Durchsetzung rechtlich geschützter Zugangsinteressen durch nutzergruppenspezifisches Digital Rights Management

Diplomarbeit

Zur Erlangung des akademischen Grades: Diplom-Informationswirt

Von

Dominik Knopf

am
Institut für Informationsrecht
Prof. Dr. iur. Thomas Dreier, M.C.J.
Fakultät für Informatik
Universität Karlsruhe (TH)

Betreuer: Prof. Dr. iur. Thomas Dreier, M.C.J.

Abgabedatum: 28.10.2004

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Der illegale Tauschhandel von Daten aller Art (Musik, Filme, eBooks etc.) blüht, und dies trotz den verstärkten Anstrengungen der Musik- und Filmindustrie dies zu verhindern. Die Industrie entwickelt immer weitere Gegenmaßnahmen, um den Handel mit Daten auf die legalen Wege zu beschränken. Solche Maßnahmen scheinen am Anfang auch mit Erfolg gekrönt zu sein. Doch meist schon kurze Zeit später gibt es eine von den Internetnutzern erdachte neue Lösung, diese Maßnahmen zu umgehen.

Beispielsweise beschloss ein amerikanisches Gerichts die Schließung der Tauschbörse Napster[1] im Juli 2001. Nach einer zwischenzeitlichen Allianz mit der Bertelsmanngruppe wurde Napster Mitte 2002 von Roxio aufgekauft und legalisiert. Nun wetteifert sie mit anderen legalen Musikläden im Internet wie bspw. dem Apple iTunes Music Store. Im Gegensatz zu den neuen Tauschbörsen[2] sind diese Läden kostenpflichtig, was natürlich den Tauschbörsen weiterhin hohe Nutzerzahlen beschert. Parallel dazu florieren aber auch die legalen Angebote, was auf das Vorhandensein von großem Marktpotenzial schließen lässt, das sich geeignet kanalisiert in Vergütungen für den Urheber umwandeln lassen sollte.

Die Produzenten der diversen Daten (aus wirtschaftlicher Sicht: immaterielle Güter) wollen sich den illegalen Handel mit diesen natürlich nicht bieten lassen, doch sie bewegen sich mit der Langsamkeit eines Giganten, im Gegensatz zu den Internetnutzern, welche sich trotz ihrer großen Zahl extrem dynamisch und flexibel an neue Gegebenheiten anpassen. So reagieren die Produzenten mit immer restriktiveren Methoden, die selbst in bislang unangetastete rechtliche Bereiche einschneiden. "Zu unrecht" - so sehen es zumindest die Verfechter der Privatkopie. Die Industrien halten dagegen: "Raubkopieren sei ein Verbrechen".

Klar ist jedoch, dass nur ein stringentes Konzept zum Erfolg führen kann, welches zudem von Content-Produzenten und Content-Konsumenten abgesegnet wird.

Zudem muss auch der Staat eingreifen um dieses gigantische Tauziehen, welches momentan im Gange ist, zu stoppen, da sonst die Gesellschaft das Nachsehen hat. Doch welche Möglichkeiten hat der Staat? Letzten Endes ist der einzige Vorteil seine Unabhängigkeit vom

[1] Siehe auch [63]; inzwischen kommerzielles Angebot.
[2] Morpheus, Kazaa, eDonkey, eMule, BitTorrent und andere. Siehe dazu Anhang A

Markt und seine legislative Gewalt. Diese wiederum beschränkt sich allerdings nur auf das eigene Territorium, in diesem Falle Deutschland. Da das Internet jedoch eine globale Einrichtung ist, hat der einzelne Staat keine Möglichkeit, den internationalen Handel mit Raubkopien zu stoppen. Aus diesem Grund setzten sich multinationale Vertragsgemeinschaften die Aufgabe, das Urheberrecht auch global durchzusetzen. Problematisch ist allerdings, dass nicht alle Staaten dabei an einem Strang ziehen.

Im Moment obliegt der Schutz des geistigen Eigentums praktisch den Firmen. Sobald der Staat die Möglichkeiten (also durchsetzbares Recht) geschaffen hat, kann er die Firmen bei dieser Aufgabe unterstützen. Dabei darf er allerdings nicht nur einseitig zu Gunsten der Nutzer eingreifen, sondern sollte ausgleichende, sozial gerechte Regelungen treffen.

Die Unternehmen, die im urheberrechtlich relevanten Sektoren tätig sind, verwenden zum Schutz ihrer Daten technische Schutzmaßnahmen. Diese reichen von einem simplen Kopierschutz zu theoretisch sicheren Systemen durch sichere Betriebssysteme. Parallel dazu gilt das Digital Rights Management (DRM) als Wundermittel gegen die Verletzung der Urheberrechte. Doch nach einer gewissen Vorlaufzeit und mehreren gescheiterten Einführungsversuchen macht sich Ernüchterung breit. Erneut wird der Schrei nach neuen, härteren Gesetzen gegen Urheberrechtsverletzer laut.

Die Staaten, in denen inzwischen gesetzgebende Maßnahmen angelaufen sind, stellen sich langsam auf die neue Situation ein und regeln sie jeweils anders. Beispielsweise in den USA durch den Digital Millennium Copyright Act, ein Anhang zum Urheberrecht, der Firmen umfassende Rechte einräumt, eigene Nachforschungen gegen die Verletzung der eigenen Urheberrechte anzustellen. In Deutschland ist die Situation noch im Umbruch befindlich. Mitte des Jahres 2003 wurde die InfoSoc-Richtlinie der EU umgesetzt, die momentan noch ihres zweiten Korbs harrt[3]. Problematisch ist schon jetzt die Umsetzbarkeit der neuen Rechte, und auch die Einseitigkeit zu Gunsten des Urhebers.

[3] vgl. [1]

2 Zielsetzung

Da unsere Gesellschaft wesentlich von den geistigen Errungenschaften ihrer Mitglieder abhängt und solche Schutz bedürfen, wurde das Urheberrecht entworfen. Es stellt eine angemessene Vergütung für Denker und Künstler für ihre Arbeiten sicher. Mit den neuen Technologien ergab sich gegen Ende des letzten Jahrhunderts ein Schritt in ein neues, digitales Zeitalter, welches die Unabhängigkeit von Inhalten und ihren Medien mit sich bringt. Dies ist zum einen ein Geschenk, da eine Verbreitung dieser Inhalte nun viel einfacher geschehen kann, zum anderen bringt es aber auch große Gefahren mit sich, da bereits jetzt ein großer Teil der Daten an ihren Urhebern vorbei "gehandelt" (sei es entgeltlich oder unentgeltlich) werden.

Daher stellen sich nun die folgenden Fragen: Warum werden die Daten am Urheber vorbei gehandelt? Was kann dagegen getan werden? Was darf man dagegen tun? Warum funktionieren DRM-Systeme bis dato nicht? Ist das Urheberrecht dem digitalen Zeitalter gewachsen? Wie kann der Gesetzgeber das Urheberrecht anpassen? Müssen nur die Urheber geschützt werden? Oder auch die Anwender? Darf der technisch mögliche Rahmen ausgeschöpft werden?

Während gerade die ersteren Fragen noch trivial zu beantworten sind, wird es im Laufe dieser Fragenreihe immer komplizierter: Die Daten werden am Urheber vorbei gehandelt, da es häufig einfach billiger ist und weil es in diesem Bereich auch noch kein richtiges Unrechtsbewusstsein gibt. Aber bereits bei der Abwägung der nächsten beiden Fragen tut man sich schwer, sie in wenigen Zeilen zu beantworten.

In dieser Arbeit soll nun versucht werden, durch eine ganzheitliche Betrachtung der rechtlichen sowie der technischen Situation eine Lösung zu finden, welche maximale Synergie-Effekte hervorbringt. Daher wird zunächst ein DRM-System (DRMS) entwickelt, welches mehr Wert auf die sozialen Faktoren, die als einer der Gründe für das Nichtfunktionieren von klassischen DRMS ausgemacht werden, sowie das bestehende Recht legt. Einer der Schlüsselfaktoren dieses DRMS ist die Einbeziehung der Schrankenregelungen, d.h. die durch das Urheberrecht vorgenommene Unterteilung der Bevölkerung in bestimmte, teils bevorzugte Nutzergruppen, und der Schaffung eines vertrauenswürdigen Umfeldes, wodurch Nutzer eher angehalten werden, das neue System auch zu verwenden.

Anschließend werden rechtliche Anpassungen vorgeschlagen, die zum einen auf das beispielhafte DRMS eingehen, und zum anderen soziale Gerechtigkeit hinsichtlich des Urheberrechtes schaffen soll. Die Arbeit

beschränkt sich dabei auf Daten, die in digitaler Form vorliegen und auch als Produkt verkauft werden. Firmengeheimnisse oder andere Daten sind nur schwerlich für ein DRMS geeignet. Diese als Produkt verkauften Daten werden durch die neuen Technologien, wie das Internet und Computer, im Allgemeinen am meisten bedroht. Aufgrund der Aktualität für Deutschland und der Herkunft des Autors wird der Vorschlag ausgehend von der deutschen Rechtslage und auch für diese gemacht. Eine Verallgemeinerung ist sicherlich möglich, doch momentan nicht beabsichtigt.

Dazu wird die deutsche Rechtslage zunächst im Einzelnen dargelegt. Anschließend wird die aktuelle Situation im Internet aufgezeigt und technische Grundlagen geschaffen, aus denen das neue Nutzergruppenspezifische DRMS[4] geformt wird. Im Anschluss daran werden verschiedene gesetzliche Hilfsmittel diskutiert und ein Vorschlag für den zweiten Korb des deutschen Urheberrechtsgesetzes formuliert, damit dieses den Anforderungen des Informationszeitalters gewachsen ist.

[4] UGS-DRMS; user group specific digital rights management system

3 Definitionen und Begriffsklärungen

Zu Beginn werden zunächst die Kernbegriffe geklärt, die die nötigen Grundlagen für diese Arbeit bilden. Weitere Begriffsdefinitionen finden sich im Glossar am Ende, da diese sonst den Rahmen der Arbeit sprengen würden. Um einen Einstieg zu finden, lässt es sich wohl am besten mit dem Titel der vorliegenden Arbeit beginnen: „Durchsetzung rechtlich geschützter Zugangsinteressen durch nutzergruppen-spezifisches Digital Rights Management“. Bei genauerer Betrachtung verbirgt sich (fast) hinter jedem Wort ein ganzes Wissensgebiet. Daher werden nun die einzelnen Bausteine genauer erläutert, gefolgt von einigen wichtigen, im weiteren Verlauf des Textes häufig verwendeten Begriffen. Zudem wird die mit den jeweiligen Bereichen verknüpfte Fragestellung dargelegt.

Durchsetzung

Es gibt den Allgemeinsatz: Das beste Recht taugt nichts, wenn sich keiner daran hält. Und genau darum geht es hier. Rechte durchzusetzen ist im Alltag, also im realen Leben eher einfach. Sofern es sich bei dem greifenden Recht um Strafrecht handelt, wird der Staat zumeist aus Eigeninitiative tätig und ermittelt die genaueren Umstände (bei Bejahung öffentlichen Interesses; sonst auf Anzeige eines Bürgers).

Im Zivilrecht ist es bereits einen Deut schwieriger. Hier muss der Geschädigte Beweise sammeln, und den Fall der Schädigung einem Gericht vortragen, welches dann entsprechend befindet. Gerade diese Beweissammlung birgt schon im „praktischen“ Leben ungeahnte Schwierigkeiten. Außer in seltenen Fällen der Beweisumkehr ist es für den Geschädigten gar nicht so einfach, genügend Beweise für einen Verstoß des Beklagten zu sammeln. Und dies gilt in besonderen Maße für Schädigungen, die im Internet passiert sind, da diese anonym erfolgen. Ein Schädiger wird nämlich nur durch eine temporär vergebene IP-Adresse identifiziert. Aus Datenschutzgründen darf diese bei den Providern nicht gespeichert und zudem nicht an andere herausgegeben werden.

Damit stellt sich für die Arbeit die Frage: Wer setzt das bestehende Recht durch? Der Geschädigte oder der Staat? Die Durchsetzung steht also für die praktische Umsetzung eines theoretisch gewünschten und auch so im Gesetz verankerten Zustandes. Diese Arbeit beschäftigt sich nun damit, die bisher nur schwer mögliche Zuordnung zwischen einem Verletzer und einer Tat herzustellen, und dies sowohl durch technische Mittel - das UGS-DRMS – als auch durch juristische Mittel, durch Schaffung einer flexiblen rechtlichen Struktur.

Rechtlich geschützt

Dieser Begriff ist selbsterklärend. Man muss lediglich das faktisch schützende Recht eingrenzen, welches in dieser Arbeit das Urheberrecht als Ergebnis diverser internationaler Verträge[5] ist. Da die Welt des Computers als Mittel für die Massendatenverarbeitung noch recht jung[6] ist, haben weder Staat, noch große Industrien sich dem neuen Strom rechtzeitig angepasst, und müssen diesen Prozess in den letzten Jahren verstärkt nachholen. Gerade Staaten bewegen sich allerdings recht langsam, was die Schaffung und Überarbeitung neuer Gesetze angeht. So musste zunächst eine Grundlage im internationalen Umfeld geschaffen werden, welche dann zunächst in EU-Recht umgesetzt wurde, und schließlich 2003 in der Urheberrechtsnovelle mündete. In der Zwischenzeit entwickelte sich das Internet und die Computer maßgeblich weiter, womit die Novelle bereits veraltet scheint.

Wichtig ist daher die Schaffung eines flexiblen Rechts, welches durch richterliche Entscheidungen flexibel gestaltet werden kann. Damit dem Grundsatz der Rechtssicherheit genüge getan wird, muss ein passender „goldener“ Mittelweg gefunden werden, zwischen einer schwammigen Gesetzgebung, die durch Präzedenzfälle fortgeschrieben wird, und einem starren System, das der dynamischen Umgebung des Informationszeitalters nicht mehr gerecht wird.

Zugangs-interessen

„Zugangsinteressen“ ist wiederum ein Begriff, über den sich trefflich diskutieren lässt, da je nach vertretener Meinung, Wissen allen zur Verfügung stehen sollte, oder auch nur dem, der dafür zahlt. Sicherlich hat die Gesellschaft zu wichtigen Erfindungen beispielsweise ein Zugangsrecht und somit auch ein Zugangsinteresse, doch wie sieht es mit diversen multimedialen Stücken aus? Bei einem Lied kann das Interesse sicherlich nicht bejaht werden, doch vielleicht bei einem wissenschaftlichen Artikel? Wiederum muss das neue Urheberrecht auf der Schwelle zwischen einer digitalen Spaltung der Gesellschaft auf der einen und nicht sachgerechten Entlohnung von Immaterialgütern auf der anderen Seite balancieren.

Nutzergruppen-spezifisch

Speziellen Zugangsinteressen trägt der Gesetzgeber dahingehend Rechnung, dass im Gesetz Schrankenbestimmungen vorgesehen sind, die speziellen Nutzergruppen einen erweiterten Zugang zu den für sie relevanten Daten garantiert. Zum Beispiel fallen hierunter Lehrer, die zu Unterrichtszwecken Kopien aus Büchern o.ä. herstellen dürfen, was sonst wegen des nicht vorhandenen Vervielfältigungsrechtes verboten wäre. Fraglich ist nun, ob eine Erweiterung der Nutzergruppen Sinn

[5] siehe auch dazu Kapitel 4.3 „Überblick über das deutsche Urheberrecht“
[6] Man kann von etwa 20 Jahren ausgehen, in denen der Computer einer breiteren Masse zugänglich ist. Davor gab es nur wenige sog. „early adopters“, die die neue Technologie bereits verwendet haben.

macht, oder ob dieses System bereits ausgedient hat, wie gerade im Bereich der Privatkopie von Seiten der Industrie zu hören ist[7].

Digital Rights Management

Für die Industrie gibt es inzwischen seit über 10 Jahren den Begriff DRM als Schlagwort. Übersetzt bedeutet es so viel wie „Digitale Rechteverwaltung". Eine einheitliche gültige Definition existiert noch immer nicht, doch sind sich alle Beteiligten einig, was damit gemeint ist. Ein DRM-System schützt Daten im Sinne des Urhebers bzw. des Rechte Inhabers, erlaubt nur legale Zugriffe, verhindert unrechtmäßige Vervielfältigung und Verbreitung. Und falls es doch einmal passieren sollte, dass der Content[8] verbreitet wird, kann der Verletzer mittels eines Wasserzeichens in den Daten schnell herausgefunden werden. Wünschenswert und möglich sind Microbilling-Systeme, genau definierte Lizenzen, und weitere Zusatzsysteme. Interessanterweise gibt es kaum[9] solche Systeme, obwohl sie nahezu eine Ideallösung für das Urheberrecht und den Urheber versprechen. Die Gründe hierfür werden in Kapitel 7 näher erläutert. Für den Anfang kann man aus dem eben beschriebenen eine brauchbare Arbeitsdefinition herleiten:

„Ein DRM-System ist ein Programm welches Rechte an digitalen Daten beschreibt, verwaltet, sichert, schützt und nachverfolgt."

So weit nun der Titel der Arbeit. Weitere relevante Begriffe werden nun im folgenden Text in Kurzform erläutert.

Content

Worum geht es bei DRM und Urheberrecht überhaupt? Es geht um geistiges Eigentum, auch genannt Daten bzw. Content. Trotz gewisser Vorbehalte gegen zu häufige Anglizismen gibt es momentan leider kein ausreichend nuanciertes und dennoch prägnantes deutsches Wort, welches die so verschiedenen Daten des Internets vereint wie „Content" es tut. „Daten" allein sind in unserem Verständnis nur eine Ansammlung von Fakten, was den gerade für DRM sehr wichtigen Bereich der Multimedia-Daten außen vor ließe. Die Worte „Daten", „Informationen" oder „immaterielle Güter" werden in dieser Arbeit synonym für Content verwendet.

[7] Siehe auch: [2]
[8] eher: Inhalt, doch würde dieses Wort zu Verwirrungen führen. In Kapitel 6.2 folgt eine Zusammenfassung aller Teilbereiche, für die Content übergreifend steht.
[9] Zu den Systemen die eine gewisse Verbreitung haben, zählen die DRMS von Microsoft und Realmedia. Doch beide sind innerhalb kürzester Zeit nach dem Erscheinen einer neuen Version geknackt, und zusätzlich werden sie bisher nur in geringem Maße genutzt. Ein weiteres funktionierendes System bietet Apple in seinem Musikportal iTunes an, doch ist dies eher ein Mittel den beliebten iPod-Player von unliebsamen Mitkonkurrenten frei zu halten. Sieh hierzu auch: [3]

Rechtliche Grundbegriffe

Dieser Content wird von jemanden erschaffen, der erstmalig die Rechte daran erhält, dem sog. „Urheber“, „Autor“ oder „Erschaffer“. Er ist der „Rechtseigentümer“ (engl.: right owner) und kann diese teilweise veräußern[10], bspw. ein Autor, der einem Verlag das Vervielfältigungsrecht einräumt. Mit dem Kauf von Content bekommt man (selbst der Endnutzer) einen kleinen Teil der Rechte an ihm übertragen, und wird dadurch (zwischenzeitlich oder permanent) zum Rechteinhaber (engl.: right holder). Die Übertragung der Rechte erfolgt vertraglich, und zwar durch Erwerb und Einräumung einer Lizenz, die dem Erwerber einen genau umrissenen Verwendungsspielraum des Contents erlaubt.

Technische Schutzmaßnahmen

In Abgrenzung zum Begriff DRM soll nun noch Begriff „Technische Schutzmaßnahmen“ (TPM[11]) eingeführt werden. Vielfach werden beide Begriffe synonym verwendet, doch sind TPM einfach Schranken die einen unsachgemäßen Gebrauch von Content verhindern sollen. DRM geht von seinem Ursprung her weiter: Es soll eine ganzheitliche Strategie bilden, an der die Kunden teilnehmen und im Idealfall nicht bevormundet werden. Beispiele für TPM sind die momentan viel diskutierten Kopierschutzmechanismen von Audio-CDs, die in vielen der älteren CD-Player nicht mehr funktionieren, oder auch Abspielsperren von Daten auf portablen Geräten oder Computern. Sie sind elementarer Bestandteil aller DRM-Systeme aber nicht mit Ihnen gleichzusetzen. Doch auch hierzu in einem späteren Kapitel mehr[12].

[10] Im deutschen Recht sind die Rechte im Gegensatz zum amerikanische nicht übertragbar. D.h. es gibt kein sog. „work-for-hire“; doch mehr im folgenden Kapitel.
[11] technical protection measures
[12] Kapitel 9.1.

4 Überblick über das Urheberrecht

Zum tieferen Verständnis der im Anschluss an dieses Kapitel folgenden Betrachtungen muss zunächst das Wirken des Urheberrechts im Bereich der digitalen Daten im allgemeinen und des Internets im besonderen dargelegt werden. Obwohl das Urheberrecht in Deutschland in seiner jetzigen Form ein vergleichsweise junges Recht ist, konnte bei seiner Entstehung der Spezialfall Internet nicht beachtet werden, da sich selbst Computer noch in der Entwicklung befanden und an eine weltweite Vernetzung noch nicht zu denken war. Dennoch tragen die meisten Regelungen, die für den analogen Bereich gedacht waren immer noch dazu bei, dass das Konstrukt Urheberrecht funktioniert. Im Jahr 2003 schließlich kam es nach verschiedenen, für den analogen Bereich relevanten Änderungen[13] zur Implementierung der EU-Richtlinie 2001/29/EG[14]. Diese brachte einige wesentliche Neuerungen mit sich, welche im Abschnitt 4.5 noch näher betrachtet werden. Davor wird das Urheberrecht als Ganzes aufgeschlüsselt, gefolgt von weiteren, für das geistige Eigentum relevanten, Rechtsfragen bzw. Überlegungen. Doch zunächst folgt ein kurzer Abriss der geschichtlichen Entstehung des Urheberrechts.

4.1 Entstehung

Das Urheberrecht ist mit der Entwicklung der Technik eng verknüpft, wie sich anhand einer einfachen Überlegung zeigt:

Warum stellte sich beispielsweise in alten Hochkulturen, wie dem Römischen Reich, oder bei den Griechen nie die Frage nach einem Schutz des geistigen Eigentums? Sicherlich gab es dort auch die so genannten „plagiatores“, und man sah diese nicht gerne, doch trotz eines fortgeschrittenen Rechtssystems gab es kein Bedürfnis nach Schutz des geistigen Eigentums. Was sind hierfür die Gründe?

Zum einen war die Welt „größer“ als heute. Bei revolutionären wissenschaftlichen Entdeckungen, die sich gleichzeitig auch vermarkten ließen, war es den Autoren meist egal, ob diese Entdeckung im Nachbarland von anderen auch verwendet wurde. Es war ganz einfach außerhalb ihres unmittelbaren Horizontes. Außerdem würden die Gewinnspannen durch einen derart weiten Transport rasch auf Null schrumpfen.

[13] Diese wurden hauptsächlich durch Nachbesserungen der internationalen Verträge initiiert an denen Deutschland teilnahm.
[14] [4]

Heutzutage hingegen hat man die technischen Mittel nahezu alles an jeden beliebigen Ort auf der Welt zu einem angemessenen Preis zu bringen. Doch mit dieser Argumentation bewegt man sich mehr im patent- denn im urheberrechtlichen Bereich. Was war nun mit rein geistigen Werken? Hier kommt nun die Technik ins Spiel. Sicherlich konnte nicht verhindert werden, dass andere ein Werk unmittelbar reproduzierten, allerdings fehlte diesen Werken entweder die Nachhaltigkeit (bspw. das Nachspielen eines Liedes durch ein Orchester) oder es dauerte einfach so lange Zeit (bspw. das händische Abschreiben eines Buches), dass der Markt nicht gesättigt werden konnte.

4.1.1 Historie

Erst im 15. Jahrhundert mit der Erfindung des Buchdruckes[15] (1452) durch Johannes Gutenberg kam es zu einer grundlegenden Veränderung der Situation: Bereits gegen Ende dieses Jahrhunderts wurde eine Vorform des Urheberrechts beschlossen, die allerdings kein Autorenrecht war, sondern ein ausschließliches Verwertungsrecht für die Verlage. Dies änderte sich erst im Laufe der Jahrhunderte.

Im 17. Jahrhundert kam ein weiterer Gedanke hinzu, der mit in das Urheberrecht aufgenommen wurde, bzw. bereits implizit enthalten war: Durch den Schutz des geistigen Eigentums wurden Autoren angespornt, ihre geistige Tätigkeit überhaupt auszuführen, und somit zum volkswirtschaftlichen Optimum der Gesellschaft beizutragen.

Diesen Gedanken folgend wurde das Urheberrecht der einzelnen Staaten immer weiter an die fortschreitende Technik angepasst. Problematisch war hierbei, dass die Gültigkeit der jeweiligen Gesetze immer nur auf das Staatsgebiet des jeweiligen Landes beschränkt war und diese damit immer weniger praktikabel wurden – in dem Maß in dem sich die Reisegeschwindigkeit erhöhte und die Welt zusammenwuchs.

4.1.2 Urheberrechtliche Verträge

Aufgrund der äußeren Erfordernisse begannen verschiedene Staaten multinationale Verträge zu schließen, mit dem Ziel auch eine grenzübergreifende Wirkung des Urheberrechts zu erreichen. Aus Platz- und Relevanzgründen kann an dieser Stelle nur auf die wichtigsten

[15] Gutenberg hatte die damals revolutionäre Idee, Wörter in einzelne Buchstaben zu zerlegen, damit man diese einzelnen Buchstaben, die aus Metall gefertigt waren wieder verwenden konnte. Zudem konnte man schnell ganze Seiten eines Buches oder einer Zeitung neu zusammensetzen, genau dies war nämlich das Problem der bis dato verwendeten Holzdruckmethode u.a.

Verträge eingegangen werden, weshalb alle bilateralen sowie einige multilateralen Verträge herausfallen müssen.

4.1.3 Die Verträge

Die Revidierte Berner Übereinkunft (RBÜ)

Der älteste noch wirksame Vertrag im Bereich des Urheberrechts und zugleich Grundlage für weitere Verträge ist die Revidierte Berner Übereinkunft[16] vom 9. September 1886. Heute gilt sie zwischen den meisten der inzwischen fast 150 Mitgliedsstaaten in der Fassung von Paris (1971)[17], was durch Art 17 RBÜ[18] ermöglicht wurde, der eine kontinuierliche Verbesserung und Erweiterung des Urheberrechtsschutzes vorsieht. Dies geschah durch bisher 7 Revisionskonferenzen. In der RBÜ werden Werke der Kunst und Literatur geschützt, sofern die entsprechenden Urheber bestimmte personen- und werksbezogene Kriterien erfüllen.

Die folgenden Punkte sind auch noch in den WIPO[19]-Verträgen verankert: So sind bspw. auch Computerwerke als Sprachwerke in den Schutz inkludiert. Der Schutz dauert bis 50 Jahre nach dem Tod des Urhebers. Wie man auch noch im deutschen Urheberrecht sehen wird, ist auch ein Schutz für Datenbanken, deren spezifische Zusammenstellung auf einer intellektuellen Leistung beruht, gesondert geschützt. Alle Teilnehmerstaaten werden verpflichtet, Umgehungen des Urheberrechtes nachzugehen. Damit die Rechtsverfolgung auch konsistent gewährleistet werden kann, werden die Bestimmungen der RBÜ als kompensatorisches Fremdenrecht betrachtet: Als die drei wesentlichen Punkte lassen sich die Inländerbehandlung, die Formfreiheit und der Grundsatz der Mindestrechte nennen.

1989 gewann die Übereinkunft zudem gegenüber dem nachfolgend erläuterten Welturheberrechtsabkommen wieder an Bedeutung.

Welturheberrechtsabkommen (WUA)

Ein weiterer internationaler Vertrag ist das Welturheberrechtsabkommen vom 6. September 1952[20] von Genf. Es wird von der UNESCO verwaltet und unterscheidet sich im wesentlichen von der RBÜ dadurch, dass sein Schutzrahmen deutlich geringer ausfällt. Seine Bedeutung liegt momentan in erster Linie darin, dass es mit weiteren Staaten, die nicht der RBÜ beitreten wollten (oder konnten), im Außenverhältnis ein Mindestmaß an urheberrechtlichem Schutz garantiert. Dieser geschieht allerdings nicht durch einen Mindestrechtskatalog, sondern durch eine

[16] siehe dazu [5]
[17] siehe dazu [6]
[18] Heute: Artikel 27 RBÜ
[19] Seit 1967 wird die RBÜ von der WIPO verwaltet.
[20] In Kraft getreten am 16. September 1955; Revidiert 24.Juli 1971 in Paris (zusammen mit RBÜ)

Verpflichtung der unterzeichnenden Staaten zu „ausreichendem und wirksamen“ Schutz durch die nationalen Gesetze[21], zur Gleichstellung ausländischer Werke mit inländischen[22] (Inländerbehandlung), sowie Erfüllung aller nötigen Förmlichkeiten für ein Copyright-Kennzeichen „©“ in Kombination mit Namen des Rechteinhabers und des Erscheinungsdatums[23]. Es wurde eine Mindestschutzfrist von 25 Jahren ab Tod des Urhebers vereinbart. Zudem stellt sich das WUA selbst hinter die RBÜ zurück[24].

Rom-Abkommen (RA)

Nachdem die beiden vorgenannten Verträge das Werk, bzw. den Urheber ins Zentrum rückten, befasst sich das Abkommen von Rom[25] darüber hinaus mit dem Schutz der ausübenden Künstler, der Hersteller von Tonträgern und der Sendeunternehmen. Das RA wurde am 26. Oktober 1965 beschlossen, das zugehörige Gesetz kam am 15. September 1965. Nur Staaten die entweder dem WUA oder der RBÜ angehören, konnten nach Art. 23, 24 II, 28 IV RA dem RA beitreten. Es geht ebenfalls[26] vom Grundsatz der Inländerbehandlung aus[27]. Bemerkenswert ist, dass die USA nicht zu den teilnehmenden Staaten gehört.

TRIPS[28]

Mit der Gründung der World Trade Organisation[29] wurde am 15. April 1994 das WTO-Übereinkommen auf den Weg gebracht, welches als Anlage 1C die Übereinkunft über "handelsbezogene Aspekte der Rechte des geistigen Eigentums“[30] enthält und für alle Vertragsstaaten verbindlich ist. Man entschloss sich zu diesem Abkommen, da der Wert von ideellen Gütern durch das Fortschreiten der Informationstechnologien drastisch gestiegen war. Damit stieg das Interesse von Fälschern, und somit auch die Schutzbedürftigkeit des geistigen Eigentums im internationalen Umfeld. Nach damaligen Umfragen ging man davon aus, dass ca. 25 % aller damals verkauften Tonträger Fälschungen waren. Seine Bedeutung erlangte das TRIPS im Wesentlichen durch die Verknüpfung von Urheberrecht und Freihandelsabkommen. Damit erreichte es über 30 neue Staaten, die bis dato keinem Abkommen zum Schutz des geistigen Eigentums beigetreten waren.

[21] [7] Artikel 1
[22] loc. cit. Artikel 2
[23] loc. cit. Artikel 3
[24] loc. cit. Artikel 17
[25] siehe dazu [8]
[26] siehe auch WUA oder RBÜ
[27] [8] Artikel 2
[28] Agreement on Trade-Related Aspects of Intellectual Property Rights
[29] WTO; Welthandelsorganisation
[30] Übersetzung von TRIPS

Die TRIPS betreffen das gesamte Immaterialgüterrecht, sowie den Schutz gegen Piraterie. Dabei versuchen sie sicherzustellen, dass durch Durchsetzungsmaßnahmen nicht auch der rechtlich einwandfreie Handel behindert wird. In seinem Schutzumfang verpflichten die TRIPS die Mitglieder des WTO-Übereinkommens in Art. 9 Abs. 1 die wesentlichen Teile der RBÜ zu befolgen. Neu sind noch spezielle Regelungen zur Durchsetzung der Rechte sowie erweiterte Leistungsschutzrechte. Des weiteren lehnen sie sich an das RA an, wenngleich sie dieses nicht wörtlich übernehmen und in manchen Punkten sogar deutlich darüber hinausgehen[31].

WIPO

Ein weiterer sehr relevanter Vertrag wurde bei Gründung der Weltorganisation für geistiges Eigentum (WIPO[32]) am 14. Juli 1967 in Stockholm geschlossen. Ihr Ziel ist es den Schutz des geistigen Eigentums durch die Zusammenarbeit der teilnehmenden Staaten und die Kooperation mit anderen internationalen Organisationen weltweit zu fördern und die administrative Zusammenarbeit zwischen den Verbänden für den Schutz des geistigen Eigentums sicherzustellen. Seit 1974 besitzt sie den Status einer UN-Sonderorganisation mit Sitz in Genf. In Wahrnehmung ihrer Aufgaben ist sie die Hüterin zweier wichtiger Verträge: Zum einen dem WCT[33] und zum anderen dem WPPT[34].

Beide Verträge stammen vom 20. Dezember 1996 und werden von der WIPO verwaltet.

WCT

Im WCT[35] wurden zusätzliche, durch das Informationszeitalter notwendig gewordene Schutzmaßnahmen für das Urheberrecht eingeführt. Darunter fiel nach Art. 4, dass Computerprogramme als Werke der Literatur schützenswert sind, oder auch nach Art. 5, dass Datenbanken als Sammelwerk und auch bezüglich ihrer Zusammenstellung geschützt werden. In den Artikeln 6 bis 8 werden Urheber mit weiterreichenden[36] Rechten betreffs der Kontrolle über Vermietung und Verbreitung ausgestattet. Hier wird auch ein "Right of Communication to the public“[37] eingeführt, ein ausschließliches Verbreitungsrecht von Kopien, welches vor allem auf den Onlinebereich abzielt, da es sich auf die Möglichkeit bezieht, dass die Öffentlichkeit auf

[31] bspw. Schutzdauer
[32] [10]
[33] WIPO Copyright Treaty
[34] WIPO Performances and Phonograms Treaty
[35] WIPO Copyright Treaty
[36] Diese Rechte gehen teilweise deutlich über die RBÜ hinaus
[37] Ein Recht auf Bereitstellung für die Öffentlichkeit (sinngemäße Übersetzung; vgl. § 15 II UrhG)

dieses Werk zu beliebiger Zeit und von beliebigem Ort aus[38], d.h. nicht programmgebunden, zugreifen kann.

Zwei weitere für den Themenkomplex Digital Rights Management relevante Regelungen finden sich schließlich in den Artikeln 11, der das noch zu thematisierende Verbot der Umgehung technischer Schutzmaßnahmen vorgibt, und 12, der die Veränderung rechte-managementspezifischer Metainformationen verbietet.

Da die WIPO eine länderübergreifende Organisation ist, muss das von ihr beschlossene Recht erst in den teilnehmenden Staaten in nationales Recht umgesetzt werden. In den USA geschah dies durch den umstrittenen Digital Millennium Copyright Act[39], in der europäischen Union mittels eines Bündels von Richtlinien[40]. Als Umsetzungsjahr war 2002 geplant, durch diverse Verzögerungen befindet sich der Umsetzungsprozess mehrheitlich noch am Laufen[41]. Interessanterweise ist noch zu erwähnen, dass der Vertrag keine Verlängerung des Copyrights vorsah, jedoch sowohl in Amerika als auch in Europa mit einer solchen einherging[42].

WPPT

Im WPPT[43] geht es speziell um die Rechte von aufführenden[44] Urhebern, wie etwa Sängern, Schauspielern und Musikern oder anderen Urhebern öffentlicher Aufführungen mit vergleichbaren Aufzeichnungen. Zwischen dem WPPT und dem WCT gibt es viele inhaltliche Parallelen. So regeln beide das ausschließliche Recht der Verbreitung von (körperlichen) Vervielfältigungsstücken[45], den juristischen Schutz von technischen Schutzmaßnahmen[46] und auch das Verbot der Veränderung sog. Metainformationen die mittels einer

[38] Originaltext Art. 8 WCT: *„...in such a way that members of the public may access these works from a place and at a time individually chosen by them.“*
[39] DMCA; in erster Linie durch die umfassenden Rechte die der DMCA Urhebern gewährt, beispielsweise wird die Privatsphäre durch einen Auskunftsanspruch von Zivilklägern gegenüber ISPs nur gering geachtet, auch wurde Artikel 17 US Code "ergänzt": Die Regelungen sind für den Normalbürger größtenteils zu komplex und irreführen und enden mit einer Kriminalisierung eines großen Prozentsatzes der Bevölkerung. Volltext: [11]
[40] Manche existierten bereits zur Zeit als der Vertrag bestätigt wurde. Drei Richtlinien decken den Inhalt des WCT im Wesentlichen ab: 91/250/EC (Urheberschutz auch für Software) 96/9/EC (Urheberschutz für Datenbankwerke) und 2001/29/EC (die sog. InfoSoc-Richtlinie siehe auch entsprechendes Kapitel)
[41] siehe auch Deutschland: Eine erste Umsetzung ist seit 2003 in Kraft, der sog. zweite Korb lässt noch auf sich warten. Ursprünglicher Termin war der 22.12.02
[42] Neue Regelung: Schutz bis 70 Jahre nach Tod des Autors; EU glich sich damit Deutschland an, welches die längste Frist vorsah, die USA zogen mit
[43] WIPO Performances and Phonograms Treaty
[44] Im Original: „performing“
[45] Art. 8, 12 WPPT; vgl. Art. 6 WCT
[46] Art. 18 WPPT; vgl. Art. 12 WCT

Rechtebeschreibungssprache beigefügt wurden[47]. Auch in diesem Vertrag werden die Grundsätze der RBÜ[48] konsistent zur Anwendung gebracht. Neu ist im WPPT allerdings, dass er auf Persönlichkeitsrechte der darstellenden Künstler eingeht.

Weitere Verträge

Wie erwähnt konnte im Rahmen dieser Diplomarbeit keine vollständige Betrachtung aller relevanten internationalen Verträge durchgeführt werden. Es soll allerdings abschließend eine kurze weitere Aufzählung von für die Materie DRM minder relevanten Verträgen folgen, mittels derer man jedoch den Hintergrund erweitern kann:

Europa:

- Grünbuch „Urheberrecht und die technologische Herausforderung - Urheberrechtsfragen, die sofortiges Handeln erfordern“ von 1988
- Grünbuch „Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft“ von 1995
- Nachfolgepapier zum „Grünbuch über Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft“ von 1996

International:

- Genfer Tonträger-Abkommen von 1971

4.2 Kollisionsrechtliche Bemerkung[49]

Besonders relevant für das Urheberrecht im Zeitalter der Globalisierung ist die Frage, welches Recht bei grenzüberschreitenden Vorgängen zur Anwendung kommt. Man denke sich ein Buch, welches in Kanada geschrieben wurde, in den USA veröffentlicht, in Deutschland auf Deutsch übersetzt wurde und schließlich in Österreich zu Unrecht vertrieben wird.

Schutzlandprinzip

Zur Lösung eines solchen Falles wurde auf die Regelungen des Internationalen Privatrechts[50] zurückgegriffen, welches das sog. lex loci protectionis vorsieht, das Schutzlandprinzip. Damit könnte man in den entsprechenden Ländern, in denen die Verletzung des Rechtes (im IPR: in welchem das Delikt begangen wurde) vorgefallen ist, durch eine Klage Schadensersatz (oder vergleichbares) erlangen. Problematisch ist dabei, dass die aktuelle Form der RBÜ keinerlei konventionsinternes Kollisionsrecht enthält, das die Problematik lösen könnte, sondern auf

[47] Art. 19 WPPT; vgl. Art. 12 WCT
[48] Inländerbehandlung Art. 4 WPPT; Mindestrechte Art. 1, 2 WPPT; Formalitätenverbot Art. 20 WPPT
[49] vgl. [22]
[50] IPR

dieses autonome Kollisionsrecht vertraut[51]. Es sieht in Deutschland nach h.M. das Schutzlandprinzip für alle Immaterialgüter vor.

Rechtsunsicherheit

Damit ergeben sich bspw. in Verbindung mit der Inländerbehandlung Rechtsprobleme: Geistiges Eigentum, das im Ursprungsland nicht geschützt war, kann hierdurch plötzlich geschützt sein. Auch im Bereich des Internets bringt diese Auslegung nach h.M. weitere Probleme mit sich. Jeder, der Daten zum Abruf zur Verfügung stellt, müsste sich versichern, dass in allen[52] Ländern diese Sendung der jeweiligen Urheberrechtsordnung entspricht. Dies führt zu einer groben Rechtsunsicherheit und verhindert in dieser Form praktisch einen legalen Internetauftritt.

Inkonsistenz

Zudem würde ein konsistenter Rechtsschutz durch ein Bündel einzelner nationaler Schutzbestimmungen ersetzt. Damit würde der Urheber selbst auch Schaden nehmen. Er müsste in jedem einzelnen Land seinen Anspruch auf den auf das jeweilige Land entfallenden Anteil des entstandenen Schadens einklagen, was dem Schutzzweck des Urheberrecht zuwiderläuft[53]. Doch auch andere Prinzipien führen in diesem Bereich zu keinem besseren Ergebnis, weshalb das Schutzlandsprinzip immer noch Gültigkeit besitzt.

Herkunftslandprinzip

Die europäische Union verwendet in ihrer Satellitenrichtlinie 93/83/EWG das Herkunftslandprinzip. Dieses ist jedoch auf die Satelliten-ausstrahlung beschränkt, eine Übertragung auf das Immaterialgüterrecht wurde im entsprechenden Richtlinienentwurf abgelehnt. Zum einen unterscheidet sich die Online-Übermittlung grundlegend von der klassischen Satellitenübertragung, zum anderen könnte ein Land mit sehr niedrigem Urheberrechtsschutzniveau die Basis für sämtliche Server mit minder legalen Inhalten bilden, die dort wiederum legal wären. Von diesem Land bekämen die restlichen Länder dann den Rechtsschutz aufoktroyiert. Möglich wäre allerdings eine beschränkte Anwendung des Herkunftslandprinzips in einer Staatengemeinschaft wie bspw. der EU. Durch die neue Einführung des Aktes des "making available to the public" durch die InfoSoc-Richtlinie[54], ergibt sich ein ähnliches Problem wie beim Herkunftslandprinzip: Dieser Akt passiert direkt am Serverstandort, wodurch man wieder bei dem Vorgang des "Country Shoppings"[55] wäre, der Suche nach dem Land mit den günstigsten Schutzbedingungen. Die Kommission lehnt daher auch die

[51] Art. 5 II 2 RBÜ wurde als solches internes Kollisionsrecht angesehen, doch widerspricht dem der französische Text, der bei Auslegungszweifeln heranzuziehen ist.
[52] allen Ländern die Internet empfangen können, also faktisch allen
[53] Mosaikbetrachtung
[54] siehe auch Kapitel 4.5 „Urheberrechtsnovelle“
[55] siehe auch [22]

Verwendung des Serverstandortes als Ort der Rechtsverletzung als nicht sachgemäß ab. Nach h.M. wird der einzelne Abruf durch die Öffentlichkeit als Akt der Bereitstellung gewertet.

4.3 Überblick über das deutsche Urheberrecht

"So I'll remove the cause - hm hahaha - but not the symptom!"
(Frank 'n' Further in The Rocky Horror Picture Show)

Dieses Zitat steht im Gegensatz dazu wie ein normaler Arzt einen Patienten – und man kann das Urheberrecht problemlos als solchen für den Patient „geistiges Eigentum im Informationszeitalter“ sehen – behandeln sollte. Sicherlich ist erwünscht, dass die Ursache von Krankheitssymptomen ausfindig gemacht und eliminiert wird, doch was bringt es, wenn man die theoretische Ursache einer Krankheit[56] behebt, die Symptome allerdings weiter bestehen bleiben. Und nichts anderes passiert momentan mittels des weltweiten und damit auch des deutschen Urheberrechts. Die Ansätze sind richtig und in Ordnung, doch wenn die Industrie sich ausschließlich hierauf verlässt, werden die entstandenen Probleme nie behoben.

Nichtsdestotrotz bietet sich zunächst an, aus der Entstehungsgeschichte heraus einen Überblick über das Urheberrecht selbst zu geben. Dabei orientiert sich der Überblick im Wesentlichen an dem Aufbau des Urheberrechts und einem Artikel von Professor Dr. Thomas Hoeren[57], der die Probleme des Urheberrechts in der Informationsgesellschaft thematisiert.

Hierbei wird die Novelle des deutschen Urheberrechts von 2003 miteinbezogen. In einem nachfolgenden Kapitel wird genauer auf die Änderungen eingegangen. Abschließend wird versucht einen Ausblick auf den sich noch in Bearbeitung befindlichen[58] sog. zweiten Korb der Urheberrechtsnovelle zu geben.

Aufbau

Das deutsche Urheberrechtsgesetz (UrhG) ist klassisch aufgebaut. Zuerst wird der Bereich der zu schützenden Werke bestimmt. Geprägt ist es von der Beziehung des Urhebers zu seinem Werk. Daher werden diesem umfangreiche Urheberpersönlichkeits- und Verwertungsrechte eingeräumt. Ergänzt wird es durch sonstige Rechte, die dem Urheber zustehen, sowie Schrankenbestimmungen die seine Rechte zugunsten

[56] Wobei es in diese Analogie notwendig ist, das Informationszeitalter als Krankheit anzusehen, da es, zugegebenermaßen sehr eindimensional betrachtet, dem Urheber momentan mehr Schaden zufügt, als dass es ihm nützt.
[57] „Welche Chance hat das Urheberrecht im Internet-Zeitalter?“; [22]
[58] Stand Mai 2004

verschiedener, privilegierter Gruppen einschränken. In weiteren Abschnitten werden noch Schutzdauer, Rechtsverkehr des Urheberrechtes und verwandte Schutzrechte, die beispielsweise dem Schutz von Datenbankherstellern, Tonträgerproduzenten o.ä. dienen, geregelt. Von größerer Relevanz für die vorliegende Thematik sind allerdings die sog. „ergänzenden Schutzbestimmungen“ in den §§ 95a bis 95d UrhG, welche extra für die Weiterverwendung des Urheberrechtes in der Informationsgesellschaft eingefügt wurden, sowie die möglichen Rechtsnachfolgen bei Verstoß gegen das Urheberrecht.

Auslagerung von gew. Rechtsschutz

Nicht Bestandteil des Urheberrechts ist der gewerbliche Rechtsschutz, welcher zum einen mit höherem Anspruch versehen ist und zum anderen in eigenen Gesetzen geregelt ist. Man siehe hierzu auch das Wettbewerbs- und Kartellrecht (UWG), sowie die Patentgesetze.

4.3.1 Bestimmung des Urheberrechts

§1 Allgemeines. Die Urheber von Werken der Literatur, Wissenschaft und Kunst genießen für ihre Werke Schutz nach Maßgabe dieses Gesetzes.“

Wie bereits zu Beginn dieses Abschnittes erläutert, ist es für die Gesellschaft, repräsentiert durch den Staat, der die Interessen des Volkes wahrnehmen soll, wünschenswert, dem Urheber die ausschließliche Verfügungsgewalt (speziell auch im wirtschaftlichen Sinne) über seinem Werk zu gewähren. Der Begriff „Werk“ wird hierbei immateriell verstanden, im Gegensatz zu einem existierenden „Werkstück“, da der Urheber verständlicherweise mit Übertragung eines einzelnen Werkstückes, bspw. eines Romans, dem Käufer sicherlich keine urheberrechtlichen Verwertungsrechte einräumt.

4.3.2 Schutzbereich

Zunächst muss klar definiert werden was unter das Urheberrechtsgesetz fällt. Der Gesetzgeber gibt eine nicht abgeschlossene Liste von Werken aus Kunst, Wissenschaft und Literatur an[59].

Kunst, Wissenschaft, Kultur

Diese drei Begriffe werden hierbei sehr weit ausgelegt, da sie in sich selbst eine abgeschlossenen Liste bilden. Und Werke die sich nicht unter einen der Begriffe einordnen lassen würden keinen Schutz genießen. Beispielsweise wurde der Quelltext von Programmen als Sprachwerk deklariert, womit das fertige Programm auch in diese Sparte fällt.

[59] vgl. §2 (1) 1.-7. UrhG

Problematischer könnte es bei weiteren Multimedialen Schöpfungen werden. Während fiktive Figuren anhand Ihres Bewegungsgitters als Werke der bildenden Kunst klassifiziert werden[60], steht diese Klassifizierung beispielsweise einer ganzen virtuellen Welt noch aus. Sicherlich lassen sich Namen und Aussehen von Figuren in dieser Welt per Urheberrecht schützen, doch wie sieht es mit Parametern wie der Atmosphäre usw. aus? Vermutlich werden sie „passend" gemacht, was allerdings auch wieder Probleme mit sich bringen kann.

Gestaltungshöhe

In §2 (2) UrhG wird schließlich die Anforderung der Gestaltungshöhe gegeben: Ein Werk kann nur Schutz genießen, wenn es eine persönliche geistige Schöpfung ist. Damit ist eine Kombination von Elementen gemeint, die zum einen wissentlich und gewollt entstanden ist, und zum anderen ein gewisses Maß an Individualität besitzt. Auch hierbei ist nur ein geringes Maß anzulegen, so dass bereits Werke mit nur geringer schöpferischer Tätigkeit bereits Urheberrechtsschutz[61] genießen. Allerdings darf die Schranke wiederum nicht zu tief angelegt sein, da das Urheberrecht immer noch als Ausnahme zur Informationsfreiheit verstanden werden muss, besonders da ein Werk bis 70 Jahre nach Tod des Urhebers geschützt ist.

Form vs. Idee

Eine weitere wichtige Unterscheidung ist zwischen Form und Gestaltung bzw. Ausprägung zu treffen. Das Urheberrecht schützt nur die Form, sprich die konkrete Zusammenstellung eines Werke. Eine zu Grunde liegende Idee wird nicht geschützt, da man bei reinen Ideen von Allgemeingut ausgeht (Geschäftsprozesse, Algorithmen, Werbemethoden, wissenschaftliche Methoden). Daher haben manche Geschäftsrichtungen, wie Werbefirmen oder Showproduzenten, das Problem, das nur die konkrete Gestaltung der Werbung bzw. der Show geschützt ist, aber nicht das Konzept selbst. Natürlich muss man als Nachahmer hier aufpassen, da man sich mit jedem übernommenen Element immer weiter dem geschützten Format nähert. Bei literarischen Werken wird insbesondere der kreative Inhalt mitgeschützt.

4.3.3 Der Urheber

In den §§ 7-10 UrhG werden die Person des Urhebers und ein Teil seiner Rechte gegenüber eventuellen Miturhebern beschrieben. Als erstes wird definiert, dass der Urheber der Schöpfer eines Werkes ist. Damit ergibt sich auch, dass nur natürliche Personen Träger des Urheberrechtsschutzes sein können, d.h. dass im Falle einer gemeinsamen Urheberschaft alle schöpferisch am Werk Beteiligten als

[60] vgl. [12]
[61] Der von einem deutschen Reichgericht geprägte Begriff der „kleinen Münze" kommt hier zum Tragen.

Miturheber anzusehen sind. Hierunter fallen nicht Personen die nur Rat gebend tätig waren. Der Begriff des Schöpfers ist eng auszulegen[62].

Kein „work-for-hire“

So ist ein im Rahmen eines Arbeitsvertrag erschaffenes Werk immer noch dem Arbeitnehmer als Urheber zuzurechnen. Aus Gründen der Billigkeit ist er jedoch verpflichtet, dem Arbeitgeber umfassende Nutzungsrechte einzuräumen.

Miturheber

Ähnlich verhält es sich bei einem aus mehreren einzelnen Teilen zusammengefügten Werk, bei dem jeder Teilurheber von den anderen aus Treu und Glauben Nutzungsrechte am gemeinsamen Werk verlangen kann. Im allgemeinen wird der Schutz solcher Entitäten unter den verwandten Schutzrechten (siehe weiter unten Kapitel 4.3.10) geregelt. Aber auch im Rechtsverkehr des Urheberrechts finden sich hierzu weitere Anmerkungen.

Vermutung der Urheberschaft

Ein für das Internet interessanter Paragraf ist noch §10, in dem die Urheberschaft an einem Werk bis auf gegenteiligen Beweis dem „auf den Vervielfältigungsstücken genannten“ zugesprochen wird. Es besteht bei Internet-Seiten zwar eine Impressums-Pflicht, allerdings nicht in allen Ländern. Damit könnte es noch eine interessante Frage werden, wer als Urheber bei Bausteinen von Seiten solcher Länder vermutet wird.

4.3.4 Urheberpersönlichkeitsrecht

Die Urheberpersönlichkeitsrechte sind die ideellen Rechte des Urhebers an seinem Werk.

Veröffentlichungsrecht

Zunächst kann hier das Veröffentlichungsrecht genannt werden. Der Urheber allein darf entscheiden ob und wann sein Werk veröffentlicht wird. Dieses Recht wird wohl im seltensten Fall ein Problem darstellen.

Namensnennungs-recht

Anders sieht es schon mit dem Namensnennungsrecht[63] des Urhebers aus. Bei gewerblich erstellten Internetauftritten wird zumeist ja eine vertragliche Regelung vorgesehen, dass der Name des Erstellers auf der Internetseite genannt wird. Doch schon bei jeder einzelnen Fotografie oder Grafik wird es schwierig. Allein aus Platzgründen verbietet es sich von selbst direkt neben den Werken den Namen des Urhebers zu nennen. Häufig wird dieses Recht daher vertraglich abbedungen, wenngleich dies nicht so vorgesehen sein kann, da gerade für Grafiker und Fotografen die Namensnennung eigentlich überlebensnotwendig sein dürfte.

Entstellungsverbot

Ein weiteres Problem bringt §14 UrhG mit sich. Er beinhaltet das Entstellungsverbot eines Werkes. Es lässt sich nämlich nur im Einzelfall

[62] Es finden sich klare Parallelen zum kontinentalen *„droit d’auteur“* im Gegensatz zum amerikanischen System.
[63] § 12 UrhG

entscheiden was als Entstellung zählt. Gerade im Zeitalter der Informationstechnologie ist es wichtig zu entscheiden ob eine Digitalisierung auch als Entstellung eines Werkes zu sehen ist? Sie ist sicherlich „geeignet, seine berechtigten geistigen und persönlichen Interessen an seinem Werk zu gefährden“. Schließlich kann das Werk nun grenzenlos kopiert werden. Außerdem bringt die Digitalisierung (wobei es von der Güte ihrer Ausführung abhängt[64]) immer einen mehr oder minder starken Qualitätsverlust mit sich, der bei nicht wenigen Werken der Kunst als Entstellung bezeichnet werden darf.

Am Rande ist noch zu erwähnen, dass Urheberpersönlichkeitsrechte im Rom-Abkommen völlig fehlen und somit eine speziell deutsche Regelung sind.

4.3.5 Verwertungsrechte

Doch nun zum eigentlichen Kern des Urheberrechts: den materiellen Rechten, den Verwertungsrechten nach §§ 15 ff. UrhG. Auch hier ist die Aufzählung der Verwertungsarten keine abgeschlossene Liste, sondern bewahrt sich die Möglichkeit zukünftige weitere Verwertungsrechte einzuschließen. Die als gängig aufgezählten Rechte sind hingegen abgeschlossen und können nicht unter Berufung auf die weitergehende Verwertung erweitert werden.

Aufzählung

Die Rechte nach § 15 UrhG die ausschließlich dem Urheber gewährt werden, sind insbesondere das Vervielfältigungsrecht (§16 UrhG), das Verbreitungsrecht (§17 UrhG), das Ausstellungsrecht und auch das Recht der öffentlichen Wiedergabe, welches in §15 II UrhG weiter konkretisiert wird. Diese Rechte werden im Internet (auch bezeichnet als „gigantische, außer Kontrolle geratene Kopiermaschine“[65]) besonders einfach und häufig verletzt. Dies liegt an der weiter fortgeschrittenen Technologie, die es erlaubt von digitalen Daten verlustfreie Kopien herzustellen, und das mit gegen Null gehenden Grenzkosten[66]. Hier hat das Urheberrecht bisher noch kein angemessenes Mittel gefunden; für eine erste Novelle siehe weiter unten bei den ergänzenden Schutzbestimmungen.

4.3.5.1. Vervielfältigungsrecht

Unter dem Vervielfältigungsrecht versteht man „das Recht, Vervielfältigungsstücke des Werkes herzustellen“[67]. Unbenommen hiervon ist

[64] Kompressionsart, Dateiformat usw.
[65] Zitat aus [13]
[66] siehe dazu auch Kapitel 6.1 „Digitale Daten“
[67] §16 I UrhG

die Zitierfreiheit[68], sowie die Möglichkeit ein sog. Abstract des Werkes zu erstellen[69]. Die Vervielfältigungsstücke müssen körperlich oder zumindest von Menschen wahrnehmbar sein. Einer solchen Vervielfältigung kann der Urheber als Inhaber des ausschließlichen Rechts die Zustimmung verweigern[70]. Es ist hierbei egal, ob die Kopien flüchtig oder von Dauer sind. Besonders im Computerbereich finden sich damit mannigfaltige Spezialfälle:

Flüchtige Kopien

Während der Download aus dem Internet oder die Erstellung einer Kopie auf einem weiteren Medium zweifelsfrei als Vervielfältigungsstück zu erkennen sind, ist der Fall ein anderer bei extrem flüchtigen Kopien, beispielsweise in Arbeitsspeicher[71] oder Cache eines Computers. Oder auch bei rein technischen Prozessen, wie dem Caching von Programmen[72], um schnelleres Navigieren bei minimalem Datenverkehr zu ermöglichen, oder der Zwischenspeicherung auf einem sog. Proxy-Server eines Internetdiensteanbieters (ISP[73]). Diese Kopien stellen für sich keinen wirtschaftlichen Wert dar, fielen allerdings trotzdem unter das Vervielfältigungsrecht des Urhebers. Hier hat die europäische Kommission allerdings Abhilfe geschaffen, da sie in Art. 5 I der InfoSoc-Richtlinie sog. „transient and incidental acts of reproduction“[74] nicht als Vervielfältigung im engeren Sinne sieht.

Erwähnt werden sollte noch dass die Veröffentlichung von Daten nicht zwangsläufig mit der Erlaubnis zur beliebigen Vervielfältigung einhergeht. So ist durch das „im Internet zur Verfügung stellen“ die Erlaubnis zur Ansicht und den damit verbundenen, nicht zustimmungspflichtigen Kopien zwar gegeben, doch ist beispielsweise ein Hyperlink auf eine fremde Internetseite, bei dem nicht klar hervorgeht, dass der Content nicht der eigene ist[75], auch als Vervielfältigung anzusehen[76], oder beispielsweise das sog. „Grabben[77]“ von Content aus fremden Datenbanken mit offenen Schnittstellen, wie es vielfach möglich ist.

[68] § 45 ff. UrhG
[69] Dies findet vor allem bei wissenschaftlichen Werken Anwendung.
[70] Ausnahmen siehe folgendes Kapitel
[71] RAM; Random Access Memory
[72] bspw. Browser
[73] Internet service provider
[74] deutsch: „Flüchtige und nebenbei geschehende Vervielfältigungen“
[75] beispielsweise das Öffnen der Seite in einem untergeordneten Frame
[76] OLG Hamburg; 22.02.2001; 3 U 247/00
[77] „Grabben“ = „Anforderung von Daten“ meist durch ein Skript und anschließende eigene Aufbereitung der Daten; zumeist unter Umgehung vorgesehener Zahlmechanismen wie Werbebannern usw.

4.3.5.2. Verbreitungsrecht

Von geringerer Relevanz für die Informationsgesellschaft ist das Verbreitungsrecht nach §17 UrhG, da es die öffentliche Zugänglichmachung bzw. Verbreitung von körperlichen Vervielfältigungsstücken regelt, womit es reine Datenübertragungen ausschließt. Nach h.M. ist auch eine analoge Anwendung auf eBooks, Programme, Filme usw. welche auch in körperlicher Form existieren nicht möglich.

Diese neue Form der Verbreitung wird im neu hinzugekommenen § 19 a UrhG[78] zusammengefasst: Unter dieser neuen Figur der öffentlichen Zugänglichmachung versteht man das Anbieten des Inhalts an die Öffentlichkeit, wobei diese Ort und Zeit der Nutzung frei wählen kann. Damit ist die Downloadmöglichkeit[79] wohl der klassische Fall dieses Paragrafen. Unklar ist zunächst, ob auch sog. Push-Dienste, sowie Hybrid-Dienste, welche sich zwischen klassischem Rundfunk und der öffentlichen Zugänglichmachung befinden, abgedeckt werden[80].

4.3.5.3. Ausstellungsrecht

Ähnlich unwichtig ist auch das dritte garantierte Verwertungsrecht im Zusammenhang mit dem Internet. Nur selten werden Daten in körperlicher Form in der Öffentlichkeit ausgestellt[81], da hierunter nur unveröffentlichte Werke der bildenden Künste oder Lichtbildwerke fallen. welche seltenst erstmals als Ausdruck bzw. Analogwandlung eines digitalen Werkes ausgestellt werden.

4.3.5.4. Öffentliche Wiedergabe

Alle anderen Aufführungsarten fallen unter §15 II UrhG, das Recht der öffentlichen Wiedergabe. Hierin wird auf die nachfolgenden fünf Paragrafen verwiesen die diesen Komplex genauer aufschlüsseln: Zentral ist § 19 UrhG. Hierin werden Vortrags-, Aufführungs- und Vorführungsrechte voneinander abgegrenzt und definiert. Das Vortragsrecht (für ein Werk der Sprache) und das Aufführungsrecht (für ein Werk der Musik) erlauben es, solche Werke mittels technischer Einrichtungen, wie Bildschirm, Lautsprecher usw., der Öffentlichkeit auch außerhalb des Raumes, in dem die Aufführung oder der Vortrag stattfindet, wahrnehmbar zu machen.

In ähnlicher Form gilt hier das Vorführungsrecht für „Werke der bildenden Künste, ein Lichtbildwerk, ein Filmwerk oder Darstellungen

[78] Siehe dazu auch Kapitel 4.3.5.4.
[79] Download on demand
[80] siehe auch [14]
[81] Ausstellungsrecht nach §18 UrhG

wissenschaftlicher oder technischer Art“, wobei durch §19 IV 2 UrhG das Recht, die Funksendung erneut öffentlich wahrnehmbar zu machen, exkludiert wird und in § 22 UrhG behandelt wird.

Recht der öffentlichen Zugänglichmachung

Im durch die Urheberrechtsnovelle 2003 neu hinzugekommenen § 19 a UrhG ist das Recht der öffentlichen Zugänglichmachung verankert, welches die bis dato bestehende Streitfrage überflüssig machte, ob öffentliche Wiedergabe die gleichzeitige öffentliche Wiedergabe meint, die ja im Internet durch die zeitlich verschiedenen Abrufzeitpunkte nicht gegeben ist. Er ist für die Informationsgesellschaft daher sehr wichtig, da bei zum Download angebotenen Materialien immer Abrufzeit und -ort vom Nutzer frei gewählt werden können, was die Voraussetzung für § 19 a UrhG bildet.

Zudem wird hierin noch die drahtlose Kommunikation der drahtgebundenen gleichgesetzt, was bereits die zukünftigen Technologien mit berücksichtigt. Die Frage, wer Angehöriger der Öffentlichkeit ist, wurde allerdings wieder nicht abschließend geklärt. Beispielsweise fallen nach dem momentanen Dafürhalten unternehmensinterne Netzwerke nicht darunter, oder auch interne Datenbanksysteme, deren Nutzer sich mit steigender Zahl nur in den seltensten Fällen kennen dürften, bzw. die in Deutschland üblicherweise zur Bewertung herangezogene persönliche Beziehung pflegen. Hier sollte im zweiten Korb zu dieser Gesetzesnovelle nachgebessert werden.

Senderecht via Funk

§ 20 UrhG regelt das Senderecht, welches Übertragungen von Werken über klassischen Funk[82] betrifft. Unter diesen Sammelbegriff fällt im urheberrechtlichen Sinn auch das Senden von Daten via Videotext. Die folgenden §§ 20 a, b UrhG setzen europäisches Gemeinschaftsrecht im Bereich der Satellitensendung und Kabelweitersendungen um.

Bearbeitungen von Werken

In den noch zu den Verwertungsrechten zählenden §§ 23, 24 UrhG werden Werke die nur Bearbeitungen oder Umgestaltungen eines anderen Werkes sind, von selbstständigen Werken, die nur geringfügigen und somit freien Gebrauch des anderen Werkes machen[83], abgesetzt. Erstere bedürfen der Einwilligung des Urhebers des Urwerkes zur Veröffentlichung und Verwertung, letztere sind davon freigestellt. Zudem muss der Urheber des Urwerkes bereits zur Herstellung eines Derivatwerkes die Erlaubnis erteilen, sofern sich hierbei um eine Verfilmung, eine Ausführung von Plänen oder Skizzen eines bildenden Künstlers, einem Nachbau eines Bauwerkes oder um eine Veränderung einer Datenbank handelt. Besonders der letzte Punkt

[82] Ton- und Fernsehrundfunk, Satellitenrundfunk, Kabelfernsehen sowie vergleichbare Technik

[83] Die Melodie eines Tonwerkes zählt hierbei allerdings nicht als geringfügig. Es genügt bereits eine erkennbare Anlehnung.

ist für das Internet interessant, da vielfach automatisierte Programme auf Datensuche gehen: Viele Datenbanken stellen ihre Inhalte frei ins Netz, könnten also ohne größere Probleme im Ganzen ausgelesen werden und zu einem kostenpflichtigen Werk weiterverarbeitet werden.

4.3.6 Sonstige Rechte

Neben den gerade dargelegten Verwertungsrechten und den Urheberpersönlichkeitsrechten finden sich in den §§ 25 – 27 UrhG die sonstigen Rechte des Urhebers. Da sie für digitale Daten nur von geringem Interesse sind, werden sie in aller Kürze abgehandelt. Hierunter fallen das Zugangsrecht[84], das Folgerecht[85] und der Vergütungsanspruch bei Miete und Verleih[86].

Zugangsrecht

Unter dem Zugangsrecht versteht man die Pflicht, dem Urheber eines Werkstückes Zugang zu diesem zu gewähren, sei es zur Herstellung von Vervielfältigungsstücken oder zur Bearbeitung des Originals. Allerdings nur, wenn dem nicht berechtigte Interessen des aktuellen Besitzers entgegenstehen. Ein Herausgabeanspruch ist damit jedoch nicht verknüpft[87]. Da es sich hierbei um Zugang zu körperlichen Werken handelt, müsste man schon eine sehr verwegene Situation konstruieren um dieses Recht in Verbindung mit dem Internet sinnvoll anwenden zu können.

Folgerecht

Dies gilt ebenso für den folgenden Paragrafen, das Folgerecht. Hierbei handelt es sich um den Verkauf bzw. die Veräußerung eines Originals oder eines Vervielfältigungsstückes eines Werkes der bildenden Künste. Der Urheber soll mit 5 % am Verkaufserlös beteiligt werden und erhält dazu umfassende Auskunftsansprüche, die allerdings nur durch eine Verwertungsgesellschaft[88] geltend gemacht werden können.

Vergütungsanspruch

Das letzte der „Sonstigen Rechte“ befasst sich mit der Vergütung bei Verleihung und Vermietung. Es greift immer dann, wenn Originale oder Vervielfältigungsstücke durch eine der Öffentlichkeit zugängliche Einrichtung verliehen werden. Das klassische Beispiel hierfür ist sicherlich die Bibliothek, daher auch der Begriff Bibliothekstantieme, der für derartige Vergütungszahlungen gebräuchlich ist. Auch hier werden Auskunftsansprüche und dergleichen eingeräumt, welche ebenfalls nur durch Verwertungsgesellschaften wahrgenommen werden können. Im Zusammenhang mit dem Stichwort der Digitalen Bibliothek kann man

[84] § 25 UrhG
[85] § 26 UrhG
[86] § 27 UrhG
[87] § 25 II UrhG
[88] § 26 V UrhG; in der Praxis zumeist durch die Verwertungsgesellschaft Bild/Kunst

sich bei diesem Recht eher eine Verwendung im informationswirtschaftlichen Bereich vorstellen: Beispielsweise der Verleih von Dateien die nach einer gewissen Zeit unbrauchbar werden, einer Art zeitlich begrenzten und nutzungsbeschränkten Kopie.

4.3.7 Rechtsverkehr

Im Gegensatz zum amerikanischen Copyright ist es beim deutschen Urheberrecht im Normalfall nicht möglich die Urheberrechte und insbesondere die Verwertungsrechte ganz oder teilweise an Dritte abzutreten[89]. Dies kann nur durch Erteilung einer Lizenz oder durch Vererbung geschehen. In letzterem Falle ist die Übertragung vollständig im Sinne des Urheberrechtes, eventuell auch an eine Erbengruppe, die damit jeweils Miturheberstatus bekommen bzw. wie es durch eine Erbauseinandersetzung geregelt wird.

Lizenzen

Der Weg der Weitergabe von Rechten via Lizenz wird in §§ 31 ff. UrhG beschrieben: Eine Lizenz ist ein Recht, ein Werk auf alle beschriebenen Arten zu nutzen. Dieses Nutzungsrecht kann zeitlich, räumlich, und auch inhaltlich abgegrenzt werden (§ 31 I 2 UrhG). Der Umfang kann beliebig gestaffelt werden, kann auch unbeschränkt sein, was in der Praxis zumeist mit der Höhe des Lizenzentgeltes korreliert.

Während die zeitlichen und inhaltlichen Beschränkungen im Onlinebereich unproblematisch sind, muss bei räumlichen Nutzungsrechten darauf geachtet werden, dass sich im Internet aufgrund der globalen Reichweite eine räumliche Abgrenzung nicht vornehmen lässt, und somit eine derartige Beschränkung keinen Sinn macht. Möglich wäre in diesem Zusammenhang eine inhaltliche Beschränkung, die auf die Sprache bezogen ist, damit dennoch eine Art räumliche Abgrenzung erreicht wird, was selbstverständlich nicht mit allen Werksarten funktionieren kann. Gerade mittels DRMS lassen sich vielfältigste Beschränkungsarten denken, welche an den Content durch eine Rechtebeschreibungssprache gekoppelt werden.

Bei der Beschränkung der Lizenzen in § 31 I UrhG findet sich auch die Unterscheidung in das einfache und das ausschließliche Nutzungsrecht. Während ersteres in oben erläuterter Art definiert wird, findet sich beim ausschließlichen Nutzungsrecht vergleichbar zur patentrechtlichen ausschließlichen Lizenz der Zusatz, dass der Inhaber dieses Rechtes von anderen (sogar vom Urheber selbst) die Unterlassung der

[89] § 29 I UrhG; der Schutz der Kreativität wird als Menschenrecht angesehen und ist somit nach deutschem (im Gegensatz zu amerikanischem oder britischen) Verständnis unveräußerlich.

Verwertung einfordern kann. Hierzu besitzt er[90] ein Klagerecht, welches er parallel zum (und wie erwähnt auch gegen) Urheber einsetzen darf.

Ausschließliche Lizenzen

Ausschließliche Nutzungsrechte sind eher selten, wenngleich große Unternehmen diese immer per Pauschalklausel sich garantieren lassen. Im Normalfall sind diese nur bei speziell für einen Auftraggeber angefertigten, individuellen Werken vorgesehen. Ein Inhaber eines ausschließlichen Nutzungsrechtes darf mit Zustimmung des Urhebers[91] einfache Nutzungsrechte weiter übertragen, was einem Inhaber einfacher Nutzungsrechte verwehrt bleibt.

Unbekannte Nutzungsarten

Ein weiteres Problem für die lizenzierte Nutzung im Onlinebereich ist der zum Schutz des Urhebers bestimmte Paragraf 31 IV UrhG. Hierin wird bestimmt, dass „die Einräumung von Nutzungsrechten für noch nicht bekannte Nutzungsarten, sowie die Verpflichtung hierzu unwirksam sind“.

Dies ist zum einen sicherlich bei Altverträgen relevant, wenn man die Veröffentlichung im Internet als eine unbekannte Nutzungsart definiert, müssten Nachverhandlungen mit dem Lizenzgeber angetreten werden, da das Berufen auf Altverträge nicht möglich ist. Zumindest im Bereich von Veröffentlichung von Werken auf CD-ROM haben mehrere Gerichte (sowohl in Deutschland als auch in Europa eine neue Nutzungsart bejaht und haben sie als vor 1990 noch unbekannt terminiert[92]. Nachverhandlungen dürften häufig logistische Probleme darstellen, da oftmals kein Rechteinhaber bzw. seine Erben mehr auffindbar ist. Im Rahmen einer arbeitsvertraglichen Schaffung eines Werkes würden Treuepflichten greifen, die eine Übertragung regeln würden. Vergleichbare Treuepflichten lassen sich auch aus § 242 BGB herleiten, woraus sich zumindest eine Nachverhandlungspflicht des Urhebers mit dem Lizenzinhaber ergibt.

Zum anderen stellt sich die Frage nach neuartigen Online-Diensten: Fraglich ist es, ob man sich pauschal alle multimedialen bzw. Online-Nutzungsarten in einer Art Risikovertrag sichern kann. Der BGH verlangt in seiner Entscheidung „Videozweitauswertung III“ allerdings, dass diese Nutzungsarten genau spezifiziert werden müssen, was derartige Konstruktionen in der Praxis unmöglich macht[93].

Zweckübertragungs-theorie

Durch die mannigfaltigen Einsatzmöglichkeiten der Werke und die verschiedenen Arbeitsschritte bei Verwendung der Nutzungsrechte, hat sich aus § 31 V UrhG die sog. „Zweckübertragungstheorie“ entwickelt.

[90] Im Gegensatz zum einfachen Lizenznehmer der sich zur Prozessstandschaft erst ermächtigen lassen muss
[91] ein weiteres Schutzrecht
[92] siehe auch [15] und [16]
[93] siehe auch [17]

Damit wird abgedeckt, dass man ein Werk der im Vertragswerk bestimmten Verwendung zuführen darf, selbst wenn dabei die Grenzen des Vertragswerkes insofern überschritten werden, dass man weitergehende Nutzungsrechte in Anspruch nehmen muss, um den gewählten Zweck zu verfolgen. Als Beispiel sei hier genannt, dass Computer allein durch den technischen Aufbau bedingt Kopien des Werkes oder seiner Teile in RAM oder Cache anfertigen. Wenn man nun ein ausschließliches Recht hätte ein eBook zu lesen, und nicht es zu kopieren, könnte man sein erworbenes Buch nicht lesen ohne es zu kopieren. Da dies selbstverständlich nicht im Sinn der Vertragsparteien sein kann, wären diese technisch bedingten Kopien vom Vertrag gedeckt[94].

4.3.8 Schrankenbestimmungen / Rollensystem

Gesetzliche Schranken des Urheberrechts

Der am heißesten diskutierte und umkämpfte Bereich des neuen Urheberrechtes dürften die Schrankenbestimmungen und damit auch das Rollenkonzept sein. Doch welchen Sinn hat es? Das Urheberrecht stellt absolutes Recht dar, ist jedoch wie die meisten Gesetze auch sozialgebunden. Die verschiedenen Schranken restringieren die künstlich erzeugte Monopolstellung des Urhebers mannigfaltig ein, da sie sonst mit dem Grundgesetz unvereinbar wäre[95]. Die einzelnen Schranken, wie sie im ersten Teil dieses Kapitels einzeln dargelegt werden, sollen danach auf ihre Berechtigung für die Allgemeinheit (auch bezüglich der „neuen“ Informationsgesellschaft) überprüft werden.

Die Schrankenbestimmungen finden sich in den §§ 44 a – 63 a UrhG. Diese Paragrafen bilden einen abgeschlossenen Katalog, der keine weiteren Ausnahmen zulässt. Dies ist aufgrund der umfangreichen Berücksichtigung der verschiedenen Gesellschafts- bzw. Nutzerbereiche auch nicht nötig[96]. Die in den Schranken getroffenen Ausnahmeregelungen lassen sich grob in 3 Bereiche unterteilen:

Zum einen gibt es die zustimmungsfreien sowie die (zusätzlich) vergütungsfreien gesetzlichen Lizenzen, zum anderen die Zwangslizenzen[97]. Letztere wurden allerdings mit Ausnahme der sog. „verwertungsgesellschaftspflichtigen Zwangslizenzen“[98] gestrichen. Die jeweils wichtigeren Lizenzgruppen sind jedoch die beiden

[94] Allerdings muss man bei diesem Beispiel auch sagen, dass dieses spezifische Problem bereits pauschal durch die EU-Kommission gelöst wurde.
[95] Außer Art. 14 Abs. 1 GG. Beispielsweise würde sie in besonderem Maß in Art. 5 (Presse, Rundfunk und Informationsfreiheit) u.a. eingreifen.
[96] Zumindest zum aktuellen Zeitpunkt
[97] vormals in § 61 UrhG
[98] Diese sind per Gesetz durchsetzbar, aber auch gesetzlich scharf umrissen, und nicht etwa vergütungsfrei.

erstgenannten: Die zustimmungsfreien gesetzlichen Lizenzen erlauben wie der Name schon sagt, das Herstellen einer Kopie, unbenommen von § 16 UrhG. Da es sich trotz allem hierbei um eine Lizenz handelt, bleibt diese vergütungspflichtig. Wie die Vergütung zu erfolgen hat, bestimmt ebenfalls das Gesetz. Einige wenige Schranken sind zusätzlich zur Zustimmungsfreiheit auch noch von einer Vergütung freigestellt. Im folgenden werden die Schranken die das Urheberrecht bereithält kurz umrissen, und gegebenenfalls auf ihre Relevanz für die Themen Internet und DRM geprüft. Für eine exakte Beschreibung des Schutzumfangs muss jedoch das Gesetz selbst dienen oder ein Kommentar zum Urheberrecht[99].

4.3.8.1. Die Schranken im Einzelnen

§ 44 a UrhG

Im nachträglich[100] eingefügten § 44 a UrhG ist gleich die erste für die Informationsgesellschaft relevante Schrankenregelung. Computer kopieren zwangsläufig und technisch bedingt Daten bei der Verarbeitung, wie zum Beispiel beim Einlesen von der Festplatte in den Arbeitsspeicher, oder das sog. „Browsing“[101]. Auch beim Senden von Daten durch das Internet werden diese an Zwischenstationen oder auch an Proxy-Servern[102] kopiert. Daher wurde diese eng ausgelegte Schranke entworfen, die sowohl zustimmungsfreie, als auch vergütungsfreie Kopien gewährt. Dazu muss allerdings erfüllt sein, dass der Prozess des Kopierens integraler Bestandteil des Systems ist und während des Sendens oder der legalen Verarbeitung der Daten geschieht. Auch muss dieser Prozess wirtschaftlich unerheblich sein.

§ 45 UrhG

Die ursprünglich erste Schranke im Urheberrecht sieht vor, dass der Staat umfassende Rechte erhält. Werke dürfen für die Verwendung vor Gerichten und vergleichbaren Instanzen, sowie in Behörden vervielfältigt werden. Im Sinn der Rechtspflege und der öffentlichen Sicherheit dürfen Bildnisse vervielfältigt werden. § 45 III UrhG erlaubt die Veröffentlichung in den gleichen Fällen.

§ 45 a UrhG

Der bereits zitierte § 45 a UrhG erlaubt es körperlich behinderten Menschen den Zugang zu Daten zu finden. Aufgrund dieser Schranke dürfen nämlich Menschen, die in irgendeiner Weise durch Behinderung keinen oder nur erschwerten Zugang zu einem Werk finden, eine Version herstellen oder herstellen lassen, die ihnen den Zugang

[99] Bspw. [18]
[100] Dieser Paragraf ist auch durch die InfoSoc-Richtlinie initiiert worden.
[101] Mit Browsing ist das Anzeigenlassen von Inhalten aus dem Internet gemeint, wie aber auch das durchstöbern von Inhalten auf einer CD o.ä. .
[102] Proxy-Server halten häufig abgefragte Daten auf Abruf bereit, wodurch die Geschwindigkeit eines Zugriffs steigt. Dabei entsteht allerdings erwähnte Kopie auf diesem Server.

erleichtert. Allerdings dürfen diese Versionen nicht erwerbsmäßig hergestellt werden und sind natürlich angemessen vergütungspflichtig. Gerade in der Informationsgesellschaft, die einen erhöhten Bedarf an Informationen mit sich bringt, wird diese Schranke für behinderte Menschen um so wichtiger. Auch neue Konzepte, wie DRM-Systeme oder TPM dürfen sie nicht verletzen.

§ 46 UrhG

Eine gesonderte Stellung genießen durch § 46 UrhG auch Kirchen und Schulen, sowie nicht kommerzielle Stätten der Weiterbildung. Diesen wird nämlich gestattet, für den Schul- und Unterrichtsgebrauch Sammlungen von mehreren Autoren speziell für den Schulgebrauch zu erstellen. Auch diese Ausnahme ist vergütungspflichtig, muss allerdings dem Urheber zusätzlich angezeigt werden, und ihr kann widersprochen werden, falls der Urheber sich das Werk nicht mehr zurechnen lassen will, und die Verbreitung eingeschränkt hat. Im Falle von Musik gilt diese Schranke ausschließlich für den Musikunterricht an Schulen, allerdings nicht für den an Musikschulen.

§ 47 UrhG

Ebenfalls dem Unterrichtszweck dient die folgende Schranke § 47 UrhG. Diese beschreibt die für den hier thematisierten Onlinebereich eher uninteressante Möglichkeit von Bildungsstellen Werke aus dem Schulfunk auf Bild- oder Tonträger zu bannen, um sie zu Unterrichtszwecken weiter zu verwenden. Sofern die Werke nur temporär benötigt werden, sind die Kopien zudem vergütungsfrei.

§ 48 UrhG

Öffentlich gehaltene Reden sind gemäß § 48 UrhG nicht durch ein Recht geschützt. Jedermann steht die Verbreitung, Vervielfältigung und öffentliche Wiedergabe solcher Reden zu, die in der Öffentlichkeit zu Themen des Tagesgeschehen gehalten wurden, oder vor öffentlichen staatlichen bzw. kirchlichen Institutionen. Im letzteren Fall dürfen die Reden allerdings nicht als Sammlung von Reden überwiegend eines Redners veröffentlicht werden.

§ 49 UrhG

Paragraf 49 UrhG erlaubt es Auszüge bzw. einzelne Artikel aus Zeitungen oder Rundfunkkommentaren aus Informationsblättern in anderen Informationsblättern wieder zu geben. Dies muss angemessen vergütet werden, sofern es sich nicht um eine Übersicht mit kurzen Auszügen handelt, bspw. einen Pressespiegel.

§ 50 UrhG

Zur Berichterstattung über Tagesereignisse sieht § 50 UrhG vor, dass Werke in einem durch den Zweck gebotenem Umfang vervielfältigt, verbreitet und öffentlich wiedergegeben werden dürfen.

§ 51 UrhG

Paragraf 51 UrhG regelt die Zitierfreiheit. Sie ist besonders für die Wissenschaft relevant, da durch sie erlaubt wird, fremde Werke per Zitat in einem eigenen zu zitieren. Diese Wiedergabe fremder Gedanken ist allerdings nur erlaubt, wenn das Werk einen geistigen Bezug zu dem eigenen Werk hat. So ist beispielsweise die Wiedergabe fremder Werke

in Datenbanken selbstverständlich nicht als Zitat anzusehen. Es wird unterschieden in Groß- und Kleinzitat, sowie Musikzitat. Für ein Zitat gilt die Vergütungsfreiheit. Um die Rechte des Urhebers allerdings zu achten, muss jedem Zitat der Urheber bzw. die Herkunft beigefügt sein.

§ 52 UrhG

Die öffentlich Wiedergabe bereits in körperlicher Form erschienener Werke ist Thema des § 52 UrhG. Er erlaubt die öffentliche Aufführung von Werken unter eng umrissenen Voraussetzungen. Sofern diese Aufführung nicht Erwerbszwecken Dritter dient, ist sie zustimmungsfrei, sofern sie zudem noch sozialen Zwecken in einem abgegrenzten Rahmen dient (ein abgeschlossener Katalog findet sich in § 52 I UrhG), ist die Aufführung auch vergütungsfrei.

§ 52 a UrhG

Bei seiner Einführung im Jahr 2003 verursachte § 52 a UrhG ähnlich viel Wirbel, wie die direkt im Anschluss zu diskutierende Privatkopie. Besonders wissenschaftliche Verlage sahen sich in Ihren Rechten beschnitten, da nämlich eine Schranke eingeführt wurde, die es erlaubt, dass sowohl für den Gebrauch im Unterricht als auch für die eigene Forschung einem abgegrenzten Personenkreis Material öffentlich zugänglich gemacht werden darf. Dies ist im Sinne des § 19 a UrhG, welcher ja vor allem für die Bereithaltung von Werken im Internet konzipiert wurde, und daher auch wichtig für das Urheberrecht in der Informationsgesellschaft ist. Die Kopien sind allerdings normal vergütungspflichtig und der Urheber muss auch vor der öffentlichen Zugänglichmachung informiert werden.

§ 53 UrhG

Diese Schranke ist die wohl am emotionalsten diskutierte Schranke des neuen Urheberrechts: Die Privatkopie. Hier soll zunächst nur eine wertungsfreie Definition erfolgen. Kritische Anmerkungen finden sich am Ende der Arbeit im Kapitel „Anpassung der rechtlichen Situation“. Die Privatkopie besagt im Wesentlichen, dass es einer natürlichen Person erlaubt ist, sofern sie nicht weder mittelbar noch unmittelbar in kommerziellem Interesse handelt, sich von legal hergestellten Werkstücken eine Privatkopie anzufertigen oder auch anfertigen zu lassen, sofern dies unentgeltlich erfolgt. Mit der neu hinzugekommenen Formulierung „rechtswidrig hergestellte Kopie“ wollte man vor allem den Download aus Tauschbörsen unterbinden. Nach h.M. kann man diesen Absatz auch dahingehend auslegen. Doch rein nach dem Wortlaut wäre es zulässig, eine rechtmäßig *hergestellte* Privatkopie rechtswidrig *öffentlich zur Verfügung stellen*. Damit wäre der Download, sprich die weitere Privatkopie erlaubt. Hier gibt es Nachbesserungsbedarf im zweiten Korb der Novelle.

Im weiteren Verlauf des § 53 UrhG findet sich ein abgeschlossener Katalog von Umständen, die eine Privatkopie erlauben. Manche Arten sind zusätzlich beim Rechteinhaber anzuzeigen. Auf keinen Fall dürfen Privatkopien verbreitet oder veröffentlicht werden.

§ 54 UrhG

In den §§ 54 – 54 h UrhG sind Regelungen über die Vergütung zusammengefasst, die ein Urheber bei Nutzung seiner Werke aufgrund von Schrankenregelungen erhalten soll. Beispielsweise ist hier die Pauschalabgabe auf Tonbänder, Videokassetten und andere Leermedien, sowie auf Aufzeichnungsgeräte geregelt. Ebenso die pauschalen Abgaben auf Kopiergeräte, sowie einzelne Kopien an öffentlichen Plätzen (wie Bibliotheken, Universitäten, Geschäften usw.). Im Gesetz ist auch ein Auskunftsanspruch gegen die Hersteller und Importeure solcher Geräte verankert. In § 54 h UrhG findet sich der Hinweis auf die Verwertungsgesellschaften: So sind die Vergütungen zumeist nur durch diese einzutreiben, und bspw. der Auskunftsanspruch auch nur durch diese einzufordern. Beispiele für Verwertungsgesellschaften sind die GEMA[103], die ZPÜ[104] oder auch die VG Wort[105]. Die Pauschalabgaben werden im Zuge des zweiten Korbes der Urheberrechtsnovelle wohl noch stark reformiert[106]. Daher soll es bei diesem Kurzüberblick bleiben, da man auch noch nicht weiß, ob sie eine und wenn welche Rolle sie im weiteren Verlauf der Debatte spielen werden.

§ 55 UrhG

Sendeunternehmen dürfen nach § 55 UrhG Kopien eines Werkes zu dessen Sendung sie berechtigt sind herstellen, welche dann in der Regel binnen eines Monats gelöscht werden müssen.

§ 55 a UrhG

Nach der Hinzunahme von Datenbanken zu urheberrechtlich geschützten Werken wurde in § 55 a UrhG auch eine Schranke geschaffen, die die Vervielfältigung bzw. Bearbeitung eines mit Zustimmung des Urhebers legal erworbenen Werkstückes, sofern dies für den bestimmungsgemäßen Gebrauch erforderlich ist. Dies gilt auch für Teile. Diese Schranke erhält einen ähnlichen Status wie § 44 a UrhG. In beiden wird das zweckmäßige Arbeiten mit legal erworbenem Content geregelt.

§ 56 UrhG

Weniger relevant für die Informationsgesellschaft ist die nun folgende Schranke in § 56 UrhG. Sie erlaubt zur Vorführung entsprechender Apparaturen in Geschäftsbetrieben das erstellen von Kopien und die öffentliche Wiedergabe. Die dabei entstandenen Kopien müssen allerdings anschließend direkt gelöscht werden.

§ 57 UrhG

Den gleichen Stellenwert wie zuvor hat die Schranke in § 57 UrhG. In der Informationsgesellschaft wie auch schon davor gibt es immer die

[103] Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte; die GEMA ist Gesellschafter der ZPÜ und verwaltet die Nutzungsrechte der Musikschaffenden in staatlichem Auftrag.
[104] Zentralstelle für private Überspielungsrechte; zuständig für Abgaben auf Leerkassetten und dergleichen im Rahmen von Privatkopien.
[105] Verwertungsgesellschaft
[106] Siehe hierzu: Kapitel 4.5.2 „Stand des zweiten Korbes“

Möglichkeit, dass beispielsweise auf einem Foto viele urheberrechtlich geschützte Dinge zu sehen sind. Doch nun jeden Rechteinhaber ausfindig zu machen, und die Rechte zu erwerben wäre Irrsinn. Daher erlaubt diese Schranke die zustimmungs- und vergütungsfreie Vervielfältigung, Verbreitung und öffentliche Wiedergabe von Werken, sofern sie nur unwesentliches Beiwerk zum eigentlichen Werk sind.

§ 58 UrhG

Paragraf 58 UrhG erlaubt die Abbildung von Werken im Sinne der Werbung bei einer Veranstaltung, wo diese Werke verkauft werden sollen. Außerdem ist es Museen, Bibliotheken und dergleichen in engem zeitlichen Zusammenhang zu einer entsprechenden Ausstellung erlaubt, Bilder von Werken zum Zwecke der Werbung oder der Dokumentation anzufertigen, wobei allerdings kein eigenständiger Erwerbszweck verfolgt werden darf. Da es sich hierbei um körperliche Werkstücke handelt, ist maximal die Werbung per Internet von Belang, weshalb diese Schranke in Verbindung mit dem Internet eher uninteressant ist.

§ 59 UrhG

Ähnlich uninteressant im Bereich DRM und Internet ist die in § 59 UrhG verankerte Schranke die den urheberrechtlichen Schutz von in der Öffentlichkeit angesiedelten Werken bzw. Gebäuden nahezu aufhebt. Jedem steht es frei, Abbildungen der Werke (bzw. der Außenfassade bei Gebäuden) zu vervielfältigen, verbreiten oder zu veröffentlichen.

§ 60 UrhG

Paragraf 60 UrhG erlaubt die Vervielfältigung und die nicht zu gewerblichen Zwecken vorgenommene Verbreitung eines Bildnisses durch den Abgebildeten bzw. nach dem Tod durch dessen nächste Verwandten. Interessant ist, dass hierunter nicht die Veröffentlichung bzw. die öffentliche Zugänglichmachung fallen. So ist es immer noch der Fall, dass man ein Bild, welches man von einem Fotografen anfertigen lässt, nicht ohne dessen Erlaubnis im Internet verwenden darf, was der heutigen Zeit nicht mehr angemessen ist.

Nicht mehr zu den Schranken kann man § 62 ff. UrhG zählen. Sie sollen dennoch der Vollständigkeit halber in diesem Kapitel aufgeführt werden.

§ 62 UrhG

Paragraf 62 UrhG enthält ein Änderungsverbot an den Werken, an denen man durch die vorgenannten Regelungen Nutzungsrechte erhält, mit Ausnahme von Übersetzungen (bei Sprachwerken), Änderungen der Tonlage (bei Musikwerken) oder Größenänderungen (bei Bildwerken). Weitere Änderungen bei Sammlungen nach § 46 UrhG, sofern sie zum Unterrichtsgebrauch notwendig sind, müssen dem Urheber angezeigt werden und bedürfen dessen Einwilligung.

§ 63 UrhG

Im vorletzten Paragrafen 63 UrhG wird die Verpflichtung definiert, dass bei entstandenen Vervielfältigungsstücken stets eine Quellenangabe in der im Verkehr angemessenen Form sichtbar beigefügt sein muss.

§ 63 a UrhG

Am Schluss des Abschnitts wurde § 63 a UrhG eingefügt, der darlegt, dass man nicht im Voraus auf die einem in diesem Kapitel zufallenden Vergütungsansprüche verzichten, sondern sie allenfalls einer Verwertungsgesellschaft übertragen kann.

4.3.8.2. Berechtigung des Rollensystems

Die Gründe für die Notwendigkeit eines Schutzes des geistigen Eigentums wurden bereits zu Anfang dieses Kapitels erläutert. Auf den Punkt gebracht dient dies dem Schutz der Innovation und des Ausdrucks der Persönlichkeit. Doch warum wurde dieses Schutzrecht wieder teilweise eingeschränkt? Dies liegt in der Wechselwirkungslehre begründet, auch Schaukeltheorie genannt. Nach dieser werden verschiedene Grundrechte gegeneinander abgewogen. Hier sind es Art. 5 GG und Art. 14 GG. Ersterer beinhaltet u.a. das Recht auf Informationsfreiheit, d.h. dass jeder Bürger das Recht hat, „sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten“. Artikel 14 GG hingegen regelt das Recht auf Eigentum und die Unantastbarkeit desselben. Dabei enthält der Artikel auch bereits seine eigenen Grenzen: „Inhalt und Schranken werden durch die Gesetze bestimmt.“ Und diese Schranken wurden in das Urheberrecht nach Abwägung integriert.

Eine uneingeschränkte Monopolstellung des Urhebers würde das Recht der Allgemeinheit auf Information zumindest in manchen Bereichen wesentlich beschneiden. So könnte ein Urheber beispielsweise aus monetären Gründen die Umsetzung von Daten in eine behindertengerechte Form verhindern. Da dies sozial ungerechtfertigt wäre, entstand beispielsweise die Schranke in § 45 a UrhG, welche Menschen, die anderweitig nicht befähigt wären ein Werk wahrzunehmen, gestattet Zugang zu diesem Werk zu finden. Wie bereits weiter oben erwähnt, ersetzt diese Schranke nur die Zustimmung des Urhebers, nicht jedoch die zu zahlende Vergütung.

Eine genauere Darlegung dieser Sachlage würde allerdings den Rahmen dieser Arbeit sprengen, weshalb es bei diesem Beispiel bleiben muss. Abschließend kann zumindest gesagt werden, dass das Rollensystem im analogen Bereich seine Berechtigung keinesfalls verloren hat. Wie es im für die Informationsgesellschaft so wichtigen digitalen Bereich aussieht, soll nun gesondert betrachtet werden.

Berechtigung im digitalen Bereich

Da das Urheberrecht auf Grund des Informationszeitalters reformiert werden muss, steht natürlich auch zur Debatte, ob das Rollensystem auf das neue Urheberrecht übertragbar ist. Die Abwägung zwischen Art. 5 und 14 GG bleibt immer noch bestehen, weshalb die Frage sich nur dahingehend formulieren ließe, ob sich an der Situation etwas dahingehend geändert hat, dass Urheber und Rechteinhaber nun

schlechter gestellt sind, als sie es vorher waren. Hier kann argumentiert werden, dass dies möglicherweise durch die erhöhte Gefahr der Verbreitung von digitalen Daten gegeben ist. Doch gleichzeitig muss man auch ganz klar sehen, dass auch das Interesse der durch die Schranken begünstigten an den Daten bzw. dem Content gestiegen ist, da das allgemeine Bedürfnis nach Information in unserer Zeit größer geworden ist, u.a. weil die Zeit auch schnelllebiger geworden ist.

Nachdem also der Sinn des Rollensystems bejaht wurde, nebenbei bemerkt er ohnehin nur halbherzig von den Rechteinhabern bezweifelt, muss ebenso diskutiert werden, ob die einzelnen Schranken gegen neue Schutzrechte durchsetzbar gemacht werden sollen oder nicht. Hiervon besonders betroffen ist die bereits mehrfach thematisierte Privatkopie. Dies soll allerdings gesondert geschehen, vor allem im Kapitel „Rechtliche Möglichkeiten des Staates“ am Ende der Arbeit.

4.3.9 Schutzdauer

Der Schutz setzt unmittelbar mit Erschaffung des Werkes ein. Er muss nicht in irgendeiner Form beantragt werden, sondern wird allein durch Erfüllung der zum Schutz berechtigenden Bestimmungen erteilt. In Deutschland währt er bis 70 Jahre nach dem Tod des Urhebers. Danach wird das Werk „gemeinfrei“. Im Falle mehrerer Miturheber erlischt es 70 Jahre nach dem Tod des am längsten lebenden Miturhebers. Auch hier ist wieder die Unterscheidung zwischen Idee und Form entscheidend: Eine Originalaufnahme (so sie existierte) der 9. Symphonie Beethovens wäre frei von Urheberrechten, während die Aufführung selbiger durch das Berliner Symphonie-Orchester unter Leitung Herbert von Karajans aus dem Jahr 1980 noch vollen Urheberrechtsschutz genießt.

4.3.10 Verwandte Schutzrechte

Hierunter fallen alle schützenswerten Leistungen, die sich jedoch nicht durch eine schöpferische Gestaltungshöhe auszeichnen, dem Schaffen des Urhebers an sich aber recht ähnlich sind. Damit bekommen sie dem Urheber recht ähnliche Rechte, allerdings logischerweise in geringerem Umfang, zugewiesen. Dieses Kapitel soll ebenso wie das nachfolgende nur im beschränkten Umfang in dieser Arbeit behandelt werden, da es für den Onlinebereich nur von minderer Relevanz ist.

Unter die verwandten Schutzrechte fallen Sonderrechte für wissenschaftliche Ausgaben, die immerhin bis 25 Jahre ab Erscheinen geschützt sind, sowie nachgelassenen Werke die trotz abgelaufenem Urheberrecht bei Ersterscheinung noch einmal 25 Jahre geschützt werden. Die gleiche Schutzzeit gilt für Lichtbilder, deren Rechte beim Lichtbildner liegen.

Auch ausübende Künstler erhalten umfassende Schutzrechte an ihrer Darbietung, die erst nach frühestens 50 Jahren erlöschen. Die gleichen Rechte erhalten Künstler die gemeinsam ein Werk aufführen, sie gelten als Miturheber. Auch die Urheberpersönlichkeitsrechte werden partiell den ausübenden Künstlern zugestanden: So haben sie ein Recht auf Namensnennung und dürfen eine Beeinträchtigung ihrer Darstellung verbieten. Die Rechte auf Verbreitung, Vervielfältigung und Veröffentlichung werden analog angewendet, ebenso die Vergabe von Nutzungsrechten.

Des Weiteren werden Tonträgerhersteller, Sendeunternehmer und Datenbankhersteller mit analogen Schutzrechten ausgestattet.

In Teil drei des Urheberrechts gibt es noch zusätzliche Regelungen bezüglich des Films. Darin wird die Rechtssituation rund um den Film und Laufbilder geregelt. So zum Beispiel die Verwertungsrechte an den Filmen, die Rechte der ausübenden Künstler und der Filmproduzenten, sowie auch wieder ein Entstellungsverbot.

4.3.11 Ergänzende Schutzbestimmungen der Informationsgesellschaft

In den neu eingefügten §§ 95 a – d UrhG und auch § 96 UrhG finden sich weitere Schutzbestimmungen für die Informationsgesellschaft. Diese werden im folgenden Kapitel dargelegt.

4.3.11.1. Protektion technischer Schutzmaßnahmen

Eine der wesentlichen Neuerungen, und zugleich eine die bei Einführung viel Streit hervorgerufen hatte, ist der gesetzliche Schutz von TPM. Damit soll verhindert werden, dass zum einen technische Schutzmaßnahmen zum Schutz des Urheberrechts überhaupt umgangen werden, und zum anderen, dass es für den normalen Nutzer zu einfach gemacht wird, eine Umgehung mittels vorgefertigten Programmen vorzunehmen, welche nämlich auch verboten sind. Zwar nicht der Besitz, so doch „die Herstellung, die Einfuhr, die Verbreitung, der Verkauf, die Vermietung, die Werbung im Hinblick auf Verkauf oder Vermietung und der gewerblichen Zwecken dienende Besitz von Vorrichtungen, Erzeugnissen oder Bestandteilen sowie die Erbringung von Dienstleistungen“ die technische Schutzmaßnahmen umgehen, und nebenbei nur einen begrenzten wirtschaftlichen Wert haben.

Dieser Paragraf birgt allerdings einige Probleme, weshalb die Regelungen im zweiten Korb konkretisiert werden müssen:

Zum einen gibt es Definitionsprobleme mit dem Begriff „wirksamer Kopierschutz“. Er wird zwar in § 95 a II UrhG noch konkretisiert, doch

sollte auch der Stand der Technik eine Rolle spielen, da ein veralteter Kopierschutz auch seine Wirksamkeit einbüsst. Beispielsweise umgeht Microsoft Windows bei deaktiviertem Autostart, was jedem Nutzer natürlich freisteht, den Kopierschutz MediaMax CD-3[107]. Hier kann man wohl nur noch schwerlich von einem wirksamen Kopierschutz sprechen, obwohl er der gesetzlichen Definition genügen würde.

Ein zweites Problem ergibt sich mit der einschränkenden Definition in § 95 a III 2 UrhG nach der Programme betroffen sind, die „abgesehen von der Umgehung wirksamer technischer Maßnahmen nur einen begrenzten wirtschaftlichen Zweck oder Nutzen haben“. Bei enger Auslegung würde das Hinzunehmen von weiteren Features, wie zusätzlichen Brennmöglichkeiten usw. unbesehen von deren Nutzen, das vormals illegale Programm legalisieren. Und dies widerspricht dem Rechtsverständnis.

4.3.11.2. Durchsetzung von Schrankenbestimmungen

In Absatz eins dieses Paragrafen 95 b UrhG findet sich eine abgeschlossene List von Schrankenbestimmungen die trotz der Verwendung von Schutzmaßnahmen durchsetzbar bleiben sollen. Das heißt, dass derjenige, der Schutzmaßnahmen nach Vorgabe des UrhG verwendet auch für die Einhaltung der Schranken zu sorgen hat. Dazu muss er entsprechende Maßnahmen zur Verfügung stellen, die den Zugriff auf die Daten im Rahmen der Schranken trotzdem erlauben. Dies wird einer der Punkte sein, die im Fortgang dieser Arbeit noch ausführlicher diskutiert werden, da das UGS-DRMS diese Durchsetzung der Schranken in seinem geschlossenen Kreislauf integriert. Im zweiten Korb wird der Schrankenkatalog eventuell noch um die Durchsetzung der Privatkopie erweitert.

4.3.11.3. Schutz der zur Rechtewahrnehmung erforderlichen Information

Ebenso wichtig für die Informationsgesellschaft ist der Schutz von Metainformationen der in § 95 c UrhG geschaffen wird. Wie später noch genauer thematisiert wird, stellen die Metainformationen oder „Informationen für die Rechtewahrnehmung“, wie das Gesetz sie nennt, die Essenz von DRMS dar. In diesen Informationen werden zumeist Lizenzen übertragen. Durch Änderungen daran können DRMS problemlos ausgehebelt werden. Daher überlässt der Gesetzgeber nicht nur dem Urheber den Schutz seiner Metainformationen, sondern schützt diese separat. Auch hier gilt: Es ist notwendig, dass die Veränderung wissentlich geschieht, und zudem dürfen solchermaßen veränderte

[107] siehe auch [19]

Daten nicht „verbreitet, zur Verbreitung eingeführt, gesendet, öffentlich wiedergegeben oder öffentlich zugänglich gemacht werden“.

4.3.11.4. Kennzeichnungspflichten

Damit Nutzer über das Vorhandensein von Schutzmaßnahmen informiert werden, legt § 95 d UrhG eine Kennzeichnungspflicht fest. Geschützte Werkstücke müssen eine Information tragen, mit Angaben zu Art und Eigenschaften des Schutzes. Zudem muss zur Möglichkeit der Durchsetzung der Schrankenregelungen nach Kapitel 4.3.11.2 auch der Name des Verwenders der Schutzmaßnahmen oder dessen Firma nebst Anschrift auf dem Werk enthalten sein.

Inzwischen haben einige Hersteller von Audio-CDs ein einheitliches Zeichen für kopiergeschützte CDs entwickelt, die trotz des Kopierschutzes in normalen CD-Playern und Computern abgespielt werden können:

Abbildung 1: Zeichen für kopiergeschützte Audio-CDs der IFPI

Denn einer der ursprünglichen Gründe für die Kennzeichnungspflicht ist der Schutz der Nutzer, die immer wieder nichts mit einem legal erworbenen Werk anfangen konnten, da dieses sich aufgrund des Kopierschutzes, der zumeist außerhalb von Normen arbeitet, nicht in älteren standardisierten Abspielgeräten verwenden ließ.

4.3.11.5. Verwertungsverbot

§ 96 beinhaltet ein totales Verwertungsverbot rechtswidriger Kopien. Sie dürfen weder verbreitet noch für eine öffentliche Wiedergabe verwendet werden. Ähnliches gilt für illegal veranstaltete Funksendungen. Diese dürfen auch nicht aufgenommen werden. In diesem Paragrafen wird im Prinzip eine Trivialität in Gesetzestext gefasst, da es wohl selbstverständlich sein dürfte, dass aus Illegalem kein Recht entstehen kann.

4.3.12 Rechtsfolgen

Damit das Gesetz auch seine Wirkung entfalten kann, muss natürlich auch eine Strafandrohung existieren. Die möglichen Rechtsfolgen einer Verletzung des Urheberrechtes sind in den §§ 97 ff. UrhG festgehalten. Sie können, genau wie in vielen anderen Rechtsgebieten, in zivil- und strafrechtliche Folgen unterschieden werden. Erstere beschreiben das

Recht zwischen den Parteien selbst, während strafrechtliche Folgen wie der Name schon impliziert durch den Staat als Strafe verhängt werden.

4.3.12.1. Zivilrechtliche Konsequenzen

Anspruchsgrundlagen für zivilrechtliche Schritte bilden die Paragrafen §§ 97 – 99 UrhG sowie § 101 a UrhG. Nach § 97 I UrhG kann der Verletzte Beseitigung der Beeinträchtigung, im Falle der Gefahr der Wiederholungstat Unterlassung und nicht zuletzt auch (im Verschuldensfalle) Schadensersatz verlangen. Zu letzterem lässt sich noch sagen, dass das vorausgesetzte Verschulden recht weit ausgelegt wird. Nach dem BGB fallen hierunter Vorsatz und Fahrlässigkeit. Während der Vorsatz recht trivial, da selbsterklärend, ist, reicht bereits eine grobe Vorstellung, dass die eigene Handlung nicht legal ist, damit sich der Verletzer den Fahrlässigkeitsvorwurf gefallen lassen muss[108]. Und dieses Wissen dürfte bei der in den Medien breitgetretenen Diskussion um Urheberrecht und Privatkopie in der heutigen Zeit nahezu immer gegeben sein. Problematisch für den Verletzer ist der zu entrichtende Schadensersatz. Er schuldet dem Verletztem ergo dem Rechteinhaber die sog. Naturalrestitution nach § 249 BGB. Selbige ist bei Urheberrechtsverletzungen allerdings nur selten möglich, weshalb sich nach § 251 BGB mehrere Berechnungsarten anbieten, zwischen denen der Verletzte jederzeit[109] wechseln kann:

Zum einen der Ersatz des entstandenen Schadens zuzüglich des entgangenen Gewinnes. Dieser dürfte aber nur schwer nachzuweisen sein, weshalb sich Berechnungsmethode Nummer zwei, Zahlung einer angemessenen Lizenzgebühr daher eher anbietet. Dies kann für den Verletzer allerdings sehr teuer werden, da eine Lizenz für die Bereitstellung einer Datei an 40 Millionen Nutzer einiges kosten dürfte[110]. Die dritte Methode schließlich bietet sich ausschließlich im Falle einer gewerbsmäßigen Verletzung des Urheberrechtes an. Sie sieht die Herausgabe des erlangten Gewinnes nach Abzug aller Kosten vor, unberührt davon, ob der Verletzte überhaupt logistische, gewerbliche u.s.w. Möglichkeiten hatte, diesen in gleicher Form zu erzielen. In bestimmten Fällen[111] ist ein zusätzlicher Schadensersatz möglich, der die Kosten zur Kontrolle der Rechtsverletzungen decken soll. Im Gegensatz zu dem in Amerika geltenden „Triple damage"-Prinzip ist es in Deutschland allerdings nicht üblich einen sog.

[108] „Irrtum / Unwissenheit schützt vor Strafe nicht" wie ein gängiger Allgemeinsatz lautet.
[109] Sowohl während als auch noch nach dem Prozess
[110] Hierbei geht der Autor von der Schaffung einer Upload-Möglichkeit in einem durchschnittlichen File-Sharing-Programm aus.
[111] Beispielsweise erreichte die GEMA einen solchen von bis zu 100%

Strafschadensersatz zu verhängen. Einen solchen fordern die diversen Industrien, welche sich von zunehmenden Urheberrechtsverletzungen betroffen sehen allerdings. Populärstes Beispiel ist wohl die Musikindustrie.

Im Unterschied zu den im BGB vorgesehenen Schadensersatzregelungen sieht das Urheberrechtsgesetz in § 97 II UrhG auch den Ersatz von Schäden vor, welche keine Vermögensschäden sind. Speziell ist hier die Verletzung des Namensnennungsrechtes zu nennen. Dies geschieht um Künstlern wie beispielsweise Fotografen, die von der Bekanntheit Ihres Namens bzw. von Mund-zu-Mund-Propaganda leben die entstehenden Schäden zu kompensieren.

Nach § 97 III UrhG sind weitere Ansprüche unberührt. Damit dürften insbesondere solche aus dem Bereicherungsrecht, Deliktrecht, der Geschäftsführung ohne Auftrag und auch dem Wettbewerbsrecht gemeint sein. Ansprüche nach dem BGB hätten zudem den Vorteil, dass sie nicht zwangsläufig ein Verschulden voraussetzen und vor allem an eine 30 jährige Verjährungszeit gebunden sind. Insgesamt spielen diese aber eher eine untergeordnete Rolle, da § 97 UrhG bewusst sehr umfangreich gehalten ist.

Eine weitere Anspruchsgrundlage findet sich in § 98 UrhG, nach der der in seinem Recht Verletzte die Vernichtung[112] aller unrechtmäßigen Kopien bzw. die Überlassung[113] gegen eine angemessene, die Herstellungskosten nicht übersteigende Vergütung verlangen kann. Sollte dies gegenüber dem Verletzter bzw. dem Eigentümer einer unrechtmäßigen Kopie gegenüber unverhältnismäßig sein, hat der Verletzte nur Anspruch auf andere den Zustand ebenfalls beseitigenden Maßnahmen. In § 99 UrhG wird bestimmt, dass mit den Vorrichtungen die zur Herstellung der rechtswidrigen Vervielfältigungsstücke kongruent zu § 98 UrhG verfahren wird. Dies bedeutet also ebenfalls Vernichtung oder Herausgabe derselben oder im Sonderfall den Zustand der Verletzung beseitigende Maßnahmen.

Als letzte Anspruchsgrundlage von zivilrechtlichen Folgen im Urheberrechtsgesetz findet sich in § 101 a UrhG ein weitergehender Auskunftsanspruch verankert. Während nach § 97 I UrhG iVm § 242 BGB der erzielte Gewinn dargelegt werden muss, verfügt § 101 a UrhG zusätzlich, dass auch der gesamte Verkehr der Vervielfältigungsstücke, d.h. Herkunft und Vertriebsweg[114] inklusive Namen und Anschrift aller bekannten Hersteller, Lieferanten, Vorbesitzer usw., zugänglich gemacht werden muss.

[112] § 98 I UrhG
[113] § 98 II UrhG
[114] außer bei Unverhältnismäßigkeit

Liegen weder Vorsatz noch Fahrlässigkeit seitens des Rechtsverletzers vor, so kann er zur Abwehr aller Ansprüche nach §§ 97 – 99 UrhG den Rechteinhaber durch Zahlung einer angemessenen Lizenzgebühr entschädigen. Als letzter Punkt im zivilrechtlichen Rechtsfolgeteil soll noch die in § 100 UrhG verankerte Haftung des Unternehmer erwähnt werden, demgegenüber der Verletzte die Ansprüche aus §§ 97 – 99 UrhG mit Ausnahme des Schadensersatzes geltend machen kann.

4.3.12.2. Strafrechtliche Konsequenzen

Die Verletzung des Urheberrechtes sowie der bloße Versuch[115] können strafrechtliche Konsequenzen nach sich ziehen. Das Gesetz sieht eine Freiheitsstrafe von bis zu 3 Jahren oder eine Geldstrafe vor. Und das bei einem Vergehen, das für den größten Teil der Deutschen allenfalls ein Kavaliersdelikt ist. Allerdings wird die Staatsanwaltschaft nicht aus eigenem Antrieb[116], sondern nur auf Strafantrag bzw. in Form einer Privatklage tätig. Für den Verletzten ist dies der bessere, da einfachere Weg. Denn der Verletzte besitzt zum einen nicht die weit reichenden Mittel der Staatsanwaltschaft, womit ein Nachweis der Verletzung sehr schwer werden dürfte. Und zum anderen ist der Weg der deutlich kostengünstigere, da der Staat beispielsweise für sämtliche Sachverständigenkosten aufkommt. Im Falle gewerblicher Vergehen gegen das Urheberrecht handelt es sich zumeist um ein Offizialdelikt, d.h. die Staatsanwaltschaft schreitet von Amtes wegen ein. Hier erhöht sich die Strafe auch auf 5 Jahre Freiheitsentzug bzw. Geldstrafe. Die Staatsanwaltschaft kann die zur Verletzung verwendeten Geräte beschlagnahmen.

Rechtlich relevant ist auch, dass seit der Urheberrechtsnovelle gemäß § 108 b UrhG auch das Umgehen bzw. das Herstellen von Programmen oder Gerätschaften zur Umgehung verboten ist.

4.3.13 Weitere Regelungen

Die bis hier dargelegten gesetzlichen Regelungen vermitteln die Grundbegriffe, die zu einer genaueren Wertung der Situation um DRM und die Informationsgesellschaft benötigt werden. Das Urheberrecht enthält noch einige weitergehende Regelungen, die sich allerdings alle mit für diese Arbeit nicht relevanten Themengebieten befassen. Zum

[115] Wobei die bloße Existenz von Materialien, die zu einer Verletzung taugen, selbstverständlich nicht ausreicht. Sonst würde hierunter bereits der Besitz eines CD-Brenners fallen, und ein Großteil der deutschen Computerbesitzer wäre zu Unrecht kriminalisiert.
[116] Mit der Ausnahme der Bejahung des öffentlichen Interesses, was bei privaten Urheberrechtsverletzungen wie bspw. den Jugendlichen Raubkopierern selten gegeben sein wird.

Beispiel die Regelungen über die Zwangsvollstreckung von Urheberrecht oder auch einen Anhang, der die pauschale Vergütung genauer regelt.

Doch soll der Überblick über das deutsche Urheberrecht nun mit einigen Rechtsfiguren außerhalb des deutschen Rechts, sowie einem Überblick über die Zukunft des Urheberrechts abgeschlossen werden.

4.4 Relevante Rechtsfiguren aus dem Ausland

Nachdem das deutsche Urheberrecht ausführlich dargelegt wurde, sollen ergänzend einige ausländische Rechtsfiguren betrachtet werden. Diese im folgenden beschriebenen Figuren kommen aus dem amerikanische Copyright law, welches sich vom deutschen, dem „droit d'auteur" verwandten Recht besonders in seiner Beziehung zwischen Werk und Autor unterscheidet.

„First Sale"-Doktrin

Während in §26 UrhG eine Beteiligung des Urhebers eines Werkes der bildenden Kunst am Weiterverkauf desselben in Höhe von 5 Prozent vorgesehen ist, hält das amerikanische Copyright am Grundsatz fest, dass sich die Rechte des Künstlers mit dem ersten Verkauf[117] erschöpfen. Das Werk darf beliebig oft ohne Zustimmung des Urhebers weiterverkauft werden[118]. Welche Relevanz das hat sehen wir am Beispiel der sog. OEM-Software von Microsoft. Microsoft lieferte günstigere Programmversionen seines Betriebssystems aus, unter dem Vorbehalt, dass weitere Händler diese nur zusammen mit einem neuen Computer vertreiben dürfen. Diese Praxis wurde allerdings in Deutschland vom Bundesgerichtshof 2001[119] für nicht wirksam erklärt, da der Weiterverkauf ohne Bindung an ein neues System nicht gegen geltendes Recht verstößt. Auch durch Verträge, welche vom Nutzer mittels Aufreißen einer Verpackung oder durch einen Mausklick geschlossen wurden versuchte man, sich weitergehende Rechte am Weiterverkauf zu sichern oder Lizenzen für die Verwendung einzuschränken. Doch auch diese Praktiken erwiesen sich als nicht rechtens.

„Public Domain"

Einen Schritt in Richtung der Verkürzung der Schutzdauer geht diese Rechtsfigur. Sie besagt, dass ein Werk, sofern es nach dem 1. Januar 1978 entstanden ist, und zudem älter als 70 Jahre ist, gemeinfrei wird, und man somit das Werk ohne Zustimmung des Urhebers genutzt werden kann.

[117] Daher der Name „First Sale"-Doktrin
[118] selbstverständlich gilt dies nicht für eine vom Verkäufer erstellte Kopie
[119] Aktenzeichen: I ZR 244/97

„Fair Use“[120]

Der sog. Fair Use ist die einzige und daher auch am meisten zitierte Ausnahme des Copyright law. Er ist in der Wirkung mit der deutschen Privatkopie vergleichbar, hat aber einen eigenen Hintergrund: Als Lizenzverhandlungen noch nicht so hochgradig automatisierbar waren, wie sie es beispielsweise durch Agentensysteme oder auch nur durch Rechtsvergabe-Servern eines DRMS im Internet heute sind, war der Fair Use als Abschwächung des Monopols der Urheber gedacht, da durch unökonomisch hohe Transaktionskosten es nicht in jedem Falle zu einer legalen Lizenzvergabe kommen konnte. Nach dem Prinzip des „Fair Use“ war eine Kopie immer dann erlaubt, falls die Transaktionskosten den Wert der Transaktion selbst überstiegen. Problematisch ist nach dieser Definition allerdings, dass die meisten Nutzer es nicht verstehen, warum etwas ursprünglich Erlaubtes nun nicht mehr erlaubt sein sollte. Ein Merkmal des Fair Use ist zudem auch seine vertragliche Abbedingbarkeit.

4.5 Urheberrechtsnovelle

Nach langem Ringen und mit einiger Verspätung[121] wurde schließlich die InfoSoc-Richtlinie in geltendes deutsches Recht unter dem Namen „Gesetz zur Regelung des Urheberrechts in der Informations-gesellschaft“ integriert. Es trat am mit der Verkündung im Bundesgesetzblatt am 13. September 2003 in Kraft in Kraft. Dabei wurde bis auf einige kleine Abweichungen der Regelungsumfang der Richtlinie übernommen. So wurde beispielsweise das Recht auf Privatkopie nicht in die Ausnahmeregelung des § 95b UrhG integriert, was die InfoSoc-Richtlinie aber ausdrücklich gestattet. Siehe dazu auch das Kapitel über die Arbeitsgruppe "Privatkopie".

4.5.1 Inhalt der Novelle

Da in Kapitel 4.3 das Urheberrecht bereits in novellierter Form präsentiert wurde, soll der nun folgende Abschnitt über die Veränderungen kurz gehalten werden. Die Veränderungen folgen der InfoSoc-Richtlinie welche bis zum 31.12.2002 umzusetzen war. Durch die Verspätung wurden alle von der EU nicht zwingend geforderten Punkte in den zweiten Korb verschoben. Die Änderung des Urheberrechts nennt sich offiziell: „Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft“[122]. In dem entsprechenden Bundesgesetzblatt findet sich auch eine vollständige

[120] Auf deutsch etwa: „angemessene Nutzung“
[121] Die ursprüngliche Umsetzungsfrist endete 18 Monate nach Veröffentlichung der Richtlinie, d.h. am 31.12.2002.
[122] siehe auch [20]

Auflistung der einzelnen Änderungen, weshalb hier nur die wichtigsten erwähnt werden sollen.

19 a UrhG

So wurde beispielsweise § 19 a UrhG eingefügt, der das Recht auf öffentliche Zugänglichmachung beschreibt. Damit wurde der veränderten Situation Rechnung getragen, die das Internet mit sich bringt im Vergleich zu bspw. Funksendungen. Während letztere nur zum Zeitpunkt des Sendens empfangen werden können, versetzt das Internet bei einem Download die Öffentlichkeit in die Lage, Zeit und Ort des Empfangs selbst zu wählen. Dieses neue Verwertungsrecht wurde konsistent im weiteren Verlauf des Urheberrechts, wo nötig, eingefügt.

Des weiteren wurden diverse Schranken angepasst. So sorgten zum Beispiel die Privatkopie in § 53 UrhG sowie die öffentliche Zugänglichmachung für Unterricht und Forschung in § 52 a UrhG für viel Wirbel. Gegen erstere wehrten sich u.a. die Produzenten von Musik, da sie ihre Rechte an dem Content durch den blühenden Tauschhandel mit Raubkopien gefährdet sehen. Das neu hinzugenommene Verbot der Privatkopie von einer rechtswidrig hergestellten Quelle reicht ihnen nicht. Gegen § 52 a UrhG liefen vor allem wissenschaftliche Verlage Sturm, da die Schranke nach ihrer Meinung direkt in ihr Hauptgeschäft eingreife.

Ein neuer Block gegen Raubkopien findet sich in den Zusatzbestimmungen für die Informationsgesellschaft in den §§ 95 a – d UrhG. Hier wird vor allem den verschiedenen Varianten von Kopierschutzmaßnahmen Rechnung getragen, die das Urheberrecht in dieser Form bis dato nicht kannte. Diese Maßnahmen werden unter Schutz gestellt, gleichzeitig werden ihnen Grenzen auferlegt, die sich in durchsetzungsfähigen Schranken niederschlagen. Dazu kommt noch eine Kennzeichnungspflicht, sowie der für DRM essentielle Schutz von Metainformationen.

Durch das Verbot der Umgehung von TPM kommt natürlich auch noch eine gesetzliche Grundlage hinzu, die den entsprechenden Tatbestand sanktioniert. Sie findet sich in § 108 b UrhG

4.5.2 Stand des zweiten Korbes

Nach der Veröffentlichung der Urheberrechtsnovelle wurde am 16. September 2003 die Arbeit am zweiten Korb des Urheberrechts durch die Bundes-Justizministerin Brigitte Zypries eröffnet. Zur Vorbereitung der Arbeiten gab es vom BMJ (Bundesministerium für Justiz) einen Fragebogen[123] mit themenbezogenen Fragestellungen. Vom September 2003 bis zum Juni 2004 arbeiteten nun elf

[123] siehe auch [21]

Arbeitsgruppen (AG) bestehend aus Experten verschiedener „Fronten“ an Vorschlägen für den zweiten Korb. Die Ergebnisse zu den jeweiligen Themen wurden in einem Dokument[124] veröffentlicht. Im folgenden soll ein Überblick über die einzelnen Arbeitsgruppen, ihre jeweilige Aufgabe und ihre Ergebnisse in Kurzform gegeben werden. Etwas umfangreichere Informationen finden sich in oben genannten Dokument des BMJ. Im Kapitel „Rechtliche Möglichkeiten des Staates“ werden dann einzelne Vorschläge der Arbeitsgruppen aus Sicht des Autors bewertet und eigene Vorschläge dargelegt, sofern die Bereiche für das in dieser Arbeit behandelte Thema relevant ist.

4.5.2.1. Arbeitsgruppe “54“

Diese Arbeitsgruppe bekommt ihren Namen durch die Paragrafen mit denen sie sich beschäftigt hat: § 54 ff UrhG. Darin geht es um das Pauschalvergütungssystem, welches die AG reformieren sollte. Bisher waren diese Abgaben als Vergütung für die Inanspruchnahme von Kopien, die durch vergütungspflichtige Schrankenregelungen gestattet waren, hauptsächlich der Privatkopie gedacht. Durch die neue digitale Technik hat sich die Lage aber drastisch verändert. Sowohl die Verfahren zur Erhebung der Kompensation, als auch die Höhe der Kompensation können erneuert werden. Unter anderem durch die verlustlose Kopie und die geringe Größe von digitalen Daten im Vergleich zu analogen Kopien entsteht hier Handlungsbedarf. Hauptaugenmerk der AG lag unterschwellig auf der Frage, ob ein solches System noch angemessen ist, und falls ja, wie eine solche Anpassung vorgenommen werden kann, da die zugehörigen Paragrafen seit 1985 unverändert sind, was ein völliges Fehlen der Informationstechnik impliziert. Auch beschäftigte sich die AG mit der Frage, wofür überhaupt eine Vergütung erhoben werden soll.

Fazit

Wie erwartet gab es keinerlei Probleme bei der Einigung, dass ein Pauschalvergütungssystem immer noch sachdienlich ist, und daher in überarbeiteter Form fortbestehen soll. Die Rahmenbedingungen sollen vom Gesetzgeber konkretisiert werden und die Vergütungshöhe durch eine Einigung zwischen den beteiligten Parteien.

Weniger Einigung gab es beim zweiten Punkt: So beschloss man zwar einstimmig, dass die Pauschalabgaben je nach Eignung des Gerätes zur Vervielfältigung anfallen sollen und deren Höhe durch die tatsächliche Nutzung zur Vervielfältigung festgelegt wird, doch bei der Frage der Hinzunahme der Reprografie (nach § 54a UrhG) und Leermedien zur Pauschalabgabenpflicht, beharrten die jeweiligen Lobbies auf ihren antagonistischen Standpunkten.

[124] siehe auch [1]

Bei der Bemessung der Höhe der Abgaben gab es kaum eine Einigung. Neben dem Beschluss die tatsächliche, urheberrechtlich relevante Nutzung als Faktor für die Höhe zu nehmen, konnte man sich weder auf weitere Faktoren verständigen, sowie ob eine prozentuale oder fixe Pauschale verwendet werden soll. Auch wurden teils gesetzliche Richtlinien zur Orientierung für die Höhe der Abgaben befürwortet. Nur bei dem verwendeten Verfahren zur Herbeiführung einer Einigung war man sich einig. So erhielt das Modell mit einer kompetenten zivilrechtlichen Schlichtungsstelle den eindeutigen Vorzug gegenüber dem an das Verwaltungsrecht angelehnten Modell. Dabei war das Votum klar für eine Entscheidungsinstanz. Zur Anlage über die Höhe der Vergütungssätze, die dem § 54 d UrhG beigeordneten ist, waren die Meinungen recht differenziert und stimmten vornehmlich in dem Wunsch überein, die Anlage beizubehalten und fortzuschreiben.

4.5.2.2. Arbeitsgruppe “Privatkopie“

Diese Arbeitsgruppe widmet sich dem wohl am erbittertst umkämpften Thema der gesamten Urheberrechtsnovelle: Der Privatkopie. Die Meinungen gehen ins Extreme. Während es für die einen dem Grundrecht auf Information gleichkommt, sich Daten kostenfrei [125]zu privaten Zwecken zu kopieren, ist es für die anderen blanker Diebstahl. Die hauptsächliche Aufgabenstellung dieser Arbeitsgruppe bezog sich auf die Entscheidung, ob die Privatkopie in das Umgehungsrecht technischer Schutzmaßnahmen nach § 95 b UrhG integriert werden soll, was die Richtlinie zulässt, oder ob sie daraus exkludiert wird.

Fazit

Zur Vorbereitung dieser Frage wurde zunächst der gewünschte spätere Schrankenumfang der Privatkopie erläutert. Dazu traf man eine nach Meinung des Autor sehr sinnvolle Unterscheidung der betroffenen Daten in drei Teilgebiete: Musik, Printmedien und Film.

Im Bereich Musik gab es bereits verschiedenste Ansichten und man kam erwartungsgemäß nicht zu einer Einigung. So wurde einerseits von der Musikindustrie das Verbot der digitalen Privatkopie bei gleichzeitigem Verzicht auf Pauschalabgaben vorgeschlagen. Andererseits wurde von Verbraucherseite eine Gestattung der digitalen Privatkopie gefordert. Andere Vorschläge, wie die Einschränkung der digitalen Privatkopie bzgl. Zeit, Menge oder Quelle wurden zumindest von den Vertretern der Industrie als Verbesserung angesehen, fanden allerdings keine breite Zustimmung. Ähnlich ging es dem Vorschlag, die aktuelle Situation beizubehalten, und lediglich bewusst auf die

[125] Laut Gesetz ist es nicht kostenfrei. Eine Tatsache, die sehr gerne übersehen wird.

Durchsetzung dieser Schranke gegen technische Schutzmaßnahmen zu verzichten.

Im Printbereich wurde nur das Verbot der Privatkopie durch dritte gefordert, und dass nur die Erstellung von dem eigenen Original rechtens sei.

Im Filmbereich wurde gegen den Widerstand von öffentlichem und privatem Rundfunk und Fernsehen die Einschränkung der digitalen Privatkopie auf die Zeit nach einem Jahr nach der Kinoverwertung gefordert.

Bei der anschließenden Diskussion um die Durchsetzung der Privatkopie ergab sich demnach auch das volle Spektrum möglicher Meinungen. Neben den beiden antagonistischen Extrempositionen gab es allerdings auch gemäßigte Ansätze. Diese stützen siech, wie bereits weiter oben erwähnt, auf eine Einschränkung entweder der zeitlichen Nutzung, des Verwendungszweckes oder auf eine Limitierung der Durchsetzbarkeit auf das eigene Original. Interessiert diskutiert wurde auch der Ansatz der freiwilligen Selbstkontrolle von Wirtschaft und Markt, wobei man allerdings deren Kompetenz hierfür in Zweifel zog. Es sollte noch die Umsetzung der Privatkopie im Onlinebereich durch eine allgemeine "Internetmaut" erwähnt werden, die allerdings wohl dem geltenden Recht widerspricht und der es zudem an praktischer Einsetzbarkeit mangelt.

4.5.2.3. Arbeitsgruppe “Schranken“

Diese Gruppe hatte die Aufgabe für einige praktische Probleme adäquate Lösungen bezüglich der im Urheberrecht fixierten Schranken zu finden.

So waren die Mitglieder mehrheitlich der Meinung, dass die Entscheidung des BGH[126] betreffs des elektronischen Pressespiegels mit den entsprechenden Einschränkungen zur Klarstellung in das Urheberrecht übernommen werden sollte.

§ 53 Abs. 2 Satz 1 Nr. 2 UrhG wurde als der Regelung der Richtlinie entsprechend erachtet. Somit sollen nur nicht kommerziellen, öffentlichen Einrichtungen das Anlegen elektronischer Archive gestattet werden.

Bei dem Thema "On the spot consultation" in Bibliotheken war man sich über die Notwendigkeit einer Schranke einig, doch erneut nicht über deren Ausgestaltung.

[126] Siehe dazu [23]

Im Zitatrecht konnte man sich einigen, dass die Beschränkung auf bestimmte Werksarten entfallen sollte, doch wurde aufgrund der im Gegensatz zu anderen Schranken bestehenden Vergütungsfreiheit seine restriktivere Anwendung gefordert.

Nach dem Urteil des BGH[127] im Fall des Kopienversands per Telefaxgeräte wurde übereinstimmend festgestellt, dass dieser gesetzlich geregelt werden sollte. Doch erneut fand sich keine Einigung über die genaue Ausprägung der Schranke. Stein des Anstoßes war hier, ob der Versand per Email zulässig sein sollte, wie es das Urteil des BGHs zwar nicht formuliert, so doch indiziert.

Im Fall des bereits in der Praxis verwendeten Drei-Stufen-Tests kam man überein, dass eine explizite Aufnahme in das Urheberrecht nicht notwendig sei, da er bereits geltendes Recht sei.

4.5.2.4. Arbeitsgruppe “31 IV“

Auch diese Arbeitsgruppe hatte einen wichtigen Punkt zu klären: Durch § 31 IV UrhG wurden viele Verlage und andere im urheberrechtlichen Bereich tätige Unternehmen an einer Verwertung ihrer Altbestände gehindert, da eine Kompilation vormals analoger Werke auf einer CD-ROM oder die Vermarktung als eBook als neue Nutzungsarten angesehen werden, an die zur Zeit des Erwerbs der Rechte an den Werken noch nicht zu denken war. Da im Laufe der Zeit viele Inhaber von Urheberrechten durch Erbe oder Umzug nicht mehr aufzufinden waren, wurde es unmöglich die Werke in den neuen Medien zu verwenden. Da dies eine für die Gesellschaft nachteilige Situation ist, ist es wünschenswert, die Verwertung des Altbestands zu ermöglichen. Ziel der Arbeitsgruppe war es zu entscheiden, zum einen über eine Neuregelung des Verbots der Übertragung unbekannter Nutzungsarten und zum anderen, wie mit Altbeständen verfahren werden soll, d.h. sowohl über die bereits angefallenen Archivbestände, wie auch über die zukünftig anfallenden, sofern dies Gesetz im Zuge des zweiten Korbs nicht geändert würde.

Fazit

Betreffs der zukünftigen Regelung war die Arbeitsgruppe sich im Ergebnis zumindest darüber einig, dass der Paragraf nicht ersatzlos gestrichen werden sollte. Eine Generallizenz zur Übertragung aller - insbesondere der unbekannten - Nutzungsarten soll weiterhin nicht möglich werden. Dennoch soll der Paragraf geöffnet werden. Dabei bestand lediglich über das Maß der Öffnung Uneinigkeit, und zwar sowohl bezüglich der Werksarten, wie auch der Fallkonstellationen für die die Öffnung gelten soll. Überwiegend war man für eine Öffnung aller Bereiche und eine angemessene Vergütung für den Urheber bei

[127] siehe dazu [24]

Verwendung eines Werkes im Sinne einer neuen Nutzungsart. Um dem sog. Archivproblem Herr zu werden und die Altbestände zu verwerten, fanden sich zwar mehrere Ideen und Modelle, aber keine allgemein akzeptierte Lösung. Vorgeschlagen wurden:

- Vermutungsregelung
- (Begrenzte) Verwertungsgesellschaftslösung
- Eigenverantwortung des Urhebers
- Rücksichtnahmegebot parallel zu § 8 II UrhG

4.5.2.5. Arbeitsgruppe “Internet“

In der Arbeitsgruppe „Internet“ stand zur Diskussion, ob dem Urheber in Deutschland ein Auskunftsanspruch gegenüber Internet Access Providern zugestanden werden soll. Hintergrund dieser Anregung ist, dass bei momentaner Rechtslage, ein Rechtsinhaber praktisch keine Handhabe gegen Nutzer hat, die seine Rechte via Internet verletzen, da dieser Nutzer nur durch eine anonyme IP repräsentiert wird.

Fazit

Generell stimmten die Teilnehmer dieser Arbeitsgruppe darin überein, dass es den Rechteinhabern ein berechtigtes Anliegen ist, Urheberrechtsverletzungen im Internet nachzugehen. Daher forderten deren Vertreter auch ein entsprechendes Auskunftsrecht. Dieses wurde allerdings sowohl von den Vertretern der Verbraucher, den Providern und den Datenschutzbeauftragten klar abgelehnt. Zum einen wurde der höhere, unverhältnismäßige Verwaltungsaufwand beanstandet, sowie praktische Probleme, zum anderen der voraussichtlich mangelhafte Datenschutz. Von Vertretern der BITKOM wurde noch ein gerichtliches, mehrstufiges System vorgeschlagen, welches allerdings auch keine breite Zustimmung fand.

4.5.2.6. Arbeitsgruppe “Film“

Diese Gruppe beratschlagte über eine Stärkung der urheberrechtlichen Position von Filmproduzenten. Dies ergab sich aus der starken Einschränkung, die die Filmindustrie durch nicht mögliche Übertragung unbekannter Nutzungsarten nach § 31 IV UrhG erfährt. Einer der Vorschläge hierzu betraf die Erweiterung der Vermutungsregelung nach den §§ 88, 89 UrhG.

4.5.2.7. Arbeitsgruppe “20b“

Einen für den Onlinebereich nicht sehr relevanten Bereich hatte diese Arbeitsgruppe zu besprechen. Hier ging es um eine Konkretisierung des § 20 b UrhG, der die Vergütung bei Kabelweitersendung durch die Kabelnetzbetreiber regelt.

Fazit

Die Kabelnetzbetreiber argumentieren, dass Ihre rein technische Dienstleistung nicht urheberrechtlich vergütungspflichtig sein kann, und wollen den Wegfall der Vergütungspflicht erreichen. Als Vergleich wird hier die Satellitenweitersendung angeführt. Selbstverständlich sind die Vertreter der Verwertungsgesellschaften von diesem Ziel wenig begeistert, und verweisen zur Unterstützung ihres Standpunktes auf diverse internationale Vereinbarungen, sowie die gängige Rechtssprechung, die die Kabelweitersendung als urheberrechtliche Nutzung sieht. Um zu einer Lösung zu finden, gab es zwei Ansätze: Zum einen sollen die Rechteinhaber zu gemeinsamen Verhandlungen verpflichtet werden, damit für die Kabelgesellschaften der Rechtserwerb transparenter gestaltet wird, und zum anderen dachte man darüber nach das Urhebervertragsrecht und § 20 b UrhG zu verbinden.

4.5.2.8. Arbeitsgruppe “87 IV“

Ebenfalls nur wenig relevant für das hier vorliegende Thema ist die Aufgabenstellung dieser Arbeitsgruppe, die sich mit § 87 IV UrhG zu beschäftigen hatte. Hierbei ging es um eine mögliche Beteiligung der Sendeunternehmen an der Leermedienpauschalvergütung, die man aus dem den Unternehmen zustehenden Leistungsschutzrechtes folgern könnte. Es gab allerdings keine Annäherung, da beide Parteien auf Ihren Standpunkten beharrten, die sie aus ihrer jeweiligen Sicht auch gut belegen konnten: So sahen die Gegner einer Beteiligung das Bundesverfassungsgericht auf ihrer Seite, welches die Nichtbeteiligung der Sendeunternehmen für rechtmäßig erklärt hatte, sowie dass die Sendeunternehmen bereits aus ihrer Filmherstellerleistung eine Vergütung erhielten. Die Sendeunternehmen hingegen argumentierten, dass die 1965 und 1985 angeführte Gründe nunmehr entfallen seien und so eine Vergütung nun angemessen wäre.

4.5.2.9. Arbeitsgruppe “Ausstellung“

Auch diese Arbeitsgruppe beschäftigt sich mit einer neuen Form der Pauschalvergütung. In diesem Fall geht es um Ausstellungen und einem Vergütungsanspruch der Künstler.

Fazit

Diskutiert wurde vor allem, welche Auswirkung ein solcher Anspruch auf Ausstellungen in Deutschland haben würde, da es sicherlich nicht wünschenswert wäre, dass weniger Ausstellungen auf deutschem Boden ausgerichtet würden.

Wie zu erwarten gab es hier ebenfalls keine abschließende Einigung, da die Vertreter der Künstler im Gegensatz zu den Ausstellern eine solche Vergütung forderten. Ihrer Argumentation nach stünden bildende Künstler zur Zeit schlechter als Komponisten und Autoren. Die

Verwaltung der Gelder könnte über die bereits existente VG Bild Kunst erfolgen.

Die Contra-Argumente bezogen sich hauptsächlich auf den negativen Effekt auf die Ausstellungstätigkeit, das Problem, dass hauptsächlich etablierte Künstler die Gelder erhielten und letztlich, dass die Hauptverwertung bildlicher Werke durch den Verkauf geschehen würde und nicht durch eine Aufführung, wie es bei Autoren und Komponisten der Fall sei. Auch gab es bereits einen Feldversuch in Österreich, welcher als misslungen wieder eingestellt wurde.

4.5.2.10. Arbeitsgruppe “27“

Auch diese Arbeitsgruppe erhält ihren Namen aus dem zu bearbeitenden Paragrafen: In Bezug auf § 27 UrhG wurde die Gleichbehandlung aller Medien in Hinsicht auf den Vergütungsanspruch bei Vermietung und Verleih diskutiert und auch ob eine Ausweitung der Vergütung auf weitere Leistungsschutzberechtigte (speziell auf Filmproduzenten) erfolgen soll. Letzteres wurde ob des Nichterscheinens der Opposition, namentlich der Filmindustrie, geschlossen abgelehnt. Die Frage bezüglich der Gleichbehandlung konnte nicht abschließend geklärt werden.

4.5.2.11. Arbeitsgruppe “Goethe“

Hinter dem nicht allzu aussagekräftigem Namen der Arbeitsgruppe „Goethe“ verbirgt sich der Ansatz gemeinfreie Werke mit einer Abgabe zu belegen, um so junge, aufstrebende Künstler zu unterstützen. Diese Abgabe wurde auch unter Namen Künstlergemeinschaftsrecht oder populärer „Goethegroschen“ bekannt.

Fazit

Auch hier gab es keine Einigung. Selbstverständlich befürworteten die Künstler die Schaffung des besagten Rechts. Ziel sei es, eine Art „Generationenvertrag“ zu etablieren, durch den renommierte und etablierte Künstler junge, nachrückende unterstützen. Gegen den Vorschlag gab es Bedenken unterschiedlichster Art seitens der verschiedenen teilnehmenden Interessenvertreter. Diese reichen von verfassungsrechtlichen über europarechtlichen bis hin zu praktischen Problemen. Daneben gab es kompetenzrechtliche Zweifel, die durch die Länder angemeldet wurden.

4.5.2.12. Nachbetrachtung der Ergebnisse

Von diesen elf Arbeitsgruppen sind nur sechs für diese Arbeit interessant, weshalb nur diese in den noch folgenden Kapiteln

herangezogen werden. Namentlich sind die sechs relevanten Arbeitsgruppen die folgenden:

- AG „54“
- AG „Privatkopie“
- AG „Schranken“
- AG „31 IV“
- AG „Internet“ und mit Abstrichen
- AG „Goethe“

Bis auf die letztgenannte Arbeitsgruppe sind die verschiedenen in einem großen Kontext zu sehen, ihre Ergebnisse insofern voneinander abhängen, dass es einen Handlungsspielraum gibt, der es erlaubt einen Ausgleich für nahezu jede spezielle Regelung zu finden, die eine einzelne Gruppe beschließt. Diese Situation wird noch genauer im Kapitel „Rechtliche Anpassungen des Staates“ zu behandeln sein.

4.5.2.13. Papier der Bundesregierung zum zweiten Korb

Ganz aktuell wurde nun auch durch die Bundesregierung am 9. September 2004 eine vorläufige Stellungnahme zum wahrscheinlichen Aussehen des zweiten Korbes mit dem Titel „Urheberrecht in der Wissensgesellschaft – ein gerechter Ausgleich zwischen Kreativen, Wirtschaft und den Verbrauchern“[128] veröffentlicht. Darin wurden einige Eckpunkte des zweiten Korbs umrissen:

- Erhalt der Privatkopie

  Die Privatkopie im digitalen Bereich wird erhalten bleiben. Lediglich der bereits beanstandete Passus „rechtswidrig hergestellte Kopien“, der das Herunterladen von Daten aus Tauchbörsen eigentlich nicht verbietet, wird umgewandelt. Eine legale Quelle darf nun auch keine rechtswidrig *genutzte* Quelle sein.
- Keine Durchsetzung der Privatkopie

  In diesem Punkt wird die bestehende Regel wohl gültig bleiben. Eine technische Schutzmaßnahme behält ihre Wirkung. Die Privatkopie findet keine Aufnahme in den § 95 b UrhG.
- Kompensation der Privatkopie durch Pauschalvergütung

  Der wesentliche Punkt hierbei ist das Nebeneinander von Kopierschutzmechanismen und Pauschalvergütung von Geräten und Leermedien die für Privatkopien genutzt werden. Dieses Gleichgewicht soll sich dynamisch verschieben, eine negative Korrelation zwischen der Höhe der Vergütung und dem Ausmaß des Kopierschutzes.

[128] siehe auch [25]

- Höhe der Pauschalvergütung

  Im Gegensatz zum jetzigen Recht soll in der kommenden Neufassung nicht mehr die Bestimmung eines Gerätes für Kopien relevant sein, sondern der tatsächliche Umfang der Nutzung für Kopien. Außerdem wird ein angemessenes Verhältnis zwischen Preis des Produktes und der Pauschalabgabe zugesichert. Auch das Verfahren zur Bestimmung der Höhe der Pauschalabgaben wird sich ändern. Aus einer Festlegung durch den Gesetzgeber wird ein Verfahren zwischen den beteiligten Parteien selbst.

- Lösung des Archivproblems

  Zum einen wird für die Zukunft die Regelung eingeführt, dass auch unbekannte Nutzungsarten vergeben werden können. Bei der Verwertung erhält der Urheber eine besondere Vergütung, sowie ein Vetorecht, das er bis zum Beginn der Verwertung einsetzen kann.

  Zum anderen wird für die Verwendung vorhandener Archive wohl die folgende Regelung getroffen: Da die Öffnung der Altbestände im Interesse der Allgemeinheit ist, wird eine Verwertung erlaubt. Dem Urheber wird parallel zur zukünftigen Regelung ein Vetorecht eingeräumt, von welchem er bis ein Jahr nach in Kraft treten des Gesetzes Gebrauch machen kann, und er erhält eine angemessene Vergütung.

- Übertragung unbekannter Nutzungsarten im Filmbereich

  Um für eine Rechtssicherheit bei Filmproduzenten zu sorgen wird in diesem Bereich eine Vermutungsregelung hergestellt, die eine Übertragung aller zweckgebundenen Rechte auch unbekannte Nutzungsarten betreffend an den Filmproduzenten vorsieht.

- Elektronische Leseplätze in Bibliotheken

  Zur Stärkung des Wissenschaftsstandortes Deutschland wird den Bibliotheken das Anbieten von Schriftstücken auf elektronischen Arbeitsplätzen gestattet, sowie der Versand von Artikeln und Ausschnitten aus Werken in elektronischer Form, sofern die Verlage nicht bereits für ein entsprechendes Angebot sorgen.

5 Grundlegende technische Maßnahmen

Dieses Kapitel soll einen Einblick in Erfolg versprechende Maßnahmen zum technischen Schutz des geistigen Eigentums anbieten. Diese werden allerdings erst in einem späteren Kapitel in den rechten Kontext gesetzt. Zunächst wird der Vorteil von Metadatensprachen respektive Metadaten selbst erläutert, gefolgt von Wasserzeichen welche es erlauben besagte Metadaten nahezu untrennbar mit (auch analogen) Daten zu verknüpfen.

Als Ansatz wird die Idee des geschlossenen Systems thematisiert, welches nur zertifizierte Programme erlaubt, und somit einen Missbrauch von Nutzerseite, nicht jedoch von Herstellerseite, ausschließen könnte. Das genaue Gegenteil dieser geschlossenen Systeme sind die durch die Open Source-Gemeinde entwickelten Werke. Diese sind zwar einerseits sehr positiv für den Fortschritt in der Computerwelt, andererseits bringen sie aber auch einen unkontrollierbaren Faktor in den Markt ein.

Im dritten Teil des Kapitels werden Grundlagen aus der Kryptografie vorgestellt, da die zum genaueren Verständnis des zu schaffenden Systems notwendig sind. Darunter fallen auch Public Key Infrastrukturen, Systeme die es erlauben ohne hohen Aufwand sich in Domänen dauerhaft zu authentifizieren.

5.1 Metadatensprachen

Ohne auf die genauere Verwendung eingehen zu wollen, soll angemerkt werden, dass Metadatensprachen ihren Hauptzweck in Kombination mit DRMS entfalten können, da sie Metainformationen standardisieren und maschinenverarbeitbar machen. Das Format der Metadatensprachen spielt eine wesentlich geringere Rollen, als die Tatsache, dass sie unverändert bleiben müssen, um von Wert zu sein. Zumeist bauen sie auf XML oder einem anderen SGML-Derivat auf. Sie legen in sog. „Tags“[129] die Nutzungsrechte für den jeweiligen Content fest.

Diese Metadatensprachen können eine Vielzahl verschiedener Codierungen beinhalten. Dabei sind nur der Fantasie des Lizenzgebers Grenzen gesetzt. So kann die Zahl der Benutzungen, ein zeitliches Intervall oder die Erlaubnis bestimmte Bearbeitungsschritte vornehmen zu dürfen mittels den Metainformationen an den entsprechenden Content gebunden werden.

[129] Tags sind Kommandos, die einer verarbeitenden Software Anweisungen für das Verfahren mit den dazwischen stehenden Inhalten geben.

Im Gegensatz zu analogen Daten bringt die direkte Integration der Erlaubnis etwas zu tun den Vorteil der Untrennbarkeit mit sich. Zumindest wenn Metadaten richtig, d.h. im DRM-Kontext angewendet werden. So wäre es beispielsweise ideal, wenn ein Buch sich weigern würde, sich kopieren zu lassen, wenn dies verboten ist. Mit DRM-geschützten Daten lässt sich dies erreichen.

5.2 Wasserzeichen

Ein inzwischen nicht mehr wegzudenkendes Mittel im Bereich des DRM sind die Wasserzeichen. Bei ihnen handelt es sich um eine für den menschlichen Nutzer unsichtbare Form Metadaten in Content zu integrieren. Dies geschieht je nach Beschaffenheit des Contents auf verschiedenste Art. Damit handelt es sich auch nicht mehr um eigentliche Wasserzeichen im analogen Sinn. Sie müssen wie erwähnt unsichtbar sein, da sie sonst den Gebrauch eines Werkes einschränken können. Doch sie dürfen für den Computer nicht zu unauffällig sein, d.h. sie müssen maschinenlesbar bleiben. Doch der wichtigste Punkt ist die Robustheit. Sie müssen gegen die gängigsten Transformationen immun sein. Darunter fällt die verlustbehaftete Kompression (MP3, JPG), die Unabhängigkeit von durch den Nutzer einfach veränderbaren Bezugsgrößen[130], Skalierung, Vergrößerung oder Beschneidung des Inhalts, sowie die nachfolgend aufgeführten Attacken. Ferner inkludiert die Anforderung der Robustheit auch die Nichtnachahmbarkeit bzw. Unveränderbarkeit der Metadaten. Und nicht zuletzt darf der Prozess der Implementierung nicht zu komplex werden, da sonst die Integration der Wasserzeichen auf Grund der in der Praxis anfallenden Masse unmöglich wird. Dies umfasst auch, dass nur eine geringe Datenmenge zusätzlich für das Wasserzeichen benötigt wird. Zusammenfassend ergeben sich nun diese vier Punkte, um die Qualität eines Wasserzeichens zu bestimmen:

- Wahrnehmbarkeit
- Maschinenlesbarkeit
- Robustheit
- Komplexität der Integration

Alle diese Punkte sind kritisch für die Verwendung von Wasserzeichen in DRMS, da wie der gängige Satz „Jede Kette ist so stark, wie ihr

[130] Bei Bildern: Kontrast, Farbpalette usw.; bei Musik: Grundlautstärkepegel, Hz-Zahl; Kanäle; Stereo/ Mono usw.; bei Schriftstücken: Formatierung usw.; bei Videos: Tonspuren, Kombination Ton-Bild usw. und schließlich bei Programmen: Installationspfad, Batchdateien, usw.

schwächstes Glied“ bereits impliziert, nur durch Wasserzeichen integrierte Metadaten die analoge Lücke[131] passieren.

Im Folgenden werden drei verschiedene Ausprägungen der Verwendung von Wasserzeichen im Umfeld von DRM beleuchtet, danach ein Beispiel für ein mögliches Wasserzeichen gegeben, und drei spezielle Angriffsarten auf dieses Wasserzeichen erläutert, sowie mögliche Wege diese Angriffe zu verhindern.

5.2.1 Verwendungsarten

5.2.1.1. Tracking bzw. Fingerprinting

Wenn illegale Kopien im Internet auftauchen, wäre es für die Rechteinhaber von großem Interesse (auch zwecks einer eventuellen Schadensersatzklage) den Verursacher dieser Kopie zu kennen. Um diesen aufzuspüren, können seine Nutzer-ID oder auch seine personenrelevanten Informationen in den Content aufgenommen werden. Dies scheint natürlich auch ein datenschutzrechtliches Problem mit sich zu bringen.

Doch genau im Bereich des Datenschutzes dürfte diese Verquickung unbedenklich sein, da die Daten vertragsgemäß nur zur Nutzung für Lizenznehmer bestimmt sind. Und dieser hat im Normalfall nicht das Recht den Content zu distribuieren, womit die persönlichen Daten eigentlich nicht in falsche Hände gelangen können. Zusätzlich muss allerdings noch gewährleistet werden, dass das Wasserzeichen zwar von Dritten verifiziert werden kann, jedoch nicht extrahiert, was gleichbedeutend mit „freien, ungebundenen Daten“ wäre. Ebenso darf der Prozess des Hinzufügens von Wasserzeichen für dritte nicht nachahmbar sein, da sonst existierende Wasserzeichen überschrieben werden könnten[132].

Beachtet werden sollte noch die unfreiwillige Verbreitung des Lizenznehmers. Sofern dieser sich nicht der Fahrlässigkeit schuldig gemacht hat, muss er die Möglichkeit besitzen sich zu exkulpieren. Ein Wasserzeichen bietet somit natürlich keine endgültige Sicherheit den Verursacher zu finden, doch gibt es immerhin die Chance dazu.

[131] Als analoge Lücke bezeichnet man die analoge Phase bei eine DAD-Wandlung. Siehe dazu auch Kapitel 7.6 „DAD-Wandlung“

[132] Beispielsweise durch eine Nullfolge oder einer inversen Folge, womit das Wasserzeichen gelöscht werden könnte.

5.2.1.2. Copied-Flag

Manche Wasserzeichen beinhalten neben den persönlichen Informationen des Nutzers auch noch bestimmte Datenbits, sog. Flags. Diese zeigen einem „eingeweihten“ Abspielprogramm an, dass die Daten nicht aus einem Original-Container stammen, sondern bereits einmal kopiert wurden, und zwar nach dem Abspielprogramm, welches dieses Bit setzt. Damit würde das Programm ein erneutes Abspielen oder Weitergeben des nun illegalen Contents verbieten. Außerdem würde dieses Bit auch die analoge Lücke überqueren, und so die redigitalisierten Daten im Idealfall ebenfalls unkopierbar machen.

5.2.1.3. Kennzeichnung für Suchprogramme

Eine weitere Möglichkeit, die sich vor allem für digitale Bilddateien empfiehlt, ist die Möglichkeit, bildlich gesprochen, eine Alarmflagge zu hissen. Das bedeutet, dass automatische Suchmaschinen im Auftrag des Urhebers oder des Rechteinhabers das Internet durchforsten, stets auf der Suche nach Dateien, die das angesprochene Wasserzeichen tragen. Von diesen wird die Lokation notiert, und anschließend nachgeprüft, ob durch die Veröffentlichung im Internet eine Rechtsverletzung besteht, was wohl in den meisten Fällen zu bejahen ist. Einer der ersten Nutzer dieser Technik war übrigens das Männermagazin „Playboy“.

5.2.2 Praxis-Beispiel

Logischerweise kann bei unterschiedlichen Content-Arten (siehe Kapitel 7.2 „Datenspezifische Eigenheiten“) nicht immer die gleich Art von Wasserzeichen zum Einsatz kommen. Damit die Metadaten wirklich nicht extrahierbar und zudem auch nicht für den Menschen wahrnehmbar sind, werden sie über winzigste Verschiebungen einzelner Werte[133] in die Daten eingebaut, die einem menschlichen Auge oder Ohr nicht auffallen können. Durch einen Abgleich mit einem nicht bezeichneten Werkstück können diese Differenzen herausgefiltert und interpretiert werden. Bei Bildern wird das Wasserzeichen entweder durch minimale Farbverschiebungen oder Verrückungen der jedem Bild hinterlegbaren Gitterlinien eingefügt. Bei Audiodaten werden die einzelnen Ausschläge der jeweiligen Töne minimalst verändert. In Filmdaten kann eine Kombination aus beiden Systemen zum Einsatz kommen.

[133] Die zu verändernden Werte differieren ebenfalls mit der Art des Content. Beispielsweise kann bei Bilder in bestimmten Pixel Helligkeitsverschiebungen vornehmen, oder im Frequenzgang bei Musikdateien unhörbare Peaks einfügen.

Die nachfolgenden Bilder zeigen zunächst ein Original bild, danach das gleiche Bild mit einem inzwischen veralteten[134] Wasserzeichen versehen und schließlich die für das menschliche Auge unsichtbare Differenz zwischen beiden Bildern, die sich aber maschinenlesbar interpretieren lässt. Alle drei Bilder sind von einer Homepage der technischen Universität Berlin[135].

Abbildung 2: Original

Abbildung 3: Original mit Wasserzeichen

Abbildung 4: Differenz

Man sieht kaum einen Unterschied zwischen den obigen Bildern, doch lässt sich die Differenz wiederum schön erkennen. Und die Differenz enthält nun die gewünschten Metadaten. Wie bereits das Alter dieser Beispielbilder vermuten lässt, ist dieses Wasserzeichen noch nicht sehr resistent gegen die verschiedensten Angriffe. Daher sollen drei Attacken auf das Wasserzeichen vorgestellt werden, denen selbst heutige Wasserzeichen kaum gewachsen sind.

[134] DigiMarc aus Corel Draw 8 von 1997
[135] Quelle: [26]

5.2.3 Angriffe

Damit Wasserzeichen einwandfrei funktionieren, dürfen die integrierten Informationen weder teilweise gelöscht, noch verändert, überschrieben oder extrahiert werden. Dazu wird zumeist der Algorithmus der zur Generation verwendet wird, sowie die genaue Form der Metadaten geheim gehalten. Daher sind die am meisten verwendeten Attacken ungerichtet. Bei genauer Kenntnis von Algorithmus usw. wäre die Gefahr der Manipulation ungleich größer. Daher soll dieser Fall, der wohl das größte Problem für ein neues Wasserzeichen wäre, nicht behandelt werden. Die in diesem Kapitel vorgestellten Beispielattacken sind:

- Collusion-Attacke
- Jitter-Attacke
- Mosaic-Attacke

Collusion-Attacke

Eine vergleichsweise einfache Attacke ist die Collusion-Attacke. Hierbei wird einfach ein Mittelwert aus verschiedenen veränderten Dateien gebildet, womit sich die Wasserzeichen vermischen und somit unbrauchbar werden. Bisher hat noch keines diese Attacke in unbeschränkter Form überstanden. Es gibt jedoch bereits Ansätze[136], durch die bis zu einer Menge P an Piraten, die ihre mit ihrer jeweiligen Identität versehenen Kopien durch eine Collusion-Attacke verschmelzen, die IDs aller Beteiligten sichtbar werden. Damit wird diese Attacke ungleich riskanter. Ihre Praxisrelevanz ist momentan noch sehr gering, da für sie mehrere Kopien mit verschiedenen Wasserzeichen vonnöten sind, was entweder bei legalem Kauf mit zusätzlichen Kosten verbunden ist oder bei anderweitiger Beschaffung einen deutlichen zeitlichen Nachteil mit sich bringt. Da zudem die Grenze P, ab der die Collusion-Attacke auch wirklich eine Unkenntlichmachung der Wasserzeichen bewirkt, unbekannt ist und wohl von den Content-Produzenten auch hinreichend hoch gesetzt wird, kann man in der Praxis vom Nichtgebrauch dieser Attacke ausgehen. Sie bleibt allerdings ein Damokles-Schwert über den Köpfen der Content-Produzenten solange sie möglich ist.

Jitter-Attacke

Ebenfalls mit unwahrnehmbaren Veränderungen verschiedener Werte einer Datei arbeitet die Jitter-Attacke. Eine Definition für den Begriff Jitter findet sich in der Wikipedia[137]:

[136] Wenn veränderte Bits in den Wasserzeichen aller P Beteiligten den gleichen Wert haben, kann dieser Wert auch nicht „herausgemittelt“ werden. Durch die Kombination der übrig gebliebenen Bits, kann man alle an der Attacke Beteiligten IDs erkennen.
[137] [27] und weiterführend [28]

> “In telecommunication, jitter is an abrupt and unwanted variation of one or more signal characteristics, such as the interval between successive pulses, the amplitude of successive cycles, or the frequency or phase of successive cycles.“

Diese Variationen der Signale sind bei herkömmlichen Jittern wie oben beschrieben ungewollt. Diese Form der Attacke auf Wasserzeichen erzeugt künstliche Jitter. Ähnlich wie bei der Kompression eines Bildes per JPG-Kompression werden benachbarte Werte übernommen. Durch die hohe Informationsdichte, die die Kapazität des menschlichen Auges oder Ohres bei weitem übersteigt, bleibt die Qualität des Content scheinbar gleich, doch kann sich für das Wasserzeichen alles ändern. Während bei Bildern beispielsweise Farb- oder Helligkeitsparameter geändert werden, werden bei Audiodaten im Frequenzgang Spitzenwerte kopiert, oder in den unhörbaren Bereich verlagert.

Mosaic-Attacke

Die Mosaic-Attacke[138] wiederum bedient hauptsächlich ein spezielles Content-Gebiet: Nämlich das der Bilddateien. Da unter den grundlegenden Anforderungen an ein Wasserzeichen in Bilddateien auch die Problematik zu finden ist, wie ein Wasserzeichen gegen Bildtransformationen zu schützen ist, darf dieses nicht auf einen zu kleinen Teil des Bildes beschränkt werden. Sonst könnt man den relevanten Teil einfach wegschneiden. Die Verbreitung des Wasserzeichens über das ganze Bild wiederum bringt aber eine Verwundbarkeit gegenüber der Beschneidung des Contents mit sich. Um zusätzlich auch den Datenverlust durch das Beschneiden des Bildinhalts zu verhindern, entwickelte sich die Mosaicattacke. Dabei wird das Bild in viele kleine Teile zerlegt, welche jeweils für sich unter der Dateigrößengrenze der Erkennbarkeit für das Wasserzeichen liegt. Ein Visualisierungsprogramm wie bspw. der Browser setzt das Bild wieder zusammen, so dass sich für das Auge des Betrachters kein Unterschied zu dem vollständigen Bild ergibt. Nur automatische Suchprogramme können kein intaktes Wasserzeichen mehr feststellen und somit auch nicht darauf ansprechen. Die einzige Möglichkeit gegen diese Attacke anzugehen bildet eine erhöhte Redundanz des Wasserzeichens in dem Content. Dabei wird allerdings sowohl die Komplexität des Integrationsprozesses als auch die zusätzlichen Datenmenge erhöht. Beides sind unerwünschte Nebeneffekte.

5.2.4 Bewertung

Abschließend zu diesem Unterkapitel ist zu sagen, dass die Möglichkeit Informationen untrennbar und unumkehrbar mit Content zu verbinden der Idealfall für DRMS wäre. Dieser kann in der Praxis aber nicht

[138] vgl. [29]

erreicht werden, da sich ein Wettlauf zwischen Codierern und Codebrechern abspielt, der außerhalb des Marktes abläuft. Keine Technologie für die Integration von Wasserzeichen wird auf die Dauer sicher bleiben.

Ein Fortschritt für die Technologie der Wassereichen ist die vom Fraunhofer-Institut patentierte Container-Technologie[139] für Wasserzeichen. Diese verhindert nämlich das Publik werden des geheimen Algorithmus', sowie des Schlüssels mit dem die Metadaten in eigene Produkte eingebaut werden, da generische Container in einer Vorphase hergestellt werden, in die dann bei Bedarf erst die Daten mit geringem Rechenaufwand und ohne Verwendung des Algorithmus' eingebunden werden. Dieses Verfahren eignet sich besonders für gleichartige Daten, die für eine große Masse verschiedener Nutzer personalisiert werden sollen, also auch für DRMS.

5.3 Geschlossene Systeme – totale Kontrolle

Das Problem, was sich bei der illegalen Verwendung von Daten ergibt, scheint untrennbar mit der Verwendung selbst geschriebener Programme verbunden, die das Knacken von Schutzmechanismen oder aushebeln von Wasserzeichen zum Ziel haben. Nach dem neuen Urheberrecht ist nun der Vertrieb, die Verwendung usw. solcher Programme verboten, woran sich allerdings kaum jemand im privaten Bereich stört. Daher kam zwangsläufig die Idee auf, in wie weit es möglich ist, die gesamte Anwendung solcher Programme zu unterbinden. Notwendig hierfür wäre ein sog. geschlossenes System. Einer der ersten Ansätze in diese Richtung lieferte Microsoft mit dem Palladium.

Ein kleiner Chip auf der Hauptplatine eines Computers soll sicherstellen, dass nur lizenzierte Hardware oder Software (ohne unerwünschte Nebenfunktionen) im Computer funktioniert. Sofern auch nur eine nicht lizenzierte Komponente enthalten ist, wird das gesamte System nicht als integer gewertet, und Abspielprogramme, die für ein solches System gedacht sind, versagen ihren Dienst. Ebenso wird Content nicht aus seiner verschlüsselten Form extrahiert, was für die Verarbeitung durch den Computer und Wahrnehmung durch den Nutzer ja notwendig ist.

Nun scheint diese Konstruktion für Content-Produzenten urheberrechtlich gesehen der Stein der Weisen. Rein aus der Sicht der Urheber hat man dies auch. Doch schießt man dabei bildlich gesprochen mit Kanonen auf Mücken, nicht einmal auf Spatzen. In so einem Modell verliert der Nutzer nämlich die vollständige Kontrolle über

[139] siehe auch [30]

seinen Computer. Er wird davon abhängig, welche Programme eine Lizenz für das geschlossene System erhalten.

Eine Kontrolle über die Lizenzierung würde demnach eine vollständige Kontrolle über die durch den Benutzer zu verwendenden Programme und somit einen Wegfall seiner Entscheidungsfreiheit bedeuten. Verständlich ist, dass sich Nutzer diese Beschneidung ihrer Mündigkeit nicht gefallen lassen wollen, weshalb das genannte System bis dato noch einer Verwirklichung harrt.

Ein besonderer Gegner von geschlossenen Systemen ist die im Folgenden behandelte Open Source-Gemeinde. Schließlich hätten die durch sie hergestellten Programme kaum eine Chance auf ein Lizenzierungsverfahren und wären somit außen vor, was die Verwendung durch den normalen Nutzer angeht. Doch geht gerade von dieser Gemeinde auch eine besondere Gefahr aus.

5.4 Open Source[140]-Bereich – totale Freiheit

Eine sehr große Gefahr für die Rechteinhaber stellt trotz des normalerweise fehlenden maliziösen Interesses die Open Source-Gemeinde dar. Hierunter versteht man Programme deren Quelltext offen liegt, und an dem so viele verschiedene Programmierer zum Wohle aller Beteiligten der Gemeinde arbeiten können. Zudem muss eine freie Distribution (ent- oder unentgeltlich) der Programme ermöglich werden. Eine der bekanntesten Lizenzen in diesem Bereich ist die sog. GNU[141] General Public License[142] (GPL). Darin wird vorgesehen, dass jedem Interessenten der Quellcode mit angemessenen Aufwand zugänglich gemacht wird, sofern man sich für die Distribution entscheidet. Der Quellcode darf nicht absichtlich verkompliziert werden. Der Anwender gibt mit dem Programm alle Rechte weiter, die man selbst auch daran hat. Keine Gruppe darf diskriminiert werden. Der Quellcode darf beliebig modifiziert werden. Und man darf nicht verhindern, dass andere die Software weitergeben. Der Kernpunkt dieser Lizenz besagt, dass der Vertrieb frei, aber nicht unbedingt kostenlos ist. Eine Tatsache die häufig übersehen wird.

Prinzipiell berühren sich die Bereiche DRM und Open Source nur am Rande, doch impliziert Open Source zumeist sehr saubere Programmierarbeit ohne versteckte Programme, die vom Anwender

[140] Eine Definition von Open Source: [31]
[141] Diese Abkürung resultiert aus einem Spaß des Begründers, der den Unterschied zwischen Unix und seinem GNU-Linux darlegen wollte, und lautet: GNU's Not Unix.
[142] Diese gibt es in verschiedenen, ihr ähnlichen Ausprägungen, bekannt sind vor allem die „GNU GPL" [32], sowie die „Lesser GPL" [33].

nicht gewünscht werden, wie bspw. Spyware[143]. Durch den offen gelegten Quellcode und der Möglichkeit sich diesen selbst zu kompilieren, kann man bei ausreichender Qualifikation bzw. einer entsprechenden Anleitung auch Software generieren, die entweder DRM-geschützte Daten ohne Beachtung der Restriktionen abspielt oder einfach interessante Alternativen zu unkomfortablen DRM-Applikationen bietet, womit die Kontrolle über das jeweilige DRMS dem Anbieter aus der Hand genommen wird. Auch können Schnittstellen programmiert werden, die zwischen den verschiedenen Programmen vermitteln. Hierbei dürften besonders Programme interessieren, die die Funktionen mehrerer Abspielprogramme vereinigen, da eine Standardisierung seitens der Industrie eher unwahrscheinlich ist.

Inzwischen sind große Open Source-Plattformen auch so benutzerfreundlich geworden, dass sogar unerfahrene Anwender sich schnell und kostenlos Programme herunterladen und installieren können. An der Open Source-Gemeinde scheiterte unter anderem auch der Ansatz eines geschützten Systems, wie es von der TCPA vorgesehen wurde und noch wird. Bei ohnehin steigendem Linux- bzw. FreeUnix-Anteil an den Gesamtbetriebssystemen bestünde die Gefahr, dass immer mehr Nutzer auf die nichtkontrollierbaren Plattformen umsteigen, womit ein geschlossenes System vollends unmöglich wird.

Der Vorteil für den Nutzer und der Nachteil für die Firmen bei Open Source ist die Verhinderung von einschränkenden, proprietären Lösungen. Nicht wenige der Programmierer as dem Open Source-Bereich betreiben dies als eine Art sportlichen Wettkampf.

5.5 Überblick Kryptografie

Abschließend zu diese sechsten Kapitel soll nun noch ein Überblick über heutige Grundlagen der Kryptografie gegeben werden, da diese für DRMS essentiell und existentiell sind, wie sich noch herausstellen wird[144].

Bereits vor Christus bestand die Notwendigkeit für Menschen, geschriebene Nachrichten vor anderen zu verbergen. Zu diesem Zwecke entwickelten sie verschiedenste Geheimschriften und Verschlüsselungen, die nach und nach immer komplexer wurden. Ebenso so groß war jedoch auch das Interesse an eben diesen verschlüsselten Botschaften. Folgerichtig versuchte man sie zu

[143] Als Spyware bezeichnet man gemeinhin Programme die Daten über den Nutzer und sein Onlineverhalten sammeln. Dies kann im einfachsten Fall nur für nutzerangepasste Werbung dienen, kann aber bis hin zu Datenspionage (Passwörter, geheime Daten) gehen.
[144] Siehe dazu Kapitel 8.1

entschlüsseln. Und auch die Codebrecher ersannen immer bessere und komplexere Verfahren, um codierte Botschaften zu entschlüsseln. Damit begann der Wettlauf zwischen Kryptologen und Kryptoanalytikern, der bis heute andauert[145]. Dieser Wettlauf folgte bisher nur 2 Prämissen: Zum einen kann jeder Code ohne Schlüssel entschlüsselt werden, und zum anderen dauert es eine gewisse Zeit, je nach Raffinesse des Codes, bis er entschlüsselt ist. Im für den Kryptoanalytiker schlechtesten Fall hat dies durch die sog. Brute-Force-Methode zu geschehen, bei der alle möglichen Schlüssel der Reihe nach durchgetestet werden.

Durch die Erfindung des Computers wurden sowohl Kryptografie, wie auch Kryptoanalyse revolutioniert. Erstere konnte nun nahezu beliebig große Schlüssel und hochkomplexe mathematische Algorithmen verwenden, die letztere gewann an Geschwindigkeit beim durchtesten der Attacken und bei statistischen Methoden. Im Laufe der letzten Jahre haben sich nun verschiedene Klassen von Algorithmen entwickelt, welche mit Ihren Vor- und Nachteilen im folgenden erläutert werden.

5.5.1 Symmetrische Algorithmen

Die erste Klasse von Algorithmen die betrachtet wird, sind die sog. symmetrischen Algorithmen. Ihr Name kommt daher, dass der Schlüssel und auch der Prozess zum Ver- und Entschlüsseln der gleiche ist. D.h. die Anwendung des Algorithmus A auf den unverschlüsselten Text M unter Verwendung des Schlüssel K führt zu einem Chiffre C. Wird der Algorithmus zusammen mit dem Schlüssel auf das nun entstandene Chiffre angewendet, erhält man wieder den Klartext. Den Algorithmen dieser Gruppe ist gemein, dass sie nicht sehr komplex zu berechnen sind, d.h. die Geschwindigkeit der Verschlüsselung ist für Echtzeitanwendungen geeignet. Allerdings wird dieser Vorteil wieder dadurch wettgemacht, dass zum einen vor dem Kontakt ein gemeinsamer Schlüssel gefunden werden muss, bei dessen Übergabe die Sicherheit essentiell ist, und zum anderen die Skalierbarkeit eher schlecht ist, da man bei n vollständig miteinander kommunizierenden Personen $\Sigma(n-1)$ Schlüssel braucht, bzw. in einem großen Kommunikationsraum nur einen allgemeinen symmetrischen Schlüssel, der allerdings um so leichter kompromittierbar ist, je mehr Personen an dem Geheimnis teilhaben. Und auch der angerichtete Schaden durch die offen gelegte Kommunikation wäre in diesem Fall größer. Bekannte symmetrische Algorithmen sind DES[146], Triple-DES[147], die bereits

[145] Nachzulesen im Buch von Simon Singh; „Geheime Botschaften“; 2001; dtv-Verlag

[146] Data Encryption Standard; Ein Blockchiffre, bei dem es verschiedene Modi gibt, wie Schlüssel und Chiffre des Vorblocks in den neuen Block mit einfließen; DES wurde 1996 per Brute Force innerhalb eines halben Jahres gebrochen.

gebrochen wurden, sowie AES[148], der momentan den Stand der Technik darstellt.

5.5.2 Asymmetrische Algorithmen

Die zweite große Gruppe der modernen Kryptografie sind die asymmetrischen Algorithmen. Sie beruhen auf dem mathematischen Phänomen, dass ein geeignetes Schlüsselpaar bestehend aus privatem und öffentlichem Schlüssel, nacheinander auf einen Klartext angewandt eben diesen Klartext wieder ergeben. Und gleichzeitig kann man bei Vorliegen des öffentlichen Schlüssels nicht den privaten erschließen, wohl jedoch umgekehrt, was bei der Erstellung des Schlüsselpaares ausgenutzt wird. Der öffentliche Schlüssel wird bei einer zertifizierten Stelle hinterlegt, der private geheim gehalten. Will nun jemand eine Nachricht an den Besitzer des öffentlichen Schlüssels senden, verwendet er diesen zur Verschlüsselung der Nachricht. Der gewünschte Empfänger kann nun seinen privaten Schlüssel zur Entschlüsselung verwenden. Diese Methode wird auch als Public Key Kryptografie bezeichnet. Ein weiterer Vorteil der asymmetrischen Verschlüsselung ist die gute Skalierbarkeit. Für n Nutzer benötigt man zu beliebig gearteter Kommunikation nur n Schlüsselpaare. Der einzige, in der Praxis allerdings sehr relevante Nachteil derartiger Algorithmen liegt in der Rechenleistung die benötigt wird, um das Chiffre zu erzeugen. Bekannte Algorithmen sind RSA, Rabin, Diffie-Hellman und El-Gamal.

5.5.3 Hybride Algorithmen

Um die Stärken beider Algorithmenarten zu vereinen, werden in aktuellen Systemen meist Hybride Algorithmen verwendet. Da asymmetrische Algorithmen sicherer sind, sich aber nur für kleine Datenmengen eignen, werden sie auch dementsprechend eingesetzt: Mit ihrer Hilfe wird der für die folgende Kommunikation verwendete Session Key versandt. Dieser wird als Schlüssel für ein symmetrisches Verfahren auf das man sich einigt für den eigentlichen Datenaustausch verwendet.

5.5.4 Aufgaben der Kryptografie

Die heutige Kryptografie kennt jedoch nicht nur den geheimen Datenaustausch, sondern erlaubt noch weitere wichtige Eigenschaften

[147] Einfach die dreifache Anwendung von DES; erhöht die Sicherheit nur marginal.
[148] Advanced Encryption Standard; auch als Rijndael bekannt. Nachfolger von DES; ermittelt 1997.

einer Botschaft bei korrekter Anwendung festzustellen, die nun im Folgenden erläutert werden sollen. Diese fünf Punkte bilden das Repertoire der modernen Kryptografie:

- Vertraulichkeit
- Authentifizierung
- Integrität
- Assoziierbarkeit
- Autorisierung

Vertraulichkeit

Die Vertraulichkeit ist der bereits in der klassischen Kryptografie beabsichtigte Zweck. Niemand Unberechtigtes sollte die Möglichkeit haben, den Inhalt der Botschaft zu erfahren. Dadurch wurde sich im Idealfall ein Informationsvorsprung erarbeitet, den der Gegner nicht kontern konnte.

Authentifizierung

Die Authentifizierung des Absenders einer Botschaft war ebenfalls bereits in der klassischen Kryptografie bekannt. Auch zur damaligen Zeit war es wichtig, dass man mit Sicherheit vom angegebenen Sender einer Nachricht ausgehen konnte. Nichts wäre schließlich schlimmer, als wenn man vom Feind aufgefordert wird, in die gestellte Falle zu laufen, und dies in der Annahme, die Nachricht kommt vom eigenen Verbündeten, auch tut. Damals musste hierzu noch mit speziellen Geheimnissen gearbeitet oder auch mit verschiedenen Formen der Verschlüsselung. Das Konzept der Public Key Kryptografie eröffnet hierfür jedoch eine ganz einfache Möglichkeit. Da die Anwendung der beiden Schlüssel eines Paares hintereinander (in beliebiger Reihenfolge) wieder den Ausgangswert ergibt, verschlüsselt der Sender die Botschaft zuerst mit seinem eigenen privaten Schlüssel und danach mit dem öffentlichen des designierten Empfängers. Dieser kann die Botschaft als einziger korrekt entschlüsseln, um danach durch Anwendung des ihm bekannten öffentlichen Schlüssels des Senders zum eigentlichen Klartext gelangen. Da der Inhaber des zum öffentlichen Schlüssel passenden privaten Schlüssel als einziger in der Lage ist, dieses Paket herzustellen, ist dessen Identität erwiesen. Der Knackpunkt ist allerdings, dass der Empfänger auch wirklich den zum Sender gehörigen Schlüssel erhält, doch gibt es verschiedenste Methoden des sicheren Austauschs, um dies sicherzustellen, weshalb hierauf nicht nähr eingegangen werden soll.

Integrität

Damit von der Integrität des Inhalts der Botschaft ausgegangen werden kann, muss irgendwie sichergestellt werden, dass der Inhalt immer noch der selbe ist, wie als er den Sender verlassen hat. In der modernen Kryptografie werden hierzu sog. Hash-Funktionen[149] verwendet. Diese

[149] Weitere Informationen über Hash-Funktionen siehe Anhang C

berechnen aus einer Nachricht einen Hash-Wert, der parallel an den Kommunikationspartner gesandt wird. Dieser kann dann die Hash-Funktion ebenfalls auf die erhaltene Nachricht anwenden und dann die Ergebnisse vergleichen. Damit ein Angreifer nicht einfach selbst den Hash seiner veränderten Nachricht berechnet und somit die Integrität vortäuscht, wird der Hash-Wert vor dem Versenden mit dem privaten Schlüssel der Versenders verschlüsselt. Der Mechanismus ist wie bei der Authentifizierung der gleiche. Nur der Empfänger kann ein entsprechendes Hash herstellen, womit klar ist, dass er das Hash gesendet hat, und somit, bei übereinstimmen des vom Empfänger generierten Werts mit dem erhaltenen Wert, ist auch die Integrität der Botschaft sichergestellt. Aufgrund der bereits erwähnten Problematik der Rechenintensität asymmetrischer Algorithmen wird der signierte Hash-Wert einer Botschaft häufig auch zur Authentifizierung eingesetzt.

Assoziierbarkeit

Der nächste Punkt, die Assoziierbarkeit einer Botschaft und ihres Erstellers, ist für die heutige Kommunikation ebenso wichtig. Denn damit der Email-Verkehr eine rechtlich ähnliche Stellung erhalten kann wie bspw. der Informationsaustausch via Fax oder Telefon, muss es der Grundsatz der Unabstreitbarkeit gegeben sein. Auch dies kann die moderne Kryptografie gewährleisten, da sich mittels den bereits beschriebenen Methoden der Verschlüsselung eine einwandfreie Zuordnung von Botschaften und ihrem Sender herstellen lässt, eben weil dieser als einziger über das Wissen seines privaten Schlüssels verfügt.

Autorisierung

Die letzte Methode für die sich die Kryptografie eignet, denkt bereits ein wenig weiter: die Autorisierung. Hier werden erste Anknüpfungspunkte zu RM-Systemen geschaffen. Durch eine Zuordnung von Zertifikaten zu öffentliche Schlüsseln können Rechte mit den für die Identitäten stehenden Schlüsselpaaren verbunden werden. Dies kommt auch in den Public Key Infrastrukturen (PKI), die lediglich die freie Bewegung innerhalb einer Domäne gewährleisten, und Privilege Management Infrastrukturen (PMI) zum tragen, die man bereits als ein rudimentäres Äquivalent zu RM-Systemen sehen kann. Da eine PMI nur den Kern eines DRMS darstellt, und hier ein eigenes System entwickelt wird, welches sich nur an sie anlehnt, werden nur die verwendeten PKI erklärt.

5.6 Public Key Infrastruktur

Die so genannte Public Key Infrastructure (PKI) dient der sicheren Kommunikation im Internet. Ihr Vorteil gegenüber dem normalen sicheren Kanal bzw. der Kommunikation über Publik Key Kryptografie, liegt darin, dass der Nutzer sich in einer ganzen Domäne anmelden

kann, und in dieser sich dann frei (d.h. ohne zeitraubende, zusätzliche Authentifikationen) bewegen, ohne dass die Sicherheit darunter leidet. Das Konzept der PKI ist schon recht lange bekannt, so wurde die hier vorgestellte Kerberos[150]-PKI bereits Ende der 70er von Needham und Schroeder vom MIT als Freeware entwickelt, und immer wieder den aktuellen Bedürfnissen angepasst. Inzwischen gibt es bereits die fünfte Generation.

Das Kernkonzept von Kerberos ist die asymmetrische Verschlüsselung, die verwendet wird um über Umwege einen symmetrischen Session Key auszutauschen, also ein hybrides System. Ein sog. Ticket Granting Ticket (TGT) mit einer Gültigkeit von acht bis zehn Stunden wird zentral von einem Server vergeben, der alle Nutzerinformationen gespeichert hat. Dieser Server nennt sich Key Distribution Center (KDC), und kann aus Gründen des Datenschutzes auch von einer vertrauenswürdigen Drittpartei gestellt werden. Es vereint einen Authentication Service (AS) und einen Ticket Granting Service (TGS).

Alle Teilnehmer an dem System kennen den Langzeitschlüssel des KDC. Zur Kontaktaufnahme wird simplifiziert die folgende Prozedur verwendet: Der Nutzer nimmt verschlüsselt Kontakt zum AS des KDC auf, bekommt, sofern er berechtigt ist, das TGT zurück, dass vom KDC mit seinem eigenen öffentlichen Server-Schlüssel verschlüsselt wurde und die Befugnisse des Nutzers enthält. Dieses TGT kann der Nutzer in signierter Form an den TGS des KDC sobald er einen Service der Domäne des KDC nutzen will. Der TGS sendet dem Nutzer ein Service Ticket (ST) zurück, welches den symmetrischen Session Key enthält. Gleichzeitig erhält der angefragte Service ebenfalls ein Paket mit dem Session Key. Nun kann der Nutzer den Service in Anspruch nehmen, die Kommunikation wird symmetrisch gesichert.

Damit muss nur ein Server alle Geheimnisse kennen und kann zeitlich begrenzten Zugang zur restlichen Domäne gewähren, erneute Authentifikations-Prozesse entfallen.

Gleichzeitig stellt dieser Server allerdings auch einen leicht angreifbaren Punkt (Single point of failure) dar, was der Ausfallsicherheit des Netzes nicht dienlich ist. Hier müssen verschiedenste Methoden zur Prävention greifen, wie bspw. eine Verteilung der KDC-Architektur.

In Anhang B findet sich ein Ablaufsdiagramm welches einen vereinfachten Überblick über das Protokoll verschafft.

[150] siehe auch [34]

6 Schwachstellen im digitalen Bereich

In diesem Kapitel sollen nun die besonderen Eigenheiten digitaler Daten im Computerzeitalter und die Schwachstellen bzgl. des Schutzes durch das Urheberrecht aufgezeigt, sowie zu Grundkonzepten des DRM hingeführt werden. Dazu wird zunächst aufgeschlüsselt, was digitale Daten so besonders macht, dass sie ein solches Problem für das Urheberrecht darstellen. Im Anschluss wird auf die in der Praxis betroffenen Problembereiche eingegangen. Dazu werden zunächst die verschiedenen gesetzlich geschützten Datenarten auf ihr Potenzial urheberrechtlich verletzt zu werden untersucht. Danach werden die hauptsächlichen, urheberrechtlich relevanten Verletzungstatbestände im Computerzeitalter gegeneinander abgegrenzt: Verbreitung und Vervielfältigung. Ergänzend werden dann noch Tauschbörsen, sowie die aus ihnen erwachsenden Probleme durch die Massendatenübertragung erläutert. Abschließend wir die analoge Lücke thematisiert, die für sich genommen bereits einen vollkommenen Schutz praktisch unmöglich macht und daher besondere Erwähnung verdient.

6.1 Digitale Daten

Im Gegensatz zu den althergebrachten analogen Daten, die meist fest mit Ihrem Medium verbunden sind, können digitale Daten zu geringen Kosten und unproblematisch in der Verbreitung kopiert werden:

Die Kosten für ein herkömmliches Produkt setzen sich aus grundlegenden Fixkosten, die langfristige Posten darstellen, wie bspw. der Bau einer Fabrik, und kurzfristig angelegten variablen Kosten zusammen. Um nun die Stückkosten eines Produktes zu erhalten, werden die Fixkosten auf die Menge der produzierten Einheiten umgelegt, womit sich ergibt, dass mit steigender Anzahl die relativen Fixkosten sinken. Besonders dramatisch ist dies nun gerade bei digitalen Gütern zu betrachten: Die Fixkosten entstehen zwar durch den Schaffungsprozess, doch beim heutigen Stand der Technik sind die variablen Kosten zur Vervielfältigung praktisch zu vernachlässigen. Damit gehen die Grenzkosten mit jeder produzierten Einheit gegen Null. Ideal wäre also eine möglichst hohe Absatzrate des Produkts. In der Theorie wäre es also möglich, den Gewinn bis zu einer Marktsättigung beliebig zu maximieren.

Doch dieser Vorteil wird durch ein zweites Phänomen partiell negiert: Durch den Fortschritt der Technik ist es inzwischen möglich, die Daten ohne Fabrik zu vervielfältigen. Ein einfacher Computer mit CD-Brenner und Drucker bzw. Internetanschluss reicht aus, um die Daten so

nachzuahmen, dass es faktisch keinen Unterschied betreffend der Daten zum Original gibt. Im ersteren Fall des Brenners kostet nun nur noch die Verbreitung und die Materialien Cent-Beträge. Im zweiten Fall entfallen sogar die Materialien ganz. Hier wird die Diskrepanz zwischen den umgelegten Fixkosten und den nahezu nicht existenten variablen Kosten deutlich. Da dem Content-Piraten keine Fixkosten (mit Ausnahme der Computerhardware, die allerdings inzwischen fast jeder Schüler sein eigen nennt) entstehen, werden seine Preise ausschließlich von den variablen Kosten bestimmt, wodurch er Dumping-Preise anbieten kann, die dem Rechteinhaber den Rang ablaufen. Dieser sieht sich nun im Zwiespalt: Entweder seine eigenen Preise senken, um durch die schiere Masse verkaufter Kopien die entgangenen Gewinne hereinzuholen, und zudem Käufer zu(rück)gewinnen, oder den illegalen Konkurrenten aus dem Geschäft zu verdrängen, sei es durch rechtliche Schritte, oder auch durch technische Schutzmaßnahmen, wie es momentan versucht wird. Verständlicherweise wählt man den zweiten Schritt, da es ja nur legitim ist, sein (wenn auch immaterielles) Eigentum rechtlich abzusichern. Nun ist an dieser Stelle aber auch problematisch, dass nicht nur groß angelegte Raubkopierer, eben besagte Content-Piraten, auf den Gedanken kommen, sich den Content über illegale Wege zu holen. Auch verschiedene private Nutzer nutzen diesen Weg, da ihnen im Gegensatz zu dem legalen Kauf im Laden praktisch keine Kosten entstehen.

6.2 Datenspezifische Eigenheiten

Nachdem bereits zu Beginn die rechtliche Situation aufgeschlüsselt wurde und auch die besonderen Eigenheiten der digitalen Daten beschrieben wurden, stellt sich nun natürlich die Frage, welche urheberrechtlich geschützten Werke überhaupt in Gefahr laufen, im digitalen Bereich illegale Verwendung zu finden. Dazu soll zunächst in zusammengefasster Form die Aufstellung schutzfähiger Werke gemäß §2 UrhG wiederholt werden:

1. Sprachwerke, wie Schriftwerke, Reden und Computerprogramme
2. Werke der Musik
3. Pantomimische Werke, einschließlich der Werke der Tanzkunst
4. Werke der bildenden Künste, einschließlich Werke der Baukunst und der angewandten Kunst und Entwürfe solcher Werke
5. Lichtbildwerke, einschließlich der Werke, die ähnlich wie Lichtbildwerke geschaffen werden
6. Filmwerke, einschließlich der Werke, die ähnlich wie Filmwerke geschaffen werden

7. Darstellungen wissenschaftlicher oder technischer Art, wie Zeichnungen, Pläne, Karten, Skizzen, Tabellen oder plastische Darstellungen.

Nicht alle dieser Werke sind in gleicher Form in das Internet abbildbar, da die stoffliche Ebene verloren geht. Relevant für die Betrachtung sind daher nur Abbildungen dieser Werke, sei es als Bild-, Lichtbild-, Film-, Schriftwerk oder Musik. Darunter fallen insbesondere die in Punkt 1 genannten Reden als Schrift-, Film- oder Tonwerk (um einen verallgemeinernden Ausdruck zu gebrauchen), die in Punkt 3 genannten Vorführungen als Film- oder Tonwerk, die unter Punkt 4 genannten Werke als Bildwerke, und schließlich die unter Punkt 7 genannten Darstellungen als spezielles Schriftwerk oder auch als Bildwerk.

4 Werksarten

Damit haben sich auch die vier für das Internet relevanten Werksarten herauskristallisiert. Computerprogramme fallen dabei unter die Schriftwerke, doch sollte ihre Einordnung noch überdacht werden[151].

Musik

Zuerst sollen die Musikwerke abgehandelt werden, da diese in der Vergangenheit wohl den meisten Wirbel in der Presse verursacht haben. Wie bereits in den rechtlichen Grundlagen behandelt, ist die Ausführung des Werkes schutzfähig und auch die verwendete Melodie. Den Musikdaten ist gemein, dass sie inzwischen extrem komprimierbar geworden sind, hauptsächlich durch verlustbehaftete Algorithmen, die für den Menschen nicht wahrnehmbare Töne aus dem Werk herausfiltern[152]. Dieser Prozess, der unter § 14 UrhG – Entstellung von Werken - fallen könnte, ist nicht zuletzt für die Misere um das geistige Eigentum mitverantwortlich. Musikdaten sind für heutige Verhältnisse klein[153] und fast standardisiert in einem frei verfügbaren Format[154], in welches man mit geringen Kenntnissen selbst Musik konvertieren kann. Und auch der Prozess der Konvertierung ist mit geringem Aufwand verbunden. Die zugehörigen Programme sind Freeware, der Prozess selbst muss nur einmal gestartet werden und dauert mit aktueller Hardware nur einige Minuten pro CD. Neben dem regen Tauschhandel im Darknet[155] gibt es nur geringes Verletzungspotential im Bereich der Musikstücke, da es noch nicht allgemein üblich sondern eher verpönt ist, eigene Internetseiten mit Musik zu hinterlegen o.ä. .

Filme

[151] mehr dazu siehe in Kapitel 13.3.3
[152] Speziell MP3
[153] pro Minute ab unter einem Megabyte, Qualität nahe der Original-CD
[154] MP3; andere Formate spielen noch nur Nebenrollen; bspw. WMA, das mit Microsofts DRMS gekoppelte Format
[155] siehe entsprechendes Kapitel 7.1; das Darknet ist ein Begriff der den Bereich des Internets umfasst, der sich mit dem Handel urheberrechtlich geschützten Materials beschäftigt.

Neben den Musikwerken sind im Darknet die Filmwerke am stärksten vertreten. Auch hier gab es große Fortschritte im Bereich der Kompression. Dazu kam noch der allgemeine Umstieg auf digitales Fernsehen, Filme auf DVD und der Verkauf von digitalen Videokameras. Filmwerke sind allerdings trotz dieser Fortschritte in der Kompression immer noch von beachtlicher Größe. Ein durchschnittlicher Kinofilm guter[156] Qualität hat immer noch fast ein Gigabyte, was selbst im Optimalfall, der außer auf offiziellen Video-on-demand-Seiten praktisch nie eintritt, einer Downloadzeit von knapp 3 Stunden bei angenommener DSL-Verbindung entspricht.

Auch die Arbeit einen solchen Film von einer DVD oder einem vergleichbaren Medium zu konvertieren, ist momentan noch beachtlich. Bis eine Kopie im stark komprimierten DivX-Format vorliegt, vergehen mehrere Stunden. Das meiste davon ist allerdings Rechenzeit, bei der der Nutzer nicht anwesend sein muss. Die zur Konvertierung verwendeten Programme sind als Freeware verfügbar oder auch einfach aus dem Internet herunter zu laden.

Häufig finden sich auch sog. Screener von minderer Qualität, die einfach im Kino abgefilmt wurden und so Filme aus den USA bereits lange vor ihrem dortigen Kinostart dem deutschen Publikum zugänglich machen. Diese Methode erfreute sich großer Beliebtheit, wird inzwischen aber von den Kinos stark bekämpft[157]. Die Eigengenerierung von digitalen Kopien von Filmwerken ist insofern problematisch, dass die Hardware auf einem vergleichbar neuen Stand sein und zudem der Nutzer immer einiges an Know How investieren muss, da im Gegensatz zur Generierung von MP3-Dateien aus Audio-CDs das Rippen einer DVD noch nicht per Knopfdruck funktioniert. Doch auch dies wird wohl bloß eine Frage der Zeit sein.

Schriftwerke

Schriftwerke sind im Vergleich kaum noch in den Tauschbörsen vertreten, es finden sich neben Computerfachbüchern allenfalls Bestsellerromane oder einige Ratgeber. Und diese wurden zumeist eingescannt. Damit fällt beim Anfertigen dieser Kopien eine viel größere Arbeit als bei Film- und Musikwerken an. Das größere Verletzungspotential findet sich hier auf diversen Homepages. Und auch, wenn man einigen großen Verlagen glauben mag, in digitalen Dokumentenkopierdiensten (hier speziell Subito[158]). Gerade im Bereich der Schriftwerke neigen viele Personen sich mit fremden Federn zu

[156] subjektiv zumindest dem Fernsehen vergleichbar; eher DVD-Qualität
[157] Neben den allgegenwärtigen Hinweisschildern, machen in amerikanischen Kinos Angestellte mit Nachtsichtgeräten Jagd auf die Kopierer
[158] Ein von Universitätsbibliotheken eingerichteter Dienst, der es Wissenschaftlern und Studenten ermöglicht, sich per Telefon Artikel aus Zeitungen einscannen zu lassen. Siehe auch [35]

schmücken, da fremde Inhalte binnen weniger Sekunden zu eigenen gemacht werden können. Die Privatkopie greift dabei nur so lange, wie die Inhalte zum privaten Gebrauch vervielfältigt werden, was bedeutet, dass eine Duplikation der im Internet publizierten Inhalte erlaubt ist, so lange diese nicht wieder veröffentlicht werden, bspw. als Teil der eigenen Homepage. Das Verweisen per Link auf fremde Texte gilt als unproblematisch, wohingegen das sog. Framing, das Aufrufen eines auf einem fremden Server gelegenen Contents rechtlich im Sinne der Urheberpersönlichkeitsrechte bedenklich ist, da §13 UrhG sehr leicht verletzt werden kann. Schriftwerke sind hauptsächlich kleinste Datenmengen. Ein besonderer Punkt ist bei diesen allerdings noch die einfache Redigitalisierung bei Überwinden der analogen Lücke: Fast alle Scanner liefern standardmäßig OCR-Programme zur automatischen Schrifterkennung mit, die inzwischen beachtliche Ergebnisse liefern.

Von den datentechnischen Gegebenheiten sind Lichtbild- und Bildwerke den Schriftwerken sehr ähnlich. Die Datei-Größe beträgt zumeist wenige Kilobyte, da dies genügt auf dem Bildschirm die Bilder in angemessener Größe darzustellen, und auch für die meisten Ausdrucke reicht. Sowohl zum Herstellen, als auch zur weiteren Verwendung von großen Bilddateien braucht man spezielle Hardware, was wohl auch der Grund für ihre Seltenheit sein dürfte. Die hauptsächlichen Urheberrechtsverletzungen finden ähnlich wie bei Schriftwerken nicht in Tauschbörsen statt[159]. Häufiger ist auch hier der Fall, dass Fotografien und Zeichnungen digitalisiert werden, und ohne die entsprechenden Rechte auf Internetseiten verwendet werden. Dieser Schritt lässt sich mit DRM-Systemen allerdings nicht verhindern, weshalb er für die hier vorgenommene Betrachtung eines DRMS irrelevant ist, nicht jedoch für die folgende Beschreibung des rechtlichen Umfelds und die juristischen Betrachtungen gegen Ende der Arbeit. Verhindert werden kann nur die illegale Weiterverbreitung digitaler Bilder, die dem Nutzer bereits in dieser Form vorliegen. Dieses Geschäftsfeld ist jedoch noch in den Kinderschuhen, da die körperliche Form der Daten bei Bildwerken[160] für den letztendlichen Preis stark ausschlaggebend ist. Ein letztes Teilgebiet der Urheberrechtsverletzungen bei Bildwerken ist die Verwendung fremder Bilder aus dem Internet für eigene Zwecke. Die private Nutzung auf eigenen Internetseiten verstößt gegen das Veröffentlichungsrecht des Urhebers, die gewerbliche Nutzung jedweder Art greift in seine Verwertungsrechte ein. Das Herunterladen veröffentlichter Dateien oder das Zwischenspeichern auf Proxy-Servern wird von ihm hingegen durch die Veröffentlichung konkludent gebilligt.

[159] Wenn man von pornographischen Bildern oder den bereits genannten eingescannten Büchern oder Zeitschriften absieht, die aber eher zu den Schriftwerken zählen

[160] Poster, hochqualitative Fotographien u.v.m.

Doch zu diesen Themen mehr im Kapitel „Schutzbereich“ der rechtlichen Grundlagen.

6.3 Verbreitung vs. Vervielfältigung

Nach der Beschreibung des Contents, der verletzt wird, sollen nun die beiden abstrakten, juristischen Hauptgebiete, in denen die meisten Verletzungen zu finden sind, gegeneinander abgegrenzt werden:

Verbreitung und Vervielfältigung sind die beiden wesentlichen Verletzungsbereiche bei digitalen Daten. Sie sind zwar nominell im Recht getrennt, hängen in der Praxis aber zusammen. Fast immer muss einer unrechtmäßigen Vervielfältigung im Privatbereich eine unrechtmäßige Verbreitung bzw. aus heutiger Sicht auch eine unrechtmäßige öffentliche Zugänglichmachung vorausgegangen sein. DRM setzt nun an beiden Punkten auf einmal an. Es kann die reine Verbreitung der Datencontainer zwar nicht verhindern, macht die auf diese Weise verbreiteten Daten für die unrechtmäßige Nutzung unbrauchbar (so ist zumindest die Absicht eines funktionierenden DRMS) und der Nutzen, der aus einer Vervielfältigung gezogen würde, entfällt auch. Zudem widersetzt es sich der Entschlüsselung der Daten, um damit die Verbreitung ungeschützter Daten, die sich zur Vervielfältigung eignen würden, so schwer wie möglich zu machen. Im folgenden sollen besonders die Tauschbörsen als Schwerpunkte des weltweiten Raubkopierens, sowie der damit eng verknüpfte technische Fortschritt im Bereich Datenübertragungsgeschwindigkeit, der die Tauschbörsen als System überhaupt erst ermöglicht, betrachtet werden.

6.4 Tauschbörsen[161]

Mit der Entwicklung Napsters der wohl immer noch bekanntesten Tauschbörse begann der „Siegeszug“ selbiger. Bis dato wurden kopierte Daten auf CD gebrannt und per Post verschickt oder direkt via LAN[162] zwischen den Computern übertragen. Diese Verbreitung wurde durch das Internet bereits stark erleichtert. Durch den Fortschritt der Technik wurden auch zunehmend größere Datenübertragungsraten möglich[163] und damit eine um so schnellere Verbreitung der digitalen Daten. Und hier kommt zudem die großen Vorteile der Tauschbörsen zum tragen:

[161] siehe auch Appendix A
[162] Local Area Network – Lokales Netzwerk
[163] 1987 lief das NSFNET mit 1,5 MBit/s; 1993 erreichte man eine Geschwindigkeit im Internet von 45 MBit/s und heute erreicht man bereits den Terrabit-Bereich. [36]

Napster wurde über einen zentralen Server gesteuert, über den die Daten der einzelnen Nutzer direkt übertragen werden konnten. Damit wurden Hunderte, zu Hochzeiten sogar Millionen Computer miteinander vernetzt, es entstand eine gigantische Sammelstelle für digitale Daten. Häufige Daten, wie aktuelle Popsongs gab es weit über 1000 Mal zum Download bereitgestellt, womit die Verbreitungsgeschwindigkeit exponentiell ansteigt.

Erste Generation

Im Gegensatz zu damaligen Warez-Seiten[164], die zum einen den gesamten Verkehr bezahlen müssen, sowie eine entsprechende Bandbreite zur Verfügung stellen müssen, leben die Tauschbörsen durch die Summe der Myriaden kleiner Leitungen. Wenn eine Million Nutzer beispielsweise 10 Kilobyte ihrer Uploadrate zur Verfügung stellen, kommt man leicht auf Raten von 10 Gigabyte pro Sekunde. Dies entspricht bei einer durchschnittlichen Liedgröße von ca. 5 Megabyte etwas 2000 Liedern oder ca. 15 Filmen, die sich pro Sekunde im Internet verteilen. Und diese Zahl wird bei aktuellen Tauschbörsen leicht um das zehn- bis dreißigfache übertroffen. Sicherlich entspricht nicht jede getauschte Dateneinheit einer real gekauften Einheit im Falle des Nichtvorhandensein der Börse, doch dass ein großer Schaden entsteht, ist offensichtlich.

Zweite Generation

Den zweiten Vorteil der Tauschbörsen brachte ihre zweite Generation mit sich: Nachdem Napster und erwähnte Internetseiten sich der unrechtmäßigen Verbreitung schuldig gemacht haben, stellten die Tauschbörsen von zentralen servergestützten Netzwerken auf dezentrale, sog. Peer-2-Peer-Netzwerke um. Darunter fallen bspw. Netze wie Kazaa oder Emule. Hierbei machen sich die Serverbetreiber keiner Verbreitung schuldig, da sie nur Verbindungen zwischen den Computern herstellen, und der Austausch ausschließlich zwischen diesen selbst abläuft. Internetzugangsanbieter (ISP[165]) versuchen den Tauschgeschäften dadurch entgegenzutreten, dass entsprechende Ports über die die Netze funktionieren gesperrt werden. Doch auch diese Gegenmaßnahmen lassen sich auf Nutzerseite denkbar einfach umgehen. Eine Möglichkeit wäre die Kontrolle des Inhalts der Pakete und Sperrung von voraussichtlich illegalem Content. Doch dies käme einer Zensur gleich und ließe sich nicht mit geltendem deutschem Recht vereinbaren.

Aktuelle Generation

Die dritte Generation von Tauschbörsen kann sogar noch weiter gehen: Teilweise abstrahieren sie vollständig von Servern und verbinden die Computer mittels kleiner Datenpakete, so dass für jede zu verteilende

[164] Internetseiten, auf denen illegal Programme und Mediendaten zum Download angeboten wurden.
[165] Internet Service Provider

Datei ein eigenes kleines Peer2Peer-Netz entsteht[166]. Wiederum andere versuchen die gesetzliche Lücke der Privatkopie auszunutzen, indem Tauschbörsen privaten Umgangs entstehen, zu denen man bspw. nur Zugang bekommt, wenn man vorher in einem entsprechenden Chat war und eine Einladung erhielt. Doch eine solche Börse ist noch nicht etabliert. Sie liefern allerdings ein exzellentes Beispiel dafür, dass einmalig frei (wenn auch illegal) in Umlauf gebrachte Daten, nie wieder an der Verbreitung gehindert werden können.

Fazit

Wichtig für dieses Kapitel ist auch die Kombination mit der Urheberrechtsnovellierung. Denn selbst bei maßvoll angehobenen Strafen (und andere kommen ohnehin nicht in Betracht) demonstriert die Entwicklung „Usenet[167] – Warez-Seiten – Napster – P2P-Netzwerke“, dass solche Dienste immer anonymer und gleichzeitig größer wurden, und nie einen Rückschlag hinnahmen. Im nachfolgenden Kapitel findet sich ein Rechenbeispiel, welches das Ausmaß der ungezügelten Misere wohl recht einfach verdeutlicht und den Regelungsbedarf deutlich macht.

6.5 Massendatenübertragung

Mit Entwicklung des Internets war es zunächst nicht absehbar, dass es sich zu einem derart urheberrechtsbefreiten Raum entwickelt und zudem so hohe Umsatzeinbußen durch den illegalen Vertrieb von Content sich ergeben würden. Die Gründe sind unter anderem auch in der grundlegenden Technik des Internets zu finden. Zu Beginn, etwa im Jahr 1994[168], war die Vorstellung ein ganzes Megabyte an Daten zu übertragen mit einer Wartezeit von etwa 5 Minuten verknüpft. Heutzutage haben sich zwei Dinge geändert: Zum einen steht das gerade beschriebene Megabyte nicht mehr für eine Sekunde[169] Musik in CD-Qualität sondern für fast eine Minute[170]. Das bedeutet, dass der Informationsgehalt der Daten auf 6000 % in 10 Jahren gestiegen ist. Und zum anderen ist die Geschwindigkeit des durchschnittlichen Internetanschlusses, den ein Privatmann besitzt, rapide gestiegen. Und nicht zuletzt wurden die Kosten des Internetzugangs durch den Wettbewerb und den Fortschritt, der an die Kunden weitergegeben wurde, extrem gesenkt. Diese drei Komponenten vergrößern die Kopierkapazität nicht nur additiv, sondern multiplikativ.

[166] beispielsweise BitTorrent
[167] Ein dem WWW vorausgehender Teilbereich des Internets, in dem vor den Tauschbörsen Content illegal distribuiert wurde.
[168] Schaffung des WWW
[169] Wave-Format, 16 Kanäle, Stereo, 44100 Hz.
[170] MP3-Format, 128 kbps

Damals

Ein Beispiel dafür, mit vereinfachten Zahlen und abstrahiert von Telefonzeiten & Währungsneuerungen, sowie teureren Hardwarepreisen usw.: Für 100 DM bekam man vor 10 Jahren (1994) legal ca. 4 Musik-CDs indem man in einen Laden ging und den Kauf abschloss. Über das Internet war dies ungleich teurer. Eine Internetminute schlug sowohl mit Zugangsgebühren durch einen Provider, als auch den ganz normalen Telefongebühren für eine stehende Leitung zu Buche. Da die wenigen zur Verfügung stehenden Einwahlknoten nur selten im unmittelbaren Nahbereich lagen, kann eine Minute mit ca. 10 Pfennigen angegeben werden. Die Geschwindigkeit eines 28800 Baud Modems (zur damaligen Zeit, war dieser Standard V.34 gerade entwickelt worden) beträgt im hier angenommenen Idealfall ca. 3,6 Kilobyte pro Sekunde. Für 100 DM konnte man also in 1000 Minuten 216 Megabyte Daten herunterladen. In CD-Qualität hätte eine Minute Musik umgerechnet 80 MB, was insgesamt knapp 3 Minuten Musik entspricht.

Der Aufwand stand damals also in keinem Verhältnis zum Nutzen. Ähnlich, jedoch schon in einem etwas besseren Verhältnis, verhielt es sich mit Programmen, die zur damaligen Zeit selten mehr als 100 MB umfassten.

Heute

Wenn man heutzutage eine ähnliche Rechnung aufmacht zeigt sich der technische Fortschritt und mit ihm auch das Ausmaß der Misere für Content-Produzenten: Eine monatliche, in Bezug auf Zeit und Transfervolumen unbegrenzte Verbindung in das Internet bzw. Darknet kostet umgerechnet ebenfalls 100 DM[171]. Die Geschwindigkeit einer solchen DSL-Verbindung liegt bei zumeist 768 kbps, umgerechnet 96 Kilobyte pro Sekunde. Wenn man nun den ganzen Monat durchgehend Daten lädt (was aufgrund der hohen Nutzerzahlen des Darknets sehr gut möglich ist) kommt man bei einer realistischen durchschnittlichen Datenrate von nur 50 Kilobyte pro Sekunde auf 129,6 Gigabyte Daten, was 129000 Minuten bzw. 2160 Stunden oder auch 90 Tagen(!) Musik in CD-Qualität entspricht. Dies entspricht einer Steigerung von über 42 Millionen Prozent. Und für das Bargeld im Laden bekäme man momentan sogar weniger als 4 CDs. Ganz abgesehen davon, dass mit der Flatrate noch genügend Kapazität bleibt, im Internet zu surfen und seine Geschäfte abzuwickeln.

Sicherlich kann dies nur ein Beispiel sein, welches es so in der Realität nicht geben wird. Aber durch die steigende Vertrautheit der Nutzer mit dem Medium Internet und dem Computer wird sich dieser Trend weiter fortsetzen. Das Problem dürfte allerdings sein, dass sich an dieser Schraube der Hebel für eine letztendliche Verbesserung der Situation

[171] Der Preis einer aktuellen Flatrate liegt bei 39 Euro zzgl. einer erhöhten Grundgebühr. Vereinfacht wird von 51,13 Euro (=100 DM)ausgegangen, damit die Vergleichbarkeit gewährleistet bleibt.

der Urheber nicht ansetzen lässt, da sie sich vielleicht mit Mühe anhalten lässt (Begrenzung der Geschwindigkeiten im Privatbereich), aber keinesfalls zurückdrehen lässt. Es kann allerdings über eine Pauschalabgabe auf Breitbandzugänge nachgedacht werden, doch dies wird in Kapitel „Anpassung der rechtlichen Situation“ genauer diskutiert.

Andere Datentypen

Diese Rechnung gilt ebenfalls für Videos, und in etwas beschränkterem Maß für Programme, da diese durch immer größere Medien, immer größere Festplatten und Arbeitspeicher ebenfalls immer umfangreicher werden. Bücher und Bilder sind dahingehend Spezialfälle, da Ihre Qualität nicht nur durch den Inhalt bestimmt wird, welcher ja problemlos kopiert werden kann, sondern auch durch die Qualität des analogen Mediums bestimmt wird[172]. Durch die stark beschränkte Größe werden sie allerdings auch kopiert.

6.6 DAD-Wandlung

Zum Abschluss des Kapitels soll hier noch die DAD-Wandlung vorgestellt werden. Unter dieses Schlagwort fallen sämtlich Methoden für die nicht auf das aktuelle Format einer Dateien zurückgegriffen wird, sondern erst an einer „digital-zu-analog“-Schnittstelle die Daten verwendet werden. Daher auch der Begriff der analogen Lücke der eben dieses bezeichnet.

Zur Aufnahme der Daten durch den Menschen muss eine solche Schnittstelle meistens bei urheberrechtlich geschützten Dateien bzw. den zugehörigen Wiedergabeprogrammen vorhanden sein. Eine Ausnahme bildet hier Software, da diese zumeist aus ausführbarem Programm-Texten besteht und damit vom Benutzer nicht direkt aufgenommen wird. Analoge Schnittstellen sind zum Beispiel Monitore für digitale Schriftstücke, Lautsprecher für Musikstücke und bedrucktes Papier wieder für Schriftstücke und weiteres. Sobald die Daten in dieser Form angezeigt / abgespielt werden, müssen alle kryptografischen Schutzmaßnahmen deaktiviert sein.

Die einzigen Schutzmassnahmen die noch in Kraft sind, gehören zu den bereits thematisierten Wasserzeichen. Letztere gehören nicht einmal zu Schutzmassnahmen im engeren Sinne. Wasserzeichen erlauben zwar im Normalfall durch die Kopplung von Daten mit Metadaten eine Zuordnung und somit eine Rückverfolgung etwaiger illegaler Kopien. Doch auch diese Metadaten sind angreifbar (siehe dortiges Kapitel).

Erst in heutiger Zeit wird die DAD-Wandlung zu einer ernst zu nehmenden Gefahr, nachdem die Qualität dieser Wandlung immens gestiegen ist. Als bestes Beispiel dienen Audio-Kassetten, mit denen bis

[172] Poster oder Postkarten, großformatige Bildbände oder Taschenbücher etc.

in die Mitte der 90er Lieder aufgenommen wurden. Es musste zwar ein Beschluss gefasst werden, dieser konnte jedoch sehr liberal ausfallen, da diese analogen Kopien weder einen hohen Wiederkopierwert besaßen, noch einfach zu verbreiten waren.

DD-Wandlung

Eine neue Variante der DAD-Wandlung ist die direkte DD-Wandlung[173]. Hierbei wird der Schritt über das analoge Medium ausgeklammert, und die Daten werden in digitaler, jedoch bereits entschlüsselter Form, die zur Weiterverarbeitung für spezialisierte Subprozessoren gedacht ist, abgefangen. Ein Beispiel ist eine Soundkarte mit digitalem Ausgang: Der Entschlüsselungsvorgang findet bestenfalls in der Soundkarte statt, danach kann der decodierte Datenstrom wieder einfachst aufgezeichnet werden.

Als Fazit lässt sich beim gegenwärtigen Stand der Technik sagen, dass es mit der beschränkten Ausnahme von Wasserzeichen, keine Möglichkeit gibt die D(A)D-Wandlung zu unterbinden. Als Beispiel hierfür sei der Kampf zwischen Microsoft und Crackern, die dessen proprietäres WMA-Format der DRM-Versionen 1 und 2 geknackt haben. Zunächst wurden die digitalen Daten auf dem Weg zwischen dem Abspielprogramm und dem Soundtreiber abgefangen. Als Microsoft in Version 2 dies durch einen sicheren Kanal zwischen Treiber und Abspielprogramm zu verhindern suchte, wurden als nächstes die Treiber der Soundkarte so modifiziert, dass sie die uncodierten Daten über den sicheren Kanal entgegennahmen, diese nun aber nicht nur zur Soundkarte schickten, sondern sie wiederum in eine nun ungeschützte Datei schrieben. Und während dieser Zeit war der Ausgang der Soundkarte, der zum Lautsprecher führte ohne Beachtung geblieben. Hier war die Qualität zwar schlechter, was auch der Grund der Nichtbeachtung war, doch dieser Ausgang wird ein nichtverschließbarer bleiben, da die angehängten Lautsprecher in absehbarer Zeit nicht mit Prozessoren versehen werden, die einen digitalen sicheren Kanal zwischen Lautsprecher und Soundkarte gewähren. Und selbst in diesem hypothetischen Fall gibt es immer eine Lücke an der das Skalpell der Cracker ansetzen kann um die frisch entschlüsselten Daten abzufangen.

[173] Digital-Digital-Wandlung

7 Problematik des Kopierens

Und warum wird nun so eifrig kopiert? Sicherlich ist die Gelegenheit günstig. Doch auch in anderen Bereichen des Lebens beweist man als normaler Mensch genügend Moral, etwas Verbotenes nicht zu tun. Selbst wenn man wohl nicht erwischt wird, werden die wenigsten Menschen in einem Laden etwas mitgehen lassen. Im Prinzip gibt es hier allerdings eine Parallele zur Raubkopie, nur dass eben geistiges Eigentum gestohlen wird. Der Unterschied ist, dass es bei Daten keine Ausschließbarkeit gibt, womit der Bestohlene zumindest nicht das Problem hat, dass er keinen Nutzen von seinem Eigentum hat, wie es bei einem Gegenstand der Fall wäre. Durch die perfekte Kopierbarkeit wiederum können sich auch unrechtmäßige Güter weiterverbreiten, und dies tun sie mit einer erhöhten Geschwindigkeit, da der Preis hierfür nur sehr gering ist (wie bspw. eben in einer Tauschbörse).

Dieses Kopieren stellt daher für die Erschaffer immaterieller Güter ein Problem dar. Doch was sind die Gründe und was kann dagegen getan werden?

Im folgenden Kapitel soll zunächst die momentane Situation auf dem Markt der Immaterialgüter dargestellt werden. Dies geschieht durch eine Charakterisierung der Beweggründe der beiden auf dem Markt vertretenen Parteien, zunächst mittels der Erklärung des sog. „Darknets“ und im Anschluss mittels des „tilting bottle“-Modells. Dieses zeigt das Tauziehen um den Content in Form einer Flasche. Zu guter letzt wird in diesem Kapitel aufgezeigt, dass es keine perfekten Schutz für Content geben kann, mit Ausnahme der Nichtveröffentlichung, welche natürlich auch nicht im Sinne des Urhebers liegt. Diese Erkenntnis ist die Grundlage dafür, dass bisherige DRM-Programme ihren Dienst versagten und es überhaupt notwendig wird ein neues System zu schaffen.

7.1 Das Darknet[174]

Dieser interessante Ansatz, den illegalen Bereich im Internet, in dem Daten nahezu beliebig kopiert werden können, zu definieren, kommt zu dem Schluss, dass es im Wesentlichen drei Annahmen gibt, denen es genügt:

- Jedes weit verbreitete Objekt wird irgendwann in einem ungeschützten Zustand einer Nutzergruppe zur Verfügung stehen[175]

[174] siehe dazu [37]
[175] Siehe zur Untermauerung auch Kapitel 7.3

- Solange es für die einzelnen Nutzer dieser Gruppe interessant und möglich ist, werden sie die Daten auch kopieren
- Die Nutzer sind untereinander durch Breitbandkanäle verbunden

Annahme eins wird durch die im Grundlagenteil dargelegten Kopiermethodiken, besonders die DAD-Wandlung, wie auch den generellen zeitlichen Aspekt begründet. Durch die Notwendigkeit, wie auch den Wunsch des Content-Produzenten, diesen in maximaler Zahl zu verkaufen, wird bei kommerziellen Daten für Privatnutzer der Zustand „weit verbreitet“ nach einer unbestimmten Zeit eintreten. An diesem Punkt kann ein DRM-System also nicht einsetzen. Es könnte lediglich die Zeitspanne vergrößern, bis Daten in ungeschütztem Zustand vorhanden sind.

Annahme drei wird durch die sich gegenseitig unterstützenden Prozesse von effizienter arbeitender Kompression und technischem Fortschritt im Infrastrukturbereich untermauert. Eine Limitierung der Zugangsdatenraten in das Internet, wäre nur durch staatliches Eingreifen regelbar, und wäre ohnehin für diesen ohne Interesse. Zudem würden die Nutzer eine derartige Maßnahme als tiefen Eingriff in ihre Selbstbestimmungsrechte sehen, womit ein auf dieser Tatsache aufbauendes System von vorneherein zum Scheitern verurteilt wäre. Die effizientere Kompression lässt sich erst recht nicht verhindern, da viele der Kompressionsalgorithmen zum einen im Open Source-Bereich entstehen, und zum anderen auch für die Firmen selbst nicht unbeachtliche Vorteile mit sich bringen.

Damit bleibt für die DRM-Systeme nur der zweite Punkt, an dem sie einsetzen können. Die Möglichkeit von Kopien lässt sich, wie bereits mehrfach thematisiert, nicht vollkommen ausschließen. Somit müssen die Nutzer das Interesse an den Kopien verlieren. Im folgenden Kapitel sollen die Kernkomponenten eines DRM-Systems, und auch Ihre Wirksamkeit bezüglich dieser Funktion. Zunächst wird ein klassisches DRM-System betrachtet. Danach werden entsprechende Strategien erläutert und schlussendlich wird jeweils eine Designentscheidung gefällt.

7.2 Das „tilting bottle“-Modell

Dieses Modell wurde vom Autor mitentwickelt, und indiziert durch Gegenüberstellung zweier am Markt teilnehmenden Parteien, den Nutzern und den Vermarktern von Content (die mit den Urhebern durchaus identisch sein können), die Richtung, die Digital Rights Management Systeme zukünftig einschlagen müssen.

Die zentrale Idee, die dahinter steckt, ist die Abbildung des generischen Marktes auf dem Content gehandelt wird als Tauziehen um eine Flasche. Das besondere an dieser Simplifizierung liegt in der besonderen Physik einer Flasche. Sobald man diese nur ein wenig kippt, und sie wieder loslässt, richtet sie sich wieder von selbst auf. Sobald allerdings ein gewisser Neigungswinkel überschritten wird, benötigt sie fremde Hilfe, um sich wieder aufzurichten. Sollte die Flasche nun losgelassen werden, wird sie kippen und kaputt gehen. Dies stellt das Marktversagen dar, welches sich bei Eintreten der vollständigen Beherrschung des Contents durch eine der beiden Parteien ergibt:

Einerseits gingen die Anreize verloren neuen Content zu schaffen, wenn mit seiner Hilfe kein Gewinn erzielt werden kann, womit die Volkswirtschaft suboptimal arbeitet. Dies wäre der Fall, wenn Daten nicht mehr vermarktbar wären, d.h. die illegalen Kopierer das Tauziehen gewinnen würden.

Wenn die Produzenten andererseits hingegen monopolistisch über den Content verfügen dürften, würden sie, wie in einer Monopolsituation üblich die Ausbringungsmenge reduzieren, womit die Gesellschaft mit Informationen (Content) unterversorgt würde, und es zu einer digitalen Spaltung der Gesellschaft käme.

Damit keiner der beiden Fälle eintreten kann, ist der Staat nun gefordert. Er muss Regeln schaffen, innerhalb derer sowohl die Produzenten vor der Umgehung ihrer Schutzsysteme, sowie die Verbraucher vor der totalen Kontrolle des Contents geschützt werden, d.h. es muss ein faires, durchsetzbares System geschaffen werden.

Im Moment ist die Flasche noch stark zur Seite der illegalen Nutzer gekippt, weshalb in den Medien vielfach über neuere und schärfere Regelungen im Informationsbereich diskutiert wird. Doch ist es wichtig, gleich von Vorneherein eine vorausschauende und gerechte Regelung zu treffen, die ein faires DRM-System in ausreichendem Maß schützt. Die ausgestalteten Vorschläge finden sich gegen Ende der Arbeit im Kapitel 13 „Anpassung der rechtlichen Situation“.

Die wichtigste Erkenntnis, die aus dem Modell gewonnen werden kann, ist die, dass es eine ganzheitliche Strategie geben muss, die durch eine parallele Entwicklung von Recht und Technik vorangetrieben wird. Und genau das versucht diese Arbeit mit dem ausgearbeiteten Entwurf zu schaffen: Ein faires System, welche das Recht integriert, und daher durch es unterstützt wird, wobei der Kunde gleichzeitig ein gutes Gefühl haben kann, dass seine Anonymität durch eine unabhängige staatliche Institution gewährleistet wird.

7.3 Totaler Stop von illegalen Kopien

Abschließend in diesem Kapitel soll nun die Kernfrage, ob bei Daten die derartige vervielfältigungstechnische Eigenheiten aufweisen, wie die digitalen Daten, je ein einhundertprozentiger Schutz bestehen kann, thematisiert werden. Und die Antwort muss klar „Nein“ lauten.

Denn sobald Daten für den Menschen wahrnehmbar werden, lassen sie sich spätestens über den Umweg eines analogen Gerätes kopieren. Ein anderer Fall sind zwar maschinenlesbare Daten, doch auch bei diesen besteht immer die theoretische Chance, dass sie entschlüsselt werden, da sie bei Ihrem Weg zwischen Hersteller und Verwender mit dem Internet einen unsicheren Bereich passieren müssen. Außerdem bilden maschinenlesbare Daten, die gleichzeitig vom Urheberrecht geschützt sind nur eine kleine Untermenge, nämlich die der Computerprogramme. Alle anderen Datenarten werden irgendwann für den Konsum durch den Menschen aufbereitet. Damit wird also die Suche nach einer Strategie notwendig, wie man mit dieser Tatsache des fehlenden Schutzes umgeht.

Dies ist das Kernproblem aller älteren DRM-Systeme, die teilweise noch von einer Erreichbarkeit eines solchen Schutzes ausgehen. In dieser Arbeit soll nun ein Grundstein für ein modernes DRM-System gelegt werden. Die Wirtschaftlichkeit steht wie so häufig, auf einem anderen Blatt.

7.4 Implikationen für das UGS-DRMS

Aus der vorangegangenen Definition des Darknets und den Implikationen des „tilting bottle“-Modells wird klar, dass nur ein Konzept, welches alle drei Säulen eines DRMS in gleicher Weise bedient (Recht, Wirtschaft, Technik) Erfolg haben kann. Jede Säule muss gleich lang sein, damit das darauf ruhende Konstrukt einen Stand hat, so fragil er auch in dem Moment noch ist. Denn erst mit ausreichender sozialer Akzeptanz wirkt das Gebilde auch stabil.

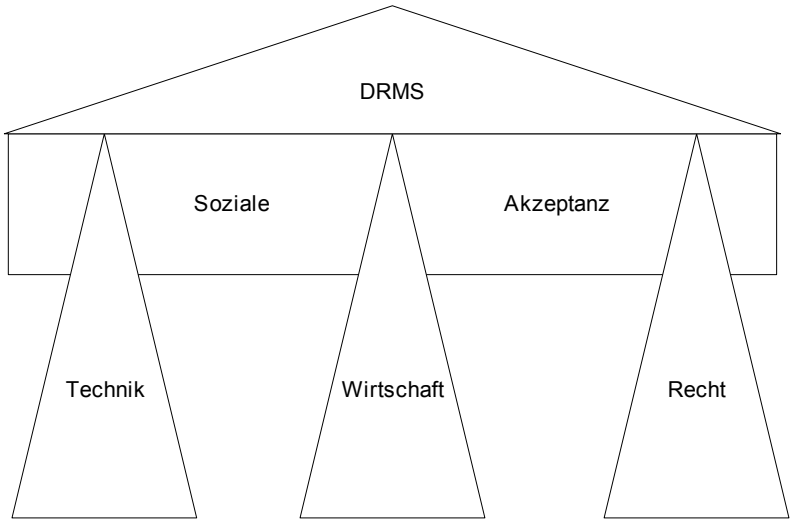

Abbildung 5: Stabilisiertes DRMS

Nicht zu vergessen ist dabei die engmaschige Vernetzung dieser vier Bauteile. Jedes hat einen Einfluss auf die anderen drei:

Zu sehr die Freiheit einschränkende technische Maßnahmen kosten zum einen viel Geld in der Entwicklung, was auf Kosten der sozialen Akzeptanz und der Wirtschaftlichkeit geht. Letztere ist ohnehin stark mit den Schutzmaßnahmen verknüpft: Zu schwache TPM fördern das illegale Kopieren, kosten aber wiederum wenig Geld und fördern die soziale Akzeptanz. Zu starke TPM fordern außerdem das eingreifen des Staates, der sie regulieren muss.

Das Eingreifen des Staates kostet wiederum in jeder Form Geld, was die volkswirtschaftliche Qualität eines DRMS schwächen kann. Außerdem kosten beschlossene Maßnahmen zur Regelung von DRMS die Unternehmen Geld, da sie Ihre Systeme dieses Regelungen konform bauen müssen. Dies hat wiederum Auswirkungen auf die Technik. So könnten manche Lösungen vielleicht funktionieren, würden aber geltenden Gesetzen widersprechen, d.h. es bestünde die Gefahr einer Überregulierung ebenso wie die einer Unterregulierung.

Ein zweischneidiges Schwert ist die soziale Akzeptanz. An diese zu gelangen ist für die meisten DRMS wohl sehr schwer und zwingt sie zur unterhalb ihrer technischen Möglichkeiten zu bleiben. Doch ohne ausreichende soziale Akzeptanz ist die Etablierung eines DRMS nahezu unmöglich (außer per staatlichem Dekret im öffentlichen Bereich). Es erfordert Feinabstimmungen, sowohl im staatlichen, technischen wie auch wirtschaftlichem Bereich.

Die vierte Säule ist schließlich die Wirtschaft und damit auch die Triebfeder für alles. Bei einer zu geringen oder gar ganz fehlenden Aussicht auf Gewinn werden Investitionen in immaterielle Güter gar nicht

erst getätigt. Und dies wäre einer der beiden angesprochenen schlechtesten Fälle. Um nun eine gewisse Wirtschaftlichkeit garantieren zu können, muss die soziale Akzeptanz eines Systems mit angemessenen Entwicklungskosten zusammenkommen. Und das Ganze muss durch den Staat unterstützt werden.

Wie an diesem Punkt schön zu sehen ist, gibt es auf allen vier Säulen nur einen geringen Spielraum. Um ein funktionierenden DRMS zu schaffen. Während die Wirtschaftlichkeit im Rahmen dieser arbeit nicht beurteilt werden kann, soll zumindest versucht werden, das Zusammenwirken der drei anderen Säulen zu optimieren, was nun in den folgenden Kapiteln passieren wird.

8 Aufbau eines DRMS

Um der Problematik der illegalen, digitalen Kopien vorzubeugen, entstand die Idee des Digital Rights Management[176]. Hierbei sollten die digitalen Daten mit einem Schutz versehen werden, und so nur dem jeweils berechtigten[177] Nutzer Zugang gewähren. Ein DRM-System besteht also zunächst aus drei Kernkomponenten - einem Schutzmechanismus, bzw. der Verschlüsselung einer Datei, die sich nur mit einem gültigen Schlüssel anzeigen und verwerten lässt, einer Möglichkeit, den Daten verwaltungstechnische Metainformationen beizumengen, welche die genauen Umstände[178] der Datenverwendung bestimmen, sowie drittens einem Anzeige- oder Abspielprogramm, welches einen konsistenten Ablauf garantiert. Diese Komponenten lassen sich noch sinnvoll erweitern, was in einem anschließenden Kapitel angesprochen wird.

In einem solchen System finden sich wiederum vielfältigste Möglichkeiten und Ansatzpunkte für einen maliziösen Verwender. Außerdem bedeutet ein sicheres System wie im vorangegangenen Kapitel aufgezeigt nicht zwangsläufig auch einen Markterfolg. Somit muss das System den äußeren Bedürfnissen eines sehr dynamischen Marktes, den Computerbenutzern, angepasst werden. Dieser Markt bringt einige wesentliche Probleme mit sich auf die in einem folgenden Kapitel näher eingegangen wird.

Als besonderer Punkt kommt noch die angesprochene soziale Akzeptanz als Komponente hinzu. Außerdem kennen sich die meisten Computerbesitzer und –nutzer noch nicht ausreichend aus um ihre Geräte mit hinreichender Sicherheit zu bedienen. Dadurch schüren sich teils unbegründete Ängste, die sich bei verantwortungsbewusstem Umgang erübrigen würden.

In den nächsten Kapiteln folgt nun eine ausführliche Analyse der angesprochenen Bereiche, bei denen ein „Standard“-DRMS, wie es in der Praxis vorkommt, häufig krankt. Zudem werden direkt im Anschluss an das jeweilige Kapitel mögliche Lösungen aufgezeigt und eine Designentscheidung für das hier zu entwickelnde System getroffen.

[176] DRM; zu deutsch etwa: digitale Rechteverwaltung.
[177] Das „Rights“ im DRM steht nicht etwa für eine juristische Seite, die zweifelsohne auch daran beteiligt ist, sondern für Nutzungsrechte bzw. Lizenzen an digitalem Content, die durch ein DRMS vergeben werden.
[178] Ort, Zeit, Zweck usw. – der Kreativität sind keine Grenzen gesetzt.

8.1 Schutz von Daten

Der Schutz der Daten stellt trotz aller Verwundbarkeit die zentrale und gleichzeitig die essentiellste Komponente eines DRMS dar, weil diese Daten, so sie einmal in ungeschützter Form akquirierbar werden, nie wieder schützbar sind. Dies sieht man schön am Beispiel der bereits erwähnten Tauschbörsen. Neuere Content-Formate bzw. neuere, kopiergeschützte Musikstücke kursieren bereits kurz nach ihrem Erscheinungstermin im Internet. Allerdings in weitaus geringerer Zahl als freie Stücke (als Beispiel seien hier mit dem DRM-System des Windows Media Player[179] geschützte Filme oder Musikstücke genannt).

Sobald es den sog. Codebrechern jedoch gelungen ist, den Schutz zu brechen, beispielsweise durch ein Entschlüsselungsprogramm, oder zu umgehen, beispielsweise durch ein alternatives Abspielprogramm, welches beigefügte Metainformationen ignoriert bzw. uminterpretiert, steigt die Zahl der vorhandenen Quellen. Sobald genügend Quellen vorhanden sind, wird es technisch und praktisch unmöglich den weiteren Verbreitungsvorgang zu unterbinden (siehe auch Kapitel Tauschbörsen). Hieraus folgt die erste Hürde, die bei der Konzeption eines DRM-Systems zu beachten ist:

Wie im Kapitel über die Kryptografie erwähnt, ist es auf Dauer unmöglich, dass ein Code Bestand hat. Damit ergeben sich im Wesentlichen vier Möglichkeiten:

Totale Prävention

Ein System mit dem Anspruch der totalen Prävention würde verhindern, dass ein verschlüsselter Container in die Hände der Verletzer fällt. Da sich generell nicht zwischen Verletzern und normalem Kunden unterscheiden lässt, müssten alle Kunden als potentielle Verletzer betrachtet werden. Eine Sichtweise der sich der normale Kunde nicht ausgesetzt sehen will. Das System müsste also verborgen sein, sicher, dennoch hochperformant und nicht zuletzt auch erschwinglich. Zusammen mit dem Problem, dass spätestens bei der Verwendung durch den Kunden das Produkt final entschlüsselt werden muss, und hier auf jeden Fall zumindest mittels Digital-Analog-Digital-Wandlung, meist noch mit weiteren Methoden eine Kopie des Werkstücks ohne Verschlüsselung erzeugt werden kann, ist diese Methode nicht praktikabel.

Modular austauschbare Verschlüsselung

In die gleiche Richtung geht der Ansatz, die Verschlüsselungsalgorithmen modular und damit austauschbar in ein Hauptprogramm zu integrieren. Sobald ein Mechanismus zur Verschlüsselung geknackt wurde, bzw. auch in bestimmten Abständen um der Entschlüsselung

[179] Dateien mit Endung *.wmv; ab Version 9 des WMP werden DRM-Komponenten integrierbar.

vorzubeugen, wird durch ein einfaches Update, welches auch per Internet installiert werden kann, die Daten mit neuer Sicherheit versehen. In diesem Fall ist der Kostenfaktor allerdings sehr hoch, da parallel zur Verwendung eines Mechanismus' dieser bereits verbessert wird um zukünftige Generationen von Daten zu schützen. Auch hier zeigt sich wieder die Gefahr der nahezu verlustlosen DAD-Wandlung. Zudem kann nicht gewährleistet werden, dass das Programm auch wirklich in regelmäßigen Abständen aktualisiert wird, wenn man nicht den Benutzer bspw. durch ablaufende Gültigkeiten seiner Dateien oder vertraglich dazu veranlasst, was wiederum zu einem Akzeptanzproblem führen würde.

Sichere Systeme

Eine komplexere Variante des modularen Schutzes ist die Schaffung einer sicheren Umgebung[180], in der die Daten gar nicht geknackt werden können. Hierzu ist allerdings eine Verzahnung von Hard- und Software vonnöten, ein System „aus einem Guss". Ein Beispiel für ein solches System ist der von Microsoft geplante, allerdings bis heute nie in die Praxis umgesetzte TCPA-Chip „Palladium" bzw. dessen Nachfolger von der Trusted Computing Group[181] (TCG). Der Benutzer des Computers gibt dabei einen großen Teil seines Selbstbestimmungsrechtes über diesen ab. Somit stehen die meisten Nutzer einem solchen System denkbar skeptisch gegenüber, was die Einführungshürde für das dahinter stehende DRM-System um so stärker ins Gewicht fallen lässt.

Nichtbeachtung

Die letzte Möglichkeit besteht ganz einfach darin, den Fortschritt der Codebrecher und Piraten zu ignorieren und seine Geschäftsstrategie anzupassen, damit man einem unaufhaltsamen Prozess nicht direkt entgegentritt, sondern ihn eher zu seinen Gunsten umlenkt[182]. So trivial und unrentabel diese Methode auch scheinen mag, sie hat ihre nicht von der Hand zu weisenden Vorteile, wie auch immer man sie gestaltet. Durch den enormen Kostenrückgang bei Verzicht auf die Entwicklung von Kopierschutzmaßnahmen und die höhere soziale Akzeptanz eines solchen Systems könnte langfristig ein Gewinnwachstum erreicht werden.

Ein interessantes Beispiel dafür, dass diese Methode durchaus Potential haben kann, zeigt die Presseverlautbarung von Sony vom 3. Oktober 2004[183], in welcher Sony bekannt gibt, ab November 2004 zumindest vorerst in Japan wieder vollständig auf einen Kopierschutz für Audio-

[180] Siehe auch Kapitel 6.3
[181] Aus der TCPA hervorgegangen. Hat vermutlich größere Chance auf Erfolg, da die wesentlichen Unternehmen der Computerbranche daran beteiligt sind.
[182] So geschehen durch Bill Gates, der hauptsächlich durch das geschickte Ausnutzen von raubkopierten Windows-Versionen zu einer Marktabdeckung von zeitweise über 90 % kam.
[183] Siehe auch: „Sony Music Japan verzichtet auf Kopierschutz" http://www.heise.de/newsticker/meldung/51755

CDs verzichten zu wollen, da die dortige Bevölkerung durch die strengeren Gesetze ein erhöhtes Unrechtbewusstsein aufgebaut habe.

Da eine ausführliche wirtschaftlich Betrachtung aller Möglichkeiten den Rahmen dieser Diplomarbeit bei weitem sprengen würden, sollen nur ein paar weitere Denkanstöße gegeben werden. Manche der nachfolgenden weiterführenden Ansätze können auch mit obigen Methoden kombiniert werden, um ein leistungsfähigeres, geschütztes System zu schaffen.

8.1.1 Weiterführende Ansätze

Niedrige Preise

Nachdem in den Grundlagen der Kostenvorteil bei Generierung und Vervielfältigung der digitalen Daten besprochen wurde, könnte ein Weg dahin gehen, diesen Vorteil an den Kunden weiterzugeben, indem die Preise aktiv gesenkt werden[184]. Ein genaues Maß anzugeben ist ohne umfangreiche Rechnungen anzustellen schlichtweg unmöglich, doch durch sich verringernde Kosten im Kryptografie- und Infrastruktur-bereich, die sich durch den Wegfall des Wettrüstens mit den Content-Piraten ergeben, dürfte in Verbindung mit dem größeren Zielmarkt[185] ein deutlich geringeres Preisniveau anzusetzen möglich sein.

Dies erfordert natürlich auch ein Umdenken der Content-Industrie, die im Gegensatz zu anderen Branchen die letzten Jahre hindurch stetig sich auf hohem Niveau befand, und daher entsprechend verwöhnt ist, was einen nun folgenden Umsatzrückgang betrifft.

Doch auch hier gibt es einen typischen Verlauf der Verkäufe, wenn man beispielsweise ein aktuelles Werk nimmt, wie den Band des Zyklus über einen Zauberlehrling[186]. Das neuste Buch gab es bereits weniger als 24 Stunden nach Veröffentlichung im Internet. Der Verkauf litt nicht im geringsten darunter, und zwar durch den angemessenen Preis. Um sich ein Buch von über 800 Seiten in einer ähnlichen Qualität wie das Original selbst herzustellen, bedarf es eines solchen Aufwandes, dass man gleich zum Laden gehen kann und es sich dort kaufen.

[184] Hier gab es ein interessantes Modell eines Warenhauses [38], dass den Preis seiner Produkte nach dessen Gesamtverkaufszahl gestaffelt hat. Damit profitieren alle Kunden gleichzeitig von einem Markterfolg. Vorausgesetzt, das Abrechnungsmodell des DRMS setzt das auch direkt um.

[185] Durch den niedrigeren Preis werden mehr Käufer, und zwar genau die, die ihren Wunschpreis zwischen dem alten und dem neuen Preis gesetzt haben, das Produkt kaufen. Zudem wird das Produkt durch Wegfall der verschiedenen Einschränkungen, die sich auf technischer Seite ergeben haben, stark aufgewertet.

[186] Der Kenner wird vermuten: Harry Potter von J.K. Rowling. Hier am Beispiel des fünften Bandes „Harry Potter und der Orden des Phönix“. Die erste Kopie wurde am Tag des englischen Verkaufstarts (21.06.2003 um Mitternacht) bereits um 20 Uhr vom Autor in Emule gefunden. Siehe dazu auch [39]

Sicherlich kann es nicht angemessen sein eine CD mit Musik für etwa 1 Euro zu verkaufen, was den Eigenkosten des Raubkopierers entspräche, doch liegt der reale Preis oft bei weit über 1500 % selbiger. Und alles was diese CD einer selbst gebrannten voraus hat, sind ein Inlay und die Legalität. Man sollte meinen das letztere an sich schon einen Anreiz darstellen sollte, doch greift hier wieder das fehlende Unrechtsbewusstsein der Internetnutzer betreffend des „freien" Contents in Tauschbörsen, welches sich durch die zu lange Duldung des Missbrauchs eingegraben hat.

Mehrwertdienste

Ein weitere Ansatz bringt das Schlagwort „Value added services" (VAS)[187] mit sich, welcher bisher mit Ausnahme der Filmbranche noch stark vernachlässigt wird. Dabei werden zu dem eigentlichen Produkt, welches der Kunde erwirbt Zusatzleistungen angeboten, bei einem Film können dies bspw. Making-Ofs oder zusätzliche Szenen sein, bei Musik bspw. Bonus-Stücke die bereits in einem speziellen Format vorliegen, damit sie nicht ebenfalls kopiert werden können. Oder auch die Tatsache, dass die Stücke bereits in einem festplattentauglichen, geschützten Format vorliegen, da eine Konvertierung den durchschnittlichen Nutzer vor größere Probleme stellt, den durchschnittlichen Piraten allerdings in Sekunden von der Hand geht. Besonders geeignet hierfür sind natürlich dingliche Materialien, die man bei Kopiervorgängen nicht oder nur unter hohem Aufwand kopieren und verbreiten kann.

Auch dies wäre mit einer Abkehr von der bisherigen Philosophie verbunden, nach der das Produkt selbst den Wert darstellt. Sie könnten allerdings ähnlich wie die niedrigeren Preise durch die geringeren Kosten gegenfinanziert werden, und rechnen sich wiederum durch die höheren Verkaufszahlen. Zur Zeit gibt es einen Feldversuch der Musikindustrie, der zwar einen Fortschritt darstellt, allerdings den Begriff VAS noch nicht ganz korrekt interpretiert. So wird nicht etwa ein bestehendes Produkt mit zusätzlichem Material ausgestattet, zu gleichem Preis, sondern der Preis variabel gestaltet. So kostet eine CD ohne Inlay weniger als die Standardversion, sowie eine CD mit Extras mehr als die Standardversion der CD. Damit wird lediglich die Methodik der Preisdiskriminierung aufgegriffen, doch nicht wirklich ein Schritt auf den Nutzer zu getan, was notwendig wäre.

Information als temporäres Produkt

Der letzte Punkt, der mit einer Paradigmenwechsel verbunden ist, ist der momentan zumindest in der Musikindustrie gängigste Ansatz: CDs werden mit immer neuen Kopierschutzmechanismen versehen, die nach einer gewissen Zeit ablaufen[188]. Im Moment wird dieses Knacken der geschützten CDs als Negativpunkt gesehen (was es auch durchaus ist),

[187] zu deutsch in etwa: „Wertsteigernde Zusatzleistungen"
[188] Dies geschieht nicht absichtlich, sondern das Ablaufen des Schutzes ergibt sich in der Praxis.

daher werden die Schutzmechanismen immer restriktiver. Dies hat allerdings auch zur Folge, dass eine große Zahl an Privatkunden Probleme mit dem Abspielen von CDs bekommt. Was natürlich die Moral des Käufers senkt. Dieses etwas glücklose Tauziehen wurde in den Grundlagen über das „tilting bottle“-Modell[189] bereits näher erläutert.

Der Knackpunkt ist wiederum, dass der Fokus auf dem Content als Produkt liegt, aber für diesen Ansatz auf der Aktualität des Produkts liegen sollte. Als Beispiel seien hier Nachrichtenagenturen oder auch Börsendienste genannt. Diesen genügt eine marginale Verschlüsselung ihrer Daten, da diese bereits nach wenigen Minuten bzw. sogar Sekunden an Aktualität und somit an Wert verlieren.

Im Bereich der Filme, der Musik oder auch der Literatur ist diese Zeitspanne sicherlich größer. Hier verlieren manche Werke nie oder nur marginal an Wert. Auch hier gibt es die oben angesprochen Verkaufskurven. Die Verkaufszahlen nehmen je nach Bekanntheit des Produktes mehr oder weniger schnell zu, steigern sich zu einem Maximum und nähern sich dann über Jahre hinweg der Null wieder[190]. Der Paradigmenwechsel bestünde nun darin, die Aktualität der Waren zu vermarkten. Prinzipiell würde es genügen, den Schutz der Daten so lange zu gewährleisten, dass das Gros der Verkäufe getätigt wird. Der prozentuale Verlust durch spätere Raubkopien wäre deutlich niedriger.

8.1.2 Zusätzliche Entwicklungen für Synergieeffekte

Rechtliche Anpassung

Parallel zu den genannten Schutzstrategien können (und müssen) zwei weitere Ansätze verfolgt werden. Zunächst muss die rechtliche Umgebung den Erfordernissen digitaler Daten angepasst werden. Ein erster Schritt wurde mit dem ersten Korb der Urheberrechtsnovelle getan. Doch der Prozess ist noch nicht abgeschlossen. Einen Überblick über die genauen Veränderungen findet sich im Kapitel 4.5.1, welches die rechtlichen Grundlagen abschließt.

Hier ist es besonders wichtig, nicht die von der Industrie geforderten drakonischen Strafen zu wählen, da diese nur zu einer Kriminalisierung der Bevölkerung beitragen, den professionellen Content-Piraten jedoch ebenso wenig vom illegalen Kopieren abhalten, wie einen Räuber das Heraufsetzen des Straflimits von fünf Jahren auf zehn Jahre vom Raub abhält. Im Normalfall gehen diese Täter davon aus nicht erwischt zu werden. Zu hohe Strafen mögen zwar in Ausnahmefällen in der Bevölkerung das in diesem Gebiet nicht vorhandene Unrechts-

[189] Siehe hierzu auch [40]
[190] Sofern es nicht durch sog. Revivals zu erneuten Umsatzsteigerungen kommt. Hierzu zählen unter anderem Verfilmungen eines Buches, Fortsetzungen, Cover-Versionen von Hits usw.

bewusstsein zu wecken, doch muss in diesem Fall als Ausgleich auch ein gewisser rechtlich gesicherter Freiraum geschaffen werden, wie ihn die Privatkopie bietet. Und nicht zuletzt müssen gesetzliche Schranken in beide Richtungen wirken, wie bereits im „tilting bottle“-Modell beschrieben, da sonst der Normalbürger sich nicht auf ein DRM-System einlassen wird. Daher bietet es sich an, die Schranken direkt in das DRM-System zu integrieren, was in dieser Arbeit unter anderem umgesetzt werden soll.

Parallel dazu sollte das Unrechtbewusstsein der Nutzer weiter geweckt werden. Sei es durch Werbekampagnen von Interessenverbänden, oder sei es durch eine konsistente und nicht etwa übertriebene Strafverfolgung.

Motivationssysteme

Eine letzte Strategie, die parallel zu den angesprochenen Schutzstrategien verwendet werden sollte, ist die Idee eines speziellen Motivationssystems, welches den Nutzer für eine bestimmungsgemäße Verwendung des Systems bzw. seine Verbreitung entlohnt. Sie fällt eher unter die sozialen Komponenten, und wird daher im zugehörigen Kapitel erläutert.

8.2 Managementinformation

Eine zweite, wesentliche Komponente, wenn auch nicht von vergleichbarer Wichtigkeit, wie der zuvor besprochene Schutzmechanismus, da ihm eher untergeordnet, sind die Metainformationen und die Art, wie sie den Daten beigefügt werden. Zum einen können sie zusammen mit den Daten transportiert werden, zum anderen können sie von ihnen getrennt aufbewahrt werden. In die erste Kategorie fallen auch die zur Identifizierung des Nutzers nötigen Zusatzdaten. Sie werden vor allem mittels Wasserzeichen in die digitalen Daten selbst aufgenommen und sind praktisch gesehen keine Beifügung mehr.

Metadaten als Teil des Datencontainers

Die erste erwähnte Methode der Metadatenbeimengung hängt stark von einem funktionierenden Schutzsystem ab, eröffnet allerdings ein genaueres Differenzieren der zu übertragenden Rechte. Um nichts anderes geht es ja beim zur Verfügung stellen von Daten, wie schon in den rechtlichen Grundlagen erläutert wurde. Nach einer vertraglichen Einigung auf entsprechende Nutzungsziele und den damit verbundenen Rechtsübertragungen können diese eins zu eins umgesetzt werden. Beispiele hierfür sind das einmalige Anschauen von Filmen, das Hören eines Liedes für 24 Stunden, oder auch das Drucken eines geschützten Dokumentes.

Wie schon erwähnt liegt hier das Problem darin, dass die Metadaten zumeist im (leicht editierbaren) Klartext vorliegen, und erst zusammen

mit den Daten verschlüsselt werden. Im Normalfall benötigt man die Metadaten nach der Entschlüsselung der Kerndaten nicht mehr, da selbige nun ebenfalls im Klartext vorliegen. Doch kann man den Prozess des Entschlüsseln zumeist einfach rückgängig machen, so man ihn einmal nachvollzogen hat, und würde dadurch voll funktionsfähige Container erhalten, die auf der sicheren Plattform bzw. dem sicheren Abspielprogramm funktionieren. Damit könnte man die vom legitimen Anbieter selbst geschaffenen Infrastrukturen verwenden, das natürlich nicht in dessen Sinn sein kann. Auch lassen sich aus der Struktur der Metadaten eventuell Ansätze für zukünftige Hack-Versuche gewinnen.

Im Prinzip lässt sich das Problem durch eine zusätzliche, eigene Verschlüsselung der Metadaten klären, doch würde man dafür einen vom Hauptverschlüsselungsalgorithmus differierenden Algorithmus benötigen, da der Angreifer, der so weit kommt, dann wohl auch keine Probleme haben dürfte, ein zweites Mal den gleichen Algorithmus zu knacken[191]. Damit würden sich die Generierungszeiten und –kosten eines solchen Containers schlagartig verdoppeln.

Zeitkritische Anforderung von Lizenzen

Die zweite Möglichkeit erfordert die Unterstützung des Internets oder eines vergleichbaren Netzes[192]. Dabei werden die Metadaten von den Daten getrennt gehalten, und direkt bei Verwendung in Form eines für das Abspielprogramm lesbaren Pakets an den Computer gesendet. Ein solches Paket würde die Rohstoffe zur Schlüsselgenerierung für die Daten enthalten, das Abspielprogramm würde bspw. aus einem Timestamp[193], einem Longterm-Key[194] und der Identifikationsnummer des Nutzers einen Schlüssel selbst generieren, oder durch einen Server generieren lassen, der in der Domain des Rechteinhabers steht, und im Normalfall die eindeutig höhere Sicherheit bietet.

Es besteht auch die Möglichkeit, die Metadaten in verschlüsselter Form bei Bezahlung auf den Computer zu laden. Diese Methode wäre im Gegensatz zur vorgenannten nicht zeitkritisch, doch besteht damit die Möglichkeit ein noch gültiges Paket zu cracken und vielleicht zu manipulieren, während im erstgenannten Fall die Informationen wenige Sekunden ihre Gültigkeit behalten und gleich verwendet werden.

---

[191] Vorausgesetzt der Angreifer hatte keine Hilfe von „innen“ bzw. einen bekannten Anker innerhalb des Containers, an dem er seine Kryptoanalyse ansetzen konnte.

[192] Als Beispiel sei hier ein Mobilfunknetz angedacht. Die Daten könnten per GPRS oder UMTS zu dem Handy gelangen, und dort per Bluetooth wieder zum Computer zurück.

[193] Timestamp: Eine zeitlich Momentaufnahme. Diese soll sicherstellen, dass alte Schlüsseldaten nicht wiederholt verwendet werden können.

[194] Mit diesem langfristigen Schlüssel kann sich das Programm einen auf einem Server gespeicherten Schlüssel mit den den Metadaten entsprechenden Eigenschaften abholen.

Bewertung

Heutzutage ist die erste Methode die gängigere, Daten werden mit verschiedenen Metadatenformaten gekoppelt. Als Beispiele seien hier zu nennen: XrML, ODRL und andere.

Für das hier generierte Programm wird, aufgrund der Entscheidung für ein Hybridsystem[195], welches auch ohne Online-Unterstützung funktionieren soll, ebenfalls der erste Ansatz gewählt werden, auch wenn dessen Sicherheit geringer ist.

8.3 Herstellung des Bezugs zwischen Nutzer und Daten

Ein weiterer wichtiger Punkt ist die Abschreckung maliziöser Verwender durch die Rückverfolgbarkeit der Daten zu dem ursprünglich berechtigten Nutzer, von dem der Missbrauch ausgegangen sein muss.

Hier kommen Wasserzeichen ins Spiel. Ihre Funktionsweise wurde bereits im entsprechenden Kapitel in den technischen Grundlagen erklärt. Daher soll nun kurz darauf eingegangen werden, welchen Wert sie für ein DRM-System haben. Wie noch genauer betrachtet wird, gibt es neben dem professionellen Angriff eines Content-Piraten, der allerdings keinerlei Probleme haben dürfte, sich über das Problem Wasserzeichen hinweg zu helfen, noch eine zweite große Gruppe von Rechteverletzern: Die privaten Nutzer.

Die mit Wasserzeichen versehenen Daten tragen den Namen bzw. die Identifikation des rechtmäßigen Nutzers wie eine unsichtbare und unfälschbare Unterschrift mit sich. Die erwähnten Möglichkeiten der professionellen Piraten stehen einem privaten Nutzer nur selten zur Verfügung, da sie einiges an Technik und auch Know-how voraussetzen. Damit geht der Nutzer bei Weitergabe der Daten immer die Gefahr ein, dass die mit seinen Informationen versehenen Daten an die Öffentlichkeit gelangen, was unter den Tatbestand der unrechtmäßigen Verbreitung fällt. Der Nutzer beginnt dadurch den Kreis seiner „Freunde“ enger zu ziehen, er nutzt die Privatkopie im vorgesehenen Rahmen. D.h. die Wasserzeichen haben einen erzieherischen Effekt.

Natürlich darf der unbedarfte Nutzer, dessen Daten durch eine Straftat entwendet wurden, nicht belangt werden. Diese Beweislast ist für beide Seiten kritisch, man kann jedoch vom durchschnittlichen Nutzer nicht erwarten, dass er es schafft, einen Beweis über Angriffe auf seinen Computer zu führen. Interessant wäre hier der Ansatz, die Identifikation des Nutzers, der die Kopie erhält, automatisch mit in die Metadaten zu übernehmen, beispielsweise durch eine einmalige Authentifizierung der

[195] Siehe Kapitel 9.1.3

Datei durch den Erstnutzer. Doch auch hier hinge der Erfolg dieser Maßnahme im Wesentlichen von einer fehlerfreien Funktion des Schutzmechanismus' ab, welcher ja nur unter sehr engen Umständen gegeben ist.

Nichtsdestotrotz bilden Wasserzeichen ein weiteres Hindernis für illegale Nutzung, und sind daher sehr wichtig für ein DRM-System, da sie das einzige Mittel sind, die Metadaten im Idealfall unextrahierbar und unlöschbar mit dem Content zu verbinden und auch die Analoge Lücke zu überwinden.

8.4 Das Abspielprogramm

Als einzige Schnittstelle des berechtigten Nutzers zu dem DRM-System muss das Abspielprogramm die meisten ablaufenden Prozesse kaschieren, damit der Nutzer im Idealfall keinen Unterschied zwischen einer geschützten und einer ungeschützten Datei merkt. Gleichzeitig muss das Abspielprogramm die gesamten Sicherheitsvorkehrungen beinhalten und wird noch den meisten Crackangriffen ausgesetzt sein, da es die Komponenten ist, die mit dem Nutzer im direkten Kontakt steht.

Da die Umstände der sozialen Akzeptanz direkt im Anschluss näher erläutert werden, sollen hier nur Stichpunkte genannt werden, die das Abspielprogramm eines DRMS erfüllen kann und soll.

Da ist zunächst der bereits angesprochene Komfort für den Nutzer zu nennen. Ein Programm, welches aus Sicht des Nutzers an unnötiger Kompliziertheit krankt, wird ein solcher nur ungern benutzen. Das heißt, das Programm muss eine intuitive Bedienungsoberfläche haben, die verschiedenen Authentifikations-Prozesse müssen nahezu ohne Nutzerinteraktion ablaufen. Im Prinzip sollte es sich außer einer einmaligen Identifikation des Nutzers nicht von einem gewöhnlichen Abspielprogramm unterscheiden. Daher wäre eine Integration in bestehende, weit verbreitete Abspielprogramme wie bspw. den Windows Media Player oder den Real Player wünschenswert. Diese unterstützen gleichzeitig noch ein breites Spektrum an verschiedenen, auch ungeschützten Formaten, womit eine Installation von verschiedenen Abspielprogrammen obsolet wird.

Idealerweise solle das Abspielprogramm auch die gesamte Kette bis hin zum virtuellen Laden des Rechteinhabers im Internet, wo man den gewünschten Content erwerben kann, umfassen.

Den Interessen der Rechteinhaber dienen unmittelbar die eingebauten Schutzfunktionen für den Content (sofern ein solches, klassisches System gewählt wurde). Hier gibt es im wesentlichen drei Komponenten:

- Schutz des Contents
- Schutz der Metainformationen
- Schutz des Wasserzeichens

Hier gibt es, wie bereits oben angedeutet, verschiedenste Wege dies zu erreichen, welche sich in ihrer Ausprägung allerdings deutlich unterscheiden. Daher muss dieser Bereich pauschal abgehandelt werden:

Notwendigerweise muss das Abspielprogramm den Mechanismus zur Entschlüsselung der Schutzsysteme enthalten, da sonst dem Nutzer der Content nicht zugänglich gemacht werden könnte. Dieser Mechanismus muss unter allen Umständen gegen eine Kompromittierung geschützt werden. Sei es, dass er seine Stärke aus der Tatsache zieht, dass er geheim ist, oder sei es dass er zwar öffentlich bekannt ist, aber nicht umkehrbar. In beiden Fällen müssen die verschiedensten Schnittstellen gesichert werden, damit bspw. Passwörter nicht im Klartext vorliegen, keine Replay-Attacken[196] u.ä. durchgeführt werden können. Des weiteren muss das Programm so weit modular aufgebaut werden, das im Falle der Kompromittierung nicht die gesamte Infrastruktur nicht mehr verwendbar wird, sondern geknackte Module ausgetauscht werden können.

8.5 Soziale Anforderungen an ein DRMS

Mit dem gerade abgehandelten Unterkapiteln rutscht man bereits in die sozialen Eigenheiten eines DRM-Systems, die beachtet werden müssen. Um es in einem Satz zu formulieren: „Das beste System taugt nichts, wenn es keiner anwendet“. Und ein System aufzuzwingen steht nicht in der Macht der Konzerne, wenn Sie es auch versuchen. An dieser Stelle soll nun versucht werden Anforderungen an ein DRMS zu formulieren, damit Nutzer sich für es entscheiden und nicht für die billigere, illegitime Alternative. Dabei finden sich im wesentlichen sechs Punkte, die immer zu einem Minimum gewährleistet werden müssen. Ein höheres Maß als das jeweils geforderte bringen einem System Bonuspunkte bei den designierten Nutzer ein. Und diese werden vonnöten sein, um ein DRMS auf einem Markt zu etablieren. Die Punkte für eine soziale Akzeptanz sind:

- Anonymität
- Preisliche Gestaltung
- Komfort

[196] Bei diesen Attacken wiederholt man bspw. Anweisungen an das Abspielprogramm mit eigenen Informationen, die man an einer der Schnittstellen abgefangen hat und so erneut verwendet.

- Standardisierung
- Fair Use bzw. Flexibilität
- Zusätzliche Motivation

Anonymität

Die erste und wichtigste Forderung an ein DRMS ist, dass es dem Nutzer die Möglichkeit gibt darüber zu entscheiden, was mit seinen Daten passiert. Es sollte die Möglichkeit geben, sich eine vollkommene Anonymität zu erhalten, wenn es denn gewünscht ist. Man mag vermuten, dass dies doch einfach selbstverständlich müsste. Doch genau das ist es nicht.

Die Produzenten von Content, sowie eigentlich auch alle anderen Firmen haben ein großes Interesse an einem möglichst vollständigen Bild ihres Kunden. Und ein DRMS bietet für sie eine große Chance, an ein Kundenprofil ohne vermehrte Kosten zu gelangen. Dies würde durch einfaches Protokollieren aller Zugriffe auf entsprechende Daten sehr einfach gelingen. Daran scheiden sich jedoch die Geister. Sowohl Verbraucherschützer, wie auch immer mehr Verbraucher selbst lehnen es ab, zu dem von den Medien prophezeiten „gläsernen Menschen“ zu werden. Die Content-Produzenten verlieren auf diese Weise nicht wenige potenzielle Kunden.

Dazu kommt noch das Misstrauen, welches Nutzer den Firmen gegenüber hegen. Da sie keinen Überblick über die tatsächlich implementierten Funktionen in einem DRMS haben, wollen sie sich nicht ausschließlich auf vollmundige Versprechungen der Rechteinhaber verlassen. Es wäre also eine unabhängige Stelle nötig, die das System überprüft und zertifiziert. Hierfür würde sich der Staat oder eine neu ins Leben zu rufende Gesellschaft eignen, welche auch im hier vorgestellten UGS-DRMS eingeführt wird. Möglich wäre auch die Zwischenschaltung einer anonymisierenden Stelle, die das System zwar nicht überprüft, aber verhindert, dass die Kundendaten mit dem jeweiligen Profil in Verbindung gebracht werden können. Damit hätten beide Seiten ihr Idealbild, doch würde dies wieder laufende Kosten verursachen.

Preisliche Gestaltung

Der nächste sehr diffizile Punkt bei der sozialen Akzeptanz eines DRMS ist die preisliche Gestaltung der Lizenzen. Es gibt bereits sehr viele verschiedene normale Systeme[197], die sich bewährt haben, ohne dass das einschränkende Moment, welches ein DRMS in den Augen der Nutzer mit sich bringt, notwendig gewesen wäre. Sicherlich bringt eine minutengenaue Abrechnung eine genaue Anpassung des Nutzers an

[197] Je nach betrachteter Komponente wären hier Abspielprogramme wie den Windows Media Player, Real Player, WinAmp usw. zu nennen, aber auch kostenlose Downloadsysteme von freier Software [41], von Testversionen [42] oder Bezahlsysteme, die online und ohne DRMS funktionieren (verschiedenste Firmen wie bspw. MacAfee)

seine tatsächliche Nutzungsmenge und somit zu dem für ihn idealen Preis.

Doch aus Sicht der Nutzer betrachtet sieht dies ein wenig anders aus: Wenn man eine unbeschränkte Nutzungserlaubnis hat, nutzt man den Content anders, als wenn man ihn kontingentiert bezahlen muss. Außerdem würde wohl kein Content-Produzent aus reiner Freundlichkeit ein solches Modell einführen. Er verspricht sich einen Gewinnzuwachs davon. Und der kommt zwangsläufig über die Nutzer des Systems. Damit sieht die Mehrzahl der Nutzer einen Nachteil in der weiteren Nutzung auf sich zukommen.

Diesem Trend entgegenzusteuern ist schon deutlich schwerer. Schließlich ist die genauere Preisdiskriminierung ein weiterer schwerwiegender Vorteil eines DRMS. Als Idee mag dienen, dass Nutzer die neuen Modelle zusätzlich zu bereits bestehenden erhalten sollten, und nicht anstelle. Es wäre beispielsweise ein deutlicher Rückschritt für einen Kunden, wenn er Musik nur noch gegen genaue Abrechnung hören könnte und nicht mehr ein pauschales, preislich angemessenes Angebot erhielte, welches er in der Praxis durch den Kauf einer CD wahrnehmen kann.

Im hier generierten System wird ein Microbilling-System als Komponente vorerst noch ausgespart, da das Hauptaugenmerk auf der Nutzergruppenspezifität liegt. Ein Nachrüsten wäre aufgrund der vorgesehenen Modularität allerdings technisch unproblematisch[198].

Komfort

Bereits im vorangegangenen Kapitel wurde kurz darauf eingegangen, dass der Komfort für Nutzer eine wesentliche Rolle bei der Akzeptanz eines neuen DRMS ist. Und dies aus nahe liegenden Gründen: Es gibt bereits funktionierende Systeme. Die Nutzer haben kein Bedürfnis für ein DRMS. Daher werden sie den gleichen Komfort von diesem System bei der Verwendung im täglichen Leben verlangen, wie von bereits existenten „Nicht-DRM“-Programmen. Ist das System komplizierter in der Installation oder Verwendung? Wie ist die Portierbarkeit des Systems auf verschiedenen Betriebssystemen[199]?

Diese Punkte betreffen vor allem das Abspielprogramm. Wie schon erwähnt, wird es problematisch alle Prozesse die ablaufen müssen, um das DRMS korrekt in Gang zu halten, verdeckt ablaufen zu lassen. Zumindest der Installationsprozess kann heutzutage sogar für absolute Laien einfachst gestaltet werden, eventuell bei ausreichend vorhandener Download-Kapazität sogar direkt vom Server des Content-Produzenten,

[198] In der Praxis können sich allerdings Probleme mit der Akzeptanz durch den Nutzer ergeben. Siehe hierzu auch Kapitel 10.6

[199] Es würde sich wohl kein Linux-Fan extra ein Windows OS installieren, nur damit er DRM-geschützten Content genießen kann.

ohne dass der Nutzer häufig in den Vorgang eingreifen muss. Dies wird vermutlich durch eine eventuelle Personalisierung des Programms der bevorzugte Ablauf der Installation sein.

Bei der Verwendung ist auf eine möglichst intuitive Bedienbarkeit zu achten, die sich möglichst an vorhandenen (Quasi)Standards orientiert. Außerdem muss das Bedienungsmenü übersichtlich und effizient gestaltet werden, damit nicht gerade die Gruppe der Laien-Nutzer abgeschreckt werden. Der Nutzer muss zudem das Gefühl haben, dass seine Daten sicher sind, wenn er im Internet agiert. Sonst wird er sich nicht zu einer Onlinezahlung bewegen lassen. Und nicht zuletzt sollten auch andere Standardformate, die nicht unbedingt DRM-geschützt sind, unterstützt werden.

Es gibt im Bereich Komfort allerdings noch weitere Punkte zu beachten: Wie einfach ist es, das DRMS zu initialisieren? Es ist bspw. wichtig, dass der Nutzer schnell und unkompliziert von seinem Sessel vor dem Computer aus alle notwendigen Schritte in Gang bringen kann und im Idealfall den erworbenen Content bereits kurz nach Erwerb einer Lizenz nutzen kann. Da das hier vorzustellende System mit einer Hardwarekomponente funktioniert, kann dem leider nicht entsprochen werden, doch bringt es zusätzliche Vorteile im Komfortbereich mit sich.

Standardisierung

Es wurde bereits eine Unterstützung von Standardformaten angesprochen. Die hier erwähnte Standardisierung zielt jedoch in eine etwas andere Richtung:

Man stelle sich vor, die Einführung eines DRMS hätte funktioniert. Da sich der Besitzer des einzig funktionsfähigen DRMS eine goldene Nase durch Lizenzierung etc. verdienen würde, bliebe er auf dem Markt nicht lange alleine. Es würden sich eine Vielzahl verschiedener Systeme entwickeln, die jeweils Kundenkreise aufbauen. Da Content-Produzenten (mit Ausnahme vielleicht einiger weniger großer) sicherlich nicht bei allen Systemen Lizenzierungsgebühr zahlen wollen, müsste sich der Nutzer je nachdem welchen Content er verwenden will bei einer Vielzahl von Systemen anmelden. Im schlechtesten Fall sind diese inkompatibel zu einander. Man kann sich vorstellen, dass diese Situation nicht gerade zu einer breiten Akzeptanz von DRMS durch die Gesellschaft beiträgt.

Einer der wichtigsten Aufgaben der entwickelnden Industrien ist es daher, sich von vorneherein auf gemeinsame Standards zu einigen. Dazu gibt es auch bereits Anläufe. Im Notfall könnte der Staat auch entsprechende Standards vorschreiben, doch dies würde wieder zu einem überhöhten Verwaltungsaufwand führen.

Der letzte Punkt die Standardisierung betreffend ist bereits fach-übergreifend zum fünften Punkt, der Flexibilität: Damit die Nutzer ihren

Content auch auf mobilen Geräten, die zumeist nicht genügend Rechenleistung haben ein komplexes DRS zu unterstützen, verwenden können, muss ein Format bzw. eine Schnittstelle entwickelt werden, welche es erlaubt die Portierung ohne Verlust des Schutzes und auch ohne Einschränkung für den Nutzer vorzunehmen.

Flexibilität

Wie der schwelende Kampf um die Privatkopie zeigt, der im Moment ausgefochten wird, vermuten die Nutzer von Content, dass mit DRMS eine drastische Beschränkung ihrer Rechte einhergeht. Und dies wohl nicht ganz zu unrecht, wie der Versuch der Interessensgemeinschaften der Urheber-Vertreter die Privatkopie abzuschaffen zeigt. Die Nutzer können und wollen nicht verstehen, dass es nicht mehr möglich sein soll, einfach einem Freund ein Lied zu überspielen, mal kurz seine CD mit ins Auto zu nehmen oder Musik auf einem MP3-Player zu hören. Es ginge einfach eine Menge an Flexibilität verloren, wenn es ganz nach dem Wunsch der Content-Industrie geht.

Verständlicherweise hilft so etwas beim Prozess sozialen Akzeptanz nicht sonderlich weiter. Mit dem angesprochenen Paradigmenwechsel, der vorsieht nicht mehr den Content auf einem zugehörigen Computer zu schützen, sondern ihn an die Person des Nutzers zu binden, wird man dem Problem zumindest teilweise Herr. Dadurch kann bei geeigneter Infrastruktur der legitime Nutzer seine Daten in geschützter Form zwischen den Systemen portieren, und auch eine Weitergabe lässt sich problemlos integrieren, was auch in dem UGS-DRMS vorgesehen wird, im Prinzip sogar dessen Kern ist.

Motivation

Ein letzter Punkt ist eigentlich nicht das Überwinden einer Hemmschwelle der Nutzer, sondern vielmehr ein reiner Zusatzpunkt. Da die Nutzer wie beschrieben einem DRMS eher skeptisch gegenüber stehen, könnte man durch ausreichende Motivationssysteme eine Art Initialzündung hervorrufen, die in der momentanen Situation im privat-wirtschaftlichen Bereich auch dringend nötig wäre.

9 Erstellung des UGS-DRMS

Nachdem im vorangegangenen Kapitel der Aufbau, die Probleme und Gründe für das Scheitern von früheren, klassischen DRMS erläutert wurden, wird nun exemplarisch das erwähnte User Group Specific Digital Rights Management System (UGS-DRMS) aufgebaut werden, welches mit dem novellierten und zusätzlich auch vom Autor angepassten Urheberrecht so zusammenarbeiten soll, dass der Gesamtnutzen des Gesellschaft maximiert wird, was ja eines der eigentlichen Ziele des Urheberrechts ist.

Die wesentlichen Komponenten eines solchen Systems sind zunächst einmal die zugangsbegrenzende Verschlüsselung, ein spezielles und sicheres Zahlungssystem (welches allerdings häufig extern zu finden ist, und daher vorerst aus dem System ausgegliedert wird) und nicht zuletzt eine Infrastruktur welches den Zugang des Nutzers zu dem erworbenen Inhalt darstellt. Diese Kernkomponenten können beinahe beliebig erweitert werden, was auch durch die Hinzunahme der technischem Implementierung der gesetzlichen Schrankenregelungen passieren wird.

Zunächst müssen jedoch einige grundlegende Design-Überlegungen erörtert werden.

Als erstes fällt die Entscheidung an, ob eine prinzipielle, nur eine optionale oder gar keine Onlineunterstützung des Systems vorgesehen werden sollte. Dann wird mittels dem Potato-Modell der Universität Ilmenau das Konzept der Superdistribution erläutert. Das dritte Unterkapitel befasst sich mit einigen Eckpunkten, die zu klären sind, wie das Einführen einer Trusted Third Party zur Wahrung der Anonymität. Danach folgt die grundlegende Idee hinter dem nun schon mehrfach angedeuteten Paradigmenwechsel, nämlich die Umstellung des Systems von der klassischen Objekt- auf die neuere Benutzer-orientierung. Und schließlich folgt eine Überlegung, wie denn nun der Zugangsmechanismus zu dem neuen System gestaltet werden soll. Im Zuge dessen wird auch ein PKK-Modell vorgestellt, welches so (noch) nicht existiert, aber für dieses DRMS ideal wäre.

9.1 Online vs. offline

Zu Beginn des Designprozesses muss man sich die Frage nach dem zu Grunde liegenden Konzept stellen. Hierbei lassen sich zwei Bereiche unterscheiden: DRMS, die optional durch eine Online-Verbindung profitieren, mehr Komfort oder auch einfach nur größere Funktionalität erlangen, stellen hierbei den einen Bereich dar. Ihnen ist zu eigen, dass sie auch auf einem völlig autarken Computersystem funktionieren

können. Auf der anderen Seite finden sich Systeme, die zum Betrieb eine stetige Verbindung in das Internet benötigen. Eine bekannte Möglichkeit ist die Errichtung eines Lizenzservers, der zum einen die mit dem Inhalt verknüpften und erworbenen Rechte in Echtzeit vergibt und dabei auch die Integrität des verwendeten Abspielsystems überprüfen kann. Beide Varianten haben ihre Vor- und Nachteile, die allerdings in verschiedenem Maße bei Anwender und Rechteinhaber lokalisiert sind, was ein weiteres Problem beim Einsatz von DRM-Systemen schafft, da beide Seiten natürlich damit an verschiedenen Lösungsmöglichkeiten interessiert sind. Daher müssen auch vom Gesetzgeber verschiedene Gesetzesrahmen für beide Möglichkeiten vorgesehen werden. Doch dazu später mehr. Um zu einer zufrieden stellenden Entscheidung für das Modell zu gelangen, werden in den nächsten Unterkapiteln die verschiedenen Konzepte vorgestellt und hinsichtlich der letztendlichen Online/Offline-Entscheidung bewertet.

9.1.1 Reine Online-Modelle

Bei der ersten Gruppe handelt es sich um DRM-Systeme, bei denen entweder die Abrechnung oder die Integritätsprüfung eine anhaltende Internetverbindung benötigt. Ein solches System hat für die Betreiber mehrere Vorteile:

Durch ständiges Abgleichen der anzuzeigenden Daten bleibt der Rechteinhaber über Zahl, Art und Muster der Verwendungen seines Contents informiert. Gerade mit heutigen Methoden des Data Mining lässt sich hieraus ein detailliertes Kundenbild gewinnen, welches sich beispielsweise für gezielte Werbung einsetzen oder auch verkaufen ließe. Zum anderen wird durch die Internetverbindung, die jeweils aufgebaut wird auch eine Möglichkeit geschaffen die Integrität des abspielenden Programms zu überprüfen. Wie erwähnt ist dies einer der essentiellsten Punkte eines DRM-Systems.

Die hierbei auftretenden Nachteile müssen nahezu ausschließlich von Nutzer getragen werden, was es um so interessanter für den Hersteller macht. Es ist nämlich für den durchschnittlichen Nutzer nicht auszumachen, was alles bei der Integritätsprüfung und auch bei der Verbindung generell an Daten zum Distributor des Contents gesendet wird. Der Nutzer gibt bei diesen Modellen einen Großteil seiner informationellen Selbstbestimmung und auch der Kontrolle über seinem Computer auf. Und das nur für die Möglichkeit auf seinem Computer unter eingeschränkteren Bedingungen als bisher Content anzuzeigen, für den er vermutlich genau so viel bezahlt hat wie bisher. Damit lässt sich der Gedankengang eines durchschnittlichen Nutzers zumindest so weit verfolgen, dass dieser dem System kein Vertrauen schenkt und

somit es auch nicht verwendet. Genau dadurch fallen sämtliche bis dato beschriebenen Vorteile weg.

An Modellen, die in diesen Bereich fallen, sind u.a. feingranulare Pay-per-View/Use-Modelle oder auch Modelle die auf Streaming-Dateiformaten basieren zu nennen. Während die ersteren bei jeder Nutzung beliebig genau abrechnen bzw. die Informationen hierüber senden, was bei aktuellen Systemen wohl im Sekundenbereich, wenn nicht noch darunter, passieren dürfte, müssen letztere eine dauernde Verbindung zum Nutzer aufrechterhalten, da der Content auf diese Weise zum Nutzer gelangt. Der Vorteil bei letzterer Methode ist, dass der Content im Normalfall nicht auf dem PC des Nutzers gespeichert wird, und dieser schon nicht mehr die Möglichkeit hat, die verschlüsselte Datei direkt zu kompromittieren. Erst muss der Datenstrom abgefangen werden, was durch die Nichtmanipulierbarkeit des DRMS aufgrund seiner andauernden Überprüfung über das Internet (fast) unmöglich wird. Somit stünde nur noch die D(A)D-Wandlung zur Verfügung, um eine Kopie zu erstellen.

Ein weiterer, allerdings immer geringer werdender Nachteil für Nutzer und Distributor ist der Kostenfaktor. Doch auf Grund der immer weiteren Verbreitung von sog. Flatrates[200] und der Bestrebung der Industrie die Welt zu „vernetzen“, bieten sich hier genügend Möglichkeiten dem Abhilfe zu schaffen.

Als Fazit lässt sich für diese Gruppe an Modellen der Schluss ziehen, dass es in naher Zukunft eher unwahrscheinlich sein wird, dass sich eine derartige Lösung durchsetzt. Zu stark wiegt der einseitige Vertrauensvorschuss, den der Nutzer dem Hersteller bzw. dem Lizenznehmer des DRM-Systems entgegenbringen muss. Selbst bei einer gesetzlichen Kontrolle durch den Staat. Es wäre natürlich möglich über die Einführung einer vertrauenswürdigen dritten Institution (TTP)[201] nachzudenken. Hierfür käme wieder nur der Staat in Frage, doch im Gegensatz zu Firmen, die sich den Gegebenheiten des Marktes schnell anpassen müssen, ist dieser zu statisch für ein so dynamisches Umfeld. Sämtliche Genehmigungsprozesse laufen zu langsam ab, was bei einer geschätzten Einsatzzeit eines Systems von unter einem Jahr natürlich nicht funktionieren kann. Außerdem wäre dieser wohl kaum bereit anstelle des Distributors die Kosten für die Infrastruktur zu übernehmen.

[200] Zeitlich unbegrenzter Zugang zum Internet (manchmal bzgl. der zu übertragenden Datenmenge limitiert)
[201] Trusted third Party

9.1.2 Reine Offline-Modelle

Der entgegen gesetzte Fall ist ein Modell ohne jegliche Notwendigkeit für eine Internetverbindung. Es wirkt sehr konstruiert, da man hierbei von der Lieferung der Daten per Post oder dem Direktkauf im Ladengeschäft ausgehen muss, womit man jegliche Vorteile des neuen Mediums vernachlässigen würde. Außerdem ist das Modell deutlich unsicherer, da es ohne jede Kontrolle vom Nutzer beliebig modifiziert werden kann. Zum Beispiel können Cracker das System knacken und „Updates“ über das Internet (oder ebenfalls auf dem Postweg) verschicken.

Hier findet sich wiederum die Problematik, dass die Nachteile auf einer Seite gehäuft auftreten: Diesmal auf Seiten des Rechteeigners. Neben den beiden bereits erwähnten Punkten der teureren Distribution und der größeren Unsicherheit des Systems kommt noch hinzu, dass es ohne das Internet nicht möglich ist, die in Mode gekommenen Mehrwertdienste für den Kunden anzubieten, um das eigene Produkt gegenüber der Konkurrenz interessanter zu machen. Und es fällt auch die im Onlinefall so reizvolle Möglichkeit detaillierte Kundenprofile zu gewinnen weg. Zudem wird ein System, welches ohne Internet funktioniert, kaum einen Investor finden, da es als „veraltet“ angesehen wird, und zugleich mächtiger gegen Veränderung sein muss und somit ohnehin schon teurer ist.

Daher kann bei diesem Konzept recht schnell zu dem Ergebnis kommen, dass ein zukunftsweisendes System sicherlich das Internet einschließen muss, wenngleich nicht in einem solchen Maß wie im vorangehenden Kapitel beschrieben. Daher soll nun eine Mischform untersucht werden, die die anfallenden Vor- und Nachteile fair aufteilt, und somit wohl größere Akzeptanz finden wird.

9.1.3 Offline-Modelle mit subsidiärem Online-Anteil

Den vielversprechendsten Ansatz liefern Modelle, die das Internet nicht ganz außen vor lassen, sondern es zur Unterstützung einbinden. Hierbei sollte es nur soweit integriert werden, wie es der Kunde wünscht, bzw. sofern ein interaktiver, modularer Aufbau, bei dem der Nutzer dies selbst entscheidet, nicht gegeben sein kann, nur so weit, dass seine Verwendung transparent bleibt.

Dabei landet man sehr nah an den „klassischen“ DRM-Modellen, wenngleich es natürlich ein wenig wunderlich ist, bei einer so neuen Technologie schon von klassischen Modellen zu sprechen. Bei diesen gibt es zumeist einen sog. Content-Server und einen Licensing-Server. Der erstere stellt die erwünschten Daten zur Verfügung, meist als geschützten Container, seltener als Datenstream. Der zweite Server

verleiht die erworbenen Lizenzen mit denen der Nutzer Zugang zu dem entsprechenden Content erlangt. Bei manchen Systemen werden Content und Lizenz bereits zusammengeführt, bevor sie zum Nutzer gelangen.

Der Zugang wird nach den verschiedensten Modellen geregelt. Zum einen gibt es Systeme, bei denen mittels einer Beschreibungssprache die einzelnen Rechte definiert und zugeordnet werden. Der Kunde zahlt per Zeiteinheit oder per Anzahl der Abrufe. Im Gegensatz zu den reinen Online-Modellen, ist die Abrechnung jedoch nicht so feingranular, dass eine ständige Verbindung notwendig ist. Ein sehr interessantes Modell in diesem Bereich ist auch das Potato-Modell der Universität Ilmenau, bei dem das Konzept der Superdistribution umgesetzt wird, welches Nutzer mittels Incentives motivieren soll, nicht nur das System zu nutzen, sondern den geschützten Inhalt auch weiterzuverteilen. Doch hierzu später mehr[202].

Bei Überprüfung der Aufteilung der in den vorangegangenen Unterkapiteln aufgezählten Vor- und Nachteilen findet sich, dass alle in ausreichendem Maß auf beide Parteien verteilt werden konnten:

Bei der Sicherheit sind diese Systeme zwar schwächer als die reinen Online-Systeme, dies wird jedoch mehr als ausgeglichen durch das praxisrelevantere Vertrauenspotential, welches durch die zu gewährleistende Transparenz vergleichsweise hoch liegt. Die Internetunterstützung garantiert des weiteren ein Mindestmaß an Benutzerfreundlichkeit, Da der Komfort durch den subsidiären Onlineanteil drastisch erhöht wird. Dennoch bleibt die Sicherheit für den Produzenten nicht ganz auf der Strecke, da automatisch eine periodische Überprüfung der Integrität des Programms und der Zertifikate vorgenommen werden kann und der gesamte Weg der Daten geschützt bleibt. Zudem sind diese noch personalisierbar, was ebenfalls für beide Seiten ein Vorteil sein kann.

Im Folgenden wird noch einmal der Motivationsaspekt aufgegriffen, welcher wie bereits erwähnt eine exzellente Möglichkeit ist, die Akzeptanz eines Systems zu erhöhen.

9.2 Das Potato-Modell[203]

Im wesentlichen handelt es sich hierbei um eine Variante der Superdistribution für MP3-Dateien. Die Idee hinter der Superdistribution besteht darin, dass nicht mehr nur der Urheber oder ein von ihm eingeschalteter Produzent die Verteilung bzw. den Verkauf der Daten

[202] siehe auch Kapitel 9.2
[203] siehe auch [43] bzw. [44]

übernimmt, sondern die Kunden gleichzeitig selbst zu Distributoren werden:

Der Urheber vertreibt die Musik über einen Server im Internet an die Nutzer. Nach Bezahlung des festgelegten Preises erhält Nutzer X den Song, bereits mit einer TAN[204] versehen. Kann er nun einen weiteren Nutzer Y davon überzeugen, diesen Song ebenfalls erwerben zu wollen, erhält dieser von X dessen TAN. Und bei Erwerb einer eigenen Lizenz, erhält sowohl der Urheber einen eigenen Anteil[205], wie auch Nutzer X.

Dieses System setzt hierbei ganz auf die „Fairness“ der Nutzer, da es komplett auf einen Kopierschutz verzichtet. Damit es funktionieren kann, darf niemand die Dateien (inkl. der Namen, welche als einziges die TAN enthalten) verändern oder die Daten außerhalb eines Verkaufshyper-links anbieten, so zum Beispiel in einer Tauschbörse. Da momentan gerade die Fairness durch die florierenden Tauschbörsen von den großen Produktionsfirmen und Verlagen bezweifelt wird, und diese somit ein solches System nicht verwenden werden, ist ein solches System nur für Urheber interessant, die keinen Vertrag mit den oben genannten Firmen haben, und auf einen Eigenvertrieb ihres Contents angewiesen sind. Die strategische Komponente der Superdistribution ist zur Motivationssteigerung für den Nutzer allerdings sehr interessant, und wird auch in dem hier erstellten UGS-DRMS Verwendung finden.

9.3 Das erweiterte DRM-Konzept

Nun werden für das hier vorgestellte Konzept weitere einfache Bausteine vorgestellt, und ihre Funktion im Gesamtkonzept erklärt.

Im vorliegenden vereinfachten Fall gibt es noch zwei Entitäten, die in Einklang gebracht werden müssen: Zum einen die Server des Content-Produzenten, zum anderen der Computer des Nutzers. Damit sichergestellt wird, dass der Nutzer bei erstmaliger Verwendung des DRMS nicht eine veränderte Version bekommt, sollten die DRM-Server die einzigen sein, wo eine Datenverwendung berechtigte Kopie erhalten werden kann.

Anonymität

Dieses Abspielprogramm wird bereits für jeden Nutzer einzeln mit einer Kennung versehen, die mit einem Schlüsselpaar verknüpft ist, welches für die sichere Kommunikation benötigt wird. Für den Produzenten lassen sich hierüber allerdings auch Nutzerprofile erstellen, was ja wieder dem Wunsch nach Anonymität des Nutzers widerspricht. Doch

[204] Vom Online-Banking bekannt: Die Transaktionsnummer
[205] Im momentanen System 43 % des festgelegten Preises. Nach Abzug von Transaktionskosten, GEMA-Gebühren (die dieses System bereits unterstützt) usw.

lässt sich dies durch eine Anonymisierung des gesamten Nutzer-Produzenten-Kontakts durch eine Trusted Third Party auf ein angemessenes Maß reduzieren. Dadurch bleibt der Vorteil erhalten, dass der Produzent wirklich anonyme Nutzerprofile erhält, und sein Angebot auf das Nutzerverhalten einstellen kann. Das Abspielprogramm bekommt neben der Kennung auch noch den öffentlichen Schlüssel des Nutzers, damit es dessen Identität verifizieren kann.

Portabilität

Damit das Abspielprogramm auch in der Praxis wirklich portabel verwendet werden kann, sollte die Dateigröße sich im unteren einstelligen Megabyte-Bereich bewegen, da sonst der Vorgang der Installation einfach zu lange dauern würde. Die installierte Version des Abspielprogramms sollte nur für einen nicht zu kurzen Zeitraum funktionsfähig sein, damit eine einmal zum Missbrauch getätigte Veränderung des Programms nur bis zur nächsten Überprüfung andauern kann. Andererseits solle der Nutzer aber auch nicht genötigt werden, in einem zu kurzen Intervall Onlineverbindungen zur Überprüfung der Integrität aufbauen zu müssen. In einem Zyklus von drei Monaten wird das Abspielprogramm auf seine Identität geprüft, sowie vorhandene, aber abgelaufene Zertifikate entsorgt, oder bei Wunsch des Nutzers erneuert. Eine solche Integritätsprüfung kann bspw. durch den Vergleich einer errechneten Prüfsumme, welche von jeden einzelnen Bit in nicht-trivialer Weise abhängt, geschehen.

Damit sind die einzigen Punkte, für die eine Onlineverbindung benötigt wird, die Akquise der gewünschten Daten, sowie einmalig für die Installation des Abspielprogramms und periodisch für eine Integritätskontrolle.

9.4 Objekt- oder benutzerorientierte Freigabe

Wie der Titel und mehrfach innerhalb dieser Arbeit bereits andeutet, wird bei dem hier konstruierten System ein Paradigmenwechsel vorgenommen.

Bisher wurde mittels technischer Schutzmaßnahmen der Content geschützt und auf dem jeweiligen, mit einer Benutzerschnittstelle versehenen Objekt (bspw. ein Computer) zum Abspielen freigegeben, sofern eine Lizenz vorhanden war. Der Nutzer musste auf anderen Geräten sich separat mit seiner Lizenz anmelden, bzw. diese sogar für ein jedes Gerät erneut erwerben. Dies schadet durch den mangelnden Komfort und eventuell erhöhte Kosten der Akzeptanz eines DRMS durch den Nutzer.

Die mangelnde Portabilität der Rechte eines Nutzers schadet, weil der Nutzer seine Lizenzen trotz des rechtmäßigen Erwerbs nicht immer mit

sich führen kann, wie es bei früheren, ungeschützten Datenformaten der Fall war, einfach durch die Orientierung der klassischen Systeme, welche nur einen Computer pro Nutzer vorsehen.

Durch den Paradigmenwechsel zu einem benutzerorientierten System kann man diese Portabilität garantieren, da nun jeder Rechner durch Nachweis der eigenen Identität Zugriff auf den rechtmäßig erworbenen Content herstellen kann[206]. Daher ist das Votum ganz klar zu Gunsten einer benutzerorientierten Freigabe zu fällen.

Der konzeptionelle Aufwand ist zwar um einiges größer, da eine erweiterte Infrastruktur geschaffen werden muss, welche innerhalb weniger, einfach vom Nutzer durchzuführender Handgriffe ein Computer so weit absichern können muss, dass er den Daten konsistenten Schutz gewährt. Auch muss es eine zentrale Stelle geben, an der der Nutzer die erworbenen Rechte speichern kann. Oder es muss eine Möglichkeit geschaffen werden, mittels derer die Rechte durch den Nutzer selbst bewegt werden können. Letztere Variante ist allerdings nur praktikabel, falls neben den Zertifikaten, die die Zugangsberechtigungen enthalten werden, auch die Daten gespeichert werden, da die Untrennbarkeit von beiden sehr wichtig für die Sicherheit der Daten ist, sofern man nicht auf ein reines Online-System umsteigen will. Andernfalls müsste man einen eigenen Verschlüsselungsmechanismus für die Metadaten entwerfen. Hier wird eine Kombination beider Möglichkeiten des Rechtetransports vorgesehen: Da die Datencontainer sowohl auf einem neuen Rechner nach gelungener Authentifizierung immer wieder herunter geladen werden können, ist diese Möglichkeit immer gegeben, wenn es auch einen Internetanschluss gibt.

Sicher sinkt die praktische Bedeutung dieser Lösung mit der Größe des geschützten Contents. So werden Filme, die leicht eine Größe von mehr als einem Gigabyte haben können, nur selten in angemessener Zeit aus dem Internet herunter geladen werden, während es bei wenige Kilobyte großen Textdateien wohl die bevorzugte Methode sein dürfte. Die Daten, die man einmal bereits in personalisierter Form in einem Laden erworben oder auch herunter geladen hat, enthalten bereits in ihrem Container sämtliche wichtige Metadaten, sowie die der Person des Nutzers zugeordneten Wasserzeichen. Zur Verwendung muss nun nur noch das entsprechende Abspielprogramm herunter geladen werden, welches auch mit der Kennung des Nutzers versehen wird, die er bereits bei dem ersten Kontakt mit dem Content-Produzenten zugewiesen bekommen hat und die er durch Authentifizierung nachweist. Dieses Programm hat dann die Fähigkeit die portierten Daten

[206] eine Internetverbindung vorausgesetzt

weiterzuverarbeiten und gemäß den enthaltenen Zertifikaten zu verarbeiten.

Eine Weiterentwicklung der benutzerorientierten Freigabe ist die benutzergruppenorientierte Freigabe. Der wesentliche Unterschied beruht darauf, dass den einzelnen Nutzern Merkmale zugeordnet werden, anhand derer sie sich zu Gruppen zusammenfügen lassen. Diesen Gruppen werden dann Rechte zugeordnet. Besonders eignet sich eine derartige Freigabe, um die gesetzlichen Erfordernisse der Schrankenregelungen zu erfüllen, die ja für einige Gruppen gemeinsam besondere Rechte vorsehen. Und diese Freigabe soll die Grundlage für das hier erstellte UGS-DRMS werden.

9.5 Authentifizierungsmechanismus

Gerade für das Konzept des nutzer(gruppen)spezifischen DRMS ist es natürlich enorm wichtig, dass auch der Nutzer vor dem entsprechenden Computer sitzt, den das System auch erwartet. Fraglich ist nun, wie man dies denn sicherstellen kann. Dazu bedarf es eines geeigneten Authentifizierungsmechanismus'.

In der Literatur[207] werden allgemein vier Wege unterschieden, wie man sich bei einem System authentifizieren kann:

- Was man weiß
- Was man hat
- Was man ist
- Wo man ist

Was man weiß

Das wohl bekannteste Authentifizierungssystem ist die klassische Kombination aus Benutzername und Passwort, welche an geeigneter Stelle in einem Programm eingegeben wird.

Diese Kategorie verwendet demnach einen Wissensvorsprung, den der rechtmäßige Nutzer im Gegensatz zu einem nicht Berechtigten hat. Das Problem bei einer derartigen Authentifizierung ist die Unsicherheit, da sie maximal rudimentären Schutz bietet. Zum einen können Passwörter auf vielfältigste Art und Weise geklaut oder mit automatisierten Verfahren erraten werden, und zum anderen kann der Benutzer sie natürlich unproblematisch weitergeben. Damit wäre es möglich, dass ein gesamter Freundeskreis auf den gleichen Content Zugriff hätte, was natürlich nicht im Sinne des Rechteinhabers sein kann.

Vorteil dieses Systems ist natürlich die kostengünstige Implementierung und Generierung, sowie die für den Nutzer einfache Möglichkeit die für

[207] Beispielsweise in einem Internetlexikon für den Computerbereich: [45]

den Zugang relevanten Teile immer bei sich zu haben, wobei manche Nutzer dies aber wohl allzu wörtlich nehmen und sich ihre Zugangsdaten auf Notizzetteln niederschreiben.

Was man hat

Eine bessere Methode ist die Authentifizierung über einen Gegenstand der die Daten unauslesbar enthält, und den man bei sich hat. Darunter fallen beispielsweise Authentifizierungssysteme die auf einer Magnetkarte oder einem Schlüssel aufbauen.

Die Vorteile dieses Systems liegen vor allem in der Unkopierbarkeit der Zugangsdaten aufgrund der stofflichen Komponente; zumindest sofern diese stoffliche Komponente gut geplant ist. Probleme bei diesem Weg der Authentifizierung bereitet vor allem, wie die Karte zum Nutzer gelangt, sowie die höheren Kosten, für jeden Nutzer eines Systems diesen Zugang herzustellen. Je nach Aufbau des Zugangsgegenstandes können zudem Kosten für die Schaffung einer Infrastruktur entstehen, um die auf dem Gegenstand enthaltenen Daten auf den Computer oder das abspielende Gerät zu übertragen, was ja passieren muss, um die Authentifizierung vornehmen zu können. Empfehlenswert ist es also schon existente Schnittstellen zu verwenden.

Ein weitere, weniger schwerwiegender Nachteil ist die Tatsache, dass der Nutzer einen Gegenstand mitführen muss, um an seine Daten zu gelangen.

Was man ist

Die sicherste, einzelne Methode ist wohl der Weg sich mit biometrischen Informationen zu authentifizieren. Beispiele für diese Daten sind Fingerabdrücke, die Retina oder die DNA eines Menschen. Die Daten sind momentan nur sehr schwer auszulesen, da die notwendige Technik noch zu komplex und auch zu teuer ist. Damit fällt dieser Weg für eine Verwendung in DRMS mit hohen Benutzerzahlen leider aus, doch kann für die Zukunft praktikabel werden.

Der klare Vorteil hierbei wäre, dass Menschen diese Daten notwendigerweise immer bei sich tragen und zudem sie nur schlecht weitergeben, bzw. sich stehlen lassen können.

Wo man ist

Der letzte Weg der Authentifizierung wird nur der Form halber genannt, da er für ein DRMS unbrauchbar ist. Hier dreht es sich um die Idee, den Zugang nur an einem bestimmten Ort zuzulassen, bspw. in einem speziellen, vom Internet abgeschlossenen Netzwerk.

Selbstverständlich können Nutzer eines DRMS nicht extra zu einem anderen Ort gehen, um ihren Content zu verwenden, doch hätte diese Methode einen ähnlich hohen Sicherheitsaspekt, wie die bereits früher beschriebenen geschlossenen Systeme. Allerdings wäre der Kostenfaktor ebenfalls nicht zu vernachlässigen.

Fazit

Die Sicherheit dieser Wege für ein Authentifizierungssystems steigt mit der gleichzeitigen Anwendung von mehreren dieser Wege. Als Beispiele seien hier eine EC-Karte zu nennen, die die Wege „Ort“, „Wissen“ und „Haben“ vereinigt: Man muss an einem EC-Automat (Ort) mit einer EC-Karte (Haben) die richtige PIN (Wissen) eingeben, um Geld zu erhalten. Für eine Authentifizierung im Computer- bzw. Internetbereich eignen sich beim heutigen Stand der Technik nur die beiden ersten Methoden, die im UGS-DRMS daher auch kombiniert werden sollen. Durch den Transfer der Zugangsdaten durch unsicheres Gebiet muss speziell darauf geachtet werden, dass es dort keine Schnittstellen gibt, an denen diese unverschlüsselt vorliegen.

Durch Addition der „Haben“-Komponente mit der „Wissen“-Komponente addieren sich die Nachteile was Kosten und Komfort angeht, doch erhöht sich die Sicherheit durch Hinzunahme der stofflichen Komponente derart, dass es sich wieder lohnt: Selbst beim Abfangen von Passwörtern die zwangsläufig über das Internet reisen müssen, kann man den Content des entsprechenden Nutzer nicht verwenden, da dieser die stoffliche Komponente noch hat.

Und in der heutigen Zeit ist es kein Problem in einen sehr kleinen Gegenstand (bspw. von der Größe eines Kugelschreibers oder eine EC-Karte) einen Kryptografieprozessor zu integrieren, der auch komplexere Verfahren zur Authentifizierung beherrscht.

9.6 Mittelbare Verschlüsselung via PKK

Im Normalfall hat jeder Teilnehmer bei der asymmetrischen Verschlüsselung zwei zu ihm gehörige Schlüssel, nämlich den privaten und den öffentlichen. Jeder Kommunikationspartner kennt nun den öffentlichen Schlüssel des Teilnehmers und kann mit diesem dem Teilnehmer eine verschlüsselte Nachricht zukommen lassen.

Sollten sich nun zwei verschiedene Kommunikationspartner „verbünden“ und ihre jeweiligen Daten über andere Teilnehmer abgleichen würden, könnten beide erkennen, dass sie (aufgrund des gleich gebliebenen öffentlichen Schlüssels) mit der gleichen Person kommuniziert haben. Dadurch könnten sie ein umfassenderes Bild von dieser erhalten. Erneut wäre also die informationelle Selbstbestimmung des Kunden in Gefahr.

Wie wäre es nun, wenn jeder Kunde mit jedem Kommunikationspartner einen eigenen öffentlichen Schlüssel hätte? Dies würde prinzipiell verhindern, dass man erkennen kann, ob man mit der gleichen Person kommuniziert hat.

Allerdings ergibt sich mit dieser Methode auch ein großer, verwaltungstechnischer Overhead. Man müsste als Teilnehmer eine

ungleich höhere Anzahl von Schlüsselpaaren verwalten und zudem wird die Zertifizierung aufwändiger, da jeder neu verwendete Schlüssel bei der Hauptzertifizierungsstelle angemeldet werden müsste.

Um dieser Problematik Abhilfe zu schaffen, könnte man eine mittelbare Verschlüsselung einführen. Dies bedeutet, dass der Nutzer nicht unmittelbar mit seinem öffentlichen Schlüssel kommuniziert, sondern mit einem dritten Schlüssel – einen Derivatschlüssel, der aus diesem öffentlichen Schlüssel mit einer Einwegfunktion gewonnen wird. Daher auch der Name der mittelbaren Verschlüsselung.

Die nun folgende Idee gibt es in der Praxis noch nicht, weshalb auch keine Aussage über die Praxistauglichkeit gemacht werden kann. Besonders bei der Sicherheit könnten massive Lücken entstehen, da man eventuell bei Vorliegen von mehreren dieser Derivatschlüssel bspw. die Kommunikation entschlüsselt werden könnte. Doch um genauere Aussagen über sicherheitstechnische Aspekte treffen zu können, bräuchte es eine ausführliche Untersuchung.

Die Vorteile, die durch die mittelbare Verschlüsselung entstehen würden sind allerdings evident. Durch die Abhängigkeit der Derivatschlüssel vom öffentlichen Schlüssel des Nutzers kann im Idealfall die TTP, welche ohnehin standardmäßig zur Bestätigung der Zertifizierung kontaktiert werden muss, bspw. mit einer Prüffunktion die Zugehörigkeit des Derivatschlüssels zum Hauptschlüssel bejahen. Der Nutzer wäre also nicht gezwungen jedes neue Derivatschlüsselpaar bei der TTP einzeln anzumelden. Damit würde dieser Teil des verwaltungstechnischen Overheads bereits wegfallen. Die Anonymität wäre wiederum selbst gegenüber einem Konsortium von Content-Produzenten gewährleistet.

Der Verwaltungsaufwand auf Seiten des Nutzers würde allerdings bleiben. Hier bestünde die Möglichkeit, alle verschiedenen öffentlichen Derivatschlüssel auf den gemeinsamen privaten Hauptschlüssel abzubilden. Dann könnte der Nutzer mit einem privaten Schlüssel, einer Funktion zum Bilden von Derivatschlüsseln und den jeweiligen öffentlichen Derivatschlüsseln seine Kommunikation gestalten. Der öffentliche Hauptschlüssel würde der Kommunikation mit der TTP vorbehalten bleiben.

Doch wie bereits erwähnt, ist diese mittelbare Verschlüsselung bis dato Spekulation und soll nur die Möglichkeit aufzeigen, dass man multiple Schlüssel gegenüber verschiedenen Kommunikationspartnern verwenden könnte um die Anonymität weiter zu verbessern.

10 Technische Elemente des UGS-DRMS

An dieser Stelle soll nun das System unter Beachtung der vorgenannten grundsätzlichen Designüberlegungen aufgebaut werden. Doch dazu soll vorher noch einmal das Fazit des letzten Kapitels wiederholt werden:

Um überhaupt eine Chance zu bekommen, das System zu etablieren müssen die Weichen in Richtung der höheren sozialen Akzeptanz gestellt werden. Dies passiert in erster Linie durch eine Anonymisierung des Datenverkehrs durch eine TTP sowie durch den Paradigmenwechsel hin zu einem nutzergruppenspezifischen System. Die Nutzergruppen orientieren sich an den juristischen Rahmenbedingungen, vor allem an den Schrankenregelungen. Das grundlegende Konzept wird einen subsidiären Onlineanteil vorsehen, da dieses den besten Trade-Off zwischen den beiden extremen Modellen bietet. Außerdem wird die Sicherheit für sowohl den Nutzer als auch den Rechteinhaber erhöht, da ein kombiniertes Authentifizierungssystem vorgesehen wird, bestehend aus einem USB-Dongle in Kombination mit einem Passwort.

Doch nun werden die technischen Komponenten erklärt und das DRMS aufgebaut. Neben der Erklärung der einzelnen Komponenten und der Erläuterung ihrer Aufgaben im UGS-DRMS wird immer auch eine Abkürzung eingeführt, die die Übersicht vereinfachen soll.

10.1 Die Serverstruktur

Da der Content in irgendeiner Form vom Rechteinhaber zum Nutzer gelangen soll, und dies nicht gerade in einer ungeschützten, unpersonalisierten Form oder über den klassischen Weg des Kaufs in einem Ladengeschäft, ist eine ausgeklügelte Serverstruktur von Nöten, die auf der Seite des Rechteinhabers das Herz der DRM-Infrastruktur darstellen soll. Diese könnte aus Einzelservern des jeweiligen Content-Produzenten bestehen, doch hier wird einer domänenbasierten Version der Vorzug gegeben, da von einer Kooperation von Produzenten gleichartigen Contents ausgegangen wird, und diese Ausgestaltung größere Synergie-Effekte mit sich bringt, da pro Domäne bspw. nur ein KDC benötigt wird, und so die Verwaltung sich vereinfacht.

10.1.1 Die Domänen mit dem Content (Dom1 ... Dom n)

Die Domänen sind verwaltungstechnisch effizientere Strukturen als Einzelserver, doch keine Notwendigkeit, bringen aber Kosten- und Aufwandsersparnis mit sich. So lässt sich auch eine PKI gut verwenden. Der Vorteil einer PKI ist die nahezu freie Bewegung durch die ganze

Domäne von Servern. Jede einzelne der Domänen umfasst eine KDC, einen oder mehrere Content-Server und einen oder mehrere Lizenz-Server. Die Gruppierung nach Domänen kann auf die verschiedensten Arten erfolgen. So können sich entweder Produzenten gleichen Contents zusammentun, ein Produzent verschiedener Arten seine Angebote zu einer Domäne zusammenfassen oder auch Anbieter, die das gleiche DRMS nutzen. Theoretisch kann ein Anbieter auch seine Server in mehrere Domänen stellen, sollte er bspw. an verschiedenen DRMS teilnehmen.

10.1.2 Der KDC der Domänen (KDC1 ... KDC n)

Jede Domäne hat ein KDC, das den Zugang zu ihr regelt. Wie bereits im Kapitel 5.6 dargelegt, ist das KDC mit umfassenden Berechtigungen ausgestattet, Zugang zur eigenen Domäne gewähren zu können. Dadurch kann es natürlich Probleme geben, wenn in einer Domäne verschiedene Anbieter sich zusammenschließen, da wohl keiner einem Mitkonkurrenten die Entscheidung über den Zugang zu eigenen Servern gestatten will. Hier könnte als eine Art Schlichtungsstelle der erste Einsatz für die TTP sein.

10.1.3 Content-Server in den Domänen (CS11 ... CS nn)

Auf den Content-Servern in den Domänen lagert, wie schon der Name vermuten lässt, der unmodifizierte Content, den die Produzenten anbieten wollen. Bei Eintreffen einer Anfrage wird der Content entsprechend der ID des Anfordernden durch ein Wasserzeichen personalisiert, und vom Content Server zum Nutzer übertragen. Diese Server müssen die maximal mögliche Sicherheit aufweisen, da die hier lagernden Daten ohne das Wasserzeichen natürlich von großem Interesse für Piraten und Cracker sind.

10.1.4 Licensing-Server der Domänen (LS11 ... LS nn)

Der Licensing-Server verwaltet einen Teil Zugriffsrechte der einzelnen Nutzer. Der Server ist eher optional zu sehen, ließe sich über ihn doch bei Einführung eines Billing-Systems auch die Bezahlung in Echtzeit abwickeln und Lizenzinformationen an das KDC verschicken, das diese an den Content-Server weitergeben könnte.

10.1.5 Die Trusted Third Party (TTP)

Die vertrauenswürdige Drittpartei erhält in dem UGS-DRMS im Wesentlichen drei Aufgaben.

- Schutz der Anonymität des Nutzers

- Verwaltung der Nutzergruppenzugehörigkeit
- Rechteverwaltung bei unterschiedlichen Unternehmen in einer Domäne

Zum Schutz der Nutzeranonymität muss nur noch wenig gesagt werden, da diese nun zur genüge diskutiert wurde. Sie stellt zugleich auch die wichtigste Aufgabe der TTP in dem System dar. An zweiter Stelle steht die Verwaltung der Nutzergruppenzugehörigkeit. Die TTP muss dazu sowohl über Integrität bzw. Unabhängigkeit, als auch über Autorität verfügen, weshalb hier eigentlich nur der Staat als solche geeignet ist.

Die dahinter sich verbergende Idee soll an dieser Stelle näher erläutert werden. In den rechtlichen Grundlagen wurden die verschiedenen Schrankenregelungen vorgestellt. Manche dieser Schranken wurden in der ersten Novellierung des Urheberrechts für so wichtig erachtet, dass sie im § 95 b UrhG den Status erhielten, dass sie über dem Schutz von TPM stehen. Dies bedeutet, dass der Rechteinhaber es zustimmungsfrei ermöglichen muss, dass durch die Schrankenregelung Begünstigte Zugang zu dem Content erhalten. Damit nun die Daten nicht dadurch in ungeschützter Form auftauchen können, wird der Schutz einfach erweitert. Durch das Gesetz ermächtigte Nutzer sollen bei Nachweis ihres Status' Zugang innerhalb des Systems erhalten.

Und dies stellt nun die TTP sicher. Entweder als Sammelstelle für Registrierungsstellen oder selbst als Registrierungsstelle gibt die TTP an die Server des Rechteinhabers die Information weiter, dass der Nutzer aufgrund einer bestimmten Schranke berechtigt ist. Um dies an einem Beispiel zu erklären: Zur Umwandlung einer Text- in eine Sprachdatei zur Wahrnehmung durch einen Blinden, was ja durch eine Schranke (§ 45 a UrhG) zustimmungs- aber nicht vergütungsfrei erlaubt ist, beantragt der Blinde (eventuell durch einen Mittelsmann) Zugriff auf die Datei. Nach Bestätigung der Zahlung und einer Rückfrage zur Bestätigung der Blindheit (bspw. durch Vorlage eines Behindertenausweises) gibt die TTP an den Rechteinhaber die Anweisung weiter, die Textdatei mit erweiterten Zugriffsrechten auszustatten, welche der Blinde zur Umwandlung der Datei benötigt. Da die TTP sowohl vom Rechteinhaber, wie auch dem Nutzer unabhängig ist, können beide Parteien der TTP vertrauen, der Nutzer muss keinen einseitigen Vertrauensvorschuss leisten und der Rechteinhaber hat die Gewissheit, dass die Daten nicht sein System verlassen um die Schranke einzuhalten. Zudem erhält er die angesprochenen Nutzerprofile vollständig anonymisierter Form, ohne dass der Nutzer sich durchleuchtet fühlen müsste.

Der dritte und letzte Punkt schließlich wurde bereits in Kapitel 8.4 angesprochen. Die TTP sollte auch die Funktion des KDC in einer gemischten Domäne übernehmen, da sich, bedingt durch die

Konkurrenzinteressen, die teilnehmenden Parteien nicht den gegenseitigen Zugang zu ihren Servern anvertrauen würden. Dies ist allerdings wirklich nur bei gemischten Domänen nötig. Theoretisch könnte hier auch eine andere Drittpartei als die oben genannte diese Aufgaben übernehmen.

10.2 Nutzeridentifikation

Für das angesprochene Authentifizierungssystem werden verschiedene Bausteine benötigt. Die wichtigsten davon sind die verschiedenen nutzerspezifischen Kennungen sowie der Dongle, der die stoffliche Komponente für das Authentifizierungssystem darstellt.

10.2.1 Die Kennungen

Es gibt viele Möglichkeiten einen Nutzer durch verschiedene Identifikationsnummern (ID) darzustellen. Beispielsweise könnte die ID im einfachsten Fall eine eindeutige Zahl sein. Oder der öffentliche Schlüssel eines Nutzers. Im folgenden sollen die benötigten Kennungen beschrieben werden. Das UGS-DRMS verwendet die Kennungen zur eindeutigen Authentifizierung des Nutzers, daher ist es von höchster Wichtigkeit, dass diese nicht nachahmbar sind. Dabei liegt die Hauptverantwortung natürlich bei dem Nutzer selbst, doch besitzt er bspw. bei seiner EC-Karte eine ähnliche Sorgfaltspflicht bei der Geheimhaltung seiner zugehörigen Geheimnummer.

Die Meta-Kennung (M)

Die generellste Kennung ist die Meta-Kennung M, welche im Idealfall auf der Welt einzigartig sein sollte, da theoretisch jeder Weltbürger einem verwendeten DRMS beitreten kann und doppelte Nummern natürlich die eindeutige Identifizierbarkeit gefährden würden. Geeignet wäre unter anderem eine aus biografischen Daten oder aus bereits vorhandenen Identifikationsnummern, wie der Personalausweisnummer oder der Sozialversicherungsnummer, generierte ID. Damit wäre einerseits die weltweite Eindeutigkeit natürlich gewährleistet, andererseits ergeben sich daraus drei Probleme:

An erster Stelle steht erneut das Problem der Anonymität. Wer gibt bei seinem Bäcker gerne so explizite Daten über die eigene Person an, auch wenn diese Daten mathematisch verändert wurden? Damit müsste zur Anonymisierung bereits an dieser Stelle die vorgenannte TTP eingreifen, um die Nutzerdaten eindeutig mit einer anonymen ID zu verbinden. Das zweite Problem wäre die Generierung einer solchen ID. Da dieses System mit einer Hardwarekomponente arbeiten soll, muss diese mit der Metakennung verknüpft werden. Damit dieser Vorgang nicht missbraucht werden kann, muss es einen sicheren Weg geben, wie diese Zuordnung bewerkstelligt werden kann. Als Idee mag wieder

die TTP dienen, die die ausgebende Stelle solcher Dongles werden könnte. Im Falle des Erfolgs könnten die Dongles viele weitere Funktionen erfüllen, wie bspw. als Krankenkassenkarte, bargeldloses Zahlungsmittel oder auch (Studenten-)Ausweis.

Die Metakennung wird in diesem Beispiel als höchste Kennung betrachtet, von der sich alle weiteren ableiten. Daher ist es vorteilhaft, sie so unkompromittierbar[208] wie möglich zu gestalten. Eine Neuvergabe dieser Kennung wäre mit großem Aufwand verbunden.

Aus der Metakennung wird ein Schlüsselpaar generiert, welches auf dem Dongle gespeichert wird.

Die nutzerspezifische ID (X)

Diese nutzerspezifische ID X besteht, wie für asymmetrische Kryptografiesysteme notwendig, aus einem privaten und einem öffentlichen Schlüssel. Der private Schlüssel ist ausschließlich bei der TTP und auf dem Dongle gespeichert. Damit sollte der private Schlüssel keinesfalls in fremde Hände gelangen können. Aber auch ein etwaiger maliziöser Nutzer bekommt nicht die Möglichkeit zur Manipulation.

Der Nutzer kann sich nun nur mit dieser ID identifizieren. Damit nicht durch einen Abgleich verschiedener Unternehmen oder innerhalb eines Unternehmen, welches verschiedene Sparten anbietet, der Nutzer nicht wieder erkannt wird, bietet es sich nun an, mit Derivaten der ID X zu arbeiten. Diese müssen in klar definierter Weise mit dem Hauptschlüssel in Verbindung gebracht werden können. Entweder kann auch diese Aufgabe die TTP übernehmen, welche in den Nutzerdatenbanken einfach eine Verknüpfung der neuen Schlüssel mit der Metakennung vornimmt, oder man könnte die im letzten Kapitel beschriebene mittelbare Verschlüsselung verwenden. Außer den beschriebenen Auswirkungen ergeben sich für das System keine weiteren, als dass die ID X nun für jeden Teilnehmer der Domäne anders lautet, und die TTP die Verwendung der verschiedenen Schlüssel absegnet.

Nutzername und Passwort (Auth)

Die dritte und letzte Authentifizierung wird eingebaut um zu verhindern, dass ein abhanden gekommener Dongle missbraucht wird. Bei Verbindung des PCs mit dem Dongle wird die Abfrage einmalig durchgeführt. Dies stellt neben dem Besitz des Dongles den zweiten (zusätzlichen) Weg der Authentifizierung dar.

Sicherlich ist eine Authentifizierung per Passwort nicht die sicherste, doch genügt sie für diesem Fall. Möglich wäre es auch für zukünftige Systeme, von der Authentifizierung per Passwort auf eine

[208] Für den Fall, dass jemand die Metakennung eines Menschen kennt, könnte er bei zusätzlichem Vorliegen des jeweiligen Algorithmus' entweder im Nachhinein an dessen Nutzerschlüssel gelangen oder gar durch Umkehrung des Generationsalgorithmus' an die persönlichen Daten. Beides sind sehr unerfreuliche Szenarien.

Authentifizierung per biometrischen Daten umzuschwenken. Doch im Moment ist das bei dem Stand der Technik noch nicht in ein Gerät wie den Dongle zu integrieren, da dieser zum einen klein und zum anderen kostengünstig sein soll.

Kennung des Abspielprogramms

Das Abspielprogramm enthält einen eigenen Schlüssel der bei der Installation mit übertragen wird. Dieser ist allerdings recht leicht auszulesen, weil im Abspielprogramm dieser Schlüssel im Klartext vorliegen muss. Daher kann er als einzige Hürde nicht funktionieren, wird aber mit der ID X kombiniert, da so sichergestellt wird, dass ein integeres Abspielprogramm mit nur zusammen mit einem passenden Dongle zusammen arbeitet.

10.2.2 Der Dongle

Der Dongle (D)

Der Dongle stellt die für die Sicherheit des Systems äußerst zuträgliche Hardwarekomponente dar. Auf ihm sind in gesicherten Speicherbausteinen das/die Schlüsselpaar(e) enthalten. Die technische Sicherung erfolgt über verschiedene Systeme. Zum einen sind die relevanten Daten nur in verschlüsselter Form auf dem Chip gespeichert und zum anderen wird auch durch technischen Schutz dieser Speicher ein Auslesen verhindert.

Dazu kommt noch ein austauschbarer Kryptografie-Prozessor, der die Verschlüsselung direkt im Dongle übernimmt, da sonst die Schlüssel über die Schnittstelle zwischen Dongle und Computer gehen müssten, was sie auslesbar machen würde. Der Dongle funktioniert also als eine Art Blackbox, die die Verschlüsselung und Authentifizierung aus dem Computer auslagert und so sicherer macht.

Der Dongle mit ID X (Dx)

Der Dongle wird von der TTP in personalisierter Version an den Nutzer weitergegeben. Das bedeutet, dass der Dongle schon bei der Herausgabe mit einem Nutzer assoziiert wird, und so keine „herrenlosen“ Varianten zu missbräuchlichen Zwecken verwendet werden können.

Die Schnittstelle des Dongles ist entweder drahtlos oder drahtgebunden. Ersteres würde den Komfort erhöhen, gleichzeitig allerdings die Kommunikation abhörbar machen. Außerdem wäre eine externe Energieversorgung für den Prozessor und die Datenspeicher von Nöten. Ein Beispiel für diese Variante ist die Anbindung des Dongles über Bluetooth[209]. Beim momentanen Stand der Technik ist eine Bluetooth-Schnittstelle allerdings noch nicht in jedem Computer integriert. Daher kann diese Variante nur als mögliche, komfortablere Version angeboten werden.

[209] Kabelloses Datentransportsystem; siehe auch [46]

Im zweiten Fall, der drahtgebundenen Variante, muss der Nutzer seinen Dongle an jedem Computer erneut anschließen, was einerseits recht mühsam sein kann, andererseits jedoch die stete Energieversorgung garantiert. Außerdem kann die Kommunikation in der Praxis nicht abgehört werden. Ein Beispiel für diese Variante ist der Anschluss via USB[210] oder Firewire[211]. Hauptsächlich der erstere ist inzwischen zum Standard-Anschluss an den meisten aktuellen Computern gereift, weshalb für dieses System der Dongle vergleichbar mit einem USB-Memory-Stick von Form und Größe gewählt wird. Er wird über das USB-Kabel mit Energie versorgt, die auch ausreicht um den zusätzlich einzubauenden Kryptografie-Prozessor zu versorgen.

10.3 Content

Content unmodifiziert (C)

Der Content ist der zentrale Punkt, um den es sich bei dem UGS-DRMS dreht. Nach der Erstellung liegt der Content beim Content-Produzenten in Reinform vor. Da um jeden Preis verhindert werden muss, dass sich diese Version im Darknet verbreiten kann, sollte bereits ab der Fertigstellung der endgültigen, personalisierten Version der Content nur noch als generischer Container vorliegen, der mit einem Hauptschlüssel des Produzenten verschlüsselt ist.

Content personalisiert (Cx)

Bei einer konkreten Anfrage nach dem Content wird dann vom Lizenz-Server und/oder vom Content-Server der generische Content personalisiert, d.h. mit einem Wasserzeichen mit der nutzerspezifischen ID versehen, die der Content-Produzent erhalten hat. Damit ist meist der jeweilige öffentliche Schlüssel ID X des Nutzers gemeint. Zusätzlich wird dann der generische Container doppelt verschlüsselt: Zum einen mit dem userspezifischen privaten Schlüssel des Content-Produzenten, von dem das personalisierten Abspielprogramm als einziges den öffentlichen besitzt. Und zum anderen wird der Container mit dem öffentlichen Schlüssel des Nutzer verschlüsselt, damit nur in der Kombination „Korrektes Abspielprogramm und korrekter Dongle“ der Content zugänglich wird.

Richtigerweise muss man allerdings davon sprechen, dass der Content eigentlich nur mit einem sicheren symmetrischen Verfahren gesichert wird und dessen Schlüssel dann wie oben beschrieben verschlüsselt wird, da wie bereits erwähnt, die asymmetrische Kryptografie zwar einen Sicherheitsvorteil besitzt, allerdings für größere Datenmengen und Echtzeitsysteme denkbar ungeeignet ist.

[210] Universal Serial Bus; entwickelt von Microsoft; Siehe auch [47]
[211] Eine Schnittstelle die von Apple entwickelt wurde. Auch genannt: IEEE 1394; siehe auch [48]

Zusätzlich werden in den Content-Container die Lizenzen zur Benutzung des Contents gepackt. Diese sind damit doppelt verschlüsselt, zum einen ebenfalls mit dem separaten Schlüssel, der jedem personalisierten Abspielprogramm zugewiesen wird, und zum anderen mit der ID X des Nutzers. Das Abspielprogramm kann so nur nach Authentifizierung durch den Dongle des Nutzers die Daten interpretieren.

Zusammenfassend soll das folgende Bild den Aufbau des Content-Containers verdeutlichen:

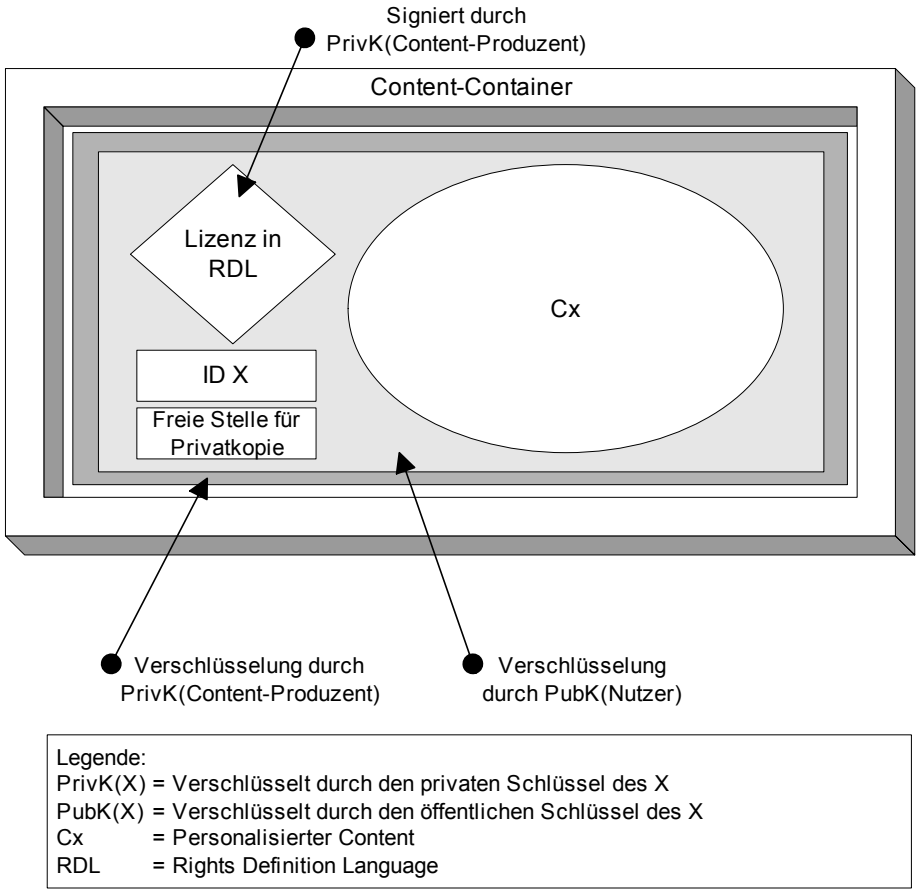

Abbildung 6: Aufbau eines Content-Containers

10.4 Das Abspielprogramm

Abspielprogramm (Abs)

Das Abspielprogramm ist die Schnittstelle zwischen den Nutzern und dem Content. Sie übernimmt für den Produzenten den vorgelagerten Schutz des Contents, für den Nutzer hingegen stellt sie ein Programm dar, welches er mit allen Komfortansprüchen verwendet. Wie bereits erwähnt muss das Abspielprogramm zwischen dieses beiden Extremen den goldenen Mittelweg finden.

Das soll geschafft werden, indem man sich an gängigen Varianten orientiert, deren Markterfolg bereits vorhanden ist. Im Idealfall kann man in einer Kooperation etablierte Programme um eine DRM-Komponente erweitern.

Damit die Daten auch konsequent durch den Nutzer auf jedem beliebigen Computer verwendet werden können, muss der Nutzer in die Lage versetzt werden, auf jedem Computer auch das Abspielprogramm installieren, da es ja die Grundlage zur Verwendung der Daten darstellt.

Abspielprogramm (Absx)

Die Installation wird über das Internet angefordert, woraufhin unter Verwendung der ID X (also dem öffentlichen Schlüssel des Nutzers) das Programm in personalisierter Form abgesendet wird. Die Personalisierung ist zwar nicht zwangsläufig notwendig hilft aber in Kombination mit der Authentifizierung per Dongle, die Sicherheit zu stärken. Denn damit existiert eine weitere Hürde die ein potenzieller Verletzer zu überwinden hätte.

Ebenso würde es nur für kurze Zeit funktionieren das Programm so zu modifizieren, dass es keinen Abgleich der IDs von Content und Programm vornimmt, da alle drei Monate ein Integritätstest von Lizenzen und Programm stattfindet. Die Sicherheit wird detailliert im nächsten Kapitel beschrieben.

Eckpunkte

Da das Programm hier nicht vollständig ausformuliert werden kann, sollen nur die Eckpunkte teilweise aus den vorangegangenen Kapiteln stichpunktartig wiederholt bzw. angesprochen werden:

- Einfache Installation

  Da eine Vielzahl verschiedener Benutzer digitale Daten nutzen will, muss es selbst Nutzern mit nur geringen Computer-Kenntnissen möglich sein, auf ihren Computern das Abspielprogramm des UGS-DRMS zu installieren. Erreicht wird dies durch die Verwendung von Standard-Installationsassistenten.

- Gute Dokumentation

  Trotz der Feststellung, dass eine fehlerhafte Dokumentation als Mangel des Produktes zu sehen ist, haben nur die wenigsten Programme eine gute, lückenlose Dokumentation. Da das System sich aber gerade auch an Laien wenden will, ist eine solche Dokumentation unerlässlich. Darin sollte in erster Linie die Funktionsweise des Systems, wie auch die generellen Vorgänge im Hintergrund des Systems einfach dargelegt werden.

- Intuitive Bedienbarkeit

  Inzwischen haben sich im Computer-Bereich Quasistandards herausgebildet, die die Bedienung von Programmen regeln. Darunter fallen vor allem die von Microsoft entwickelten

Kommandoleisten, oder bspw. das Kontextmenü, welches über die rechte Maustaste erreichbar ist. Auch sollte gerade bei der Wiedergabe von Medien darauf geachtet werden, eine konsistente Beschriftung der einzelnen Bedienelemente wie sie auch im Hifi- oder auch Video-Bereich zu finden ist.

- Unterstützung der meisten gängigen Formate im jeweiligen Bereich

  Besonders wichtig für den Erfolg eines DRMS ist die Unterstützung von zusätzlichen Formaten, die für den Nutzer interessant sind, selbst wenn sie nicht zum DRM-geschützten Bereich zählen. Je vielfältiger ein Programm einsetzbar ist, desto weniger besteht die Möglichkeit, dass der Nutzer es als unnütz von seinem Computer verbannt und wieder versucht den Content auf illegale Weise, dafür aber in von ihm präferierten Formaten zu erhalten. Beispielsweise sollte ein Abspielprogramm im Audiodatenbereich neben dem eigenen Format auch die gängigen Formate MP3, WMA, Midi und Wav unterstützen.

- Funktionsvielfalt

  In die gleiche Richtung geht die Prämisse, dass das Programm mehr können muss, als nur das abspielen des Contents. Je nachdem welche weitergehenden Rechte der Nutzer hat, sollte er die Möglichkeit bekommen (allein schon des Schutzes wegen) alle diese Rechte innerhalb des Abspielsprogramms wahrnehmen zu können. Zusätzliche Funktionen sind allerdings nicht verkehrt, da diese die Attraktivität eines Programms weiter erhöhen. Um wieder ein Musikabspielgerät als Beispiel zu nehmen, können als Beispielsfunktionen die Verwaltung von Musiklisten, die Einbindung eines Equalizers, grundlegende Funktionen wie „Wiederholung“ und „Zufallsmodus“ etc. genannt werden. Dennoch sollte die Übersichtlichkeit gewahrt bleiben, indem man die Funktionen auch ausblendbar macht. Ein gutes Beispiel für ein beliebtes Abspielprogramm (allerdings ohne besondere DRMS-Fähigkeiten) ist Winamp[212], welches zur Zeit in der fünften Version als Freeware zum Download zur Verfügung steht.

- Modularer Aufbau

  Dieser Punkt ist eher für den Content-Produzenten wichtig. Sollte sich ein bestimmter Baustein des Systems als unsicher herausstellen, sei es durch Programmierfehler oder durch das Knacken des Schutzes, kann dieser Baustein ohne große Probleme gegen einen gleichwertigen mit den gleichen Schnittstellen usw. ausgetauscht werden. Dadurch spart man sich die Überarbeitung des gesamten Programms.

[212] siehe auch [49]

- Transparenz & Blackbox

  Besonders schwer ist diese Anforderung zu erfüllen. Sie kommt direkt im Anschluss an die einfache Installation. Einerseits soll der Nutzer nämlich von dem DRMS kaum etwas bemerken, außer dem ersten Einloggen per Dongle, andererseits muss ihm eine ausreichende Transparenz zugestanden werden, damit er sich sicher fühlen kann, dass seine Daten in den richtigen Händen (nämlich den eigenen) sind. Diese Mischung aus den beiden Extremen wird erreicht, indem der Nutzer mittels eines Reglers das Level an Informationen bestimmt, welche er über die Vorgänge erhält.

- Angemessene Dateigröße

  Da es immer noch nicht selbstverständlich ist, dass ein durchschnittlicher Computer überhaupt über eine Internetverbindung verfügt, bzw. dass es sich auch um eine Breitbandverbindung handelt, sollte das Abspielprogramm nur eine geringe Größe haben. Gering zu definieren ist nicht einfach, da sich auch die Datenträger im Wandel befinden. Gängige USB-Memory-Sticks fassen mindestens 32 MB, diese Obergrenze wäre wohl für die installierte Version zur Übertragung auf einen internetfreien PC akzeptabel, doch dauert das Herunterladen dieser Datenmenge selbst über einen schnellen DSL-Anschluss deutlich zu lange. Wie weit man allerdings programmtechnisch mit einer Obergrenze von bspw. einem Megabyte kommen würde, ist ebenso fraglich. Daher kann die Frage nicht abschließend beantwortet werden.

- Verschiedene Betriebssysteme

  Im Zeitalter der schwindenden Dominanz von Microsoft-Betriebssystemen wird es immer wichtiger auch verschiedene Betriebssysteme zu bedienen und nicht vollkommen auf Windows aufzubauen. In den näheren Kreis aufzunehmen sind (in Reihenfolge absteigender Wichtigkeit): MS Windows, Linux, MacOS und mit Abstrichen auch Unix, OS/2.

- Einfaches Wahrnehmen der Rechte

  Gerade da dieses System auf der lückenlosen Durchsetzung des Schutzes trotz des Vorhandenseins von gesetzlichen Schranken setzt, muss die Zusammenarbeit zwischen Gesetz und Programm auch einwandfrei und einfach funktionieren. Dazu sollten die Vorgänge automatisierbar sein. So ist es auch bei diesem System vorgesehen.

- Motivationssystem

  Das Motivationssystem des UGS-DRMS kann mehrere Bestandteile umfassen. In diesem Fall wird ein dreistufiges System vorgesehen.

Zunächst soll dem Nutzer der Einstieg in die Verwendung der Systems schmackhaft gemacht werden. Dies geschieht durch ein nicht mit dem Programm verbundenes Incentive. So erhält bspw. der Nutzer eines DRMS im Bereich der Musik ein Album seiner Wahl kostenlos zur Verfügung, so lange er das System verwendet oder bei einem DRMS im Printbereich ein Abonnement einer Zeitung seiner Wahl für ein Quartal.

Die zweite Stufe ist die Integration von (noch) nichtdurchsetzbaren Schranken nach § 95 b UrhG, wie beispielsweise der Privatkopie. Dieses Zugeständnis bewegt einerseits die Nutzer das System eher zu verwenden, da eine Funktionalität garantiert, die der von ungeschützten Daten nahe kommt, und bringt andererseits auch weitere Nutzer zur Teilnahme an dem System. Denn um eine Privatkopien von geschützten Daten zu verwenden bedarf es natürlich ebenfalls einer Instanz des Abspielprogramms und einem gültigen Dongle. Wie der Vorgang genau funktioniert klärt das Kapitel 11.2.2.

Die dritte und letzte Stufe ist die Vergütung der Werbung ähnlich dem Potato-Modell. Wenn ein Nutzer eine Privatkopie für sich vollständig nutzbar machen will, und diese daher bezahlt, erhält der, der sie ihm ursprünglich gegeben hatte, eine Vergütung in Form von Bonuspunkten oder Treuepunkten, wie man es auch nennen mag. Bei entsprechender Menge können diese dann gegen weitere Daten zur eigenen Verwendung eingetauscht werden.

Kurz gefasst: Es muss zunächst ein funktionales Programm entwickelt werden, welches ein Nutzer auch verwenden möchte, und es darf diesem keine Designruine aufoktroyiert werden. Zu viel Aufmerksamkeit wird immer noch dem Schutz der Daten gewidmet.

10.5 Metadaten

Die Metadaten können in beliebiger Form dem Content beigefügt werden. Von ihrer Ausprägung hängt die Funktion des Systems nicht unmittelbar ab. Es wäre natürlich wünschenswert, wenn diese Daten einem definierten Schema folgen würden oder zumindest so aufgebaut sind, dass sie maschinenlesbar sind. Sonst müsste ein Abspiel-programm zwangsläufig für jeden Teilnehmer auf Produzentenseite neue Informationen erhalten, wie die Metadaten interpretiert werden sollen.

Rechtedefinitions-sprache (RDL)

Inzwischen weit verbreitet ist XML nebst entsprechender Schemata[213]. Weitergehende semantische Sprachen sind zwar inzwischen auch schon zu Standards gereift[214], doch ist die Unterstützung durch die Industrie bisher kaum existent. Die Vorteile der weitergehenden Sprachen besteht darin, dass sie nicht nur maschinenlesbar sind, wie eben XML, sondern auch maschinenverständlich sind.

Des weiteren gibt es inzwischen mehrere verschiedene Rechte-definitionssprachen (RDL), wie XrML[215] oder ODRL[216]. Beide Sprachen bauen auf XML und damit auf SGML auf und sind dazu gedacht, die genauen Rechte eines Nutzers an Content festzulegen.

Da es nicht notwendig ist, eine deutlich komplexere Ontologie in das UGS-DRMS zu integrieren, ohne dass man eine Verwendung dafür hat, bietet es sich an bei diesem System die Metadaten durch eine der spezialisierten RDL darzustellen. Und in dem Fall wird aus Kosten- und Sympathiegründen die ORDL verwendet, da diese im Geiste des Open Source frei lizenzierbar ist, also schon einmal Kosten spart.

10.6 Weitere Elemente eines DRMS

In dem letzten Abschnitt dieses Kapitels folgen nun noch einige mögliche Zusatzsysteme die ein DRMS beinhalten kann, aber nicht zwangsläufig beinhalten muss.

Microbilling-System

Die wohl für Content-Produzenten interessanteste zusätzliche Komponente ist das sog. Microbilling-System. Dieses zeichnet jede kleinste Verwendung eines Nutzers auf und berechnet diese idealerweise in Echtzeit. Diese Komponente wurde nicht in das UGS-DRMS aufgenommen, da zum einen eine stetige Onlineverbindung benötigt wird, mit allen Vor- und Nachteilen wie in Kapitel 9.1.1 beschrieben, und zum anderen das Misstrauen der Nutzer gegen eine solche Form der Abrechnung immer noch recht hoch ist. Sie befürchten häufig nicht zu Unrecht, dass sie durch die „angepassten“ Preise des Content-Produzenten insgesamt mehr bezahlen, warum sollte dieser sonst ein solches System einführen.

Ubiquitäre Informationsplattform

Ein weiteres Zusatzsystem könnte es möglich machen, den Content so auf den Servern des Content-Produzenten zu verankern, dass der Nutzer über diese Server Zugang zu seinem legal erworbenen Content erhält.

[213] DTD (Doctype Definition) oder XMLS (XML Schema)
[214] RDF (Resource Description Framework) oder bspw. OWL (Web Ontology Language); siehe hierzu auch [50]
[215] siehe auch [51]
[216] siehe auch [52]

Geräte-Unabhängigkeit

Immer mehr technische Geräte sind mit Prozessoren ausgestattet, die für ein DRMS ausreichend sind. Durch weitgehend plattform-unabhängige Programmierung ist eine Ausweitung auf andere Systeme, wie bspw. Handys oder PDAs möglich.

11 Überprüfung auf praktische Tauglichkeit

Nachdem nun die beteiligten Elemente des Systems erläutert wurden, soll es nun auf seine Praxistauglichkeit untersucht werden. Dazu wird das Programm sowohl aus Sicht des Content-Produzenten, als auch des Nutzers betrachtet.

Der wohl für den Content-Produzenten wichtigste Punkt bei DRMS ist die Sicherheit der einzelnen Daten, da ja bereits bei den Grundlagen aufgezeigt wurde, dass diese nach einmaliger ungeschützter Verbreitung nicht mehr schützbar sind. Allerdings sind die Daten, wie ebenfalls bereits aufgezeigt, nicht auf Dauer schützbar. Daher wird nun im Folgenden ein Sicherheitssystem entwickelt, welches die hehre Aufgabe hat, die Daten mit angemessenem Aufwand zu schützen.

Zur Gewährleistung dieser Sicherheit wird von der Zuverlässigkeit und Sicherheit der Public Key Kryptografie ausgegangen. Darauf aufbauend werden Verbindungen über das Internet via PKI gemanagt. Des Weiteren wird die für dieses System so wichtige lückenlose Schutzkette genauer erläutert, die selbst die gesetzlich zugelassenen Ausnahmelizenzen einschließt.

Aus Sicht des Nutzers ist natürlich neben der Sicherheit der Daten auch das persönliche Sicherheitsgefühl von höchster Priorität. Dies soll u.a. durch Einrichtung einer vertrauenswürdigen Drittpartei gesichert werden, welche kein kommerzielles Interesse haben darf, sowie die Umsetzung des bereits im vorigen Kapitel skizzierten Motivationssystems.

11.1 Sicherheit der Daten

Damit die Sicherheit der Daten genauer beleuchtet werden kann, ist es notwendig, die möglichen Angreifer zu kennen. Man kann bei diesen im Wesentlichen vier Arten unterscheiden, was sich allerdings relativieren wird:

- Der maliziösen Nutzer
- Der private Rechtsverletzer
- Der Cracker
- Der Content-Pirat

11.1.1 Angreifer

Maliziöser Nutzer

Der maliziöse Nutzer ist mit programminternen Kenntnissen ausgestattet und besitzt legalen Zugang zum Programm und gegen Bezahlung auch zu den Daten. Damit hat er einen beachtlichen Wissensvorsprung, den

er auch weitergeben könnte, sowohl freiwillig, als auch unfreiwillig, indem ein anderer sich in den Computer des Nutzers hackt (wobei man im letzteren Fall sicherlich nicht von der Böswilligkeit des Nutzers ausgehen kann, sondern eher vom Unvermögen seinen Computer zu schützen).

Da in den meisten DRM-Systemen auf Grund der Verbreitung es recht einfach gemacht werden soll, daran teilzunehmen, kann man davon ausgehen, dass der maliziöse Nutzer eher ein Überbegriff für das Maß an Information des Angreifers ist, und seine Motivation sich durch die folgenden drei Angreifersubformen erklärt. Es ist also zwischen einem wissenden Angreifer (maliziöser Nutzer) und einem unwissenden Angreifer zu unterscheiden, deren Motivation sich jeweils in die des Crackers, des Piraten und des privaten Rechtsverletzers aufspaltet.

		Privater Nutzer	Hacker	Content-Pirat
Maliziöser Nutzer	= viel systeminterne Informationen	Wunsch: mehr bzw. freiere Verwendung des Contents	Verstehen und Umgehen des Systems	Einstieg in den Markt mit fremdem Content
Aussen-stehender	= wenig systeminterne Informationen	Verwendung des Contents	Verstehen und Umgehen des Systems	Einstieg in den Markt mit fremdem Content

Tabelle 1: Aufschlüsselung der Angreiferarten

Man sollte immer vom schlechtesten Fall ausgehen, wenn man ein Programm auf Sicherheit überprüft, was bedeutet, dass der unwissende Angreifer vernachlässigt werden kann, da ihm (mit Ausnahme eventueller höherer fachlicher Qualifikation) keinerlei Möglichkeiten offen stehen, die einem mit höherem Kenntnisstand versehenen Angreifer nicht auch zur Verfügung stehen würden.

Die Motivationen der einzelnen Angreifer eines System stellen sich nun wie folgt dar:

Content-Piraten

Der für den Autoren und den Distributor des Contents schlimmste Fall, ist der Einstieg eines Content-Piraten in das eigene Marktsegment. Dieser versucht nämlich sich die einmaligen Produktionskosten der digitalen Güter zu sparen, indem er das fremde geistige Eigentum selbst vermarktet, ihm dabei aber nur die geringen Vervielfältigungskosten anfallen. Dadurch fällt es ihm nicht schwer die Daten in gleicher Qualität (aufgrund der verlustfreien Kopierbarkeit der digitalen Daten), aber vor allem zu deutlich geringeren Preisen auf dem Markt anzubieten. Damit entsteht für die Content-Produzenten eine Konkurrenzsituation gegen die eigenen Produkte.

Ein Beispiel hierfür ist die Offlinedistribution auf vielen Straßenmärkten in Fernost. Die Distribution solcher Datenträger, bzw. auch nur der Daten selbst, kann allerdings schneller und effizienter über das Internet per bezahlten Download geschehen. Hier regiert wiederum die Angst der Nutzer vor solchen Daten. Nur ungern, und damit auch selten sind sie bereit Kreditkartennummern u.ä. Zahlungsinformationen an offensichtliche Piraten herauszugeben.

Die Daten, die Piraten verkaufen, bekommen diese zumeist von den legal verkauften Werkstücken aus dem Handel, damit sie nahezu die gleiche Qualität wie der legale Produzent gewährleisten können. Es gibt natürlich auch andere Quellen, wie etwa Insidergeschäfte, wenn ein Mitarbeiter einer Firma ungeschützte Werksstücke herausgibt, oder an Kritiker versandte Vorabversionen im Internet auftauchen. Da diese sich allerdings selbst mit einem DRM-System nur schwerlich verhindern lassen, sollen diese Methoden vernachlässigt werden. Ebenso wird der direkte Einbruch in den Content-Server des Produzenten[217] außen vor gelassen.

Unter der oben genannten Unterteilung bzgl. des maliziösen Nutzers ist klar, dass gerade die Piraten sich auch als Nutzer eintragen können, und somit über das erwähnte Zusatzwissen über interne Abläufe verfügen werden. Dies ließe sich nur mit einer genauen Überprüfung jedes neuen Mitglieds umgehen, doch damit würde man dem Gedanken widersprechen, dass der Nutzer Vertrauen in das System bekommt, weil er nicht durchleuchtet wird. Außerdem wäre dieser Ansatz durch die schiere Datenmenge kaum bewältigbar.

Ein kurzer Gedanke soll dieser Idee dennoch gewidmet werden: Sofern sich ein System bewährt, welches wie das hier vorgestellte auf einer vertrauenswürdigen Drittpartei beruht, könnte man die Überprüfung des Nutzers automatisiert der Drittpartei übergeben. Dabei dürfte der Content-Produzent allerdings nur eine abstrakte Risikoeinschätzung erhalten, die sich nicht eindeutig dem Kunden zuordnen lässt.

Besondere Punkte, an denen Piraten das System aushebeln können und wollen, sind zum einen die nahe liegenden: Entfernung des Wasserzeichens, Entfernung des Schutzes, Erlangung eines Schlüssels. Zum andern finden sich aber auch an Schnittstellen des Systems bzw. bei der DAD- und DD-Wandlung Ansatzpunkte, an denen sich eine Attacke lohnt.

Private Nutzer

Die zweite große Gruppe ist die der privaten Verwender, die sich ohne große Kosten Daten zur eigenen Verwendung aus dem Internet laden wollen. Hier ist die Motivation im Normalfall gänzlich anders. Zum einen

[217] Dieser kann verhindert werden, indem die Daten bereits in verschlüsselter Form, bzw. in Bruchstücken verteilt auf verschiedenen Servern liegen.

haben die Privatnutzer weder die Ressourcen, noch die technischen Möglichkeiten der Piraten. Zum anderen fehlt aber auch das Interesse an der weiteren Distribution für Geld.

Es ist sinnvoll die Gruppe der privaten Nutzer in zwei Untergruppen einzuteilen, um präziser auf die Unterschiede im Verhalten eingehen zu können. Zum einen gibt es den durchschnittlichen Nutzer, der zu den Datenmengen des im Internet kursierenden Content nur über einfache, für ihn präparierte Programm und unter Anleitung Zugang findet. Zum anderen gibt es den fortgeschrittenen Nutzer, der sowohl über ein höheres Know How, als auch über leistungsstärkere Hardware verfügt.

Diese zweite Nutzergruppe ist es zumeist, die die erste Nutzergruppe, den sog. Mainstream überhaupt erst an den Content heranführt. Große Verteilernetze, die bereits erwähnten Tauschbörsen, lassen sich nur aushebeln, wenn ihre Verwendung aufgrund von Strafverfolgung oder anderen Sicherheitsmaßnahmen so komplex gestaltet werden muss, dass der Mainstream hier nicht mehr mitziehen kann. Und selbst dann wird der Tausch dort noch florieren, da wie bei großen Systemen üblich wenige aktive Nutzer bereits einen Großteil der Daten zur Verfügung stellen. Wenngleich es nicht für derartige Formen von Märkten entwickelt wurde, so kann das Pareto-Prinzip[218] auch hier zur Modellierung Anwendung finden. Bekannt wurde es als die 80/20-Regel, die besagt, dass 20 Prozent aller Teilnehmer eines Marktes zusammen ca. 80 Prozent aller Transaktionen durchführen. Die genauen Prozentsätze sind im fraglichen Bereich zwar unbekannt, doch hat sich die Tendenz, die die Regel aufzeigt, bestätigt.

Unglücklicherweise für die Produzenten deckt sich die besonders aktive Masse der „Marktteilnehmer“ einer Tauschbörse in etwa mit den erfahreneren Nutzern, eben wegen dem gerade erwähnten Know How- und Ressourcen-Vorsprung. Und diese Gruppe ist es auch, die den Industrien mit Weiterentwicklungen ein Schnippchen schlägt, da sie überalterte Modelle von Tauschbörsen stets durch neue Kniffe den Gegenmaßnahmen der Industrie überlegen macht.

Dennoch gibt es einen Ansatzpunkt, die Macht der Tauschbörsen zu brechen: Die monetäre Marktmacht erstreckt sich über die gesamten 100 Prozent der Teilnehmer. Durch das Abschneiden des Mainstreams von der Quelle der Daten werden nicht etwa nur 20 Prozent der Ressourcen frei, sondern 80 Prozent, da der durchschnittlich Nutzer ebenso über ein Teilkapital verfügt, wie der fortgeschrittene. Diese Arbeit muss parallel geleistet werden, um den momentanen Zustand wieder zu normalisieren, in dem Content praktisch frei ist.

[218] Nach Vilfredo Pareto; 1897; Bei der Erforschung der Verteilung von Einkommen und Reichtum.

Doch zunächst muss, so gut es eben geht, verhindert werden, dass der Content überhaupt in das Internet gelangt. Die für die privaten Nutzer interessante Situation ist die Möglichkeit den Content kostenfrei verwenden zu können, und zudem unbeschränkt, was die Verwendung bzgl. des Mediums, des Geräts oder der Zeit betrifft. Auch die Möglichkeit der Weitergabe „der eigenen" Dateien ist wichtig, das Äquivalent zur Privatkopie. Von geringerem Interesse, sofern man nicht Teil einer Tauschbörse sein will, ist das (Nicht)Enthaltensein eines Wasserzeichens.

Die primären Angriffspunkte für private Nutzer sind damit die enthaltenen Zertifikate. Diese dürfen nicht manipulierbar werden. Andererseits kann man durch angemessene Preise bzw. großzügige Rechtevergabe seitens der Content-Produzenten durchaus auf ein Level kommen, dass wieder von den für den Verbraucher mehr als nur ärgerlichen Kopierschützen[219] weggeht, und beispielsweise wieder die Privatkopie integriert.

Damit ließe sich an der Motivation der Angreifer arbeiten. Da technische Maßnahmen jeglicher Art wie erwähnt auf die Dauer keinen Bestand haben, ist dies der einzige Punkt der strategisch gedacht ist. Doch sollte auf einen Schutz nicht vollständig verzichtet werden.

Als zweiter Angriffspunkt findet sich für die Nutzer die Portierbarkeit auf Plattformen, die das DRM-System nicht unterstützen oder umgekehrt. Die normalen, nicht „intelligenten" Geräte, beispielsweise eine HiFi-Anlage oder tragbare MP3-Player, haben zumeist nicht die Rechenleistung, aufwendige DRM-Systeme zu unterstützen. Allerdings sind die Hersteller aus verständlichen Gründen (Wegfall des Schutzes auf solchen Plattformen) an einer Portierung des Contents nur wenig interessiert.

Noch immer werden viele Geräte ohne jeden Ansatz eines Schutzes hergestellt. Hier wäre es möglich eine gesetzliche Regelung zu treffen die die Hersteller von solchen verpflichtet, ihre Abspielgeräte mit einem lizenzfreien Schutzsystem auszustatten, bei dem sich der Hersteller des Content nun aussuchen mag, ob er dieses System in seine Infrastruktur integrieren will. Solch eine gesetzliche Regelung wäre natürlich sehr restriktiv und wohl nicht durchzusetzen, gerade ob der Verbreitung von MP3-Playern und anderen digitalen Abspielgeräten. Doch es gibt auch in diesem Bereich ohne eine gesetzliche Regelung andere Ansätze. So hat bspw. Apple mit dem IPod ein Abspielgerät entwickelt, welches sowohl Apples proprietäres DRMS unterstützt, als auch normale ungeschützte Datenformate (wie eben MP3) abspielt. Auch ist die

[219] Siehe in diesem Zusammenhang das Kapitel 13 „Anpassung der rechtlichen Situation"

Rückübertragung von Musikstücken auf den Computer nicht möglich, womit das Kopieren doch stark eingeschränkt wird.

Der umgekehrte Fall findet sich, sobald der Nutzer eine CD oder eine DVD auf seinen Computer übertragen will. Nach heutiger Rechtslage ist dies nicht erlaubt, sofern ein Kopierschutz (wie auf den meisten DVDs und CDs vorhanden) besteht, doch viele der Nutzer wünschen dies. Auch hier ließe sich eine gesetzliche Regelung treffen, dass bspw. der Hersteller der Daten ein Abspielprogramm bzw. ein Konvertierungsprogramm zur Verfügung stellen muss, welches die Daten in den geschlossenen Kreis des DRM-Systems integriert, sofern er wünscht, dass seine Daten geschützt bleiben. Doch dies ist mit einem großen technischen Aufwand verbunden, der auf seine Sinnhaftigkeit überprüft werden müsste.

Hacker und Cracker

Die dritte und letzte Gruppe, die für das System eine Gefahr darstellen kann, sind die Hacker und Cracker, wobei jedoch eine klare Abgrenzung zwischen dem Begriff Hacker, der im Volksmund eindeutig negativ belegt ist und den Crackern zu treffen ist, einer Subgruppe der Hacker, welche der Volksmund eigentlich meint, wenn er von Hackern spricht. Diese Cracker betreiben das Verändern von Software gewissermaßen als Sport. Je aufwendiger und schwerer eine Software zu knacken scheint, desto interessanter wird es, genau dies zu versuchen. Eigentlich wäre dies kein Problem, da auch diese Gruppe im Normalfall kein monetäres Verletzungsinteresse hat. Doch durch die Publikation der Ergebnisse, wird es anderen maliziösen Gruppen möglich, eben diese Ergebnisse für ihre Zwecke zu missbrauchen.

Da die Cracker zumeist im Verdeckten operieren, ist es nur im Nachhinein möglich, und das auch nur bei ausreichender, guter Kenntnis der Community, die entsprechende Person zu identifizieren und zu bestrafen, was nach neueren gesetzlichen Regularien möglich ist.

Auch hier ergeben sich wieder rechtliche Probleme. So kann eine Publikation eines Crackers mit einem Mindestmaß an Phantasie (und Anwälte sind da oft erfinderisch) als wissenschaftliche Forschung inklusive der wissenschaftlichen Publikation der Ergebnisse betrachtet werden, was erlaubt ist. Denn dem Schutz der Wissenschaft sollte im Zweifel Vorrang eingeräumt werden.

Die Gruppe der Cracker ist durch Ihre Verborgenheit eines der größten Probleme, da gegen deren Aktivitäten praktisch keine Prävention möglich ist. Und im Nachhinein die Scherben aufzusammeln, kann nicht im Sinn der Content-Produzenten sein.

Im strategischen Bereich finden sich allerdings auch für dieses Problem wieder Lösungsmöglichkeiten, die für ein großes DRMS allerdings

kontraproduktiv sein können. Beispielsweise könnte man durch eine Ausschreibung eines Geldpreises, die sich erst bei fortgeschrittenen Hackaktivitäten finden lässt(!)[220], die Cracker dazu bewegen, ihre Ergebnisse nicht zu veröffentlichen, sondern dem Hersteller des DRMS zu überlassen, eben gegen Auszahlung der ausgelobten Geldsumme. Der Hersteller verpflichtet sich daraufhin, keinerlei rechtliche Schritte gegen diesen Cracker in diesem speziellen Fall anzustellen. Bis andere an die gleiche Stelle gelangen, hat der Hersteller des DRMS Gelegenheit das Programm zu verbessern und es sicherer zu machen, was durch die modulare Gestaltung des Programms problemlos funktionieren sollte. Damit würde man die Cracker quasi auf seine Seite ziehen und als „Betatester“ anstellen und gleichzeitig deren Namen erfahren. Dabei ist allerdings nicht auszuschließen, dass Cracker sich bewusst den Preis entgehen lassen, um das DRMS bloßzustellen.

Eine andere Möglichkeit wäre das Interesse der Gruppe der Cracker an dem System gering zu halten. Beispielsweise würden Nachrichten über gelungene Knackversuche die Sicherheit des System schlecht wirken lassen, weshalb viele Cracker das Interesse daran verlieren würden, ein solch löchriges System zu knacken. Leider gilt dies auch für eventuelle Geschäftspartner, deren Interesse ähnlich schnell dahin schmelzen wird.

Zu guter letzt besteht die Möglichkeit, das System auf eine geringe Anzahl von Nutzern zu beschränken, da sich unter diesen nur mit geringer Wahrscheinlichkeit ein maliziöser Nutzer mit entsprechendem Know How finden wird. Aber eine Vielzahl verschiedener Systeme zu betreiben kostet natürlich auch ein Vielfaches des Geldes, das für ein einzelnes System aufzuwenden wäre. Und gerade eine gute Skalierbarkeit ist in der heutigen Zeit für ein System sehr wichtig.

Besondere Stellen, an denen Cracker angreifen sind zumeist Schnittstellen und Protokolle die über das Internet laufen, da es (außer bei besonders harten Nüssen) gegen den Crackerethos verstößt, ein Programm zu verwenden und es „von innen“ zu hacken. Dies fällt eher den maliziösen privaten Nutzern zu.

11.1.2 Angriffsziele

Nach der Klassifikation der Angreifer und der für sie relevanten Angriffsziele, sollen nun diese einzelnen Angriffsarten auf das Systems erläutert werden und die jeweilige(n) Lösung(en) vorgestellt werden, und auf Kompatibilität mit den strategischen Zielen des Systems geprüft werden. Bisher steht das UGS-DRMS in folgender Form da: Ein Dongle zum Zugang, ein Abspielprogramm, eine Content-Server-Infrastruktur

[220] Eine öffentliche Ausschreibung würde gerade eine Vielzahl von Angriffen provozieren, die natürlich unerwünscht sind.

des Produzenten, eine Licensing-Server-Infrastruktur, der Zugang via PKI und zur Wahrung der Vertraulichkeit der Nutzerdaten die TTP.

Die Möglichkeiten für einen Angriff reichen über ein weites Spektrum. Daher werden die Angriffsarten in verschiedene, grundlegende Methoden unterteilt:

- Technische Angriffe
- Brachiale Angriffe
- Sicherheitslücken
- Systeminterne Angriffe

Gleich welcher Angriff stattfindet, es muss für den Nutzer auf jeden Fall eine Art Hotline existieren, bei der der Nutzer den Verlust seines Dongles melden kann, worauf die spezielle ID X des Nutzers dann ihre Gültigkeit verliert. Aus der Meta-Kennung kann der neue Besitzer des Dongles zwar eine neue ID X generieren, doch hat die durch die Deaktivierung des Dongles ebenfalls ihre Wirkung verloren. Der rechtmäßige Nutzer kann dann bei der TTP wieder einen neuen Dongle beantragen.

11.1.2.1. Technische Angriffe

Technische Angriffe verlaufen meist außerhalb des Systems, d.h. sie greifen das System nicht direkt an, sondern versuchen die Infrastruktur des Systems bzw. des Internets auszunutzen, um dem System zu schaden. Oft sind technische Angriffe allerdings nicht auf Informationsgewinn ausgerichtet, sondern darauf, andere von der Information abzuschneiden. Sie können daher durch das System selbst nur schlecht abgefangen werden. Um dennoch ein Mindestmaß an Sicherheit zu garantieren, müssen Komponenten, welche die Daten in unverschlüsselter digitaler Form erhalten würden, in das System einbezogen werden. Dabei ist allerdings wieder problematisch, dass der Nutzer bis zu einem gewissen Punkt die Kontrolle über seinen Computer abgeben muss. Im Folgenden werden technische Angriffe auf die einzelnen Bausteine des System betrachtet und soweit möglich verschiedene Lösungswege diskutiert.

- Masquerading/Spoofing

  Prinzipiell ist es möglich, dass eine Person sich unter dem Namen eines anderen in ein System einschleicht. Dieser Prozess des Vorgebens einer anderen Identität (bspw. einer anderen Absender-IP) wird auch Masquerading bzw. Spoofing genannt. Im Internet ist dies ein recht problematisches Phänomen, da nur selten eine sichere Verbindung aufgebaut wird, die auch wirklich die Korrektheit des Absenders überprüft.

Das DRMS kommuniziert genau aus diesem Grund nie im Klartext über unsichere Medien (und hierzu zählen eigentlich auch Schnittstellen innerhalb eines Computers). Außerdem werden nur mit den jeweiligen Schlüsseln des Absenders signierte Informationen als gültig erkannt.

- Auslesen des privaten Schlüssels von Dongle, Server oder Abspielprogramm

  Das technische Auslesen der ersten beiden Schlüssel muss unmöglich sein. Diese Schlüssel stellen den zentralen Punkt des Systems dar, wo es auch am verwundbarsten ist. Daher sind die Schlüssel auch so eng mit der Person des Nutzers verbunden.

  Ohne diese Verbindung könnte ein Nutzer seinen Schlüssel auslesen, was mit genügend Zeit und technischem Know How nicht zu verhindern ist, und den Schlüssel dann im Internet verteilen. Da ab dann alle Kopiervorgänge mit seinem Namen verknüpft wären, wird er es bedingt durch die Verknüpfung unterlassen.

  Sicherlich ist es möglich den Schlüssel eines gestohlenen Dongles auszulesen, doch kann und muss dieser vorher vom rechtmäßigen Nutzer gesperrt werden, ähnlich wie eine EC-Karte, Kreditkarte oder eine verlorene Handy-SIM-Karte.

  Der Schlüssel des Abspielprogramms ist ebenfalls mit dem Namen des Nutzers verknüpft und spielt ohnehin nur eine untergeordnete Rolle. Daher wäre sein Verlust weniger tragisch.

  Schließlich bleibt noch der/die Schlüssel auf den Computern des Content-Produzenten bzw. der TTP. Diese Meta-Schlüssel sind von allergrößter Wichtigkeit, da mit Hilfe der Meta-Schlüssel andere korrekte Schlüssel generiert werden können und damit das gesamte System ausgehebelt werden kann. Dementsprechend hoch sollte also das Sicherheitsniveau der TTP sein.

  Gleiches gilt für die Schlüssel der Content-Produzenten, da Nutzer schnell das Vertrauen verlieren, wenn die Kommunikation mit dem Betreiber des Systems nicht klappt. Im schlimmsten Fall können so legal erworbene Lizenzen gestohlen werden und so die Daten mit dem Wasserzeichen des eigentlich berechtigten Nutzers in Umlauf gebracht werden.

- Angriff auf die Daten auf dem Content-Server

  Besonders interessant für Content-Piraten bzw. auch für private Nutzer wäre es, Daten in generischer Form, also ohne Wasserzeichen und Verschlüsselung in die Hand zu bekommen. Die Rückverfolgbarkeit wäre ausgehebelt und der freien Verbreitung stünde nichts im Wege.

Ob der Schwere der Konsequenzen dieses Szenarios darf ab Fertigstellung des Contents in digitaler Form selbiger nur noch in verschlüsselter Form vorliegen. Am besten wäre die Herstellung eines generischen Containers, welcher quasi im Voraus berechnet wurde und der nur auf die Eingabe der ID X des Nutzers, sowie des zugehörigen Wasserzeichens wartet und mit minimalem Aufwand fertig gestellt werden kann.

- Trojanische Pferde[221], Viren[222] und Würmer[223]

  Der letzte technische Angriff ist zugleich der vielfältigste und daher nur dem Namen nach zusammen zu fassen. Alle drei genannten Schädlinge verbreiten sich auf unterschiedlichste Art auf den Computern der Nutzer (und manchmal auch auf denen der Hersteller).

  Wie man immer wieder in den Medien mitbekommt, gibt es leider sehr viele unzureichend gesicherte Computer, was teilweise auch am lückenhaften Betriebssystem des Computers liegen mag. Durch mangelndes Wissen der Nutzer ist der Befall nicht zu vermeiden.

  Prinzipiell sollte dem Nutzer also so viel Hilfestellung wie möglich geboten werden. Darunter fallen auch Dienste die nicht unbedingt etwas mit dem DRMS selbst zu tun haben, wie bspw. die Bereitstellung eines Virenscanners.

  Speziell in das DRMS lässt sich jedoch die Funktion einbinden, dass der Nutzer eine Routineüberprüfung des Systems auf Integrität anfordern kann. Sollten Dateien von diesem befallen sein, würde das zwangsläufig als nicht integer auffallen. Durch die Verknüpfung der Authentifizierung per Passwort mit der Hardwarekomponente „Dongle“ wirkt sich ein einfacher Diebstahl des Authentifizierungs-Passwortes nicht allzu tragisch aus.

11.1.2.2. Brachiale Angriffe

Brachialen Angriffen kann ein System ähnlich wie den technischen Angriffen nur bedingt widerstehen. Bei solchen Angriffe wird nicht mit

[221] Trojanische Pferde sind Spionageprogramme die sich meist in anderen Programmen verstecken, und die, nachdem jemand sie (freiwillig oder unfreiwillig) auf dem Computer hat, den Computer ausspionieren. Dazu zählt das Aufzeichnen von Passwörtern, das Durchstöbern der Dateien auf dem Computer oder auch die Erstellung von Protokollen dessen, was der Eigentümer tut.

[222] Viren sind meist schadhafte Programme, die Dateien des befallenen Computers infizieren und dann ihre Wirkung entfalten. Und dieser Wirkung setzt nur die Fantasie des Virenschreibers eine Grenze.

[223] Würmer sind sich fortpflanzende Viren. Sie infizieren durch ein Replikationssystem meist alle mit dem befallenen Computer verbundenen Rechner.

dem „Skalpell“ operiert, wie bei den vorgenannten technischen Angriffen, sondern eher mit einem Fleischerbeil. Die Ziele können durchaus die gleichen sein, doch diese Art der Angriffe beruht hauptsächlich auf reiner Rechenkraft des angreifenden Computers.

Es gibt im Wesentlichen zwei Unterarten der brachialen Angriffe: Zum einen kann versucht werden, sich als berechtigter Nutzer zu präsentieren, indem man sich mit einem korrekten Passwort anmeldet, welches man durch einen sog. „Brute Force“-Angriff (bspw. durch einen Wörterbuch-Angriff[224]) erlangt hat. Zum anderen kann das System aber auch einfach gestört werden, durch sog. Denial-of-Service-Attacken[225].

Im ersteren Fall bieten sich allerdings im Gegensatz zu den technischen Angriffen nur Benutzerschnittstellen an, da die mit PKK geschützten Schnittstellen praktisch[226] unmöglich per Brute Force zu knacken sind. Darunter fällt bei dem hier aufgebauten System eigentlich nur die Authentifizierung des Donglebesitzers beim Anmeldevorgang. Und auch dann nur in dem seltenen Fall, dass man im Besitz eines fremden Dongles ist, ohne dass der Besitzer diesen deaktivieren lassen hat.

Dies ist allerdings recht leicht zu verhindern, indem man ähnlich wie bei einer EC-Karte eine Beschränkung der falschen möglichen Eingaben pro Zeiteinheit vorsieht, die auch technisch nicht umgangen werden kann. Als Beispiel wird hier von drei erlaubten Fehlauthentifizierungen pro Tag ausgegangen. Damit wird die TTP nicht zusätzlich belastet und das Erraten eines Passwortes wird stark erschwert, womit der Nutzer Zeit hat, den Verlust des Dongles bei der verantwortlichen Stelle zu melden. Sollte das Passwort dreimal hintereinander innerhalb von 24 Stunden eingegeben worden sein, muss es allerdings durch die TTP entsperrt werden, was durch persönlichen Kontakt geregelt werden sollte, damit ein möglicher Dieb diese Möglichkeit nicht nutzen kann.

Im Fall der DoS-Attacken muss dafür gesorgt werden, dass vor einer rechen- und zeitaufwendigen Verifizierung (oder wofür die angegriffene Stelle speziell sorgen sollte), immer ein ganz kurzer sog. Handshake[227]

[224] Da die meisten Nutzer als Merkhilfe existierende Worte verwenden, kann man den Kreis möglicher Buchstabenkombinationen deutlich einschränken, indem man zunächst im Wörterbuch verwendete Begriffe verwendet.
[225] DoS-Attacken; zielen durch eine Überlastung von essentiellen Schnittstellen, Servern usw. darauf ab, dass diese ihren Dienst quittieren, und sich eventuell dadurch eine Lücke im System öffnen lässt, oder aber der Service einfach nicht mehr funktioniert. In der Vergangenheit wurden diese Attacken beispielsweise gegen Yahoo oder Microsoft mehrfach als Machtdemonstration eingesetzt.
[226] Durch einen Zusammenschluss von mehreren tausend Computern ist dies auch schon gelungen, allerdings mit einem Rechen- und Zeitaufwand, der in keinem Verhältnis zum möglichen Gewinn steht.
[227] Der Handshake ist eine meist sehr kurz gehaltene Erstkommunikation von Rechnern. Sie kann verschiedene Aufgaben haben.

stattfindet, der bereits eine Berechtigung bzw. den Anfragenden mehr Rechnerleistung kostet als den Server selbst. Dies wird meist in Form eines „Rätsels“ sicher gestellt. Während es den Computer eines normalen Nutzers keineswegs überfordert, das eine Rätsel zu lösen, wirkt es gegen große Anfragemengen maliziöser Nutzer als Bremse dieser Anfragen.

Auch kann über die Verteilung der Serverstruktur einer DoS-Attacke entgegengewirkt werden, weil durch die Verteilung der Server auch die Last verteilt wird, und immer nur ein Server ausfällt, was allerdings bei lang andauernden Attacken auch nur wenig nutzt. Doch Attacken von sehr großen Ausmaßen sind höchst selten und im Normalfall auf prestigeträchtigere Objekte wie eben Microsoft gerichtet.

Betroffen von dieser Art der Attacken wäre vor allem die TTP, sowie die Server des Content-Produzenten. Durch die autarke, nur teilweise onlineabhängige Konstruktion des UGS-DRMS ist allerdings eine weitere Verwendung des Systems durch den Nutzer möglich, selbst wenn kurzfristig die integrierten Server ausfallen. Allerdings nur insofern, dass man bereits erworbene Rechte weiterverwenden kann. Das Erwerben neuer Rechte funktioniert für diese Zeit nicht.

11.1.2.3. Sicherheitslücken

Die dritte Art der Attacken wird meist von Crackern verwendet, die über Sicherheitslücken (auch: „Backdoors“), Softwarefehler („Bugs“) oder andere Nachlässigkeiten einen Zugang zu dem System suchen. Leider ist es praktisch unmöglich, ein System, welches je nach Komplexität aus mehreren Millionen Zeilen Quelltext besteht, vollkommen ohne solche Lücken zu gestalten. Damit dennoch kein großer Schaden entsteht, muss das System während der Benutzung parallel auf diese Fehler untersucht werden und sog. „Hot-Fixes“[228] zur Verfügung gestellt werden.

Zusätzlich muss ein für den Benutzer optional abschaltbarer Updateservice in das Programm integriert werden, welcher für laufende Sicherheit sorgt (sowohl durch Hot-Fixes, als auch durch Erneuerung der kryptografischen Mechanismen). Von diesen Lücken im System geht mit die größte Gefahr aus, doch ist absolut kein präventive Möglichkeit gegeben. Sie müssen mit der Zeit geschlossen werden.

Zu den Sicherheitslücken sind natürlich auch übel wollende Mitarbeiter hinzuzurechnen. Doch auch gegen diese kann man, mit Ausnahme von

[228] Übersetzt etwa: „Heiße (=kurzfristige) Reparatur“; ein kleines Update, welches kritische Fehler in einem größeren Programm behebt. Meist innerhalb weniger Stunden nach bekannt werden des Fehlers veröffentlicht.

rechtlichen Schritten nach der Entdeckung, nur schlecht Vorkehrungen treffen, da sie sich außerhalb des Systems bewegen.

11.1.2.4. Systeminterne Attacken

Attacken auf...

Die systeminternen Angriffe sind in der nun zuletzt genannten Subgruppe zusammen zu fassen. Diesen Attacken muss beim Design des Systems die größte Aufmerksamkeit geschenkt werden, da hier sonst eine extrem hohe Nachbesserungsnotwendigkeit entstehen würde. Es gilt, möglichen Angriffe, die es in der Vergangenheit bereits gegen DRM-Systeme gab, und zusätzlich neue, eventuell für dieses System relevante Angriffe vorauszusehen, und bereits präventiv darauf zu reagieren. Daher werden nun die einzelnen Komponenten des Systems aufgezählt, dazu mögliche, zusätzliche Angriffstaktiken und die Reaktionen auf solche Angriffe beschrieben.

...den Dongle

Der für den Zugang zum System mitzuführende Dongle besteht aus einer Übertragungsschnittstelle, dem enthaltenen privaten Schlüssel in sicherem Speicher und einem kryptografischen Prozessor, zur Verarbeitung der Informationen.

Höchste Priorität hat natürlich die Fälschungssicherheit des Dongles, da dieser sonst, ähnlich wie eine EC-Karte, missbraucht werden kann, um in fremdem Namen Content zu empfangen oder auch zu verbreiten. Da der Dongle dazu allerdings in die Hände des Fälschers gelangen müsste, weil die relevanten Schlüssel unauslesbar auf ihm gespeichert sind, kommt der Fall dem Verlust des Dongles gleich, mit dem Unterschied, das der rechtmäßige Besitzer den Fall nicht melden kann. Darum wäre eine Abfrage angebracht, die bei gleichzeitigem Gebrauch des Dongles von zwei verschiedenen Computern, von zwei verschiedenen Netzwerken (bspw. feststellbar anhand der IPs) aus, den Dongle sperrt.

Dazu muss auch für den Fall eines Verlustes vorgesorgt werden. Daher wird der Dongle wie beschrieben durch eine zusätzliche Passwortabfrage gesichert, die bei jedem ersten Aufruf des Abspielprogramms nach dem Booten des Systems in Kraft tritt.

Ein Schutz gegen technische Angriffe auf den Dongle wurde bereits erläutert, weshalb man davon ausgehen kann, dass der private Generalschlüssel auf dem Dongle sicher ist.

Damit der Dongle seine Daten ungefährdet übertragen kann, muss die Schnittstelle zum Computer so gestaltet werden, dass erst das zu übertragende Paket, welches bereits fertig verschlüsselt ist, an einen Ausgang gelangt, da sonst einer der privaten Schlüssel (eine der verschiedenen IDs X) oder Klartext sichtbar werden würde. Denn mit

neuster Technik fällt es nicht schwer, anhand der Stromschwankungen bei der Übertragung auch von außerhalb des Kabels die Sendefolge zu erkennen.

Eine kabelgebundene Verbindung ist einfacher zu sichern als eine kabellose, da selbst beim Senden von verschlüsselten Informationen diese aufgefangen werden können, und eventuell eine Hilfe zum Entschlüsseln leisten. Da über die kabelgebundene Verbindung im Moment auch gleichzeitig der Strombedarf des Dongle für kryptografische Prozesse gedeckt werden kann, dürfte die Verbindung des Dongles via USB (wie bereits angesprochen) aus funktionaler Sicht vorteilhaft sein. Doch zukünftig werden kabellosen Technologien (W-LAN oder Bluetooth) zwangsläufig den Vorrang erhalten, wobei eben beachtet werden muss, dass sich nicht korrekt authentifizierende Geräte nicht an der Kommunikation teilnehmen dürfen. Dies kann geschehen, indem nach der Kontaktaufnahme ein einmaliger Sessionkey ausgemacht wird, der die fortlaufende Kommunikation sichert.

...die Server-Infrastruktur

Damit das gesamte System auf lange Sicht funktionieren kann, verlässt es sich stark auf die Server-Infrastruktur. Die wesentlichen Komponenten, wobei jeder einzelne Server wiederum aus mehreren, parallel geschalteten Servern bestehen kann, sind der Content-Server und der Licensing-Server, welche sich beide in der Domäne des jeweiligen Content-Produzenten befinden, sowie den Zertifikats-Server der TTP.

Zur gefahrlosen Übertragung von Daten zwischen dem Nutzer und den jeweiligen Instanzen wird die in den Grundlagen bereits angesprochene Public Key Infrastructure verwendet. Dadurch kann der Nutzer sich innerhalb der Domänen frei bewegen, ohne dass er sich immer erneut verifizieren muss, und dennoch bleibt die Sicherheit gewährleistet. Da die Kommunikation zwischen den Servern und dem Nutzer über das Internet abläuft, also über eine öffentliche und damit prinzipiell unsichere Plattform, muss die Kommunikation gegen die verschiedensten aus dem Internet bekannten Angriffe gesichert sein. Darunter fallen nahezu alle passiven und aktiven Angriffe, wie Masquerading[229], Abhören, Datenveränderung, Man-in-the-middle-Angriffe[230] und andere. Diese recht einfachen grundlegenden Angriffe sollten allerdings durch ein aktuelles kryptografisches System verhindert werden.

...das Abspielprogramm

Ohne größere Probleme wird ein fähiger Cracker den Aufbau eines Programms, welches sich auf seinem Computer befindet, zerlegen und verstehen können. Daher ist wichtig, dass keine wichtigen Daten, wie bspw. private Schlüssel, Lizenzen oder auch der Content selbst jemals

[229] Siehe hierzu auch Kapitel 11.1.2.1
[230] Diesen Angriffen wurde inzwischen durch aktuelle Protokolle die Gefahr genommen.

in Reinform vorliegen. So einfach sich diese Regel anhört, so schwer ist sie allerdings einzuhalten. Irgendwann muss das Abspielprogramm die Schlüssel, Lizenzen oder den Content auch verwenden. Und auch das Abfangen von Daten an computerinternen Schnittstellen[231] ist für einen versierten Cracker einfach. Eine Verschlüsselung hingegen derart feingranular zu gestalten, dass sie an diesen Schnittstellen noch ohne nennenswerte Performanz-Einbußen funktioniert, ist kaum möglich. Es sei denn wiederum, ein sicheres System würde die Verschlüsselung direkt in die Hardware integrieren. Doch genau das soll mit diesem Ansatz verhindert werden, um dem Nutzer nicht ein System aufzuoktroyieren, welches dieser nicht will.

Daher kann man davon ausgehen, dass Daten, welche auf der Festplatte lagern, unsicher sind. Zumindest falls sie ohne eine externe Schlüsselkomponente entschlüsselt werden können, sei es der Schlüssel des Nutzers auf dem Dongle oder der des Content-Produzenten auf dessen Server. Die Konsequenz daraus ist, dass essentielle Daten, die einem Angreifer eine Komponente in die Hand spielen könnten, die dieser zum Brechen des Systems nutzen kann, nur mit Hilfe externer Schlüssel verwendet werden dürfen.

Zertifikate muss das Programm lesen können um sie umzusetzen, und es ist unkritisch, wenn ein Angreifer dies auch tun kann. Der Generierungsprozess der Zertifikate muss allerdings wiederum eine externe Komponente integrieren, da ein Angreifer sich sonst vergleichsweise einfach beliebige Rechte einräumen könnte. Daher werden Daten zusammen mit den entsprechenden Zertifikaten ausschließlich auf den Servern des Content-Produzenten generiert.

Der Content schließlich muss ebenfalls verarbeitet werden und dazu spätestens beim Verwenden des Abspielprogramms in eine Form gebracht werden, die die Ausgabekomponente des Computers auch verarbeiten kann. Hier tritt wieder die Problematik der verschiedenen Schnittstellen innerhalb eines Computers auf. Prinzipiell ist es wünschenswert den Zeitpunkt, an dem die Daten das erste Mal unverschlüsselt vorliegen, so weit wie möglich in Richtung der darstellenden Komponente zu verschieben.

Dies ist mit hohem Aufwand zumindest auf Seiten des Herstellers des DRMS verbunden, da im Prinzip in den internen Aufbau Computers des Nutzers eingegriffen werden muss. Auch hier ist wieder die Balance zu finden, zwischen für den Nutzer unzumutbaren Eingriffen in die Selbstbestimmung über seinen Computer und einem Höchstmaß an Sicherheit. Da die Daten gegen DAD-Wandlung ohnehin nicht schützbar sind, versucht man wenigstens zu verhindern, dass die Daten in

[231] Bspw. zwischen RAM und Cache

digitalem Format abgefangen werden können, damit der Schritt über die analoge Wandlung gegangen werden muss, was mit zusätzlichem Aufwand für den maliziösen Nutzer verbunden ist[232].

...die Schnittstellen

Schließlich folgen die bereits angesprochenen Schnittstellen, an denen weitere potenzielle Angriffspunkte lokalisiert werden können. Bei diesem System sind im wesentlichen drei verschiedene Schnittstellen auszumachen:

- Schnittstelle Dongle / Computer

  Nachdem durch den kabelgebundenen Dongle die Gefahr des Abhörens durch fremde Personen gebannt wurde, finden sich an dieser Schnittstelle nur Ansatzpunkte für Teilnehmer, die ohnehin in das System eingebunden sind. Damit die Kennung X des Nutzers geheim bleiben kann, muss verhindert werden, dass diese entschlüsselt werden kann. Da wie bereits dargelegt, der private Schlüssel, also die Kennung X nicht ausgelesen werden kann, besteht an der Schnittstelle nur die Gefahr, dass eventuell die Kennung durch kryptoanalytische Methoden erraten werden kann. Dazu zählt auch, wenn man immer wieder anders lautende Anfragen stellen kann, die nach für die Kryptoanalyse günstigen Gesichtspunkten ausgesucht werden. Daher sollte ein sicherer Kanal zwischen dem Dongle und dem Programm erstellt werden, zumindest um dem Angreifer weitere Steine in den Weg zu legen. Sollte dieser allerdings alle Mittel einsetzen, stünde es ihm frei das Abspielprogramm zu modifizieren, welches die Anfragen in seinem Sinn an den Dongle stellt.

  Der sichere Kanal würde bspw. durch einen kryptografischen USB-Treiber geschaffen werden, der bei Anfragen des Abspielprogramms eingreift, und den sicheren Kanal etabliert. Zu bedenken ist auch hier wiederum der Eingriff in den Computer des Nutzers, welchen dieser nicht gutheißen wird.

- Computerinterne Schnittstellen

  Dieser Punkt kann recht kurz abgehandelt werden, da es einfach noch nicht möglich ein hoch performantes, für den Nutzer auch erschwingliches System zu schaffen, welches eine Mikrokryptografie umsetzen kann. Doch zum Glück bleibt das Abhören dieser Kommunikation nur den besten Crackern vorbehalten.

- Schnittstelle Computer / Ausgabekomponente

  Weiter oben bereits angesprochen, folgt an dieser Stelle nun die genaue Ausgestaltung der Ausweitung des Schutzes: Damit der

[232] Dies ist auch eine Maßnahme um dem Angreifer „privater Nutzer“ die Entfernung von Lizenzen so unkomfortabel wie möglich zu machen.

Content nicht bereits im Inneren des Computers unverschlüsselt vorliegt, soll ein Treiber mit kryptografischen Fähigkeiten, der sich nur für Übertragungen zwischen DRMS und Ausgabekomponente einschaltet, den Content erst bei der unmittelbaren Verwendung entschlüsseln. Denn bspw. modifizierte Audiotreiber könnten sonst die an die Soundkarte gerichteten Daten abfangen, und in eine Datei ohne Schutz umlenken.

Doch das Problem wird damit nur ein wenig herausgezögert. Spätestens an einem digitalen Ausgang liegen die Daten wieder unverschlüsselt vor und nach Verlassen des Computers kann die Verschlüsselung nicht mehr aufrecht gehalten werden, weil die Endgeräte (Monitor, Lautsprecher usw.) nicht in der Lage sind, solcherlei Daten zu verarbeiten.

Fazit

„Die Kette st nur so stark, wie Ihr schwächstes Glied."
So lautet ein bekannter Spruch, und auch bei einem DRM-System ist dies so. Nachdem nun die einzelnen Komponenten so sicher, wie möglich gemacht wurden, stellt sich nunmehr die Frage nach immer noch offen stehenden Türen für die Angreifer, und wie diese zu verbarrikadieren sind, wenn sie sich schon nicht verschließen lassen.

Eine weitere Möglichkeit, die allerdings auch nur geringen Schutz verspricht, wäre es, dem Dongle die Aufgabe einer Integritätsprüfung zu übertragen. Doch hier scheitert es wohl an Rechenleistung und an der mangelnden Update-Fähigkeit[233] des Dongles, welche aus sicherheitstechnischen Überlegungen notwendig ist.

Insgesamt ist zu sagen, dass das System zwar recht sicher gestaltet werden kann, es aber einem versierten Angreifer mit dem festen Vorhaben es zu knacken nur das Leben schwer machen, diesen jedoch nicht zurückhalten kann.

11.2 Sicherheit des Nutzers

11.2.1 TTP

Da das Konzept der Trusted Third Party nun schon häufiger bemüht wurde, soll an dieser Stelle nun ein praktisches Beispiel folgen, welches das grundlegende Konzept am besten erläutern kann. Es ist vorgesehen, dass für entsprechende Ausnahmen immer passende TTPs gewählt werden, da so der Aufwand zur Schaffung dieses doch recht komplexen Systems minimiert wird. Ins Auge gefasst werden bspw. die

[233] Bei einem Update des DRMS ändert sich auch der auf dem Dongle eingetragene Prüfwert, womit der Dongle ebenfalls ein Update erhalten müsste.

Universitäten bezüglich der Wissenschaft oder Gerichte bzw. Staatsanwaltschaften im Fall der Rechtspflege.

Beispiel

Für das Beispiel will der Student S sich ein geschütztes, von seinem Professor P jedoch für die Lehre verwendetes Buch des Verlages V herunterladen und ansehen. Normalerweise müsste dieser Prozess nicht über den Verlag laufen, da die Ausnahme vom Gesetz garantiert wird, doch im Interesse eines lückenlosen Schutzes, sieht der Verlag diese Möglichkeit vor. Genau dies soll noch einmal hervorgehoben werden, da dieser Punkt genau den Unterschied zwischen dem hier entwickelten UGS-DRMS und einem herkömmlichen DRMS ausmacht.

In diesem UGS-DRMS funktioniert der Ablauf ähnlich reibungslos und dazu mit höherem Komfort, wie ohne die Teilnahme des Content-Produzenten. Denn der Aufwand des Kopierens würde wegfallen und durch zwei Eintragungen in das System der TTP ersetzt.

Da es sich hier um ein Beispiel aus der Lehre bzw. Wissenschaft handelt, wird die entsprechende Universität als TTP ausgewählt, da diese ohnehin über Kenntnis ihrer Studenten bzw. Professoren verfügt.

Ablauf

Im Beispiel nun meldet Professor P das Buch des V als Lehrmittel für seine Studenten an, mit entsprechender Seitenangabe falls nötig. Die Studenten, die an der jeweiligen Vorlesung teilnehmen, melden dieses Vorhaben ebenfalls an. Hier würde das Studiensekretariat in Frage kommen, da es ohnehin studentische Belange verwaltet.

Nach der Meldung können die Studenten bequem vom Computer aus die angegebene Literatur anfordern. Sie melden sich mit ihrer Kennung X[234] bei dem Verlag. Dieser fragt bei der TTP, also der Universität an. Selbige verfügt über die Metakennung der Studenten, und kann daher einen Bezug zwischen der gesendeten Kennung X und einem bestimmten Studenten herstellen. Sofern dieser Student als Teilnehmer der Vorlesung eingetragen ist, gibt die TTP eine bestätigende Meldung an den Verlag zurück, woraufhin dieser dem Studenten eine DRM-geschützte Version des Buches zuschickt, zusammen mit einer Lizenz, die die Rechte auf die notwendige Verwendung beschränkt. Also bspw. „Nur-Lese-Zugriff für ein halbes Jahr, drucken einmal möglich“.

Fazit

Alle drei Seiten haben aus diesem Szenario klare Vorteile. Der Professor muss sich nicht mehr um die Zugänglichmachung der Lehrmaterialien kümmern, wofür er eventuell wertvollen Etat seines Lehrstuhls opfern müsste. Der Student hat keinerlei Nachteile aus der Situation, da seine Daten ausschließlich bei der Universität verbleiben.

[234] Davon ausgehend, dass sie den Dongle (beispielsweise integriert in den Studentenausweis bei der Immatrikulation) und das personalisierte Abspielprogramm schon haben. Genaueres zum Ablauf siehe Kapitel 12.

Er hat gleichzeitig aber ubiquitären Zugriff auf die Daten, da der Zugriff immer wieder und vor allem von verschiedenen Computern aus funktioniert. Und schließlich hat der Verlag den Vorteil, dass das Buch nicht den Kreislauf des DRMS verlässt, der Schutz also weiterhin besteht.

Außerdem erlaubt dieser Vorgang in anderen Gebieten eine genauere Erhebung der vergütungspflichtigen Kopiervorgänge, die ja für die Höhe der Pauschalabgaben erforderlich sind. Ebenso kann der Content-Produzent in anderen Bereichen, bspw. beim Vertrieb von Musik anhand der ihm übermittelten ID X anonyme Benutzerprofile erstellen und darauf sein Angebot ausrichten.

Der einzige Nachteil dieses Szenarios ist unbestritten die Kostenfrage. Denn für den Parallelbetrieb der vielen verschiedenen TTP fallen nicht unerhebliche Kosten an. Würden diese auf den Nutzer umgesetzt werden, wäre dieser wohl kaum bereit die entstehenden Preise zu bezahlen. Gleichzeitig ist den TTPs im Normalfall nicht zuzumuten diese Kosten selbst zu tragen, da ihr Amt wie im Beispiel der Universität eher ehrenamtlich ist.

11.2.2 Motivationssystem

Da die Daten nicht vollkommen sicher vor unautorisiertem Zugriff gestaltet werden können, bildet ein Motivationssystem eine zentrale Rolle in einem neuen DRMS. Das Motivationssystem des UGS-DRMS besteht, wie in Kapitel 10 angedeutet, aus drei Schichten. Wobei die erste Schicht, das sog. Give-away, wohl keiner Erklärung bedarf.

Zusätzliche Möglichkeiten

Schicht zwei besteht aus zusätzlich integrierten Umsetzungen von Schrankenregelungen. Dadurch, dass das System funktioniert, kann sich der Content-Produzent es leisten, weitere gesetzliche Ausnahmen in sein System einzubauen, obgleich diese nicht durchsetzungsfähig nach § 95 b UrhG wären. Wie dies funktionieren kann, soll am Beispiel der Privatkopie durchexerziert werden. Selbstverständlich kann man analog auch weitere Schrankenregelungen umsetzen, doch ist die Privatkopie wohl die wichtigste.

Die Daten sind als Container vorhanden, und diesen Container darf das Abspielprogramm (weil ohne einen der privaten Schlüssel) nicht verändern können, da sonst Angreifer einen vergleichsweise einfachen Weg zur Manipulation des Contents finden können. Die Idee wird vorrangig auf einer abstrakten Ebene dargestellt, um nicht mit programmiertechnischen Details zu verwirren.

Der Content-Container wird mit einer von außen zugänglichen Schnittstelle versehen, auf die das Abspielprogramm Zugriff haben kann

und soll. Man kann sie sich als Platz für ein Etikett vorstellen, welches die ID X des begünstigten der Privatkopie tragen soll. Bei Erwerb der vollen[235] Lizenzen für den Content, wird dieser ja bereits mit dem „Etikett“ des Erwerbers versehen.

Der Vorgang der Privatkopie erfolgt nun durch den Anschluss des Dongles des Begünstigten an den Computer mit dem Abspielprogramm des Erwerbers. Das Abspielprogramm setzt nun die ID X des Begünstigten auf den freien Etikettenplatz[236]. Nun kann der Begünstigte den Content-Container ganz normal auf seinen eigenen Computer portieren und auch verwenden. Natürlich mit dahingehend eingeschränkter Funktionalität, dass bspw. bei Texten ein Ausdruck nicht möglich ist, bei Liedern das Überspielen auf externe Geräte usw.. Und auch eine weitere Privatkopie ist nicht möglich, der dafür vorgesehene Platz ist ja nun durch die ID des neuen Nutzers besetzt..

Ein Missbrauch des Systems ist zwar nicht ausgeschlossen, doch da erstens ein persönlicher Kontakt zwischen Erwerber und Begünstigtem vorliegen muss (wie es das Gesetz eigentlich auch vorsieht), und beide IDs im Container gespeichert sind, wird man sich genau überlegen, an wen man seinen Content privat weiterkopiert.

Vorteile dieser Zugeständnisse sind mannigfaltig: Zunächst einmal erhält der Nutzer ein weitaus flexibleres Programm und kann dadurch entsprechend mehr mit seinem erworbenem Content anfangen. Er erkennt zusätzlich auch den guten Willen des Content-Produzenten. Für ihn ist dies also eine Art Mehrwertdienst (VAS). Auf der anderen Seite profitiert der Content-Produzent vom gestiegenen Vertrauen des Nutzers. Zudem erhält er bei geeigneter Implementierung, wie bspw. der Onlinemeldung einer Privatkopie einen Überblick über das Gesamtaufkommen von Privatkopien, was zum Festlegen der Höhe von Pauschalabgaben herangezogen werden kann. Die direkte Vergütung sollte der Content-Produzent nicht anstreben, da sonst der Vorteil des Mehrwertes einer Privatkopie sich eher ins Gegenteil verkehrt, und die Nutzer darin nur eine neue Möglichkeit sehen, dass der Produzent einen ehemals freien[237] Vorgang nutzt um noch mehr Geld „abzuzocken“.

Ein weiterer Vorteil ist die Erzeugung von Netzeffekten. Bei Weitergabe des Contents braucht der weitere Nutzer natürlich ebenfalls das

[235] Der oben beschriebene Student S bekommt bspw. keine Privatkopiefunktionalität bei dem ihm zugeteilten Content.
[236] Dies muss eventuell über den Umweg des Content-Servers geschehen, da der Container mit dem Schlüssel des Erwerbers verschlüsselt ist und das Abspielprogramm diese Verschlüsselung nicht ändern kann.
[237] Zumindest nach ihrer Sichtweise war der Vorgang der Privatkopie in der Praxis schon jeher frei. Die dahinter stehende gesetzliche Regelung dürfte nur wenigen bekannt gewesen sein.

Abspielprogramm des UGS-DRMS. Und viele werden wohl für kostenlosen Content sich anmelden und das Abspielprogramm herunterladen. Und wenn es einmal auf dem Rechner ist, ist schon der erste Schritt getan, dass der neue Nutzer eventuell auch teilnimmt.

Der letzte Vorteil betrifft speziell die Umsetzung der Ausnahme „Privatkopie“. Der oben beschriebene Vorgang erlaubt erst die Nutzung des Bonussystems:

Bonussystem

Die dritte Schicht schließlich ist das Bonussystem. Es kombiniert die Umsetzung der Privatkopie im UGS-DRMS mit dem grundlegenden Konzept der Superdistribution, wie es im Potato-Modell verwendet wurde.

Ausgehend von der erwünschten Weitergabe von Content auf dem Wege der Privatkopie setzt das Bonussystem ein und generiert weiteren Mehrwert für den Nutzer. Wenn der Begünstigte der Privatkopie sich entscheidet eine unbeschränkte Version des Contents zu erwerben, meldet er dies unter Vorlage eines Zahlungsnachweises dem Content-Produzenten und erhält von diesem, nachdem die alte Version deaktiviert wurde, eine neue Version, bei der er der Erwerber und somit auch der Privatkopierberechtigte ist.

Um es mit obigem Beispiel auszudrücken: Das Etikett mit seiner ID X wandert vom zweiten Feld auf das erste, und Etikett des ersten Feldes wird benutzt um dem Distributor eine Bonusgutschrift zu geben.

Diese Bonusgutschrift kann vielfältigster Natur sein. Im Normalfall allerdings werden es wohl virtuelle Münzen sein, mit denen man bei dem Content-Produzenten weiteren Content oder auch Prämien erwerben kann, wenn genügend dieser Münzen angesammelt wurden. Die ideale Höhe dieser Vergütung lässt sich ohne genauere Studie nicht bestimmen, doch muss sie hoch genug sein, um einen Anreiz zu bieten, aber doch niedrig genug, damit nicht der Gewinn zu sehr schmilzt. In der Praxis dürfte sie wohl bei etwa drei bis fünf Prozent des Wertes der kopierten Ware liegen.

Zum Abschluss soll noch darauf hingewiesen werden, dass sicherlich der Wunsch nach weitergehender Superdistribution und der Wunsch nach weniger Privatkopien bei den Produzenten gegeneinander arbeiten, doch muss sich der ideale Balance-Punkt erst in der Praxis finden.

Fazit

Dieses dreischichtige Motivationssystem ist sicherlich geeignet, die Motivation der Nutzer zu erhöhen, doch wird es nicht über anderweitige Fehler hinwegtäuschen, die sich in ein solches DRM-System einschleichen können. Daher darf ein DRMS nicht einfach um die Komponente „Motivationssystem“ erweitert werden, sondern muss

ganzheitlich auf ein Miteinander von Nutzern und Content-Produzenten ausgelegt sein, damit es überhaupt in der Praxis eine Chance haben kann.

12 Funktionsweise des UGS-DRMS

Abschließend soll nun das implementierte System anhand eines typischen Vorgangs vorgestellt werden.. Es wird unterschieden, zwischen den Vorgängen, die der Benutzer sieht, und den im Hintergrund ablaufenden Prozessen, welche das eigentlich UGS-DRMS ausmachen.

Die handelnden Personen sind die des vorangegangenen Kapitels, die Namensgebung der Komponenten orientiert sich an den in Kapitel 11 eingeführten Kurzbezeichnungen. Der Vorgang wird anhand der folgenden, im Ablaufdiagramm auf nächsten Seite ersichtlichen, Prozeduren dargestellt:

- Akquise des Abspielprogramms
- Authentifizierung
- Akquise des Contents
- Überprüfung der Lizenz
- Abspielvorgang

12.1 Strategische Initialisierung des UGS-DRMS

Damit dieses komplexe System in Kraft treten kann, muss zunächst die Infrastruktur geschaffen werden. Darunter fallen die folgenden Punkte, auf die nicht näher eingegangen werden soll.

- Bestimmung von TTPs für die jeweiligen Bereiche
- Produktion generischer Dongles
- Verteilung der personalisierten Dongles an Nutzer
- Schaffung der Server-Infrastruktur
- Schaffung einer Stelle zur Akquisition des Dongles
- (Schaffung der rechtlichen Grundlagen)

Danach kann das eigentliche UGS-DRMS benutzt werden. Der letzte Punkt ist, wenn auch sehr wichtig, lediglich subsidiär für die Funktion des Systems und wurde daher eingeklammert.

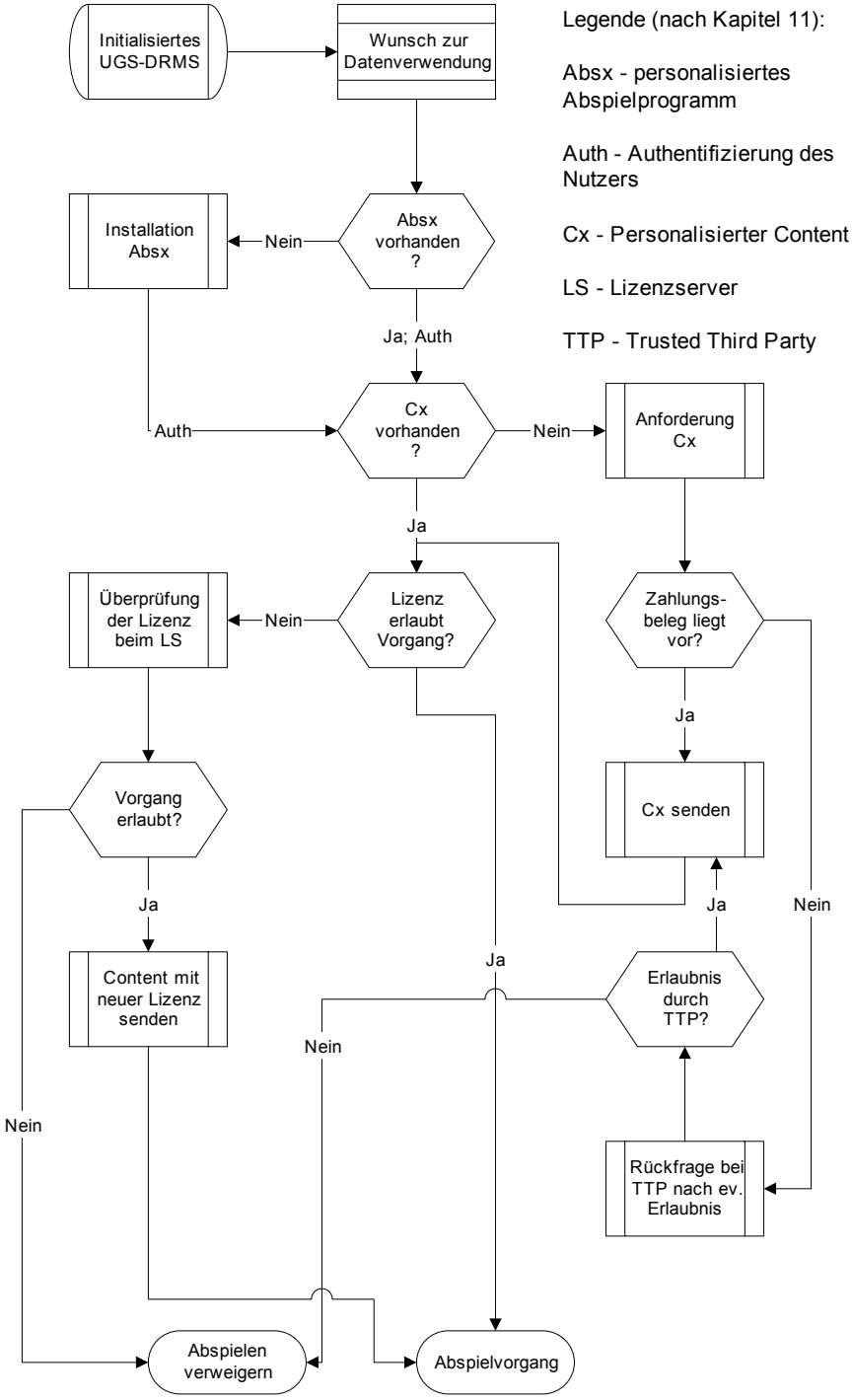

Abbildung 7: Ablaufdiagramm

12.2 Akquise des Abspielprogramms

12.2.1 Generell

Bei Erstkontakt oder Verwendung eines fremden Computers wird das Abspielprogramm des UGS-DRMS nicht vorinstalliert sein, weshalb bei Auftreten des Wunsches Content aus der Domäne des entsprechenden Content-Produzenten zu verwenden, der Computer des Nutzers vor der ersten Verwendung eines Daten-Containers angepasst werden muss.

Der Nutzer erhält eine Version, die eine vom Licensing-Server neu generierte Kennung enthält, welche dieser zu der gesendeten ID X des Nutzer in Bezug setzt.

12.2.2 Sichtbar

Student S besucht die Homepage des Verlages V und erstellt einen Account. Sobald er eingeloggt ist, steckt er den Dongle ein. Das personalisierte Abspielprogramm wird installiert. Diesen Vorgang kann er jederzeit von jedem beliebigen Computer aus wiederholen.

12.2.3 Verborgen

Sobald S den Dongle mit dem Computer verbunden hat, stellt die Internetseite des V eine Verbindung zum Dongle her, sendet den eigenen öffentlichen Schlüssel und erfährt dafür von diesem die ID X[238]. Dabei wird sowohl der Schlüssel des V, als auch die ID X des Nutzers von der TTP bestätigt. Der Dongle speichert ID X und den Schlüssel des V ab. V generiert ein neues Schlüsselpaar Z, das er mit ID X in Verbindung setzt und fügt den privaten Schlüssel in das Abspiel-programm ein und sendet den öffentlichen an den Dongle. Das personalisierte Abspielprogramm wird installiert. Nun ist der Computer für die Verwendung des Contents präpariert.

12.3 Authentifizierung

12.3.1 Generell

Wie beschrieben ist die Authentifizierung notwendig, damit mit einem fremden Dongle kein direkter Missbrauch betrieben werden kann.

[238] Entweder wird die ID X neu generiert oder der Dongle sendet eine bekannte, falls er feststellt, dass er den Schlüsse von V bereits kennt.

12.3.2 Sichtbar

Der Student S steckt seinen Dongle in den Computer und authentifiziert sich einmalig im daraufhin aufgehenden Fenster. Er gibt seinen bei Erhalt des Dongles frei gewählten Nutzernamen und anschließend das festgelegte Passwort ein. Ab diesem Zeitpunkt funktionieren seine Daten wie gewohnt.

12.3.3 Verborgen

Der Dongle bekommt ein durch den privaten Schlüssel des Abspielprogramms signiertes und seinen eigenen öffentlichen Schlüssel verschlüsseltes Paket gesendet, welches eine Zufallszahl, sowie einen Zeitstempel[239] enthält. Zusätzlich erwartet er ein zweites Paket, welches den gleichen Zeitstempel enthält und zudem Nutzernamen und Passwort. Dann entschlüsselt der Dongle beide Pakete und verschlüsselt Zeitstempel und die Zufallszahl mit dem zur ID X gehörigen privaten Schlüssel.

12.4 Akquise des Contents

12.4.1 Generell

Ebenso wie bei der Akquise des Abspielprogramms nimmt der Nutzer Kontakt zum Content-Produzenten, nur geschieht es in diesem Fall über das Abspielprogramm. Sofern der Content also noch nicht auf dem Computer vorhanden ist, wählt der Nutzer den gewünschten Content bspw. als Kennung aus einem Online-Katalog aus. Da in diesem UGS-DRMS noch kein Bezahl-System integriert wurde, wird von dem Vorliegen eines externen Zahlungsbeleges ausgegangen.

12.4.2 Sichtbar

Student S surft auf die Internet-Seite des V und findet dort in einem Katalog das Buch, welches P als Lehrmittel gekennzeichnet hat, und fragt dieses an. Dazu steckt er seinen Dongle ein und gibt die Kennung des Buchs in das Abspielprogramm ein, welches den Content herunter lädt.

[239] Der Zeitstempel soll ausschließen, dass jemand einfach die Pakete abfängt und sie in verschlüsselter Form ohne wissen über den Inhalt wieder verwenden kann (Replay-Attacke).

12.4.3 Verborgen

Das Abspielprogramm übermittelt V die Kennung des gewünschten Buchs. Nun prüft der Licensing-Server des V zunächst ob in seiner Datenbank eine Lizenz oder ein Zahlungsbeleg vorliegt, die S berechtigt dieses Buch als Vollversion zu erhalten. Sofern dies der Fall ist, wird das Buch präpariert und an S übermittelt.

In dem bewusst gewählten Beispiel findet der Licensing-Server weder eine Lizenz, noch einen Zahlungsbeleg, da es keinen gibt. Weil S bei der Meldung sich als Student identifiziert hat, frägt der Licensing-Server des V nun bei der TTP – also der Universität[240] – nach, unter Nennung der ID X. Die TTP bestätigt in der Tat, dass es sich bei S um einen Teilnehmer der Vorlesung des P handelt und dass P dieses Buch (eventuell mit entsprechenden Seitenzahlen) als Lehrmittel angegeben hat.

Der Licensing-Server weist daraufhin den Content-Server an, das Buch in eingeschränkter Form zu präparieren und schließlich an S zu senden. Wäre S kein Student, würde die TTP ablehnend antworten und der Licensing-Server entsprechend einen ablehnenden Bescheid an das Abspielprogramm des S senden, mit der Bitte, den Content zu erwerben.

12.5 Überprüfung der Lizenz

12.5.1 Generell

Wenn ein Nutzer Content immer wieder verwendet, wird dieser im Allgemeinen bereits auf dem Rechner vorliegen. Zur Vorbereitung des Abspielens wird zunächst die Lizenz, die dem Container beigefügt ist überprüft und festgestellt, ob die gewünschte Verwendung auch erlaubt ist. Schließlich könnte sich in der Zwischenzeit einiges verändert haben. Bestes Beispiel dafür sind Lizenzen, die nur für einen bestimmten Zeitraum gültig sind. Damit eine stetige Onlineverbindung nicht notwendig ist, werden langfristige Status-Änderungen[241] nur beim Integritätscheck quartalsweise oder auf Initiative des Nutzers hin online überprüft.

12.5.2 Sichtbar

Student S startet sein Abspielprogramm, authentifiziert sich und startet den Content.

[240] Entweder könnte man hier eine Baumstruktur schaffen, damit V sich immer nur an eine TTP wenden muss, oder S muss weitergehende Informationen über seine Universitätszugehörigkeit preisgeben.
[241] Bspw. die Exmatrikulation, eine Behinderung und dergleichen

12.5.3 Verborgen

Da in diesem Fall der Content vorhanden ist, entschlüsselt das Abspielprogramm unter Zuhilfenahme des Dongles die Lizenzinformationen, die dem Content beigefügt sind. Sofern nach diesen Informationen die gewünschte Verwendung des Contents rechtens ist, startet der Vorgang.

Sollte die Lizenz jedoch anderes ergeben, kontaktiert das Abspielprogramm den Licensing-Server des V und lässt die Lizenz von diesem überprüfen. Bei positivem Prüfergebnis wird der Content erneut mit nun gültiger Lizenz an den Nutzer übertragen. Bei negativem Prüfergebnis hingegen wird der Nutzer darüber informiert und der Content-Container wird gelöscht.

12.6 Abspielvorgang

12.6.1 Generell

Der Abspielvorgang tritt nach den vorangegangenen Schritten je nach Ergebnis nun in Kraft oder auch nicht. Wie bereits thematisiert ist hier die kritischste Stelle des ganzen Systems, da nun der Content im Klartext vorliegen muss und nur das Wasserzeichen die letzte Barriere vor der weltweiten, freien Distribution bildet.

12.6.2 Sichtbar

Je nach Art des Contents beginnt Musik aus den Lautsprechern zu tönen und/oder der Bildschirm einen Text oder Film anzuzeigen. Im Beispiel kann S nun das Buch des V lesen.

12.6.3 Verborgen

Das Abspielprogramm erhält das Paket von der Authentifizierung und sendet den Content an den Dongle zur Entschlüsselung. Damit bei der Rücksendung des Contents in entschlüsselter Form der Content nicht abgefangen werden kann, wird zuvor über einen speziellen kryptografischen USB-Treiber, sowie über spezielle kryptografische Treiber der Ausgabe-Komponenten ein sicherer Kanal durch den Coputer hindurch aufgebaut, damit die Daten zumindest innerhalb des Computers geschützt sind. Wichtig ist hierbei auch, dass immer nur Teile des Contents unverschlüsselt in den verschiedenen Speichern des Computers vorliegen.

13 Anpassung der rechtlichen Situation

In den letzten Jahrhunderten hat das Urheberrecht im analogen Bereich gute Dienste geleistet. Durch die Möglichkeiten der neuen Technik beginnt es seinen Einfluss zu verlieren und ein Bedarf für Veränderungen entsteht. Das folgende Kapitel will nun Änderungen beleuchten, die dem Urheberrecht zum Sprung in das Informationszeitalter verhelfen könnten. Eine umfassende Bewertung dieser Änderungen ist im Rahmen dieser Arbeit leider nur sehr rudimentär möglich.

Dazu die Frage gestellt werden, ob das Urheberrecht ausgedient hat oder ob es erneuert werden kann, sei es indem der analoge und der digitale Bereich getrennt werden, oder sei es, dass nur die bereits geltenden Regelungen reformiert werden. Es sei an dieser Stelle bereits verraten, dass die Trennung in analoges und digitales Urheberrecht befürwortet wird.

Für den digitalen Bereich werden Änderungen nötig, die diesen vom analogen Bereich abgrenzen und auf die Besonderheiten eingehen. Anhand der Arbeitsgruppen, welche in Kapitel 4.5.2 vorgestellt wurden, werden sechs spezielle Einzelthemen aufgegriffen und einzeln betrachtet.

Im Anschluss daran werden einige zusätzliche Punkte beleuchtet, die einer Klärung bedürfen. Hierunter fällt bspw. die Problematik, wie ein faires DRMS, wie das hier vorgestellte, weitergehende Unterstützung durch das Gesetz erhalten kann.

Besonders wichtig ist es für das reformierte Urheberrecht, dass es bereits in der Praxis bestehende Probleme löst. Daher soll als Abschluss im speziellen auf einige Beispiele eingegangen werden.

13.1 Abschaffung oder Erneuerung des UrhG?

Man mag sich die Frage stellen, ob das Urheberrecht im Informationszeitalter überhaupt noch einen Sinn hat. Beispielsweise gibt es immer wieder Vorstöße von Befürwortern eines freieren Umgangs mit Information[242]. Das Urheberrecht schränkt den Umgang mit Informationen fraglos ein. Doch würde der Markt sich ohne das Urheberrecht auch wirklich selbst regulieren? In Anbetracht der

[242] Prominentes Beispiels ist die Aussage des US-Softwarepioniers Richard Stallmann: "Nur ein Polizeistaat kann im Zeitalter des Computers die Einhaltung des derzeit geltenden Urheberrechts garantieren"; anlässlich dem Forum des Jahres 2002 der European Media Master of Arts. Siehe dazu auch [53] und [54]

Situation, in der viele Content-Produzenten härteste Regularien fordern, damit eben der Datenklau aufhört, und sich immer mehr Nutzer formieren, die teilweise am Content-Produzenten vorbei sich die Daten beschaffen, ist dies doch stark zu bezweifeln.

Das Urheberrecht würde seine Daseinsberechtigung nur verlieren, wenn es die sich selbst gesteckten Ziele nicht mehr erreichen würde. Diese Ziele sind zum einen der Schutz des geistigen Eigentums und der daraus erwachsenden Interessen[243] und zum anderen das Wohl der Gesellschaft. Auch wenn dies pauschal formuliert ist, ergeben sich hieraus im Wesentlichen die Zieldefinitionen:

- Sicherstellung der Verwertung von geistigem Eigentum
- Erhaltung des „informationellen" Wohls der Gesellschaft

Gerade der erste Punkt wird zwar im analogen Bereich ausreichend gesichert, doch nicht in dem für die Informationsgesellschaft wichtigeren digitalen Bereich. Daher bemühen sich auch die bereits angesprochenen Vertragspartner multinationaler Verträge wieder den Schutz zu gewährleisten. Doch im Gegensatz zur früheren Situation, in der Content und Medium noch nicht trennbar waren, kann der Staat dies nicht alleine schaffen. Seine Aufgabe besteht nunmehr darin, ein geeignetes Rahmenregelwerk bereit zu stellen, anhand dessen sich Content-Produzenten und Nutzer arrangieren.

Diese Aufgabe ist deutlich komplexer, als es den Anschein hat. Denn es ist nicht allein die Tatsache, dass die drohende digitale Spaltung der Gesellschaft verhindert werden und auch den Produzenten ein wirksames Gesetz zur Seite gestellt werden muss[244]. Vielmehr muss dieses Gesetz auch in der Lage sein, in einer extrem kurzen Zeitspanne auf Änderungen der Umgebungsvariablen zu reagieren, da sich die Informationstechnik und im Speziellen das Internet noch in der Entwicklung befinden und diese rasant voranschreitet. Ein Gesetz, welches auf dem üblichen Weg beschlossen wird, ist beinahe schon beim Termin der Erscheinens veraltet und hätte neuen Überarbeitungsbedarf.

Wie kann also ein derart dynamische(re)s Urheberrecht erreicht werden?

Aufspaltung des UrhG

Zunächst einmal bietet es sich an, die digitale Welt, die etwas bisher nie da gewesenes darstellt, auch vollständig von der analogen zu trennen. Damit würde auf der einen Seite der Prozess entfallen, bei der Schaffung neuer Gesetze auf den analogen Bereich Rücksicht nehmen

[243] Dieser ist sogar in der „Allgemeinen Erklärung der Menschenrechte der Vereinten Nationen" in Artikel 27 II zu finden. [55]
[244] Diese Implikationen ergeben sich aus dem „Tilting bottle"-Modell.

zu müssen. Auf der anderen Seite jedoch müssten geeignete Gesetze für den Übergang geschaffen werden und es gäbe das Problem, dass das gleiche Immaterialgut je nach seiner aktuellen „Form“ unterschiedlichen Gesetzen unterliegen würde, was natürlich nicht gerade für Rechtssicherheit sorgt.

Getreu dem abgedroschenen, aber dennoch allzu wahren Grundsatz “Never change a winning Team[245]“ könnte das alte Urheberrecht, der Einfachheit ab sofort als analoges Urheberrecht (UrhG) bezeichnet, in unveränderter Form seinen Dienst verrichten. Das neue (digitale) Urheberrecht (DUrhG) erwächst zunächst aus seinem analogen Ahnen, kann sich aber ab sofort entsprechend den Notwendigkeiten weiter entwickeln.

Das ganze müsste natürlich mit den internationalen Vertragspartnern abgestimmt werden. Zudem müsste auch ein Prozess in Gang gebracht werden, der es Vertragsstaaten bspw. der RBÜ erlaubt, schneller auf eine Veränderung der urheberrechtlichen Situation zu reagieren.

Vom Aufbau soll das DUrhG zunächst aus einem recht groben Rahmengesetz bestehen, welches im Zweifel bei Regelungslücken zu einer vorläufigen[246] Auslegung durch die Gerichtsbarkeit als Generalklausel herangezogen werden kann. Dazu gibt es kleinere Themenkomplexe, wie bspw. die Schrankenregelungen oder der Schutz technischer Maßnahmen, die den entsprechenden Bereich genauer regeln.

13.2 Nachbesserung

In den folgenden Kapiteln werden nun Regelungen für das DUrhG besprochen, die jedoch noch einer umfassenderen kritischen Betrachtung bedürfen, als dass sie der Umfang dieser Arbeit zulässt. Dazu werden zunächst die in den Kapiteln 4.5.2.1 bis 4.5.2.11 bereits aufbereiteten Arbeitsgruppen für den zweiten Korb der Urheberrechtsnovelle wieder aufgegriffen. Wie schon in Kapitel 4.5.2.12 erwähnt, sind für das hier behandelte DUrhG nur sechs Arbeitsgruppen vorrangig interessant. Und diese werden nun für die jeweiligen Themenkomplexe des DUrhG herangezogen.

Ein besonderes Problem ist die starke Verflechtung, die alle diese neuen Bereich miteinander haben. Bei der endgültigen Abwägung muss darauf geachtet werden, dass grundsätzlich keine der Parteien übervorteilt wird und zudem trotz allem immer noch der Nutzen für die Gesellschaft vorhanden ist. Daher ist es nicht zu vermeiden, dass bei den jeweiligen

[245] „Verändere nie ein siegreiches Team“.
[246] Zumindest bis eine gesetzliche Regelung besteht.

Arbeitsgruppen auch Themen der anderen Bereiche aufgegriffen werden.

13.2.1 Arbeitsgruppe Pauschalabgaben

In Deutschland erfreuen sich Pauschalvergütungssysteme großer Beliebtheit. Dies gilt zumindest, so lange man die Gesetzgeber fragt. Weder Wirtschaft noch Nutzer stimmen damit überein. Die Wirtschaft reklamiert für sich, dass neue individuelle Vergütungssysteme heute an die Stelle der aus ihrer Sicht veralteten Pauschalvergütung treten soll[247]. Die Nutzer wiederum wollen am liebsten keinerlei Abgaben zahlen.

Eine Lösung dieses Konfliktes bedarf grundlegender Berechungen, doch zunächst kann schon einmal auf der Vorarbeit der Arbeitsgruppe aufgebaut werden.

Das Pauschalvergütungssystem wird also beibehalten. Die betroffenen Geräte werden ausgeweitet. Vor allem sollten neben den bereits mit Abgaben belegten Leermedien insbesondere zum Kopieren geeignete Geräte herangezogen werden. Darunter fallen bspw. auch Geräte, die...

1. ...sich zum Abspielen von freier Musik eignen (MP3-Player[248] u.a.),
2. ...das Anfertigen einer Kopie als Hauptzweck haben (Scanner) oder
3. ...dazu geeignet sind, für Privatpersonen unwahrscheinliche Datenmengen zu speichern (HDDs jenseits der 60 GB).

Die Liste der mit Pauschalabgaben belegten Geräte könnte stetig fortgeschrieben werden. Die Aufnahmekriterien können dann dynamisch den Gegebenheiten der Situation angepasst werden. Ausnahmen zu diesen Regelungen können bspw. im geschäftlichen Bereich gemacht werden.

Bemessung der Pauschalabgaben

Die jeweiligen Geräte werden mit Pauschalabgaben belegt, genau wie es die AG vorsieht, nämlich je nach dem realen Prozentsatz ihrer Nutzung für vergütungspflichtige Kopien. Bei der Frage, wie die genaue Höhe der Pauschalabgaben sein soll, wird auf die von der AG vorgeschlagene Einigung zwischen den Parteien vertraut.

Die Höhe der Fixkosten sollt durch den schnellen Werteverfall nicht prozentual erfolgen, sondern nach gestaffelten Sätzen, je nach Leistungsfähigkeit eines Gerätes oder Datenträgers[249].

Rückerstattung

Um dennoch den Wünschen der Industrie ebenfalls zu entsprechen kann ein System etabliert werden, welches diese Pauschalabgaben

[247] Siehe auch [56} und [57]
[248] So führte Kanada unlängst eine Abgabepflicht auf MP3-Player ein. [58]
[249] Siehe loc. cit.

quasi rückerstattungsfähig macht, ähnlich wie es bei der Mehrwertsteuer funktioniert. Sollte ein Nutzer nachweisen, dass er bei einem individuellen Abrechnungsprogramm teilnimmt, kann er eine Kostenrückerstattung gegen Vorlage der Rechnung beantragen. Bei dieser Lösung steigt der Verwaltungsaufwand natürlich erheblich, doch würde man so beiden Wünschen entsprechen, dem des Staates und dem der Wirtschaft. Die Rückerstattungsfähigkeit würde dann auch Firmen zu Gute kommen, da diese im Normalfall bspw. keine Privatkopien anfertigen.

Ähnlich könnten die Pauschalabgaben auch für andere vergütungspflichtige Kopien geregelt werden. Natürlich nur insofern, falls sich der Aufwand rechnet, und nicht die entstehenden Mehreinnahmen durch die Verwaltung kompensiert werden.

Breitbandzugänge

Ein weiteres Thema stellt die Abgabenpflicht auf Breitbandzugänge dar. Manch einer verstünde dies als eine Art „Internetmaut“, welche ihn dabei behindert, seinem Recht auf Information nachzugehen. Doch kritisch betrachtet muss gefragt werden: Welche Privatperson (um bei der Privatkopie zu bleiben) benötigt selbst bei exzessiver, legaler Nutzung des Internets mehr als bspw. 5 GB Datenverkehr pro Monat? Eine genaue Grenze für die monatliche Datenmenge müsste noch festgestellt werden, doch bietet es sich an, private Breitbandzugänge ab dieser Grenze mit einer Abgabe zu belegen.

Damit wird die Privatperson nicht in seinem Wunsch nach Information eingedämmt, für den die angesprochene GB-Menge ausreicht und gleichzeitig wird der intensiven Nutzung von Tauschbörsen u.a. Steine in den Weg gelegt. Denn in der Praxis wird es wohl kaum anders funktionieren, geht man von dem Grundsatz eines *durchsetzbaren* Gesetzes aus.

Doppelte Abgaben

Die teilweise doppelte Abgabe, wie sie etwa bei Breitbandzugang in Kombination mit einer großen Festplatte anfällt, hat durchaus seine Rechtfertigung. Schließlich darf keine Produkt durch eine im Missverhältnis zu seinem Preis stehende Abgabe unverkäuflich werden, Dieser Grundsatz führt allerdings dazu, dass manche Produkte unter ihrem eigentlichen Potenzial mit Abgaben belegt werden. Und genau dies kann mit der doppelten Abgabe teilweise kompensiert werden.

13.2.2 Arbeitsgruppe Privatkopie

Die Privatkopie wurde in der Öffentlichkeit sehr emotional diskutiert und stellt ein eigenes Thema für sich dar. Hier soll zunächst die Frage geklärt werden, ob und in welcher Form die Privatkopie im DUrhG überhaupt gestattet werden soll. Im Anschluss daran erfolgt die Diskussion der Durchsetzbarkeit.

Rechtfertigung alt...

Die ursprüngliche Rechtfertigung der Privatkopie war die Minimierung des sog. Dead-Weight-Loss zum Wohle der Gesellschaft. Durch die immer feingranulareren Möglichkeiten der Zahlsysteme würde diese Rechtfertigung wohl in naher Zukunft entfallen. Dazu muss gesagt werden, dass die Industrie die Zahlsysteme zwar immer wieder ins Spiel bringt, aber es in der Praxis wohl noch kein solches mit ausreichender Verbreitung und Bedeutung gibt. Und dahingehend sollte sich der Gesetzgeber eine gewisse Skepsis behalten. Es können sehr wohl Regelungen vorgesehen werden, die solchen zukünftigen Systemen bereits Rechnung tragen, doch sollte sich die Gesetzgebung zunächst an der momentanen Situation orientieren, in der diese Systeme noch auf sich warten lassen.

...und neu

Es stellt sich nun die Frage, ob der Privatkopie nicht eine neue Rechtfertigung gegeben werden sollte, quasi als soziales Auffangbecken zu Verhinderung der digitalen Spaltung der Gesellschaft. Eine Pauschalabgabe auf Medien und wie vorgeschlagen auf Breitbandzugänge würde die gesamte Gesellschaft abfangen. Reiche, die sich mehr Kopien leisten, zahlen mehr und ärmere Menschen weniger. Durch den Freibetrag bei den Breitbandzugängen wäre das elementare Informationsbedürfnis abgedeckt und weitere Privatkopien über das Internet wären mit der Abgabe belegt. Diese Rechtfertigung scheint aufgrund des bisherigen Verständnis der Gesellschaft von der Privatkopie angemessen.

Aufteilung

Die Vielfalt der Daten, die unter das DUrhG fallen[250] rechtfertigt die von der Arbeitsgruppe vorgenommene Aufteilung in die jeweiligen Datenarten: Literatur, Film, Musik. Da diese Aufteilung nicht ganz ausreichend erscheint[251], sollen an dieser Stelle Computerprogramme als eigenständige Datenart hinzugenommen werden.

Musik

In der Arbeitsgruppe wurde von Seiten der Musik-Industrie das Verbot der Privatkopie im Bereich digitaler Musik bei gleichzeitigem Verzicht auf Pauschalabgaben vorgeschlagen. Dies mag für die ursprüngliche Rechtfertigung der Privatkopie eine probate Lösung sein, doch sollte die reformierte Privatkopie auch im digitalen Bereich weiterhin existieren.

Da die momentane Situation, in der die Daten heiß umkämpft sind, allerdings sicher nicht als ideal angesehen werden kann, wäre ein Mittelweg denkbar. Die Privatkopie von neuer Musik sollte erst nach einem angemessenen Zeitraum legal werden, dies entspricht auch der Idee, die bereits in Kapitel 8.1 angesprochen wurde: Der Nutzer würde in erster Linie für die Aktualität des Contents zahlen und die „Sperrfrist“ würde dennoch einen angemessenen Absatz ermöglichen.

[250] siehe hierzu Kapitel 6.1
[251] siehe hierzu Kapitel 13.3.3

Film

Ähnlich verhält es sich mit Filmwerken. Eine Privatkopie im digitalen Bereich ist gerade angesichts der zunehmenden Verbreitung digitalen Fernsehens unumgänglich. Schließlich soll dem Nutzer bspw. die Möglichkeit, Content aus dem Fernsehen aufzunehmen, nicht genommen werden. Da der Industrie jedoch große Verluste dadurch entstehen, dass Filme teilweise aus den USA schon vor dem deutschen Veröffentlichungstermin (illegal) aus dem Internet geladen werden können, wäre auch hier eine zeitliche Beschränkung der Privatkopie denkbar. Diese sollte so lange verboten werden, bis ein Film aus den *heimischen* Kinos genommen und zudem auf Datenträgern für bspw. ein halbes Jahr erstvermarktet wurde.

Literatur

In der Literatur spielen vornehmlich zwei verschiedene Teilgebiete hinein. Zum einen gibt es die wissenschaftliche Literatur und zum anderen den Rest. Gerade im wissenschaftlichen Bereich wird der Kampf besonders erbittert geführt. Die Herausgeber von Fachmagazinen votieren energisch gegen die Durchführung der Privatkopie durch Dritte, in diesem Fall die Bibliotheken[252]. Eine Einigung kann nur eine abschließende gesetzliche Regelung bringen.

Und diese sollte definitiv im Sinne der Wissenschaft ausfallen. Denn in diesem speziellen Fall darf nicht vergessen werden, dass die Fachmagazine keinesfalls eigene geistige Werke abdrucken, sondern lediglich ein Medium darstellen, durch welches der wissenschaftliche Fortschritt vorangetrieben wird. Außerdem stützen sich die geistigen Werke selbst wiederum auf geistige Werke anderer. Daher ist es nur fair, der Wissenschaft die Werke wieder in umfassender Form zukommen zu lassen.

Dass dies zweifellos im Sinne der Gesellschaft ist, ist unstrittig. Daher wird die Regelung als sinnvoll erachtet, dass für Zwecke der Lehre und der Wissenschaftlichen Forschung ein Recht auf Anfertigung einer vergütungs- und zustimmungsfreien Kopie bestehen soll. Diese Kopie darf durch Dritte angefertigt werden, welche hierfür allerdings nur die eigenen Unkosten verlangen dürfen. Eine Weitergabe dieser angefertigten Kopie ist dem Empfänger nicht erlaubt. Gleichzeitig gilt eine zeitliche Befristung von bis zu zwei Jahren, nach der die Kopie erneut angefertigt werden muss.

Im Bereich der restlichen Literatur außerhalb der Forschung bzw. Lehre gibt es hingegen keine Rechtfertigung für eine besondere Änderung der Privatkopie. Dementsprechend gilt hier die eigene Anfertigung einer digitalen Privatkopie zu privaten Zwecken.

[252] Im Falle des Dokumentenlieferdienstes Subito wurde bereits eine Klage angestrengt.

Computerprogramme

Für die Computerprogramme und Datenbankwerke als letzten Bereich soll ein eigenes Recht entworfen werden, welches im Wesentlichen durchaus auf den Vorgaben des analogen Urheberrechts aufbaut. Zusätzlich soll es sich an den ohnehin praktizierten Lizenzsystemen orientieren, nach denen ein Programm pro Arbeitsplatz an dem es verwendet wird bezahlt wird. Im Prinzip entfällt in diesem Bereich damit die Privatkopie. Eine Möglichkeit wäre, obwohl es bis dato kein Verlangen nach einer Privatkopie in diesem Bereich gab, die gemeinsame Verwendung eines Programms in einem Privathaushalt zu gestatten, da es wohl für Nutzer nicht verständlich ist, warum ein Programm mehrfach bezahlt werden muss, bloß weil bspw. Vater und Sohn dieses verwenden wollen. Der geschäftliche Bereich muss davon allerdings getrennt werden.

Durchsetzung

Abschließend zu diesem Kapitel kommt nun die Frage nach der Durchsetzbarkeit im Sinne des §95 b UrhG. Die vorgeschalteten multinationalen Organisation ließen den beteiligten Staaten bewusst den Spielraum, ob die Privatkopie nun durchsetzbar gestaltet wird oder nicht.

Für eine Durchsetzung spricht die bereits erwähnte Umdeutung des Ziels der Schranke „Privatkopie“. Dagegen spricht bspw. das hohe Missbrauchspotenzial in der heutigen Situation. Doch dieses wiegt keinesfalls den erstgenannten Grund auf. Durch die Verankerung der Durchsetzbarkeit im Gesetz würde zwar für das UGS-DRMS ein wichtiger Punkt bzgl. des Motivationssystems wegfallen, doch sollte dies den Gesetzgeber nicht daran hindern, die Möglichkeiten auszuschöpfen, die die InfoSoc-Richtlinie ihm gewährt. Dabei sollte logischerweise die Legalität der Privatkopie beachtet werden, denn nur falls diese legal ist, darf sie durchgesetzt werden. Damit würde die Durchsetzbarkeit für die oben definierten Sperrfristen wegfallen.

Je nach Ausgestaltung der Voraussetzungen für DRMS die noch zu erläutern sind, könnte allerdings auch auf die Durchsetzung verzichtet werden, sofern anderweitig eine faire Lösung gefunden wird. Dies wäre wohl eher im Sinne der Content-Produzenten.

Um es abschließend antagonistisch zu Frau Zypries[253] zu formulieren: „Das DUrhG kennt ein Recht auf Privatkopie.“

13.2.3 Arbeitsgruppe Schranken

Unter diesem Überbegriff sind sechs einzelne Fragestellungen zusammengefasst, die jeweils mit Schrankenregelungen des Urheberrechts zu tun haben.

[253] Siehe dazu [66]

Elektronischer Pressespiegel

Hier ist der Vorschlag genau der, den die Arbeitsgruppe auch abgegeben hat: Dem Urteil des BGH folgend ist es ratsam, den Passus in das Gesetz aufzunehmen.

Elektronische Archive

Nur öffentliche, nicht kommerzielle Einrichtungen sollten zur Wahrung ihres Bestandes elektronische Archive anlegen dürfen. Denn prinzipiell ist eine Herstellung eines elektronischen Archivs eine Sache, die nur vorbehaltlich einer expliziten Erlaubnis erfolgen sollte. Schließlich kann der Content-Produzent diese Dienstleistung ebenfalls verkaufen wollen, weshalb das Anlegen elektronischer Archive ein Eingriff in seine Verwertungsrechte wäre. Bei nicht kommerziellen Einrichtungen besteht die Gefahr nicht im gleichen Maß, wie bei auf Profit ausgerichteten Einrichtungen. Möglich wäre noch die Überlegung, ob man gemeinnützigen Vereinen ebenfalls gestatten sollte, ihren Bestand auf diesem Wege zu sichern.

On the spot consultation

Prinzipiell befürchten Verlage zu recht, dass ihr Umsatz bei Bibliotheken gemindert wird, falls diesen eine Mehrfachverwendung bestimmter (besonders interessanter) Bücher gestattet wird. Doch durch die Beschränkung der On the spot consultation auf den Ort der Bibliothek wird diese Regelung genug eingeschränkt. Deshalb kann den Bibliotheken die gleichzeitige Verwendung von Content unbeschränkt gestattet werden, sofern sich zumindest noch ein Exemplar zugänglich im Haus befindet.

Zitatrecht

Durch die weitgehenden Befugnisse des Zitatrechts[254] wurde eine enge Auslegung von selbigem gefordert. Dem kann man durchaus nachkommen, aber nur insoweit die Wissenschaft dadurch nicht zu umfassend eingeschränkt wird. Gerade hier wäre auch eine dynamische Regelung angemessen, die sich in einem längeren Prozess an ein Idealmaß herantastet. Eine Beschränkung auf bestimmte Werksarten kann im Gegenzug entfallen.

Kopienversand

Da der Versand von Kopien per Email im Informationszeitalter den per Telefax wohl ablöst, spricht nichts gegen eine explizite Aufnahme der Email in diesen Paragrafen. Hier findet sich allerdings bereits eine Anwendung des noch in Kapitel 13.3.1 vorzustellenden Übergangs von analogem nach digitalem Content. Der Versand per Email von ehemals analogem Content soll nur erlaubt werden, falls die Digitalisierung auch im Umfang der Lizenz zur Verwendung des Contents enthalten ist.

Drei-Stufen-Test

Schließlich kann auch hier die Meinung der Arbeitsgruppe übernommen werden. Da der Drei-Stufen-Test bereits praktiziertes Recht ist, muss er nicht zwangsläufig in die Novelle Eingang finden.

[254] u.a. die Vergütungsfreiheit

13.2.4 Arbeitsgruppe Altbestände

Prinzipiell ist dem Paragrafen 31 IV UrhG nicht zu widersprechen, da dieser zum Schutz des Urhebers gedacht war. Dieser sollte davor geschützt werden, dass er durch die Übertragung noch unbekannter Nutzungsarten übervorteilt wird. Inzwischen hat sich durch die digitale Verarbeitung eine vollkommen neue Nutzungsart ergeben, die es möglich macht Altbestände zu werten, welche bis dato im Laufe der Jahre einfach in Vergessenheit gerieten.

Altbestand

Da die Erhaltung dieses Wissens für die Gesellschaft wünschenswert ist, muss nun eine angemessene Regelung gefunden werden, um die Verwertung von Altbeständen zu ermöglichen, bei denen keine aktuellen Rechteinhaber auffindbar sind.

Hier wäre es angemessen, die Rechteinhaber in die Pflicht zu nehmen, da sie aus der Verwertung von altem Material durch die zu zahlenden Lizenzgebühren profitieren. Dies tun die Verleger bspw. auch, doch würde ein der Aufwand der Recherche der Rechteinhaber für diese in keinem Verhältnis zum zu erwartenden Gewinn stehen, weshalb sie die Altverwertung wie bisher wohl unterlassen würden.

Angedacht ist eine Generalerlaubnis für die Verwendung von Altbeständen unbekannter Herkunft, sofern bereits ein Vertrag zur Verwertung vorlag und zum Zeitpunkt des Erlöschens der Sperrfrist noch nicht beendet war. Da dies der bisherigen Rechtsprechung zuwider läuft, muss aber für einen angemessenen Übergang gesorgt werden, auch um nicht mit dem Rückwirkungsverbot in Konflikt zu geraten, da es nur erlaubt ist das geltende Recht rückwirkend zu verändern, falls zwingende überwiegende Gründe des öffentlichen Wohls vorliegen. Dies ist hier eher zu bejahen.

Da der Rechteinhaber bereits ohne sein zutun bei Schaffung eines Werkes umfassende Schutzrechte erhält, ist es ihm also durchaus zuzumuten, seine Zustimmung oder Ablehnung zur Verwertung kundzutun, sofern er sein Werk monetär verwertet hat. Damit stünde der Weg für eine Verwertung des Altbestandes offen.

Eine Übergangsregelung könnte vorsehen, dass ab Ablauf einer Sperrfrist von bspw. zwei Jahren nach Erlass dieser Regelung Altbestände unbekannter Herkunft verwertet werden dürfen. Dies könnte bspw. gegen Zahlung einer angemessenen Lizenzgebühr in einen Treuhandfond geschehen. In der Sperrfrist haben die Urheber die Gelegenheit ihr präventives Veto gegen eine Neuverwertung an einer zentralen Stelle eintragen zu lassen. Dieses Veto-Recht bleibt auch nach der Sperrfrist bestehen.

Zukünftige Verwertung

Für die Zukunft wird es dem Urheber ermöglicht über die Verwertung seines geistigen Eigentums durch zukünftige Nutzungsarten zu verfügen. Doch es bleibt ihm auch hier ein Veto-Recht bestehen, welches er bei Verwertung seines Contents über eine neue Nutzungsart einlegen kann. Zusätzlich wird ihm eine angemessene Vergütung garantiert. Damit wird das Urheberrecht bezüglich seines Regelungsspielraumes dynamischer gestaltet.

13.2.5 Arbeitsgruppe Auskunftsanspruch

Prinzipiell ist dem Urheber ein Interesse daran zuzugestehen, Verletzungen seiner Rechte im Internet zu verfolgen. Fraglich ist nur, ob dies ihn dazu berechtigen sollte, einen Auskunftsanspruch ohne staatliche Kontrolle gegenüber den ISPs zu erlangen.

Dies muss ganz klar verneint werden. Dem Internetnutzer steht wie auch allen anderen Bürgern ein Recht auf informationelle Selbstbestimmung zu. Anderweitig könnte ein solcher Auskunftsanspruch zu Zuständen ähnlich denen in den USA führen, wo die RIAA nahezu wahllos Teilnehmer an Tauschbörsen verklagt.

Ein Auskunftsanspruch unter staatlicher Kontrolle wäre hingegen eine genauere Betrachtung wert. Durch den Weg über die staatliche Kontrolle, bspw. über eine gerichtliches System, wie von der BITKOM vorgeschlagen, könnte geregelt werden, dass auch wirklich ausreichende Gründe vorhanden sind, die Daten des Nutzers herauszugeben.

Da ISPs nur für kurze Zeit die Zuordnung zwischen Nutzer und IP-Adresse speichern dürfen, müsste die Anweisung vorgeschaltet werden, dass die Daten des Nutzers gespeichert werden dürfen. Diese Auskunft kann dann dem Staat zur Prüfung zugänglich gemacht werden. So kann der Internetnutzer auf seine Anonymität vertrauen, solange er nichts gesetzwidriges macht. Und selbst falls er etwas unrechtmäßiges tut, steht nicht dem Verletzten die Auskunft zu, sondern dem Staat.

Zudem muss ein rechtlicher Anspruch (außer der Auskunft an den Staat) der Rechtinhaber gegen den ISP ausgeschlossen werden.

13.2.6 Arbeitsgruppe Allgemeinfreiheit

Auch die Verwertung gemeinfreier Werke bedarf einer Regelung im neuen Urheberrecht. Der sog. Goethegroschen könnte eingesetzt werden, um junge Künstler zu fördern. Auch wenn die Gruppe der Verwerter gegen diese Schmälerung ihres Gewinns ist, ist es nur rechtens, wenn Leistungen, die die Gesellschaft letzten Endes erbracht hat, auch nach dem Ende des Urheberrechtsschutzes Einkommen für

die Gesellschaft generieren. Schließlich generieren sie für die Verwerter ebenfalls ein Einkommen.

In die gleiche Kasse könnten Zahlungen und Zinsen aus dem oben erwähnten Treuhandfond fließen, sofern diese durch den Urheber nicht nach Ablauf einer angemessenen Frist für sich reklamiert wurden.

13.3 Weiterer Regelungsbedarf

Im Folgenden sollen noch einige Punkte diskutiert werden, die sich im Laufe der Zeit als problematisch herausgestellt haben oder sich noch als problematisch herausstellen können. Dazu werden in den folgenden Kapiteln die angesprochenen Situationen jeweils kurz umrissen und eine Lösung angeboten.

13.3.1 Digitalisierung vs. Analogisierung

Wie bereits erwähnt, ergibt sich durch die Trennung des Urheberrechts in das neue, digitale und das alte, analoge Urheberrecht Probleme bei der Regelung des Übergangs zwischen den beiden Bereichen.

Hier sind die beiden Übergänge zu unterscheiden: Digital zu analog (Analogisierung) und analog zu digital (Digitalisierung).

Der erste Vorgang ist eher unproblematisch, da sich die Regelungen vom Übergang analog zu analog nicht sonderlich von der Analogisierung unterscheiden. Und diese Regelungen bestehen schon seit langem und haben sich bewährt. Gerade der Prozess der Verbreitung geht im analogen Bereich eher langsam voran, womit die Probleme des Informationszeitalters sich nicht auf die Analogisierung erstrecken.

Die Digitalisierung hingegen ist der Punkt, an dem die Probleme des Informationszeitalters einsetzen und zwar aufgrund der bereits beschriebenen Eigenschaften digitaler Daten.

Eine Möglichkeit das Problem zu lösen wäre hier im pauschalen Verbot der Digitalisierung von fremden geistigen Eigentum. Dies könnte man mit dem Verbot der Entstellung begründen und würde praktisch eine Einschränkung der Schrankenregelungen darstellen. Sicherlich müsste das noch genauer ausgearbeitet werden. So müssten bspw. flüchtige Digitalisierungen wie sie bei einem Fotokopiervorgang entstehen davon ausgenommen werden.

13.3.2 Trennung Literatur und Software

Mit der Einführung eines DUrhG bekäme man nun auch die Möglichkeit, die etwas unglückliche Einsortierung von Software als Literatur wieder

zu revidieren. Ein Online-Kultur-Magazin[255] schreibt dazu sinngemäß: „Jeder Softwareentwickler ist ein kleiner Grass“.

Die Einsortierung der Software in das Urheberrecht kam ursprünglich von dem Wunsch, Software nicht langwierigen und teuren Patentverfahren zu unterwerfen. Doch im Angesicht der drohenden Software-Patente zeigt sich, dass die Regelungen des Urheberrechts für die Software nicht ausreichend geeignet waren. Somit könnte man die Gelegenheit ergreifen und ein angemessenes Softwarerecht gestalten.

13.3.3 Strafrecht

Einer interessanten Betrachtungsweise[256] der Tatsache, dass immer mehr Hersteller von Audio-CDs ihre Produkte mit Kopierschutzmechanismen versehen, gingen die Juristen Tarek Abdallah, Björn Gercke und Peter Reinert nach.

Sie untersuchten die Frage, ob sich die Kopierschützer sich nicht durch ihre Schutzmaßnahmen strafbar machen können, was sich eventuell aus § 303 a StGB herleiten lässt:

> *(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.*
>
> *(2) Der Versuch ist strafbar.*

Zur Strafbarkeit würde ausreichen, dass sich aus dem Kauf bspw. einer CD das Recht auf die ungestörte Benutzung ableiten ließe. Dies gälte ebenso falls die Privatkopie tatsächlich durchsetzbar gestaltet würde.

Sicherlich kann es nicht der Sinn dieses Paragrafen sein, dem Urheber das Leben schwer zu machen, doch sollte er durchaus Anwendung finden, falls kopiergeschützte Daten trotz legaler Verwendung bspw. Geräte des Nutzers beschädigen können, wie bei einem Audio-CD-Kopierschutz geschehen[257].

13.3.4 Innovative Tauschbörsen

Nachdem nun die Privatkopie von offensichtlich illegal hergestellten Quellen nicht mehr erlaubt ist, herrscht wie in den rechtlichen Grundlagen beschrieben immer noch Nachbesserungsbedarf bei der Formulierung des Paragrafen 53 UrhG. Doch selbst wenn nun die

[255] vgl. [59]
[256] vgl. [60]
[257] Allerdings liegen diese Geschehnisse nun schon eine Weile zurück. Siehe dazu [61]

Formulierung der illegalen öffentlichen Zugänglichmachung hinzugenommen würde, ändert es nichts an der Situation.

Mit Tricks und Kniffen könnte man auch eine solch neue Formulierung aushebeln. Die Frage ist nämlich, ob denn dann eine Tauschbörse legal wäre, bei der eine Art „Kennenlern"-Phase vorgeschaltet würde, in der man sich speziell auf zu tauschende Daten einigt, welche vorher nicht per Suchmaschine abfragbar sind. Damit fiele der Vorgang nicht unter die öffentliche Zugänglichmachung, sondern wäre wieder eine „normale" Privatkopie.

Es ist sicherlich schwer eine adäquate Formulierung zu finden, um das Herunterladen von Daten aus Tauschbörsen zu verhindern, doch sollte das Thema klar definiert werden. Denn sonst können sich immer wieder Schlupflöcher ergeben.

13.3.5 Unterstützung von DRMS

Aufgrund der im Laufe der Arbeit dargelegten Umstände, dass ein DRMS in der Theorie die ideale Alternative für das Urheberrecht darstellt, verdient es besonderen Augenmerk im Gesetz. Dabei muss auch der Tatsache Rechnung getragen werden, dass ein funktionierendes DRMS mehr ist, als bloße TPM.

Wie bereits im „tilting bottle"-Modell erläutert, darf die Unterstützung von DRMS aber nicht zu einseitig ausfallen, da sich die möglichen Nutzer kein System aufzwingen lassen werden.

Wie könnte nun eine solche Unterstützung von DRMS aussehen?

Zunächst einmal sollten den Herstellern auch Vorteile durch die Verwendung von fairen DRMS erwachsen. Bisher wurden in diesem Kapitel die Rechte der Hersteller recht stark eingeschränkt. Im Gegenzug kann hier den Content-Produzenten die Hand gereicht werden.

Bei Einsatz eines funktionierenden DRMS, welches die verschiedenen speziellen Nutzergruppen berücksichtigt, die das Urheberrecht vorsieht, soll dem Hersteller zugebilligt werden, dass *sämtliche* Schranken, die sein System unterstützt, nur über selbiges abgewickelt werden dürfen. Der Schutz, den das System gewähren würde, wäre somit lückenlos. Damit hätten die Hersteller den Anreiz ein System, wie das in dieser Arbeit vorgestellte auch zu implementieren, und gleichzeitig würden die Nutzer in den vollen Umfang des Schutzes durch die Schranken des Urheberrechts kommen.

Da dieser Vorschlag natürlich stark in die bisherigen Rechte der Nutzer eingreift, müssen sehr restriktive Bedingungen aufgestellt werden,

denen das System folgen muss. Dabei sollten die folgenden Punkte in der einen oder anderen Form berücksichtigt werden:

- Kennzeichnungspflicht

  Ähnlich wie der bereits vorhandenen Kennzeichnungspflicht bei kopiergeschützten Daten muss ebenfalls eine Kennzeichnungspflicht für DRM-geschützte Daten eingeführt werden. Die Selbstbestimmung eines eventuellen Nutzers soll immer noch so weit gehen, dass er sich aktiv für oder gegen das DRMS entscheiden kann.
- Datenschutzrechtliche Mindestgarantie

  Durch diese Regelung soll es dem Nutzer erleichtert werden, Vertrauen zu dem neuen System zu fassen, da er klar überblicken kann, was ein System, dem er sich anvertraut, mit seinen Daten tun darf.
- Zertifizierung

  Damit die in der Theorie geforderten Regelungen auch eingehalten werden, muss eine regelmäßige Zertifizierung aller DRMS erfolgen. Diese muss durch eine unabhängige staatliche Organisation durchgeführt werden.
- Forderung einer Kompatibilitätsnorm

  Diese Regelung ist ebenfalls als Handreichung für den Nutzer zu verstehen. Um das bereits vorhandene Misstrauen weiter abzubauen, müssen die DRMS einer gemeinsam mit den Produzenten zu erarbeitenden Kompatibilitätsnorm genügen. Damit soll sichergestellt werden, dass der Nutzer auch eine aktive Wahl zwischen verschiedenen funktionierenden Systemen hat, und keines vom Content-Produzenten aufoktroyiert bekommt.

13.3.6 Legalisierung von illegalen Beständen

Idealerweise sollte ein Passus in das digitale Urheberrecht aufgenommen werden, der es für eine Übergangsfrist erlaubt, illegal erworbene Datenbestände nachträglich gegen eine angemessene Lizenzgebühr zu legalisieren, ohne dass dadurch ein Nachteil entsteht. Selbstverständlich kann von diesem Paragrafen im Falle einer drohenden Verurteilung kein Gebrauch mehr gemacht werden.

13.4 Beispiele in der Praxis

In der Praxis haben sich immer wieder Situationen herausgebildet, die zeigen, dass das alte Urheberrecht dem Informationszeitalter nicht mehr gewachsen war. In den folgenden zwei Fällen soll jeweils ein solcher

Missstand aufgezeigt werden und eine mögliche Lösung im Sinne des DUrhG vorgeschlagen werden.

13.4.1 Abmahnwelle

In der aktuellen Tagespresse ist immer wieder von einer sog. Abmahnwelle zu hören. Verschiedene Anwälte haben sich bereits einen Namen als „Abzocker“ gemacht, die das Internet auf der Suche nach nicht korrekten Homepages durchstöbern (lassen), und den Inhabern dieser Seiten eine Abmahnung verbunden mit hohen Anwaltsgebühren zusenden.

Diese Praxis ist zwar rechtens, doch mutet es bedenklich an, dass das deutsche Rechtssystem einer solchen Vorgehensweise Vorschub leistet, die für Internetnutzer sehr nahe in Richtung Selbstjustiz zu gehen scheint. Denn nur die wenigsten Nutzer des Internets haben ein ausreichendes Verständnis von der Materie des Internets, um die Legalität ihres Verhalten im Ansatz zu begreifen.

Daher sieht das DUrhG vor, gerade im Fall von Kleinstunternehmen und Privatpersonen, bei einem Erstvergehen bspw. gegen Urheber-persönlichkeitsrechte einen „Strafzettel“ vor, der mit einer geringen Bearbeitungsgebühr in Höhe von ca. 20 bzw. 50 Euro für Privatpersonen bzw. Kleinstunternehmen verknüpft ist.

Des weiteren kann es diesen Personen nur bedingt[258] zugemutet werden, dass sie der rapiden Entwicklung des Internetrechts folgen können. Solange sie nicht ändern, machen sie im Fall von Änderungen nichts falsch, und gelten betreffend den Änderungen als ob sie noch kein Vergehen begangen hätten. Hier wäre ein Beispiel außerhalb des Urheberrechts zu nennen: Nutzer die eine Homepage betreiben, und seit der Einführung der Impressumspflicht an dieser nichts mehr verändert haben, wären demnach nicht für ein fehlendes Impressum zu belangen.

Ab einer bestimmten, noch festzulegenden Größe der Firma gilt dieses Recht nicht mehr. Doch auch hier hat nur der Staat auf Hinweis eines Verletzten das Recht, den Nutzer abzumahnen.

13.4.2 Fotografien

Ein weiteres Problem, welches in der Praxis aufgetaucht ist, betrifft die Online-Verwertung von Fotografien. Wenn eine Person zu einem Fotografen geht, und sich mit einem Mindestmaß an künstlerischem Aufwand fotografieren lässt, liegen die Rechte am Foto sogar insoweit

[258] bspw. bei ausgeprägtem Wissen über die Rechtssituation, wie es bei Informatikern oder Juristen zu finden ist.

bei dem Fotografen, dass das Bild ohne ausdrückliche Erlaubnis und Namensnennung nicht auf einer privaten Homepage publiziert werden darf. Sicherlich sind die Rechte des Fotografen an seinem Werk vorhanden, doch sollte für das DUrhG definiert werden, dass die Digitalisierung und öffentliche Zugänglichmachung zu privaten Zwecken in den Umfang der Rechte des Nutzers aufgenommen werden.

13.5 Fazit

Durch die vorgeschlagene Trennung des Urheberrechts ist man nahe einem Paradigmenwechsel. Das Urheberrecht wandelt sich von einem fast ausschließlichen Schutzrecht für den Content-Produzenten und den Urheber zu einem Gesetz, welches die Interessen der Beteiligten stärker gegeneinander abwägt.

Die Waage neigt sich im vorgeschlagenen DUrhG vergleichsweise stark in Richtung des Nutzers, weg vom Urheber. Anhand der aktuellen Situation, in der die Urheber nach einem umfassenderen Schutz verlangen, mag dies sonderbar anmuten.

Die Erklärung hierfür ist jedoch sehr einfach. Viele der Zugeständnisse für den Verbraucher dienen zur Stärkung des Vertrauens in die neue Technik. Dies ist ein Vorgang, dem die Content-Produzenten bis dato kaum Interesse geschenkt hatten. Und daher tut es der Staat.

Sicherlich kann das vorgeschlagene DUrhG nicht mehr als ein grobes Konstrukt sein, welches einer deutlicheren Ausarbeitung bedarf. Gerade bei so länderübergreifenden Themen wie dem Urheberrecht ist es außerdem schwer die Rolle des Vorreiters einzunehmen. Viele der genannten Regelungen sind ohne internationalen Beistand kaum durchsetzbar.

Auch der Verwaltungsaufwand, der monetär wie auch bürokratisch hinter der vorgeschlagenen Reform steht, ist immens. Erst nach einer genauen Abwägung von Kosten und Nutzen könnten die vorgeschlagenen Maßnahmen umgesetzt werden.

Daher bleibt es vorerst bei einer Sammlung von Ideen, die helfen könnten, DRM auf einen sozial- und damit auch nutzerverträglichen Kurs zu bringen.

Ein großes Problem für das Urheberrecht im digitalen Bereich ist auch die Tatsache, dass die Technik schneller denn je voranschreitet. Niemand, sei es eine Firma, ein Konsortium, ein Staat oder ein Staatenbund beherrscht die Technik so weit, wie sie momentan schon fortgeschritten ist. Und nun soll eine Gesetz geschaffen werden, welches zukünftige Entwicklungen voraussieht und teilweise integriert. Dieser Ansatz ist wohl mittelfristig zum scheitern verurteilt, sofern der

Gesetzgebungsprozess nicht der Geschwindigkeit der Technik angepasst wird. Doch selbst bei Umstellung des Rechtssystems auf Richterrecht, welches mit Präzedenzfällen ähnlich der USA geltendes Recht schafft, kann es kaum mit der Geschwindigkeit der Informationszeitalters mithalten.

14 Schlusswort

Nachdem nun sowohl das UGS-DRMS erstellt wurde, als auch das Urheberrecht deutlich reformiert wurde, bleibt nur noch die Rückkehr zum Fragenblock, der in der Zielsetzung gestellt wurde: Dieser soll der Einfachheit noch einmal wiederholt werden:

„Warum werden die Daten am Urheber vorbei gehandelt? Was kann dagegen getan werden? Was darf man dagegen tun? Warum funktionieren DRM-Systeme bis dato nicht? Ist das Urheberrecht dem digitalen Zeitalter gewachsen? Wie kann der Gesetzgeber das Urheberrecht anpassen? Müssen nur die Urheber geschützt werden? Oder auch die Anwender? Darf der technisch mögliche Rahmen ausgeschöpft werden?“

Die Nutzer von digitalem Content handeln aus vielerlei Gründen wider dem Urheberrecht. Zum einen ist die Verlockung durch den günstigen Preis des Contents aus dem Internet verknüpft mit dem mangelnden Unrechtsbewusstsein vieler. Zum anderen auch das Verhalten der Urheber selbst, denen nicht zu Unrecht ein kontraproduktives Verhalten vorgeworfen werden kann, weil sie zunächst nichts gegen die drohende Gefahr unternommen haben und dann zu spät reagiert haben und dies auch mit den falschen Mitteln.

Dazu kommt noch die Schwemme an neuen Errungenschaften, die mit einer bisher nie gekannten Geschwindigkeit über die Informations-gesellschaft hereinbrechen. Kaum eine Entwicklung bekommt die Zeit zu reifen, sondern wird schnell ins kalte Wasser des Marktes geworfen. Das dies auf Dauer nicht funktionieren kann, erkennt man in der momentanen Unsicherheit auf allen Seiten. Weder Staat, noch Bürger, noch Wirtschaft wissen wirklich einen Ausweg aus der Krise.

Durch zu harte Restriktionen auf Seiten der Wirtschaft wurden bis dato eventuell kooperative Nutzer bereits im Vorhinein abgeschreckt. Die Flasche des „tilting bottle“-Modells neigt sich weiter in Richtung der Nutzer. Durch immer stärkere Restriktionen gelangt man sicher nicht ans Ziel. DRM wird als ultimatives System zum Geld verdienen und Content schützen gesehen. Doch auch die Nutzer sehen dieses Potenzial darin und sind daher skeptisch.

Es ist ohnehin das Verschwinden der sozialen Marktwirtschaft zu beklagen, und zurück bleibt die reine Marktwirtschaft. Durch das jeweilige Streben nach Maximierung des eigenen Nutzens[259] beider Parteien – Nutzer und Content-Produzent – arbeitet jede an der anderen

[259] Und der Nutzen wird auch bewusst auf Kosten des jeweils anderen maximiert.

vorbei. Der Nutzen wird nicht bzw. nicht in dem Maße wie möglich durch Austausch der Güter Content und Geld geschaffen. Für die Nutzer untereinander gibt es einfachere Wege. Der Markt droht zu versagen.

Ein übriges tut dazu das momentan noch vollkommen überforderte Urheberrecht, welches allerdings schon auf dem Weg der Besserung ist. Dabei ist allerdings wichtig zu bedenken, dass das novellierte Urheberrecht keine Momentaufnahme bleibt, sondern sich mit der Gesellschaft formt. Niemand kann in die Zukunft schauen, weshalb auf neue Situationen eine schnelle Anpassung erfolgen muss.

Das UGS-DRMS legt besonderen Wert auf eine beiderseitig angemessene Lösung des urheberrechtlichen Konfliktes. Dies kann gelingen, da bei diesem System alle beteiligten Parteien zusammenarbeiten.

Der Nutzer wird durch Motivationssysteme gewonnen. Der Content-Produzent erhält die Aussicht auf langfristigen und nachhaltigen Schutz seiner Lebensgrundlage. Und schließlich der Staat versichert sich einerseits, dass die Gesellschaft zumindest von dieser Seite nicht digital gespalten wird, und andererseits, dass sich Kreativität und Forscherdrang auszahlen.

Das UGS-DRMS funktioniert in der Theorie, da es nicht gegen das Gesetz arbeitet, sondern dieses integriert, und ebenso nicht gegen den Nutzer arbeitet, sondern mit ihm.

Selbstverständlich steht vor einer möglichen Verwirklichung ein großer verwaltungstechnischer und auch monetärer Aufwand, welcher wohl dafür sorgen wird, dass lieber kurzfristige Varianten gewählt werden. Ohnehin wäre es nicht sicher, ob das vorgeschlagene System die Kosten wirklich vollständig egalisieren würde.

Doch zumindest die Grundvoraussetzungen, unter denen ein DRMS überhaupt eine Chance haben kann, sind klar ersichtlich:

- Verabschiedung des Dogmas: „Daten sind vollständig schützbar.“
- Restriktiver Schutz ist zumeist kontraproduktiv.
- Die Zusammenarbeit mit dem Kunden steht im Vordergrund.
- Motivation ist kein Bonus, sondern essentiell.
- Eine faire gesetzliche Situation muss geschaffen werden.
- Die Unkontrollierbarkeit der Technik muss berücksichtigt werden.

Abkürzungsverzeichnis

AES	Advanced Encryption Standard
AG	Arbeitsgruppe
AS	Authentication Service
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BMJ	Bundesministerium für Justiz
CD	Compact Disk
CD-ROM	Compact Disk Read-Only Memory
CS	Content-Server
DAD	Digital-Analog-Digital
DD	Digital-Digital
DES	Data Encryption Standard
DM	Deutsche Mark
DMCA	Digital Millennium Copyright Act
DNA	Desoxyribonucleinacid
DoS	Denial of Service
DRM	Digital Rights Management
DRMS	Digital Rights Management System
DSL	Digital Subscriber Line
DTD	Doctype Definition
DUrhG	Digitales Urheberrechtsgesetz
DVD	Digital Versatile Disk
EC	Eurocheque
EG	Europäische Gemeinschaft
EU	Europäische Union
EWG	Europäische Wirtschaftsgemeinschaft
GB	Gigabyte

GEMA	Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte
GG	Grundgesetz
GNU	GNU's Not Unix
GNU GPL	GNU General Public License
GPRS	General Packet Radio Service
HDD	Hard Disk Drive
ID	Identification Number
IP	Internet Protocol
IPR	Internationales Privatrecht
ISP	Internet Service Provider
JP(E)G	Joint Photographic Experts Group
kB	Kilobyte
kbps	Kilobit pro Sekunde
KDC	Key Distribution Center
LAN	Local Area Network
LS	Licensing Server
MB	Megabyte
MD5	Message Digest 5
MIT	Massachusetts Institute of Technology
MP3	MPEG Layer-3
MPEG	Motion Pictures Expert Group
OCR	Optical Character Recognition
ODRL	Open Digital Rights Language
OEM	Original Equipment Manufacturer
OLG	Oberlandesgericht
OS	Operating System
OWL	Web Ontology Language
P2P	Peer to Peer
PC	Personalcomputer
PDA	Personal Digital Assistent

PKI	Public Key Infrastructure
PKK	Public Key Kryptografie
PIN	Personal Identification Number
PMI	Privilege Management Infrastructure
RA	Rom-Abkommen
RAM	Random Access Memory
RBÜ	Revidierte Berner Übereinkunft
RDF	Resource Description Framework
RDL	Rechtedefinitionssprache
RIAA	Recording Industry Association of America
RM	Rechtemanagement
RSA	Rivest, Shamir, Adleman
SGML	Standard Generalized Markup Language
SHA	Secure Hash Algorithm
SIM	Subscriber Identification Module
ST	Service Ticket
StGB	Strafgesetzbuch
TAN	Transaktionsnummer
TCG	Trusted Computing Group
TCPA	Trusted Computing Platform Alliance
TGS	Ticket Granting Service
TGT	Ticket Granting Ticket
TPM	Technical Protection Measures
TRIPS	Agreement on Trade-Related Aspects of Intellectual Property Rights
TTP	Trusted Third Party
UGS-DRMS	User Group Specific DRMS
UMTS	Universal Mobile Telecommunication System
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
UrhG	Urheberrechtsgesetz

URL	Uniform Resource Locator
USA	United States of America
USB	Universal Serial Bus
UWG	Gesetz gegen den unlauteren Wettbewerb
VAS	Value Added Services
VG	Verwertungsgesellschaft
WCT	WIPO Cooperation Treaty
WIPO	World Intellectual Property Organization
W-LAN	Wireless LAN
WMA	Windows Media Audio
WMP	Windows Media Player
WMV	Windows Media Video
WPPT	WIPO Performances and Phonograms Treaty
WTO	World Trade Organization
WUA	Welturheberrechtsabkommen
WWW	World Wide Web
XML	eXtensible Markup Language
XMLS	XML Schema
XrML	eXtensible rights Markup Language
ZPÜ	Zentralstelle für private Überspielungsrechte

Ressourcen- und Literaturverzeichnis

Die verwendeten Internet-Quellen sind, soweit nicht anders angegeben, zuletzt am 27.10.2004 abgerufen worden.

Primärliteratur:

[1] BMJ; „Urheberrechtsreform (zweiter Korb) – Zusammenfassung der Ergebnisse der Arbeitsgruppensitzungen“; 2004; http://www.urheberrecht.org/topic/Korb-2/bmj/707.pdf

[2] IFPI; „Positionspapier der Deutschen Landesgruppe der IFPI e.V. und des Bundesverbandes der Phonographischen Wirtschaft e.V. zum so genannten „Zweiten Korb“ einer Urheberrechtsnovelle“; 2003; http://www.ifpi.de/news/318/positionspapier.pdf

[4] EU; „Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft“; 2001; http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=DE&numdoc=32001L0029&model=guichett

[5] Wikipedia.org; „Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst“; o.J.; http://de.wikipedia.org/wiki/Berner_%C3%9Cbereinkunft_zum_Schutz_von_Werken_der_Literatur_und_Kunst

[6] Berne Convention for the Protection of Literary and Artistic Works; 1979; http://www.wipo.int/clea/docs/en/wo/wo001en.htm

[7] Welturheberrechtsabkommen; 1971; http://www.uni-muenster.de/Jura.itm/hoeren/material/welturheberrechtsabkommen.htm

[8] Rome convention 1961; http://www.wipo.int/clea/docs/en/wo/wo024en.htm

[9] Becker, Buhse, Günnewig et al.; “Digital Rights Management”; 2003; Springer-Verlag; Berlin Heidelberg

[10] WIPO; Gründungsvertrag der World Intellectual Property Organization; 1979; http://www.wipo.int/clea/docs/en/wo/wo029en.htm

[11] US-Government; “The digital millennium copyright act of 1998”; 1998; www.copyright.gov/legislation/dmca.pdf

[12] Schulze, ZUM 1997, S.77

[13] Dreier, Nolte; „The German Copyright – Yesterday, Today, Tomorrow“; 2003; in: [9]

[14] Dreier, Nolte; The German Copyright – Yesterday, Today, Tomorrow; 2003; in: [9]; S. 492

[18] Dreier/Schulze: „Urheberrecht – Kommentar“, 2004; Beck Juristischer Verlag; München

[20] Bundesgesetzblatt Jahrgang 2003 Teil I Nr. 46, ausgegeben zu Bonn am 12. September 2003; 2003; http://www.bmj.bund.de/media/archive/126.pdf

[21] BMJ; „Fragen zur weiteren Reform des Urheberrechts in der Informationsgesellschaft“; 2003; http://www.urheberrecht.org/topic/Korb-2/bmj/Fragebogen-orig.pdf

[22] Hoeren; “Welche Chancen hat das Urheberrecht im Internetzeitalter?”; 2003; in: [65] S. 5 ff.

[25] BMJ; „Urheberrecht in der Wissensgesellschaft – ein gerechter Ausgleich zwischen Kreativen, Wirtschaft und den Verbrauchern“; 2004; http://www.bmj.bund.de/media/archive/749.pdf

[26] Michl; „Schutz digitaler Bilder durch digitale Wasserzeichen“; 1999; http://ig.cs.tu-berlin.de/oldstatic/w99/1332l501/ref1/wasserzeichen/

[27] Wikipedia.org; “Jitter”; o.J.; http://en.wikipedia.org/wiki/Jitter

[28] Webster Web Dictionary; “Jitter”; o.J.; http://www.webster-dictionary.org/definition/jitter

[31] Perens; “The Open Source Definition”; 1997; http://www.opensource.org/docs/definition.php

[32] Open source initiative; “The GNU General Public License (GPL)”; 1991; http://www.opensource.org/licenses/gpl-license.php

[33] Open source initiative; “GNU Lesser General Public License (LGPL)”; 1999; http://www.opensource.org/licenses/lgpl-license.php

[34] Needham, Schroeder; “Kerberos: The Network Authentication Protocol”; http://web.mit.edu/kerberos/www/

[36] Autor unbekannt; „Entwicklung der Computertechnologie und des Internet“; o.J.; http://www-gewi.kfunigraz.ac.at/fula/themen/internet/internet-geschichte.html

[37] Biddle, England, Peinado et al.; “The Darknet and the future of conent protection”; 2003; in [9]; S. 344 ff.

[40] Knopf, Sorge; “Model-oriented analysis of user - right holder relations and possible impacts of DRM”; Information Services and Use 24, no. 1 (1/2004), S. 235-239

[43] Autor unbekannt; “Wie funktioniert das PotatoSystem?”; o.J.; http://www.potatosystem.com/info/ger/system.html

[44] Grimm; „Digital Rights Management: Technisch-organisatorische Lösungsansätze“; 2003; in: [65]; S.104

[45] ComputerBase.de; “Authentifizierung”; o.J.; http://www.computerbase.de/lexikon/Authentifizierung

[46] Autor unbekannt; „Was ist Bluetooth?“; o.J.; http://www.m-indya.com/mwap/bluetooth/bluetooth.htm

[47] Autor unbekannt; „USB On-The-Go“;o.J.; http://www.usb.org/developers/onthego/

[48] Apple; “FireWire”; o.J.; http://developer.apple.com/firewire/

[51] Autor unbekannt; „About XrML“; o.J.; http://www.xrml.org/about.asp

[52] Autor unbekannt; „Open Digital RightsLanguage (ODRL)“; o.J.; http://www.odrl.net/1.1/ODRL-11.pdf

[54] Stallman; „Science must ‘push copyright aside’“; 2001; http://www.nature.com/nature/debates/e-access/Articles/stallman.html

[55] UN; “Universal Declaration of Human Rights”; 1948; http://www.unhchr.ch/udhr/lang/ger.htm

[56] BSA; „BSA kritisiert Regierungsentwurf zur Urheberrechtsreform“; 2004; http://global.bsa.org/deutsch/press/newsreleases/2002-08-28.1274.phtml

[59] Podszun; „Das Ende der kulturellen Kuschelecken - Der Zugang zum geistigen Eigentum erlebt einen Paradigmenwechsel“; 2000; http://www.kultura-extra.de/extra/feull/urheberrecht.html

[61] Abdallah, Gercke, Reinert; Zur Strafbarkeit von Kopierschutzmaßnahmen auf Audio-CDs gemäß § 303a StGB“; 2003; http://www.hrr-strafrecht.de/hrr/archiv/03-07/index.php3?seite=6

[64] Autor unbekannt; Peer-To-Peer Netze“; o.J.; http://p2p.at-web.de/p2p.htm

[65] Arnold Picot; „Digital Rights Management“; 2003; Springer-Verlag; Berlin Heidelberg

[66] Interview mit Frau Brigitte Zypries, Bundesjustizministerin; „Das Urheberrecht kennt kein Recht auf Privatkopie“; http://www.heise.de/ct/04/16/158/

Sekundärliteratur:

Büllersbach, Dreier; „Wem gehört die Information im 21. Jahrhundert?“; 2004; Verlag Dr. Otto Schmidt; Köln

Fränkl; Karpf; „Digital Rights Management Systeme - Einführung, Technologien, Recht, Ökonomie und Marktanalyse“; 2004; pg Verlag; München

Gerichtsentscheidungen

[15] LG Hamburg; Urteil vom 19.08.1997 - 308 O 284/96: "CD-ROM als neue Nutzungsart"

[16] Bezirksgericht Amsterdam; Urteil vom 24.9.1997 - D 3. 1294: "CD-ROM und Internet als neue Nutzungsarten"

[17] BGH; Urteil vom 26.1.1995 ZUM 1995, 715 – Videozweitauswertung III

[23] BGH, Urteil vom 11. Juli 2002 (I ZR 255/00)

[24] BGH, Urteil vom 25. Februar 1999 (I ZR 118/96)

Meldungen:

[3] John Borland; „RealNetworks breaks Apple's hold on iPod“; 2004; http://zdnet.com.com/2100-1104_2-5282063.html

[19] Heise Newsticker; „Tastendruck "umgeht" CD-Kopierschutz“; 2003 http://www.heise.de/newsticker/meldung/print/40906

[30] Fraunhofer-Intitut; „Digitale Medien-Wasserzeichen im produktiven Einsatz“; 2004; http://www.ipsi.fraunhofer.de/ipsi/press/press_releases/2004/040301_container_wasserzeichen.html

[39] Heise Newsticker; “Harry Potter und das Darknet”; 2003; http://www.heise.de/newsticker/meldung/37907

[53] Heise Newsticker; „FSF-Präsident Stallman: Urheberrecht teilweise abschaffen“; 2002; http://www.heise.de/newsticker/meldung/28213

[57] Autor unbekannt; „DRM und Pauschalabgaben - der Kunde zahlt doppelt“; 2004; http://www.mp3-world.net/news/67726-drm-und-pauschalabgaben-der.html

[58] Heise Newsticker; „Kanada führt Pauschalabgaben für MP3-Player ein“; 2003; http://www.heise.de/newsticker/meldung/42939

[60] Heise Newsticker; „Strafbarkeit der Opfer? “; 2003; http://www.heise.de/tp/deutsch/special/copy/15372/1.html

Quellen:

[29] Quelle der verwendeten Bilder: http://ig.cs.tu-berlin.de/oldstatic/w99/1332l501/ref1/wasserzeichen/

[62] Quelle: http://www.microsoft.com/technet/images/prodtechnol/windows2000serv/maintain/security/images/kerb01_BIG.gif

Weiterführende URLs:

[35] Internet-Seite „Subito“; Dokumentenlieferdienst; http://www.subito-doc.de

[38] Internetseite “Lets buy it”; Internetversandhaus; www.letsbuyit.com

[41] Internet-Seite “Sourceforge”; Open source Software Plattform; www.sourceforge.net

[42] Internet-Seite “Download.com”; Shareware-Seite; www.download.com

[49] Internet-Seite “Winamp”; Audio-Abspielprogramm; http://www.winamp.com

[50] Internetseite des „World Wide Web-Consortium“; „Standards von OWL; RDF; XML“; http://www.w3c.org

[63] Internet-Seite „Napster“; Legalisierte ehemalige Tauschbörse; http://www.napster.de/

Verwendete Gesetzestexte:

„Bürgerliches Gesetzbuch“; 2002; C.H. Beck; München

„Strafgesetzbuch“; 2002; C.H. Beck; München

„Urheberrecht“; 2003; C.H. Beck; München

Appendix

Anhang A – Übersicht über Tauschbörsen

Der Dschungel der Tauschbörsen wird immer größer. Inzwischen gibt es weit über zwanzig verschiedene Systeme, größtenteils mit jeweils verschiedenen Zugangsprogrammen. Daher soll an dieser Stelle eine Aufzählung der wichtigsten Tauschbörsen in alphabetischer Reihenfolge gegeben werden. Nur die wenigsten erreichen Nutzerzahlen von mehreren Millionen Teilnehmern, doch stellt die Gesamtsumme der Teilnehmer ohne Zweifel ein Problem für die Content-Produzenten dar. Eine ausführlichere Übersicht mit einer Bewertung findet sich im Internet[260].

Eigenständige Systeme:

- BitTorrent
- DirectConnect
- iMesh
- Freenet (verschlüsselt)
- Morpheus
- Overnet
- Soulseek

Gnutella:

- BearShare
- LimeWire

Kazaa:

- Kazaa
- Sharezaa
- Kazaa lite

Napster:

- Napster
- WinMX
- Wrapster

eDonkey-Netzwerk:

- eDonkey2000
- eMule
- mlDonkey

[260] siehe dazu [64]

Anhang B – Kerberos 5 – Struktur

Dieses Bild findet sich zur Erläuterung der Kerberos-Struktur auf der Microsoft-Homepage[261]. Der Ablauf ist zwar stark simplifiziert, doch enthält er die wesentlichen Komponenten.

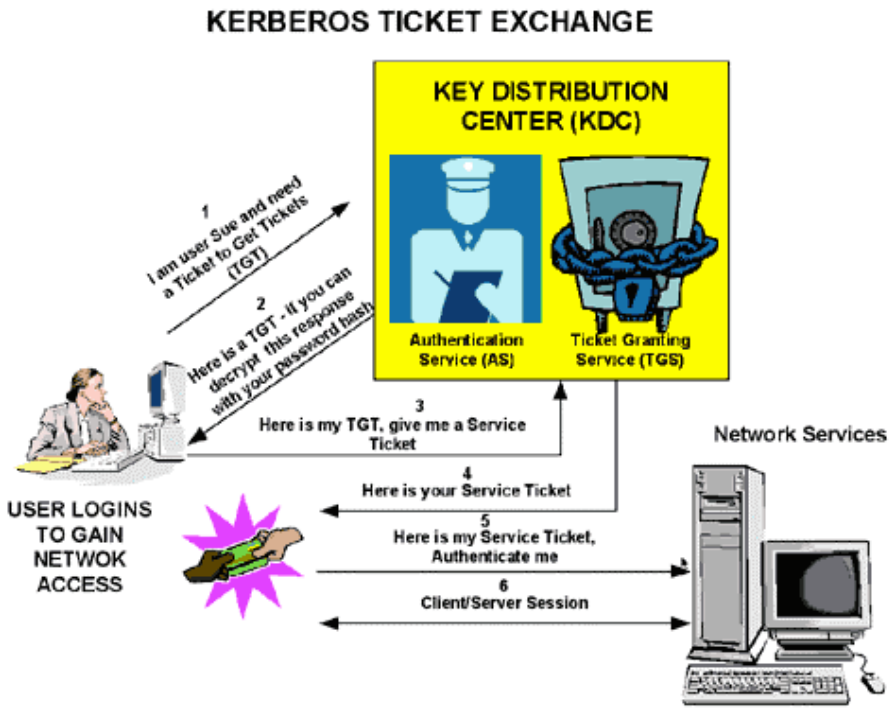

Abbildung 8: Ablauf von Kerberos

[261] Quelle: [62]

Anhang C – Hash-Funktionen

Hash-Funktionen erleichtern die Kommunikation per Kryptografie erheblich. Ihre genauere Bezeichnung „One-Way-Hash-Funktionen“ lässt bereits erahnen, dass sie auf die Eigenschaft der Unumkehrbarkeit vertrauen.

In der Praxiswerden sie verwendet um den sog. Hash-Wert eines Dokuments zu bilden. Die Funktion bildet durch eine komplizierte Berechnung[262] ein Dokument auf einen vergleichsweise kurzen Wert ab. Dieser ist bspw. bei dem recht verbreiteten MD5-Hash-Algorithmus 128 Bit lang. Der Hash-Wert wird dann mit dem privaten Schlüssel des Sendenden verschlüsselt und zusammen mit dem Dokument an den Empfänger gesendet.

Der Empfänger entschlüsselt nun mit dem öffentlichen Schlüssel seines Gegenübers den Hash-Wert und führt seinerseits den Hash-Vorgang mit dem Dokument durch. Sein Ergebnis vergleicht er mit dem gerade entschlüsselten Wert, der auf Grund der Verschlüsselung mit Sicherheit von seinem Kommunikationspartner stammt. Bei einem Übereinstimmen hat er eine sehr hohe Sicherheit, dass die Nachricht auf dem Weg an ihn nicht verändert wurde. Gleichzeitig entfällt der Aufwand die gesamte Nachricht mit dem komplexen asymmetrischen Verfahren zu verschlüsseln.

Damit eine Hash-Funktion auch sicher ihren Dienst erfüllt, bedarf es vier Voraussetzungen, denen sie genügen muss:

- Die Berechnung darf nicht umkehrbar sein. Dies ist durch die verlustbehaftete Berechnung immer gegeben.
- Es ist sehr schwer, zu einem gegebenen Text M einen Text M2 zu finden, der den gleichen Prüfwert hat.
- Es ist sehr schwer zu einem gegebenen Hash-Wert x eine Nachricht M zu finden, deren Hash-Wert x ist.
- Eine Hash-Funktion muss für einen Computer in vertretbar kurzer Zeit zu berechnen zu sein.

[262] Die je nach verwendetem Algorithmus wie bspw. MD5 oder SHA anders funktioniert.