrenzen hinaus erstrecken.

Einige Abkommen, die urheberechtliche Fragen über die Staatsgrenzen hinweg regeln sollen, sind in der Folge aufgeführt:

- Die RBÜ (Revidierte Berner Übereinkunft)
  Bei der RBÜ handelt es sich um einen völkerrechtlichen Vertrag zum Schutz von Werken der Literatur und Kunst, den die meisten Staaten der Welt unterzeichnet haben, seit 1989 auch die USA. Die erste Version ist datiert vom 9. September 1886, zuletzt revidiert wurde sie in Paris am 24. Juli 1971.
  Die RBÜ erklärt nationales Urheberrecht auch für Ausländer anwendbar. Ausländische Urheber werden in den Ländern, die den Vertrag unterzeichnet haben behandelt wie Inländer, umgekehrt werden aber jedem Ausländer auch Mindestrechte (z.B. Recht zur Erstveröffentlichung, Anerkennung der Urheberschaft und Schutz vor Entstellung) zugestanden.[96]
- TRIPS
  TRIPS dient zum Schutz des geistigen Eigentums, das Urheber-, Leistungsschutz- und Nutzungsrechte umfasst. Die Regelungen für ausländische Urheber sind ähnlich wie bei der RBÜ, die Mindestrechte werden aber ausgeweitet. Neu hinzu kommt der Begriff der *Mindestbegünstigung*, d.h. alle Vorteile die einem Mitgliedsstaat gewährt werden müssen auch allen anderen zugute kommen.[97]
- WIPO Copyright Treaty (WTC)
  Der WTC der WIPO (World Intellectual Property Organization) bezieht sich auf die Übereinkunft von Bern. Im Sinne von Art. 20 der RBÜ handelt es sich um eine „Erweiterung“ der RBÜ – es bleiben also alle Bestimmungen der RBÜ

[96] Weinknecht, Grundlagen des nationalen und internationalen Urheberrechts.

[97] Weinknecht, Grundlagen des nationalen und internationalen Urheberrechts.

erhalten, der WTC kann aber nur unter den Ländern Gültigkeit annehmen, die auch die RBÜ unterzeichnet haben. In Bezug auf neue Medien sind im WTC präzisierende Angaben zum Schutz von Computerprogrammen (Art. 4) , Schutz von Datenbanken (Art. 5) sowie zur Regelung von Vermietung und Vertrieb (Art. 6 und Art. 7) enthalten.

- WPPT (WIPO Performances and Phonograms Treaty)
  Der Vertrag regelt die internationalen Rechte von Urhebern im Bereich der Musik und "performenden" Künste.

Ein Prozess wird also immer nach nationalem Recht durchgeführt, so dass in vielen Fällen der Aufwand erheblich ist. So stellt sich die Frage, ob sich die Verfolgung einer Urheberrechtsverletzung im Ausland überhaupt lohnt. Sofern es sich nicht um einen grossen Konzern handelt, der seine Rechte, zum Beispiel an einer Software oder Musik-CD, verteidigen will, ist dies wohl zu verneinen. Aber auch die grossen Konzerne sind zurzeit gegenüber einigen Modellen wie dem Gnutella File-Sharing ziemlich machtlos.

Zusammenfassende Schlussbetrachtung

Die rasante technische Entwicklung der neuen Medien, insbesondere die des Internets, hat zu erheblichen rechtlichen Herausforderungen im Bereich des Urheberschutzes geführt. Unsere Nachforschungen haben ergeben, dass die urheberrechtlichen Grundlagen in den einzelnen Ländern meist gegeben sind – einige Anpassungen im Bereich des Schutzes von Software und Datenbanken dienen als sinnvolle Ergänzung. Auch für internationale Regelungen wurde gesorgt, mit Abkommen wie RBÜ, TRIPS oder WCT. Allerdings wird die Vermittlung von urheberrechtlich geschützten Daten nur in den Richtlinien der EU behandelt. Da diese Thematik vor allem bei P2P-Systemen zentral ist, wird es unabdingbar sein, dass auf internationaler Ebene mit der Richtlinie der EU vergleichbare Bestimmungen durchgesetzt werden. Ansonsten genügt der Stand des Rechts dem der Technik.

Es hat sich jedoch gezeigt, dass die praktische Umsetzung des Rechts und insbesondere die Durchsetzung desselben aufgrund der neuen Globalität der Probleme und der nach wie vor rasanten Entwicklung im technischen Bereich äusserst schwierig ist.

Gerade bei P2P-Systemen sind technische Schutzmassnahmen zur Durchsetzung von Urheberrechten nur dann sinnvoll, wenn sie flächendeckend eingeführt werden, wobei dies aufgrund der grossen Auswahl an P2P-Software nur mit erheblichem Aufwand seitens der Rechtsinhaber erreicht werden kann. Lösungen, wie Urheberrechte mit Schutzmassnahmen durchgesetzt werden können, bieten etwa DRM Systeme. Sie sollen die Urheberechte in differenzierter Weise in ein technisches System abbilden. Dabei gilt insbesondere zu beachten, dass mit den heutigen, unflexiblen Schutzmassnahmen oft (Teil-)Werke geschützt werden, welche die Schutzvoraussetzungen gar nicht erfüllen.

Ein weiteres Problem stellt der Schutz von Software dar. Weder das Urheberrecht noch der Patentschutz dient als angemessenes und befriedigendes Rechtsinstrument, um Software zeitgerecht zu schützen. Solange es keine besseren technischen Schutzmassnahmen gibt oder die heute realisierbaren Lösungen nicht konsequent eingesetzt werden, ist der Schutz von Software durch das Urheberrecht nur unzulänglich gesichert. Die Tatsache, dass der Patentschutz primär die allgemeine Software-Entwicklung bremst und die Machtposition der grossen Software-Hersteller stärkt, zeigt, dass auch dies keine befriedigende Lösung hervorbringt. Daher verstärkt sich der Gedanke nach einer auf internationaler Ebene geschaffenen, effektiven, neu definierten Rechtsgrundlage. Je länger eine solche Umsetzung dauert, desto mehr ist anzunehmen, dass sich der Open-Source Trend durchsetzt und Software definitiv zum Allgemeingut der Gesellschaft wird.

Zürich, 13. Juni 2002

Beat Hangartner Lukas Hohl Tobias Koch Till Quack