TECHNISCHE UNIVERSITÄT WIEN

VIENNA UNIVERSITY OF TECHNOLOGY

DIPLOMARBEIT

Digital Rights Management

ausgeführt am Institut für
Softwaretechnik und interaktive Systeme
der Technische Universität Wien

unter der Anleitung von

O.Univ.Prof. Dipl.-Ing. Dr.techn. A Min Tjoa
und
Univ.Ass. Dipl.-Ing. Dr.techn. Mag.rer.soc.oec. Edgar Weippl
als verantwortlich mitwirkenden Universitätsassistenten

durch

Dr. Wolfgang Freund
Im Werd 3/4
1020 Wien

Datum Unterschrift

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die den benutzten Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Datum Eigenhändige Unterschrift

0. Kurzfassung/Abstract

Der Begriff Digital Rights Management oder abgekürzt - und durchaus um einiges öfter in dieser Kurzform verwendet - DRM ist heutzutage ein in der Öffentlichkeit als auch in Fachmedien viel gebrauchter Terminus. Viele Personen, sowohl in der Wissenschaft als auch Wirtschaftstreibende, befassen sich mit dieser Entwicklung und versuchen sie voran zu treiben und weiter zu entwickeln als auch von ihr zu profitieren. Aber es gibt auch eine ganze Reihe an Kritikern in Fachliteratur als auch populären Medien, die dieser neuen Technologie fast skeptisch bis geradezu ablehnend gegenüber stehen und als Gründe für ihre Verdammung etliche Defizite und Nachteile in der Anwendung von Digital Rights Management auflisten.

In dieser Arbeit sollen die Möglichkeiten, elektronische Inhalte und die Rechte daran zu schützen dargestellt werden. Das Ziel ist, festzuhalten, dass nur ein Zusammenspiel von rechtlichen Vorschriften und technischen Komponenten einen umfassenden Schutz gegen unberechtigte Verwendungen bieten können.

Dafür werden zunächst die rechtlichen Rahmenbedingungen, welche im Wesentlichen das Urheberrecht vorgibt, untersucht. In diesem Kapitel werden werden die einzelnen Rechte, welche dem Urheber zustehen, präsentiert und auf ihre Anwendbarkeit auf digitale Inhalte analysiert.

Im darauffolgenden Kapitel werden Aspekte des Datenschutzes und seine Auswirkungen vorgestellt und überprüft, welche Rolle der Datenschutz im Zusammenhang mit elektronischen Rechten und/oder Rechten an elektronischen Inhalten und eben Daten spielt.

Im technischen Teil der Arbeit werden einzelne technische Maßnahmen, die im Zusammenhang mit Digital Rights Management zum Einsatz kommen in ihren wesentlichen technischen Grundlagen und Funktionsweisen sowie Ausgestaltungen beleuchtet werden. Im Zusammenspiel mit den rechtlichen Grundlagen soll erörtert werden, welche Schutzqualitäten diese eingesetzten Technologien den einzelnen Rechten jeweils bieten können.

Am Ende dieser Arbeit sollen schließlich kurz zwei Beispiele aus der Praxis dargestellt werden.

The term Digital Rights Management or abbreviated – and much more often used in this shortform - DRM is today an epxression one would find regularly in the public as well as in specilaised media. Many, bei t in the academic world as well as in the business, contribute to the development, and attempt to profit, of DRM. On the other hand, many critical voices are sceptical or even adverse to this new technology and can list many reasons and disadvantages.

This thesis will present certain possibilities to protect electronic content. The aim is to show that only the close interaction of appropriate legal provisions as well as technical components will give a comprehensive protection against unwarranted use.

Therefore, initially the legal framework is to be reviewed, which mainly consists of laws on copyright. In this chapter, the specific rights that are granted by statute to the creator will be presented and alaysed in respect of digital content.

The following chapter focuses on data protection and after an intial overview of the rules and provision of data protection, it will be demonstrated, which role data protection plays in respect of eletronic rights or rights on electronic data.

The technical part will illustrate certain technical measures used in connection with Digital Rights Management, ist technological essentials and functionality. In view of the legal basis, it will be evaluated, which level of protection these technologies can present.

At the end of the thesis, two practical examples will be introduced.

Inhaltsverzeichnis

1. Einführung

1.1. Was ist Digital Rights Management?

Eine einheitliche Definition des Begriffes Digital Rights Management oder DRM System liegt bislang nicht vor und hat sich nicht durchsetzen können [Wiebe03-2, Arlt]. Ein wesentlicher Grund dafür scheint zu sein, dass an der Entwicklung bzw beim Gebrauch von Mechanismen und Tools des Digital Rights Management verschiedene Beteiligte involviert sind, die verschiedene Interessen an Digital Rights Management einbringen und die entsprechend ihrer Zielrichtung und ihrem spezifischem Hauptaugenmerk den Schwerpunkt der eingesetzten Techniken etwas anders gewichten. Obgleich aber somit der Begriff verschieden definiert wird, dürfte insgesamt doch ein relativ einheitliches Verständnis vorliegen [CEN].

In einer wohl eher vereinfachenden Betrachtungsweise wird festgehalten, „DRM soll dafür sorgen, dass sich digitale Informationen zukünftig wie ein Gebrauchsgut verhalten“ [Günnewig02].

Eine andere Definition setzt an der Substanz von Digital Rights Management an und inkludiert dessen Funktionalität: „Digital Rights Management (DRM) is a type of server software developed to enable secure distribution – and perhaps more importantly, to disable illegal distribution – of paid content over the web.“ [Rump]

Von einigen Anderen wieder wird der Begriff Digital Rights Management ausschließlich funktional beschrieben: „DRM is a term used to describe a range of techniques that use information about rights and rights holders to manage copyright material and the terms and condition on which it is made available to users.” [Department]

Wiebe seinerseits grenzt den Begriff von dem Begriff der „technischen Schutzmaßnahmen“ ab, welche der Oberbegriff dazu wären und definiert schließlich ein DRM System als ein „elektronisches Vertriebssystem für digitale Inhalte, das eine effektive und differenzierte Rechteverwaltung integriert“. Er grenzt dabei diese Systeme als eine Untergruppe aller „technischen Systeme, die die Nutzung und Vervielfältigung digitaler Daten beschränken“, also „die dazu bestimmt sind, entweder die Verletzung von Urheberrechten und verwandten Schutzrechten oder einen unberechtigten Zugang zu geschützten Werken und Leistungen zu verhindern“ [Wiebe03-2].

Die aus meiner Sicht wohl treffendsten Beschreibungen sind aber: „DRM ist ein modulares System, mit dem digitale Inhalte wie Musik, Text und Filme vor unrechtmäßiger Nutzung geschützt und Nutzungsbedingungen der Rechteinhaber effektiv durchgesetzt werden können“ [Günnewig], „DRM Systeme regeln den Zugriff, die Verwendung und den Handel mit elektronischen Inhalten“, „A Rights Management that uses digital technology and applies to intellectual property in digital form“ oder „DRM is a general term for a set of intertwining technologies that can be used to establish secure distribution of digital content” [Guth].

Rein sprachlich betrachtet besteht der Begriff Digital Rights Management zunächst aus drei Worten. Allerdings geht es bei Digital Rights Management nach dem von mir in dieser Arbeit zugrunde gelegten Verständnis nicht um „Digital Rights“, also digitale Rechte, wie der Begriff zunächst vermuten ließe. Die digitale Umgebung, also insbesondere die Verwendung des Internet, schafft hier keine neuen Rechte. Es dürfte mittlerweile wohl verstanden sein, dass insbesondere das Internet aber auch die sonstige elektronische Kommunikation bzw der Austausch von Inhalten auf elektronischem Wege im Grunde den gleichen Spielregeln sowie insbesondere Rechtsregeln unterliegen wie die so genannte „analoge“ Welt. In der Digitalisierung liegt somit keine Schaffung eines neuen Rechts. Was in der analogen Welt rechtens ist, bleibt auch in der digitalen Welt des Internet rechtens bzw umgekehrt, was hier nicht erlaubt ist, ist auch dort verboten.

Vielmehr geht es um das „Rights Management“, nämlich die Verwaltung von bereits bestehenden, durch die Rechtsordnung zuerkannten, Rechten. „A DRM system is facilitating the ’digital management of rights’“ [Guth] bzw genauer abgegrenzt: „It is important to note that DRM is the ’digital management of rights’ and not the ’management of digital rights’“ [Ianella]. Die technischen Systeme ermöglichen aber nun eine „effektive und differenzierte Rechteverwaltung“ und eröffnen eine „ungeahnt weitgehende Kontrolle über die Verbreitung und Nutzung digitaler Inhalte“ [Bechtold02].

Von einigen werden unter Digital Rights Management nur Technologien verstanden, welche neben der Möglichkeit der individuellen Nutzungskontrolle, insbesondere die Nutzung individuell abrechnen zu können, bieten [Arlt]. Nimmt man den zweiten Aspekt dieses Definitionsversuches ernst, so werden simplere Kopierschutzmechanismen ausgegrenzt. Denn obgleich diese auch ein Mittel darstellen, welches mit technischem Einsatz umgesetzt wird, um die Rechte an dem urheberrechtlich geschützten Werk zu „managen“, ist dabei eine individuelle Abrechenbarkeit nicht implementiert. DRM Systeme gehen typischerweise auch über bloße Kopierkontrollverfahren hinaus.

Wikipedia erläutert kurz und bündig Digital Rights Management als „ein Verfahren, mit dem die Verbreitung digitaler Medien kontrolliert werden kann“, gibt aber dann sowohl eine weit gefasste Definition: „DRMS stellen eine technische Sicherheitsmaßnahme dar, um einem Rechteinhaber von Informationsgütern die Möglichkeit zu geben, die Art der Nutzung seines Eigentums durch Nutzer auf Basis einer zuvor getroffenen Nutzungsvereinbarung technisch zu erzwingen“ als auch eine engere Definition „Elektronische Schutzmechanismen für digitale Informationen nennt man DRMS. Sie ermöglichen die Verwertung von digitalen Inhalten über eine reine Pauschalvergütung hinaus und erlauben zusätzlich die individuelle Lizenzierung/Abrechnung nach Häufigkeit, Dauer oder Umfang der Nutzung. Damit wird einerseits die unbegrenzte Nutzung einschränkbar, andererseits werden On-Demand-Geschäftsmodelle ermöglicht, die vorher kaum zu realisieren waren“.

Kritiker interpretieren die Abkürzung DRM gern als „Digital Restrictions Management“, da die Rechte der Benutzer erheblich eingeschränkt werden können, ohne dass daraus für den Benutzer ein direkter Nutzen entsteht“ vermeint

[Juraschko]. Er führt aus, dass „die Folgen von DRM vielseitig sind und von Problemen mit dem Datenschutz, über eine enge Kundenbindung bis hin zu Auswirkungen auf das Urheberrecht reichen“.

Im in dieser Arbeit gebrauchten Sinne soll Digital Rights Management alle Maßnahmen erfassen, die einer unrechtmäßigen oder unerlaubten Nutzung einer digitalen Datei vorbeugen und somit den digitalen Inhalt schützen. Dabei sollen auch allfällig als negativ empfundene Seiten analysiert und einer Betrachtung unterzogen werden, da auch diese möglicherweise soziale Auswirkung von Digital Rights Management relevant ist.

Der Begriff Digital Rights Management wird aber, wie oben zum Teil dargestellt, manchmal so weit verstanden, dass er auch Geschäftsmodelle und Systeme der Verbreitung von Inhalt umfasst. Guth identifiziert sechs unterschiedliche Perspektiven von Digital Rights Management, einschließlich sozialen und ökonomischen Aspekten. Weder diese Aspekte noch Abrechnungsmethoden, die Erfassung von Nutzungsvorgängen selbst oder Zahlungsvarianten, noch Probleme bei der praktischen Behandlung von Geschäftsabläufen oder der Abschluss von Verträgen zur Übertragung und Nutzung von digitalen Inhalten sollen aber hier Gegenstand dieser Untersuchung sein. Ebenso wenig sind die rechtspolitischen Interessen und Sichtweisen, also eine Bewertung, ob Digital Rights Management „gut“ oder „böse“ ist und damit erlaubt oder gar verboten sein sollte, im Folgenden dargestellt.

1.2. Die Bedeutung von Digital Rights Management

Gerade wegen der vielen verschiedenen Aspekte, die mit dem Begriff Digital Rights Management verbunden sind, stellt sich die Frage, weshalb Digital Rights Management Systeme in der heutigen Zeit eine Rolle spielen oder zumindest spielen sollten.

Die in Österreich aber auch in Europa und im angloamerikanischen Raum zurzeit vorherrschende Ansicht ist nun, dass dem Erschaffer einer geistigen Schöpfung ein Vorrecht an diesem Werk im Hinblick auf dessen kommerzielle Ausnutzung und Verwertung zukommt. Diesem Prinzip wird dadurch Rechnung getragen, dass das geltende Urheberrecht dem Schöpfer eine vorstehende Rolle zugesteht.[1] Eine wesentliche Zielsetzung des Urheberrechts ist es, Innovation zu ermöglichen und zu fördern [Fallenböck02]. Dabei ist es notwendig, die Kontrolle und Einfluss des Schöpfers über sein Werk einerseits mit den Möglichkeiten der Öffentlichkeit davon zu profitieren andererseits, in Einklang zu bringen.

Die Bedeutung von Digital Rights Management ergibt sich nun vor allem aus der angenommenen Unzulänglichkeit der derzeit geltenden rechtlichen Bestimmungen zum Schutze geistigen Eigentums. Ein Ansatz dabei ist, dass nicht alle Handlungen, die als ungerechtfertigt empfunden werden, möglicherweise auch untersagt sind. Ein anderer Aspekt dieser Unzulänglichkeit sind auch die ungeahnten geographischen Entfernungen, die eine digitale Datei auf kürzestem Weg zurücklegen kann. Damit

[1] Im Detail dazu weiter unten 2..

sind auch exotische und weit entlegene Gebiete erreichbar. Auf der anderen Seite können sich Beteiligte in diese Regionen zurückziehen und sind dabei den rechtlichen Belangen eines tatsächlich Berechtigten aufgrund der Schwierigkeiten in der Rechtsdurchsetzung über Staatsgrenzen hinweg relativ gut entzogen. Diese Schwierigkeiten zeigen sich einerseits daran, dass ein Verstoß gegen eine Rechtsordnung nicht notwendigerweise auch in der anderen Rechtsordnung geahndet wird, andererseits ist eine Verfolgung von Rechten über Grenzen aufwendig, damit teuer und oftmals aufgrund des Wertes somit nicht rentabel. Nur in außergewöhnlichen Konstellationen, etwa bei massiven Eingriffen, wird sich ein solches Vorgehen auch im wahrsten Sinn des Wortes auszahlen.

Mit dem Einsatz von Digital Rights Management werden technische Komponenten zur Sicherung von digitalen Gütern in den Vordergrund gestellt. Gerade Beispiele wie Tauschbörsen für Musikdateien im Internet und die Reaktion der Rechteinhaber darauf zeigen, dass der vom Urheberrecht gewährte Schutz von den Rechteinhabern als nicht ausreichend empfunden wird. Dementsprechend sind die Hersteller urheberrechtlich geschützter Werke seit einiger Zeit an der Entwicklung von technischen Verfahren beteiligt, die einen Schutz vor solchen ungerechtfertigten Eingriffen und Verwendungen bieten sollen.

Digital Rights Management soll es somit ermöglichen, dass der Schöpfer die weitere Verwendung seiner Idee kontrolliert und steuert.

Hintergrund dieser Entwicklung ist die Tatsache, dass die Digitalisierung eines Werks die verlustfreie Vervielfältigung desselben in einem vorher nicht bekannten Ausmaß erlaubt. Jede (digitale) Kopie gleicht dabei dem (digitalen) Original bis ins letzte Detail und kann von diesem nicht unterschieden werden. Digitale Güter haben damit eine grundlegende Eigenschaft physischer Güter verloren. Die Vervielfältigung analoger Inhalte ist dagegen zumeist im Vergleich durchaus zeitaufwendig und meist relativ kostspielig.

Auch führt der Kopiervorgang eben nicht zum Verlust von Qualität, wie es aus der „analogen“ Welt bekannt war, obwohl aus anderen Gründen, nämlich um die Größe der Dateien, insbesondere für deren Übermittlung über elektronische Netzwerke, zu reduzieren in der Praxis aber vor allem verlustbehaftete Kompressionsmechanismen verwendet werden. Die dabei in Kauf genommenen Verluste beeinträchtigen aber die Qualität im Verhältnis zum Vorteil der Kompression nur minimal [Guth], so dass gegenüber der analogen Kopie noch ein erheblicher Qualitätsvorsprung bestehen bleibt. Für lange Jahre hat nun der rechtliche Schutz ausgereicht, um den Schöpfer mit angemessenen Mitteln entsprechend zu schützen. Lange Zeit war es einfach, eine Kopie vom Original zu unterscheiden und deshalb wurden technische Schutzmaßnahmen nur in einigen Bereichen angewandt.

Die elektronische Vervielfältigung impliziert aber auch den zweiten Aspekt, der für Digital Rights Management relevant ist: die Lösung von einem Trägermedium. Während bisher geschützte Inhalte mit einem Trägermedium fix verhaftet waren, etwa ein literarisches Werk mit dem Papier, das es letztlich zum altbekannten Buch

macht, oder ein Musikstück mit der LP oder CD, so können dank der Entwicklung des Internet elektronische Kopien ohne Trägermedium übertragen werden.

Letztlich ist aber auch durch technologische Entwicklungen die Verbreitung auf elektronischem Weg erleichtert. Wohl erst das Aufkommen des Internet, das zwar lange Zeit verfügbar war, allerdings erst Mitte der 90er Jahre seinen Aufschwung zu dem heute weltumspannenden Netzwerk erlebt hat, hat eine entsprechend kommerzialisierte digitale Verteilung ermöglicht. Daneben sind leistungsstarke Komprimierungsmethoden notwendig, um das Datenvolumen, das bei der Digitalisierung von analogen Dateien entsteht, auf ein solches Maß zu reduzieren, dass eine elektronische Versendung nicht nur technisch, sondern auch kostenoptimal möglich ist. Parallel dazu steht die Erhöhung der Kapazitäten der Teile des Internet für einen großen Teil der Erdbevölkerung („Breitband“), so dass auch entsprechende Bandbreiten zur Verfügung stehen.

Aufgrund des Einsatzes von Digitalisierungstechnik ist es aber nunmehr für den Rechteinhaber schwieriger, seine Rechte durchzusetzen. Zudem bieten gerade digitale Technologien die Möglichkeit, neue effizientere Methoden für die Überwachung einzusetzen. Es ist daher notwendig, die bestehenden Rechte am geistigen Eigentum an diese neue Technologie anzupassen [Fallenböck02]. Mit diesen digitalen Technologien werden dem Rechteinhaber auch neue Methoden der Kontrolle eingeräumt. Er kann damit nicht nur unzulässige Nutzung verhindern, sondern praktisch jede beliebige [Fallenböck02].

Somit unterliegen Handlungen in einem elektronischen Umfeld - etwas vereinfacht gesehen – sowohl rechtlichen und technologischen Schranken. Einerseits gibt das geltende Recht Grenzen jeder Tätigkeit vor, insbesondere im gegebenen Zusammenhang die Regelungen des Urheberrechtes - oder mit dem angloamerikanischen Ausdruck „copyright“. Auf der anderen Seite geben eben technologische Maßnahmen wie Digital Rights Management einen Rahmen vor.

Bislang scheint noch kein DRM System tatsächlich einen Umfang erreicht zu haben, der den Einsatz wirtschaftlich sinnvoll macht. Aus wirtschaftlicher Sicht sind auch die Einstellungen und Präferenzen der potenziellen Kunden zu berücksichtigen und es verwundert nicht, dass einige Anbieter aus Bereichen wie digitalen Musikdateien, die stets an erster Stelle im Zusammenhang mit Digital Rights Management erwähnt werden, weiterhin ganz bewusst auf den Einsatz von Digital Rights Management verzichten [Standard].

Gleich an dieser Stelle soll aber nicht unerwähnt bleiben, dass beide Werkzeuge, rechtliche wie technische, somit einem Rechteinhaber als auch dem Nutzer eines Werks dienen können; sie sind aber nicht notwendigerweise voneinander abhängig:

Auch solche Werke, die nicht mittels Digital Rights Management geschützt sind, unterliegen, sofern die dafür erforderlichen Voraussetzungen erfüllt sind, dem Schutz des Urheberrechts. Andererseits können auch solche Werke, denen ein urheberrechtlicher Schutz nicht zukommt, technologisch in ihrer Verwendung beschränkt werden.

Daneben kann Digital Rights Management eine neue Flexibilität für Geschäftsmodelle erreichen. Während in einem konventionellen Umfeld mit der Bezahlung des Entgelts jegliche Kontrolle des Herstellers weggefallen ist, kann durch Digital Rights Management auch erreicht werden, dass etwa ein Musikstück nur dann bezahlt werden muss, wenn es auch tatsächlich angehört wird („pay per listening"). Dadurch kann theoretisch jeder einzelne Abspielvorgang zu einem viel geringeren Preis erfolgen, als dasselbe Musikstück bei einer vollständigen Übertragung kosten würde. Ähnliches gilt für Vervielfältigungen, die in einem so erweiterten Geschäftsmodell einzeln abgerechnet werden könnten. Wiederum ergibt sich für wenige Kopien ein preislicher Vorteil.

Ein Aspekt bei Digital Rights Management ist sicherlich die Akzeptanz durch die Nutzer. Dabei spielt die Benutzerfreundlichkeit der tatsächlichen Implementierung genau so eine wichtige Rolle, wie die Interoperabilität zwischen verschiedenen proprietären Modellen. Aber auch die generelle psychologische Komponente, nämlich das (wenn gleich fehlerhafte) Verständnis einer Vielzahl an Nutzern – insbesondere derjenigen, die das Internet stark in ihrem Alltag verwenden -, dass digitale Inhalte frei und leicht zugänglich sein sollten, ist nicht zu unterschätzen. Denn letztlich existiert kein technisches System um seiner selbst Willen. Auch der Einsatz von Digital Rights Management kann am Ende aus Sicht der Rechteinhaber nur „funktionieren", wenn durch die Verwendung solcher Schutzmechanismen nicht der Effekt eintritt, dass kein Benutzer mehr diese so versehenen digitalen Inhalte nutzt. Der Druck der „Internet-Gemeinde" auf den Verzicht von Digital Rights Management bei MP3 Dateien oder anderen Formaten für Musikstücke dürfte auch ausreichend groß gewesen sein, um einige Anbieter sozusagen zum Umdenken zu bewegen. In jüngsten Medienberichten war zu lesen, dass namhafte Provider bereits daran denken, auf Digital Rights Management wieder zu verzichten, oder zumindest die Nutzung zu erleichtern.

1.3. Die Kombination von Recht und Technik

Digital Rights Management ist daher, wie oben dargestellt, nicht (nur) mit Kopierschutz gleichzusetzen und ein (komplexeres) DRM System besteht aus zwei einander ergänzenden Komponenten [Günnewig02]:

- auf der einen Seite der Schutz durch technische Maßnahmen,
- auf der anderen Seite der Schutz durch rechtliche Maßnahmen.

Dieser Wechselwirkung zwischen der Technologie und dem Recht wurde zuletzt etwa auch in der Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22.5.2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der vorhandenen Schutzrechte in der Informationsgesellschaft, der so genannten Info-Richtlinie, auf die später noch näher Bezug genommen wird, ausdrücklich Rechnung getragen.

Historisch betrachtet lässt sich erkennen, dass der Schutz des Schöpfers eines Werks stets einem Wechselspiel aus rechtlichen und technischen Schutzmaßnahmen

unterworfen war. So ist auch das gesamte heute bekannte Konzept des Urheberrechts letztlich eine Entwicklung, die auf geänderte technische Umstände zurückgeht. Auch in diesem „Anlassfall“ war die Ursache für eine Änderung des bestehenden Rechtssystems der durch die technischen Umstände hervorgerufene geringere Aufwand beim Kopieren eines Werks.

Denn bis zum Ende des 15. Jahrhunderts waren die Möglichkeiten zur Kopie eines Schriftstückes nicht sehr einfach. Bis zum Ende des Mittelalters musste eine Kopie handschriftlich angefertigt werden. Dementsprechend war auch der mögliche Schaden durch Kopisten für den Hersteller des Urstücks nicht allzu groß.

Diese Situation änderte sich mit der Erfindung der Druckerpresse mit beweglichen Lettern durch Johannes Gutenberg [Dillenz]. Durch diese neue Technik gab es nun die Möglichkeit, die Vorlage mit wirtschaftlich geringerem Aufwand zu vervielfältigen und danach zu verbreiten.

Dementsprechend war auch die potenzielle Beeinträchtigung des ursprünglichen Werkerstellers entsprechend höher. Relativ schnell nach dieser Erfindung wurden daher monopolartige Sonderstellungen desjenigen, der zuerst das Werk erstellt hatte, nötig. Interessanterweise war in der Anfangszeit der urheberrechtlichen Entwicklung der Begünstigte dieses Schutzes der Drucker, nicht aber der Autor. Erst in der folgenden Zeit hat sich das Urheberrecht nach und nach zu dem entwickelt, wie es sich heute in Österreich darstellt.

In der Geschichte zeigt sich noch öfters, dass stets der Schutz des berechtigten Schöpfers auf zwei Ebenen, nämlich sowohl auf einer technischen als auch auf einer rechtlichen Ebene, erfolgt ist. So wurde mit Erfindung, aber vor allem der massenhaften Verbreitung von Tonbandgeräten, die so genannte „Leerkassettenvergütung“ eingeführt. Dementsprechend wurde diese Art der Vergütung in Deutschland etwa in den 60er Jahren, in Österreich mit der Urheberrechtsgesetznovelle 1980, eingeführt und existiert auch in anderen, aber nicht allen, europäischen Ländern. Da nun Musikstücke, die über den Rundfunk verbreitet wurden, von jedem Hörer aufgenommen und (beinahe) beliebig oft wieder abgespielt werden konnten, musste ein Ausgleich für die Urheber und sonstigen Berechtigten gefunden werden. Mit der Leerkassettenvergütung wurden die Interessen der Werkersteller und sonstigen Rechteinhaber wirtschaftlich für die Einschränkungen ihrer Exklusivitätsrechte für die Fälle des privaten Gebrauchs entschädigt, auch weil technisch keine Alternativen zur Verfügung standen.

Auf der anderen Seite zeigt auch die technische Entwicklung, dass der technische Schutz alleine nicht ausreichend ist. Die derzeit vorhandenen technischen Schutzmöglichkeiten werden offensichtlich als unzureichend empfunden bzw auch für diese gibt es stets Umgehungsmöglichkeiten. Die Entwicklung sowie die potenziellen Verletzer solcher technischen Schutzmöglichkeiten liefern sich geradezu ein Wettrennen. Daher wurden in letzter Zeit Stimmen laut, die wiederum eine Verstärkung des rechtlichen Schutzes gefordert haben. Dieser zusätzliche rechtliche Schutz dient nun auch insbesondere den technischen Schutzmaßnahmen bzw

verbietet deren Umgehung. So wurde in einigen neuesten legislativen Maßnahmen stets ein Verbot der Umgehung solcher technischen Maßnahmen vorgesehen.

Daneben ist natürlich jeder Schutz in das jeweilige rechtliche System eingeordnet. Typischerweise werden Rechte an einem Objekt oder Werk durch Vertrag oder vertragsähnliche Konstruktion eingeräumt. Auch aus der Position eines Vertragspartners hat jede der Parteien Rechte und Pflichten. Weder auf diese Rechte und Pflichten, noch die möglichen Ausgestaltungen von Lizenzverträgen und deren Zustandekommen oder überhaupt elektronische Verträge und den Vertragsschluss auf elektronischem Weg und deren jeweilige rechtliche Grundlage soll aber in dieser Arbeit im Weiteren eingegangen werden.

2. Urheberrecht

2.1. Allgemeines

Für das grundlegende Verständnis wichtig ist, dass es kein einheitliches Urheberrecht mit weltweiter Geltung gibt, sondern die Beantwortung der Frage, welche Rechte einem Schöpfer zustehen, immer einer nationalen Rechtsordnung unterliegt [Bortloff].

Der Begriff des Urheberrechts wird auch oft mit dem angloamerikanischen Terminus copyright gleichgestellt. Aus der wörtlichen Bedeutung dieser beiden Begriffe zeigt sich aber eine etwas andere zielgerichtete Ausprägung. Während der österreichische Begriff auf den Urheber, also den Schöpfer eines Werks, und seine Person abstellt, steht im Konzept des copyright (wörtlich „Kopierrecht") der Vorgang der Vervielfältigung im Vordergrund der rechtlichen Betrachtung. Trotz dieser Unterschiede sind natürlich dennoch den beiden Rechtssystemen auch etliche Gemeinsamkeiten eigen.

Zu Beginn sollen daher die rechtliche Situation und die einzelnen Rechte, die gewährt werden, beleuchtet werden. Dies beginnt mit einem kurzen Abriss internationaler Übereinkommen und Rechtsvorschriften. In weiterer Folge werden dann die in Österreich geltenden Rechtsvorschriften analysiert. Aufgrund der großen Tragweite soll ein kurzer Blick in die Rechtsordnung der USA zu demselben Thema folgen. Im Mittelpunkt des Interesses stehen dabei einerseits die eingeräumten Rechte, andererseits die Ausnahmen dazu sowie schließlich besondere Vorschriften über technologische Maßnahmen zur Verhinderung ungerechtfertigter Nutzung der Werke als auch die Regelung des Zugriffs.

Vorausgeschickt sei dabei, dass nicht jedes Produkt auch durch das Urheberrecht geschützt wird. Abgesehen von so genanten freien Werken, welche das Gesetz von seinem Schutz ausdrücklich ausnimmt, bedarf es einer bestimmten Qualität des Erzeugnisses, um unter den Begriff des „Werks" nach den urheberrechtlichen Vorschriften zu fallen. Als Werke werden dabei nur (1) eigentümliche geistige Schöpfungen geschützt, die (2) der Literatur, der Tonkunst, der bildenden Künste oder der Filmkunst entstammen. Diese beiden Merkmale müssen kumuliert vorliegen [Bücherle].

In der gegenständlichen Arbeit wird vorausgesetzt, dass es schutzwürdige und dem prinzipiellen Urheberrechtsschutz unterliegende digitale Werke gibt. Wie Bücherle darstellt, ist eine digitale Datei letztlich eine Ansammlung binärer Daten, die nur durch das entsprechende Anwendungsprogramm wieder in eine für den Menschen verständliche Form gebracht werden. Erst mit der Ausgabe erhalten diese Daten eine wahrnehmbare Gestalt. Letztlich ist dies aber für die urheberrechtliche Einordnung nicht relevant, ebenso wenig das tatsächliche Format, wie etwa unterschiedliche Graphikformate oder gar die Einbettung von Graphiken in Text oder die Ausgabe von Text in einem Graphikformat. Spätestens mit dem Zeitpunkt der Transformation des digitalisierten Werkes in eine analoge Ausgabeform wird es für die menschlichen

Organe wahrnehmbar und kann dann einer bekannten, sozusagen analogen, Kategorie zugeordnet werden [Bücherle].

Allerdings ist dabei zu bedenken, dass nicht jede Datei automatisch urheberrechtlichen Schutz genießt. Insbesondere aber digitale Bilder, digitale Töne (Musik) und digitale Tonvideos als Kombination der beiden erstgenannten, können ohne Zweifel dem prinzipiellen Werkbegriff unterstellt werden.

Zu Beginn sollen einige internationale Rechtsgrundlagen, die insbesondere in das österreichische Recht Eingang gefunden haben, dargestellt werden. Dieser Teil umfasst internationale Verträge, als auch die europarechtliche Grundlage. Auf dieser Basis aufbauend wird die österreichische Rechtslage dargestellt und schließlich ein kurzer Einblick in das amerikanische copyright gewagt.

2.2. Berner Übereinkunft

Die Berner Übereinkunft zum Schutze von Werken der Literatur und Kunst ist ein völkerrechtlicher Vertrag, der 1886 in Bern angenommen wurde. Sie begründete zum ersten Mal die Anerkennung des Urheberrechts zwischen souveränen Nationen.

Die Berner Übereinkunft sieht vor, dass jeder Vertragsstaat den Schutz an Werken von Bürgern anderer Vertragspartner genauso anerkennt wie den Schutz von Werken der eigenen Bürger. Der Schutz erfolgt gemäß der Berner Übereinkunft automatisch, somit werden keine Registrierung und kein Copyright-Vermerk vorausgesetzt. Die Berner Übereinkunft legt ein Mindestmaß an geschützten Rechten dar und definiert die geschützten Werke.

2.3. TRIPS

2.3.1 Allgemeines

Die Welthandelsorganisation (WTO, World Trade Organisation) ist eine internationale Organisation mit etwa 150 Mitgliederländern. Im Rahmen der WTO wurde im Jahre 1994 nach Verhandlungen über mehrere Jahre das Agreement on Trade Related Aspects of Intellectual Property Rights, der so genannte TRIPS-Vertrag, abgeschlossen. Dieser beschäftigt sich mit dem Urheberrecht und den dazu verwandten Rechten.

Der TRIPS-Vertrag implementiert einen Minimalanspruch von Schutzrechten, der nach der Vorgabe des TRIPS-Vertrags von jedem Mitgliedstaat umzusetzen ist. Als interessanter Aspekt ist dabei zu erwähnen, dass der Schutz von geistigem Eigentum auch der technischen Innovation sowie dem Transfer von Technologie dienen soll. Sowohl die Hersteller als auch die Nutzer sollen dadurch profitieren und der wirtschaftliche und soziale Wohlstand verstärkt werden.

2.3.2 Schutzrechte

Der TRIPS-Vertrag trat am 1. Jänner 1995 in Kraft. Der TRIPS-Vertrag etabliert dabei selbst keine eigenen Schutzrechte, sondern verweist auf die Berner Übereinkunft. Der wesentliche Zweck des TRIPS-Vertrags ist die Harmonisierung der Durchsetzung von Schutzrechten.

Auch hinsichtlich der Ausnahmen zu diesen Rechten ist der TRIPS-Vertrag nicht spezifisch. Er verweist lediglich darauf, dass entsprechende Beschränkungen und Ausnahmen für besondere Umstände vorzusehen sind, die die normale Verwertung des Werks nicht behindern und die sonstigen berechtigten Interessen des Rechteinhabers nicht unvernünftigerweise beeinträchtigen.

2.3.3 Digitale Schutzmaßnahmen

Der TRIPS-Vertrag verlangt allerdings nicht wie andere internationale Verträge oder nunmehr nationale Rechtsordnungen Schutzmaßnahmen für die digitale Verbreitung.

2.4. WIPO Copyright Treaty

Die World Intellectual Property Organization (WIPO) ist eine internationale Organisation zur Nutzung und zum Schutz von geistigem Eigentum. Mitglieder dieser Organisation sind derzeit 182 Staaten.

Ende des Jahres 1996 wurde der Copyright Treaty abgeschlossen. Er wurde mittlerweile von vielen Ländern ratifiziert.

2.4.1 Schutzrechte

Auch der WIPO Treaty verweist zunächst auf die Konvention von Bern und bestimmt, dass alle Vertragsparteien sich an diese zu halten haben. Darüber hinaus bestimmt der WIPO Treaty allerdings ganz bestimmte Werke als geschützt und umfasst nunmehr etwa auch Computerprogramme und Datenbanken.

In Artikel 6 regelt der WIPO Treaty das ausschließliche Recht des Urhebers, das Original und Kopien seiner Werke der Öffentlichkeit zur Verfügung zu stellen, sei es durch Verkauf oder sonstige Übertragung der Verfügungsbefugnis. In Artikel 7 werden für spezielle Werke die Rechte im Zusammenhang mit der Vermietung und Verleihung festgelegt.

Wie in anderen Vertragswerken und gesetzlichen Grundlagen zum Thema Urheberrecht enthält auch der WIPO Treaty Beschränkungen und Ausnahmen. Mit denselben Worten wie der TRIPS-Vertrag will er solche Umstände, die die normale Verwertung des Werks und die sonstigen geschützten Interessen des Urhebers nicht unnötigerweise beeinträchtigen, als zulässig ansehen.

2.4.2 Digitale Schutzmaßnahmen

Im Bereich der digitalen Umwelt sind die Artikel 11 und 12 von besonderer Bedeutung.

Gemäß Artikel 11 haben die Vertragsparteien die Verpflichtung, adäquaten rechtlichen Schutz, einschließlich effektiver rechtlicher Durchsetzungsmöglichkeiten dieses Schutzes, gegen die Umgehung von effektiven technologischen Maßnahmen, die durch den Urheber im Zusammenhang mit der Ausübung seiner Rechte gemäß dem Treaty oder der Konvention von Bern eingesetzt werden, zu bieten, sowie Maßnahmen oder Tätigkeiten im Hinblick auf das geschützte Werk, welche durch den Urheber nicht autorisiert worden sind, oder sonst durch Gesetz erlaubt sind, zu verhindern. Dieser Artikel stellt somit spezielle auf technologische Umsetzungen im Bereich des Digital Rights Management an.

Sein „Zwillingsbruder", nämlich Artikel 12, verlangt von den Vertragsparteien ebenso Verpflichtungen hinsichtlich des Schutzes von Informationen über die Wahrnehmung von Rechten („rights management information"). Diese Bestimmung enthält auch eine Definition des Begriffes „Rechteverwaltungsinformation". Nach dieser Definition handelt es sich dabei um Information, welche das Werk, dessen Autor, den Inhaber eines Rechtes an diesem Werk oder Bedingungen für die Nutzung des Werks einschließlich von Zahlen oder einem sonstigen Code, welcher diese Informationen darstellt, umfasst, wenn diese Information dem Werk oder einer Kopie davon beigefügt oder mit diesem gemeinsam veröffentlicht wird.

Nach Artikel 12 ist es untersagt, elektronische Informationen zum Rechtemanagement ohne entsprechende Befugnis zu entfernen oder zu verändern oder Werke bzw Kopien davon zu verbreiten oder sonst der Öffentlichkeit zur Verfügung zu stellen, wenn elektronische Rechteverwaltungsinformation ohne Befugnis entfernt oder verändert worden ist.

Nach dem Wortlaut und offenbar der Intention hinter der Formulierung, welche schließlich Eingang in den Vertrag gefunden hat, umfasst diese Bestimmung nur die tatsächliche Umgehung von technologischen Maßnahmen. Im ursprünglichen Vorschlag war daneben noch die Verbreitung von Gegenständen, welche der Umgehung dienen, also eine Hilfstätigkeit dazu, umfasst. Dieser zweite Aspekt ist in der letztlich verabschiedeten Fassung nicht mehr enthalten. Andererseits umfasst Artikel 11 nur effektive technologische Maßnahmen. Diese Bestimmung darf allerdings nicht zu einschränkend ausgelegt werden. Ansonsten bliebe kein Anwendungsraum, da effektive technologische Maßnahmen definitionsgemäß nicht umgangen werden könnten.

2.5. Europarechtliche Grundlagen

Auch die Europäische Union hat zahlreiche Rechtsgrundlagen im Gebiet des Urheberrechts zur Vereinheitlichung des Schutzniveaus in ihren Mitgliedsländern geschaffen. Zu nennen sind hier die Richtlinie 91/250/EWG des Rates über den Rechtsschutz von Computerprogrammen (Software-Richtlinie), die als Hauptziel die

Vereinheitlichung des Schutzes von Computerprogrammen hat, die Richtlinie 92/100/EWG des Rates zum Vermietrecht und Verleihrecht sowie zu bestimmten dem Urheberrecht verwandten Schutzrechten im Bereich des geistigen Eigentums (Vermiet- und Verleih-Richtlinie), die Richtlinie 93/98/EWG des Rates zur Harmonisierung der Schutzdauer des Urheberrechts und bestimmter verwandter Schutzrechte (Schutzdauer-Richtlinie), die Richtlinie 96/9/EG des Europäischen Parlaments und des Rates über den rechtlichen Schutz von Datenbanken (Datenbank-Richtlinie), insbesondere und im Hinblick auf das Thema dieser Arbeit mit weitem Abstand vor den anderen die aber die Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (Info-Richtlinie) und zuletzt die Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates zur Durchsetzung der Rechte des geistigen Eigentums (Richtlinie zum Schutz der Rechte an geistigem Eigentum).

2.5.1 Die Info-Richtlinie

2.5.1.1 Grundsätzliches

Mit dieser Richtlinie sollten aus Sicht des europäischen Gesetzgebers die einschlägigen Regelungen des Binnenmarkts harmonisiert werden. Dementsprechend normiert die Richtlinie als wesentliche Eckpfeiler die folgenden Rechte:

- das Vervielfältigungsrecht (Art 2);
- das Recht der öffentlichen Wiedergabe und der öffentlichen Zugänglichmachung sonstiger Schutzgegenstände (Art 3);
- das Verbreitungsrecht (Art 4);

sowie dazu jeweils Ausnahmen und Beschränkungen (Art 5).[2]

2.5.1.2 Die technische Schutzmaßnahmen

Die Info-Richtlinie trägt in Erwägungsgrund 5 ausdrücklich auch den technischen Entwicklungen Rechnung. Die Info-Richtlinie führt aus, dass zwar kein Bedarf an neuen Konzepten für den Schutz des geistigen Eigentums besteht, jedoch den neuen Formen der Verwertung in angemessener Weise Rechnung zu tragen ist.

Auch an weiteren Stellen, etwa in Erwägungsgrund 10, nimmt die Richtlinie auf Multimediaprodukte ausdrücklich Bezug und in Erwägungsgrund 17 bezieht sie sich auf die durch die Digitaltechnik bedingten Erfordernisse.

Vor diesem Hintergrund verankert die Richtlinie folglich in Artikel 6 die Verpflichtung an die Mitgliedstaaten, einen angemessenen Rechtsschutz gegen die Umgehung wirksamer technischer Maßnahmen vorzusehen. Dieses Verbot von Umgehungen erfasst dabei nicht nur die eigentliche Umgehungshandlung, sondern

[2] Auf die einzelnen Rechte und die Auswirkung der Info-Richtlinie für Österreich wird unten eingegangen.

daneben auch die Herstellung, die Verbreitung und Verkauf oder Vermietung oder die Werbung sowie zudem den Besitz zu kommerziellen Zwecken von Vorrichtungen, Erzeugnissen oder Bestandteilen sowie die Erbringung von Dienstleistungen, jeweils mit dem Ziel der Umgehung wirksamer technischer Maßnahmen. Der Text der Richtlinie umfasst dabei in einer weit gefassten Definition auch solche Vorrichtungen und Erzeugnisse, die zwar nicht ausschließlich der Umgehung gewidmet sind, aber abgesehen von der Umgehung von wirksamen technischen Maßnahmen nur einen begrenzten, anderen wirtschaftlichen Zweck oder Nutzen haben oder hauptsächlich dafür für diese Umgehung entworfen, hergestellt, angepasst oder erbracht werden.

Dabei ist allerdings sicherzustellen, dass die Rechteinhaber ihre Werke den Begünstigten im Ausmaß der im Urheberrecht vorgesehenen Ausnahmen, insbesondere für die Nutzungen für den privaten Gebrauch, zur Verfügung stellen.

Daneben normiert die Richtlinie, dass auch Informationen über die Rechtewahrnehmung geschützt sind. Die Entfernung oder Änderung solcher elektronisch angebrachten Informationen für die Wahrnehmung der Rechte als auch die Verbreitung, Einfuhr, öffentliche Wiedergabe oder öffentliche Zugänglichmachung von Werken, bei denen diese Informationen entfernt oder geändert wurden, soll dabei verboten sein.

In regelmäßigen Abständen hat die Kommission dem Europäischen Parlament, dem Europäischen Rat und dem Europäischen Wirtschafts- und Sozialausschuss einen Bericht über die Anwendung dieser Richtlinie zu unterbreiten, in dem sie unter anderem auf der Grundlage der von den Mitgliedstaaten mitgeteilten Informationen, insbesondere die Anwendung der Artikel 5 (das sind die Ausnahmen und Beschränkungen zu den Rechten), 6 (das sind die Pflichten in Bezug auf technische Maßnahmen) und 8 anhand der Entwicklung des digitalen Marktes prüft. Im Falle des Artikels 6 muss sie dabei insbesondere prüfen, ob dieser ein ausreichendes Schutzniveau sicherstellt und ob sich der Einsatz wirksamer technischer Maßnahmen nachteilig auf gesetzlich erlaubte Handlungen auswirkt. Erforderlichenfalls hat sie – insbesondere um das Funktionieren des Binnenmarkts im Sinne von Artikel 14 des Vertrags sicherzustellen - entsprechende Änderungsvorschläge zu dieser Richtlinie vor zu legen.

Die Richtlinie setzt damit den WIPO Treaty beinahe wortwörtlich um.

2.5.2 Die Mitteilung der Kommission

Die Mitteilung der Europäischen Kommission an den Europäischen Rat, das Europäische Parlament und den Europäischen Wirtschafts- und Sozialausschuss über die Wahrnehmung von Urheberrechten und verwandten Schutzrechten im Binnenmarkt beschäftigt sich unter anderem auch ausdrücklich mit Digital Rights Management.

Die Kommission ist dabei der Meinung, dass die Entwicklung von Digital Rights Management-Systemen prinzipiell von der Akzeptanz aller Interessenträger,

einschließlich der Verbraucher, sowie von der Haltung des Gesetzgebers zum Urheberrecht abhängt. Eine Grundvoraussetzung, einen gemeinschaftsweiten Zugang zu DRM Systemen und –Dienstleistungen sowohl durch Rechteinhaber wie auch Nutzer als auch insbesondere Verbraucher zu gewährleisten, liegt in der Interoperabilität von DRM Systemen und –Dienstleistungen.

Die Kommission geht sogar so weit, DRM Systeme als ein wichtiges, wenn nicht das wichtigste Instrument der Rechtewahrnehmung für die neuen digitalen Dienste im Binnenmarkt zu benennen.

Allerdings meint die Kommission, dass Digital Rights Management zum Zeitpunkt der Erstellung der Mitteilung keine politische Lösung zur Gewährleistung eines angemessenen Gleichgewichts der beteiligten Interessen, nämlich der Interessen der Urheber als auch anderer Rechteinhaber oder der Anliegen der rechtmäßigen Nutzer, Verbraucher und anderer beteiligter Dritter (Bibliotheken, Service-Provider und andere) bietet. DRM Systeme sind nach der Meinung der Kommission nämlich nicht ohne weiteres als eine Alternative zur Politik des Urheberrechts anzusehen, Parameter in Bezug auf den Schutz des Urheberrechts, seiner Ausnahmen und seiner Beschränkungen aufzustellen, die seit jeher von der Gesetzgebung angewendet werden.

Die Kommission wiederholt daher, dass der Schutz von DRM Systemen gegen Umgehung, gegen die Herstellung und den Vertrieb von Umgehungsvorrichtungen und der Schutz von Urheber- und Leistungsschutzrechten gegen jede Form der Piraterie deshalb eine unerlässliche Voraussetzung ist, um dieses Risiko auf ein Minimum zu beschränken und die legale Nutzung von geschütztem Inhalt sowie die Akzeptanz auf Seiten der Rechteinhaber, der gewerblichen Nutzer und der Verbraucher gleichermaßen zu gewährleisten. Die notwendige Akzeptanz der Verbraucher ist dabei, wie die Kommission ausführt, der eigentliche Schlüssel zum Erfolg der DRM Systeme. Die Kommission streicht dabei auch den Schutz der Privatsphäre (einschließlich die Gewährleistung von Sicherheit) hervor. Getreu der Aufgabenstellung der Mitteilung erkennt die Kommission, dass DRM Systeme und Vergütungssysteme, mit denen die Nutzung von geschützten Inhalten auf einer kommerziellen Basis ermöglicht wird, unterschiedliche Funktionen erfüllen. Die Kommission bemängelt dabei, dass die eingesetzten DRM Systeme den Zugang zu Werken lediglich nach Ermessen der Ersteller (oder ihrer Lizenznehmer) bieten, denn Anwendungsgrundlage sind hier ausschließliche Rechte (zur Genehmigung oder Untersagung der Nutzung).

2.5.3 Die Empfehlung der Kommission zu Online-Musikdiensten

In der Empfehlung der Kommission vom 18. Mai 2005 für die länderübergreifende kollektive Wahrnehmung von Urheberrechten und verwandten Schutzrechten, die für legale Online-Musikdienste benötigt werden (2005/737/EG), setzt sich die Europäische Kommission neuerlich mit dem Schutz von digitalen Daten, diesmal konkret Musikwerken auseinander. Anders als die Info-Richtlinie hat diese Empfehlung keinen bindenden Charakter, gibt aber die Ansicht der Kommission wieder. Es ist daher denkbar, dass die darin vertretenen Standpunkte in Zukunft

auch tatsächlich übernommen werden oder von der Kommission in verbindliche Kriterien umgesetzt werden.

Die Kommission [folgende Darstellung nach Kommission05] spricht in der Empfehlung ausdrücklich Online-Musikdienste an und erkennt die Defizite der momentanen Rechtslage. Sie hält dabei fest, dass „neue Technologien eine neue Generation gewerblicher Nutzer hervorgebracht haben, die Musikwerke und andere Inhalte online verwendet. Die Bereitstellung legaler Online-Musikdienste berührt eine Reihe von Urheber- und Leistungsschutzrechten“ [Kommission05]. Die Kommission erkennt auch deutlich, dass „eine Kategorie dieser Rechte das ausschließliche Vervielfältigungsrecht ist, das sich auf alle im Zuge der Online-Verbreitung von Musikwerken vorgenommenen Vervielfältigungen erstreckt. Andere Kategorien von Rechten sind das Recht der öffentlichen Wiedergabe eines Musikwerkes, das Recht auf angemessene Vergütung für die öffentliche Wiedergabe anderer Inhalte und das ausschließliche Recht der öffentlichen Zugänglichmachung eines Musikwerks oder anderer Inhalte“ [Kommission05]. Nach der vorgenommen Definition der Empfehlung ist dabei ein Musikwerk breit gefasst und umfasst jedes Werk der Musik aber auch andere Inhalte. Die Kommission [Kommission05] definiert folglich den Begriff der „Online-Rechte“ als eines der (ausschließlichen) Rechte auf „(i) Vervielfältigung in der Form von unkörperlichen Kopien, die im Zuge der Online-Verbreitung von Musikwerken vorgenommen werden, (ii) öffentliche Wiedergabe eines Musikwerks, entweder in der Form eines Rechts zu erlauben oder zu verbieten, oder eines Rechts auf angemessene Vergütung. Diese Rechte erstrecken sich auf Webcasting, Internet-Radio und Simulcasting oder „Near-on-Demand“-Dienste, die entweder auf einem PC oder auf einem Mobiltelefon empfangen werden, als auch (iii) öffentliche Zugänglichmachung eines Musikwerks, das „On-Demand“ oder andere „interaktive“ Dienste umfasst“ [Kommission05].

Lizenzen sind, wie die Empfehlung weiter ausführt [Kommission05], oft auf ein Territorium beschränkt – wobei dies oftmals das Gebiet eines Mitgliedsstaates der Europäischen Union ist. Dies zwingt nach Ansicht der Kommission gewerbliche Nutzer, für jedes in der Online-Nutzung benötigte Recht in jedem Mitgliedstaat von jeder jeweiligen Verwertungsgesellschaft eine Lizenz zu erwerben. Im Zeitalter der Online-Nutzung von Musikwerken brauchen daher gewerbliche Nutzer in den Augen der Kommission aber ein multiterritorial ausgelegtes Lizenzierungssystem, das der Grenzenlosigkeit der Onlinewelt gerecht wird. Es sollte daher für eine multiterritoriale Lizenzierung gesorgt werden, um für gewerbliche Nutzer mehr Rechtssicherheit für ihre Tätigkeit zu fördern und das Wachstum legaler Online-Dienste zu fördern, wodurch sich wiederum die Einnahmen der Rechteinhaber erhöhen würden. Wie insbesondere der letzte Aspekt zeigt, ist diese Empfehlung der Kommission natürlich – gemäß ihrem Auftrag – im Sinne der Vereinheitlichung des Binnenmarktes innerhalb der Europäischen Gemeinschaft gefasst. Das Verhältnis zwischen Rechteinhabern und Verwertungsgesellschaften soll schließlich, unabhängig davon, ob der Wahrnehmungsauftrag auf vertraglichen Vereinbarungen oder statutarischen Mitgliedschaftsbestimmungen basiert, für die Rechteinhaber einen Mindestschutz in Bezug auf alle Rechte beinhalten, die für die Bereitstellung legaler Online-Musikdienste erforderlich sind. Verwertungsgesellschaften sollten

nach Ansicht der Kommission Rechteinhaber im Hinblick auf ihren Sitzstaates oder ihre Staatsangehörigkeit nicht unterschiedlich behandeln.

Die Mitgliedstaaten werden von der Kommission eingeladen, „die notwendigen Schritte zu unternehmen, um das Wachstum von legalen Online-Musikdiensten zu ermöglichen, indem sie rechtliche Rahmenbedingungen zur optimalen Wahrnehmung von Urheberrechten oder verwandten Schutzrechten für die Erbringung legaler Online-Musikdienste auf Gemeinschaftsebene fördert“ [Kommission05]. Rechteinhaber sollen dabei „das Recht haben, die Wahrnehmung aller Online-Rechte, die zum Betrieb legaler Online-Musikdienste notwendig sind, in einem territorialen Umfang ihrer Wahl einer Verwertungsgesellschaft ihrer Wahl anzuvertrauen; der Sitzstaat oder die Staatsangehörigkeit der Verwertungsgesellschaft bzw des Rechteinhabers sollte hierfür keine Rolle spielen“ [Kommission05].

Obgleich die Empfehlung nun schon etwas länger zurückliegt, bleibt zu sehen, ob aus dieser letztlich ein konkreterer Rechtsrahmen resultiert.

2.6. Österreich

Im österreichischen Urheberrechtsgesetz (Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte, BGBl. Nr. 111/1936 BGBl idgF, nachfolgend „UrhG“), welches die oben angeführten internationalen Vereinbarungen umsetzt, werden dem Schöpfer eines Werks sowie unter Umständen anderen Personen verschiedene Rechte zuerkannt. Die sprachliche Verwendung der Begrifflichkeiten ist für den österreichischen Rechtsraum auch nicht präzise, denn das Urheberrecht als solches besteht eigentlich nicht. Diese Rechte unterteilen sich wiederum in so genannte Verwertungsrechte und Persönlichkeitsrechte.

Urheber ist dabei derjenige, der ein Werk geschaffen hat. Diesem steht zunächst das ausschließliche Recht zu, sein Werk zu verwerten. Dieses Recht fußt in dem Gedanken des Gesetzgebers, dass eine Schöpfung einen Beitrag zu Allgemeinheit liefert. Der Urheber soll in der Lage sein, diesen Beitrag auch entsprechend wirtschaftlich zu nutzen.

2.6.1 Das Vervielfältigungsrecht

Nach der Konzeption des Gesetzes ist das Vervielfältigungsrecht das Wesentlichste im Rahmen der Verwertungsrechte.

2.6.1.1 Grundsätzliches

Gegenstand der Vervielfältigung ist die Herstellung eines körperlichen Gegenstücks. Dieses kann, seit der Präzisierung der Gesetzesstelle durch die Umsetzung der Info-Richtlinie, ausdrücklich vorübergehend oder dauerhaft sein.

Gemäß dem Wortlaut des Gesetzes sind aber auch für einige Werke andere Verfahren und Techniken als Vervielfältigung aufzufassen, so ist auch das Festhalten

eines Vortrags oder Aufführung eines Werks etwa auf Film oder Platte als Vervielfältigung definiert.

2.6.1.2 Digitale Inhalte

Der Begriff der Vervielfältigung ist allerdings nicht von einer körperlichen Vervielfältigung im herkömmlichen Sinne abhängig. Auch die digitale Herstellung einer Kopie von einem digitalen Original sowie die Digitalisierung eines Werkstückes, also die Umsetzung von analogen Signalen in einen binären Zahlencode, so dass dieser Zahlencode abspeicherbar und abrufbar ist, ist ein Festhalten des Werks. Dieses gestattet es ebenfalls, nach Rückverwandlung des digitalen Signals in Schallwellen unter Zuhilfenahme entsprechender technischer Einrichtung, das Musikstück wiederum sinnlich wahrzunehmen. Gleichgültig ist dabei auch das Speichermedium für den binären Zahlencode.

Sowohl die Erstspeicherung als auch die Übertragung der digitalen Daten von einem Speicher in einen anderen ist eine Vervielfältigung. Der Oberste Gerichtshof hat in einer Entscheidung auch dazu ausgeführt, dass das dem Urheber zugestandene Vervielfältigungsrecht ihm zugleich ein Entgelt für Nutzungshandlungen sicherstellen soll [OGH99]. Diese Nutzungshandlungen entstehen eben aufgrund des Werkgenusses durch Vervielfältigungen des Originals. Das Original kann nur einem relativ beschränkten Personenkreis ermöglichen, das Werk zu genießen. Durch die Vervielfältigung tritt ein Multiplikationseffekt ein, so dass ein sehr viel größerer Personenkreis erfasst werden kann. Die Interessen des Urhebers liegen nun darin, diese Vervielfältigungen von seiner Zustimmung abhängig zu machen bzw dass er sie eben gegen Entgelt gestatten kann. Daher sind solche Handlungen eine Vervielfältigung im urheberrechtlichen Sinn, die in irgendeiner Form die Verwertungsmöglichkeiten des Urhebers beeinträchtigen. Dementsprechend ist eben auch die Speicherung eines Musikstückes auf der Festplatte einer Computeranlage allenfalls auch eben nach dessen digitaler Umwandlung eine Vervielfältigung, weil dadurch die Nutzungsmöglichkeiten dieses Stücks im Verhältnis zu den Nutzungsmöglichkeiten der ursprünglichen Tonquelle sowohl quantitativ als auch qualitativ erweitert werden.

Die Ansicht des Gesetzgebers, dass Vervielfältigungen nicht nur in körperlicher Weise passieren müssen, ergibt sich auch aus einer Betrachtung der Bestimmungen des UrhG für Computerprogramme. Auch dort erfolgt ein zumindest temporärer Vervielfältigungsschritt, wenn das Computerprogramm von dem Festplattenspeicher in den Arbeitsspeicher (RAM) „geladen“ wird. Für diese Vervielfältigungsschritte, die bestimmungsgemäß notwendig sind, gibt es gemäß § 40d Abs 2 UrhG eine entsprechende Ausnahme vom Vervielfältigungsrecht, das sonst generell bestehen würde.

2.6.2 Das Verbreitungsrecht

Neben dem Vervielfältigungsrecht gesteht das UrhG dem Urheber auch das ausschließliche Recht zu, Werkstücke zu verbreiten.

2.6.2.1 Grundsätzliches

Voraussetzung für das Bestehen eines Verbreitungsrechts ist die Vorlage eines physischen Werkexemplars [Dillenz]. Verbreitet wird ein Werk, wenn es „in den Verkehr gebracht wird", wenn also einem anderen die tatsächliche oder rechtliche Verfügungsmacht über ein Werkstück eingeräumt wird [OGH60]. Schon das Anbieten ist allerdings ein vorbehaltener Akt der Verbreitung [OLG85]. In derselben Entscheidung wurde auch festgehalten, dass Entgeltlichkeit kein Tatbestandsmerkmal ist.

2.6.2.2 Digitale Inhalte

Wesentlich für digitale Werke ist, dass nach allgemeiner Auffassung die Verbreitung nicht die Wiedergabe des Inhaltes erfasst, sondern nur die Verbreitung von körperlichen Werkexemplaren [Bücherle]. Die zu Grunde liegende Bestimmung des UrhG ist auch nicht im Rahmen der Umsetzung der Info-Richtlinie angepasst worden. Dies ist insbesondere von Interesse, als etwa die Bestimmung über das Vervielfältigungsrecht novelliert wurde und eben seither ausdrücklich auch eine vorübergehende Vervielfältigung mit einschließt.

Damit ist die unkörperliche Online-Übertragung nicht vom Begriff der Verbreitung im Sine des UrhG umfasst.

2.6.3 Das Senderecht

2.6.3.1 Grundsätzliches

Gemäß § 17 UrhG hat der Urheber das ausschließliche Recht, das Werk durch Rundfunk oder eine ähnliche Art zu senden. Gemäß Absatz 2 dieser Gesetzesstelle steht es einer Rundfunksendung gleich, wenn ein Werk der Öffentlichkeit ähnlich wie durch Rundfunk mit Hilfe von Leitungen wahrnehmbar gemacht wird. Nicht nur die „klassische" Rundfunksendung sondern auch Kabelfernsehen ist somit erfasst.

Die Definition des § 17 UrhG ist allerdings soweit gefasst, dass auch Datenströme im world wide web vom Wortlaut erfasst sind. Kernelement des Senderechts ist die Wiedergabe an die Öffentlichkeit, also an eine Mehrzahl von Personen, die nicht nach einem Kriterium bestimmt abgegrenzt sind und weder durch gegenseitige Beziehungen noch durch Beziehungen zum Veranstalter persönlich untereinander verbunden sind. Markantes Merkmal des Senderechts ist daher die Point to Multipoint-Ausstrahlung [Bücherle].

2.6.3.2 Digitale Inhalte

Soweit digitale Inhalte bloß zum Abruf bereitgestellt werden, fallen sie nicht unter den Begriff des Senderechts. Modernere Techniken – „Push"-Technologien – allerdings, übermitteln die Daten stetig, ohne weitere Anforderung des Nutzers. Sofern eine entsprechende Öffentlichkeit gegeben ist, ist auf solche Inhalte das Senderecht anwendbar [Bücherle].

2.6.4 Das Vortrags-, Aufführungs- und Vorführungsrecht (öffentliche Wiedergabe)

Der Gegenstand dieses Rechts sind bloß Sprachwerke, Werke der Tonkunst und der bildenden Künste sowie Filmwerke. Das Vortrags-, Aufführungs- und Vorführungsrecht ist im Wesentlichen ein nicht interaktives Recht.

Gerade vor dem Hintergrund der Schwierigkeiten, den Umfang dieses Rechts auszulegen, vom Senderecht genau abzugrenzen und insbesondere auf digitale Inhalte anzuwenden, wurde das Recht der Zurverfügungstellung eingeführt.

2.6.5 Das Zurverfügungstellungsrecht

2.6.5.1 Grundsätzliches

Wie oben kurz angerissen, war lange Zeit umstritten, ob die Nutzung von Werken und Leistungen in digitalen Netzen als Vervielfältigung und Verbreitung oder als öffentliche Wiedergabe anzusehen ist.

Mit Umsetzung der Info-Richtlinie, welche für den Urheber ein Recht der öffentlichen Wiedergabe sowie der öffentlichen Zugänglichkeit vorsieht, wurde der neue § 18 a UrhG in Ergänzung der übrigen Bestimmungen eingefügt. Gemäß diesem Recht hat der Urheber das ausschließliche Recht, das Werk der Öffentlichkeit drahtgebunden oder drahtlos in einer Weise zur Verfügung zu stellen, dass es Mitgliedern der Öffentlichkeit von Ort und zu Zeiten ihrer Wahl zugänglich ist. Damit werden insbesondere „on demand" Dienste miterfasst.

Dieses Recht stellt nur auf das Bereithalten für den Abruf ab, umfasst aber nicht die Vorgänge des Abrufens selbst [Handig04-1]. Diese müssen gesondert beurteilt werden.

Im WWW erfolgt das Zurverfügungstellen mit dem uploading, also dem Abspeichern auf einem Webserver. Danach ist der Abruf durch Mitglieder der Öffentlichkeit möglich. Sobald also das Werk auf einem Webserver liegt, auf dem es von sozusagen jedermann eingesehen werden kann, ist das Recht verbraucht. Ein Hyperlink, der auf dieses Werk zeigt, greift nicht in das Zurverfügungsstellungsrecht ein [Handig].

2.6.5.2 Digitale Inhalte

Dieses Recht wurde gerade für digitale Inhalte geschaffen und ist damit jedenfalls auf sie anwendbar.

2.6.6 Die Leerkassettenvergütung

2.6.6.1 Grundsätzliches

Die Leerkassettenvergütung wurde oben in Punkt 1.3 bereits erwähnt. Ihr wesentlicher Zweck dient dem Ausgleich der wirtschaftlichen Interessen der Urheber und sonstigen Berechtigten an einem Werk und Vervielfältigungen, die

nicht gesondert abgegolten werden. Aufgrund der Bedeutung dieser Vergütung auch für den digitalen Bereich soll hier die Grundlage etwas beleuchtet werden.

Die entsprechende Bestimmung des UrhG (§ 42 b) spricht hierbei von Werken, die durch Rundfunk gesendet oder auf einem zu Handelszwecken hergestellten Bild- oder Schallträger festgehalten worden sind, nach deren Art es zu erwarten ist, dass sie durch Vervielfältigung zu privaten oder eigenem Gebrauch auf einen Bild- und Schallträger festgehalten werden. In diesem Fall hat der Urheber Anspruch auf eine angemessene Vergütung für im Inland gewerbsmäßig in Verkehr gebrachtes Trägermaterial. Als Trägermaterial gelten gemäß den Gesetzesbestimmungen unbespielte Bild- oder Schallträger, die für solche Vervielfältigungen geeignet sind.

Seit der zugrunde liegenden Novelle des UrhG werden daher von jeder verkauften leeren Tonkassette - und um diesen Träger geht es (ging es bisher) im Wesentlichen - eine Abgabe an die gesetzlich anerkannten Verwertungsgesellschaften gezahlt. Diese Verwertungsgesellschaften sind die gesetzlich vorgesehenen Gemeinschaften, die sich für und anstelle der eigentlichen Urheber und sonstigen Rechteinhaber um die Durchsetzung und Verfolgung der Urheberrechte kümmern.

Hintergrund der Leerkassettenvergütung war, wie gezeigt wurde, die entsprechende technische Entwicklung bei der Vervielfältigung. Durch die größere Verbreitung von Kassettenrecordern konnten Werke, die im Rundfunk übertragen wurden, nun auch einfach mit entsprechend ausreichender Qualität aufgenommen werden. Diese Aufnahme konnte beinahe beliebig oft abgespielt werden und ersetzt dadurch die Notwendigkeit des privaten Nutzers, eine für den Handel hergestellte „autorisierte“ Originalschallplatte oder –kassette zu erwerben. Selbstverständlich gilt das entsprechend gleiche System auch für Videokassetten und Videoanlagen. Ebenso besteht in diesem Fall für den privaten Seher keine Notwendigkeit eine Originalvideokassette zu erwerben. Interessant ist an diesem Aspekt, dass nicht versucht wurde mit technischen Maßnahmen oder anderen rechtlichen Instrumenten, etwa Verboten, der technischen Entwicklung Einhalt zu gebieten. Vielmehr wurde ein System nach Vorbild der deutschen Gesetzgebung eingeführt, dass die wirtschaftlichen Interessen der Urheber zu schützen versucht.

Zu bemerken ist an dieser Stelle, auf welche Träger die Bestimmung Anwendung findet. Nach manchen Kommentatoren ist hier auf typische und wahrscheinliche Vorgänge abzustellen. Diese Typizität und Wahrscheinlichkeit kann aber im Laufe der Zeit sich ändern. So wird in einem Kommentar aus 1999 noch festgehalten, dass „auf die klassischen Computerdisketten auch Musik aufgenommen werden kann, typischerweise geschieht dies aber nicht“ [Dillenz]. Diese Ansicht ist mittlerweile sicherlich durch die Entwicklungen im Bereich der digitalen Musik überholt.

2.6.6.2 Anwendung der Leerkassettenverordnung auf digitale Medien

In Österreich kassiert die „austro mechana“ die Leerkassettenvergütung für ihre eigenen Rechteinhaber (Komponisten, Textautoren und Musikverleger) und auch für andere Berechtigte, die durch andere Verwertungsgesellschaften vertreten werden.

Mit Entscheidung des Obersten Gerichtshofs [OGH05] wurde nun entschieden, dass Festplatten in Personal Computer nicht vergütungspflichtig sind, allerdings hat der OGH im selben Urteil Trägermaterial, das in MP3-Playern integriert ist, und wechselbare Speicherkarten für solche als im Sinne des Urheberrechts vergütungspflichtig erkannt. In seiner Begründung hat der Gerichtshof festgehalten, dass externe als auch interne Festplatten, „auf Grund des technischen Fortschritts regelmäßig zu einem gewichtigen und nicht zu vernachlässigenden Teil auf eine Weise genutzt werden können und auch genutzt werden, die mit der Abgeltung für die Vervielfältigung zum eigenen Gebrauch in keinerlei Zusammenhang steht (EDV, Programmsteuerung, Textverarbeitung, Speicherung privater digitaler Text- und Bilddateien uvm)". Daher würden bei einer Einhebung der Leerkassettenvergütung auf diese Medien die Begünstigten regelmäßig mehr erhalten, „als ihnen der Gesetzgeber nach dem erklärten Ziel dieser Vergütung zugedacht hat". Damit konnte er eine Abgabe für multifunktionale Geräte nicht für rechtmäßig erachten. MP3-Player werden nach Ansicht des OGH allerdings verwendet, „um Musik zu hören; die dafür geeigneten Speichermedien werden derzeit in weit überwiegendem Maß für Vervielfältigungen verwendet, deren Abgeltung das Gesetz anstrebt." Das Gericht hat sich auch mit der Argumentation auseinander gesetzt, dass Speichermedien sowohl in MP3-Geräten als auch anderen Geräten, etwa digitalen Kameras benutzt werden können. Er hat diesen Ansatz allerdings abgelehnt, da nach seiner Meinung diese Verwendungsmöglichkeiten wirtschaftlich „nicht ins Gewicht fallen". Zu beachten ist allerdings, dass diese Entscheidung im Sommer 2005 gefällt wurde, so dass aufgrund der stark in die Begründung der Entscheidung einfließenden tatsächlichen und wirtschaftlichen Gegebenheiten zum heutigen Zeitpunkt eine anders lautende Entscheidung insbesondere über die wechselbaren Speichermedien denkbar sein könnte.

Damit hat der OGH letztlich auch festgestellt, dass nach dem UrhG kein erkennbarer Unterschied zwischen digitalen und analogen Medien zur Speicherung gemacht werden kann. Im Vergleich zu den analogen Medien hat der OGH auch eine Vergütung in Abhängigkeit der Speichergröße und somit im – wenngleich mittelbaren, weil auch von Faktoren wie etwa vom Kompressionsgrad abhängigen - Zusammenhang mit der Menge an Musik, die speicherbar ist, anerkannt.

In Österreich ist damit die Bedeutung von Digital Rights Management für die Musikindustrie möglicherweise wieder gestiegen, andererseits können Gegner von Digital Rights Management das Argument, dass die urheberrechtlich Berechtigten ohnedies einen wirtschaftlichen Ausgleich erhalten, nicht mehr zur Gänze aufrecht erhalten. Offen geblieben ist allerdings dennoch die Problematik, dass eben nun sehr wohl aufgrund der Abgabe für MP3-Geräte eine Vergütung erfolgt, so dass eine nochmalige Vergütung für das einzelne Musikstück möglicherweise als „zuviel" angesehen werden könnte.

2.6.7 Die Reprografievergütung

Nach der Leerkassettenvergütung ist auch die so genannte Reprografievergütung zu nennen. Diese ist der Leerkassettenvergütung stark angeglichen und mit dieser gemeinsam geregelt. Gegenstand der Reprografievergütung ist die Vervielfältigung

mit Hilfe reprografischer oder ähnlicher Verfahren, also insbesondere die Fotokopie. Allerdings ist auch das Verfahren von Telefaxgeräten und Scangeräten darunter einzuordnen. Anders als in der Leerkassettenvergütung ist Gegenstand bzw Anknüpfungsobjekt nicht das Trägermaterial, sondern das Vervielfältigungsgerät.

Selbstverständlich werden weder mit den leeren Tonträgern noch mit Reprografiegeräten ausschließlich urheberrechtlich geschützte Werke vervielfältigt bzw aufgenommen. Dennoch versucht das Gesetz mit einer kursorischen, alle sozusagen Beteiligten idealerweise gleich verteilt treffenden, Belastung dem doch nicht fern liegenden Gedanken Rechnung zu tragen, dass die Mehrheit der damit aufgenommenen bzw vervielfältigten Werke sehr wohl urheberrechtlich geschützt sein wird.

2.6.8 Die Urheberpersönlichkeitsrechte

Neben den vorhin angeführten Verwertungsrechten stehen dem Urheber auch noch Persönlichkeitsrechte zu. Diese dienen nicht den wirtschaftlichen sondern den geistigen Interessen am Werk, insbesondere der Verbundenheit des Werks mit seinem Schöpfer. Im Gegensatz zu Verwertungsrechten, die übertragen werden können, verbleiben die Urheberrechte stets beim Urheber und sind weder verzichtbar noch übertragbar.

2.6.8.1 Das Recht der Urheberschaft

Das UrhG gibt dem Urheber das Recht, jederzeit seine Urheberschaft zu behaupten und für sich in Anspruch zu nehmen. Dieses Recht gilt gegen jedermann, der die Anerkennung seiner Urheberschaft bestreitet oder sich selbst die Urheberschaft anmaßt.

2.6.8.2 Die Urheberbezeichnung

Der Urheber hat wiederum das ausschließliche Recht darüber zu entscheiden, ob und mit welcher Urheberbezeichnung sein Werk versehen wird.

2.6.9 Die Beschränkungen und Ausnahmen zu den Verwertungsrechten

Mit den so genannten freien Werknutzungen sollen im Sinne der Allgemeinheit gewisse Handlungen vom Ausschließlichkeitsrecht des Urhebers ausgenommen werden. Hierbei ist zu bedenken, dass das exklusive Recht des Urhebers zur Sicherung seiner dem Werk inhärenten Vermögenswerte dient. Jede Einschränkung mindert somit seine „Rendite aufs Werk“ [Noll].

2.6.9.1 Die Vervielfältigung zum eigenen und zum privaten Gebrauch

Sinn der freien Werknutzung zum eigenen bzw privaten Gebrauch, einer der zweifellos wichtigsten oder zumindest derzeit am meisten diskutierten aller freien Werknutzungen, ist es, einen Vervielfältigungsakt, der sich in der Privatsphäre abspielt, vom Recht des Urhebers freizustellen [Dillenz]. Das Gesetz gibt dabei

relativ enge Schranken vor, innerhalb dessen eine Vervielfältigung nicht gegen den urheberrechtlichen Schutz verstößt und stellt verschiedene Einzelfälle hervor.

Die entsprechende Gesetzesstelle wurde durch die Umsetzung der Info-Richtlinie adaptiert. Nun unterscheidet das Gesetz zwischen dem eigenen und dem privaten Gebrauch und differenziert zwischen dem Papier oder einem ähnlichen Träger einerseits und anderen Trägern andererseits bzw als dritte Kategorie in gewissen Fällen den analogen Trägern.

Der Begriff des eigenen Gebrauchs ist der Info-Richtlinie fremd und entstammt der alten, vor der Novelle geltenden Fassung des UrhG. Ein solcher liegt jedenfalls dann nicht vor, wenn die Vervielfältigung zum Zwecke der Zugänglichmachung der Kopie der Öffentlichkeit vorgenommen wird. Nicht gefordert ist allerdings dabei der persönliche Gebrauch. Dementsprechend darf das Vervielfältigungsstück auch weitergegeben werden, solang dies innerhalb der Privatsphäre bleibt und nicht an die Öffentlichkeit erfolgt bzw kann der Zweck auch beruflichen Zwecken des Vervielfältigers dienen.

Gemäß der nun herrschenden Rechtslage darf jedermann Vervielfältigungen zum eigenen Gebrauch auf Papier oder einem ähnlichen Träger zum eigenen Gebrauch herstellen, auf sonstigen Trägern allerdings nur für Zwecke der nicht-kommerziellen Forschung.

Der private Gebrauch ist dabei als Unterfall des eigenen Gebrauchs anzusehen, soweit es natürliche Personen betrifft [Thiele]. Auch dürfen mit einem Vervielfältigungsstück weder unmittelbar noch mittelbar kommerzielle Zwecke verfolgt werden.

Interessanterweise erlaubt das Gesetz in § 42 a nicht nur die Vervielfältigung zum eigenen Gebrauch, sondern auch die Vervielfältigung zum eigenen Gebrauch eines anderen, sofern dies auf Bestellung und unentgeltlich erfolgt. Eine entgeltliche Vervielfältigung ist nur dann zulässig, wenn die Vervielfältigung mit Hilfe reprografischer oder ähnlicher Verfahren vorgenommen wird, oder ein Werk der Literatur oder Tonkunst durch Abschreiben, also mit der Hand oder einer ähnlichen arbeitsaufwendigen Vervielfältigungsmethode vervielfältigt wird oder im Rahmen einer Medienbeobachtung, also der Berichterstattung über Tagesereignisse erfolgt.

Weiters dürfen Schulen und Universitäten für Zwecke des Unterrichts bzw der Lehre in dem durch diese Zwecke gerechtfertigten Umfang Vervielfältigungsstücke in der für eine Schulklasse bzw Lehrveranstaltung erforderlichen Anzahl herstellen und verbreiten. Ausgenommen von diesem Recht der Schulen und Hochschulen sind verständlicherweise solche Werke, die gerade für den Schul- bzw Unterrichtsgebrauch geschaffen wurden, also nach ihrer Beschaffenheit und Bezeichnung dafür bestimmt sind.

Ein weitere Ausnahme besteht zugunsten von Sammlungen, also Bibliotheken oder Museen, die einerseits jeweils ein Vervielfältigungsstück von eigenen Werkstücken sozusagen als Sicherungskopie erstellen sowie auch Vervielfältigungen von veröffentlichten aber nicht erschienen oder vergriffenen Werken herstellen dürfen.

Gerade das Recht der Vervielfältigung zum eigenen (privaten) Gebrauch wird von manchen als Grundlage für die Zulässigkeit der Erstellung von Kopien von im Internet zur Vergütung gestellten Kopien von Musiktiteln im MP3 Format gebraucht. Dies setzt natürlich voraus, dass zunächst an einer MP3 Datei ein Urheberrecht besteht. Nicht jede MP3 Datei ist aber urheberrechtlich geschützt, bei einigen Dateien ist der urheberrechtliche Schutz aufgrund Zeitablaufs vielleicht beendet, oder verzichtet auch der Berechtigte ausdrücklich auf seinen Schutz und stellt die Nutzung jedermann frei. Bei vielen vor allem populären Liedern ist allerdings das Gegenteil der Fall und diese sind tatsächlich geschützt, so dass eine Kopie ohne die ausdrückliche Berechtigung des Rechteinhabers prima facie gegen das Urheberrecht verstoßen wird.

Geht man vom bloßen Wortlaut der Bestimmung des § 42 UrhG aus, so erscheint ein Herunterladen eines Titels aus dem Internet nicht gegen das Gesetz zu verstoßen. Denn jedermann darf von einem Werk einzelne Vervielfältigungsstücke auf Papier zum eigenen Gebrauch bzw darf eine natürliche Person einzelne Vervielfältigungsstücke auf einem anderen Träger zum privaten Gebrauch herstellen. Das Gesetz selbst sieht aber keinen Unterschied vor, ob die Vorlage, von welcher das Vervielfältigungsstück hergestellt wird, selbst rechtmäßig, also in Einhaltung des Urheberrechts hergestellt worden sein muss, oder ob auch eine unrechtmäßig erstellte Vorlage eine taugliche Grundlage einer Vervielfältigung zum eigenen (privaten) Gebrauch sein kann. In Deutschland etwa wurde diese Frage klargestellt und das Gesetz erklärt nunmehr eine Vervielfältigung für unzulässig, wenn die Vorlage offenbar rechtswidrig hergestellt war. Da gerade die auf Musiktauschbörsen angebotenen MP3 Dateien traditionell nicht lizenzierte, also rechtmäßig hergestellte, Kopien sind, ist dieser letzte Fall relevant.

Berücksichtigt man den Zweck der Bestimmung, so erscheint die Möglichkeit, eine rechtmäßige Kopie von einer unrechtmäßigen Vorlage zuzulassen, nicht richtig. Dadurch würden ja gerade die berechtigten Interessen des Rechteinhabers, die eigentlich durch das Urheberrecht geschützt sein sollen, beeinträchtigt.

2.6.9.2 Die Berichterstattung über Tagesereignisse

Zur Berichterstattung über Tagesereignisse sind Eingriffe in das Urheberrecht in einem durch den Informationszweck gerechtfertigten Umfang gestattet.

2.6.9.3 Behinderte Personen

Ebenso ist nun nach Umsetzung der entsprechenden Bestimmung der Info-Richtlinie eine spezifische freie Werknutzung für behinderte Personen eingeführt worden.

Dadurch ist nun die Vervielfältigung für und Verbreitung an behinderte Personen in einer für sie geeigneten Form, soweit ihnen wegen der Behinderung der Zugang zum Werk durch sinnliche Wahrnehmung eines erschienen Werkstücks nicht möglich oder erheblich erschwert ist, zulässig, sofern dies nicht kommerziell erfolgt.

Zu betonen ist, dass diese freie Nutzung allerdings vergütungspflichtig ist. Die angemessene Vergütung ist von den Verwertungsgesellschaften einzuheben.

2.6.9.4 Die freie Werknutzung an Werken der Literatur

Neben den genannten Rechten bestehen freie Werknutzungen an Werken der Literatur. Diese stehen im Zusammenhang mit Reden in öffentlichen Angelegenheiten, Aufsätzen in Zeitungen oder Zeitschriften, der Erstellung von Sammelwerken oder Eingliederung in Werke zum Schulgebrauch sowie dem so genannten Zitatrecht, wenn einzelne Stellen eines veröffentlichen Sprachwerks angeführt werden, sowie mit bestimmten öffentlichen Vorträgen.

2.6.9.5 Die freie Werknutzung an Werken der Tonkunst

Diese Rechte bestehen ähnlich den Rechten für Literaturwerke für Sammlungen oder Schulgebrauch, bestimmte öffentliche Aufführungen, etwa Gratisveranstaltungen oder Brauchtumsmusik.

2.6.9.6 Ein Recht auf freie Werknutzung?

Diese freien Werknutzungsrechte stellen aber meines Erachtens kein Recht des „Berechtigten" dar, sondern lediglich Ausnahmen zum gegenüberstehenden dem Urheber eingeräumten ausschließlichen Recht. Mit anderen Worten der Urheber kann sein Verwertungsrecht im Anwendungsbereich der freien Werknutzungen nicht geltend machen bzw dem Nutzer nicht entgegenhalten. Der Nutzer darf andererseits aber vom Urheber nicht verlangen, diese freien Werknutzungshandlungen auch durchführen zu dürfen. Dies ergibt sich meines Erachtens aus dem Charakter dieser Bestimmungen als Ausnahmen, was insbesondere im Wortlaut „jedermann darf" bzw „jede natürliche Person darf …" ergibt.

Auch die Info-Richtlinie sieht in ihrem Text ausdrücklich die Möglichkeit vor „Mitgliedsstaaten können in den folgenden Fällen Ausnahmen oder Beschränkungen in Bezug auf das in Artikel 2 [der Richtlinie] vorgesehene Vervielfältigungsrecht vorsehen" (Artikel 5 Abs 2). Dazu normiert Abs 5 des Artikels 5 der Info-Richtlinie, dass die genannten Ausnahmen und Beschränkungen nur in jenen Sonderfällen angewandt werden dürfen, in denen die normale Verwertung des Werkes nicht beeinträchtigt wird und die berechtigten Interessen des Rechteinhabers nicht ungebührlich verletzt werden.

2.6.10 Die Schutzfristen

Die genannten Rechte werden durch das UrhG allerdings nicht für immer und ewig eingeräumt, sondern in Einklang mit internationalem Gebrauch nur für einen bestimmten, wenn auch durchaus beträchtlichen Zeitraum.

So endet das Urheberrecht siebzig Jahre nach dem Tod des Urhebers, bzw dem letzten Urheber, sofern das Werk von mehreren geschaffen wurde.

2.6.11 Die technischen Schutzmaßnahmen

Der österreichische Gesetzgeber hat die Vorgaben auf internationaler und insbesondere europarechtlicher Ebene in § 90 c UrhG umgesetzt. Darin heißt es, dass der Inhaber eines Ausschließungsrechtes, der sich wirksamer technischer Maßnahmen bedient, um eine Verletzung dieses Rechtes zu verhindern oder einzuschränken, einen Anspruch auf Unterlassung und Beseitigung hat, wenn diese Maßnahmen durch eine Person umgangen werden.

Hierfür muss ein wesentliches Handeln bzw ein Handeln, dem die Umstände einer solchen Umgehung bekannt sein mussten, vorliegen. Tatbestandsmäßig ist es auch, wenn Umgehungsmittel hergestellt, verbreitet, verkauft, vermietet und zu kommerziellen Zwecken besessen werden oder für den Verkauf oder die Vermietung von solchen Umgehungsmitteln geworben wird, oder Dienstleistungen zur Umgehung erbracht werden.

Wesentlich ist für diesen Rechtsanspruch, dass die gewählten Maßnahmen „wirksam" sind. Als wirksame technische Maßnahmen sind dabei neutral alle Technologien, Vorrichtungen und Bestandteile zu verstehen, die im normalen Betrieb dazu bestimmt sind, eben diese Rechtsverletzungen zu verhindern und einzuschränken und die Erreichung dieses Schutzziels auch sicher zu stellen. Demgegenüber sind etwa vertragliche Regelungen, wie eben Nutzungsbeschränkungen in Softwarelizenzen nicht darunter aufzufassen [Eustacchio]. Auch ist nicht verlangt, dass ein vollständiger Schutz gewährleistet wird. Würde diese Anforderung gestellt, so wäre ein Verbot des Umgehens sinnlos, da es definitionsgemäß nicht erfolgen kann. Mit anderen Worten ist nicht durch das erfolgte Umgehen dargetan, dass die technische Maßnahme gar nicht „wirksam" war. Relevant ist hier wohl der Durchschnittsnutzer [Eustacchio].

Das Gesetz sieht dabei diese Voraussetzungen nur als erfüllt an, wenn hierdurch eine Zugangskontrolle oder ein Schutzmechanismus wie Verschlüsselung, Verzerrung oder sonstige Umwandlung des Werks, oder ein anderer Mechanismus zur Kontrolle der Vervielfältigung erfolgt. Das Gesetz schließt diese Rechte allerdings an Computerprogrammen aus.

Der Begriff „umgehen" ist hierbei sehr weit gefasst und muss technologieneutral verstanden werden. Daher dürfte jegliche Handlung erfasst sein, die letztlich den Schutzmechanismus aushebelt, egal ob dabei der Eingriff in das DRM System direkt erfolgt oder etwa Abläufe auf der Ebene des Betriebssystems ausgespäht werden, um somit ungesichert auf den eigentlichen digitalen Inhalt zuzugreifen.

Parallel normiert nun § 90 d UrhG, dass ein Anspruch auf Unterlassung und Beseitigung besteht, wenn Kennzeichen verwendet werden und diese entfernt oder geändert werden oder nach Entfernung oder Änderung Vervielfältigungsstücke verbreitet und zur Verbreitung eingeführt oder für eine Sendung öffentliche Wiedergabe oder öffentliche Zurverfügungstellung verwendet werden. Als Kennzeichnung sind dabei Angaben zu verstehen, die in elektronischer Form festgehalten, mit dem Vervielfältigungsstück des Werks verbunden sind und entweder eine Bezeichnung des Werks des Urhebers oder jedes anderen

Rechteinhabers enthalten oder die Modalitäten und Bedingungen für die Nutzung des Werks festlegen.

§ 91 UrhG stellt Zuwiderhandeln gegen diese Schutzmaßnahmen unter eine Strafdrohung von bis zu sechs Monaten.

Kritiker sehen im Schutz der technischen Schutzmaßnahmen eine neue Qualität des Urheberrechts für digitale Inhalte. Denn technische Schutzmaßnahmen schützen jeglichen digitalen Inhalt ohne Rücksicht darauf, ob der Inhalt überhaupt entsprechenden urheberrechtlichen Schutz genießt oder dieser vielleicht bereits abgelaufen ist. Denn die technischen Schutzmaßnahmen sind in der Lage, nicht nur rechtswidrige Verwertungshandlungen zu verhindern, sondern auch Verwertungshandlungen, die als freie Werknutzungen zulässig sind. Fraglich bleibt dabei, ob die Umgehung von technologischen Maßnahmen in einem Bereich, der nicht mehr von den Rechten des Urhebers erfasst ist, auch unter die Bestimmung des Verbots fällt. Auf der Grundlage, dass die technologische Schutzmaßnahme den Autor gerade in seinen Rechten schützen soll, wurde das Argument angebracht, dass zu einem Zweck, der nicht davon erfasst ist, eine Umgehung zulässig sein könnte [WIPO]. Es wird als Voraussetzung für den Schutz der technischen Maßnahmen angesehen, dass damit ein urheberrechtlich geschütztes Werk mit technischen Mitteln geschützt wird. Daraus müsste geschlossen werden, dass die Umgehung von Schutzmaßnahmen, welche ein Werk umfassen, das nicht diesen urheberrechtlichen Schutz genießt, nicht Gegenstand des Verbots sind. Als Zwischenfall kommt in Betracht, dass ein Werk geschützt wird, das teilweise auf urheberrechtlich geschütztes Material und sich teilweise auf freie Inhalte bezieht. Sofern hier, wie manche Autoren behaupten, der Schutz der technischen Maßnahmen auf das gesamte Produkt auszudehnen ist [Arlt], so erscheint dies fragwürdig. Damit könnte der Hersteller durch Kopplung eines nicht dem Urheberrechtsschutz unterliegenden Werkes mit einem urheberrechtlich geschützten Teil, die den ihm vom Gesetz eigentlich zukommenden Schutz erheblich ausweiten.

Der österreichische Gesetzgeber hatte erkannt, dass technische Schutzmaßnahmen in einem Spannungsverhältnis zu den zulässigen freien Werknutzungen stehen. Es wurde darauf verwiesen, dass erwartet wird, dass Rechtsinhaber, die technische Schutzmaßnahmen anwenden, freiwillige Maßnahmen ergreifen, um den Begünstigten dieser Ausnahme die Mittel zur Nutzung der betreffenden Ausnahme zur Verfügung zu stellen, soweit der betreffende Begünstigte rechtmäßig Zugang zu dem geschützten Werk oder Schutzgegenstand hat. Auch wurden aus Sicht des Gesetzgebers zum Zeitpunkt der Novelle des UrhG nur in relativ eingeschränktem Umfang technische Maßnahmen eingesetzt, durch die die Inanspruchnahme der freien Werknutzungen unmöglich gemacht wird. Aus diesen Gründen war damals offenbar kein Handlungsbedarf, Ausnahmen für den Einsatz von technischen Schutzmaßnahmen vorzusehen und der Gesetzgeber hat sich auf freiwillige Maßnahmen verlassen. Im Regierungsprogramm für die XXIII. Gesetzgebungsperiode hat die Regierung ihre Ansicht geändert und legt nun dar, dass eine Aufgabenstellung für die nahe Zukunft „im Urheberrecht die Klärung des Verhältnisses ‚freie Werknutzung – technische Schutzmaßnahmen' im Bereich der digitalen Rechte im Vordergrund steht. Das Recht auf Privatkopie digitaler

Datenträger soll auch durchgesetzt werden. Ferner soll es zu einem Ausbau der Rechte im nichtgewerblichen Umgang mit digitalen Inhalten kommen, ohne dadurch das gesetzliche Schutzniveau des Urheberrechts für die Kunstschaffenden abzubauen."

Damit ist ein ausdrückliches Recht, das dem Begünstigten ein durchsetzbares Recht auf Zurverfügungstellung eines Werkes ohne entsprechende technische Maßnahme für berechtigte Zwecke, welche um Urheberrecht und damit ausschließliches Recht des Berechtigten ausgenommen sind, nicht gegeben. Daraus ergibt sich aber, dass die wirksamen technischen Schutzmaßnahmen aber auch dann nicht umgangen werden dürfen – sofern sie vom Rechtsinhaber angewendet werden und tatsächlich ein urheberrechtlich geschütztes Werk betreffen – wenn es in Ausübung einer freien Werknutzung geschieht. Damit werden bestimmte Handlungen, die das Urheberrecht sonst im öffentlichen Interesse privilegiert, insbesondere das Zitat, unmöglich und können durch „technische Schutzmaßnahmen" wirksam unterbunden werden. Damit wird auch die Schaffung neuer Werke erschwert [Gehring]. Es wird auch das Urheberrecht, das klassischerweise am Werkstück hängt, erweitert und bisher zulässige Handlungen, etwa die Weiterverbreitung verwehrt. So wird einem Sekundär- und Tertiärmarkt (Antiquariate, Flohmärkte usw) der Nachschub entzogen [Gehring].

Daran knüpft die Frage an, ob eine identische Kopie, die also den Kopierschutz auch für das Vervielfältigungsstück aufrecht lässt, eine Umgehung des technischen Schutzes ist [Arlt].

Nach dem Sinn der Schutzvorschriften kann dies wohl nicht vorliegen. Denn Hintergrund der Schutzvorschriften ist gerade den Rechteinhaber vor unberechtigten Vervielfältigungen zu schützen. Mit der Kopie sind die Rechte, sofern tatsächlich die technische Schutzmaßnahme „mitkopiert" wurde, geschützt. Auch das Vervielfältigungsstück kann nicht ungerechtfertigterweise eingesetzt werden.

Anders als in Österreich hat sich der deutsche Gesetzgeber dazu entschlossen, die Ausnahmen und Beschränkungen des urheberrechtlichen Schutzes auch im Zusammenhang mit den technischen Maßnahmen genauer festzulegen. So ist der Rechteinhaber dieser Maßnahmen verpflichtet, einem Begünstigten, soweit dieser rechtlichen Zugang zu dem Werk oder Schutzgegenstand hat, die notwendigen Mitteln zur Verfügung zu stellen, um von diesen Bestimmungen in dem erforderlichen Ausmaß Gebrauch machen zu können (§ 95 b Abs 1 dUrhG). Dies geht soweit, dass Vereinbarungen zum Ausschluss dieser Verpflichtungen unwirksam sind. Der Begünstigte hat auch gemäß Abs 2 dieser Regelung ein Recht, von Rechteinhaber die zur Verwirklichung seiner Befugnis benötigten Mittel herauszuverlangen. Dieser Anspruch ist verschuldensunabhängig [Arlt].

Interessant ist, dass mangels Ausnahmetatbeständen eine Umgehung der technischen Schutzmaßnahmen auch dann verboten ist, wenn das damit bezweckte Verhalten von einer Urheberrechtsschranke erfasst ist– also ein erlaubtes Ziel verfolgt wird. Es gilt der strikte Vorrang des Umgehungsverbots bzw der absolute Schutz der Integrität eingesetzter DRM Systeme [Arlt].

Zu erwähnen ist, dass der deutsche Gesetzgeber eine Ausnahme zu den Schutzmaßnahmen im Hinblick auf Aufgaben und Befugnisse öffentlich-rechtlicher Stellen zum Zweck des Schutzes der öffentlichen Sicherheit und der Strafrechtspflege eingefügt hat. Für diese Zwecke darf somit offenbar eine Umgehung der technischen Schutzmaßnahmen durchgeführt werden.

Einen ähnlichen Schutz bildet die Richtlinie 98/84/EG des Europäischen Parlaments und des Rates vom 20. November 1998 über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten (Zugangskontrollrichtlinie). Über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten sehen in ähnlicher Weise für die dort normierten geschützten Dienste verbotene Handlungen vor. Diese umfasst (Artikel 4) die Herstellung, Vertrieb, Verkauf, Vermietung oder Besitz illegaler Vorrichtungen sowie die Installierung, Wartung und Austausch dieser illegalen Vorrichtungen jeweils zu gewerblichen Zwecken sowie den Einsatz der kommerziellen Kommunikation zur Förderung des Inverkehrbringens dieser illegalen Vorrichtungen. Als illegale Vorrichtungen sind definiert jedes Gerät oder Computerprogramm, das dazu bestimmt oder entsprechend angepasst ist, um den Zugang zu einem geschützten Dienst in verständlicher Form ohne Erlaubnis des Diensteanbieters zu ermöglichen (Artikel 2 lit d). Geschützte Dienste sind sowohl Fernsendungen als auch Radiosendungen als auch Dienste der Informationsgesellschaft im Sinne, dieser Schutz überschneidet sich mit dem urheberrechtlichen Rechtsschutz. Anders als die Schutznormen im Bereich des Urheberrechts ist für den Schutz nach dem Zugangskontrollgesetz, welches in Österreich die Zugangskontrollrichtlinie umgesetzt hat, nicht von einer speziellen Qualität, wie eben der urheberrechtliche Werksanspruch Voraussetzung. Da somit der Schutz nach dem Zugangskontrollgesetz allfassend ist, scheint es denkbar, auf diese Weise die urheberrechtlichen Beschränkungen ins Leere laufen zu lassen. Durch ein vorgeschaltetes Zugangskontrollrecht könnten die Beschränkungen hinsichtlich der technischen Maßnahmen zur Benutzungskontrolle im Urheberrechtsbereich im Ergebnis umgangen werden [Arlt]. Letztlich ist wohl im Rahmen eines sinnvollen Zusammenspiels dieser beiden Rechtsvorschriften die urheberrechtliche Zugangskontrolle als speziellere Norm anzusehen. Damit hat sie im Rahmen ihres Anwendungsbereiches vorrangigen Charakter und der Zugangskontrolle nach dem Zugangskontrollgesetz (der Zugangskontrollrichtlinie) hat dort nur subsidiär zur Anwendung zukommen. Mit anderen Worten sofern ein urheberrechtlich geschütztes digitales Werk geschützt wird, sind allein und ausschließlich die Regelungen des Urheberrechtes maßgeblich. Sofern diese Schutznormen mangels Werkqualität nicht zur Anwendung gelangen, gelten die Vorschriften des Zugangskontrollgesetzes [Arlt].

2.6.12 Vertraglicher Schutz

Es soll auch nicht unerwähnt bleiben, dass neben dem gesetzlichen, urheberrechtlichen Schutz natürlich aus rechtlicher Sicht auch der Schutz des Werkes durch vertragliche Vereinbarung denkbar ist und in der Regel auch zum Einsatz kommt. Je nach Ausgestaltung kann dieses Instrument einen noch wirksameren Schutz bieten. Soweit dem nicht die gesetzlichen Bestimmungen entgegenstehen,

kann der Schöpfer die Verwendung seines Werks vertraglich regeln, typischerweise durch einen so genannten Lizenzvertrag. Dieser Vertrag enthält die Regelungen auf welche Weise und in welchem Umfang ein Werk benutzt werden darf. Der Schöpfer kann damit ganz spezifisch, für den Einzelfall oder bei Verwendung von standardisierten Verträgen auch für eine Reihe von Fällen, festlegen, ob etwa das Werk vervielfältigt und/oder weitergegeben werden darf.

Dieser vertragliche Schutz erstreckt sich aber immer nur auf den jeweiligen unmittelbaren Vertragspartner. Erfolgt einmal eine – berechtigte oder auch unberechtigte – Weitergabe, so wird nur in speziellen Konstellationen der vertragliche Schutz ausgeweitet. In der Regel wird wohl davon auszugehen sein, dass keine vertragliche Grundlage zwischen dem dritten Nutzer und dem Schöpfer mehr besteht. Damit bestehen aber in diesem Verhältnis eben keine spezifischen Regelungen mehr. In diesem Fall ist der Schöpfer somit ausschließlich auf die urheberrechtlichen Rechte verwiesen. Genau aus diesem Grund kann eine vertragliche Vereinbarung nur mit flankierenden technischen Maßnahmen einen auch im Falle der Weitergabe, etwa der Superdistribution, rechtlichen Schutz bieten.

2.7. Copyright in den USA

2.7.1 Grundsätzliches

Das US-amerikanische Urheberrecht – „copyright" – unterliegt einem etwas anderen System als das österreichische Urheberrecht.

Auch in den USA entsteht das copyright mit dem Erstellen eines Werks. Das oft angebrachte Symbol © weist zwar auf einen Schutz hin, dieser besteht aber unabhängig vom Hinweis, bzw nutzt der Hinweis auch nicht, wenn das Werk selbst nicht schutzfähig sein sollte. Ähnlich wie auch in Österreich, knüpfen an die einzelnen Kategorien von Werken unterschiedliche Regeln an. Auf die einzelnen Kategorien, sowie Grundsätze, wann ein Werk schutzfähig ist, kann hier nicht eingegangen werden.

2.7.2 Die Rechtsgrundlagen

In der Rechtsordnung der USA ist das dortige copyright in Abschnitt 17 des United State Codes eingearbeitet. Dies ist die wesentliche rechtliche Grundlage des copyright, allerdings ist das amerikanische copyright stark von einzelnen Urteilen und den darin ersichtlichen Grundaussagen geprägt.

Gemäß § 106 des United State Codes („USC") werden dem Inhaber des copyright exklusive Rechte zugestanden. Diese Rechte umfassen das Recht

- zur Reproduktion des Werks;
- zur Herstellung von Bearbeitungen und sonstiger Derivative des Werks;

- zur Verteilung von Kopien oder Tonaufnahmen an die Öffentlichkeit einschließlich des Rechts zum Verkauf oder andere Übertragung der Eigentumsrechte des Vermietens und Verleihens;

- zur Aufführung;

- zur öffentlichen Wiedergabe und insbesondere;

- für Tonaufnahmen das Werk im Wege einer digitalen Übermittlung öffentlich abzuspielen.

Daneben kennt das US-Recht auch gewisse Autorenrechte („moral rights"), die neben dem exklusiven copyright bestehen, nämlich das Recht:

- die Autorenschaft für ein gewisses Werk in Anspruch zu nehmen ;

- nicht als Autor eines Werks, das nicht von einem erstellt wurde, genannt zu werden;

- als Autor genannt zu werden, wenn das Werk in einer Weise bearbeitet oder verstümmelt wurde, die dem Autor nicht zur Ehre gereichen würde.

Die genannten Rechte entsprechen den österreichischen Rechten in mancher Hinsicht, wenn auch im Einzelfall sicherlich Unterschiede bestehen.

2.7.3 Fair use

Auch das US-Recht kennt Ausnahmen zum Recht des Urhebers. Die dem Inhaber des copyright eingeräumten exklusiven Rechte erfahren in § 107 USC einige Einschränkungen.

In diesem Zusammenhang ist insbesondere das Prinzip des *fair use* zu nennen. Soweit die Verwendung eines durch copyright geschützten Materials im Rahmen des fair use erfolgt, stellt es keine Verletzung dar.

§ 107 USC implementiert hierbei einen 4-fachen Test mit folgenden Elementen:

(i) der Zweck und Charakter der Nutzung einschließlich der Frage, ob es zu einer kommerziellen oder nicht kommerziellen Nutzung kommt;

(ii) die Qualität des Werks - hierbei wird berücksichtigt, welchen kreativen Grad das Werk besitzt;

(iii) der Umfang und das Ausmaß, in welchem das Werk benutzt wird; und

(iv) die Auswirkungen, die diese Nutzung auf eine potenzielle Verwertung bzw wirtschaftliche Nutzung oder den Wert des geschützten Werks hat.

Nicht alle diese Faktoren werden dabei aber in jedem Fall in gleicher Weise und mit dem gleichen Gewicht berücksichtigt. Ein wesentlicher Aspekt ist dabei der Zweck

der Nutzung. Das Gesetz selbst listet dabei als mögliche Zwecke Kritik, Kommentar, Berichterstattung, Unterricht und Lehre oder Forschung. Aber auch andere Aspekte wie Parodie sind anzuerkennen [Office]. Als möglicherweise wichtigster Faktor ist in der Rechtsprechung die wirtschaftliche Implikation der Nutzung genannt worden. Eine wirtschaftliche Beeinträchtigung soll daher nur selten als im Rahmen des fair use akzeptabel gelten. Der Hintergrund dafür ist, dass das copyright dem Inhaber auch die wirtschaftlichen Verwertungsrechte zugesteht. Diese Vorrangstellung der Nutzung und des Zwecks des Gebrauchs wurde allerdings in anderen Urteilen auch abgelehnt [Office].

2.7.4 Die technischen Schutzmaßnahmen

Mit dem Digital Millennium Copyright Act of 1998 („DMCA“) wurden die Vorgaben des WIPO Treaty über die technischen Schutzmaßnahmen umgesetzt. Nunmehr normiert § 1201 USC das Verbot der Umgehung effektiver technologischer Zugangskonrollmechanismen. Dabei wird sowohl der unzulässige Zugang zu einem geschützten Werk als auch das unauthorisierte Kopieren geschützt [Office]. Wie der WIPO Treaty vorsieht, werden auch die Herstellung und der Vertrieb von Geräten oder Technologien, welche Zugangsbeschränkungen umgehen, verboten. Dabei sind neben Geräten und Technologien, die auf die Umgehung abzielen, auch solche erfasst, die neben der Umgehung keinen weiteren nennenswerten wirtschaftlichen Zweck erfüllen oder für die Umgehung angepriesen werden.

Zu diesem Schutz gibt es aber auch eine Reihe von Ausnahmen. So wird zunächst ausdrücklich festgehalten, dass diese Bestimmungen die sonst statuierten Rechte und Ausnahmen, insbesondere die auf fair use, nicht einschränken. Zudem zählt das Gesetz eine Reihe von Fällen auf, in denen keine verbotene Umgehung stattfindet:

- Büchereien, Archiven und sonstigen Einrichtungen für Zwecke der Erziehung und Unterricht wird gestattet, technologische Maßnahmen zu umgehen, um festzustellen, ob sie dieses Werk anschaffen wollen.

- Dem rechtmäßigen Nutzer eines Computerprogramms wird gestattet, im Ausmaß jener Rechte, die ihm im Zusammenhang mit reverse engineering, also dem Vorgang der Rückführung des Programms auf seine Ideen und Grundlagen, eingeräumt werden, auch Schutzmaßnahmen zu umgehen.

- Schutzmaßnahmen dürfen umgangen werden, um die Verschlüsselungstechnik zu erforschen und deren allfällige Schwachstellen aufzudecken.

- Sofern die Schutzmaßnahme oder das damit geschützte Werk persönliche Daten von natürlichen Personen über deren Online-Verhalten sammeln, ist eine Umgehung zulässig.

- Zum Zwecke der Durchführung von Sicherheitstest für Computer und Computer-Systeme ist ebenfalls eine Umgehung zulässig

- Ganz allgemein ist für die Zwecke der staatlichen Rechtsdurchsetzung eine Ausnahme geschaffen.

Die Vorgabe des WIPO Treaty, Rechteinformationen zu schützen, ist in § 1202 USC umgesetzt worden. Somit ist es verboten, falsche Information („Copyright Mangement Information“) wissentlich einzubinden oder solche zu verbreiten sowie Rechteinformation ohne Einwilligung des Berechtigten zu entfernen oder Werke, an denen die Rechteinformation unzulässigerweise entfernt wurde, zu vertreiben.

Wiederum besteht eine Ausnahme für staatliche Behörden.

Ein Vorschlag in den USA möchte aller Hersteller digitale Mediengeräte verpflichten, geprüfte und zugelassene technische Schutzmaßnahmen in diesen zu implementieren. Damit darf kein digitales Mediengerät verwendet, beschaffen oder veräußert werden, ohne dem entsprechenden Schutzstandard zu entsprechen. Dabei sind solche Geräte, jegliche Hardware oder Software, erfasst, die urheberrechtlich geschützte Werke wiedergeben oder darstellen können [Fallenböck04].

Es wird von einigen Autoren vorgebracht, dass durch die Zulassung, ja Unterstützung von technischen Schutzmaßnahmen nunmehr ein Übergewicht des Schutzes des Rechteinhabers gegenüber den berechtigten Interessen der Begünstigten nach der *fair use* Doktrin erreicht wird. Die technische Schutzmaßnahme kann auch für zulässige Zwecke nur durch Umgehung außer Kraft gesetzt werden. Allerdings ist eine solche Umgehung prinzipiell nicht gestattet. In Abschnitt 1201 (b) DMCA wird allerdings eine Ausnahme vom Verbot der Umgehung von Kopierschutzmaßnahmen gerade für diesen Zweck geschaffen. Allerdings ist diese Ausnahme möglicherweise nicht weitgehend genug [Fallenböck04]. Einerseits ist nicht absehbar, wie in entsprechenden Gerichtsverfahren diese Ausnahmen tatsächlich angewandt werden wird. Andererseits muss für die Umgehung, auch wenn sie zulässig ist, eine entsprechende Expertise des Nutzers vorhanden sein bzw er in der Lage sei, entsprechende umgehungsfähige Geräte zu erhalten. Aber gerade dort scheitert das System, weil der Vertrieb dieser Geräte dennoch illegal ist. Damit ist tatsächlich der Anwendungsbereich der *fair use* Doktrin eingegrenzt. Dies ergibt sich auch aus dem Umstand, dass die Abgrenzung, ob *fair use* vorliegt oder nicht, sehr Einzelfall bezogen ist und daher im Allgemeinen schwierig zu ziehen sein wird. Damit ist es auch technisch schwierig bis wahrscheinlich fast unmöglich entsprechende technische Aufnahmen in die Schutztechnologie zu implementieren. Damit haben nur mehr Hacker die entsprechenden Möglichkeiten die Privilegien, die durch die *fair use* Doktrin eingeräumt werden, zu nutzen.

Daran knüpft sich gerade die Frage ob *fair use* ein Rechts- oder bloß eine Ausnahme ist. Einige Autoren sehen sehr wohl ein ausdrückliches Recht, das entsprechend durch gesetzliche Maßnahmen zu schützen ist. Sofern dies nicht der Fall wäre, gäbe es eine inhärente Ausnahme um Schutzmaßnahmen zu entgehen, soweit sie eben den *fair use* nicht zulassen.

Als Gegenposition dazu steht ein Urteil eines amerikanischen Gerichtes[3], in dem festgehalten wurde, dass der Supreme Court nie *fair use* als unter der Verfassung garantiert angesehen hat. Auf der anderen Seite ist ein Argument dafür, dass kein Recht besteht, dass durch die entsprechenden digitalen Technologien mehr an Content zu einem geringeren Preis den Nutzern zur Verfügung gestellt werden kann. Dementsprechend hat daher das Gericht im genannten Fall Cally auch festgehalten, dass die *fair use* Doktrin nicht darauf abstellt, dass die Vervielfältigung, sofern sie überhaupt zulässig ist, mit der optimalen Methode oder im identischen Format des Originals erfolgt. Eine DVD kann daher kopiert werden, wenn etwa die Wiedergabe vom Fernseher mittels einer Kamera dupliziert wird. Als Extremposition wurde auch vertreten, dass *fair use* nur deswegen gestattet wird, als es wirtschaftlich nicht sinnvoll wäre diese Beeinträchtigungen zu verfolgen. Sofern allerdings die ineffiziente Technologie ersetzt werden kann, fällt auch *fair use* weg.

Sowohl dem amerikanischen als auch dem europäischen Recht ist eigen, dass es nicht nur wie etwa der WIPO *Treaty* die direkte Umgehung von technologischen Maßnahmen erfasst, sondern auch Vorbereitungsschritte wie etwa die Herstellung und Verteilung von umgehungsfähigen Geräten verbietet. Wohl richtigerweise sehen die beiden Vorschriften den besseren Hebel dort an, wo nicht nur die Umgehung selbst womöglich im privaten Rahmen und für den Rechteinhaber feststellbar erfolgt, sondern bereits dort, wo entsprechende Hilfsmittel zur Umgehung herstellt werden.

Ebenso vor demselben Hintergrund steht die rechtliche Prämisse auch bereits jene Helfer jede Hilfstätigkeit zu regulieren, welche zwischen dem Rechteinhaber und dem Nutzer stehen. Diese Mittelsmänner werden daher nunmehr stärker in die Verantwortung genommen. Dementsprechend implementiert Artikel 512 des *US-Copyright Act* auf der Grundlage des DMCA die Verpflichtung eines Internetproviders nach Benachrichtigung einer potentiellen Urheberrechtverletzung den Zugang zu diesen Materialien zu verhindern. Folgt er dieser „notice and takedown procedure" nicht, so bleibt er weiter haftbar. Als Gegenstück dazu gibt es genauso Vorschriften, die den Provider verpflichten, nach Einspruch des Kunden, der das Material eingestellt hat, den Zugang wieder zu ermöglichen.

Ähnlich regelt Artikel 14 der so genannten E-Commerce Richtlinie[4] eine Ausnahme von einer sonst allenfalls bestehenden Haftung eines Internet Service Providers, wenn er von der unzulässigen Information keine Kenntnis hatte und auch sonst aus den Tatsachen oder Umständen bewusst ist, aus denen die rechtzeitige Tätigkeit oder Information offensichtlich wäre. Auch wird er nicht haftbar, wenn er, sobald er Kenntnis oder Bewusstsein erlangt, er unverzüglich tätig wird, um die Information zu entfernen oder den Zugang zu ihr zu sperren.

Diese Vorschrift wurde in § 16 des österreichischen E-Commerce-Gesetzes implementiert.

[3] Universal City Studios Inc. V. Cally.
[4] bitte genaue Bezeichnung einfügen

2.8. Einige Fallbeispiele

Anhand einiger ausgewählter, auch durch entsprechende Prominenz in der Berichterstattung von tagesaktuellen Medien bekannt gewordener Fälle soll dargestellt werden, dass der Schutz von digitalen Inhalten tatsächlich mit Mitteln des Urheberrechts erfolgt.

2.8.1 Napster

Napster steht wohl als Synonym für eine Revolution der Verbreitung von Musik und soll hier als Beispiel für die Relevanz von Urheberrechten im Internet als auch technischen Aspekten des Schutzes von wertvollen digitalen Inhalten dienen.

Napster war eine Entwicklung eines Studenten, Shawn Fanning. Er hat mit Napster die erste weltweite Musiktauschbörse entwickelt. Der Austausch von Musikstücken wurde dabei unentgeltlich bewerkstelligt. Ermöglicht haben diesen rasanten Aufstieg zwei Technologien, einerseits MP3, andererseits der Einsatz von Peer-to-Peer Verbindungen.

2.8.1.1 MP3

In den Anfangszeiten der Digitalisierung von Musik war die Audio CD das wesentliche Medium zur Verbreitung von digitalisierten Klängen. Nach dem Format einer Audio CD werden die Daten unkomprimiert gespeichert. Daneben gab es weitere Entwicklungen, Musik digital zu codieren.

Die aus heutiger Sicht revolutionäre Standard MP3 wurde Ende der 80er und Beginn der 90er Jahre vom Fraunhofer-Institut für Integrierte Schaltungen entwickelt. Es ist Teil der Entwicklung der Moving Picture Experts Group („MPEG"), die sich als von der International Organisation for Standardisation (ISO), das ist eine regierungsunabhängigen Vereinigung einer Vielzahl an nationalen Standardisierungsinstituten und –behörden, gegründete Expertengruppe mit der Standardisierung von digitalen Video- und Audioformaten beschäftigt. MP3 beschreibt dabei den Layer 3 des Audio Teils des Verfahrens.

Ein wesentliches Element von MP3 ist, dass es die Audiodaten komprimiert [Kappes]. Dadurch wird für das Musikstück weniger Speicherplatz benötigt. Allerdings verwendet MP3 ein verlustbehaftetes Modell zur Kompression, somit wird jeder Klang nicht exakt digitalisiert, sondern ein Teil der Information abgeschnitten. Zu erwähnen ist an dieser Stelle, dass auch ein grundsätzlich nicht verlustbehaftetes Verfahren wie jede Digitalisierung eines analogen Signals zu einem Verlust an Information führt, weil die bei der Digitalisierung erreichten Werte einerseits endlich sind, andererseits Zwischenwerte aufgrund der Abtastung nivelliert werden. Dies kann aber unberücksichtigt bleiben, wenn die Abtastrate ausreichend hoch ist. Das Ausmaß der Kompression wird bei MP3 durch die Bitrate angegeben. Diese ist bei der Kodierung der Datei entsprechend einzustellen. Je höher die Bitrate, desto umfangreicher wird die Datei in ihrem Speicherbedarf, auf der anderen Seite ist die Qualität entsprechend „besser". Weiters ist bei MP3 die Bandbreite einstellbar, also die höchste gespeicherte Frequenz. Um die Qualität des

Musikstücks trotz Kompression und Verlust von Information aber nicht zu stark zu beeinträchtigen, bedient sich MP3 eines „Tricks“.

MP3 macht sich zu Nutze, dass das menschliche Gehör Informationen in einem Audio Signal unter Umständen gar nicht wahrnimmt. So werden leise Töne von lauteren Tönen überlagert und werden nicht separat vernommen. Auch kann das menschliche Gehör zwei Töne nicht differenzieren, wenn diese nahe beieinander liegen, also eine sehr ähnliche Frequenz haben. Zudem kann das menschliche Gehör nur Frequenzen bis maximal etwa 22 kHz (in höherem Alter sogar weniger) wahrnehmen. Im gesamten Geräusch sind somit Informationen enthalten, die das menschliche Gehör ohnedies nicht wahrnimmt, damit kann diese Information weggelassen werden, ohne dass dies für den menschlichen Hörer Auswirkungen auf das Hörerlebnis hat. MP3 bearbeitet nun das Audiosignal in einer Weise, die genau diese Hintergrundinformationen ausfiltert, wobei die digitalisierte Aufnahme für den (durchschnittlichen) menschlichen Hörer keinen Unterschied zum analogen Original erkennen lässt.

Aufgrund des Umstands, dass mit MP3 kodierte Dateien relativ klein sind, hat sich dieses System als Standard im Internet durchgesetzt. Insbesondere in den früheren Jahren des Internet waren für private Nutzer nur kleinere Kapazitäten für den download verfügbar, so dass nur eine entsprechend kleine Dateien bequem herunter zu laden waren.

2.8.1.2 Peer-to-Peer

Die Besonderheit einer Peer-to-Peer Verknüpfung besteht darin, dass sie ohne Server, der eine zentrale Verwaltung von Datenbeständen und Serviceleistungen bereitstellt, auskommt. Es handelt sich um eine direkte Verbindung zwischen zwei gleich gestellten („peers“) Computern. Napster war insofern nicht im engsten Sinne ein Peer-to-Peer Systemen, denn es war dennoch und insofern von einem Server abhängig, als dieser die Verwaltung jener Computer sowie die darauf gespeicherten Musiktitel übernahm, die an der Musiktauschbörse teilgenommen haben. Später entwickelte Nachfolgersysteme kamen ohne die zentrale Instanz aus (und waren deshalb noch weniger erkennbar und für jene Personen, die in dieser Tätigkeit einen inkriminierten Tatbestand sehen, aufspürbar und greifbar).

Die Kommunikation erfolgte in der Art, dass der suchende Teilnehmer in der zentralen Verwaltung ein Lied suchen konnte. Nach der Rückmeldung des Servers mit einer Liste der IP Adressen jener Computer, auf denen sich das gesuchte Lied befand, konnte er eine direkte Verbindung mit diesem zum Austausch der Datei aufnehmen, daher die Peer-to-Peer Verbindung. Napster hat auf dem zentralen Server selbst keine Musikdateien gespeichert, verwaltet wurden somit lediglich Zugangsdaten, nämlich Verbindungsdaten zu jenem Computer und Speicherplatz, auf dem ein gewünschter Titel verfügbar ist. Der eigentliche Daten- und Musikaustausch erfolgte ohne Beteiligung von Napster direkt durch die beiden kommunizierenden Computer.

2.8.1.3 Der Kampf der Musikindustrie

Der Musikindustrie war Napster ein Dorn im Auge, da durch die Verbreitung die Gefahr von massiven Einbußen im Umsatz gesehen wurde. Wenn nunmehr jeder eine Kopie seiner CD's mittels Equipment, das jedem quasi im Wohnzimmer zur Verfügung steht, erstellen und verbreiten kann, entgehen entsprechende Einnahmen auf konventionellen Vertriebswegen.

Die Band „Metallica" hat schließlich eigenständig den rechtlichen Weg beschritten und gegen Napster Inc. Klage eingebracht. Dieser Rechtsstreit endete mit einem Vergleich, aufgrund dessen Napster seinen Dienst nach Stücken der Band filtert.

Bereits davor hatte die Recording Industry Association of America (RIAA) die rechtlichen Schritte mehrerer Plattenfirmen konzentriert und deren Steuerung übernommen. In seiner Entscheidung vom 12. Februar 2001, obgleich diese lediglich zu der Frage der Zulässigkeit einer einstweiligen Verfügung, mit der Napster seine Dienstleistung untersagt wurde, ergangen ist mit entsprechend weit reichender Bedeutung, hielt der United States Court of Appeal Napster schuldig, das Urheberrecht an den über seine Dienstleistung verbreiteten Musikstücken verletzt zu haben.[5]

Napster selbst konnte keine direkte Verletzung des Urheberrechts vorgeworfen werden, da es bloß ein Computersystem zur Verfügung gestellt hat, das aber ohne sein weiteres Zutun urheberrechtlich geschütztes Material verbreitete. Für eine solche Tätigkeit besteht nach US-amerikanischer Rechtsansicht keine Haftung. Es wurde aber festgestellt, dass die Nutzer von Napster selbst eine Urheberrechtsverletzung mit dem unbefugten Kopieren von Musikdateien begehen. Deren Verstoß besteht einerseits gegen das Recht auf Verbreitung als auch das Recht auf Vervielfältigung.

Napster wird sodann in diesem Urteil Beihilfe zur Urheberrechtsverletzung vorgeworfen. Voraussetzung für eine solche Verurteilung für Beihilfe ist, dass Napster wusste, oder zumindest wissen musste, dass sein System zu urheberrechtlichen Handlungen verwendet wurde und Napster die eigentlichen Störer dazu veranlasst hat oder zur Urheberrechtsverletzung einen wesentlichen Beitrag geleistet hat. Im Verfahren wurde festgestellt, dass Napster tatsächlich Kenntnis von solchen Verstößen hatte. Auch wurde betont, dass ohne die Verwaltung der Listen durch Napster ein Datenaustausch nicht möglich gewesen wäre.

Da Gericht hat schließlich als Argument herangezogen, dass es Napster sehr wohl möglich sei, die Urheberrechtsverletzungen durch die Benutzer zu kontrollieren und unterbinden. Dies sei durch einen entsprechenden Abgleich der Listen mit einem Verzeichnis urheberrechtlich geschützter Musiktitel durchaus möglich. Das Gericht hat dabei auch ausdrücklich festgehalten, dass Napster ein direktes finanzielles Interesse an den Urheberrechtsverletzungen durch die Nutzer hat.

---

[5] Siehe Summary unter http://www.riaa.com/news/filings/napster.asp.

Napster hat zu seiner Verteidigung vorgebracht, dass nach der Doktrin des „fair use“ die Herstellung von Kopien doch gerechtfertigt gewesen sei und somit im Endeffekt keine Verletzung des Urheberrechts bestanden habe. Diese Argumentation wurde vom Gericht allerdings nicht akzeptiert. Ebenso hat das Gericht die Verteidigungslinie von Napster, dass sein System durchaus auch einen legalen Anwendungsbereich hat und nicht ausschließlich dem Zweck der Urheberrechtsverletzung dient, nicht aufgegriffen. Dabei wurde die Absicht von Napster heran gezogen, die bisherige Musikindustrie zu unterwandern und deren Geschäft zu stören, wenn nicht gar zu zerstören.

Wesentlich ist hervorzuheben, dass nicht prinzipiell das Peer-to-Peer System verboten wurde. Lediglich die spezifische Ausgestaltung und die Hilfestellung durch Napster Inc. selbst wurden in dem konkreten Fall behandelt.

2.8.1.4 Die Folge

Als Konsequenz hat Napster einen entsprechenden Filter installiert, der urheberrechtlich geschütztes Material unterdrücken sollte. Obwohl der Filter, der mit dem Abgleich von Namen und Titeln operierte, zwangsläufig technische Einschränkungen hatte, hatte dies doch einen Rückgang der Nutzer zur Folge und nach einer vergleichsweisen Einigung mit der RIAA und einer Zahlung eines Schadenersatzes wurde der Dienst eingestellt. Nach dem Erwerb von Napster durch den Bertelsmann Konzern bietet Napster nunmehr kostenpflichtige Musik an.

2.8.2 Gnutella, KaZaa

Nach dem Vorbild von Napster haben sich auch andere Musiktauschbörsen entwickelt. Insbesondere auf der technischen Seite haben sich jedoch diese Netze über die Technik von Napster weiterentwickelt. Ein wesentlicher Aspekt bei diesen neuen Entwicklungsstufen war insbesondere, dass sie auf semizentralen oder tatsächlich dezentralisierten Systemen aufgebaut waren oder noch sind.

2.8.2.1 Noch dezentraler: Gnutella

So ist nach dem (vorläufigen) Abschalten von Napster mit Gnutella ein Netzwerk einer dezentralen Tauschbörse entstanden. Das Gnutella-Netzwerk ist eine Weiterentwicklung von Napster. Es handelt sich dabei allerdings nicht um eine spezifische Software, sondern ein Protokoll. Viele verschiedene Programme bauen heute auf diesem Protokoll auf, dessen Funktionsweise sich von Napster unterscheidet. Die einzelnen MP3 Dateien sind entgegen dem Konzept von Napster nicht mehr auf einem zentralen Server gespeichert, sondern befinden sich stets auf der Festplatte der einzelnen Nutzer und können von einem anderen Mitglied der Gemeinde von Tauschinteressierten direkt von diesem Rechner herunter geladen werden.

Während bei Napster der zentrale Server, über den alle Suchanfragen laufen mussten, das Herzstück war, von dessen Existenz das gesamte System abhängig war bzw mit dessen Sperrung das gesamte Netzwerk zum Erliegen kam, ist die Idee hinter Gnutella different. Hier werden die Suchanfragen von Rechner zu Rechner

weitergeleitet. Ein zentraler Server existiert nicht mehr. Um diesen Aspekt Rechnung zu tragen hat sich auch für die Mitglieder von Gnutella die Bezeichnung als Servants eingebürgert, dieser Begriff ist eine Mischung aus den Worten „Server“ und „Client“.

Wie funktioniert nun Gnutella: Bei jedem Start versucht die Software zunächst, eine Verbindung zu einem Server auf zu bauen. Dieser Server listet jene Adressen jener Gnutella-Servants, die ebenfalls gerade eine gültige Verbindung zu Gnutella aufgebaut haben. Für den Fall, dass eine Verbindung zu diesem Server, aus welchem Grund auch immer, nicht möglich ist, verwendet die Software IP-Adressen aus einem internen Speicher, der in der Vergangenheit bei früheren Verbindungen mit dem Server gebildet wurde.

Schließlich baut die Software eine Verbindung zu einer auf diese Art und Weise gefundenen IP-Adressen auf. Diese IP-Adresse gehört aber nicht Gnutella, sondern einem der User. Damit werden direkt zwei Computer verbunden, über diese Datenleitung erfolgt schließlich der Transfer des digitalen Inhalts. Gnutella hat zu diesem Zeitpunkt seine Funktion erfüllt und ist nicht mehr Teil der eigentlichen Übertragung.

Wie sich Wikipedia entnehmen lässt, wurde „das Gnutella-Protokoll von Justin Frankel definiert, der am 14. März 2000 als erste Software für das Gnutella-Netzwerk die Beta-Version des ebenfalls Gnutella bezeichneten Programms zum kostenlosen Herunterladen im Internet freigab. Frankels Arbeitgeber AOL zwang ihn jedoch nach kurzer Zeit, das Projekt aufzugeben und das Programm nicht weiter zu veröffentlichen. Das Programm war jedoch zu diesem Zeitpunkt bereits weit verbreitet und durch fremde Webseiten oder Peer-to-Peer-Netzwerke weiterhin verfügbar.“

Auch nachdem somit rasch der erste Entwickler seine Arbeit einstellen musste, wurde das Gnutella-Protokoll von findigen Nutzern des Internet weiterentwickelt und dokumentiert. Die Idee blieb somit weiterhin bestehen.

Im Mai 2006 zählte das Gnutella-Netzwerk schätzungsweise 2,2 Millionen Nutzer [Wikipedia].

Nun ist zu beachten, dass zwar, wie oben dargestellt, kein zentraler Server mehr als „Angriffspunkt“ dienen konnte, allerdings sind die Nutzer von Gnutella nicht anonym, sondern es werden ihre IP-Adressen gespeichert und verteilt. Dadurch ist auch ihre Identifizierung möglich, wenn auch nicht für jedermann, so doch durch den jeweiligen Internet-Provider.

Nach ihrem Kampf gegen Napster hat sich die Musikindustrie genau diese Tatsache zunutze gemacht, um ihre Interessen auch gegen Nutzer von Gnutella zu verfolgen und durchzusetzen. Seit Mitte 2001 überwacht somit nun die RIAA das Gnutella-Netzwerk systematisch. Wenn die von der RIAA oder einzelnen Musikern beauftragten Firmen entdeckt haben, dass ein Servant copyrightgeschützte MP3s zum Tausch anbietet, schicken sie E-Mails an dessen Provider und verlangen, dass dieser den jeweiligen Account sperrt. Aufgrund der geltenden Rechtslage kommen die meisten ISPs dem Verlangen der Musikindustrie nach. [Deters]

Bisher ist aber noch kein Fall bekannt, in dem gegen Gnutella oder einen Hersteller der Software gerichtlich vorgegangen wurde.

2.8.2.2 KaZaA

Wie das Beispiel von Kazaa zeigt, kann es aber auch zu der genau gegenteiligen Entwicklung kommen. Die Software arbeitet nach eigenen Angaben offenbar auch dezentral, ist also ähnlich wie Gnutella nicht von einem zentralen Computer abhängig. Im Gegensatz zu Gnutella, das von der Internet Gemeinde weiterentwickelt wurde, ist Kazaa allerdings ein Produkt einer Softwarefirma und der Algorithmus nur teilweise öffentlich bekannt.

Kazaa bzw die Eigentümer der Software waren in der Vergangenheit in einige Gerichtsverfahren verwickelt, die unterschiedlich zu Ende gegangen sind, letztlich aber als gemeinsamen Tenor ein Verbot der Software implizieren. Der urheberrechtliche Schutz von digitalen Inhalten hat sich damit in diesem Kapitel durchgesetzt.

In einem der zeitlich ersten Gerichtsverfahren hat vor einem niederländischen Gericht der damalige Eigentümer der Software noch in zweiter Instanz Recht bekommen. In erster Instanz wurde zunächst Kazaa BV verurteilt, in zweiter Instanz wurde aber der Anspruch einer niederländischen Verwertungsgesellschaft abgewiesen. Diese hatte verlangt, dass Kazaa Maßnahmen zur Verhinderung des Austausches von urheberrechtlich geschütztem Material mittels ihrer Software setzen müsste, weil sonst die Rechte der Urheber aufgrund der Verwendung von Kazaa verletzt würden. Die Berufungsinstanz hat allerdings festgestellt, dass das Programm nicht ausschließlich für den Austausch von geschützten Musiktiteln erstellt wurde und somit auch ein zulässiger Gebrauch möglich ist. Damit war nach Ansicht des Gerichts keine Grundlage für eine Untersagung bzw Verpflichtung zur Aufnahme von verhindernden Maßnahmen gegeben.

Aufgrund des Urteils in den Niederlanden in erster Instanz, welches noch der Musikindustrie Recht gegeben hatte, waren allerdings die Rechte an der Software mittlerweile übertragen. Der neue Eigentümer hat sich weiteren Verfahren vor Gerichten verschiedener Länder ausgesetzt gesehen.

Ganz im Gegensatz zu den Niederlanden hat ein Gericht in Australien Kazaa als für Verstöße gegen Urheberrechte verantwortlich erkannt. Dieses Gericht hat als erwiesen angesehen, dass es den Betreibern von Kazaa sehr wohl bewusst war, dass dieses Programm zur Verbreitung von geschütztem Material verwendet wird und dass es damit Urheberrechtsverletzungen in Kauf genommen hat. Die von Kazaa vorgenommenen Schritte wurden dabei als unzureichend empfunden. Kazaa hatte seinerseits in die Vereinbarung, mit welcher Nutzer die Lizenz zur Nutzung von Kazaa erworben hatten, Bestimmungen aufgenommen, wonach die Software nicht zur Verletzung von Urheberrechten verwendet werden darf. Dies sowie weitere Hinweise auf der Website waren dennoch nicht ausreichend. Interessant an diesem Urteil ist, dass es nur die Urheberrechtsverletzungen in Australien selbst zum Gegenstand hatte. Dieser Aspekt der Territorialität zeigt sich auch daran, dass Kazaa

danach mit einem Hinweis auf seiner Webseite die Nutzung in Australien untersagt hat.

Zuletzt hat sich Kazaa in einem außergerichtlichen Vergleich mit Vertretern der Musikindustrie geeinigt, Filter einzubauen, die den Tausch von geschützten digitalen Inhalten unterbindet. Daneben musste Kazaa eine erhebliche Summe an Wiedergutmachung für bereits entstandenen Schaden leisten. Diesem Vergleich war ein Verfahren in den USA vorausgegangen.

Zu erwähnen ist zu Kazaa auch, dass im Jahr 2004 ein Gericht in Cottbus, Deutschland einen Nutzer von Kazaa strafrechtlich wegen der Verletzung des (deutschen) Urheberrechtsgesetzes aufgrund unerlaubter Vervielfältigung und Verbreitung urheberrechtlich geschützter Werke verurteilt hat. Der Nutzer hatte eine Mehrzahl an Musiktiteln mittels Kazaa per Internet zum Download zur Verfügung gestellt. Das Gericht hat dabei insbesondere festgestellt, dass der Täter die Urheberrechte bewusst verletzt hatte, „da davon auszugehen ist, dass der Täter die seit einiger Zeit hierzu öffentlich geführte Diskussion in den Medien zur Kenntnis genommen hat“.

2.8.3 Google

Im Dezember 2004 hat das Unternehmen Google, bekannt für einen sehr erfolgreichen Suchdienst im World Wide Web, die Ankündigung erlassen, den Bestand einiger Bibliotheken zu digitalisieren, online zu stellen und damit einer breiteren Öffentlichkeit zugänglich zu machen. Obgleich einige dieser Bibliotheken offenbar bereits Erfahrung mit der Digitalisierung von Büchern hatten, hat dieses Projekt von Google jedoch weit reichende Aufmerksamkeit in der Öffentlichkeit erzeugt. Einerseits war dabei der Umfang des Projekts als auch die damit verbundenen Kosten ein Aspekt, der für Interesse gesorgt hat. Andererseits kam auch die Befürchtung hinzu, dass dadurch berechtigte Interessen geschädigt würden, weil nun urheberrechtlich geschütztes Material unberechtigter Weise, aber vor allem, ohne Entgelt, zur Verfügung gestellt wurde. Das Projekt wurde unter Google Book Search aber auch Google Library bekannt und war in den Schlagzeilen der Medien vertreten.

Unter digitalen Bibliotheken werden Sammlungen verstanden, die Bücher und andere Printmedien in digitaler Form enthalten und bereitstellen. Diese Formen der Verbreitung sind in Kritik geraten, weil sie angeblich mit dem Urheberrecht in Konflikt stehen. Einige der bekannteren Projekte, etwa das Projekt Gutenberg, haben sich daher darauf verlagert, nur solche Werke aufzunehmen, die keinem urheberrechtlichen Schutz mehr unterliegen. Aufgabe digitaler Bibliotheken ist es, Wissen, das in digitaler Form vorliegt, zu sammeln und anderen Personen zugänglich zu machen. Der Zugriff auf eine solche digitale Bibliothek ist im Gegensatz zu einer traditionellen Bibliothek nicht ortsgebunden. Vielmehr ermöglichen digitale Bibliotheken den Zugriff von beliebigen Orten aus, zum Beispiel über das Internet [Hofmair].

Das Spannungsfeld zwischen digitalen Bibliotheken und Digital Rights Management besteht augenscheinlich in der Möglichkeit bzw in dem Versuch zu verhindern, dass die in der Bibliothek enthaltene digitale Information unerlaubt kopiert oder gar abgeändert wird.

Google hat offenbar versucht, den bestehenden und öffentlich vorgetragenen Bedenken Rechnung zu tragen. So werden Bücher, an denen vordergründig kein Urheberrecht (mehr) besteht, im Volltext erhältlich sein, bei anderen Werken soll aber ohne Zustimmung des Berechtigten zwar das gesamte Buch elektronisch eingespeist werden, aber nur ein kleiner Auszug daraus wird auch tatsächlich öffentlich zugänglich gemacht. Dennoch haben mehrere Parteien Google wegen Verletzung von Copyright geklagt. Soweit ersichtlich sind diese Verfahren noch nicht beendet und es besteht daher Unklarheit, ob die Vorgehensweise von Google aus rechtlicher Sicht einwandfrei oder doch beanstandenswert war und ist.

Relativ unstrittig dürfte sein, dass nach einer Betrachtung dieser Vorgehensweise nach US-amerikanischem Recht die elektronische Vervielfältigung in ein allenfalls bestehendes Copyright eingreift. Denn die Kopie muss nicht in derselben Form wie das Original existieren. Sie muss nur ebenso an ein Trägermedium gebunden und für Dritte wahrnehmbar sein. Dies ist aber bei einer Digitalisierung der Papiervorlage eines Buches der Fall. Somit bleibt zu untersuchen, ob es für das Projekt allenfalls eine Rechtfertigung gibt. Die augenscheinlichste und von Google selbst ins Treffen geführte Verteidigungslinie ist „fair use“. Fair use ist in kurzen (und im Detail unzureichenden) Worten die ausnahmsweise doch zulässige Verwendung von geschütztem Material in besonderen Umständen. Fair use ist immer auf den Einzelfall bezogen. Zwar lassen sich auch einige Argumente für Google’s Position finden, und es ist nicht auszuschließen, dass ein Gericht fair use als gegeben ansehen wird. Vor dem Hintergrund aber, dass Google die elektronische Bibliothek wohl aus kommerziellen Gründen errichtet, zumindest um mit Werbeeinnahmen Profit zu erzielen, jeweils das geschützte Buch in seiner Gesamtheit kopiert wird, aber auch dem geplanten großen Umfang des Projekts und des damit voraussichtlich gegebenen Einflusses auf den vorhandenen Büchermarkt, sprechen die vermeintlich stärkeren Begründungen gegen die Annahme von fair use und damit für eine Urheberrechtsverletzung.

2.9. Zusammenfassung

Wie die vorstehenden Kapitel zeigen, hat der Urheber einige Rechte an dem von ihm geschaffenen oder ihm sonst zugeschriebenen Werkstück. Zu diesen Rechten bestehen allerdings auch einige Ausnahmen. Die verschiedenen Stufen der Rechtsordnung, angefangen von internationalen Verträgen und europarechtlichen Richtlinien bilden dafür die Grundlage. Da Österreich Mitglied der europäischen Gemeinschaften ist, war es verpflichtet, die Info-Richtlinie umzusetzen und hat dies auch getan. Ebenso ist Österreich der Berner Übereinkunft beigetreten und hat die darin statuierten Mindestrechte übernommen. Schließlich hat Österreich zwar den WIPO Copyright Treaty unterschrieben, bisher ist er allerdings nicht ratifiziert worden, so dass es nicht für Österreich bindend ist.

In den staatlichen Umsetzungen, etwa in Österreich und den USA, sind selbstverständlich die internationalen Vorgaben genauer ausgeprägt.

Der Rechtsrahmen gibt dabei insbesondere auch einen Schutz für technische Maßnahmen, die zum Schutz von Werken eingesetzt werden, vor.

3. Datenschutz

In der elektronischen Übermittlung kommt es in vielen Fällen auch zur Erfassung von Daten, die sich auf eine konkrete Person beziehen. Im Internet spielt daher auch Datenschutz eine tragende Rolle.

3.1.1 Die datenschutzrechtliche Aspekte im Internet

Der Bereich Datenschutz ist in rechtlicher Hinsicht in Österreich seit vielen Jahren geregelt. Gerade aber mit der Zunahme der Verwendung elektronischer Kommunikation und dem Eindringen von elektronischen Datenverarbeitungsgeräten in private Haushalte und jedes Unternehmen hat der Anwendungsbereich einen größeren Umfang erfahren. Das Datenschutzrecht wurde nun auch durch die Datenschutzrichtlinie europaweit vereinheitlicht. Wenngleich die Umsetzung in den einzelnen Rechtsordnungen durchaus unterschiedlich ausgefallen ist, so sind doch die Grundsätze die gleichen. Allerdings wird dem Problembereich des Datenschutzes offenbar in den USA kein so großer Stellenwert eingeräumt, so dass hier eine Lücke im tatsächlichen Schutz der betroffenen Personen bestehen dürfte.

Wenn die einschlägigen Berichte stimmen, entwickelt im Internet jede Tätigkeit und jede Eingabe ein Eigenleben und bleibt für lange Zeit, wenn nicht alle Ewigkeit bestehen und aufbewahrt. Im Gegensatz zur Vorstellung des wohl unbedarften Benutzer scheint es, als würde auch jeder noch so flüchtige Beitrag in einem Forum oder Newsgroup nicht mehr nur vorübergehend existieren, sondern auch lange nach der Aktualität noch auffindbar sein. Damit ergeben sich aber Konsequenzen, mit denen der einzelne nicht rechnet und oftmals auch nicht rechnen konnte. So gab es zuletzt einige Medienberichte, die dieses unerwartete Phänomen beschreiben. Insbesondere bei der Stellenbewerbung sind offenbar immer mehr Unternehmen daran interessiert, welche Information sich über den Bewerber im Internet finden, natürlich hat kein Bewerber daher Interesse, dass für ihn nachteilige Stellen aufgefunden werden können. Mit der Dienstleistung „Search and Destroy“, die seit kurzem angeboten wird, soll es auch möglich sein, Beiträge oder sonstige Einträge, die von einer Person stammen oder über diese vorhanden sind, nach längerer Zeit aufzuspüren und, dies ist der wichtigere Teil der Leistung, auch zu löschen. So können Stellungnahmen, die sich zeitlich überholt haben, aber für den Betroffenen auch noch zu einem viel späteren Zeitpunkt aufgrund überholter Umstände nachteilig auswirken könnten, wieder gelöscht werden.[6]

Erst kürzlich hat auch die Österreichische Nationalbibliothek angekündigt, alle Websites mit der Endung .at automatisch zu speichern und somit auch künftigen Generationen zugänglich zu machen. Zweimal im Jahr soll eine Bestandsaufnahme gemacht werden und ein Crawler durchs Netz geschickt werden, der die Seiten automatisch speichern soll.[7]

[6] Wirtschaftsblatt 23.1.2007, „Bewerber lassen ihre dunklen Geheimnisse aus dem Netz löschen“.
[7] http://futurezone.orf.at/it/stories/214363/

Bereits seit 1996 beschäftigt sich Alexa Internet mit der Präservierung des Internet. Nach eigenen Angaben[8] speichert die „Wayback Machine" eine Vielzahl an öffentlich zugänglichen Websites und zwar historisch, so dass auch Informationen, die in der derzeitigen Version nicht mehr angeführt werden, noch enthalten sind. Auch Darstellungen, die absichtlich gelöscht wurden, etwa weil sie falsch waren oder sich überholt haben, sind damit noch auffindbar. Insgesamt sind nunmehr rund 2 Petabyte an Daten gespeichert, allerdings verdoppelt sich die Menge in kurzen Abständen. Die Betreiber des Web Archives scheinen aber dem Umstand Rechnung zu tragen, dass nicht jeder mit einer zeitlich unbefristeten Speicherung seiner Gedanken und Aussagen zufrieden ist und stellen, neben den sonstigen Einschränkungen der Speicherung, die sich ohnedies nur auf einen begrenzten Teil all der im Internet verfügbaren Information beschränkt, auch die Möglichkeit zur Verfügung, einzelne Einträge oder alte Websites zu löschen.

Im Rahmen einer Gerichtsverhandlung gegen eine Frau, die ihren Mann ermordet haben soll, ist nun offenbar bekannt geworden, dass sie etwa zehn Tage vor dem Mord Suchbegriffe bei Google eingetippt hat: „undetecable poisons", „how to purchase guns illegally" und „fatal insulin doses". Weshalb diese Information offenbar noch irgendwo gespeichert war, ist unbekannt.

Die Möglichkeit der Selbstbestimmung über seine eigenen Aussagen und sonstigen Daten ist damit offenbar nur eingeschränkt möglich.

3.1.2 Das Grundrecht auf Datenschutz

Das Datenschutzgesetz[9] in Österreich normiert als grundlegende Feststellung, dass jedermann ein verfassungsrechtlich geschütztes Recht, also ein Grundrecht, auf Geheimhaltung der ihn betreffenden personenbezogenen Daten hat, wenn und soweit an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse besteht. Das Grundrecht ist daher nicht allumfassend, erstreckt sich aber nicht nur auf den intuitiv erfassten Bereich von Daten, sondern auf eine Vielzahl an Aspekten einer Person. Dies ist die Prämisse des Datenschutzes und daraus folgt, dass jede Verarbeitung von personenbezogenen Daten solange unzulässig ist, als nicht ein besonderer Tatbestand, der seine Grundlage im Datenschutzgesetz findet, diese Verarbeitung zulässig macht.

Das Grundrecht selbst kennt aber bereits die wichtigste Ausnahme vom Schutz auf Geheimhaltung, nämlich die Zustimmung des Berechtigten selbst. Das Grundrecht ist damit weitgehend ein Recht zur Selbstbestimmung. Diejenige Person, über die Daten gespeichert werden soll, kann dieser Verarbeitung selbst zustimmen und damit einen beherrschenden Einfluss auf das Schicksal der Daten nehmen.

Dieses Grundrecht, das zunächst gegen den Staat als Obrigkeit gerichtet ist, erfährt einfachgesetzlich eine entsprechende Erweiterung, so dass nicht nur die Erhebung und Speicherung von Daten durch Behörden oder von diesen autorisierte Stellen erfasst sind, sondern auch die Verwendung von Daten anderer durch private Stellen.

[8] http://www.archive.org/about/faqs.php#The_Wayback_Machine.
[9] BGBl I Nr 165/1999 idF BGBl I Nr 13/2005.

3.2. Begriffe des Datenschutzgesetzes

Der Begriff „personenbezogene Daten“ ist im Datenschutzgesetz definiert und umfasst alle Angaben über Betroffene, das sind wiederum die Personen, deren Daten verwendet werden, deren Identität bestimmt oder bestimmbar ist. Das Gesetz normiert dabei eine Kategorie von nur indirekt personenbezogenen Daten, sofern bei diesen die Identität des Betroffenen mit rechtlich zulässigen Mitteln durch den Auftraggeber nicht bestimmbar ist, dennoch eine Zuordnung, wenn auch durch eine andere Person, möglich ist. Ist allerdings die Identität gar nicht mehr feststellbar, so handelt es sich um anonyme Daten, die nicht unter das Datenschutzgesetz fallen. Der Begriff von personenbezogenen Daten ist somit weit gefasst und geht über den bloßen Namen geräumig hinaus; er erfasst auch weitere Attribute einer Person. Natürlich ist eine email Adresse ein personenbezogenes Datum, aber auch eine IP Adresse ist einer Person zugeordnet und fällt daher unter den Anwendungsbereich des Datenschutzrechts.

Eine weitere wesentliche Kategorie an Daten sind die so genannten sensiblen Daten, das sind Daten über die rassische und ethnische Herkunft, politische Meinung, Zugehörigkeit zu einer Gewerkschaft, religiöse oder philosophische Überzeugung, Gesundheit oder das Sexualleben einer natürlichen Person.

Daneben definiert das Datenschutzgesetz das Begriffspaar Auftraggeber und Dienstleister. Auftraggeber ist jene Person, die den Zweck der Verarbeitung festlegt und die Entscheidung über die Verwendung der Daten trifft. Dienstleister ist eine Person, welche im Auftrag des Auftraggebers die tatsächliche Verwendung, also Bearbeitung, der Daten durchführt. Es ist zu beachten, dass durch die Begriffsbestimmungen sehr weite Begriffe festgelegt werden, das Verarbeiten und Verwenden von Daten umfasst jegliche Handlung mit Daten. Bereits das Erfassen von Daten fällt unter die Verwendung und etwa das Ausfüllen eines Formulars oder von Datenfeldern in einem Webformular ist als erster Schritt erfasst. Ab diesem Zeitpunkt unterstehen die Daten dem Datenschutz. Dabei ist zu beachten, dass das österreichische Gesetz prinzipiell auf Handlungen in Österreich abstellt, somit die Eingabe von personenbezogenen Daten durch einen Nutzer in Österreich unabhängig davon, wo der Anbieter seinen Sitz hat, dem österreichischen Datenschutzgesetz unterfällt. Dieser Aspekt wird von vielen Anbietern wohl übersehen.

Eine Datenanwendung ist nun die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte, die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwender) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen. Jede Datenanwendung darf nun nach den Bestimmungen des Datenschutzgesetzes die Daten nur nach Treu und Glauben und in rechtmäßiger Weise verwenden, die Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke ermitteln und nicht in einer mit diesen unvereinbaren Weise weiterverwenden. Zudem dürfen die Daten nur verwendet werden, soweit sie für den Zweck der Datenanwendung wesentlich sind, und der Verwender muss danach trachten, dass sie sachlich richtig sind – daher muss er sie, wenn nötig, auf den jeweils neuesten Stand bringen. Schließlich dürfen

die Daten nur solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke erforderlich ist. Wiederum ist auch diese Begriffsbestimmung weit gefasst. Bereits aus dem Gesetz selbst lassen sich viele Handlungen und Schritte ablesen, die alle unter diesen Begriff fallen, etwa das Erfassen, das Speichern, das Verknüpfen, das Vervielfältigen, das Ausgeben, aber auch Löschen und Vernichten von Daten.

Es ist wesentlich herauszustreichen, dass nicht nur automationsunterstützte verarbeitete Daten vom Umfang des Datenschutzgesetzes erfasst sind, sondern auch manuell verarbeitete Daten diesen Vorschriften unterliegen. Das ist dann der Fall, wenn die Daten in einer Datei erfasst sind. Darunter versteht das Gesetz wiederum eine strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind. Die Beispiele dafür sind etwa Karteien oder ähnliche gegliederte Ablagesysteme.

3.3. Zulässigkeit der Datenanwendung

3.3.1 Die Verarbeitung von Daten

Das Gesetz normiert, dass Daten nur dann zulässigerweise verarbeitet werden, wenn Zweck und Inhalt der Datenanwendung den rechtlichen Befugnissen des jeweiligen Auftraggebers entsprechen. Hierbei ist von den gewerberechtlichen Genehmigungen, Konzessionen eines Unternehmens oder Statuten eines Vereins auszugehen. In der Regel ist für dieses Erfordernis zu fragen, ob die erhobenen Daten mit dem Unternehmensgegenstand oder dem Vereinszweck des Auftraggebers (gerade noch) in Einklang zu bringen sind.

Für einen Wirtschaftstreibenden ist daher festzuhalten, dass er grundsätzlich jene Datenanwendungen vornehmen darf, die für die Erreichung seines Geschäftes erforderlich sind. Jedenfalls ist dabei aber zu bedenken, dass im Einzelfall die Verarbeitung spezifischer Daten nicht mehr dadurch gedeckt sein kann, wenn hierfür bestimmte Umstände vorliegen, etwa eine notwendige Zustimmung widerrufen wird.

Der Zweck der Datenerhebung muss dabei eindeutig festgelegt werden, wobei auch diese Festlegung im Vorhinein erfolgen muss. Die Verwendung für einen anderen Zweck oder Aufgabenbereich wäre nur unter den Voraussetzungen für eine Übermittlung von Daten (dazu sogleich) zulässig.

Daneben darf die Verwendung der Daten nicht die schutzwürdigen Geheimhaltungsinteressen der Betroffenen verletzten. Für diese schutzwürdigen Interessen an Geheimhaltung sieht das Gesetz einen Katalog an Fällen vor, wann eine Verletzung nicht gegeben ist. Dies umfasst insbesondere

- die ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten,

- oder die Zustimmung des Betroffenen, wobei ein Widerruf jederzeit möglich und nach diesem Widerruf eine weitere Verwendung nicht mehr zulässig ist, oder

- lebenswichtige Interessen des Betroffenen die Verwendung erfordern, oder

- überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern.

Gerade für die an letzter Stelle genannte Generalklausel sind im Gesetz weitere Beispielsfälle angeführt, insgesamt ist hierbei eine Interessenabwägung vorzunehmen, so dass die Daten nur dann verwendet werden dürfen, wenn tatsächlich hier die Interessen des Auftraggebers überwiegen.

Für die Verwendung von sensiblen Daten sieht das Datenschutzgesetz noch strengere Regelungen vor. Hier zählt es einen Katalog an Fallkonstellationen auf, in denen die Verwendung zulässig ist. In jedem anderen Fall ist die Verwendung unzulässig und verstößt gegen das Datenschutzgesetz. Als die wohl wichtigsten Fälle sind hier einerseits die ausdrückliche Zustimmung des Betroffenen und andererseits die Verarbeitung zur Wahrung lebenswichtiger Interessen des Betroffenen oder eines Anderen zu nennen.

3.3.2 Die Übermittlung von Daten

In ähnlicher Strenge verlangt das Datenschutzgesetz, dass personenbezogene Daten nur übermittelt werden, also einen anderen Auftraggeber zur Verwendung für dessen eigene, selbstständige Zwecke, übertragen werden, wenn sie

- aus einer zulässigen Datenanwendung stammen und

- der Empfänger seine ausreichende rechtliche Befugnis glaubhaft gemacht hat und

- der Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt.

Die Daten dürfen auch nur übermittelt werden, wenn die entsprechenden gesetzlichen Voraussetzungen erfüllt sind. Eine Übermittlung innerhalb Österreichs als auch eine Übermittlung an einen Empfänger in der Europäischen Union bedarf keiner weiteren Genehmigung. Anders ist dies mit Übermittlungen von Daten in Drittstaaten, welche keinen angemessenen Datenschutz gewährleisten. Hier ist grundsätzlich vorweg eine Genehmigung der Datenschutzkommission einzuholen. Diese gilt als erteilt, wenn im Einzelfall für die konkrete Übermittlung ein angemessener Datenschutz besteht und ein ausreichendes Schutzniveau nachgewiesen werden kann, sei es durch die Art der verwendeten Daten, die Zweckbestimmung oder die Dauer der Verwendung oder durch speziell auf diesen Fall im Empfängerland anzuwendende Normen und Standards oder durch vertragliche Zusicherungen des Empfängers.

Darüber hinaus sind manche Übermittlungen genehmigungsfrei, insbesondere solche für welche der Betroffene die Zustimmung erteilt hat oder die zur Erfüllung eines im Interesse des Betroffenen abgeschlossenen Vertrags oder Geltendmachung von Rechtsansprüchen vor ausländischen Behörden erforderlich sind.

3.4. Der Dienstleister

Bedient sich der Auftraggeber eines Dienstleisters, so hat er sich zu vergewissern, dass dieser die notwendigen Voraussetzungen erfüllt. Das Datenschutzgesetz normiert Pflichten des Dienstleisters, die dieser unabhängig von vertraglichen Vereinbarungen mit dem Auftraggeber jedenfalls zu erfüllen hat. Diese Pflichten versuchen den Missbrauch von Datenverwendungen anzuhalten und schränken den Dienstleister in der Verarbeitung der Daten auf die Aufträge und Zwecke des Auftraggebers ein. Sie verpflichten den Dienstleister zur Setzung entsprechender Maßnahmen zur Datensicherheit und zur Löschung der Daten nach Erfüllung oder Beendigung des Dienstleistungsverhältnisses.

3.5. Datensicherheitsmaßnahmen

§ 14 DSG normiert gesetzliche Datensicherheitsmaßnahmen, die jedenfalls einzuhalten sind. Diese Norm geht von organisatorischen Trennungen und Maßnahmen als auch technischen Maßnahmen wie Zugriffsberechtigungen auf Daten oder Räumlichkeiten, Protokollierungen von Verwendungsvorgängen und insgesamt einem Schutzniveau, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist, aus.

3.6. Das Datenverarbeitungsregister

Grundsätzlich ist jede Datenanwendung dem so genannten Datenverarbeitungsregister zu melden. Dies ist ein Register, welches die Datenschutzkommission führt.

Jedermann ist berechtigt, in das Register Einsicht zu nehmen und allenfalls Informationen über Datenanwendungen zu erlangen. Hinsichtlich der Meldepflicht bestehen einige Ausnahmen, die praktisch wesentlichste dafür ist die Ausnahme von so genannten Standardanwendungen.

Eine Standardanwendung liegt vor, wenn eine Datenanwendung von einer großen Anzahl an Auftraggebern in gleichartiger Weise vorgenommen wird und angesichts des Verwendungszweckes und der verarbeiteten Datenarten die Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist und diese Datenanwendung durch den Bundeskanzler per Verordnung zur Standardanwendung erklärt wurde. Im privaten Bereich, insbesondere für private Unternehmen, sind dabei die drei folgenden Standardanwendungen „Rechnungswesen und Logistik“, „Personalverwaltung für privatrechtliche Dienstverhältnisse“ und letztlich „Kundenbetreuung und Marketing für eigene Zwecke“ wesentlich. Die Standardanwendung „Rechnungswesen und Logistik“ umfasst die in vielen Unternehmen notwendige Kunden- und

Lieferantendatenverarbeitung. Die Standardanwendung „Personalverwaltung“ umfasst - wie der Name sagt - die Verarbeitung und Übermittlung von Mitarbeiterdaten, speziell Lohn-, Gehalts- und Verrechnungsdaten der Beschäftigten. Die Standardanwendung „Kundenbetreuung“ legt den Fokus auf Kunden für weitere Geschäftsanbahnung und hat somit einen anderen Zweck als die Anwendung Rechnungswesen, weil auch potenzielle Kunden vor Geschäftanbahnung erfasst werden können. Herauszustreichen ist dabei, dass Daten aus dieser Anwendung auch an Adressverlage und Direktwerbeunternehmen übermittelt werden dürfen, obgleich gerade der Adresshandel in der Öffentlichkeit sehr verpönt ist.

Sofern nicht eine Ausnahme von der Datenmeldung besteht, ist die Datenanwendung mit den von der Datenschutzkommission aufgelegten Formblättern zu melden. Der Betrieb der Datenanwendung darf dabei typischerweise unmittelbar nach Abgabe der Meldung aufgenommen werden. Lediglich einige aufgezählte Datenanwendungen dürfen erst nach Bestätigung durch die Datenschutzkommission begonnen werden; dazu zählen etwa Datenanwendungen, die sensible Daten enthalten.

3.7. Die Pflichten des Auftraggebers

Der Auftraggeber hat weit reichende Pflichten. Zunächst hat er bei der Ermittlung der Daten die Betroffenen in geeigneter Weise über den Zweck der Datenanwendung sowie seinen eigenen Namen und Adresse zu informieren. Er darf dies allerdings unterlassen, wenn dem Betroffenen diese Information bereits vorliegt. Auf der anderen Seite hat er darüber hinaus weitere Information zu erteilen, wenn dies nach Treu und Glauben erforderlich ist. Diese Bestimmung soll gewährleisten, dass die Betroffenen Kenntnis von der Datenverarbeitung erlangen. Diesem Zweck entspricht auch die Pflicht, bei Übermittlungen und Mitteilungen an den Betroffenen die Identität des Auftraggebers offen zu legen. Dabei hat er etwa die Registernummer (DVR-Nummer) anzuführen.

3.8. Die Rechte der Betroffenen

Komplementär dazu haben die Betroffenen eine Reihe an Rechten. Zunächst hat der Betroffene das Recht, vom Auftraggeber Auskunft über die ihn verarbeitenden Daten zu verlangen.

Der Betroffene hat sein Auskunftsbegehren in schriftlicher Form (nicht aber email) zu stellen, wobei der Auftraggeber aber auch andere Ersuchen akzeptieren kann. Im Rahmen dieses Ansuchens hat der Betroffene seine Identität in geeigneter Form nachzuweisen, um gerade die Verletzung der Pflicht zur Geheimhaltung gegenüber einem unberechtigten Dritten hintan zu stellen. Die Auskunft des Auftraggebers muss schließlich die verfügbaren Informationen über Herkunft der Daten, die Art der verarbeitenden Daten sowie allfällige Empfänger, den Zweck der Datenanwendung und die Rechtsgrundlage hierfür anführen. Der Auftraggeber hat hier abzuwägen, ob nicht überwiegende berechtigte Interessen eines Dritten, insbesondere eines anderen Betroffenen, dessen Daten durch die Auskunft offen

gelegt würden, der Auskunft entgegenstehen. Schließlich normiert das Gesetz, dass ein Auskunftsbegehren innerhalb von acht Wochen zu erfüllen ist und hier kein Entgelt verlangt werden darf. Nur bei einem neuerlichen Auskunftsersuchen im selben Kalenderjahr kann ein Kostenersatz in geringfügiger Höhe gestellt werden.

Schließlich ist der Auftraggeber verpflichtet, unrichtige Daten zu korrigieren und Daten, die er unzulässigerweise verarbeitet, zu löschen. Diese Pflicht besteht sowohl wenn er die Unrichtigkeit oder Unzulässigkeit erkennt als auch wenn ein entsprechender begründeter Antrag des Betroffenen vorliegt.

Ein weiteres Recht des Betroffenen ist auch das Widerspruchsrecht, das geltend gemacht werden kann, wenn die Verwendung der Daten zwar grundsätzlich zulässig ist, sie allerdings nicht gesetzlich vorgesehen ist und der Betroffene in der spezifischen Situation dagegen überwiegende schutzwürdige Geheimhaltungsinteressen geltend machen kann.

3.9. Der Rechtsschutz durch das Datenschutzgesetz

Das Datenschutzgesetz normiert einen zweigleisigen Rechtsschutz.

Zunächst kann jedermann eine Eingabe an die Datenschutzkommission wegen der behaupteten Verletzung seiner Rechte unter dem Datenschutzgesetz machen. Die Datenschutzkommission hat diese zu überprüfen und kann zur Herstellung des rechtmäßigen Zustandes Empfehlungen aussprechen. Sie darf dabei vom Auftraggeber alle Unterlagen und Aufklärungen verlangen sowie auch Einsicht in seine Räumlichkeiten nehmen. Kommt der Auftraggeber einer solchen Empfehlung nicht innerhalb der gesetzten Frist nach, so kann die Datenschutzkommission ein Verfahren zur Überprüfung der Registrierung einleiten, allenfalls Strafanzeige wegen Verletzung strafrechtlicher Bestimmungen erstatten oder bei schwerwiegenden Verstößen im privaten Bereich Klage vor dem zuständigen Gericht erheben oder bei Verstößen von Auftraggebern im öffentlichen Bereich das jeweils zuständige oberste Organ informieren.

Verletzt ein Auftraggeber das Recht auf Auskunft, so kann der Betroffene Beschwerde an die Datenschutzkommission einlegen. Für sonstige Ansprüche gegen Auftraggeber des privaten Bereichs sind die ordentlichen Gerichte zuständig, insbesondere für die Rechte auf Geheimhaltung, Richtigstellung oder Löschung. Allenfalls kommt hier auch eine einstweilige Verfügung in Betracht. Sofern dem Betroffenen ein Schaden durch die schuldhafte Verletzung durch den Auftraggeber entstanden ist, kann er auch Schadenersatz geltend machen. Kommt es dabei durch die öffentlich zugängliche Verwendung von besonders geschützten Daten, nämlich sensiblen Daten, strafrechtlich relevanten Daten oder Daten über die Kreditwürdigkeit eines Betroffenen, zu einer Verletzung des Betroffenen, so steht dem Betroffenen ein Anspruch auf angemessene Entschädigung für die erlittene Kränkung zu.

Die Verletzung der Bestimmungen des Datenschutzgesetzes ist mit gerichtlicher Freiheitsstrafe bedroht, wenn Daten, die ausschließlich aufgrund einer

berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die sonst widerrechtlich verschafft wurden, vom Verletzter selbst benützt oder einem Anderen zugänglich oder veröffentlich werden, wenn dies in der Absicht geschieht, sich einen Vermögensvorteil zu verschaffen oder einem Anderen einen Nachteil zuzufügen, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat.

Die sonstigen Verstöße gegen das Datenschutzgesetz, etwa die Ermittlung und Verarbeitung von Daten ohne Erfüllung der Meldepflicht oder Übermittlung ins Ausland ohne Genehmigung der Datenschutzkommission, sind Verwaltungsübertretungen.

3.10. Datenschutz und Telekommunikation

Neben den allgemeinen Regelungen zum Bereich Datenschutz kennt das österreichische Recht – wiederum auf der Grundlage europarechtlicher Vorschriften - besondere Bestimmungen für die Geheimhaltung von personenbezogenen Daten im Rahmen der Telekommunikation. Diese Vorschriften finden sich im Telekommunikationsgesetz 2003 idgF.

3.10.1 Telekommunikationsgesetz 2003

Das TKG 2003 statuiert zunächst den Begriff des Kommunikationsgeheimnisses, dass also Tätigkeiten im Zusammenhang mit der Kommunikation im Fernsprechwege, aber auch erfolglose Verbindungsversuche prinzipiell geheim zu halten sind. Eine Verletzung des Kommunikationsgeheimnisses liegt vor, wenn ein anderer als der Benutzer ohne Einwilligung aller beteiligten Benutzer Nachrichten abhört, mithört, aufzeichnet, abfängt oder sonst wie überwacht oder Verkehrsdaten oder Standortdaten unberechtigt erfasst. Diese Vorschriften richten sich an alle Betreiber, also auch etwa Internet-Provider.

Stammdaten, das sind „alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind, nämlich Familienname und Vorname, akademischer Grad, Wohnadresse, Teilnehmernummer und sonstige Kontaktinformation für die Nachricht, Information über Art und Inhalt des Vertragsverhältnisses und Bonität“, dürfen von einem Betreiber grundsätzlich erfasst und aufgezeichnet werden, allerdings nur für Abschluss, Durchführung, Änderung oder Beendigung des Vertrages mit dem Teilnehmer, Verrechnung der Entgelte, Erstellung von Teilnehmerverzeichnissen, und Erteilung von Auskünften an Notrufträger.

Verkehrsdaten, das sind Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden, dürfen nur in speziellen Fällen gespeichert werden und sind vom Betreiber nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren. Die Speicherung ist nur erlaubt, so fern dies für Zwecke der

Verrechnung von Entgelten erforderlich ist. Die Speicherung hat aber nach Ablauf der Frist, innerhalb derer die Rechnung rechtlich angefochten werden oder der Anspruch auf Zahlung geltend gemacht werden kann, zu enden.

Inhaltsdaten, also die eigentlichen Inhalte der übertragenen Nachrichten, dürfen - sofern die Speicherung nicht einen wesentlichen Bestandteil des Kommunikationsdienstes darstellt - grundsätzlich nicht gespeichert werden. Sofern aus technischen Gründen eine kurzfristige Speicherung erforderlich ist, hat der Anbieter nach Wegfall dieser Gründe die gespeicherten Daten unverzüglich zu löschen.

Standortdaten sind Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben. Andere Standortdaten als Verkehrsdaten, dürfen ausnahmsweise verarbeitet werden, wenn sie entweder anonymisiert werden oder eine Zustimmung des Nutzers vorliegt.

3.10.2 Die Vorratspeicherung

Insbesondere im Rahmen der Bekämpfung des internationalen Terrors zeigt sich aber, dass eine Vielzahl von Informationen über elektronische Kanäle abgewickelt wird. Die internationalen Strafverfolgungsbehörden versprechen sich daher eine bessere Aufklärung von Verbrechen, wenn sie auch auf Daten dieser Kommunikation zugreifen könnten. Seit einiger Zeit wird daher innerhalb der Europäischen Union die Möglichkeit einer längerfristigen Speicherung von Daten diskutiert.

Wie auf Schmidbauer erläutert, vertreten „Verwertungsgesellschaften die Meinung, Internetprovider müssten schon jetzt alle Daten speichern, die sie zur Erfüllung ihrer Auskunftspflicht nach § 87b UrhG benötigen. Diese Ansicht ist juristisch nicht haltbar. Die Auskunftspflicht kann sich nur auf Daten beziehen, deren Speicherung rechtlich zulässig ist. Der Datenschutz ist ein Grundrecht, Einschränkungen sind zwar möglich, müssen aber explizit geregelt sein. Eine Speicherung aller Daten aller Internetnutzer, nur weil in einzelnen Fällen die Daten vielleicht einmal für ein berechtigtes Auskunftsbegehren benötigt werden, entspricht nicht dem Prinzip der Verhältnismäßigkeit. Wenn das so wäre, wäre die geplante Vorratsdatenspeicherung ohnedies hinfällig, weil schon jetzt alle Daten auf ewige Zeit (der Auskunftsanspruch ist zeitlich nicht beschränkt) gespeichert werden müssten.“ [Schmidbauer]

Anfang des Jahres 2006 wurde dazu die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (Richtlinie zur Vorratsspeicherung) erlassen. In Österreich wird diese Richtlinie in Kürze umzusetzen sein. Der diesbezügliche Gesetzesentwurf sieht eine Novellierung des TKG 2003 vor. Diese Novelle bringt eine Anpassung der Begriffsbestimmungen an jene der Richtlinie, die Verpflichtung von Diensteanbietern und Netzbetreibern zur

Vorratsspeicherung von Daten für sechs Monate, eine taxative Aufzählung der zu speichernden Daten, eine Verpflichtung zur Löschung der Daten nach Fristablauf, eine Verpflichtung von Diensteanbietern und Netzbetreibern zur Auskunftserteilung an das Bundesministerium für Justiz sowie Strafbestimmung für den Fall der Nichteinhaltung der Verpflichtung zur Vorratsspeicherung bzw der Auskunftserteilung. Die Frist von sechs Monaten zur Aufbewahrung liegt dabei an der Untergrenze des von der Richtlinie vorgegebenen Zeitrahmens von sechs Monaten bis zwei Jahren. Allerdings beschränkt sich der Entwurf nicht nur auf schwerwiegende Straftaten, sondern macht die Vorratspeicherung bereits für Taten, die mit mehr als einjähriger Freiheitsstrafe bedroht sind, möglich.

„Mit dieser Vorratsdatenspeicherung wird insoferne ein neues Kapitel aufgeschlagen, als die Daten nicht mehr im Nachhinein im Zuge der Strafverfolgung erhoben werden, sondern vorweg alle Teilnehmer der Kommunikationsnetze (und somit praktisch alle Bürger) quasi bespitzelt werden. Dabei handelt es sich um einen sehr massiven Grundrechtseingriff, bei dem nicht nur die Sinnhaftigkeit sehr umstritten ist, sondern bei dem auch höchste Zweifel bestehen, ob er in Anbetracht der nationalen Grundrechte überhaupt zulässig ist.“ [Schmidbauer]

3.11. Datenschutz und Digital Rights Management

3.11.1 Grundsätzliches

Datenschutz ist im Zusammenhang mit dem Internet ein oft diskutiertes Thema. Gerade der Einsatz von Cookies oder ähnlichen Mechanismen, die Daten über einen Benutzer und sein Verhalten sammeln, kann unter Umständen gegen Rechte eines Individuums verstoßen und dem Datenschutz zuwider laufen. Auch und gerade im Rahmen der Bezahlung von online erworbenen Gütern ist Datenschutz ein Thema. Während bei einem Kauf einer Ware in einem Geschäft gegen Barzahlung die Identität des Käufers keine Rolle spielt und somit dem Verkäufer gegenüber nicht aufgedeckt werden muss, so ist aufgrund der Tatsache, dass im Internet kein Äquivalent zur Barzahlung existiert, der Bereich der Anonymität automatisch kleiner. Natürlich ergibt sich eine ähnliche Argumentation, wenn die Ware nicht unmittelbar übergeben wird, sondern, zumindest wenn es sich nicht um Software oder digitale Inhalte handelt, physische Gegenstände, die geliefert werden müssen und somit der Kontaktname und eine Lieferadresse angegeben werden müssen. Sobald diese Informationen übergeben werden, ist der Schutzrahmen durch gesetzliche Vorschriften zum Datenschutz gefragt, um einen Missbrauch hintan zu halten.

Datenschutz und Digital Rights Management verfolgen offenbar konträre Zielsetzungen. Während der Datenschutz auf die Selbstbestimmung der Daten und die Geheimhaltung von persönlichen Daten abstellt, werden in einigen DRM Systemen Daten über den Nutzer oder sein persönliches Verhalten erzeugt, verarbeitet und ausgewertet. Offenbar besteht aber bei vielen Nutzern ein Wahrnehmungsproblem, als dass sie sich gar nicht über die potenziellen Gefahren bewusst sind. Relevant sind daher Dabei geht es insbesondere um die Rechte und

Pflichten von Akteuren, die ein Interesse an urheberrechtlich geschütztem Material haben und mit der Verwaltung digitaler Rechte befasst sind [Datenschutzgruppe].

Dieses Spannungsverhältnis wurde bereits früh erkannt, so verweist Helberger [Helberger] darauf, dass bereits anlässlich des W3C DRM consultation workshop die Problematik diskutiert wurde. Derzeit scheint dies aber noch nicht zu einer Lösung geführt zu haben. Dazu trägt auch bei, dass die tatsächlich von DRM Systemen erhobenen Daten nicht transparent sind. Augenscheinlich besteht aber auch von den Anbietern nur wenig Interesse, in dieser Hinsicht gegenüber den Nutzern Aufklärung zu betreiben, so dass weit gehend Mutmaßungen über tatsächlichen empirischen Ergebnissen stehen.

So wird wohl etwa in all jenen Systemen, in denen der Nutzer einen Schlüssel oder eine Lizenz zur Benutzung einer Datei erwerben muss, eine gewisse Identifizierung vorgenommen werden, um einen späteren Missbrauch eben dieses Schlüssels oder dieser Lizenz zu verhindern oder zumindest verfolgen zu können.

Im Zusammenhang mit dem Einsatz von Technologien, die die Kennzeichnung von Dateien oder Individualisierung von Information ermöglichen, wird ebenfalls eine persönliche Beziehung zum Nutzer erzeugt und werden diese Daten abgespeichert. Ein Beispiel dafür ist etwa Fingerprinting (siehe im Folgenden).

Bechthold führt dazu aus, „dass DRM Systeme sich verschiedener Mechanismen bedienen, um Nutzer innerhalb des Systems zu identifizieren und zu verfolgen“, so dass „potenziell nachvollzogen werden kann, welche Medienangebote Nutzer lesen, hören oder ansehen“. Er sieht darin ein „Spannungsverhältnis zwischen DRM Systemen und dem Datenschutz“ [Bechtold06].

Vor dem Hintergrund der Gesetzgebung zum Bereich Datenschutz muss sichergestellt sein, dass die entsprechenden Regelungen eingehalten werden und die Rechtsvorschriften befolgt werden, so dass der gesetzlich gewährte Schutz dem Nutzer auch zukommt. Die Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten (Artikel – 29 – Datenschutzgruppe) bei der Verarbeitung personenbezogener Daten hält dazu fest: „Die Erhebung personenbezogener Daten durch Rechteinhaber ist an bestimmte Datenschutzgrundsätze gebunden“. Vor diesem Hintergrund hält die Datenschutzgruppe die Notwendigkeit fest, „Transaktionen im Internet anonym oder pseudonym durchführen zu können“. Auch die Europäische Verbraucherschutzvereinigung hat etwa dargetan, dass „DRM Techniken ihre Nutzer in die Lage versetzen, die Art und Weise der Nutzung digitaler Inhalte zu beobachten und Verbraucherprofile anzufertigen“ [Datenschutzgruppe].

Ein wesentlicher Aspekt in der dargestellten massiven Sammlung an personenbezogenen Daten dürfte wohl auch in Marketingzwecken zu finden sein. Über die Zusammenführung verschiedener personenbezogener Daten, die bei der Authentifizierung zur Inhalts- oder Produktfreischaltung erhoben werden, lassen sich personenbezogene Kundenprofile erstellen. Diese Profile können die Inhaltsanbieter im Rahmen eines zielgerichteten Direktmarketings oder anderen Formen des Customer Relationship Management kommerziell verwerten [Hansen].

Diese Nutzung der so gewonnenen Daten ist aber ebenso datenschutzrechtlich bedenklich.

Aus diesem Spannungsverhältnis wurde auch die Forderung gestellt, DRM Systeme müssten vor ihrer Verwendung einer Überprüfung unterzogen werden, ob sie die Regelungen des Datenschutzes einhalten [Helberger]. Diese Forderung erscheint aber insofern überzogen, als auch andere Wirtschaftstreibende keiner ähnlichen Kontrolle unterworfen sind. Zudem geht ein solcher Anspruch wohl gerade im Zusammenspiel mit dem Internet ins Leere, weil in verschiedenen Rechtsordnungen kein oder ein geringerer Standard an Datenschutz gestellt wird, so dass es letztlich zu einem Ausweichen der Anbieter in diese Länder käme. Eine Überwachung dieser Aktivitäten scheitert wohl an der faktischen Unmöglichkeit.

In diesem Zusammenhang zeigt sich vor allem das Problem unterschiedlicher Rechtslagen und Rechtsanwendungen zwischen verschiedenen Rechtsordnungen oder insgesamt einem regionalen Rechtsverständnis. Typischerweise kann ein Nutzer das in seinem Heimatland gewährte Schutzverständnis nicht auch in allen anderen Rechtsordnungen erwarten. Die Datenerfassung über Ländergrenzen hinweg ist gerade aber im Internet-Zeitalter problemlos möglich, so dass ein Nutzer sich zwar rechtlich geschützt wähnt, tatsächlich diesen Schutz aber nicht durchsetzen kann. Auf europarechtlicher Ebene ist dies vermeintlich sichergestellt. Auch Artikel 2 Absatz 3 Buchstabe a der Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums verweist darauf, dass sie die Richtlinie 95/46/EG nicht berührt und folglich die Datenschutzgrundsätze zu beachten sind.

3.11.2 Eine Studie zeigt Defizite

Die intuitive Vermutung, dass DRM Systeme den recht hohen Anforderungen des Datenschutzes nicht gerecht werden, wurde durch die Studie [Grimm] bestätigt. Wie diese Studie zeigt, sind die tatsächlich erhobenen oder zumindest theoretisch erzielbaren Daten durchaus vielfältig [Grimm]:

Die Datenspuren lassen sich vor allem einteilen in:

- Vom System erzeugt bzw erhoben: Dazu gehören z.B. Informationen, die über das System oder den Browser unabhängig vom Nutzer weitergegeben werden.

- Vom Nutzer erzeugt: Dazu werden alle persönlichen Informationen gezählt sowie Daten, die durch das Nutzerverhalten im System anfallen.

- In das Produkt einkodiert: Unabhängig von den ersten beiden Kategorien zählen hierzu alle personenbezogenen Daten, die vom Diensteanbieter in das fertige Produkt einkodiert werden.

Weiters unterscheidet die Studie die folgenden fünf Kategorien von Datenflüssen:

- Datenfluss vor Vertragsschluss

  - Bei Vorbereitung des Kaufs
  - Bei Anmeldung des Nutzers
  - Bei Auswahl der Ware
- Datenfluss bei Vertragsschluss
  - Für den Abschluss des Vertrags
  - Bei Auslieferung der Ware (Daten bei Anbieter / Daten im Produkt)
  - Bei Bezahlung
- Datenfluss bei Überprüfung der Rechte zur Nutzung
  - Zur Initialisierung/Aktivierung des Produkts
  - Bei routinemäßiger Nutzung
  - Bei Änderungen der Berechtigung (Neuaushandlung, Verlust, neue Hardware)
  - Ohne konkreten Anlass
- Datenfluss für andere Zwecke
  - Informationen zur „Verbesserung des Angebots"
  - Daten für Direktmarketing
  - Angaben zur Erhaltung der Systemsicherheit
  - Gegebenenfalls weitere Informationen
- Datenfluss durch verborgene Schnittstellen und Verkettung verschiedener Funktionen
  - Verborgene Kanäle, z.B. mittels Cookies und Pixeltags
  - Verkettung von Daten, z.B. mögliche Verbindung verschiedener Datenbestände
  - (Nutzungsdaten, Bestandsdaten, etc.)

Nach Angaben dieser Untersuchung zeigt „die datenschutzrechtliche Analyse der verschiedenen Verkaufsplattformen und DRM Verfahren eine ganze Reihe datenschutzrechtlicher Defizite auf". So werden bereits am Beginn der Transaktion der von der Studie erfassten Systeme personenbezogene Daten des Nutzers erhoben, die für die eigentliche Abwicklung keine Bedeutung haben. Die Erfassung dieser Daten ist somit nicht durch das Gesetz gedeckt und die Systeme bedürfen eigentlich der datenschutzrechtlichen Zustimmung des jeweiligen Nutzers. Eine solche

Einwilligung liegt gemäß der Studie allerdings nicht vor. Auch wenn die Beurteilung nach deutschem Recht erfolgt, lässt sich aus der zugrunde liegenden Argumentation doch ableiten, dass auch nach dem österreichischen Datenschutzgesetz keine ausreichende Zustimmung vorliegen dürfte und somit insgesamt die Datenerhebung in Österreich nicht zulässig wäre. Auch darüber hinaus werden offenbar mehr Daten als erforderlich erhoben und verarbeitet und ist der Zweck nicht erkennbar sowie die tatsächliche Nutzung der Daten nicht transparent. Nach den Ergebnissen der Studie werden auch personenbezogene Daten in die digitalen Inhalte direkt eincodiert. Eine solche Verwendung von Daten erscheint jedenfalls zu weitgehend und durch das Datenschutzgesetz nicht mehr gedeckt. Soweit die Anbahnung der Geschäftsbeziehung auf eine dauerhafte Relation abzielt, etwa im Rahmen eines Abonnementdienstes, ist die Erhebung personenbezogener Daten sowohl für die Erfüllung des Vertrags durch den Provider als auch die Bezahlung durch den Kunden relevant. Beide müssen sich über ihren Geschäftspartner klar sein und auch an den richtigen Erwerber liefern. Da aber durchaus der Erwerb eines digitalen Inhalts auch lediglich eine einmalige Transaktion sein kann, ist zweifelhaft, ob hier eine ausreichende Grundlage für die Erhebung von personenbezogenen Daten gegeben ist. Die in der Studie ausgesprochene Vermutung, dass mit diesen Daten vor allem „Möglichkeit gesichert werden soll, die Nutzung des Inhaltes auf den Ersterwerber zurückzuverfolgen“ erscheint logisch. Eine systematische Sammlung von Daten aller Kunden zu diesem Zweck erscheint aber wohl überschießend. Denn damit werden die personenbezogenen Daten aller Nutzer jenseits einer konkreten Erforderlichkeit auf Vorrat gespeichert, um potenzielle Rechtsverletzer ermitteln zu können. Eine umfassende Vorratsdatenspeicherung stellte die Nutzer unter Globalverdacht. Solche Speicherungen auf Verdacht dürften nicht mit den Prinzipien des Datenschutzrechts in Einklang zu bringen sein. Wie [Hansen] darstellen, ist es problematisch, wenn „ein digitaler Inhalt nur in personalisierter Form abgegeben“ und danach „der Inhalt legal weitergegeben werden darf“, da „unter diesen Umständen der Nutzer gezwungen wäre, seine personenbezogenen Daten mit an den Dritten zu übermitteln“. Das hat zur Folge, dass „eine legale Nutzung von Inhalten damit nur unter Aufgabe des eigenen Persönlichkeitsschutzes möglich wäre“.

Als Fazit der Studie lässt sich festhalten, dass die untersuchten Systeme mehr personenbezogene Daten sammeln als für den Kaufabschluss des vom Kunden gewählten Produktes nötig sind. Die Verfasser haben festgestellt, dass „eine nicht geringe Anzahl von verborgenen und geheimen Schnittstellen existiert, sowohl durch das Einbringen von personenbezogenen Daten in den Inhaltscode, als auch durch das Verbinden und Verketten von Kundenverhaltensdaten und Kundenvertragsdaten“. Einerseits verwenden Online-Shops Informationen über ihre Kunden dazu, einen besseren Service anzubieten, indem sie z.B. Informationen über schon gekaufte oder angesehene Produkte anbieten. Andererseits ist es nicht notwendig, diese Informationen mit tatsächlichen Kunden und ihrem Verhalten, Vorlieben oder persönlichen Beziehungen zu anderen Nutzern zu verknüpfen. Verborgene Schnittstellen und im Inhalt versteckte persönliche Daten zeigen, dass Anbieter ihren Kunden nicht vertrauen. Die so genannte „zweite Verteidigungslinie“ (z.B. durch Watermarking) ermöglicht eine Verfolgung von Kunden, die Produkte illegal weiter vertreiben. Aber mit dem generellen Einbringen von Kundendaten in

Produkte werden alle Kunden gleichzeitig verdächtigt. Wenn dies intransparent, das heißt ohne Wissen der Kunden, geschieht, verlieren diese umgekehrt das Vertrauen in die Shops, die damit ihr Ansehen bei den Kunden einbüßen.

3.11.3 Eine Entscheidung zum Datenschutz

Ob allerdings die Mittel des Datenschutzrechtes richtigerweise und in ausbalancierter Art eingesetzt werden, bleibt ob einer Entscheidung der österreichischen Datenschutzkommission dahingestellt. In ihrer Empfehlung vom 5. November 2006 hat die Behörde festgehalten, dass es einem Internet-Provider untersagt ist, die IP-Adresse eines Nutzers nach Abschluss der technischen und organisatorischen Abwicklung der Verbindung ohne Zustimmung des Benutzers weiterhin zu speichern.

Im Anlassfall hatte der Internet-Provider den betroffenen Nutzern dynamische IP Adressen zugeordnet, also Adressen, die von Sitzung zu Sitzung des jeweiligen Nutzers wechseln. Obgleich die Nutzer mit einem flat-rate Verrechnungssystem abgerechnet wurden, somit die jeweiligen Daten weder für Zeitberechnungen noch sonstige Abrechnungszwecke notwendig waren, hat der Provider die Zuordnung nicht unmittelbar gelöscht. Diese Löschung ist aber im österreichischen Recht für solche so genannten Verkehrsdaten zwingend vorgesehen. Letztlich konnten die Nutzer über diese Daten ausgeforscht und wegen Verletzung von Urheberrechten - sie hatten Musikstücke zum Download zur Verfügung gestellt – verurteilt werden.

Aufgrund der in der Zwischenzeit ergangenen Richtlinie zur Vorratsspeicherung wird allerdings diese Ansicht nicht lange Bestand haben, da nach erfolgter Umsetzung alle Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, über einen Zeitraum von sechs Monaten gespeichert werden müssen.

3.11.4 Privacy Rights Management

Korba und Kenny haben nun vorgeschlagen, Systeme zum Digital Rights Management so anzuwenden, dass damit der Umgang mit personenbezogenen Daten kontrolliert werden kann [Korba]. Damit würde ein System zum Privacy Rights Management (PRM) entstehen. In dem von Korba und Kenny vorgeschlagenen PRM System sind, parallel zum datenschutzrechtlichen Verständnis wiederum der Auftraggeber, der Betroffene und der Verarbeiter die handelnden Personen oder Stellen, wobei der Betroffene auch als Eigentümer der relevanten personenbezogenen Daten angesehen wird.

Zentraler Bestandteil eines PRM Systems ist dabei der Auftraggeber-Webserver, der als Schnittstelle zwischen allen Beteiligten fungiert. Der Betroffene überantwortet dabei seine persönlichen Daten an den PRM Server, der wiederum den Schutz übernimmt, wobei es allerdings durch den Auftraggeber kontrolliert wird. Der PRM Server enthält dabei mehrere Datenbanken mit unterschiedlicher Funktion. Eine Rechtedatenbank enthält die Information, wie die personenbezogenen Daten

verwaltet werden sollen. Weiters gibt es Datenbanken, die die Aktivitäten des Auftraggebers und der Verarbeiter aufzeichnen. Informationen über den Auftraggeber und die Verarbeiter selbst sind wiederum in weiteren Datenbanken enthalten.

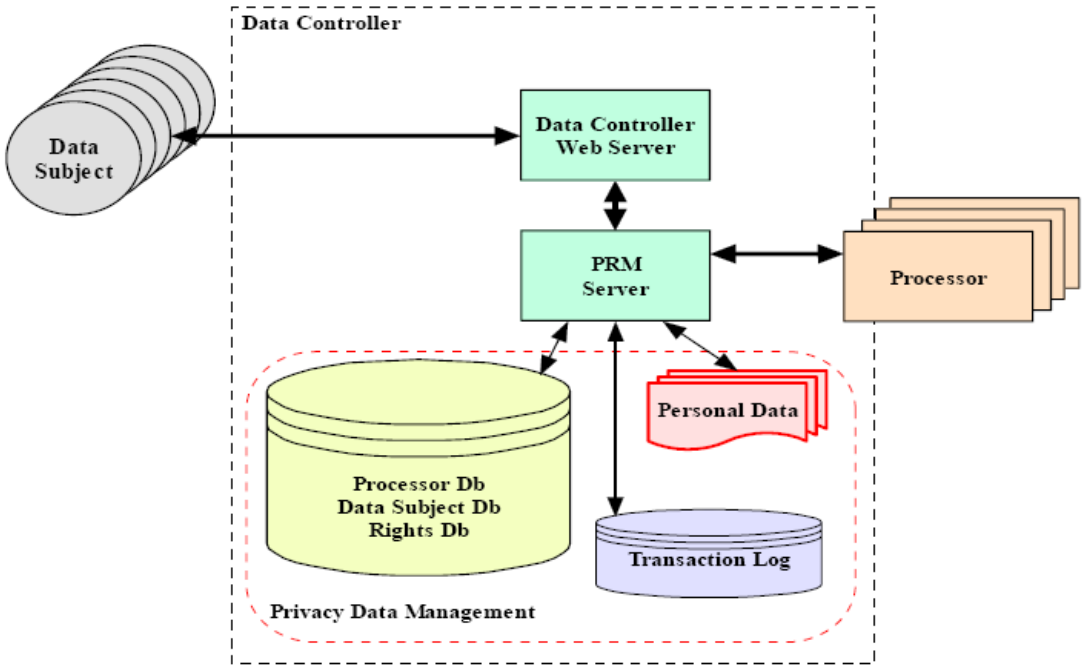


Figure 2. A simplified PRM system.

[Darstellung eines Privacy Rights Management nach Korba und Kenny]

Die drei wesentlichen Funktionalitäten eines DRM Systems, die dabei für PRM zur Anwendung kommen, sind die Erstellung von Inhalten, die Verwaltung der Inhalte und deren Nutzung. Bei der Erstellung von Inhalten können diesem Rechte zugewiesen werden. Die Verwaltung erfolgt nun unter Beachtung dieser Rechte. Dabei kommen die Möglichkeiten der Rechteverwaltung in DRM Systemen zum Tragen. Die Nutzung umfasst nun die Verwaltung der Rechte als auch eine Überwachung der Nutzung. Insbesondere durch Ausnutzung von Rechtesprachen (siehe unten)– die Autoren stellen ein Modell von PRM auf der Grundlage von XrML vor – kann somit eine Funktionalität auf der Basis von Techniken von Digital Rights Management geschaffen werden, die personenbezogene Daten verwalten kann.

4. Technische Methoden

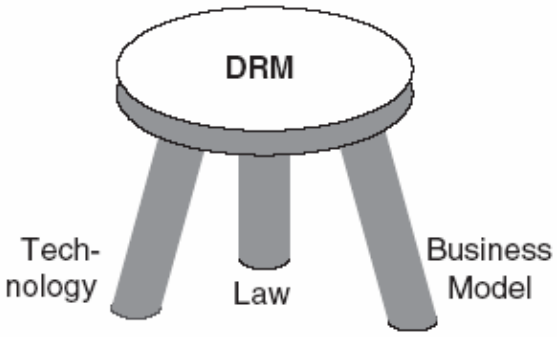


Fig. 3. Three Crucial Elements of DRM — the "three Legged Stool"

[Abbildung 1: Das „Drei Säulen Modell" [Rump]]

Rump [Rump] beschreibt die drei Säulen eines DRM Systems vergleichsweise ähnlich einem dreibeinigen Sessel. Sobald ein Bein zu kurz ist, kippt der Sessel um. Wie bereits oben besprochen, soll das „Bein" Business Model hierin ausgeklammert werden, aber die beiden anderen Säulen diskutiert werden. Nach der Ausführung zu den rechtlichen Aspekten ist das folgende Kapitel den technologischen Ideen zu Digital Rights Management gewidmet und es wird sich zeigen, welche der Rechte in der digitalen Umwelt durch technische Methoden tatsächlich geschützt werden können. Dabei wird allerdings außer Acht gelassen, ob diese Methoden auch praktisch Relevanz haben oder haben können, ebenso wenig wird berücksichtigt, ob diese Maßnahmen ökonomisch Sinn machen. Wie schon Rump an gleicher Stelle angeführt hat, macht es keinen Sinn, Inhalt, der etwa 5 Euro wert ist, mit einer Methode zu schützen, die 10 Euro kostet. Somit ist der hier gewählte Ansatz theoretischer Natur.

4.1. Einführung

Wie in diesem Werk zu Beginn festgehalten, geht es in diesem Teil der Arbeit um die ansatzweise Erörterung, welche Maßnahmen technischer Herkunft zum Schutz von Rechten im digitalen Umfeld eingesetzt werden, und welche der im Vorkapitel aufgezählten vom Gesetz eingeräumten Rechte damit denn überhaupt geschützt werden können.

Dabei sollen die verschiedenen technischen Werkzeuge kurz dargestellt werden, in der Folge wird ihre jeweilige Bedeutung und Schutzqualität geprüft. Ein besonderer Schwerpunkt soll dabei den digitalen Wasserzeichen zukommen, weil hier eine spezielle Technik zum Einsatz kommt, die im in dieser Arbeit hergestellten Zusammenhang besonders relevant ist.

4.2. Allgemeines

Es ist mittlerweile wohl allgemein anerkannt, dass technologische Schutzmaßnahmen und Kontrollsysteme das effiziente Verwalten von Rechten, aber nicht zu vergessen auch deren Ausnahmen erleichtern können [Kommission].

Ein wesentliches Kriterium von Digital Rights Management soll dabei sein, dass jedem digitalen Objekt („content") jene Regeln und Rechte zugewiesen werden, die dann auf diesen Inhalt anzuwenden sind. Es ist daher notwendig, ein Rechtemodell, also eine Spezifikation jener Rechte und deren Verknüpfungen zueinander, zu entwerfen, die auf einen gewissen content anzuwenden sind [Rosenblatt].

Die jeweiligen Rechte werden dabei stark vom Zweck und Nutzen des content sowie auch von dem jeweiligen DRM System oder von der Nutzung des Systems zugrunde liegenden kommerziellen Modells abhängen. Die einzelnen Verwendungsmöglichkeiten und damit Rechtseinräumungen sind letztlich unzählig und hängen einerseits von der technologischen Ausgestaltung des DRM Systems und den darin vorgesehenen Unterscheidungsmöglichkeiten ab, andererseits von der Implementierung und Einstellung durch den Rechteinhaber. DRM Systeme lassen sich funktional grob in zwei Gruppen einteilen: Zugangs- und Nutzungskontrollsysteme [Arlt].

Von einer anderen Betrachtungsweise können die Techniken in aktive und passive Kontrollmaßnahmen eingeteilt werden. Passiven Schutz bieten dabei

- die Maßnahmen, solange der content noch im Verfügungsbereich des Urhebers ist, etwa Zugriffskontrolle auf dessen Server
- der Schutz im Übertragungsweg
- die Schutzmaßnahmen, sobald der content beim Empfänger eingetroffen ist
- die Maßnahmen zur Aufspürung von unberechtigten Kopien.

Komplementär dazu umfassen aktive Maßnahmen

- die Aufklärung über Lizenzrechte und den Umfang derselben
- die Identifizierung und die Authentifizierung der Lizenznehmer
- die Mechanismen zur Überwachung und Durchsetzung von Verwendungsarten während der Verwendung, somit auf dem System des Nutzers
- die automatische Deaktivierung oder die Löschung der Software nach Eintritt eines Ereignisses, wie unbefugter Nutzung oder Zeitablauf.

Biehl teilt die Ziele, die beim Schutz von digitalen Daten verfolgt werden in vier Klassen ein:

- der Beweis der Urheberschaft: Mechanismen, mit deren Hilfe ein Urheber seine digitalen Daten mit dem Nachweis seiner Urheberschaft versehen kann.
- der Nachweis der Datenmodifikation: Techniken kommen zum Einsatz, die es dem Urheber und eventuell den Benutzern ermöglichen, Veränderungen an

den Daten zu erkennen und nachzuweisen, etwa um Fotomontagen als solche entlarven zu können.

- die Verhinderung der Herstellung von Raubkopien: Verfahren werden verwendet, die die Herstellung von Raubkopien verhindern oder erschweren.

- der Nachweis unberechtigter Weiterverbreitung: Methoden, die es erlauben, Raubkopien als solche zu erkennen und darüber hinaus den Hersteller einer Raubkopie zu identifizieren, sollen als Abschreckungsmaßnahme dienen.

DRM Systeme bestehen typischerweise aus der Zusammenarbeit von mehreren Technologien, die jeweils einen funktionalen Part in der Verwaltung spielen. Ein wesentlicher Teil der Aufgabe kommt dabei der Verschlüsselungstechnik zu (siehe etwa das DRM pillar-Model in [Hartung]).

4.3. (Bloßer) Kopierschutz

In der Literatur ist derzeit nicht klar, ob relativ einfache Kopierschutzmechanismen auch zu Digital Rights Management gezählt werden können bzw als DRM Systeme gelten sollen. Dies hängt selbstverständlich stark von der letztlich zu klärenden Definition des Begriffes ab. Wie auch schon erwähnt bieten moderne und ausgereiftere DRM Systeme neben dem Kopierschutz auch Kanäle für die Verbreitung sowie Bezahlung und Abrechnung der genutzten Inhalte.

Meines Erachtens sind aber auch solche „bloßen" Kopierschutzverfahren im gewissen Rahmen und Umfang geeignet, einige der Rechte des Schöpfers der Software zu kontrollieren und damit bedingt zu verwalten, so dass sie zumindest als Vorstufe zu den heutigen DRM Systemen angesehen werden können.

Im Sinne eines weiten Begriffsverständnisses sollen im Folgenden auch Kopierschutzmaßnahmen als technische Schutzmaßnahmen betrachtet und in die weitere Abhandlung miteinbezogen werden.

4.3.1 Früher Kopierschutz

Unter Kopierschutz wird ein System verstanden, dass die Grenzen der erlaubten Kopiertätigkeiten, wie sie zwischen dem Hersteller und dem Nutzer vereinbart wurden, absteckt und die Nutzung auf die erlaubten Verhaltensweisen einschränkt. Der Kopierschutz kann dabei auch die Verbreitung von Kopien bzw des Inhalts, einschließlich der Verteilung im Internet erfassen. Dabei wird aber der Zugang selbst nicht kontrolliert [CEN].

In der praktischen Umsetzung dieser Kopierschutzmaßnahmen kamen verschiedene Techniken zum Einsatz. Es ist beinahe als selbstverständlich zu bezeichnen, dass auch solche Schutzmaßnahmen von versierten Fachleuten („Cracker") umgangen bzw aus der Software entfernt werden konnten. Jedoch dem „normalen" Nutzer wurde dadurch ein Hindernis für die ungerechtfertigte Weitergabe in den Weg gelegt.

4.3.2 Schutz durch Passwort oder Textabfrage

Bereits mit dem Zeitpunkt des Aufkommens von Heimcomputern und der stärkeren Trennung von Hardware- und Software-Providern wurden erste Mechanismen zum Schutz von Computer-Software eingesetzt. Bereits in den frühen 80er Jahren gab es Kopierschutzmechanismen für die damaligen Heimcomputer von Commodore und Apple.[10] Solche Kopierschutzverfahren sollten das unerlaubte Kopieren von Datenträgern verhindern oder zumindest die Nutzung der Software nur rechtmäßigen Inhabern gestatten.

Auf relativ primitiver Ebene stehen etwa Abfragen nach einem selbstgewählten oder auch vorgegebenem Passwort oder gar bestimmten Textpassagen aus dem zur Software gehörenden Handbuch. Passwortabfragen gehören auch heute im Internet gewissermaßen zum Standardrepertoire.

Bei der Abfrage des Textes wurde natürlich bei jedem Start des Programms eine andere Stelle des Handbuchs oder Beilage eingefordert und der Nutzer musste die entsprechende Stelle im Text ausforschen und in die Abfragemaske eingeben. Dieser Zugang sollte den einfachen Vorgang des elektronischen Kopierens der Software zumindest insofern erschweren, als auch zur Weitergabe bzw Weiternutzung der Software eine Kopie des Handbuchs erforderlich ist. Damit wurden zwar der Aufwand und die Kosten einer Weitergabe erhöht, dennoch war der Level des Schutzes nur begrenzt. Teilweise konnten auch in Programmen die relevanten Stellen der jeweiligen Abfrage von kundigen Personen erforscht und danach entfernt werden, so dass eine - wenn auch unrechtmäßige - Kopie ohne Schutzmechanismus entstand.

Bei der Passwortabfrage erhält jeder Nutzer ein Passwort; dies kann dasselbe für alle Nutzer oder natürlich jeweils ein spezifisches pro Nutzer sein. Die Passwortweitergabe ist aber natürlich in keinster Weise unterbunden. Allenfalls kann bei personalisierten Kennwörtern ein Rückschluss auf den ursprünglich Berechtigten, der unzulässigerweise seine Kennung weitergegeben hat, gezogen werden. Ebenso wie bei der Textabfrage kann auch die Passwortabfrage programmtechnisch umgangen oder aus dem Programm ganz gelöscht werden. Wiebe zeigt, dass damit ein begrenzter Raum für solche Mechanismen in der Zugangs- und Nutzungskontrolle bleibt, etwa bei tagesaktueller Information, die bereits nach kurzer Zeit ihren Wert verliert.

4.3.3 Dongles

Bereits in den 80er Jahren des 20. Jahrhunderts wurde Software durch den Einsatz so genannter „Dongles“ zu schützen versucht. Es handelt sich hierbei um einen noch relativ einfachen Versuch des Schutzes, wenngleich auch um eine gegenüber der Abfrage von Textpassagen etwas ausgefeiltere Technik.

Ein Dongle ist ein hardwaremäßiger Schutz gegen das Kopieren von Software. Dabei ist es notwendig, den Dongle, ein kleines zusätzliches Stück Hardware, das vom

[10] Siehe auch http://encyclopedia.thefreedictionary.com/technical%20protection%20measures.

Softwarehersteller mit dem Programm mit geliefert wird, an den Computer anzuschließen, damit dieser die Nutzung der Software sozusagen frei gibt [Fallenböck02]. Nur wenn das abzuspielende Computerprogramm am Beginn die erwartete Rückmeldung des Dongle erhält, ist eine vollständige Nutzung ermöglicht [Wayner]. Ist der Dongle nicht angeschlossen, so wird der Start des Programms abgebrochen und die eigentliche Nutzung ist damit unterbunden. Damit war zwar das Kopieren eines Programms ohne Dongle möglich, nicht aber die Verwendung, die Kopie daher unbrauchbar. Auf diese Weise konnte die unberechtigte Verwendung eingeschränkt werden.

Der dadurch erreichte Schutz war nicht sehr hoch, die Abfragen konnten von entsprechend versierten Programmierern entfernt oder Dongles, die teilweise technisch einfach aufgebaut waren, nachgebaut werden [Wiebe].

4.3.4 Smartcards

Ähnlich wie Dongles benötigt auch bei einem Schutzmechanismus unter Einsatz von Smartcards der Verwender ein weiteres Bauteil. In diesem Fall ist der fehlende Schaltkreis in einer Smartcard, also einer standardisierten Plastikkarte mit integriertem Chip. Dieser Chip besitzt einen eigenen Mikroprozessor und Speicher, ist also gewissermaßen ein Computer in kleinem Maßstab. Die Speicherung von Daten erfolgt dabei auch ohne Stromzufuhr in dauerhafter Weise.

Die technische Erweiterung gegenüber Dongles – und damit ein wesentlicher Schritt in die Richtung „echten“ Digital Rights Management - ist sicherlich auch die Verhinderung technischer Manipulationen der Smartcard, da die Information von der Smartcard nicht auslesbar ist. Aufgrund der Konstruktion ist es auch nicht möglich, die Smartcard zu öffnen, ohne dabei die Information selbst zu zerstören. Die auf der Smartcard gespeicherten Daten können somit nur über die definierte Schnittstelle gelesen werden.

Smartcards finden heute bereits vielfältig Anwendung in dieser Funktion, etwa für Pay-TV Systeme.

4.3.5 Der Schutz des Datenträgers

Gerade die Musikbranche bemüht sich stark um technische Schutzmaßnahmen für ihre wertvollen Werke. Daher gibt es verschiedene Techniken, Audio CD’s zu schützen.

Das Magazin c’t berichtete etwa über eine Variante, die „offenbar auf manipulierten TOC-Einträgen (TOC = Table of Contents) im Lead-in der CD beruht; so wird auf allen CD-Spielern als Gesamtlaufzeit ein Wert von 28 Sekunden statt rund 42 Minuten und oft eine negative Restlaufzeit nach Überschreiten eben dieser ersten halben Minute angezeigt. Wenn sich ein PC mit CD-ROM-Laufwerk auf die in der TOC vermerkte Gesamtlaufzeit verlässt, bricht er nach 28 Sekunden die Wiedergabe oder das Einlesen der Audiodaten ab. Auch Auto-CD-Spieler, die sich normalerweise die CD-Position beim Ausschalten merken, fangen immer wieder bei Track 1 an“ [ct].

In der Praxis scheint es aber, dass solche Maßnahmen weniger das unerlaubte Vervielfältigen unterbinden, als dass sie eher zu Problemen bei der Benutzung des Tonträgers führen. Aufgrund der Vielzahl an verschiedenen Geräten, mit denen Audio-CDs nunmehr abgespielt werden können, kommt es offenbar zu fehlerhafte Interpretationen des Schutzmechanismus und auch Original-CDs können nicht mehr auf jedem CD-Spieler wieder gegeben werden.

4.3.6 DVD

Ein moderneres Verfahren des Kopierschutzes wurde bei DVD eingesetzt. Es beruht im Wesentlichen auf Verschlüsselungstechnologie („Content Scrambling System"-CSS). Da diese Technologie mittlerweile aber nicht mehr als sicher gilt, wird offenbar bereits in der Praxis wieder auf diesen Schutz verzichtet. Mit CSS wird die Information auf einer DVD verschlüsselt.

CSS basiert auf einem einmaligen Master-Key. Jedes Abspielgerät selbst hat auch einen Schlüssel, einen Geräte-Schlüssel, den es aus einem Satz von etwa 400 Schlüsseln zugeteilt erhält. Dieser Player-Key muss in einem geschützten Bereich untergebracht sein, um vor unberechtigtem Auslesen gesichert zu sein. Mit diesem kann der Inhalt wieder entschlüsselt werden und schließlich verarbeitet werden. Des Weiteren besitzt jede DVD in einem geschützten Bereich 400 Kopien des Master-Keys, jeweils mit den 400 unterschiedlichen Player-Keys verschlüsselt, einen Disk-Key und bis zu 99 Title-Keys. Zusätzlich enthält die DVD noch einen 5 Byte großen Hashwert seines entschlüsselten Disk-Keys. Das CSS-Modul des DVD-Players identifiziert sich mit seinem Player-Key bei der DVD, indem es versucht mit seinem Key einen der verschlüsselten Master-Keys zu entschlüsseln. Bei gelungener Authentifizierung gibt die DVD sodann ihren Disk-Key und ihre Title-Keys an den Player weiter und der Player kann damit die Videodaten entschlüsseln.

Zudem enthält jede DVD als zweites, unabhängiges Schutzelement, einen regionalen Code („Regional Playback Control RPC") zugewiesen, gemäß dem eine DVD nur auf einem DVD-Player mit dem entsprechenden selben regionalen Code abgespielt werden kann. Damit sind DVDs nur in einer bestimmten Region verwendbar, insbesondere sind US-amerikanische DVD nicht in Europa einsetzbar. Insgesamt wird damit eine Einteilung in sechs regionale Gebiete erreicht. Hintergrund war offenbar, dass Filme auf DVD zu unterschiedlichen Zeitpunkten in unterschiedlichen Regionen zum Verkauf und Verleih bereitgestellt wurden. Um die Rentabilität anderer Vertriebskanäle wie Kino oder Pay-TV nicht zu gefährden, sollte es nicht möglich sein, auf anderen Märkten eine DVD bereits abzuspielen, obwohl diese auf diesem Markt noch nicht im Handel erhältlich ist.

Interessant ist an CSS, das es Gegenstand eines der bekanntesten Fälle der Umgehung von Schutzmaßnahmen geworden ist, jener über DeCSS. In zwei Gerichtsverfahren in Amerika, nämlich Universal City Studios, Inc., v. Corley und DVD Copy Control Association v. Brunner, wurde dieses Programm Gegenstand der Verhandlungen. Im ersten Fall wurde ein Verleger, der dieses Computerprogramm weiter verbreitet hatte, dazu verurteilt, die weitere Verbreitung zu unterlassen. Da DeCSS im Wege des Reverse Engineering erstellt wurde, diese Methode aber durch

US-Recht als unzulässig erklärt wurde, ist das Programm rechtswidrig. Ebenso wurde ihm in einem weiteren Urteil untersagt, Links auf andere sites, auf denen dieses Programm gefunden werden konnte, weiterhin aufrecht zu halten. Das Gericht hat dabei sehr wohl erwogen, dass ein Verbot, Links zu setzen durchaus weitgreifend ist und einen starken Eingriff in die Gestaltungsfreiheit des Erstellers der jeweiligen Web Seite darstellt. Eine Haftung für Links dürfe es daher nur in engen Grenzen geben. Allerdings hat das Gericht es als erwiesen angesehen, dass der Beklagte als Linkprovider zum Zeitpunkt des Anbringens des Links Kenntnis davon hatte, dass sich das Programm auf der verlinkten Webseite befindet, dass dieses nicht rechtmäßig angeboten werden kann und er den Link geschaffen hat, um die Umgehungstechnologie zu verbreiten.

Im zweiten Fall wurde einem website-Operator allerdings letztlich gestattet, auf seiner website das Programm zur Verfügung zu halten. Der Court of Appeal hat dabei den Source Code als von der amerikanischen Verfassung geschützten Ausdruck des Autors sowie Information über die Entschlüsselung von DVDs angesehen. Damit war das Programm gemäß dem ersten Zusatz zur amerikanischen Verfassung nach dem Prinzip der „free speech“ geschützt [Fallenböck02].

4.3.7 Schutz durch explizite Freischaltung

Eine Methode, die bereits in früherer Zeit Verwendung gefunden hat, mit dem Einzug des Internet in beinahe jeden Haushalt aber noch eine viel einfachere Handhabung besitzt, ist die explizite Freischaltung. Für diesen Mechanismus ist es notwendig, dass der Nutzer der Software sich bei einer zentralen Stelle, etwa dem Hersteller oder einem von diesen beauftragten Dritten, registriert. Der Registriervorgang kann dabei in der Theorie über jedes beliebige Medium erfolgen, in der Praxis war aber zunächst die telefonische Anmeldung, in jüngerer Zeit die Verbindung per Internet die gängigste Variante. Nach der Registrierung und Validierung der Stelle, dass eine berechtige Kopie der Software vorliegt, zumeist durch Abfrage der Seriennummer und Überprüfung, dass diese bis zu diesem Zeitpunkt nicht bereits schon einmal freigegeben worden ist, erhält der Nutzer in der Regel eine Nummer zur Eingabe in das Programm und damit Freischaltung. Ein dafür bekanntes Produkt ist etwa Microsoft Windows, zuletzt mit dem Betriebssystem Windows XP, das eine solche Freigabe nach dem Kauf vorsieht.

Diese Technik machen sich auch heute noch einige DRM Systeme zu Nutzen, etwa aber auch in der Abwandlung, dass eine Freischaltung vor jedem einzelnen Gebrauch notwendig ist, nicht bloß einmalig am Beginn der Nutzung.

Auch ist es denkbar, nicht nur die Software frei zu schalten, sondern auch Hardware Teile über eine eindeutige Kennung zu aktivieren oder eben deaktivieren. Ethernet Karten etwa besitzen eine eindeutig zuordenbare Adresse, die Media Access Control Adresse und können somit identifiziert werden.

4.3.8 Welche Rechte werden geschützt?

Es stellt sich nun die Frage, welche der vom Urheberrecht dem Urheber oder dem sonstigen Berechtigten zugewiesenen Rechte tatsächlich durch diese teilweise schlichten Maßnahmen geschützt werden können.

Am relevantesten erscheinen dabei das Vervielfältigungsrecht, wie auch das Verbreitungsrecht und das Recht auf Zurverfügungstellung. Intuitiv ist man geneigt, diese Rechte als geschützt zu erachten, da diese auf den Kopiervorgang abstellen. Dabei zeigt sich aber, dass die einfachen Mechanismen des Kopierschutzes, wie zum Beispiel die Textabfage, eine Verletzung gerade dieser Rechte in keiner Weise verhindern können. Die Datei selbst kann natürlich weiterhin kopiert und auch weiter gegeben werden. Lediglich der damit verbundene Aufwand wird erhöht, weil auch Textbücher kopiert und verteilt werden müssen. Dadurch kommt es zwar möglicherweise zur Unwirtschaftlichkeit des Vorgehens, nicht aber einer Verhinderung des Eingriffs. Auch der Einsatz von Dongles kann die Vervielfältigung und Weitergabe nicht verhindern. Allerdings ist die Beeinträchtigung des Rechteinhabers reduziert, weil der Empfänger einer Kopie diese nicht nutzen kann. Damit ist das Ziel, nämlich die Verwendung des vervielfältigten Materials zu unterbinden doch auch erreicht.

Demgegenüber verhindert der Kopierschutz von CSS und je nach dem eingesetzten Verfahren bei Audio-CDs zumindest teilweise tatsächlich die physische Vervielfältigung. Denn hier unterbleibt bereits der eigentliche Kopiervorgang.

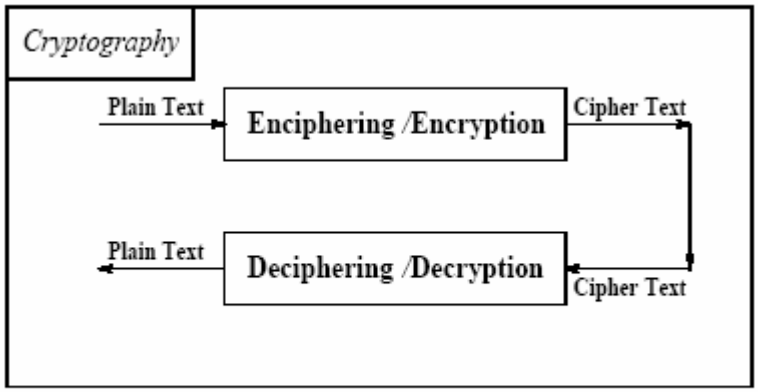
Andere Rechte, wie insbesondere die Urheberpersönlichkeitsrechte, bleiben aber in dieser Betrachtung gänzlich ungeschützt.

4.4. Verschlüsselungsverfahren

4.4.1 Allgemeines

Eine weitere wichtige Technologie im Rahmen von Digital Rights Management ist das elektronische Verschlüsselungsverfahren. Verschlüsselung wird von einigen geradezu als die Kerntechnologie angesehen. So hält etwa ein Autor fest: „Encryption of content is the keystone of current copy protection efforts“ [Besek].

Im Grunde ist eine Verschlüsselung die Substituierung eines bestimmten Zeichens eines Textes durch ein willkürlich gewähltes anderes Zeichen [Berlakovich]. Mit einem solchen Verfahren wird also der ursprüngliche Text, der so genannte Klartext, mittels eines festgesetzten Mittels, des Schlüssels in einen anderen Text, das Chiffrat oder auch als Schlüsseltext sowie Ciphertext bezeichnet, übergeführt. Mit Hilfe des inversen Schlüssels wird im umgekehrten Entschlüsselungsvorgang aus der verschlüsselten Information wieder der ursprüngliche Gehalt gewonnen. Dies bedeutet, dass ein Dritter, der den Schlüssel nicht kennt und besitzt, auf die solcherart veränderte Information nicht zugreifen und diese lesen kann. Gegenüber diesem Dritten ist die Information geschützt bzw bleibt sie geheim.



(b) Cryptography

[Abbildung 2: Beschreibung des Vorgangs der Verschlüsselung [Mohanty]]

In der Praxis wird heute im Wesentlichen zwischen symmetrischen Verschlüsselungsverfahren, welche für die Ver- und Entschlüsselung der Daten denselben Schlüssen verwenden und asymmetrischen Verschlüsselungsverfahren, welche unterschiedliche Schlüssel für die Verschlüsselung als auch Entschlüsselung verwenden, unterschieden.

Der entscheidende praktische Nachteil des symmetrischen Verschlüsselungsverfahrens ist gerade, dass eben derselbe Schlüssel verwendet wird. Dieser muss vor der Verwendung über einen sicheren Kanal zwischen Sender und Empfänger ausgetauscht werden. Denn jeder, der den Schlüssel besitzt, kann sowohl Nachrichten entschlüsseln, als auch neu verschlüsselte Nachrichten versenden.

Der (bislang noch) bestehende Nachteil der asymmetrischen Verfahren ist die Komplexität und damit einhergehende benötigte Rechenkapazität bzw Dauer der Ver-/Entschlüsselung.

Einige Verfahren, wie etwa das weit verbreitete Programm PGP, wenden daher eine Kombination aus symmetrischen und asymmetrischen Schlüsseln an. Der, relativ zum Klartext gesehen, kleine (symmetrische) Schlüssel wird mit einem asymmetrischen Verfahren verschlüsselt und auf diese Weise sicher an den Empfänger transportiert. Die eigentliche Information wird mit diesem symmetrischen Verfahren einfacher und schneller entschlüsselt.

Allen Verschlüsselungsverfahren ist gemein, dass sie zwei Prinzipien möglichst weitgehend gehorchen sollten:

(1) Konfusion: Die Verbindung zwischen einem Eingabewert und dem Ausgabewert sollte möglichst zufällig sein.

(2) Diffusion: Die Verschlüsselung eines Zeichens soll in gleichmäßiger Weise nicht nur vom Klartextzeichen, sondern auch von allen seinen Nachbarn bestimmt sein. Damit fließt idealerweise der gesamte Klartext in die Verschlüsselung jedes Zeichens und Auswirkungen im Klartext ergeben einen stark abweichenden Ciphertext bzw führen geringfügige Änderungen im Ciphertext bei der Entschlüsselung zu einem anderen Klartext.

4.4.2 Die symmetrische Verschlüsselung

Die bekanntesten symmetrischen Verschlüsselungsverfahren sind DES (Data Encryption Standard) oder nunmehr, da DES aufgrund der verwendeten Schlüssellänge nicht mehr als ausreichend sicher empfunden wird, dessen Nachfolger AES (Advanced Encryption Standard).

4.4.2.1 Das Verfahren DES

DES erfolgt in verschiedenen Runden mit relativ einfachen Berechnungen. Grundlegende Funktion ist dabei das „exclusive or" (xor) sowie Transformationen durch die so genannten S-Boxen und Permutationen durch die so genannten P-Boxen.

DES verwendet für seine Verschlüsselung jeweils Blöcke mit einer Länge von 64 Bit. Die Länge des Schlüssels selbst beträgt ebenfalls 64 Bit, jedes achte Bit dient allerdings bloß als Paritätsbit und wird daher in den eigentlichen Prozess der Verschlüsselung nicht eingebunden. Aus den verbleibenden 56 Bit wird in jedem Schritt, den so genannten Runden, ein Teilschlüssel mit schließlich 48 Bit generiert.

Gleichzeitig wird jeder Klartextblock in zwei 32 Bit Blöcke unterteilt, der L-Block und der R-Block. Die Verschlüsselung erfolgt nun in 16 gleichlaufenden Runden.

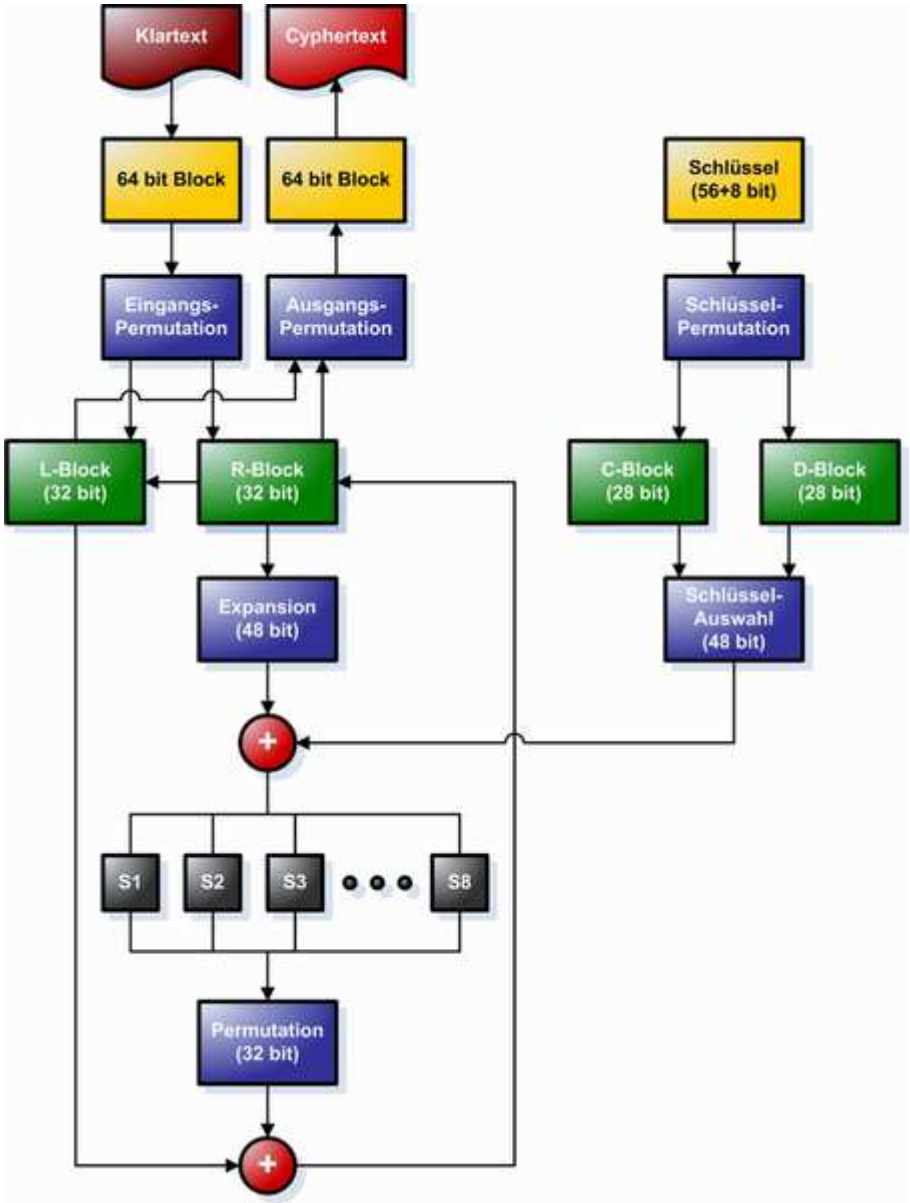
Dabei wird der R-Block mit Hilfe der so genannten „Expansion" auf 48 Bit „verbreitert", er hat damit die gleiche Länge wie der Schlüssel. Die Expansion erfolgt wiederum auf Einheiten von 4 Bits, wobei jeweils das letzte Bit des vorherigen Blocks das neue erste Bit wird und das erste Bit des nachfolgenden Blocks das neue sechste Bit darstellt. Der solcherart expandierte R-Block wird nun mit der XOR-Funktion mit dem Teilschlüssel verknüpft. Im nächsten Schritt wird das Resultat in acht Gruppen zu je sechs Bit zerteilt. Auf jede dieser Gruppe werden nun mit Hilfe der fix vorgegebenen so genannten Substitutionsboxen („S-Boxen") Substitutionen durchgeführt, die als Ergebnis pro Gruppe einen Wert der Länge 4 Bit errechnen. Dabei bestimmen das erste und sechste bit die Zeile und das zweite und fünfte bit die Spalte in der S-Box Tabelle. Mit diesen S-Boxedn soll Diffusion erzeugt werden. Zum Abschluss der Runde folgt eine Permutation, ebenfalls nach einer festen Regel („P-Box"). Aufgrund der Einschaltung der P-Box kommt es dazu, dass einzelne Bitänderungen sehr schnell und kurzfristig weitergeleitet werden und somit einen relativ großen Einfluss auf das Gesamtergebnis haben. Dieses Ergebnis bildet schließlich aufgrund einer XOR-Verknüpfung mit dem L-Block den R-Block der nächsten Runde.

In der nächsten Runde werden der R-Block der ersten Runde zum L-Block der zweiten Runde und der gleiche Prozess nochmals durchlaufen.

Die Entschlüsselung erfolgt durch den gleichen Algorithmus, allerdings in umgekehrter Reihenfolge.

Der Vorteil an DES liegt in seinem Aufbau, da einzelne Schritte sehr vorteilhaft in Hardware umgesetzt werden können und aufgrund dieser direkten Schaltung eine

schnelle und effiziente Berechnung ermöglicht wird. Damit ist der Einsatz in der Praxis leichter und bereits bei kleineren Anwendungen mit geringem Aufwand möglich.



[Abbildung 3: Darstellung der Funktionsweise von DES; http://de.wikipedia.org/wiki/Data_Encryption_Standard]

4.4.3 Das asymmetrische Verfahren

Beim asymmetrischen Verfahren entfällt der oben genannte Nachteil, dass der Schlüssel für die Verschlüsselung und der Schlüssel für die Entschlüsslung ident sind. Daher eignet sich diese Methode besser für den Einsatz vor allem bei einer Vielzahl von potenziellen Kommunikationspartnern und vereinfacht die Verteilung des Schlüssels, die nicht geheim erfolgen muss. Man spricht daher auch oft von „public key" Verfahren, weil hier das zur Anwendung kommende Schlüsselpaar einerseits aus dem öffentlichen Schlüssel, dem public key, und andererseits dem private key, einem geheimen Schlüssel, besteht. Der Absender verschlüsselt die

Nachricht mit dem öffentlichen Schlüssel des Empfängers, der nur von diesem (sofern der geheime Schlüssel tatsächlich geheim geblieben ist) mit dem „private key“ entschlüsselt werden kann.

Den Beginn dieser Verschlüsselungstechnik markieren wohl die Erkenntnisse von Whitfield Diffie und Martin Hellmann, die bereits Mitte der 70er Jahre ein Verfahren für public key Verschlüsselung entdeckt haben

4.4.3.1 Das Verfahren RSA

Das wohl bekannteste Verfahren der asymmetrischen Verschlüsselung ist der so genannte RSA-Algorithmus, benannt nach den Anfangsbuchstaben in den Namen seiner Erfinder. Dieser Algorithmus nutzt die Schwierigkeiten, die heute auf der Grundlage der derzeit vorhandenen technischen Mittel bei der Faktorisierung von großen Zahlen, also die Zerlegung dieser Zahlen in ihre Primfaktoren, bestehen. Obgleich es nicht mathematisch bewiesen ist, dass dieses Problem tatsächlich als schwierig einzustufen ist, gibt es schlicht zur Zeit keine praktischen Verfahren, die diese Problemstellung, zumindest innerhalb angemessener Zeit, zu lösen. Das Schlüsselpaar hängt dabei von einem Paar von relativ großen Primzahlen ab. Relativ groß bedeutet hier eine Zahl in binärer Darstellung von mehr als 1000 bit. Tatsächlich ist es aber auch schwierig, solche Primzahlen zu identifizieren. Auf der einen Seite stellt sich die Frage, wo man nach diesen großen Primzahlen suchen soll, denn aufgrund der vielen potenziellen Teiler werden große Primzahlen regelmäßig weiter von einander entfernt zu finden sein als kleine. Auf der anderen Seite ist es auch aufwendig, festzustellen, ob eine Zahl, die als mögliche Primzahl identifiziert wurde, auch tatsächlich diese Eigenschaft besitzt.

Nach der Auswahl zweier Primzahlen (von entsprechender Größe) p und q, die nicht ident sein dürfen, wird schließlich die Zahl N = p * g sowie eine Zahl e berechnet bzw zufällig ausgewählt, die zum Produkt (p-1)(q-1) teilerfremd ist. Schließlich wird die Zahl d berechnet, welche zur Zahl e in dem Verhältnis steht, das das Produkt e * d kongruent 1 bezüglich des Modulus (p-1)(q-1) ist.

Der öffentliche Schlüssel besteht dann aus dem Zahlenpaar N und e, der private Schlüssel besteht aus dem Zahlenpaar d und N.

Der Geheimtext C wird schließlich aus dem Klartext K mit folgender Formel unter Zuhilfenahme des öffentlichen Schlüssels berechnet:

$$C \equiv K^e \mod N$$

Umgekehrt kann mit dem geheimen Schlüssel aus dem Klartext K der Geheimtext C errechnet werden:

$$K \equiv C^d \mod N$$

4.4.4 Die elektronische Signatur

Als sozusagen Ableger der Verschlüsselungsverfahren werden auch elektronische Signaturen eingesetzt. Die elektronische Signatur setzt wiederum auf dieselbe Technologie des asymmetrischen Verschlüsselungsverfahrens.

Anders als bei der Verschlüsselung, wo der Inhalt vor einem unbefugten Zugriff geschützt werden soll, wird aber bei der Signatur die Authentizität des Inhalts geschützt und die Identität des Erstellers verifiziert. Daher verschlüsselt der Absender den Inhalt mit seinem privaten Schlüssel. Jeder, der den dazupassenden öffentlichen Schlüssel besitzt kann auf den Inhalt zugreifen, dieser ist somit frei zugänglich. Andererseits kann der Empfänger sicher sein, dass nur der Besitzer des privaten Schlüssels der Absender sein kann. Zudem ist durch die Verschlüsselung auf dem Übertragungsweg der Inhalt vor Veränderungen geschützt.

In der Praxis wird nicht der gesamte Inhalt verschlüsselt, da der Aufwand unverhältnismäßig groß wäre. Mittels einer so genannten Streuwertfunktion (Hash-Funktion) wird der Inhalt in einen kurzen Wert verwandelt. Die Streuwertfunktion zeichnet sich dadurch aus, dass sie unterschiedliche Werte für unterschiedliche Eingaben liefert, so dass eine kleine Veränderung des Ursprungsinhalts zu einem anderen Wert führt. Damit sind Ungleichheiten leicht erkannt. Bei der Signierung wird nun ein Streuwert gebildet und nur dieser verschlüsselt mit dem eigentlichen Inhalt gemeinsam versandt. Der Empfänger entschlüsselt den Streuwert, berechnet seinerseits den Wert aus dem mitgesandten Inhalt. Sind diese identisch, ist die Signatur echt.

4.4.5 Der Einsatz von Verschlüsselung

Durch den Einsatz von Verschlüsselung kann nur derjenige auf den Inhalt zugreifen, der den notwendigen Schlüssel hat, also eine entsprechende Berechtigung besitzt. Damit ist aber auch gewährleistet, dass die Information zwar beliebig kopiert werden kann - gegen den Kopiervorgang an sich ist ein Schutz durch Verschlüsselung nicht gegeben -, die kopierte Information kann aber ohne entsprechenden Schlüssel nicht entschlüsselt und damit verwertet werden. Typischerweise erhält aber nur der berechtigte Nutzer den Schlüssel zur Verfügung gestellt.

Weitere wesentliche Bestandteile im Rahmen von typischen DRM Systemen sind aber neben der Verschlüsselung somit die Verwaltung der Schlüssel als auch die Verteilung der Zugriffsbedingungen.

Der Einsatz von Verschlüsselungstechnologie erfolgt typischerweise durch so genannte „Wrappers“ oder „Packagers“. Dabei wird der zu schützende Inhalt mit Verschlüsselungsmaßnahmen sozusagen eingepackt oder umhüllt.

Park [Park] unterscheidet je nach dem Level der Kontrolle über den digitalen Inhalt 4 unterschiedliche Kategorien, nämlich

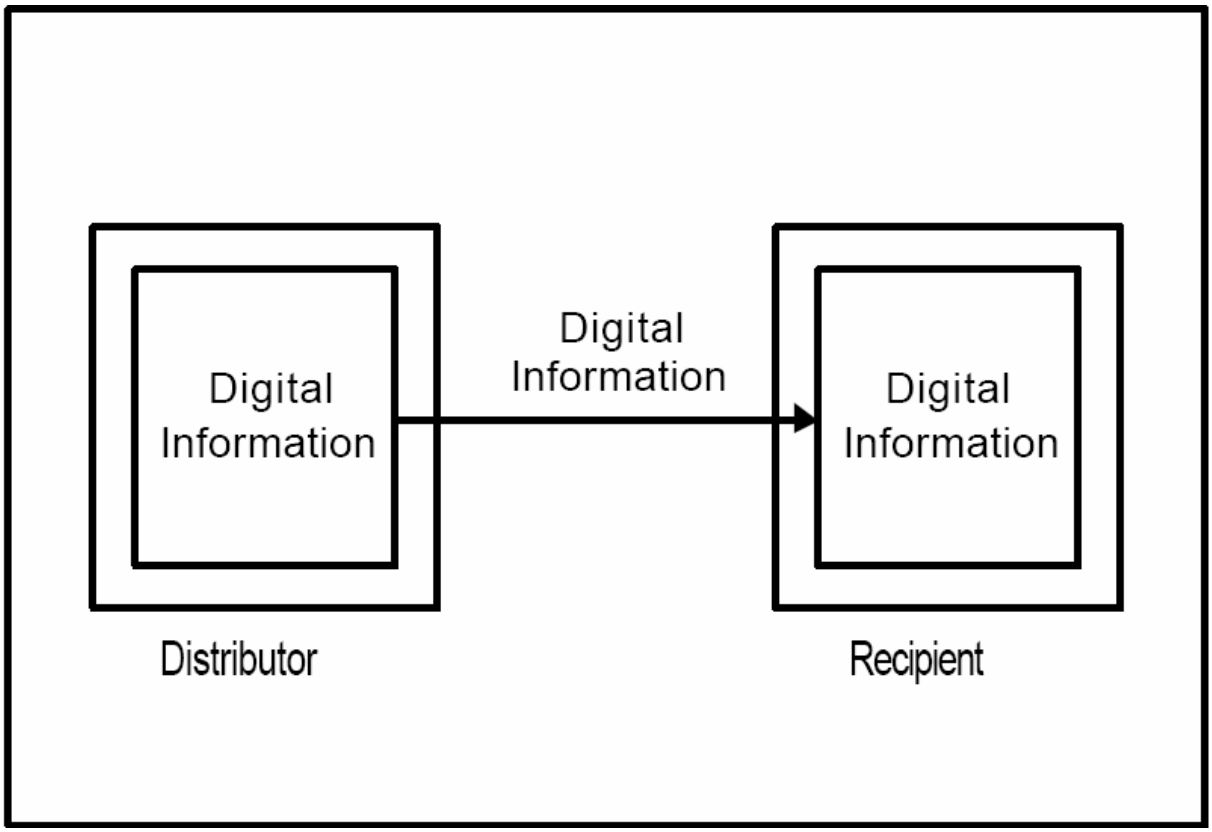
- (1) Keine Kontrolle

- (2) Fixe Kontrolle – hierbei sind die Regeln in dem Empfängergerät fix vorgegeben
- (3) Eingebettete Kontrolle - in diesem Fall sind die Regeln in der verteilten Datei eingebettet
- (4) Externe Kontrolle – die Regeln werden separat von der Datei festgelegt und überprüft.

Bei jeder dieser unterschiedlichen Kontrollstufen sieht er darüber hinaus Unterschiede je nach Verteilungsmethode, ob der Inhalt direkt vom Sender dem Empfänger zugänglich gemacht wird, oder ob eine Stelle („Repository“) dazwischen geschaltet ist.

4.4.5.1 Keine Kontrolle

Simpel eingesetzt kann eine Verschlüsselung nur Sicherheit während der Übermittlung bieten. Sobald der Inhalt beim Empfänger eingetroffen ist und die Entschlüsselung erfolgt ist, liegt die Information im Klartext vor und ist nicht länger geschützt [Miller]. Dies ist typischerweise im Zusammenhang mit dem Schutz der Information unzureichend und nicht endgültig zum Ziel führend.

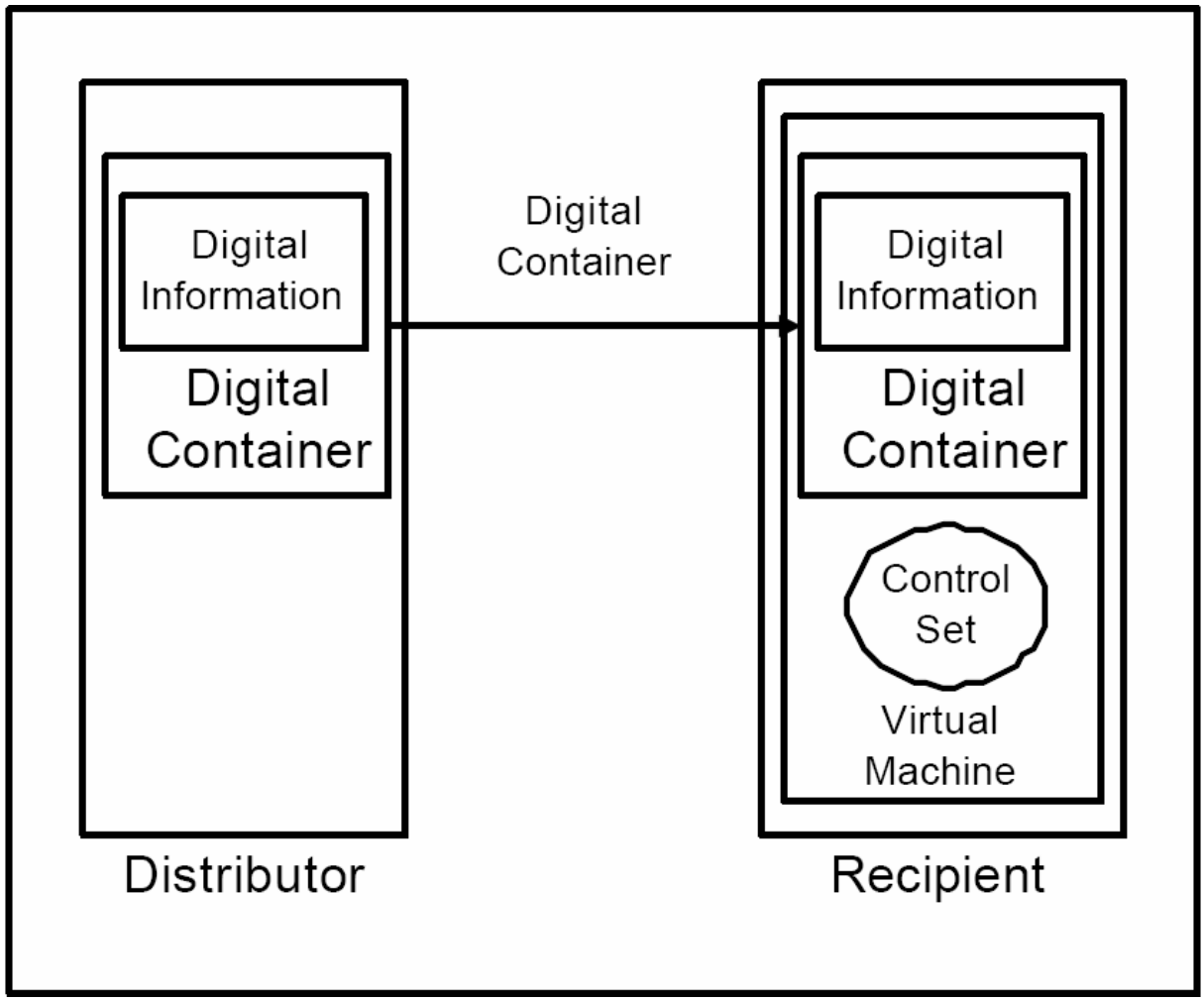


[Abbildung 4: Kontrolllevel 1 für verschlüsselte Inhalte [Park]]

Es gibt somit nach Verteilung keine weitere Kontrolle, wobei die Verteilungsmethode hierbei keinen Unterschied bringt [Park].

4.4.5.2 Die fixe Kontrolle

In diesem Fall sind die Regeln, die auf den digitalen Inhalt angewandt werden können, vorgegeben und im Gerät des Empfängers eingegeben. Nachdem der Empfänger das Gerät erhalten hat und es zum Einsatz eingerichtet ist, können diese Regeln nicht mehr geändert werden.



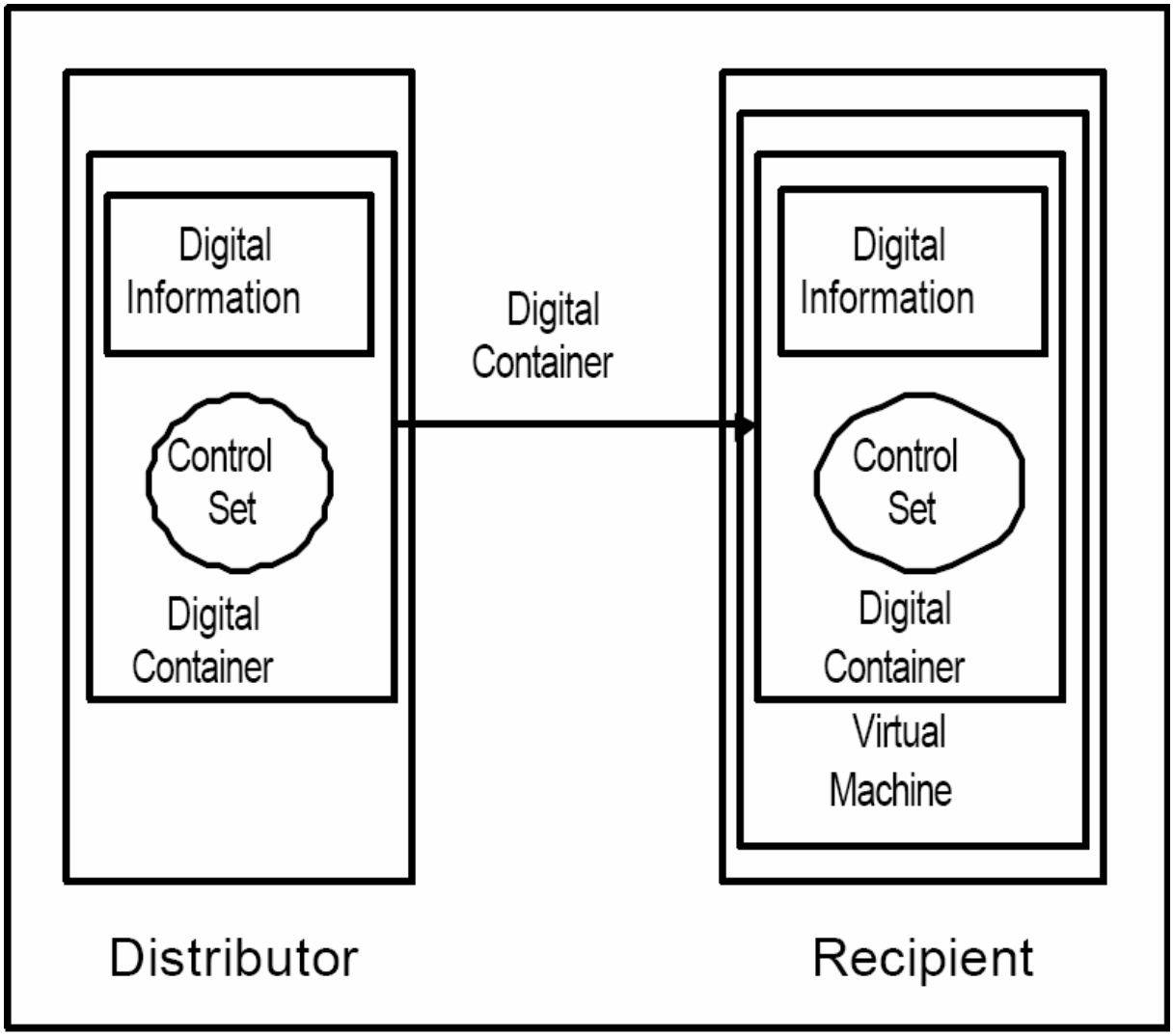
[Abbildung 5: Kontrolllevel 2 für verschlüsselte Inhalte [Park]]

4.4.5.3 Die eingebettete Kontrolle

In dieser Variante werden die Zugriffsbedingungen, also insbesondere die Rechte des jeweiligen Nutzers, gemeinsam mit der eigentlichen Datei verpackt, weshalb man den Begriff des „secure containers“ dafür auch benutzt. Das sind intelligente Software Pakete, die für die entsprechende Sicherheit und die Verwaltung des Inhalts sorgen. Der Inhalt selbst bzw dessen Charakter oder Art spielt dabei keine oder nur eine untergeordnete Rolle.

Solange der Container etwa über das Internet verbreitet wird, stellt er eine Hülle um den Inhalt dar. Diese Hülle wird durch Verschlüsselung erzeugt. Ein digitaler Container ist daher eine verschlüsselte Form eines digitalen Inhalts [Bechtold02].

Auch in diesem Fall kann der Ersteller die Regeln nach Verteilung der Datei nicht mehr verändern, allerdings kann er denselben Inhalt mit unterschiedlichen Regeln zu unterschiedlichen Zeitpunkten oder an unterschiedliche Empfänger versenden.



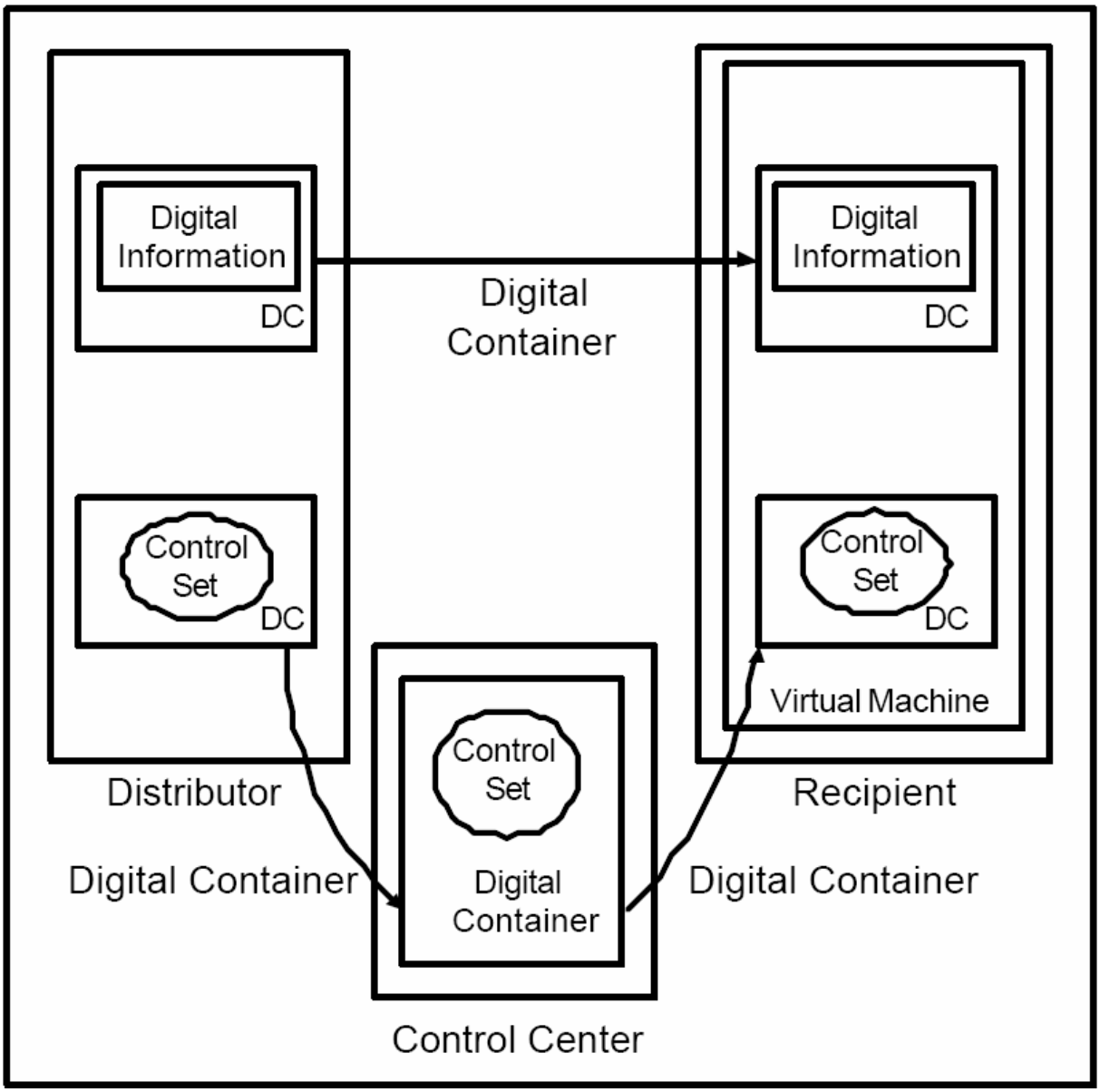
[Abbildung 6: Kontrolllevel 3 für verschlüsselte Inhalte [Park]]

Anders als bei der bloßen Verschlüsselung, die wie vorhin aufgezeigt, ihren Zweck bereits erfüllt hat und damit den Schutz bereits aufgibt, wenn der Inhalt entschlüsselt wird, erfolgt bei dem secure container lediglich der zeitweise Zugriff auf den Inhalt durch Kenntnis des Schlüssels. Der Inhalt wird dadurch nicht ungeschützt preisgegeben. Manche der eingesetzten Lösungen bedürfen keiner speziellen Software beim Empfänger des container, typischerweise wird aber eine angepasste technische Umgebung für den lückenlosen Schutz des Inhaltes notwendig sein.

Neben dem Einsatz von Verschlüsselung spielen insbesondere bei dieser Variante auch spezielle Sprachen zur Beschreibung der Rechte eine wesentliche Rolle, um die Möglichkeiten des Zugriffs über die Alternativen der völligen Blockade oder des völligen Zugriffs ausgefeilter zu gestalten. Die Zugriffskontrolle wird dabei über Metadaten geregelt (siehe dazu im Folgenden).

4.4.5.4 Die externe Kontrolle

Bei dieser Variante sind die Zugriffsbedingungen vom Inhalt als auch vom Empfängergerät getrennt. Die Kontrolle des Zugriffs erfolgt über eine externe Stelle, wobei dies typischerweise über das Internet geschieht. Je nach Ausgestaltung bedarf es hier einer einmaligen Abfrage bei der kontrollierenden Stelle oder einer dauerhaften Verbindung während der Benutzung.



[Abbildung 7: Kontrolllevel 4 für verschlüsselte Inhalte [Park]]

4.4.5.5 Die Authentifizierung

Neben der Verhinderung eines unbefugten Zugriffs werden Verschlüsselungstechniken auch eingesetzt, um die Authentifizierung eines Zugriffs zu überprüfen. Insbesondere bei DRM Systemen, bei denen die Kontrolle über eine zentrale Stelle geregelt wird, etwa weil der Inhalt zentral gespeichert ist und nur von dieser Stelle abgerufen und benutzt werden kann oder weil die zentrale Stelle eine

einmalige Kennung zur Berechtigung des Zugriffs austeilt, ist die Feststellung der Zulässigkeit eines Zugriffs notwendig.

Dabei werden, wie oben zu elektronischen Signaturen ausgeführt, in der Regel asymmetrische Verschlüsselungen verwendet, um die Identität einer Person fest zu stellen. Damit kann nur jene Person auf den Inhalt zugreifen, die sich durch eine gültige elektronische Signatur als berechtigt ausgewiesen hat, jeder andere Zugriff ist allerdings gesperrt.

In einer solchen Individualisierung des Zugriffs ist es auch leicht möglich, Regeln und spezifische Ausgestaltung der Zugriffsrechte ad personam fest zu legen als auch natürlich zu überprüfen und durchzusetzen.

4.4.6 Schutz durch den Einsatz von Verschlüsselung

In einer Betrachtung wieder derjenigen Rechte, die dem Urheber und in anderer Weise berechtigten Personen eingeräumt sind, zeigt sich, dass durch den Einsatz von Verschlüsselungstechniken zwar wieder nicht die Vervielfältigung an sich unterbunden werden kann, aber ein unbefugter Benutzer, der nicht über den geeigneten Schlüssel verfügt, den eigentlichen Inhalt nicht nutzen kann. Der Schutzzweck, nämlich die unbefugte Nutzung scheint damit vollständig erreicht, sofern man der Verschlüsselungstechnologie unterstellt, gänzlich gegen Umgehungsmaßnahmen immun zu sein. Jedenfalls erhöht sich für den Einzelnen der Aufwand das Verschlüsselungssystem zu „knacken“ in hohe Dimensionen.

In dieser Überlegung darf man aber den folgenden Aspekt nicht aussparen: auch wenn durch den Einsatz von „Trusted Computing“ Systemen oder Komponenten (siehe dazu unten) der digitale Inhalt auf seinem gesamten Weg innerhalb des Computersystems geschützt werden kann, so verlässt er doch irgendwo die digitale Domäne, letztlich muss der Inhalt irgendwo an den Benutzer ausgegeben werden, sonst existiert er nur zum Selbstzweck. Beim Wechsel in die analoge Welt ist aber auch endgültig der Schutz durch Verschlüsselung verloren. Ab diesem Zeitpunkt existiert der Inhalt jedenfalls ungeschützt. Er kann dann durch entsprechende Technologien wieder von analog in digital gewandelt werden, so kann etwa ein Bild elektronisch abfotografiert werden oder eine Musikdatei von einem Aufnahmegerät wieder digitalisiert werden. Je nach Umgebung ist der dabei entstehende Qualitätsverlust geringer oder doch erheblich und der „Wert“ einer solchen Kopie wird sicherlich leiden. Gerade bei für den jeweiligen Nutzer als höherwertig eingestuften Inhalten ist aber auch hier sicher noch Interesse relevanter Kreise gegeben. Als Beispiel sei hier die Legion an so genannten „boot legs“ angeführt, wo ein neuer Kinofilm während der Vorführung mit einer Digitalkamera mitgefilmt wird. Die Qualität dieser Aufnahmen sind sowohl in bildlicher als auch akustischer Dimension weit von dem Standard eines herkömmlichen Videos entfernt, dennoch gibt es reges Interesse in jenen Gebieten des Globus, in denen der betreffende Film noch nicht in Kinos gezeigt wird.

Die Technologie der Verschlüsselung kann auch, in entsprechendem Einsatz, etwa als elektronische Signatur, manche der Urheberpersönlichkeitsrechte schützen, da eine Veränderung anhand der Signatur erkannt werden kann.

4.5. Die Metadaten

Metadaten sind im Wesentlichen Informationen, die der eigentlichen Datei als weitere Daten angeschlossen und mitgegeben werden. Sie betreffen nicht den eigentlichen Inhalt, sondern regeln eben die Nutzungsbedingungen oder dienen der näheren Beschreibung der Inhaltsdaten. Bei Metadaten im Zusammenhang mit Digital Rights Management sind insbesondere Informationen über den Inhalt der Datei, also die eigentliche Information selbst, über den ursprünglichen Rechteinhaber, über erteilte Rechte und Verwendungsmöglichkeiten sowie andere Personen, wie Benutzer, von Relevanz.

Diese Metadaten müssen aber auch richtig interpretiert und umgesetzt werden. Dazu werden rights expression languages (Rechtesprachen) eingesetzt. Sie sind formalisierte Protokolle, die die beigefügten Metadaten anwenden können. Wesentlicher Aspekt ist, dass rights expression languanges in maschinenlesbarer Form vorliegen, damit kann der Computer automatisch die Daten verarbeiten.

Ein typischer Ablauf ist hier [Wiebe], dass das Dokument zunächst mit einem symmetrischen Verschlüsselungsverfahren verschlüsselt wird. Dieser Schlüssel wird selbst mit einem asymmetrischen Verfahren verschlüsselt. Wie oben dargestellt, wird durch diese Kombination der Aufwand der Verschlüsselung stark reduziert. Der Schlüssel, nun selbst in verschlüsselter Form, wird gemeinsam mit dem verschlüsselten Dokument in einem Container zusammengefasst und mit Metadaten versehen. Der gesamte Container wird nun seinerseits elektronisch signiert. Durch diese Signatur sind Manipulationen an den Metadaten ausgeschlossen. Auf diese Art und Weise kann der Container auch über freie Kanäle, wie insbesondere das Internet, verteilt werden. Das Empfängersystem prüft nach Erhalt den Container bzw seine Signatur. Ist diese authentifziert, können die Metadaten entnommen werden und regeln die weitere Verwendung durch den Nutzer. Nun kann der Schlüssel mittels des privaten Key des Empfängersystems entschlüsselt werden und dient seinerseits der Entschlüsselung des Inhalts. Dabei werden die in den Metadaten enthaltenen Nutzungsbedingungen berücksichtigt. Eine Aufbewahrung innerhalb des Empfängersystems erfolgt dabei immer verschlüsselt, um eine unbefugte Manipulation zu verhindern.

In einigen Fällen ist eine individuelle Verschlüsselung für jeden Nutzer nicht möglich. Dabei kommen Verfahren zur Anwendung, die die Verschlüsselung des Inhalts mit einem einzigen Schlüssel erlauben, wobei allerdings eine Mehrzahl an Schlüsseln zur Entschlüsselung möglich ist „point-to-multipoint encryption“ [Bechtold02].

Ein derzeitiges technisches Problem der Verwendung von Metadaten ist die Verständigung und Zusammenarbeit zwischen verschiedenen Sprachen. Hier besteht offenbar noch ein Defizit in der Praxis.

Ein relevanter Aspekt an Metadaten ist die Verbindung dieser Daten mit dem eigentlichen Objekt. Um eine Verarbeitung der Daten zu gewährleisten, muss eine dauerhafte Zuordnung erfolgen, die auch (idealerweise) durch einen unzulässigen Vorgang aufgehoben werden darf. Mit anderen Worten, es ist wesentlich, dass der Inhalt nicht von den Metadaten getrennt wird, anderenfalls ist ein ungeschützter oder unkontrollierter Zugriff auf die eigentlich zu schützende Information möglich.

Allerdings ist auch notwendig, dass die Metadaten nicht in einem unverhältnismäßigen Ausmaß zu den eigentlichen digitalen Inhaltsdaten stehen. Gerade die Komprimierung der digitalen Daten stellt ja, wie oben dargestellt, den Charme dieser Verbreitungsform dar. Wenn nun eine Datei durch die Metadaten wesentlich „aufgebläht" würde, ohne dass dadurch der Vorteil für die beteiligten Parteien dies aufwiegt, geht ein wesentlicher Aspekt der Digitalisierung verloren.

4.5.1 Identifier

Als Identifier werden eindeutige Kennzeichnungen von digitalen Daten bezeichnet. Gerade jene DRM Systeme, die interoperabel agieren wollen, setzen voraus, dass eine digitale Einheit eindeutig bezeichnet ist, um ihr die jeweils richtigen Metadaten zuzuordnen. Selbstverständlich muss ein digitales Werk nicht nur einen Identifier besitzen, allerdings muss ein Identifier eine unzweideutige Zuordnung ermöglichen. Ein relativ bekanntes Beispiel ist dabei DOI (Digital Object Identifier). DOI ist ein digitaler, eindeutiger und permanenter Identifier für digitale Objekte, welcher von der DOI Foundation verwaltet wird.

Ein kritisches Kriterium für Identifier ist die dauerhafte Zuordnung. Um ein benutzbares System zu schaffen, darf diese Zuordnung nicht aufgehoben oder etwa durch Zeitablauf ungültig werden. Ein ähnliches Phänomen ist im WWW bekannt, in dem URLs nicht mehr belegt sind, so dass Links „ins Leere" gehen. Für Identifier wäre eine ähnliche Unterbrechung ein nur schwerlich wieder zu behebender Systemfehler.

Ein schwieriger Aspekt für Identifier sind Bearbeitungen eines digitalen Objekts. Soweit Bearbeitungen legitim und vom tatsächlich Berechtigten erfolgen, sollte sich die Zuordnung nicht ändern. Bearbeitungen können aber auch neue Objekte schaffen, die dann unter einem eigenen, separaten Identifier zugänglich sind.

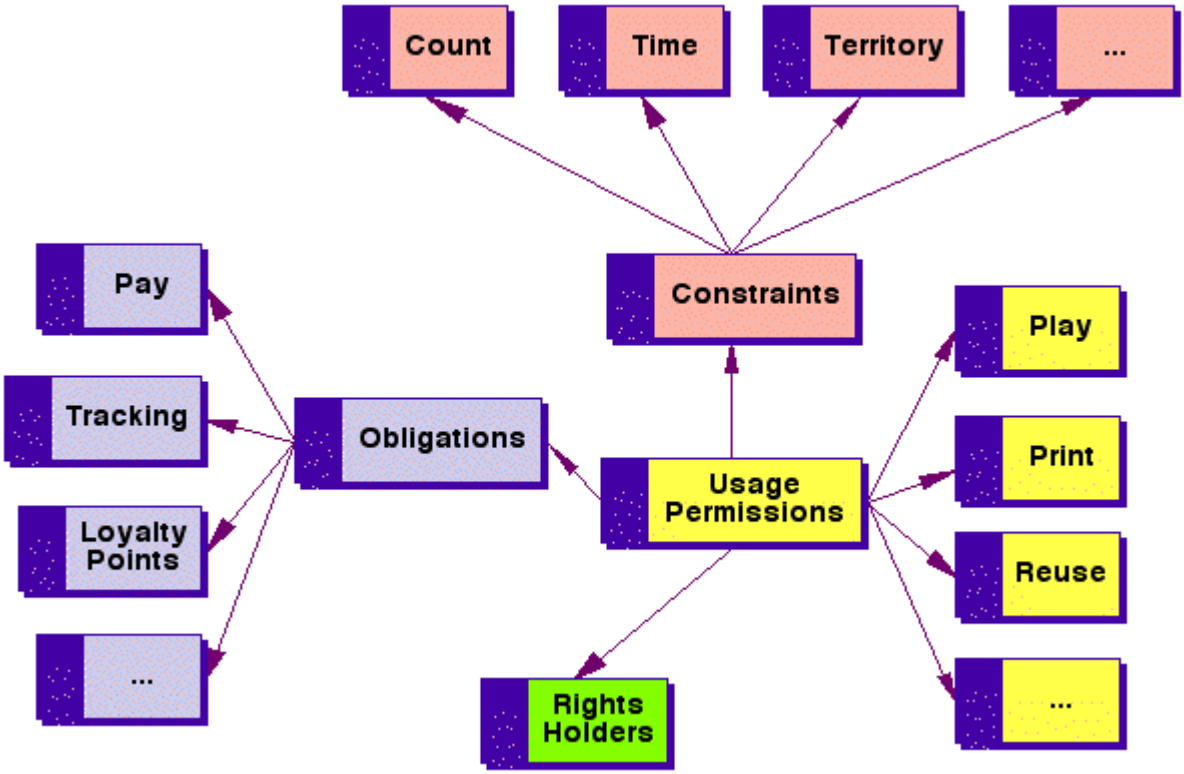
4.5.2 Die Rechtesprachen

Solche Sprachen sind mehr oder weniger umfangreich und flexibel und damit mehr oder weniger mächtig. Einige wichtige Beispiele sind die Open Digital Rights Language (ODRL), welche von der ODRL Initiative entwickelt wurde und eXtensible rights markup language (XrML), eine Sprache von ContentGuard, einem gemeinsamen Unternehmen von Xerox und Microsoft.

Die Rechtesprache muss folglich eine entsprechende Syntax und Semantik besitzen. Typischerweise ist die Problematik einer allfälligen Zahlung für die Nutzung nicht

Gegenstand der Sprache. Grundsätzlich bestehen die rights expression languages aus drei grundlegenden Elementen [Guth].

Zunächst sind hier die Rechte an sich zu nennen, welche Nutzungs- oder Zugriffsrechte auf die digitale Datei darstellen. Diese Rechte können von Voraussetzungen abhängen oder Einschränkungen unterliegen. Beispiele für solche Einschränkungen wären etwa die zahlenmäßige Beschränkung der Zugriffe, der Wahl des Zeitpunkts oder ähnliches. Als weiteres Element ist eine Bezeichnung der digitalen Datei zu nennen. Diese Bezeichnung muss einzigartig sein. Letztlich ist ein wesentliches Element der rights expression languages die Person, welche in einer Beziehung zu der digitalen Datei steht. Dies können der Rechteinhaber, aber auch zB der Nutzer oder andere beteiligte Personen, sein.



[Abbildung 8: Rights expression model [Iannella]]

Rechtesprachen sind dabei sehr mächtig. Wie Berthold darstellt, lassen sich „mit Hilfe einer rights expression language etwa die Berechtigung zum Kopieren, Löschen, Ändern, Einbetten, Ausführen, Exportieren, Extrahieren, Annotieren, Anmerken, Installieren, Sichern, Verleihen, Verkaufen, Weitergeben, Vermieten, Abspielen, Drucken, Anzeigen, Lesen, Wiederherstellen, Übertragen, Deinstallieren, Verifizieren, Sichern, Erhalten, Herausgeben, Besitzen und Zurückholen des Inhalts in maschinenlesbarer Form ausdrücken“. Er hält dabei auch Kritikern entgegen, die anmerken, dass bestimmte Nutzungen durch Digital Rights Management unterbunden werden und damit bisher erlaubte Handlungen nicht mehr ausübbar sind entgegen, dass, „wenn sich Nutzungsarten, die unter einer urheberrechtlichen Schrankenbestimmung erlaubt sind, nicht in einer rights expression language ausdrücken lassen, diese Interessen einfach nicht im DRM System existieren“.

Selbstverständlich muss jene Software, welche dem Nutzer letztlich die digitale Datei ausführen lässt, die rights expression languages entsprechend verstehen. Dafür ist somit ein entsprechender interpreter in den viewer, das ist jene Datei, die den eigentlichen Inhalt für den Menschen verständlich darstellt, also „anzeigt", einzubauen. Der Interpreter „übersetzt" daher die Information aus der rights expression language wieder in eine solche Information, die für die eigentliche Software verständlich ist. Erst danach ist der Inhalt durch die Darstellungssoftware verarbeitbar. Folglich muss der Interpreter daher die Syntax und Semantik aller jener rights expression languages kennen und verstehen, die er „übersetzen" soll [Guth].

4.5.3 XRML

XRML wurde Mitte der 90er Jahre von Xerox entwickelt und ursprünglich unter der Bezeichnung Digital Property Rights Language (DPRL) bekannt. XRML basiert auf der Sprache XML (eXtensible Markup Language), welche Grundlage für mehrere Sprachen wurde und hält sich dabei an die von XML vorgegebenen Regeln. XML selbst definiert als Standard lediglich die Regeln für den Aufbau, ähnlich einer Baumstruktur. Seit ihrer ursprünglichen Erstellung wurde sie konstant weiter entwickelt, insbesondere durch den tatsächlichen Einsatz und Rückmeldung aus der Industrie.

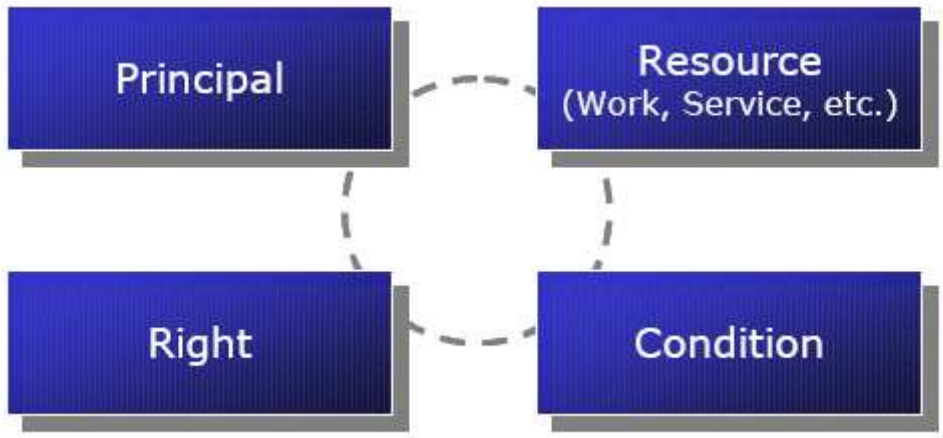
XRML ist heute Ausgangspunkt für eine ganze Reihe an Versuchen einer Rechtesprache, insbesondere einer Standardisierung einer solchen Sprache. Dabei ist wohl insbesondere MPEG-21 zu nennen, welches offiziell von XRML 2.0 als Ausgangspunkt akzeptiert wurde. Bei MPEG-21 handelt es sich um eine Spezifikation der Moving Pictures Expert Group (MPEG), die versucht, einen einheitlichen Standard zur Benennung von Rechten, Ermächtigungen und Einschränkungen für digitalen Inhalt für die Verbreitung solchen Inhalts vom Erzeuger zum Nutzer zu schaffen.

Mit XRML kann jeder, der digitale Inhalte herstellt oder diese danach vertreibt, alle Berechtigten identifizieren, die diese digitalen Inhalte nutzen dürfen. Dabei können die jeweiligen Rechte als auch die Bedingungen der Nutzung spezifiziert werden. Diese Zuordnung von Rechten einerseits zu Berechtigten und die genauen Bedingungen sind die zentrale Funktionalität von XRML, es ist gerade nicht ausreichend, die Rechte alleine zu definieren.

XRML beruht auf einem relativen simplen Modell von vier Objekten und deren Beziehung zu einander. Dieses Grundlagenmodell ist aber erweiterbar und flexibel für Anpassungen. Dabei enthält das „Core Schema" die Definitionen jener vier Konzepte, die eben das Kernstück von XRML bilden. Das sind die Begriffe Prinzipal („principal"), Recht („right"), Mittel („resource") und Bedingung („condition"). Die Beziehung zueinander wird durch den Begriff „grant", also Bewilligung, dargelegt.

Daneben kennt XRML das Standard Extension Schema, welches Definitionen von typischen und generell wertvollen Konzepten, die aber dennoch nicht das eigentliche Kernstück bilden, enthält. Dazu gibt es ein Content Management Schema, das

Konzepte zur Rechteverwaltung für digitale Inhalte, allerdings allgemeiner Natur, definiert.



[Abbildung 9: Das XrML 2.0 Data Model [Contentguard]]

Das Element Prinzipal kapselt dabei Informationen über jene Instanz, der die jeweiligen Rechte eingeräumt werden. Jeder Prinzipal ist dabei eindeutig einem einzigen Objekt zugeordnet, das entsprechend identifizierbar sein muss. Objekt muss dabei aber nicht eine physische Person sein, der Begriff Prinzipal ist abstrakt zu verstehen und kann etwa auch ein Gerät umfassen. Auch verfügt das Objekt Prinzipal über die Funktionalität, eine Authentifizierung, also die Prüfung der Identität vorzunehmen.

Mit „right“ werden wiederum die Rechte bezeichnet, die einem Prinzipal zugeordnet werden. Typischerweise spezifiziert dabei dieses Recht eine Handlung oder eine Kategorie an Handlungen, die der Prinzipal an einer spezifischen Resource vornehmen darf. Im Core Schema sind dabei grundlegende Rechte definiert, sowie ausgeben („issue“), widerrufen („revoke“) und erhalten („obtain“). Diese Rechte können in einer Extension erweitert werden, etwa um DRM spezifische Rechte wie „play“ oder „copy“.

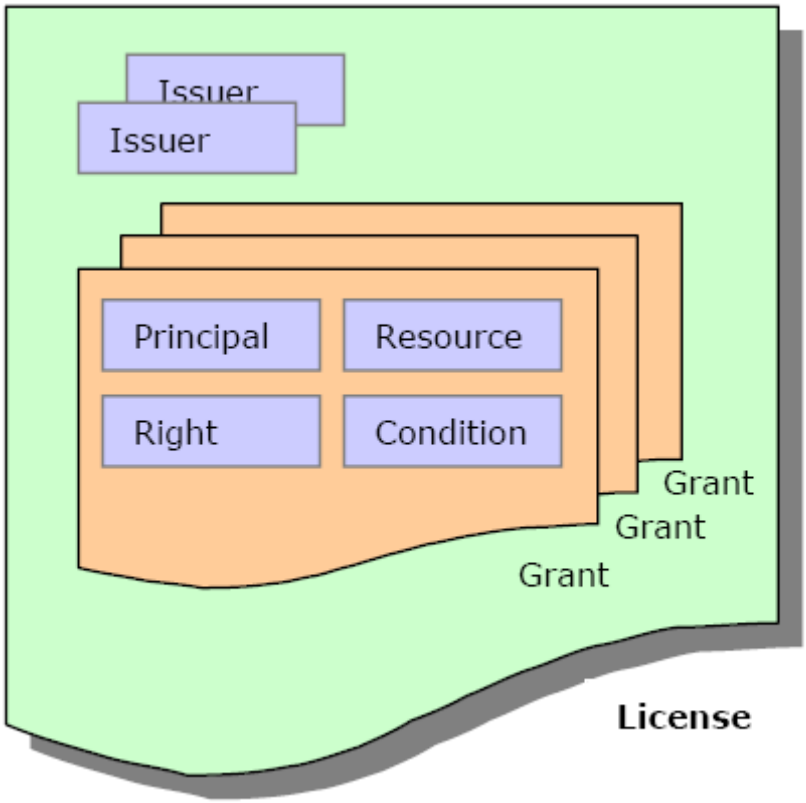
„Resource“ ist nun das jeweilige Objekt, auf das sich das Recht des Prinzipals bezieht. Es ist also der eigentliche Gegenstand der Beziehung. Typischerweise ist die Resource eben ein digitaler Inhalt, es kann aber auch eine Dienstleistung oder anderes sein.

Mit „Condition“ wird schließlich festgelegt, zu welchen Bedingungen die Rechte ausgeübt werden können. In einem einfachen Szenario kann etwa eine zeitliche Beschränkung festgelegt werden, aber auch komplizierte Bedingungen, wie etwa die Abhängigkeit einer Bedingung vom Eintritt einer anderen Bedingung oder die Verknüpfung und der gleichzeitige Eintritt mehrer Bedingungen sind möglich und denkbar.

Das zentrale Konstrukt rund um diese vier Dateneinheiten ist eine Lizenz („license“). Dabei beschreibt die Lizenz die Zuordnung von Rechten und Bedingungen, identifiziert den oder die Prinzipal(en) , die die Lizenz ausgegeben haben und damit

die Bewilligung an die Empfänger begeben haben sowie darüber hinaus gehende Information und Beschreibung der Lizenz, wie etwa ein Ablaufdatum.

Die Bewilligung ist dabei innerhalb der Lizenz jenes Element, das dem Prinzipal die Berechtigung verleiht. Es gibt ihm die Möglichkeit, ein identifiziertes Recht an einer identifizierten Resource auszuüben, wenngleich möglicherweise abhängig von Bedingungen und Auflagen. Die Bewilligung enthält daher Information über den Prinzipal, das ihm zugeordnete Recht, die Resource, auf die sich das Recht bezieht, und die Bedingungen, die für die Ausübung des Rechts notwendigerweise vorweg erfüllt sein müssen.



[Abbildung 10: Das zentrale Element Licence in XrML [Contentguard]]

Im Core Schema hat dabei XRML eine Spezifikation, so dass jedes Element Unterelemente enthalten kann. Das Element „license“, das einzelne Grants enthält, und so zu sagen ein Container für Grants ist, verfügt über die folgenden Unterfelder:

Title — Dieser enthält eine beschreibende Darstellung über die Lizenz, die vor allem für die menschlichen Benutzer gedacht ist und für die Interpretation durch die Maschinen weniger Relevanz besitzt.

Grant/GrantGroup — Über dieses Element werden Genehmigungen durchgestellt, jede License muss zumindest einen Grant enthalten. Über grantGroup können Grants gebündelt werden.

Issuer — In diesem Element sind zwei Angaben enthalten, nämlich die Daten über den Issuer bzw die Umstände gemäß derer er die Lizenz erteilt

(etwa Datumsangaben, Widerrufsmechanismen) und eine digitale Signatur für den Issuer.

Inventory — Durch dieses Element soll Redundanz vermindert werden, indem Elemente, die mehrmals verwendet werden, definiert werden können.

(Any) — Dieses Element ist ein Platzhalter für Erweiterungen, aufgrund dessen weitere Informationen und Inhalte eingestellt werden können, die nicht Bestandteil des Core Schema sind.

EncryptedLicense — Mit diesem Hilfsmittel kann die Lizenz verschlüsselt werden und damit vor Nichtberechtigten verborgen bleiben.

Das Element Grant, das geradezu das Kernstück der Semantik in XRML bildet, verfügt über folgende Unterelemente:

ForAll — Dieses Element definiert eine Variable, die Mitglieder einer Gruppe identifiziert und auf die von verschiedenen Elementen des Grant zugegriffen werden kann, so dass ein Grant für mehrere Principals, Rights, Resources oder Conditions anwendbar ist.

Principal — Hiermit wird der Principal identifiziert. Dieses Element wird oft durch andere Ersatzelemente ersetzt, etwa „Keyholder".

Right — Für Right gilt ähnliches wie für Principal, hier wird das Right spezifiziert, auch hier wird oft ein anderes Element eingesetzt, etwa ein spezifisches Recht, das in der Content Extension definiert ist.

Resource — Für Resource gilt ähnliches wie für Principal, hier wird die Resource, für die das Right gilt, spezifiziert. Auch hier wird oft ein anderes Element eingesetzt, etwa eine spezifische Resource, die in der Content Extension definiert ist.

Condition — Jene Condition, die für das Right vorliegen muss, damit es ausgeübt werden darf.

DelegationControl — Der Issuer kann definieren, ob der Grant an weitere Personen weitergegeben werden darf. Es ist auch möglich, Grundsätze für die Umstände festzulegen, wann eine solche Delegation erfolgen darf.

EncryptedGrant — Mit diesem Element wird angegeben, dass der Grant verschlüsselt ist.

Das Element Principal, identifiziert entweder über das Unterelement Keyholder einen spezifischen Prinzipal oder bündelt eine Menge an Prinzipalen mittels „AllPrincipal".

Das Element Right verfügt über folgende Unterelemente:

Issue Dieses Recht erlaubt, Lizenzen zu vergeben. Diese Möglichkeit ist insbesondere dort notwendig, wo in einer Kette von Gliedern mehrere berechtigt sein sollen, Lizenzen zu erteilen, etwa weil die Verteilung über eine hierarchische Ebene erfolgt. Damit wird auch Superdistribution ermöglicht.

Revoke Mit diesem Recht kann einer Person das Recht eingeräumt werden, die Signatur des Principals zu widerrufen. Dies dient vor allem in Umgebungen, wo eine spezifische Stelle beauftragt ist, die Signaturen zu überwachen und selbständig zu widerrufen, falls entsprechende Umstände eintreten.

PossessProperty Mit diesem Element werden eigentümergleiche Rechte eingeräumt.

Obtain Hiermit wird ermöglich, weitere Rechte zu erlangen, konzeptuell entspricht dies einem Angebot oder Bewerbung weiterer Rechte.

Das Element Resource kennzeichnet die benutzte Resource und verfügt sonst über keine Unterelemente. Resource kann dabei eine Datei selbst oder auch der Speicherort, etwa eine Website, sein.

Das Element Condition schließlich verfügt über die folgenden Unterelemente:

AllConditions Hierdurch wird angegeben, dass alle nachfolgenden Conditions erfüllt sein müssen, somit kumulativ vorliegen müssen, um das Right „freizugeben".

ValidityInterval Mit diesem Parameter wird ein Zeitintervall festgelegt.

RevocationFreshness Diese Angabe legt fest, nach welchem Zeitverlauf die Gültigkeit der Signatur überprüft werden muss, um festzustellen, ob diese nicht zwischenzeitig widerrufen worden ist.

ExistRight Mit diesem Feld wird definiert, dass der Principal ein spezifisches Recht haben muss, um ein anderes Right ausüben zu können, wobei dieses Recht nicht notwendigerweise gültig sein muss.

PrerequisiteRight Diese Angabe ist ähnlich wie ExistRight, nur muss diesmal das erforderliche Recht notwendigerweise gültig sein.

XRML ist damit eine universelle Methode, Rechte und Nutzungsbedingungen von digitalen Inhalten und Diensten sicher zu charakterisieren und im Gebrauch durchzusetzen. Sie war lange Zeit der Vorreiter der Rechtesprachen und dürfte die zurzeit einzige Rechtesprache sein, die tatsächlich in echten, auf dem Markt befindlichen, DRM Systemen eingesetzt wird. Ein besonderes Augenmerk wurde bei XRML auch auf die Interoperabilität gelegt, so dass eine Zusammenarbeit zwischen mehreren unterschiedlichen DRM Systemen, die auf XRML basieren, möglich sein soll. Auch die Vertrauenswürdigkeit verschiedener Komponenten oder Systeme ist ein wichtiges Element, das bei XRML berücksichtigt wurde. Da XRML Verschlüsselung einsetzt und zulässt, ist auch die Vertraulichkeit der Lizenz

gewährleistet und diese vor unberechtigten Zugriffen durch andere Parteien geschützt.

XRML basiert auf der XML Hierarchie und verwendet Elemente, denen entsprechende Attribute zugewiesen sein können. Dabei sind die Art und Anzahl der Elemente vorgegeben, die Attribute, die mit jedem Element verknüpft sein können, sowie ob es, und wenn ja welche, Sub-Elemente enthalten kann.

4.5.4 Die Metadaten und das Urheberrecht

Die Metadaten oder konkreter die Rechtesprachen, wenn richtig eingesetzt und umgesetzt, können nun tatsächlich die Urheberrechte schützen. Dabei ist eben das Umfeld notwendig, etwa insbesondere eine solche Verknüpfung der Metadaten mit dem eigentlichen Inhalt, die eine Manipulation der Metadaten ausschließt. Zudem bedarf es eines Abspielgeräts, das die Metadaten einerseits versteht, andererseits auch tatsächlich umsetzen kann.

Mit den Metadaten kann eben genau festgelegt werden, welche zulässigen Handlungen gesetzt werden dürfen. Somit ist sowohl die Vervielfältigung geschützt, als auch andere Verwertungsrechte. Theoretisch sollte es auch möglich sein, Nutzungen des geschützten Stücks, welche urheberrechtlich zulässig sind, mit Rechtesprachen zuzulassen. Allerdings bedürfte es dazu einer relativ präzisen Definition dieser zulässigen Nutzungen und einer Überprüfung der jeweiligen Bedingungen, die eine komplexe Außenwelt voraussetzt. Zudem sind diese freien Nutzungen oftmals nicht simpel formuliert und bedingt, wie etwa eine Privatkopie oder noch mehr „fair use“ nach US-amerikanischer Denkweise, so dass die tatsächliche Umsetzung wohl (noch) an der Komplexität dieser Problematik scheitert.

Auch die Urheberpersönlichkeitsrechte könnten durch entsprechende Metadaten geschützt werden, da eben Angaben über den Urheber innerhalb der Metadaten Platz finden könnten.

4.6. Trusted Computing

Ein wesentlicher Aspekt am technologischen Schutz von digitalen Inhalten - vor allem durch Verschlüsselung - ist die Tatsache, dass zu irgend einem Zeitpunkt die Information ungeschützt vorliegt, ja vorliegen muss, da nur so diese Information durch die Software bearbeitet und damit eigentlich verwendet werden kann. Zu diesem Zeitpunkt muss die Datei die schützende Schale verlassen. Man denke hier daran, dass eine zunächst geschützte MP3 Datei ja auch ausgegeben werden muss, also in Ton verwandelt werden muss, der vom Hörer schließlich wahrgenommen wird. In einem herkömmlichen Computer muss dabei die Information zunächst der Soundkarte zugeführt werden und schließlich über die Lautsprecher ausgegeben werden. Hier liegt auch die mögliche Angriffstelle für allfällige Versuche, den Inhalt ungeschützt aufzufangen. Während dieser Übertragung von zunächst geschütztem Inhalt innerhalb des Computersystems oder auch allenfalls zu Komponenten des Systems außerhalb des eigentlichen Rechners kann von einem entsprechend engagiertem Benutzer die nunmehr ungeschützte Information so zu sagen „frei“

gelesen und allenfalls auch kopiert werden. Oftmals wird gerade aus diesem Grund Trusted Computing und Digital Rights Management beinahe synonym verwendet, jedenfalls aber als kongruente Technologien angesehen. Ja, manchmal wird offenbar sogar behauptet, dass Digital Rights Management ohne Trusted Computing nicht möglich sei, da eben sonst die oben aufgezeigten Lücken übrig blieben. Richtigerweise handelt es sich aber um von einander unabhängige Ideen, die aber unzweifelhaft zusammen eingesetzt werden können und im gemeinsamen Einsatz Synergieeffekte erzielen und somit das gewünschte Schutzniveau erhöhen. Die Kritik, die beide Techniken einstecken müssen, orientiert sich an derselben Zielrichtung und ähnlichen Argumenten.

Während daher andere Komponenten und Verfahren von Digital Rights Management auf der Software Seite angesiedelt sind, ist auch die Hardware Seite nicht zu vernachlässigen. Auch die Hardware und natürlich das Betriebssystem müssen den zunächst softwareseitig dargebotenen Schutz weiter gewährleisten. Andernfalls könnte auf dieser Ebene der digitale Inhalt ausgelesen werden. Zu denken wäre hier auch etwa an Emulatoren, die das Verhalten einer Komponente widerspiegeln, tatsächlich aber nur den Schutz, um die Information entfernen, und Zugriff ermöglichen.

An dieser Stelle setzt das Konzept von Trusted Computing an, das aufgrund der oben angeführten Konstellation aber eine gute Ergänzung zu anderen Schutzmechanismen in Digital Rights Management bieten könnte.

4.6.1 Was ist Trusted Computing?

Trusted Computing wurde zunächst ins Leben gerufen, um ein Netzwerk von Computern zu erschaffen, die sich untereinander vertrauen können. Der ursprüngliche Beweggrund hatte daher keine Verbindung mit Digital Rights Management, sonder ergab sich aus der Entwicklung der Computer, die von einem stand-alone-Gerät durch zunehmende Vernetzung, insbesondere über das Internet, nun einer Vielzahl von Gegenübern ausgesetzt war, deren Identität und Intention nicht bekannt war. Vorreiter dieser Innovation sind die Trusted Computing Platform Alliance (TCPA) und die Trusted Computing Group, welche sich später aus der Trusted Computing Platform Alliance gebildet hat. Trusted Computing kann dabei einzelne Dateien oder besonders sensitive Daten schützen, als auch einzelne Komponenten des Systems auf den Zustand bzw Veränderung prüfen.

Kernstück der derzeitigen Spezifikation von Trusted Computing ist dabei ein spezieller Chip (der Trusted Platform Module, „TPM"), der in den PC integriert werden muss. Er ähnelt einer smartcard und sammelt zunächst, ausgehend von einem vertrauenswürdigen Zustand, Informationen über die anderen Komponenten als auch Software. Sofern der TPM eine Veränderung der Umgebung identifiziert, verweigert er den Zugriff auf die von ihm verwaltete Komponente.

Daneben gibt es als weitere Bestandteile noch den Core Root of Trust for Measurement und den Trusted Platform Support Service. Das Core Root of Trust for Measurement ist eine Software, die während des Startens des Betriebssystems

(„boot“) ausgeführt wird und ein sicheres Booten ermöglicht. Der Trusted Platform Support Service bildet die Schnittstelle zwischen TPM und Firmware bzw Betriebssystem.

4.6.2 Die Funktionsweise von Trusted Computing

Das System funktioniert dabei folgendermaßen: Ist TCPA aktiviert, überprüft der Chip zunächst das BIOS und startet die CPU. Danach testet er alle BIOS-Erweiterungen der Steckkarten im Rechner, bevor er den Prozessor auf sie zugreifen lässt. Bei jedem Schritt speichert der TCPA-Chip eine Prüfsumme (SHA1 Hash) ab und bewertet danach den Zustand des PC. Der SHA1-Hash-Algorithmus berechnet aus einem beliebig langen Datenstrom wie dem BIOS-Inhalt und einem Schlüssel einen 160 Bit langen eindeutigen Wert. Ändert jemand das BIOS oder verwendet einen anderen Schlüssel, entsteht eine andere Prüfsumme und TCPA schlägt Alarm.

Im nächsten Schritt wird die Platte auf TCPA-Konformität geprüft, dann der Bootsektor, der Betriebssystem-Lader, der Kernel, die Gerätetreiber und alles, was zum Start des Betriebssystems in den Speicher geladen wird.

Kommt es an einer Stelle zu Unstimmigkeiten - etwa weil der Anwender neue Hardware eingebaut hat, dann ist der Rechner nicht mehr TCPA-konform und muss neu zertifiziert werden. Dies geschieht online anhand einer Liste mit geprüfter Hardware (HCL) und gesperrten Seriennummern (SRL). [Plura]

Eine zentrale Rolle spielt der Endorsement Key. Dieser Schlüssel ist für jedes TPM einzigartig und existiert kein zweites Mal, dh jeder Computer mit einem TPM kann sich über diesen Schlüssel als genau ein bestimmter Rechner ausweisen. Der Endorsement Key wird entweder direkt im TPM erzeugt oder extern erzeugt und dann im TPM abgelegt. Im TPM können weitere Schlüssel vom Endorsement Key abgeleitet werden.

Neben dem Endorsement Key gibt es im TPM den Storage Root Key. Dieser Schlüssel wird im TPM erzeugt und dient als Grundlage zur Verschlüsselung weiterer Schlüssel. Mit diesen Schlüsseln können dann Daten und Speicherbereiche verschlüsselt werden. Da der Storage Root Key ähnlich wie der Endorsement Key nur im TPM existiert und nicht von externen Stellen ausgelesen werden kann, sind auch die durch den Storage Root Key geschützten Schlüssel sicher.

Trusted Computing umfasst insgesamt fünf grundlegende Konzepte, von denen einige für Digital Rights Management relevant sind.

„Secure input and output“ bezieht sich dabei auf einen Schutz der Ein- und Ausgabe zwischen dem Benutzer und der Software. Damit soll der Versuch unterbunden werden, Eingaben des Benutzers auf dem Weg im System abzufangen, etwa durch Software, die jede einzelne Tasteneingabe abfängt („keyboard loggers“). Im Rahmen des Trusted Computing wird über checksums festgestellt, dass die Software, welche die Eingabe letztlich erhalten soll, nicht manipuliert wurde. Mit anderen Worten kann somit eine unerlaubte Beeinflussung erkannt werden.

In einer anderen Implementierung können spezielle Bereiche des Speichers spezifisch geschützt werden („Memory curtaining"). Beispielsweise kann jener Bereich des Speichers, in dem Verschlüsselungsinformation abgelegt ist, gesperrt werden und nur mit spezieller Berechtigung freigegeben werden.

Bei „sealed storage" ist der Zugriff auf Daten nur bei Vorliegen derselben Konfiguration von Software und Hardware erlaubt. Auf diese Weise ist etwa eine Weitergabe von Daten unterbunden, da diese in einer anderen Umgebung nicht benutzbar sind.

Mittels „remote attestation" ist es möglich, Veränderungen an einem Computer durch Fernzugriff festzustellen. Dieses Recht kann etwa Dritten eingeräumt werden, die somit den Zustand eines spezifischen Systems überwachen können.

4.6.3 Trusted Computing und das Urheberrecht

In Kombination dieser oben dargestellten verschiedenen Konzepte kann etwa ein Musikstück, das auf einem System abgespielt wird, nicht zwischen dem Speicher und dem Lautsprecher abgefangen werden. Durch memory curtaining ist der Zugriff im Arbeitsspeicher nicht möglich, wenn es auf einem anderen Gerät abgespielt würde oder nachdem es auf Festplatte gespeichert wurde. Denn beide dieser Vorgänge verändern die Systemumgebung – dadurch wird ein neuerliches Abspielen verhindert. Durch die Funktion remote attestation kann sogar von außen überprüft werden, etwa durch die lizenzierende Stelle, dass das Abspielgerät lizenziert und berechtigt ist.

Mit einer solchen Funktion können die Ideen des Trusted Computing dazu genutzt werden, den Schutz von Rechten an digitalen Inhalten zu verstärken. Trusted Computing kann keinerlei Rechte an digitalen Inhalten erzeugen und bietet auch keinen unmittelbaren, allein stehenden Schutz von digitalen Inhalten, kann aber in Verbindung mit anderen Techniken als Ergänzung zum verstärkten Schutz dienen.

Trusted Computing oder dessen Elemente kann dabei in Form von secure input and output das Vervielfältigungsrecht schützen bzw Verstöße gegen unerlaubte Kopien verhindern, sofern dieser Schutz durch die weitere Umgebung geboten ist.

Im Wirken von sealed storage und remote attestation ist es zwar nicht möglich, die Vervielfältigung an sich zu unterbinden, aber eine so erstellte Kopie wird nutzlos, weil sie auf einem anderen System nicht verwendbar ist.

Auch die übrigen Verwertungsrechte, aber nicht die sonstige Urheberrechte, werden durch Trusted Computing mit Schutz versehen.

Trusted Computing kann aus meiner Sicht aber selbstverständlich eine technische Schutzmaßnahme im Sinne der oben angeführten gesetzlichen Regelungen des UrhG darstellen. Eine Umgehung dieses Schutzes ist somit nach den einschlägigen Regelungen verboten. Über diesem Umstand erzielt vielleicht Trusted Computing wiederum ein höheres Schutzniveau.

4.6.4 Trusted Computing und der Datenschutz

Wie Bechtold allerdings aufzeigt, ergibt sich durch Trusted Computing aber auch eine möglicherweise unzulässige Korrelation mit dem Datenschutz.

Da jeder TPM angeblich, wenn gleich von der Trusted Computing Group nicht öffentlich zugegeben, eine eindeutige Kennung besitzt, kann mittels Trusted Computing jeder Computer eindeutig identifiziert werden und allenfalls könnte diese Information von Dritten verwendet werden, etwa um ein Nutzerprofil auszuarbeiten. Zwar sehen die TCPA-Spezifikationen die Möglichkeit vor, anonyme Identitäten anzunehmen, ähnlich einem Pseudonym, ein einziger Nutzer kann auch mehrere solcher Pseudonyme verwenden, allerdings ist (noch) nicht sichergestellt, dass nicht doch auf die tatsächliche Identität geschlossen werden kann. Diese Unsicherheit resultiert aus dem Umstand, dass die Zuordnung durch entsprechend vertrauenswürdige zwischengeschaltete dritte Parteien (Trusted Third Party) erfolgen muss. Wer eine solche Funktion übernehmen kann und wird, steht aber nicht fest.

Auf der anderen Seite wird oftmals positiv dargestellt, dass Trusted Computing bzw der TPM auch einen konstruktiven Beitrag zum Datenschutz bieten kann, da durch den Einsatz dieser Technologie sensible Daten, etwa auch persönliche Daten, besser geschützt werden können und die Datensicherheit insgesamt erhöht wird.

Die TPM Funktionalität kann auch ausgeschaltet werden, der Benutzer kann also frei und aus eigenem wählen, ob er die Möglichkeiten tatsächlich für sich verwenden möchte.

4.7. Digitale Wasserzeichen („Watermarking“)

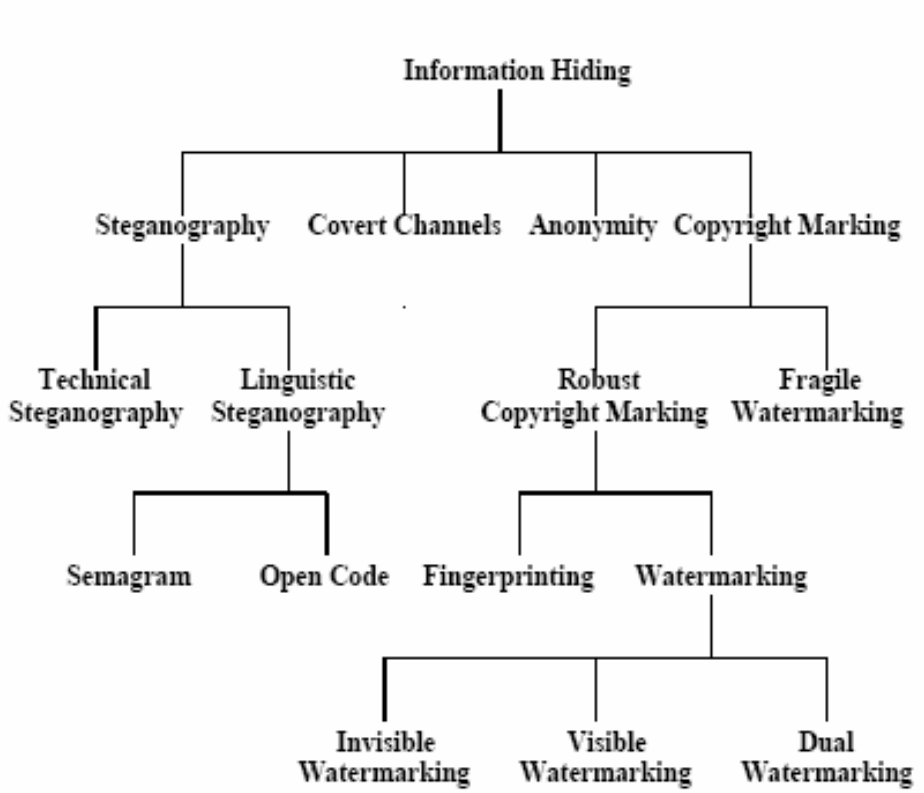


Figure 1: Information Hiding Techniques

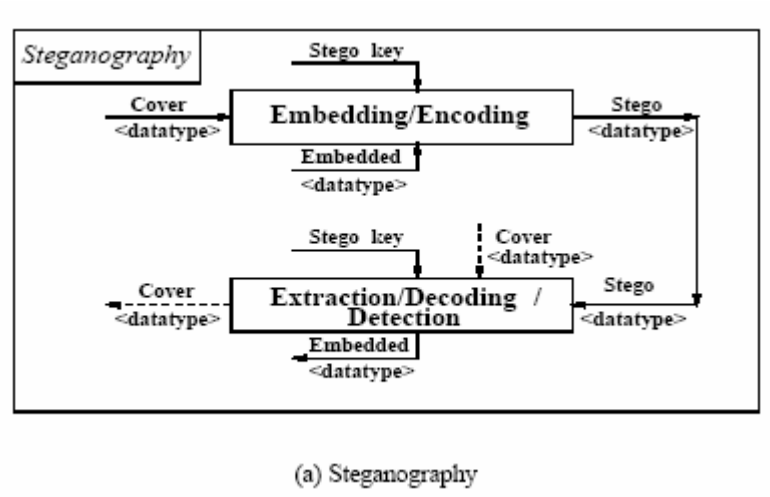
[Abbildung 11: Übersicht über Techniken der Datenkapselung [Mohanty]]

4.7.1 Grundsätzliches

Eine der derzeit im Rahmen von Digital Rights Management eingesetzten Technologien sind so genannte digitale Wasserzeichen („Watermarking“). Als Wasserzeichen wurde bereits herkömmlicherweise im Papier ein nur in der Durchsicht erscheinendes Muster, das zur Charakterisierung von Papiersorten oder als Markenzeichen oder Echtheitsnachweis dient, bezeichnet [Rosenblatt02]. Noch heute werden Wasserzeichen etwa zur Kennzeichnung bzw als Echtheitsmerkmal von Banknoten eingesetzt, obgleich diese Methode in ihren Grundlagen einige hundert Jahre alt ist.

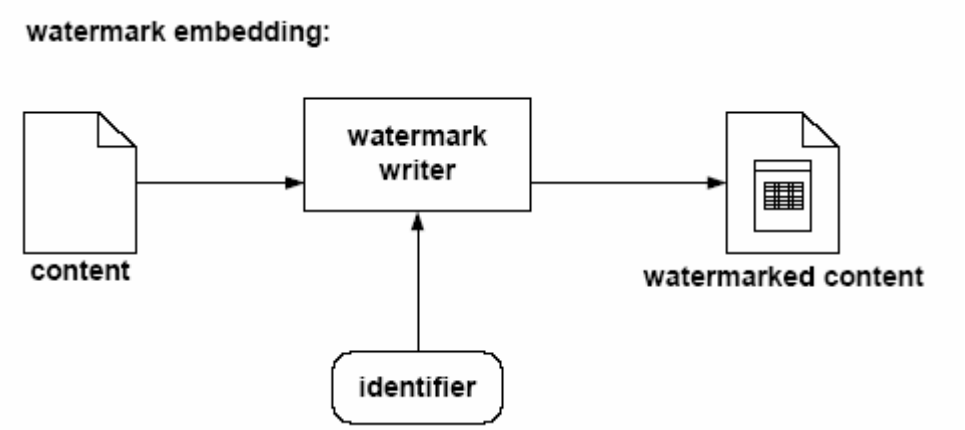
Bei digitalen Wasserzeichen verwendet man technologische Maßnahmen, um zusätzliche Information direkt in den originalen Inhalt eines digitalen Werks einzubetten [Podilchuk]. Ähnlich wie beim Wasserzeichen ist dabei diese Information zwar enthalten, aber nicht notwendigerweise unmittelbar erkennbar. Dies erfolgt auf solche Weise, dass idealerweise bei der gewöhnlichen Darstellung oder Wiedergabe des Inhaltes keine Veränderung für den gewöhnlichen Betrachter oder Verwender erkennbar ist. Watermarking basiert daher auf der in dieser Hinsicht eingeschränkten Wahrnehmungsfähigkeit, weil der Mensch für ihn unwichtige Informationen ausblendet. Ähnlicher Mechanismen bedient sich etwa die verlustbehaftete Kompressionstechnologie [Miller].

Diese Technik ist auch unter den Bezeichnungen „Information Hiding“ oder Steganographie bekannt, die schon seit langer Zeit für „versteckten Botschaften“ eingesetzt wird.



[Abbildung 12: Beschreibung des Vorgangs der Steganographie [Mohanty]]

Etwas abstrakter kann man Watermarking als einen Prozess darstellen, der zwei verschiedene Informationen zusammenführt, ohne dass diese von unterschiedlichen Erkennungsprozessen wieder ausgelesen werden können. Eine Quelle ist dabei die Mediumsdatei, wie etwa ein Photo oder Musikstück, die vom menschlichen Betrachter erkannt wird. Die andere ist das Wasserzeichen, die von einem entsprechenden Detektor erkannt wird [Miller].



[Abbildung 13: Darstellung der Einbettung eines Wasserzeichens [Schmucker]]

Wasserzeichen können bei beliebigen Dateien eingesetzt werden, im Wesentlichen kommen sie aber bei Bilddateien zum Einsatz.

Der spiegelbildliche Part des Verfahrens ist das Auslesen oder Erkennen des Wasserzeichens. Hierbei wird entweder festgestellt, dass ein Wasserzeichen überhaupt vorhanden ist oder es wird das Wasserzeichen insgesamt ausgelesen und allenfalls die darin enthaltene Information weiter verarbeitet.

Denkbar ist natürlich auch die Kombination des Einsatzes eines Wasserzeichens mit anderen Techniken, insbesondere der Verschlüsselung. Dabei kann etwa das

Wasserzeichen vor dem Einbetten verschlüsselt werden, damit auch im Falle eines unbefugten Auslesens diese Information nicht unberechtigterweise verarbeitet werden kann.

4.7.2 Die Merkmale eines digitalen Wasserzeichens

4.7.2.1 Die Erkennbarkeit

Bei digitalen Wasserzeichen unterscheidet man gewöhnlich zwischen sichtbaren und unsichtbaren Wasserzeichen. Diese Unterscheidung nimmt lediglich zum Ansatz, ob das Vorliegen eines Wasserzeichens für den Benutzer offenkundig erkennbar ist oder nicht, etwa ob bei der Darstellung eines Bildes in diesem erkennbar ein Logo oder ähnliches Kennzeichnungsmerkmal dargestellt ist. Manche bezeichnen diese Form auch als „Tattoo“, also ähnlich sichtbar und unveränderbar wie eine Tätowierung des Bildes.

Ein gewollt unsichtbares Wasserzeichen sollte somit weder erkennbar sein, aber auch idealerweise die Bildqualität nicht beeinträchtigen. Unsichtbare Wasserzeichen sollten auch auf anderem Weg als der Betrachtung des Bildes nicht erkennbar sein bzw es sollte auch keine anderen Hinweise auf ihre Existenz und Einbindung in einer Datei geben. Die Zufälligkeit und Unverdächtigkeit der eingebrachten Information sind dabei für die Wasserzeichentechnologie von Bedeutung.

Ein sichtbares Wasserzeichen sollte sowohl in farbigen als auch monochromen Darstellungen sichtbar bleiben. Andererseits sollte es aber auch den eigentlichen Bildinhalt nicht, zumindest nicht wesentlich, stören. Gerade bei einem sichtbaren Wasserzeichen wird die Robustheit (siehe sogleich) noch stärker ausgeprägt sein müssen.

Miller/Cox [Miller] verwenden an Stelle des Begriffs Erkennbarkeit („perceptility“) den Begriff „fidelity“. Gerade bei Veränderungen der Datei im Wege von Kompressionen könnten unerkennbare Wasserzeichen stark verändert oder gar entfernt werden.

Für Zwecke des Digital Rights Management werden klassischerweise unsichtbare digitale Wasserzeichen eingesetzt. Die digitale Datei enthält somit Information über den Urheber, welche dem Nutzer unmittelbar, also im Rahmen der gewöhnlichen Darstellung oder Wiedergabe des Inhaltes, nicht zugänglich sind.

4.7.2.2 Die Robustheit

Robustheit ist die Eigenschaft, dass die als Wasserzeichen verpackte Information auch nach Veränderung der Daten noch vorhanden ist sowie immer noch in ausreichender Qualität vorliegt, so dass sie für einen Detektor erkennbar ist. [Miller] Idealerweise sollte ein Wasserzeichen jede Veränderung, sei diese gewollt oder ungewollt, einer Datei, in diesem Zusammenhang insbesondere von Bilddateien, „überleben“. Ein Wasserzeichen darf nicht „gelöscht“, also aus der gekennzeichneten Datei unberechtigterweise entfernt werden, ohne dass dies auch zu einer

Beschädigung oder Zerstörung der Datei selbst oder deren Inhalts führt, wodurch diese unverwendbar wird.

Bei solche Veränderungen, die in der Praxis bei Tests von Wasserzeichen eingesetzt werden, ist insbesondere an Kompressionen, dabei wiederum verlustbehaftete Techniken, aber auch Skalierungen, Rotationen, Ausschnitte, Vergrößerungen, Filterungen, Änderungen der Farbtiefe oder Auflösung und ähnliche Maßnahmen zu denken. Besonders ausgefeilte Wasserzeichen sind sogar noch erkennbar, wenn die digitale Datei in eine analoge Kopie übergeführt worden ist. Idealerweise „überlebt" eine robuste Watermark auch Digital-Analog Wandlungen und weitere Analog-Digital Wandlungen, wie etwa Ausdrucken und Einscannen.

Um das Wasserzeichen folglicherweise weniger anfällig für Attacken zu machen, wird in etwas aufwändigeren Techniken das Wasserzeichen über die gesamte Datei verteilt.

Ein Angreifer soll selbst dann, wenn er im Besitz mehrerer Kopien eines markierten Objektes ist, nicht in der Lage sein, das Watermark zu entfernen [Federrath].

Soweit ersichtlich gibt es derzeit keine Technik, die all diese „Angriffe" völlig zur Zufriedenheit übersteht, je nach eingesetzter Technik können allerdings mehr oder weniger starke Veränderungen noch erkannt werden. Insbesondere bei sichtbaren Wasserzeichen ist es von großer Bedeutung, dass diese möglichst schwierig für einen nicht legitimierten Benutzer zu entfernen sind.

Wesentliches Element dieses Merkmals „Robustheit" ist auch, mit welcher Wahrscheinlichkeit ein Wasserzeichen in einer veränderten Datei noch nachgewiesen werden kann. Mit anderen Worten, wie viel vom ursprünglichen Wasserzeichen übrig geblieben sein muss, damit man zuverlässigerweise noch von einer gekennzeichneten Datei sprechen kann.

Generell ist zu sagen, dass ein Wasserzeichen im hohen Frequenzbereich weniger leicht zu entdecken, allerdings dafür weniger robust und beständig ist. Die Robustheit wird bei der Einbettung in niedrigere Frequenzen erhöht, allerdings kommt es dadurch unausweichlich zu einer Veränderung des Signals.

Gleiches gilt im Bildraum. Ist das Wasserzeichen im signifikanten Teil des Bildes eingebettet, ist es besonders robust gegen Attacken.

Zum Thema Robustheit ist anzumerken, dass es in manchen Umständen gerade zu erwünscht sein kann, dass ein Wasserzeichen eine Veränderung des Bildes oder einen Kopiervorgang nicht unbeschadet übersteht. Als Beispiel in der analogen Welt dienen hier die Wasserzeichen an Geldscheinen. Gerade das Fehlen eines Wasserzeichens impliziert, dass es sich um keinen Originalschein handelt. Ähnliche Anwendungen sind auch in der digitalen Welt denkbar. Bereits kleinste Änderungen sollen dann das Wasserzeichen entfernen oder unleserlich machen, so dass die Originalität des Urstücks bzw Bearbeitungen nachgewiesen werden kann. In diesem Fall wird die Eigenschaft als fragil bezeichnet [Miller].

4.7.2.3 Die Sicherheit

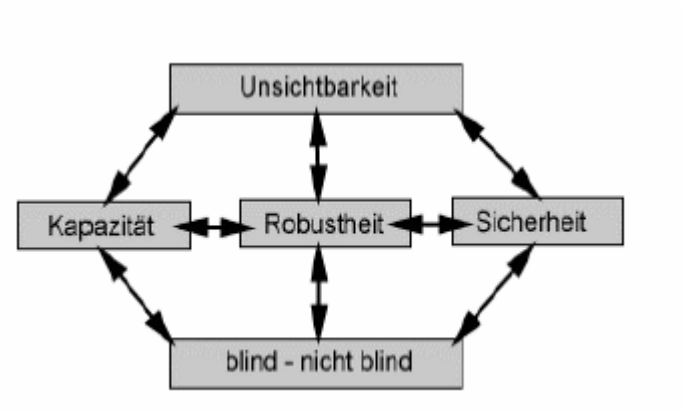
Digitale Wasserzeichen werden als sicher bezeichnet, wenn die eingebrachten Informationen weder zerstört, aufgespürt oder gefälscht werden können [Jahnke]. Derzeit gibt es wohl kein wirklich sicheres Wasserzeichen, jede der bisherigen Entwicklungen hat Schwachstellen.

4.7.2.4 Die Kapazität und Effizienz

Unter der Kapazität versteht man die Eigenschaft des Wasserzeichens, soviel Daten als möglich zu enthalten. Mit anderen Worten wird dabei die Länge der eingebetteten Nachricht umschrieben. Je größer die Kapazität, desto mehr Information lässt sich verstecken.

Mit Effizienz wird die Dauer, die man benötigt, um ein Wasserzeichen einzubetten bzw auszulesen, angegeben. Hierbei sind insbesondere die erforderliche Rechenzeit bzw die notwendigen Hardwareelemente von Bedeutung. Im Aufwand an Rechenzeit, der für das Einbetten einerseits, aber auch für das Erkennen andererseits benötigt wird, liegt gerade bei „streaming media“ wie Audio oder Video und den dort zu verarbeitenden großen Datenmengen bzw den daraus resultierenden Anforderungen an das technische Equipment ein Problem des Einsatzes von Wasserzeichen.

Eine andere Einteilung bei Wasserzeichen ist die Unterscheidung in blinde und nicht-blinde Verfahren. Als blinde Verfahren bezeichnet man dabei jene Methoden, die für Auffindung des Wasserzeichens im gekennzeichneten Material die Originalinformationen, also etwa das ursprüngliche noch nicht veränderte Bild nicht benötigen. Solche Verfahren haben natürlich, wie intuitiv erkennbar ist, einige Vorteile, sind aber durchaus komplexer, da simple Vergleichsalgorithmen nicht ausreichen, sondern das Wasserzeichen aus dem zu prüfenden Inhalt extrahiert werden muss.



[Abbildung 14: Abhängigkeitsverhältnisse der Anforderungen an Wasserzeichen untereinaner [Jahnke]]

4.7.3 Der Einsatzzweck von Wasserzeichen

Elektronische Wasserzeichen dienen der Kennzeichnung einer Trägerdatei. Durch Einfügen des Wasserzeichens des Urhebers können sie die Herkunft der Datei kennzeichnen.

Wasserzeichen können aber auch dazu dienen, um Veränderungen an dem gekennzeichneten Bild festzustellen. In diesem Fall kann typischerweise nicht die originale „Watermark" ausgelesen werden, aber das veränderte Bild muss noch ausreichend die Information enthalten, um das ursprüngliche Wasserzeichen nachweisen zu können. Für diese Feststellung muss zwischen dem ursprünglichen Wasserzeichen und der ausgelesenen Kennzeichnung noch ein ausreichend genauer Zusammenhang bestehen. Hierfür ist relevant, einen Grad der Abweichung festzulegen, bis zu dem das Wasserzeichen noch als erkannt gilt.

Typischerweise wird Watermarking bei Bilddokumenten eingesetzt. Allerdings gibt es auch Verfahren, die für Textdokumente geeignet sind. Für Texte wird vorgeschlagen, die Wasserzeicheninformation im Layout oder Format des Dokumentes einzusetzen [Podilchuk]. Dies kann durch leichte Änderungen im Abstand zwischen den Zeichen oder Wörtern oder leichte Modifikation der Zeichen nach vorgegebenen Mechanismen erfolgen. Diese Techniken können allerdings leicht durch OCR-Verfahren erkannt und ausgeglichen werden; damit wird das Wasserzeichen gelöscht.

Die Ziele, die damit in unterschiedlicher Intensität erreicht werden können, sind daher [Effelsberg]

(1) Authentizität: Nachweis der Identität des Urhebers durch eine eindeutige Kennzeichnung mit dem Wasserzeichen des Urhebers.

(2) Zugriffsschutz: Eine Kontrolle des Zugriffs kann durch die Integration eines Wasserzeichens in die Datei alleine nicht erreicht werden. Hierfür bedarf es eines weitergehenden, umfassenderen Mechanismus, der allerdings auch darin bestehen kann, dass das Programm zur Verwendung der Datei eine Darstellung oder Verwendung einer Datei ohne Wasserzeichen nicht zulässt.

(3) Vertraulichkeit: Ebenso wie zu Punkt (2) oben festgehalten, bedarf es für die Verhinderung des Zugriffs von unberechtigten Dritten eines vielfältigeren System, das auf einem Wasserzeichen aufbaut, aber über dessen bloße Einbettung hinausgeht.

(4) Integrität: Eine Veränderung, die auch zu einer Änderung des (fragilen) Wasserzeichens führt, lässt eine Manipulation erschließen.

Es mag auch notwendig sein, ein einmal eingebettetes Wasserzeichen nachträglich zu verändern oder mehrere Wasserzeichen in derselben Datei zu verwenden, die entsprechende Kombinationen an Restriktionen oder Rechten zulassen.

Es ist klar, dass das Wasserzeichen möglichst so in das digitale Objekt eingebracht werden muss, dass es nicht zu Beeinträchtigungen des Dokumentes kommt. So sollten Watermarks in Grafiken bzw Videos nicht sichtbar, in Sounddateien nicht hörbar sein.

4.7.4 Die Methoden von digitalen Wasserzeichen

Formal kann bei einer Datei S_0 und dem Wasserzeichen W die gekennzeichnete Datei S_w mit $S_w = S_0 + f(S_0, W)$ beschrieben werden.

Prinzipiell kommen bei Bilddateien zwei grundsätzliche Verfahrensarten in Betracht. Die eine Art verändert die Ursprungsdatei im Bildbereich, die andere arbeitet im Frequenzbereich.

Die meisten der eingesetzten Methoden bei Wasserzeichen sind „additiver Natur" [Podilchuk]. Im Wesentlichen besteht „watermarking" in dem Prozess, zwei Signale miteinander zu verbinden. Das eine ist das Trägersignal, das die eigentliche Information enthält, also ein Bild, ein Video oder ein Text. Das zweite Signal ist das Wasserzeichen, welches nur für einen Wasserzeichendetektor erkennbar sein sollte.

Die Gestalt des Wasserzeichens kann jedoch natürlich vielfältig sein.

Die Wasserzeichentechnik ist, wie oben bereits kurz angerissen, unterschiedlich, je nachdem auf welchen Typ an Daten sie angewandt werden soll. Im Folgenden soll als Grundlage jeweils eine Bilddatei angenommen werden.

Bildraumverfahren verwenden die Farb- und / oder die Helligkeitsinformationen eines Bildes, um die Daten des Wasserzeichens zu speichern. Ein häufig angewendetes Verfahren, Wasserzeicheninformationen in den räumlichen Wertebereich eines digitalen Bildes einzufügen, erfolgt durch Einflechten eines pseudo-zufälligen Musters in den Luminanz-oder Chrominanzwerten der Bildpunkte des digitalen Bildes [Jahnke].

4.7.4.1 Die Least significant Bit Methode

In einer besonders einfachen Form wird das Wasserzeichen jeweils in jenem Bit der Trägerdatei, welche am wenigsten Aussagewert hat (least significant Bit) eingefügt. Zur Erläuterung eines Wasserzeichens soll folgendes Beispiel dienen: X1, X2, … XN sind die Pixel eines Bildes. Jedes XN besteht aus mehreren Bits. Das Wasserzeichen, welches selbst aus einer vorgegebenen Anzahl von Bits besteht, wird nun jeweils in das least significant Bit der Original-Pixel eingefügt. Der daraus resultierende Unterschied im Farbwert ist bei einer entsprechend großen Auflösung der Farbtiefe minimal, weil entweder gar keine Änderung erfolgt (wenn zufällig das least significant Bit bereits den gewünschten binären Wert hat) oder nur der unmittelbar in der Farbskala angrenzende Farbwert gewählt wird. Aufgrund des Umstandes, dass das Wasserzeichen selbst in den least significant Bits enthalten ist, ist es somit für den gewöhnlichen Benutzer (für das menschliche Auge) unsichtbar.

Aus denselben Gründen ist es allerdings nicht sehr robust und kann relativ einfach entdeckt und entfernt werden [Memon]. Ebenso überlebt ein mit dieser Methode eingefügtes Wasserzeichen oft keine verlustbehaftete Kompression, so verändert etwa JPEG gerade das least significant Bit [Ruanaidh].

In anderen Verfahren wird das Wasserzeichen gerade in jene Bereiche eingebettet, die exponierter hinsichtlich der Wahrnehmbarkeit sind. Dabei besteht die größere Gefahr der Erkennbarkeit, allerdings - wie oben bereits angeführt - reduziert sich die Gefahr einer unberechtigten Entfernung oder Zerstörung des Wasserzeichens.

4.7.4.2 Die Block-Mittelwert Methode

Eine relativ simple Methode teilt die vorhandene Bilddatei in einzelne Blöcke: Jeder Pixel aus dem Block wird in seiner Intensität um einen Wert k erhöht, um den binären Wert 1 darzustellen, bzw um diesen Wert vermindert, um den Wert 0 darzustellen [Memon, Ruanaidh].

4.7.4.3 Das Verfahren „Blaukanal“

Bei diesem Verfahren nach Kutter wird die Unempfindlichkeit des menschlichen Auges gegenüber der Farbe blau ausgenutzt. Dementsprechend wird der Blauanteil des Bildes bei einzelnen nach einem Zufallsprinzip ausgewählten Pixel abgeändert. Dabei bedeutet s jeweils ein Bit {0,1} des Wasserzeichens, $B_{i,j}$ den Wert des Blaukanals und $L_{i,j}$ die Helligkeit des Bildes jeweils an der Position i,j. q ist ein Faktor für die Stärke und Robustheit des Wasserzeichens. Das neue, gekennzeichnete Bit wird nach der folgenden Formel berechnet:

$$B_{i,j\ neu} = B_{i,j\ alt} + (2s - 1) * L_{i,j} * q$$

Die Sichtbarkeit und Datenrate sind bei diesem Verfahren schlechter als bei einem Frequenzraumverfahren. Andererseits lässt sich das Wasserzeichen auch ohne Kenntnis des Originalbilds und Vergleich damit erkennen, dieses Verfahren wird daher der Gruppe der so genannten „blinden“ Methoden zugerechnet [Jahnke].

Zum Auslesen des Wasserzeichens nach diesem Verfahren sind Annahmen über den Originalwert des Pixels bzw dessen Blauwert notwendig. Es werden die Blauwerte der Nachbarschaft verglichen. Liegt der Wert erheblich darüber oder darunter, so wird die Annahme getroffen, dass dieses Pixel durch das Wasserzeichen verändert wurde.

Die korrekte Wiedererkennung des Wertes des eingebetteten Bits ist durch diese Technik zwar wahrscheinlich, kann aber nicht garantiert werden. Die Funktion, die den Wert des eingebetteten Bits wieder herstellt, ist nicht symmetrisch zur Funktion der Einbettung, die eine Funktion ist also nicht die Umkehrfunktion der anderen. Allerdings kann die Wahrscheinlichkeit, dass das Bit nicht korrekt wieder erkannt wird, durch ein mehrfaches Einbetten dieses Bits reduziert werden. Das Blaukanal Verfahren ist ein blindes Verfahren, so dass es bei der Erkennung nicht auf die Originalinformation zurückgreift und somit ein potenziell größeres Einsatzgebiet hat.

4.7.4.4 DCT

Eine Methode nach Zhao und Koch verwendet den Frequenzraum. Verfahren im Frequenzraum verknüpfen die Wasserzeicheninformationen mit den niedrigen oder hohen Frequenzen des zu markierenden Bildes. Basis dieser Methode im Frequenzraum bildet die Transformation von Bildblöcken und deren Bildpunkte durch Kodierungen, wie etwa die Diskrete Cosinus Transformation oder Diskrete Fourier Transformation, welche auch in Verfahren zur Komprimierung von Daten eingesetzt werden. Dadurch erhofft man sich eine große Robustheit gegenüber den aktuellen JPEG und MPEG Kompressionsverfahren, sowie unterschiedlichen Operationen der heutigen Bildverarbeitung, also einen deutlichen Widerstand gegen Manipulation durch diese. Ein Wasserzeichen in den zentralen Komponenten der Frequenzen eines digitalen Datenstromes unterzubringen, erhöht die Sicherheit sowie Robustheit des Wasserzeichens gegenüber Angriffen enorm, da jede Veränderung dieser Komponenten eine starke Auswirkung auf die Qualität des digitalen Dokumentes hat. Die Koeffizienten der jeweiligen Transformationen stellen solche wichtigen Frequenzkomponenten dar und werden entsprechend der technischen Anforderungen dieser Systeme bestimmt. Die Wasserzeicheninformationen, bzw deren Bestandteile in Form von Datenbits, werden bevorzugt in den wichtigsten mittleren Frequenzen eines digitalen Signals untergebracht, da festgestellt wurde, dass die Veränderungen der unteren Frequenzkoeffizienten starke visuelle Artefakte erzeugen und die hohen Koeffizienten sehr anfällig auf Rauschen, unterschiedliche Filtermethoden sowie Kompressionsverfahren reagieren [Jahnke].

Mit dem hier dargestellten Verfahren nach Zhao und Koch wird jedes Bit einer Bitfolge, die in ein Bild eingebettet werden soll, durch ein Verhältnis zwischen drei Frequenzkoeffizienten im mittleren Bereich eines DCT-Blockes dargestellt.

Die Diskrete Cosinus Transformation (DCT) ist eine lineare, orthogonale Transformation, welche ein zeitdiskretes Signal vom Orts- in den Frequenzbereich transformiert. Dabei wird ein Bild in Blöcke einer Größe von 8x8 Pixel zerlegt. Für diesen 64 Pixel-Block werden nun die 64 DCT-Koeffizienten in der zweidimensionalen Transformation nach folgender Formel berechnet:

$$F_{x,y} = \frac{C(x) \cdot C(y)}{4} \cdot \sum_{i=0}^{7} \sum_{j=0}^{7} f_{i,j} \cos\left(\frac{(2i+1) \cdot x \cdot \pi}{16}\right) \cdot \cos\left(\frac{(2j+1) \cdot y \cdot \pi}{16}\right)$$

Der Koeffizient im obersten linken Eck wird als DC-Koeffizient bezeichnet, die übrigen als AC-Koeffizient. Der DC-Koeffizient hat den größten Einfluss auf die Rekonstruktion und ist der wichtigste. Die Gewichtung der weiteren Koeffizienten nimmt in Richtung rechts unten ab.

Zaoh und Koch haben nun acht Koeffizienten auf speziellen Positionen in dem 8x8 DCT-Block aus dem mittleren Frequenzbereich als besonders signifikant identifiziert. Aus diesen werden drei zufällig ausgewählt.

Dazu werden drei DC-Koeffizienten aus dem mittleren Frequenzbereich so verändert, dass ihr Verhältnis zueinander ein Bit darstellt.

4.7.4.5 Fraktale Wasserzeichenverfahren

Weitere nennenswerte Wasserzeichenverfahren [Darstellung nach Jahnke] basieren auf fraktalen Kompressionstechniken. Bei diesen Verfahren wird das Bild zunächst in zwei verschiedene Auflösungen zerlegt. Die erste Auflösung teilt das zu markierende Bild in Werteblöcke der Größe n*n. Die zweite Auflösung hingegen zerlegt das Bild in räumliche Blöcke der Größenordnung 2n*2n. Für jeden Werteblock wird nun mit einem speziellen Algorithmus, beschrieben als „Interated Function System“ (IFS), nach einem passenden räumlichen Block gesucht, bei welchem die mittlere quadratische Fehlerquote minimal ist. Bevor jedoch der Werteblock mit dem räumlichen Block verknüpft wird, wird der räumliche Block weiter fakturiert zerlegt, so dass dieser die gleiche Dimension wie der Werteblock erhält. Schlussendlich werden noch entsprechende Skalierungsfaktoren und die Offsetwerte der Bildluminanzen angepasst und das zu markierende Bild kann vollständig über eine Beziehung zu dem Werteblock und einen Indexwert des am besten geeigneten räumlichen Blockes, den Skalierungsfaktoren und den Offsetwerten der Bildluminanzen beschrieben werden. Die Wasserzeicheninformationen werden in das zu markierende Bild eingefügt, indem entsprechende Werteblöcke speziellen räumlichen Blöcken exakt zugeordnet werden. Die Wasserzeichenbits werden bei diesem Verfahren durch eine spezielle Zuordnung abgebildet. Die Zuordnung erfolgt durch das Hinzufügen von künstlichen lokalen Ähnlichkeiten in dem zu markierenden Bild. Bei der Detektion des Wasserzeichens werden die optimalen fraktalen Zuordnungen zwischen den Werteblöcken und den räumlichen Blöcken berechnet. Wenn eine statistisch bedeutsame hohe Ausprägung dieser Zuordnung mit der vordefinierten Zuordnung des Wasserzeichens übereinstimmt, so ist das Wasserzeichen erkannt.

4.7.5 Der Nachweis von Wasserzeichen

Der Einsatz von Wasserzeichen ist typischerweise nur dann sinnvoll, wenn das Wasserzeichen auch wieder ausgelesen oder zumindest erkannt werden kann.

Ist das Wasserzeichen in dem zu untersuchenden Material noch vollständig enthalten, spricht man vom „Auslesen“ (extraction), ist es nicht mehr vollständig enthalten, aber noch wahrnehmbar, so spricht man von der „Erkennung“ (detection). Ab einem gewissen Grad der Zerstörung oder Veränderung des Wasserzeichens kann es nicht mehr mit der notwendigen Wahrscheinlichkeit nachgewiesen werden. Auf der anderen Seite sollte auch nicht fälschlicherweise eine unmarkierte Datei als markiert ausgewiesen werden und entsprechend dadurch Restriktionen unterliegen, die eigentlich nicht anzuwenden wären („false positive rate“) [Miller].

Um ein Wasserzeichen auszulesen oder nur zu erkennen, ist insbesondere bei geheimen Wasserzeichen die Kenntnis von Eigenheiten dieses Wasserzeichens notwendig. So ist erforderlich zu wissen, wie das Wasserzeichen aufgebaut ist, andernfalls ist ein Vergleich nicht möglich.

Liegt zum Erkennen des Wasserzeichens die Originalvorlage vor und kann zum Vergleich herangezogen werden, so spricht man auch von „nicht-blinden“ Verfahren. Ist dies nicht der Fall, und muss die extraction oder detection ohne Original verfolgen, so tituliert man dies als „blinde“ Verfahren [Jahnke]. Typischerweise sind blinde Verfahren aufwändiger und etwas weniger genau.

4.7.6 Watermarking und das Urheberrecht

In der Literatur wird die Einsatzmöglichkeit von digitalen Wasserzeichen für die Zwecke der Rechteverwaltung bezweifelt. Diese Autoren beurteilen die bisherigen Umsetzungsversuche für die digitalen Wasserzeichen als gescheitert, da diese alle auf der menschlichen Wahrnehmung basieren. Allerdings gibt es keine gesicherten Theorien und Annahmen über diese menschliche Wahrnehmung, so dass damit auch keine endgültigen Aussagen über Wasserzeichentechniken getroffen werden können. Somit kann nach dieser Ansicht ein digitales Wasserzeichen keinen Beitrag zur Erhöhung der Sicherheit für digitale Inhalte bieten.

Ganz ohne nähere Erläuterung ist wohl offensichtlich, dass der Einsatz von digitalen Wasserzeichen, damit ist hier gemeint lediglich durch Einbettung der Wasserzeichen in die digitale Datei, nicht in der Lage ist, Kopien an sich zu verhindern [Günnewig, Rosenblatt]. Ein Schutz des Vervielfältigungsrechts, aber auch des Verbreitungsrechts und des Rechts auf Zurverfügungstellung mit digitalen Wasserzeichen ist somit dadurch nicht möglich und eine Verletzung dieser Urheberrechte nicht direkt zu verhindern. Der Schutz dieser Rechte durch digitale Wasserzeichen wird nur indirekt erreicht. Kann der Berechtigte eine gekennzeichnete Kopie ausfindig machen, so kann er in Kombination (oft mit weiteren verfügbaren Informationen) feststellen, ob es sich um eine zulässige oder unerlaubte Kopie handelt. Kann er auch den Verwender dieser Kopie identifizieren, kann er seine Rechte auf herkömmlichen Weg geltend machen. Wasserzeichen werden daher auch als „passive Schutzmaßnahmen“ qualifiziert, im Gegensatz zu „aktiven“ Technologien, die den unzulässigen Zugriff tatsächlich verhindern.

Andererseits ist aber auch wesentlich, dass Wasserzeichen in dieser Form geeignet sind, die Urheberschaft des Schöpfers nachzuweisen [Petitcolas]. Die Authentizität der Inhalte ist gewährleistet, wenn das Wasserzeichen unverändert enthalten ist. Auch dies setzt allerdings voraus, dass ein gekennzeichnetes Bild vom Rechteinhaber überhaupt ausfindig gemacht wird. Erst nach Identifikation eines Verletzers kann der Berechtigte seine Urheberschaft und die damit verbundenen Rechte geltend machen und ausüben.

Das Wasserzeichen kann auch selbst Informationen enthalten, etwa Regeln über das Recht, eine oder mehrere Kopie(n) des Inhalts anzufertigen. Die Abspielgeräte haben dann jene Regeln zu befolgen [Miller]. Dieser Kopierschutz ist aber sicherlich dann nicht vollständig, wenn technisch nicht anderweitig gewährleistet wird, dass die Datei auf anderen Geräten nicht abgespielt werden kann. Hierfür ist also wiederum ein weiterer Schutzmechanismus notwendig. In der Praxis werden Wasserzeichen regelmäßig in Ergänzung zu kryptographischen Verfahren eingesetzt [Miller].

Unsichtbar zerbrechliche Wasserzeichen werden zerstört sobald die Originaldaten modifiziert werden [Jahnke]. Aus diesem Grund sind sie geeignet, die Bearbeitung nachzuweisen und können daher das Bearbeitungsrecht insofern schützen, als Bearbeitungen erkannt werden. Wiederum können sie aber gerade eine Bearbeitung und deren Verbreitung nicht unterbinden.

Wie sich aus dieser Beurteilung zeigt, ist das Wasserzeichen allein daher wohl nur eine nützliche und wesentliche Komponente in einem DRM Modell, aber kann alleine nicht ausreichend sein, einen umfassenden Schutz des digitalen Inhalts zu gewährleisten [Hartung]. Ein Einsatzgebiet ist aber sicherlich die Bewusstseinsbildung, die durch den Einsatz insbesondere von sichtbaren Wasserzeichen aber auch durch die vielleicht abschreckende Wirkung von unsichtbaren Wasserzeichen erreicht werden könnte.

4.8. Das Fingerprinting

Eine dem Wasserzeichen ähnliche aber doch davon zu unterscheidende Technik ist das so genannte Fingerprinting. Hierbei gibt es in der Literatur zwei unterschiedliche Ansätze.

4.8.1 Die Kennzeichnung der Kopie

Der erste Ansatz ist sozusagen eine Fortführung des elektronischen Wasserzeichens. Im Gegensatz zum „gewöhnlichen" Wasserzeichen wird nicht die Datei als solche mit einer Kennzeichnung versehen, sondern jede einzelne Kopie erhält eine distinkte Markierung. Dadurch erhält jeder Nutzer eine individualisierte Fassung der Datei. Gibt es etwa 100 verschiedene legalisierte Kopien eines Bildes, so enthält jede einzelne Kopie einen jeweils unterschiedlichen Fingerprint. Auf diese Weise ist es möglich, auch den Verteilungsweg eines ganz spezifischen Bildes nachzuvollziehen.

Bei dieser Variante des Fingerprintings, auch asymmetrisches Fingerprinting bezeichnet [Biehl], müssen daher um eine entsprechende Nachverfolgung gewährleisten zu können, zu jeder Kopie und damit zu jedem Kauf- oder sonstigen Übertragungsvorgang in einer Datenbank der entsprechende Steckbrief des jeweiligen Markierungsmusters sowie allenfalls Name und Adresse des Käufers/Empfängers abgespeichert werden.

Damit geht mit diesem System auch ein Verlust an Anonymität des Konsumverhaltens des Käufers einher, dass einerseits nicht wünschenswert und akzeptabel ist, andererseits meines Erachtens mit Bestimmungen über Datenschutz und Privatheit möglicherweise nicht vereinbar ist.

Für die technischen Grundlagen gilt ähnliches wie oben zu den Wasserzeichen angeführt. Auch hier sind Erkennbarkeit und Robustheit ein Thema.

Ein besonderes Angriffsziel bieten die Fingerabdrücke, da eben jede Kopie eine andere Identifikation enthält. Sind somit mehrere Kopien bekannt, kann durch die darin enthaltenen Unterschiede in einem kollusiven Zusammenwirken mehrerer

möglicherweise ein Rückschluss auf den Fingerprint oder zumindest die Methode oder Ort der Einbettung erfolgen, der wiederum einen „Angriff“, also den Versuch einer unzulässigen Beeinträchtigung oder Entfernung des Fingerabdrucks ermöglicht oder erleichtert.

4.8.2 Die typischen Merkmale der Datei

Mit einer etwas anderen Überlegung versucht eine andere Methode ein Identifikationsmerkmal und damit eine eindeutige Nachweisbarkeit wie bei einem Fingerabdruck aus einem Bild herauszulesen. Diese Merkmale sind allerdings bereits dem Original-Bild immanent und sind auch für Veränderung der Farbe, Formatierung, Kompression oder anderen Transformationen nicht geändert. Auf diese Art und Weise ist es möglich, ein Bild eindeutig zuzuordnen. Dieser Mechanismus ist dem menschlichen Fingerabdruck ähnlich [Johnson].

Diese Technik orientiert sich an dem Umstand, dass jene Bildbestandteile, die so hervorstechend sind, dass sie die Einzigartigkeit des digitalen Inhalts darstellen, nicht verändert werden können, ohne dass das Bild selbst zerstört wird.

Die von Johnson vorgeschlagene Methode untersucht dabei in einer Bilddatei die Gradienten und selektiert jene Punkte, die einen hohen Gradientenwert aufweisen. An dieser Stelle entsteht eine Spitze, die Summe dieser Spitze ist nach der vertretenen Ansicht markant für ein Bild und kann damit zur Identifizierung herangezogen werden.

Während etwa bei Wasserzeichen oder der oben beschriebenen Variante des Fingerprinting die Datei am Beginn der Verbreitung bearbeitet werden muss, ist dies bei dieser Technik nicht notwendig und es ist auch möglich, die Kennzeichnung zu einem viel späteren Zeitpunkt nach Erstellung des digitalen Inhalts vorzunehmen bzw zu erarbeiten. Dagegen ist aber gerade der interessante Aspekt der individuellen Kennzeichnung einer Datei natürlich bei dieser Methodik nicht denkbar, da es um spezifische Merkmale des digitalen Inhalts geht, der ident (oder beinahe ident) sein muss, um die gleichen Attribute auszulösen. Weiters ist davon auszugehen, dass sowohl Techniken der Verschlüsselung als auch Methoden zur Kennzeichnung mit Wasserzeichen ständig weiterentwickelt werden. Dadurch wird aber auch ein technologischer Zyklus ausgelöst, denn um einen Inhalt auch nach einem technischen Entwicklungssprung sicher vor unbefugtem Zugriff oder Veränderung oder Löschung des Wasserzeichens zu gestalten, ist eine neuerliche Bearbeitung mit dem verbesserten Verschlüsselungs- oder Wasserzeichenstandard notwendig. Eine solche neuerliche Behandlung fällt durch die Fingerprinting-Technik, wie gerade dargestellt, allerdings weg. Denn die spezifischen Charakteristika des digitalen Inhalts bleiben unverändert.

Ein Nachteil dieses Fingerprintings ist aber wohl der Aufwand an Computer Ressourcen gegenüber dem Watermarking. Während der Aufwand für das Auslesen des Wasserzeichens und der Vergleich mit der Vorlage ein statischer Aufwand ist, ist der Vergleich des Ergebnisses des Fingerprinting-Prozesses mit der Datenbank an

bestehenden Bildern abhängig von deren Anzahl und steigt damit mit der Größe des Bestands an digitalen Inhalten.

Ein ähnliches Verfahren, das zur Erkennung von Charakteristika dienen soll, wurde übrigens kürzlich für Computerprogramme vorgestellt. Dabei wird das spezifische Verhalten einer Software analysiert und verglichen [Martin]. Mit dieser Methodik sollen sich Urheberrechtsverletzungen an Programmen, konkret solchen, die mit der Sprache JAVA geschrieben wurden, entdecken lassen. Die Proponenten dieses Verfahrens identifizieren dabei so genannte Muttermale („Birthmarks“) in der Software. Neu ist offenbar an dieser Methode, dass es nicht einzelne Teile des Codes beurteilt, sondern das Verhalten des Programms. Da JAVA objekt-orientiert arbeitet, untersucht das Kopierschutzverfahren die Art und Weise, wie ein Programm zum Zeitpunkt der Ausführung des Codes mit Objekten umgeht. Besonderes Augenmerk wird dabei auf die Zusammenarbeit des Programms mit seiner es umgebenden Umwelt gelegt. Gerade in diesem Zusammenspiel mit anderen Komponenten liegt eine spezifische Charakteristik, die weniger als interne Abläufe innerhalb des Programms verschleiert oder leicht adaptiert werden können, um eine Verschleierung zu erzeugen. Die Prämisse der Erfinder dieser Methode geht dabei davon aus, dass diese Art und Weise einzigartig ist und daher das Auftreten der selben Verhaltensweise eine (zumeist unerlaubte) Kopie impliziert.

4.8.3 Fingerprinting und das Urheberrecht

Für das Fingerprinting gelten im Hinblick auf das Schutzniveau der Urheberrechte die gleichen Aussagen wie für Wasserzeichen. Weder durch das Integrieren einer eindeutigen Kennung, noch weniger aber durch die Berechnung spezifischer Kennzeichen eines Bildes wird eine Vervielfältigung, eine Verbreitung oder eine Zurverfügungstellung unterbunden. Wiederum kann der Schutz all dieser Rechte nur auf dem Umweg erreicht werden, dass eine Verletzung aufgrund eben des Fingerprintings leichter erkannt und bewiesen werden kann – dies setzt aber wiederum zunächst das Entdecken einer unerlaubten Kopie voraus. Im Gegensatz zum Wasserzeichen lässt sich aber mit der Methode des Fingerprintings, welche eine eindeutige Identifikation jedes Einzelstücks erlaubt, die Verfolgung einer Verletzung erleichtern.

5. Der Einsatz in der Praxis

5.1. Digimarc

Einer der bekanntesten Branchenvertreter, der in seinen Produkten Watermarks einsetzt, ist Digimarc. Digimarc ist in den USA ansässig und besitzt auch eine Vielzahl von Patenten im Zusammenhang mit digitalen Wasserzeichen. Bereits 1996 hat Adobe in seinem bekannten Produkt Photoshop die Technologie von Digimarc eingesetzt.

Ein Wasserzeichen von Digimarc enthält Informationen über den Ersteller oder Verteiler eines Bildes, allenfalls Informationen über das Bild selbst. Nach eigenen Angaben kann das Wasserzeichen in jedes gängige Bildformat, zB TIFF, JPEG, GIF oder BMP, und in Farb- oder Graustufenbilder eingesetzt werden. Das Wasserzeichen wird in den Helligkeitswert des Bildes eingearbeitet und ist somit unabhängig von den Farben und „überlebt" auch Farbwechsel. Auch Formatwechsel und einige Veränderungen, wie Skalierungen und Ausschneiden von Teilen soll das Wasserzeichen überstehen können, allerdings sind diesen Vorgängen Grenzen gesetzt.

Im Folgenden sind einige der Produkte von Digimarc, soweit diese Information erhältlich war, in ihrer grundlegenden Funktionsweise dargestellt. Diese Angaben basieren weitestgehend auf von Digimarc veröffentlichtem Material.

5.1.1 ImageBridge

Ein anderes kommerzielles Anwendungsprodukt von Digimarc ist ImageBridge. Dieses bietet die Integration eines einzigartigen Wasserzeichens in einem Bild. Ähnlich wie MediaBridge wird aufgrund des Erkennens des Wasserzeichens durch die Reader-Software, die auch als plug-in für Produkte anderer Hersteller, etwa Adobe oder Corel PhotoPaint erhältlich sind, der Nutzer zu weiterführenden Informationen, etwa über den Urheber oder Bedingungen der Nutzung, geleitet.

Die Digimarc ImageBridge watermark kann dabei die folgenden Informationen enthalten:

- Digimarc Ersteller ID
- Jahr des Schutzes
- Bild/Transaktions ID Nummer
- Sowie weitere Attribute etwa:
    - Eingeschränkte Nutzung
    - Nicht jugendfreier Inhalt

- Nicht zur Kopie berechtigt (diese Einstellung wird allerdings nicht von allen Applikationen unterstützt.

In ImageBridge ist es auch möglich, einen Link zur Homepage des Verwenders einzubetten.

Sobald eine Applikation, die die ImageBridge versteht, geöffnet wird, wird das Bild automatisch nach dem Wasserzeichen durchsucht. Sollte eines tatsächlich gefunden werden, zeigt die Software durch das Copyright Zeichen („©“) an, dass das betreffende Bild entsprechend geschützt ist.

5.1.2 MarcSpider

Die Überwachung eines unauthorisierten Nutzungsvorgangs erfolgt durch „MarcSpider“, eine Software, die öffentliche websites nach Bildern absucht, die mit der Digimarc ImageBridge eingebrachte Wasserzeichen enthalten. Software dieser Art und Weise bzw die damit einhergehende Gesamtheit an Verfahren und Infrastruktur wird einschlägig auch manchmal als Copy Detection Systems bezeichnet. Dabei muss natürlich ein effektiver Weg durch die Unzahl an Informationen im Internet gefunden werden. Prinzipiell sollte jede beliebige Internet Seite auch erreicht werden, wobei das System vor allem überprüft, ob die betreffende Website seit dem letzten Besuch verändert wurde. Auch spezielle Websites, auf denen in der Vergangenheit bereits Bilder gefunden wurden, werden regelmäßig überprüft. Von diesen ausgehend werden auch Links überprüft, sowie vor allem jene sites, die stark verlinkt sind. Dies, da ein eindeutiger Zusammenhang zwischen der Anzahl an Links auf eine Seite und der Häufigkeit, wie oft diese aufgesucht wird, besteht. Dabei gefundene Bilder werden an das System rückgemeldet und die dabei aufgearbeitete Information dem jeweiligen Nutzer zur Verfügung gestellt. Dadurch wird ein allfälliger unauthorisierter Gebrauch der gekennzeichneten Bilder aufgedeckt. MarcSpider hat allerdings keinen Zugriff auf gesperrte, insbesondere durch ein Passwort geschützte Bereiche einer Internet Seite. In solchen Zonen kann klarerweise eine Überprüfung nicht stattfinden. Damit ist MarcSpider kein undurchlässiger Schutz gegen unberechtigte Kopien oder sonstige Verwendung von mit Digimarc behandelten Bildern, bietet aber offenbar doch ein gewisses Schutzniveau.

5.1.3 MediaBridge

Die Idee hinter dem Produkt MediaBridge, das jünger ist, als die beiden anderen genannten Erzeugnisse, ist, die Brücke zwischen digitalem Inhalt und gedruckter Darstellung zu finden. Dabei wird ein digitales Wasserzeichen in gedrucktem Bildmaterial eingesetzt, etwa Werbematerial, Eintrittskarten, CD oder Bücherumschlägen, Visitenkarten, Katalogen. In dieser Anwendung beginnt der Prozess mit einem digitalen Bild, in welches das Wasserzeichen eingebettet wird. Dieses Bild wird mit herkömmlichen Druckverfahren erstellt. Sobald dieses Bild wieder digitalisiert wird, etwa über einen Scanner oder mittels einer digitalen Kamera (zB Web-camera), erkennt die Reader-Software das eingebettete Wasserzeichen. Dieses Wasserzeichen stellt einen Indexeintrag für eine Datenbank

dar. In der Datenbank wiederum ist eine Internet-Adresse eingetragen, die automatisch angewählt und anschließend dargestellt wird. Das Produkt schafft somit eine „Brücke“ zwischen gedrucktem Material und dem Internet, ohne dass ein Zwischenschritt, etwa die manuelle Eingabe der Internet-Adresse erforderlich ist.

Nach eigenen Angaben von Digimarc wird das Wasserzeichen sowohl im Frequenzbereich als auch im Bildraum eingesetzt, insofern wird eine Mischtechnik angewandt. Das Signal im Frequenzbereich wird dafür zum Zweck der Synchronisation eingesetzt, der eigentliche Inhalt wird in den Bildraum eingespeist.

5.1.4 Digimarc und das Urheberrecht

Wie nach den obigen Ausführungen für Wasserzeichen zu erwarten, können die Produkte von Digimarc offenbar nicht die Kopie eines Bildes verhindern. Das Vervielfältigungsrecht und das Verbreitungsrecht als auch das Zurverfügungsstellungsrecht können daher mit Digimarc nicht direkt geschützt werden.

Mit MarcSpider steht allerdings ein Werkzeug zur Verfügung, mit dem Urheberrechtsverletzungen zumindest verfolgt werden können. Hat der Urheber damit die Verletzungen seiner Rechte einmal festgestellt, kann er, vorausgesetzt, die faktischen Gegebenheiten stehen dem nicht entgegen, etwa durch die geographische Lage des Verletzers und Schwierigkeiten in der Rechtsverfolgung über Ländergrenzen hinweg, insbesondere durch prohibitive Kosten als auch Sprachschwierigkeiten, entsprechende Konsequenzen setzen.

Allerdings sind sie in der Lage Urheberpersönlichkeitsrechte zu schützen, da der Urheber des Bilds identifiziert werden kann. „Fair use“ ist mit wasserzeichengeschützten Bildern möglich, da die Verwendung nicht unmittelbar beeinträchtigt wird. Soweit ersichtlich ist es aber nicht möglich, mit Digimarc detaillierte Rechte zu vergeben und somit Kontext- oder Situationsabhängige Einstellungen zu ermöglichen.

5.2. Microsoft Windows Media DRM

Nachfolgend wird der Windows Media DRM näher dargestellt und dessen einzelnen Eigenschaften präsentiert[11]. Im Anschluss soll untersucht werden, welche Rechte nun damit geschützt werden.

5.2.1 Grundsätzliches

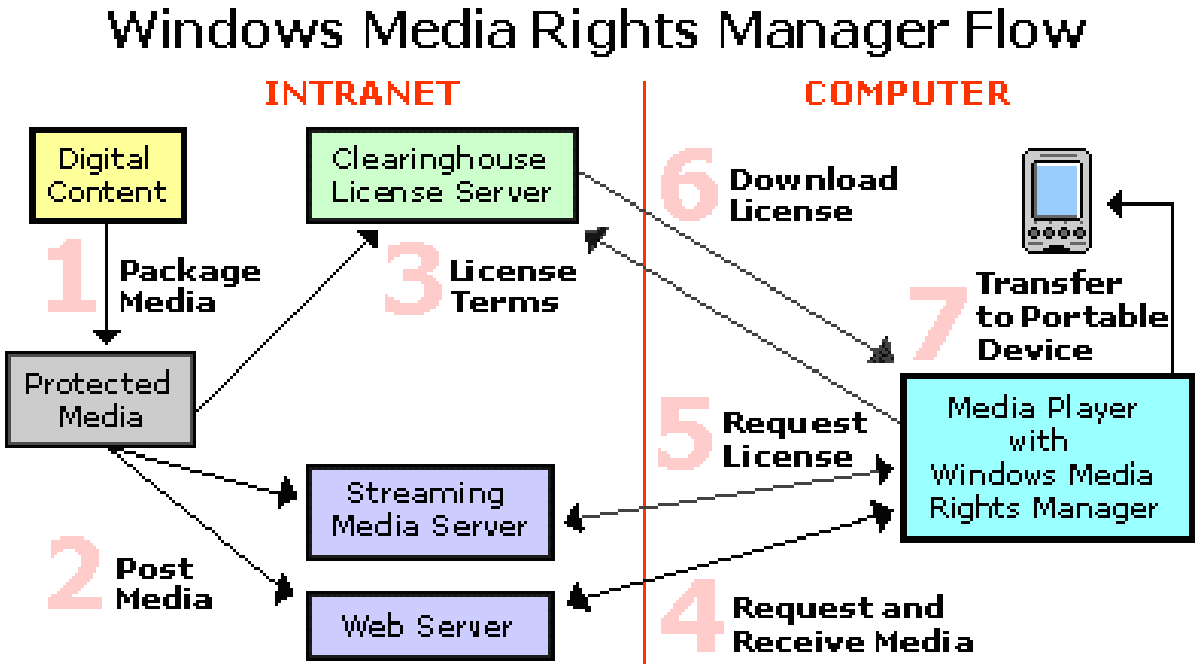
Der Microsoft Windows Media DRM ist eine Plattform zum Schutz und sicheren Übermitteln von individuellen und abonnierten Inhalten für die Wiedergabe auf einem Computer, einem tragbaren Gerät oder einem Netzwerkgerät [Microsoft FAQ]. Sie besteht aus mehreren Komponenten, darunter Werkzeugen für die

[11] Die Darstellung basiert im Wesentlichen auf eigenen Angaben von Microsoft (www.microsoft.com).

Entwicklung von mobilen Geräten oder Netzwerkgeräten. Die neueste Version der Technologie ist Windows Media DRM 10. Die Kernpunkte dieser Plattform sind:

- Der Windows Media Rights Manager ist dabei jenes Software Paket, mit dem die Dateien zunächst verpackt, also geschützt, werden und die Rechte festgelegt werden sowie Lizenzen produziert werden.
- Diese nun geschützten digitalen Mediendateien werden über beliebige Kanäle, etwa auch das Internet verteilt.
- Über eine Clearingstelle können Lizenzen für diese geschützte Datei erworben werden.
- Auf einem entsprechenden Abspielgeräte, etwa dem Windows Media Player kann, bei entsprechender Lizenz, die Datei wieder abgespielt werden.

Schematisch lässt sich der Ablauf eines Prozesses im Windows Media DRM folgendermaßen darstellen:



[Abbildung 15: Prozessschema des Windows Media DRM (Microsoft)[12]]

5.2.2 Die wesentlichen Eigenschaften

Windows Media DRM enthält eine Reihe von Eigenschaften, um die Inhaltsdateien zu schützen, aber auch zur Erleichterung neuer Business Modelle. Diese Features zur Verbesserung und Verstärkung der Sicherheit umfassen [nach Microsoft FAQ]:

(1) Individualisierung - Jedes digitale Abspielgerät ist einmalig und es wird fix mit dem Hostcomputer, also der Hardware verknüpft. Damit wird das Risiko verringert, dass ein gefährdeter Player eine weite Verbreitung über das Internet findet. Durch

[12] http://www.microsoft.com/windows/windowsmedia/howto/articles/drmarchitecture.aspx.

die Individualisierung ist es möglich, einen gefährdeten Player während des Lizenzierungsvorgangs zu identifizieren und zu deaktivieren.

(2) Anwendungsausschluss - Windows Media DRM ermöglicht es dem Lizenzaussteller, dafür zu sorgen, dass eine Anwendung bestimmte verpackte Dateien nicht wiedergeben kann.

(3) Ausschluss von DRM Komponenten - Windows Media DRM ermöglicht es dem Lizenzaussteller, Lizenzen für Anwendungen zu verweigern, die eine DRM Komponente verwenden, die beschädigt ist oder deren Gefährdung bekannt ist.

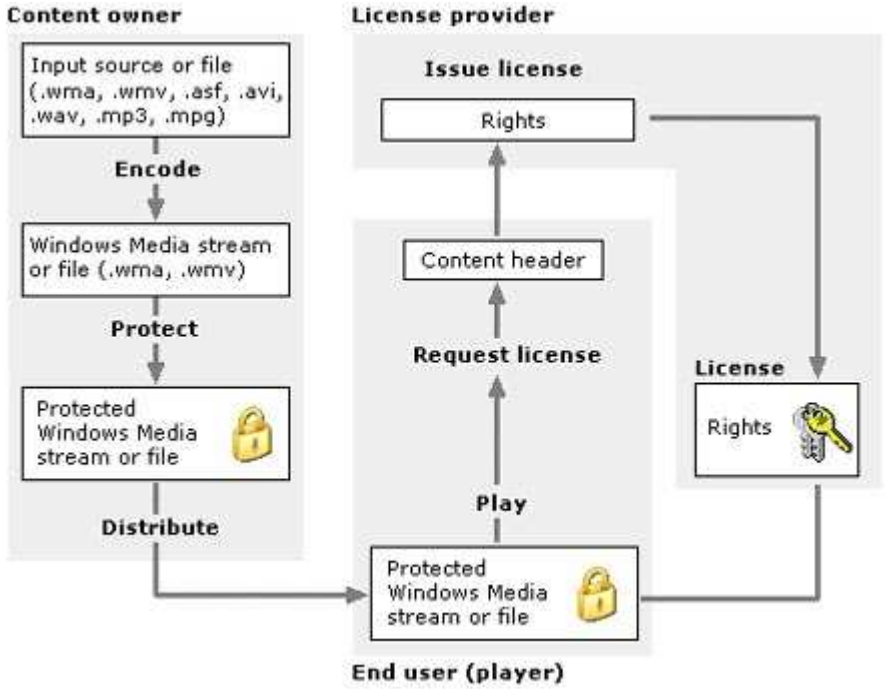
(4) Secure Audio Path - Windows Media DRM stellt den Schutz digitaler Mediendateien bei den Betriebssystemen Microsoft Windows Millennium Edition, Windows XP und künftigen Versionen des Windows-Betriebssystemen im Betriebssystem vom Player bis zum Soundkartentreiber sicher. Diese sichere Beziehung verringert die Wahrscheinlichkeit, dass ein nicht autorisiertes Programm einen digitalen Medienstream innerhalb eines Geräts aufzeichnet. Es wäre denkbar, die digitalen Mediendatei auf dem Weg zum Soundtreiber „abzufangen", also zu einem Zeitpunkt, nachdem sie entschlüsselt wurde und im System frei verfügbar ist. Mit der Secure Audio Path-Technologie ist auch dieser Transfer vom Mediaplayer zur Soundkarte geschützt, weil die Verschlüsselung solange als möglich aufrecht bleibt. Eine unverschlüsselte Kopie in digitaler Qualität soll somit verhindert werden. Eine zertifizierte Microsoft-Komponente überprüft dabei, ob alle untergeordneten Komponenten (einschließlich des Soundkartentreibers) ebenfalls zertifiziert sind. Sie entschlüsselt den Datenstrom nicht, wenn nicht autorisierte oder gefährdete Komponenten erkannt werden. Der Rechteinhaber kann dabei einstellen, dass die Soundkarte gewisse Anforderungen an Sicherheitsaspekten erfüllt, bevor die Freigabe des Inhalts erfolgt. Damit wird nach Ansicht von Microsoft den Inhabern der Rechte ein erhöhter Level von Schutz ermöglicht, wenn sie digitale Inhalte online verbreiten. Erst in der Soundkarte kann der digitale Datenstrom tatsächlich verarbeitet werden. Tatsächlich wird in diesem Verfahren nach der Dekomprimierung und Entschlüsselung des digitalen Inhalts im Player ein Rauschen zur eigentlichen Musik addiert. Wird in diesem Zeitpunkt der Datenstrom abgefangen, ergibt dieser lediglich ein undefiniertes Rauschen. Dieses Rauschen wird erst in der Soundkarte wieder entfernt, selbstverständlich, nach dem diese von Secure Audio Path authentifiziert wurde.

(5) Dauerhafter Schutz - Windows Media DRM „sperrt" digitale Mediendateien mit einem Lizenzschlüssel, um den Schutz der Inhalte auch bei einer weit reichenden Verteilung dieser Dateien zu gewährleisten. Jedem Computer wird eine eindeutige Lizenz zugewiesen. Damit wird die illegale Verteilung digitaler Mediendateien verhindert.

(6) Starke Verschlüsselung - Windows Media DRM enthält bewährte Verschlüsselungsschemas, die verhindern, dass verteilte digitale Mediendateien der Piraterie oder sonstigen illegalen Verwendungszwecken zum Opfer fallen.

5.2.3 Die Funktionsweise

Zur Erstellung einer Datei, die im Zusammenhang mit dem Windows Media DRM verwendet werden soll, sind mehrere Schritte notwendig.



[Abbildung 16: Struktogramm des Windows DRM (Microsoft)[13]]

5.2.3.1 Der Encoder

Zunächst muss die Datei in ein entsprechendes Windows Media Format gebracht werden.

Grundlage dieses Formats ist ein robuster Dateicontainer nach dem Advanced Systems Format (ASF). ASF ist ein erweiterbares Dateiformat, das zum Speichern synchronisierter Multimediadaten bestimmt ist. ASF unterstützt die Datenübertragung über verschiedenste Netzwerke und Protokolle, ist jedoch ebenfalls zur lokalen Wiedergabe geeignet. ASF unterstützt erweiterte Multimediafunktionen, zum Beispiel erweiterbare Medientypen, den Komponentendownload und skalierbare Medien.

Dieser Dateicontainer speichert dabei sowohl Audio- und Videodaten, als auch Metadaten sowie Index- und Skriptbefehle. Das Format legt dabei nicht fest, wie die Audio- oder Videodaten („streams“) kodiert werden, sondern nur die Struktur. Um dennoch die Kodierungen kompatibel zu gestalten, werden die folgenden Dateierweiterungen verwendet:

- WMA für Dateien mit Audiodaten, die mit dem Windows Media Audio-codec komprimiert wurden

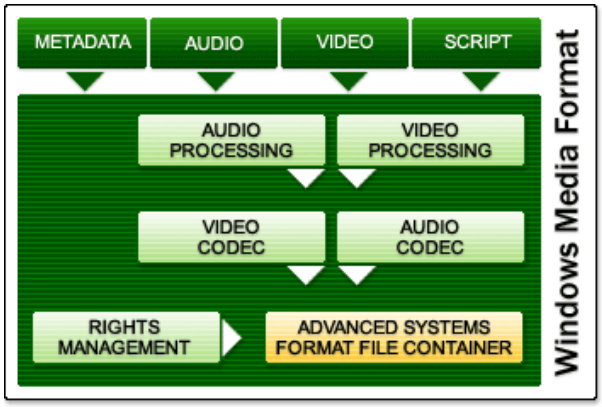
[13] http://www.microsoft.com/windows/windowsmedia/howto/articles/ProtectContent.aspx.

- WMV für Dateien mit Audio- und Videodaten, die mit dem Windows Media Audio- und dem Windows Media Video-codec komprimiert wurden

- Mit anderen codecs komprimierte Inhalte sollten in einem ASF file gespeichert werden.

Als codec (Wortkreuzung aus den englischen Begriffen coder und decoder) bezeichnet man ein Verfahren bzw Programm, das Daten oder Signale digital codiert und decodiert. Beim direkten Umwandeln von einem Format in ein anderes (bspw. MPEG-2 zu MPEG-4 oder MP3 zu WMA) spricht man auch vom Transcodieren. Die Windows Media codecs enthalten also selbst keinerlei Information oder DRM Eigenschaften, diese ergeben sich durch den ASF container, der seinerseits den WMA/WMV stream enthält.

Schematisch lässt sich dieser Teil folgendermaßen darstellen:



[Abbildung 17: Darstellung des Windows Media Format (Microsoft)[14]]

Die Basisorganisationseinheit eines ASF file ist das ASF object. Es besteht aus einem GUID („globally unique identifier“), einem weiteren Feld, welches die Objektgröße angibt und aus Objektdaten variabler Länge. Der ASF container ist als Objektstruktur aufgebaut und enthält drei unterschiedliche Objekte (Top-Level Objects):

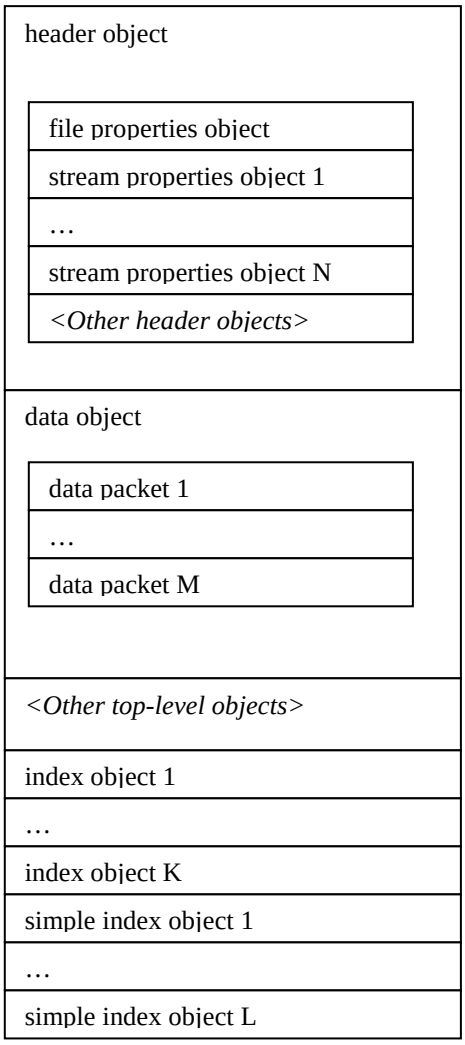
- header object

- data object

- index object(s).

Das header object muss am Beginn jedes ASF file stehen. Das data object ist ebenso verpflichtend vorgesehen und muss dem header object folgen. Das oder die index object(s) sind optional und müssen, wenn sie vorkommen, am Ende des ASF file angebracht werden. Die Struktur dieser Objekte sieht folgendermaßen aus:

[14] http://www.microsoft.com/windows/windowsmedia/de/format/default.aspx.



[Abbildung 18: Diagramm der ASF File Structure [Microsoft]]

Das header object stellt eine wohldefinierte Bytesequenz am Anfang eines ASF file dar. Es enthält alle notwendigen Informationen, um den Inhalt des data object zu interpretieren. Zusätzlich kann es Metadaten enthalten.

Das header object ist das einzige Top-Level Objekt, welches weitere Objekte enthalten kann. Es muss ein file properties object, ein header extension object, und zumindest ein stream properties object enthalten. Das file properties object enthält die globalen Dateieigenschaften, zB die Anzahl der Daten-Pakete (data packets) im data object. Das header extension object ermöglicht das Hinzufügen zusätzlicher Funktionalität bei gleichzeitiger Gewährleistung von Abwärtskompatibilität. Ein stream properties object gibt die Charakteristika des einzelnen Medienstromes innerhalb des ASF file dar und enthält so die Informationen, wie zugehörige Daten des data object zu interpretieren sind (der Medientyp). Durch diesen Parameter wird einem stream eine Datenstruktur zugeordnet, welche Registrierungsdaten zu Struktur und Format des im stream enthaltenen Medienobjektes aufnimmt.

Ein optionales content description object nimmt bibliographische Aspekte wie Titel, Autor, Beschreibungen und Copyright auf und referenziert dabei auf den gesamten Inhalt des ASF file. Dieses Objekt darf, wenn es überhaupt verwendet wird, maximal

einmal vorkommen. Ein script command object enthält Befehle, die während der Wiedergabe abgearbeitet werden können.

Das data object repräsentiert den gesamten digitalen Inhalt eines ASF file. Die Daten sind dabei in der Form von ASF packets gespeichert, diese wiederum haben eine fix vorgegebene Länge.

5.2.3.2 Die Verschlüsselung/ Das Verpacken

Danach folgt das Verpacken, das mit der Verschlüsselung zusammenfällt.

Hierfür wird zunächst ein Schlüssel generiert. Dieser basiert einerseits auf einem geheimen Wert (license key seed), sowie andererseits auf einem Identifikationswert für den Schlüssel (key ID). Der license key seed muss sowohl dem Ersteller als auch jener Stelle, die die Lizenberechtigungen überprüft, bekannt sein, da beide aufgrund dieses Eingangswertes denselben Schlüssel für die spezifische Mediendatei erstellen können müssen. Mit diesem Schlüssel wird die Datei verschlüsselt. Neben dem nunmehr verschlüsselten Inhalt enthält die verpackte Datei Metadaten im so genannten content header. Dieser enthält:

- Die oben genannte key ID
- Eine optionale content ID, die den Inhalt näher spezifiziert
- Die Adresse, an der eine Lizenz bezogen werden kann (license acquisition URL)
- Sowie wiederum optional weitere Metadaten.

Welche Technologie hierfür eingesetzt wird, ist aus öffentlich zugänglichen Quellen nicht zu erschließen. Microsoft behauptet, dass der Windows Media Rights Manager die Mediendatei mit einem „konzentrierten Verschlüsselungsalgorithmus“ bearbeitet, wobei dieser Algorithmus auf veröffentlichten Verschlüsselungen basiert, „die der eingehenden Prüfung durch die Kryptografiecommunity standgehalten haben“. Zumindest frühere Versionen von Microsoft DRM dürften auf einem Elliptische-Kurven-Kryptosystem, einem asymmetrischen Verschlüsselungssystem aufbauen, sowie auch DES, als Blockchiffre, und RC4, als Stromchiffre, und SHA-1, als Streuwertfunktion, verwenden.

Der content header wird vom Ersteller mit seinem geheimen Schlüssel signiert, um eine Manipulation an diesen Informationen zu verhindern.

Der Windows Media Rights Manager verpackt zunächst die Datei, diese wird verschlüsselt und mit einem „Schlüssel“ versehen. Zusätzlich werden weitere Informationen des Inhalteanbieters in der Datei gebündelt. Das Ergebnis ist eine verpackte Datei, die nur von der Person wiedergegeben werden kann, die eine Lizenz erworben hat. Diese Lizenz enthält den Schlüssel zum Öffnen der Datei.

Im Windows Media Format-Dateicontainer ist kein Entschlüsselungsschlüssel enthalten.

Die Zuteilung von Lizenzen ist nicht innerhalb des Windows Media Rights Manager System geregelt, sondern obliegt dem Ersteller der WMA/WMV Datei.

5.2.3.3 Die Rechtevergabe

Die durch den Windows Media Rights Manager vergebenen Nutzungsrechte können vielfältig sein. Der Ersteller kann die erlaubten Handlungen des Nutzers und damit das Ausmaß seiner Kontrolle in vielerlei Hinsicht steuern:

- ob (AllowPlay) und wie oft die Datei abgespielt werden kann (PlayCount)
- ob eine Kopie erstellt werden darf (AllowCopy) und allenfalls die Anzahl der Kopien, die erstellt werden dürfen (CopyCount)
- ob die Datei an ein Gerät, das mit SDMI nicht (AllowTransferToNonSDMI) oder schon (AllowTransferToSDMI) übereinstimmt, übertragen werden kann. Hier kann spezifiziert werden, wie viele Übertragungen erlaubt sind (TransferCount). SDMI ist die Secure Digital Music Initiative, eine Vereinigung von Industriepartnern aus Musik- und Computerindustrie mit dem Ziel der Entwicklung von technischen Schutzmaßnahmen
- ob eine Sicherheitskopie der Lizenz erlaubt ist (AllowBackupRestore)
- ob eine Kopie auf eine CD erlaubt ist (AllowPlaylistBurn). Zu beachten ist, dass nach diesem Kopiervorgang kein Kopierschutz mehr besteht
- die Dauer der Lizenz bzw Beginn (BeginDate) und Ende (ExpirationDate) der Rechte, wobei die Dauer auch ab dem Zeitpunkt des ersten Abspielvorgangs definiert sein kann (ExpirationAfterFirstUse) oder ab dem Zeitpunkt, mit dem die Datei das erste Mal auf dem Gerät des Nutzers abgespeichert wird (ExpirationOnStore). Um die Lizenzdauer nicht manipulieren zu können, wird die Lizenz gelöscht, wenn die interne Uhr des Computers des Nutzers zurückgesetzt wird (DeleteOnClockRollback) oder die Lizenz zumindest vorübergehend ausgesetzt wird, bis die Zeit wieder richtig gestellt wird (DisableOnClockRollback). Es besteht auch die Möglichkeit, eine Dauer anzugeben, während dessen die Datei auch noch gespielt werden darf, obgleich DeleteOnClockRollback oder DisableOnClockRollback ausgelöst wurde (GracePeriod)
- auf welche Geräte, etwa tragbare Abspielgeräte, die Datei übertragen werden kann durch festlegen des Sicherheitslevels des Abspielgeräts (MinimumSecurityLevel), so dass der Schutz gewährleistet ist.

Windows Media Rights Manager verwendet als rights expression language XRML [Guth].

5.2.3.4 Die Verteilung

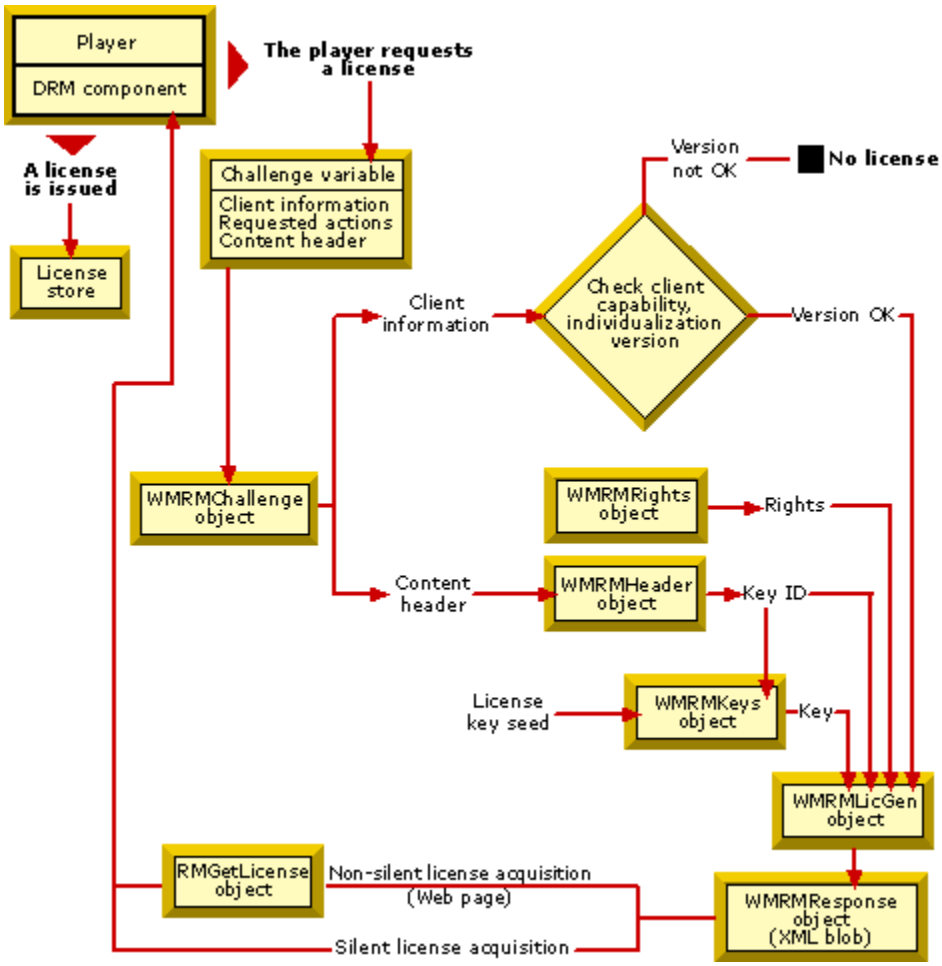
Die Verteilung kann auf jede beliebige Weise, also insbesondere auch mittels Verbreitung über das WWW erfolgen. WMRM schützt dabei nicht vor der Vervielfältigung an sich, nur die Nutzung der Kopie erfordert eine eigene Lizenz.

5.2.3.5 Die Wiedergabe und Lizenzerstellung

Um die geschützte Datei schließlich nutzen und abspielen zu können, benötigt der Nutzer eine Lizenz sowie einen Player, der das WMA/WMV Format unterstützt sowie die Funktionalität des Windows Rights Managers integriert.

Sofern die Lizenzerstellung und -verwaltung nicht vom Ersteller der Mediendatei selbst durchgeführt wird, ist ein sicherer Kommunikationskanal zwischen Nutzer und Ersteller notwendig, da zumindest der license key seed übermittelt werden muss, aber auch die jeweiligen öffentlichen Schlüssel ausgetauscht werden müssen. Der öffentliche Schlüssel des Erstellers ist notwendig, um die Signatur des content header zu überprüfen. Der öffentliche Schlüssel der Lizenzstelle ist für den Ersteller für weitere Kommunikation, etwa beim Rückruf einer Datei erforderlich.

Sofern eine geschützte Datei in einem solchen Player abgespielt wird, sucht der Player nach einer entsprechenden Lizenz auf dem System des Nutzers, oder versucht automatisch eine Lizenz einzuholen, wenn ein Zugang bekannt ist, oder verweist den Nutzer an eine Stelle, an der die Lizenz erworben werden kann. Letztere Information ist eine der Metainformationen, die im Container enthalten sind:



[Abbildung 19: Schematische Darstellung der Lizenzvergabe im Windows Right Manager (Microsoft)[15]]

Mit der Anforderung der Lizenz sendet der Nutzer den content header der Mediendatei an die lizenzvergebende Stelle. Aus dem content header kann diese Stelle die key ID auslesen und mit der license key seed den Schlüssel für die Datei nachgenerieren und damit die Lizenz erstellen.

Die Lizenz enthält schließlich den Schlüssel, der das Windows Media file entschlüsseln kann. Darüber hinaus enthält die Lizenz jene Nutzungsbedingungen, zu denen die Datei benutzt werden kann.

Eine Lizenz erlischt, wenn die für sie festgesetzte Zeit abgelaufen ist, oder die Mediendatei rückgerufen wird. Darüber hinaus erlischt sie etwa, wenn die festgesetzten Rechte vollständig ausgeübt wurden, etwa die Anzahl an Abspielvorgängen erschöpft ist.

Wesentlich ist aber, dass die Lizenz separat vom eigentlichen Inhalt verteilt wird. Somit ist eine Clearing Stelle immer erforderlich. Dies setzt auch voraus, dass diese Clearing Stelle möglichst stets erreichbar und verfügbar ist.

[15] http://msdn2.microsoft.com/en-us/library/bb649429(VS.85).aspx.

5.2.4 Ein Versuch einer Beurteilung von Windows Media DRM

Microsoft selbst streicht eine Eigenschaft von Windows Media DRM heraus, die wohl Datenschützer und sonstige um die Verwertung von persönlichen Daten besorgte Personen nicht schätzen werden: Beim Registrieren von Lizenzen können die vergebenden Unternehmen wichtige Informationen über ihre Kunden sammeln, die dazu führen, dass sie wissen, was ihre Kunden wünschen.

Die Nutzer können Lizenzen selbst nicht teilen oder kopieren, allerdings können sie kopiergeschützte Dateien vervielfältigen. Der Vervielfältigungsschutz und Verbreitungsschutz ist damit nicht gewährleistet, auch das Zurverfügungsstellungsrecht ist wohl nicht geschützt. Allerdings können die kopierten Dateien ohne eigene Lizenz nicht abgespielt werden, so dass die Beeinträchtigung der Rechte wohl materiell nicht vorliegt.

Damit erreicht Windows Media DRM offenbar einen recht guten Schutz der Vervielfältigungsrechte. Die Vervielfältigung kann erlaubt aber auch wirksam unterbunden sein. Allerdings erscheint es, dass Windows Media DRM „fair use“ nicht berücksichtigt, sofern nicht die Lizenzvergabe selbst entsprechend ausgestaltet ist und einem Nutzer, der „fair use“ Gründe angibt, eine entsprechende Lizenz erteilt.

Zuletzt gab es nun Berichte, nach denen der Kopierschutz von Microsoft „geknackt“ worden wäre und somit nur mehr unzureichenden Abspielschutz bietet [Spiegel]. Damit ist gezeigt, dass auch komplexere Technologien einen begrenzten Schutz bieten.

6. Zusammenfassung und Ausblick

Es ist hinlänglich bekannt, dass das Internet in vielerlei Hinsicht ein komplexer Raum geworden ist. Zahlreiche interessierte Teilnehmer präsentieren sich selbst als auch seit einigen Jahren in zunehmendem Ausmaß ihre Waren und Dienstleistungen. Im Rahmen dieser geschäftlichen Tätigkeiten möchten sie ihre ihnen zustehenden Rechte schützen. In ähnlicher Weise und möglicherweise noch viel größerem Umfang stellen sich aber auch Probleme in Bereichen, die nicht unmittelbar im geschäftlichen Bereich anzusiedeln sind. Dabei ist insbesondere der Austausch von Musikdateien zu nennen, der auch in vielen Medienberichten als auch gerichtlichen Verfahren diskutiert und problematisiert wurde.

Die Rechtsordnung zieht keinen Unterschied zwischen der analogen und der elektronischen Welt. Jene Werke, die herkömmlicherweise geschützt sind, genießen eine Reihe an Rechten daher geradezu selbstverständlich auch im Internet. Digitale Inhalte genießen somit auch in der digitalen Welt urheberrechtlichen Schutz, sofern die üblichen und generellen gesetzlichen Voraussetzungen für diesen Schutz erfüllt sind. Insbesondere Musikstücke sind daher natürlich auch in digitalisierter Form geschützt. Wie dargestellt wurde, ist allerdings das Rechtsgebiet des Urheberrechts (Copyright) ein vielfältiger Begriff. Einige der dem Berechtigten zukommenden Rechte, insbesondere aber das Vervielfältigungs- und das Verbreitungsrecht sowie das Zurverfügungsstellungsrecht, sind wohl in vielen Fällen durch die Digitalisierung und Verbreitung im Internet betroffen.

Wie in der Aufgabenstellung angesprochen, zeigt sich, dass Digital Rights Management, verstanden als die Verwaltung von Rechten an digitalen Inhalten ein vielschichtiges Gebilde aus Recht und Technik ist, bei dem Elemente aus diesen beiden Gebieten stark verwoben sind. Einerseits hilft die technische Komponente, den digitalen Inhalt zu schützen, der seinerseits (potenziell) den Schutz des Urheberrechts genießt. Darüber „stülpt“ sich als weitere Schicht wieder das Recht, das die unerlaubte Manipulation an den technischen Schutzmaßnahmen verpönt und für unzulässig erklärt. Nicht zu vergessen ist dabei, dass letztlich das Verhältnis zwischen Hersteller und Nutzer ein Vertragsverhältnis ist, das entsprechend durch Vereinbarungen adaptiert werden kann.

In der Analyse des Niveaus des gebotenen Schutzes zeigt sich, dass die vorgestellten technischen Schutzmaßnahmen von digitalen Wasserzeichen und Techniken der Verschlüsselung jede für sich eine gewisse Sicherheit bieten können. Gerade in der Kombination der beiden dürfte aber die Stärke liegen und eine wohl umfassende Sicherung der kostbaren Datei erreicht werden. Während durch den Einsatz von Verschlüsselung der eigentliche Kopiervorgang zwar nicht unterbunden werden kann, aber die Verwendung der Kopie zumindest erschwert wird, kann durch Wasserzeichen Information über den Urheber integriert werden und verbotene Vervielfältigungen festgestellt und verfolgt werden.

Eine tragende Rolle in der tatsächlichen Anwendung spielen in komplexen DRM Systemen auch die Rechtesprachen, rights expression languages, die die Nutzungsbedingungen und Zugangskontrollen festlegen sollen. Damit diese

Kontrolle nicht an Schnittstellen des Computersystems des Anwenders verloren gehen, sind aber spezielle Komponenten (trusted parts) notwendig, die den vom jeweiligen DRM System gebotenen Schutz durchgängig gewährleisten.

Dennoch wird auch der rechtliche Aspekt nicht zu vernachlässigen sein. In dieser Hinsicht wird gerade die Zukunft weisen, ob das Verbot von Umgehungsmaßnahmen gegen technische Schutzeinrichtungen tatsächlich einen fassbaren Nutzen hat und damit den Rechteinhabern in der Tat einen erhöhten Schutz bietet oder ob dieses Verbot nicht doch praktisch ins Leere geht. Ohne ein solches Verbot wäre aber jede technische Maßnahme zum Teil „zahnlos". Denn wie die Vergangenheit zeigt, zieht jede Entwicklung einer technischen Schutzmaßnahme den fast unmittelbaren Versuch nach sich, diese zu umgehen. Als Beispiele sollen dafür das angeführte DeCSS oder auch Meldungen, dass der Windows Media Rights Manager „geknackt" werden konnte, dienen.

Aus heutiger Sicht ist natürlich ungewiss, welchen Weg DRM nehmen wird. Gerade jüngste Meldungen zeigen aber eher, dass DRM als Massenprodukt (noch) kein Anwendungsfeld gefunden hat. So haben zuletzt Musikanbieter entweder angekündigt, gänzlich auf Digital Rights Management zu verzichten [Presse] oder wie iTunes – eigentlich ein Vorreiter im Bereich Digital Rights Management - ihr Angebot an „freier" Musik zu erweitern. Es entsteht der Eindruck, dass Digital Rights Management Technologien stärker in jenen Bereichen eingesetzt werden, in denen der Wert des zu schützenden Produkts höher ist, so dass sich auch die Kosten der Entwicklung der Techniken als auch der spezifischen Produkte relativieren und in einem angemessenen Verhältnis stehen. Wesentlich wird hierbei sein, tatsächlich alle hierin angeführten Komponenten eines Digital Rights Management Systems zu verwenden, da nur dann ein vollständiger Schutz gewährleistet werden kann. Auch hierin liegt derzeit eine „Schwachstelle" in Produkten für jedermann, da naturgemäß (noch) nicht jeder Heim-PC mit dem notwendigen Equipment ausgestattet ist.

Ein bislang wohl ungelöstes Spannungsfeld ist jedenfalls der technische Schutz von an sich urheberrechtlich nicht geschützten Produkten sowie bislang durch das Urheberrecht erlaubte Handlungen an solchen Werken, die dem Urheberschutz prinzipiell unterliegen. Gerade zu den letzteren hat sich der Begriff „fair use" aus dem angloamerikanischen Raum auch in unseren Breiten eingebürgert, obwohl inhaltlich die amerikanischen Ausnahmen zum Copyright stark von den Ausnahmebestimmungen zum Schutz des Urheberrechts im österreichischen Gesetz abweichen. Beiden ist aber gleich, dass solche Ausnahmen in spezifischen Fällen gewährt werden und somit das Urheberrecht nicht uneingeschränkt besteht. Es besteht die Aussicht, dass „fair use" durch den Einsatz von technischen Schutzmaßnahmen wohl eine neue Bedeutung erfahren wird, da die bisher eingesetzten Techniken offenbar die darunter verstandenen Rechte bzw zulässigen Eingriffe nicht umsetzen, aber wie von entsprechender Seite vorgebracht wird, auch wohl nicht adäquat umsetzen können, da hier oft einzelfallbezogene Aspekte eine nicht zu unterschätzende Rolle spielen. Gerade die Problematik, dass schon der Begriff des „fair use" bzw die darunter verstandenen Ausnahmen aus dem Schutz des Urheberrechts in jeder Rechtsordnung teilweise anders verstanden werden und somit eine technische Schutzmaßnahme eine Unzahl an nationalen Umsetzungen

implementieren müsste, führt zu einer nicht mehr verwaltbaren Komplexität. Für diese rechtlichen Ausnahmen scheint es kein technisches Äquivalent zu geben, so dass der technische Schutz auch in diesen Bereichen sozusagen in überschießender Weise greift. Dem Nutzer eines mit DRM geschützten digitalen Inhalts kommen somit eingeschränktere Nutzungsmöglichkeiten zu, als er in der analogen Welt zulässigerweise für das gleiche Werk hätte. Besonders an diesem Aspekt stoßen sich Kritiker von Digital Rights Management.

7. Literaturverzeichnis

Alle Hyperlinks aktiv am 9. Jänner 2008

[Alattar]	*Alattar, Adnan*	Bridging printed media and the Internet via Digimarc's watermarking technology	http://www.digimarc.com/tech/docs/dmrc_bridging_printed_media.pdf (2000)
[Arlt]	*Arlt, Christian*	Digital Rights Management-Systeme; Begriff, Funktion und rechtliche Rahmenbedingungen nach den jüngsten Änderungen des UrhG – insbesondere zum Verhältnis der §§ 95 a ff UrhG zum Zugangskontrolldienstesc hutzgesetz (ZKDSG)	GRUR 7/2004, 548 (2004)
[Bechtold02]	*Bechtold, Stefan*	Vom Urheber- zum Informationsrecht	Verlag C.H. Beck München (2002)
[Bechtold05]	*Bechtold, Stefan*	Trusted Computing	Computer und Recht, 2005, 393 (2005)
[Bechtold06]	*Bechtold, Stefan*	Rechtliche Technikgestaltung von Digital-Rights-Management-Systemen – ein Blick auf ein entstehendes Forschungsgebiet	Technikfolgenabschätzung – Theorie und Praxis Nr. 2, 15. Jg., August 2006 http://www.itas.fzk.de/tatup/062/bech06a.pdf (2006)
[Berlakovic]	*Berlakovich, Agnes*	Kryptographie aus rechtlicher und technischer Sicht	http://www.it-law.at/uploads/tx_publications/berlakovich-krypto.pdf (2001)
[Besek]	*Besek, June*	Anti-circumvention laws and copyright: A report from the Kernochan Center for law, media and the arts	Columbia Journal of Law & the Arts, Summer 2004 http://www.columbia.edu/cu/law/easls/papers/Besek%20-%20Anti-Circumvention%20Laws%20and%20Copyright.doc (2004)
[Biehl]	*Biehl, Ingrid*	Copyright-Schutz digitaler Daten durch	in: Colloquia Academica,

		kryptographische Fingerprinting-Schemata	Akademievorträge junger Wissenschaftler, N 1998, 7 (1998)
[Blumenthal]	*Blumenthal, John*	Digital Rights Management Technology	http://www.nap.edu/html/protecting_children/ch11.html (2002)
[Bortloff]	*Bortloff, Nils*	Internationale Lizenzierung von Internet Simulcasts durch die Tonträgerindustrie	GRUR Int. 8-9/2003, 669 (2003)
[Bücherle]	*Bücherle, Manfred*	Das Urheberrecht im World Wide Web	Dissertation, Verlag LexisNexis Orac ARD, Wien (2002)
[Buchinger]	*Buchinger, Johannes/Zivny, Thomas*	Urheberrecht: Kampf den Raubkopien	Die Presse/Rechtspanorama vom 7.4.2003 (2003)
[CEN]	*CEN (European Standard Committee)*	Digital Rights Management - Final Report	http://ec.europa.eu/enterprise/ict/archives/2003/drm.pdf (2003)
[Contentguard]	*Contentguard*	XrML 2.0 Technical Overview	http://www.xrml.org/Reference/XrMLTechnicalOverviewV1.pdf (2002)
[Craig]	*Craig, Cameron/ Graham, Richard*	Rights management in the digital world	CLSR Vol. 19 No. 5, 2003, 356 (2003)
[ct]		Audio-CD-Kopierschutz verärgert Kunden und Händler	http://www.heise.de/ct/00/04/083/ c't 4/2000 (2000)
[Datenschutzgruppe]	*Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten (Artikel – 29 – Datenschutzgruppe)*	Arbeitspapier Datenschutzfragen im Zusammenhang mit Immaterialgüterrechten	WP104, 10092/05/DE http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp104_de.pdf (2005)
[Department]	*Department of Communications, Information Technology and the Arts*	A Guide to Digital Rights Management; DRM and the law	http://web.archive.org/web/20030608093648/www.dcita.gov.au/drm/ (2003)
[Deters]	*Deters, Michael*	MP3, Napster und die	http://www.inpreko

		Folgen	rr.de/361-nap.htm (2001)
[Dillenz]	*Dillenz, Walter/Gutmann, Daniel*	Praxiskommentar zum Urheberrecht	Springer, Wien (2004)
[Dittrich]	*Dittrich, Robert*	Die Festplatte - ein Trägermaterial iSd § 42b UrhG	ÖJZ 2001, 754 (2001)
[Effelsberg]	*Effelsberg, Wolfgang/ Steinmetz, Ralf*	Foliensatz zur Vorlesung Multimediatechnik im WS 2001/2002:Digitale Wasserzeichen	http://www.informatik.uni-mannheim.de/pi4.data/content/courses/2001-ws/multimedia/mm9-1-dt.pdf (2001)
[Ehlers]	*Ehlers, Sabrina*	Sicherheitskonzepte im Internet: Digital Rights Management	Proseminararbeit an der Universität Tübingen, Lehrstuhl Rechnerarchitektur (2002)
[Ernst]	*Ernst, Stefan*	Kopierschutz nach neuem UrhG	CR 1/2004, 39 (2004)
[Eustacchio]	*Eustacchio, Andreas*	Raubkopien aus dem Internet	Lex:itec 04/06, 26 (2006)
[Fallenböck02]	*Fallenböck, Markus/ Haberler, Michael*	Technische Schutzmaßnahmen und Urheberrecht in der Informationsgesellschaft	ecolex 2002, 262 (2002)
[Fallenböck03]	*Fallenböck, Markus/Weitzer, Johann*	Digital Rights Management: A New Approach to Information and Content Management?	CRi 2/2003, 40 (2003)
[Fallenböck04]	*Fallenböck, Markus*	From Anticircumvention Provisions to Intermediary Liability: Digital Rights Management Legislation in Europe and the U.S	MR-Int 2004 (Vol. 1), 11 (2004)
[Federrath]	*Federrath, Hannes*	Steganographie in Rechnernetzen	http://www-sec.uni-regensburg.de/publ/1999/Fede1_99DFNStego.pdf (1999)
[Feigenbaum]	*Feigenbaum, Joan/Freedman, Michael J./ Sander, Tomas/Shostack,*	Privacy Engineering for Digital Rights Management Systems	in *Sander, Tomas* (HG), Security and Privacy in Digital Rights Management,

	Adam		76-105 (2002)
[Flechsig]	*Flechsig, Norbert P.*	Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft	CR 4/1998, 225 (1998)
[Fromm]	*Fromm, Michael/Gruber, Hermann/Schütz, Manfred*	Evaluation of Digital Rights Management Systems	Seminararbeit, Wirtschaftsuniversität Wien, 28. Jänner 2003 (2003)
[Gehring]	*Gehring, Robert*	Digital Rights Management: Ökonomie und Politik im Reich der Ideen	http://www.josefstal.de/mac/days/2004/buch/Gehring-DRM-2005.pdf (2005)
[Geiger]	*Geiger, Christophe*	Right to Copy v- Three-Step Test	CRi 1/2005, 7 (2005)
[Gladney]	*Gladney/Lotspiech*	Safeguarding Digital Library Contents and Users	D-Lib Magazine, May 1997 (1997)
[Graig]	*Craig, Cameron/ Graham, Richard*	Rights management in the digital world	CLSR Vol. 19 No. 5, 2003, 356 (2003)
[Grimm]	*Grimm, Rüdiger/Puchta, Stefan/Müller, Michael/Bizer, Johann/Möller, Jan/Will, Andreas/Müller, Anja/Jazdzejewski, Stefan*	privacy4DRM, Datenschutzverträgliches und nutzungsfreundliches Digital Rights Management	http://www.datenschutzzentrum.de/drm/privacy4drm.pdf (2005)
[Günnewig02]	*Günnewig, Dirk/Hauser, Tobias*	Musik im Hochsicherheitstrakt; Digital Rights Management – Stand der Dinge	c't 16/2002, 182 (2002)
[Günnewig06]	*Günnewig, Dirk*	Digital Rights Management (Präsentation Teilprojekt III: Schutz elektronischer Güter)	http://www.datensicherheit.nrw.de/Daten/WS06122002/guennewig.pdf (2006)
[Guth]	*Guth, Susanne*	Interoperability of Digital Rights Management Systems via the Exchange of XML-based Rights Expressions	Dissertation (2004)
[Handig03]	*Handig, Christian*	Urheberrechtsnovelle 2003; Wesentliche	ÖBl 2003, 212 (2003)

		Änderungen infolge der Anpassung an die Informationsgesellschaft	
[Handig04-1]	*Handig, Christian*	Das Zurverfügungsstellungsrecht und die Hyperlinks	ecolex 2004, 38 (2004)
[Handig04-2]	*Handig, Christian*	Die Nutzung des World Wide Web aus urheberrechtlicher Sicht	ÖBl 2004, 196 (2004)
[Hansen]	*Hansen, Markus/ Möller, Jan*	Digital Rights Management zwischen Sicherheit und informationeller Selbstbestimmung	https://www.datenschutzzentrum.de/vortraege/050510_hansen-moeller_bsi.htm (2005)
[Hartung]	*Hartung, Frank/Ramme, Friedhelm*	Digital Rights Management and Watermarking of Multimedia Content for M-Commerce Applications	IEEE Communications Magazine, November 2000, 78 (2000)
[Hassler]	*Hassler, Vesna*	Security Fundamentals for E-Commerce	Artech House Computer Security Series (2000)
[Helberger]	*Helberger, Natali*	Digital Rights Management and Consumer Acceptability	http://www.indicare.org/tiki-download_file.php?fileId=111 (2005)
[Himmelein]	*Himmelein, Gerald*	Der digitale Knebel	C't 2002, Heft 15, 18 (2002)
[Hofmair]	*Hofmair, Philip*	Asset- und Rechtemanagement im Umfeld digitaler Bibliotheken	http://www.know-center.tugraz.at/content/download/576/3503/file/2004_Dip_PHofmaier.pdf (2005)
[Holznagel]	*Holznagel, Bernd/Brüggemann, Sandra*	Das Digital Right Management nach dem ersten Korb der Urheberrechtsnovelle	MMR 12/2003, 767 (2003)
[Huppertz]	*Huppertz, Marie-Thérèse*	The Pivotal Role of Digital Rights Management Systems in the Digital World	CRi 4/2002, 105 (2002)
[Iannella]	*Iannella, Renato*	Digital Rights Management (DRM) Architectures	D-Lib Magazine, Volume 7 Number 6, ISSN 1082-9873; http://www.dlib.org/dlib/june01/iannell

			a/06iannella.html (2001)
[Jahnke]	*Jahnke, Tino*	Die Bedeutung von digitalen Wasserzeichen in elektronischen Bildern	Diplomarbeit http://www.knowledgebay.de/upload/media/veranstaltung/262/docs/Diplomarbeit%20Tino%20Jahnke%20-600dpi.pdf (2002)
[Johnson]	*Johnson, Neil F./Duric, Zoran/Jajodia, Sushil*	Information Hiding: Steganography and Watermarking - Attacks and Countermeasures	Kluwer Academic Publishers (2000)
[Juraschko]	*Juraschko, Bernd*	Digital Rights Management und Zwangslizenz	Bibliotheksdienst 40. Jg. (2006), H. 7 http://www.zlb.de/aktivitaeten/bd_neu/heftinhalte2006/Recht010706.pdf (2006)
[Kappes]	*Kappes, Andre*	Die Audiokodierung mp3	http://www.mp3encoding.de (2002)
[Koch]	*Koch, Franz A.*	Urheberrechtliche Zulässigkeit technischer Beschränkungen und Kontrolle der Software-Nutzung	CR 9/2002, 629 (2002)
[Kommission 04]	*Mitteilung der Kommission an den Rat, das Europäische Parlament und den Europäischen Wirtschafts- und Sozialausschuss*	Die Wahrnehmung von Urheberrechten und verwandten Schutzrechten im Binnenmarkt	KOM(2004) 261 endgültig (2004)
[Kommission 05]	*Kommission der Europäischen Gemeinschaften*	Empfehlung der Kommission vom 18. Mai 2005 für die länderübergreifende kollektive Wahrnehmung von Urheberrechten und verwandten Schutzrechten, die für legale Online-Musikdienste benötigt werden (2005/737/EG)	Amtsblatt Nr. L 276 vom 21/10/2005 (2005)
[Korba]	*Korba,*	Applying Digital Rights	Journal of Computers

	Larry/Kenny, Steve	Management Systems toPrivacy Rights Management	and Security, November 2002. NRC 44955 http://iit-iti.nrc-cnrc.gc.ca/iit-publications-iti/docs/NRC-44955.pdf (2002)
[Martin]	*Martin, Gerd*	Software-Muttermale verraten diebische Programmierer	www.computerzeitung.de/kn31246895 (2007)
[Memon]	*Memon, Nasir/Wong, Ping Wah*	Protecting Digital Media Content	Communications of the ACM, July 1998, Vol. 41, No. 7, 35 (1998)
[Microsoft]	*Microsoft Corporation*	Advanced Systems Format (ASF) Specification, December 2004	http://www.microsoft.com/windows/windowsmedia/forpros/format/asfspec.aspx (2004)
[Microsoft FAQ]	*Microsoft Corporation*	Häufig gestellte Fragen (FAQ) zu Windows Media DRM	http://www.microsoft.com/windows/windowsmedia/de/drm/faq.aspx (2008)
[Miller]	*Miller, Matt/Cox, Ingemar/Linnartz, Jean-Paul/Kalker, Ton*	A review of watermarking principles and practices	Digital Signal Processing in Multimedia Systems, Ed. K. K. Parhi and T. Nishitani, Marcell Dekker Inc., 461-485 (1999)
[Mitchell]	*Mitchell, Iain G.*	Humpty Dumpty, DRM and the InfoSoc Directive	MMR 9/2003, Editorial, 549 (2003)
[Mohanty]	*Mohanty, Saraju*	Digital Watermarking : A Tutorial Review	http://www.cs.unt.edu/~smohanty/research/Reports/MohantyWatermarkingSurvey1999.pdf (1999)
[Muharemagic]	*Muharemagic, Edin/Furht, Borko*	Multimedia Security: Watermarking Techniques	http://www.cse.fau.edu/~borko/MulChapter,%20Watermarking%20IEC2004.pdf (2004)
[Noll]	*Noll, Alfred J.*	Der Musik-Download im Lichte des Dreistufentests	MR 6/04, 400 (2004)
[Office]	*Office of Legal*	Regents Guide to	http://www.usg.edu

	Affairs	Understanding Copyright & Educational Fair Use	/legal/copyright/ (1997)
[OGH60]	*Oberster Gerichtshof*	4 Ob 317/60, 26.4.1960	SZ 33/45 (1960)
[OGH99]	*Oberster Gerichtshof*	4 b 345/98h, 26.1.1999	SZ 72/11 (1999)
[OGH05]	*Oberster Gerichtshof*	4 Ob 115/05y, 12.7.2005	SZ 2005/99 (2005)
[OLG85]	*Oberlandesgericht Wien*	19.12.1985	MR 1986 H2, 23 (1986)
[Pack]	*Pack, Thomas*	Digital Rights Management: Can Technology Provide Long-Term Solutions?	Econtent, May 2001, 22 (2001)
[Park]	*Park, Jaehong*	Digital Rights Management and Beyond	http://www.list.gmu.edu/infs767/infs767fall01/lec9.pdf (2001)
[Perry]	*Perry, Burt/MacIntosh, Brian/Cushman, Dave*	Digimarc MediaBridge - The birth of a consumer product, from concept to commercial adaptation	http://www.digimarc.com/tech/docs/dmrc_media_bridge.pdf (2002)
[Petitcolas]	*Petitcolas, Fabien*	Watermarking schemes evaluation	www.petitcolas.net/fabien/publications/ieeespm00-evaluation.doc (2000)
[Picot]	*Picot, Arnold*	Digital Rights Management	Springer-Verlag Berlin Heidelberg (2003)
[Plura]	*Plura, Michael*	TCPA: Microsoft und Intel 'sichern' den PC	c't 22/2002, 204 http://www.heise.de/ct/02/22/204/ (2002)
[Podilchuk]	*Podilchuk, Christine I./Delp, Edward J.*	Digital Watermarking: Algorithms and Applications	IEEE Signal Processing Magazine, July 2001, 33 (2001)
[Presse]	*Die Presse*	Digitale Musik: Die Raubkopierer haben gewonnen	Die Presse – Pressenachricht vom 11.1.2008 (2008)
[Retzer]	*Retzer, Karin*	On the Technical Protection of Copyright	CRi 5/2002, 134 (2002)
[Rosenblatt 02]	*Rosenblatt, Bill/Trippe, Bill/Mooney, Stephen*	Digital Rights Management, Business and Technology	M&T Books, New York (2002)
[Rosenblatt]	*Rosenblatt, Bill*	Integrating DRM with P2P Networks: Enabling	http://www.drmwatch.com/resources/w

		the Future of Online Content Business Models	hitepapers/article.php/11655_3112631_1 (2003)
[Ruanaidh]	*Ruanaidh/Dowling /Boland*	Watermarking digital images for copyright protection	IEE Proc.-Vis. Image Signal Process., August 1996, Vol. 143, No.4, 250 (1996)
[Rump]	*Rump, Niels*	Digital Rights Management: Technological Aspects	E. Becker et al. (Eds.): Digital Rights Management, Springer-Verlag Berlin Heidelberg (2003)
[Schmidbauer]	*Schmidbauer, Franz*	Internet&Recht	http://www.internet4jurists.at/ (2007)
[Schmucker]	*Schmucker, Martin*	Protection of coded music	http://www.interactivemusicnetwork.org/wg_protection/upload/musicnetwork-de4-5-2-prot-protection-of-coded-music_v1-3.pdf (2005)
[Schwarz-Gondek]	*Schwarz-Gondek, Nicolai*	Digital Rights Management durch Kopierschutzmaßnahmen in Audio-CDs: Technische und urheberrechtliche Aspekte	TKMR 4/2003, 250 (2003)
[Screamer]	"*Beale Screamer*"	Microsoft's Digital Rights Management Scheme - Technical Details	http://cryptome.org/ms-drm.htm (2001)
[Spiegel]	*Spiegel Online*	Microsofts Musik-Kopierschutz geknackt	http://www.spiegel.de/netzwelt/tech/0,1518,434036,00.html (2006)
[Spindler]	*Spindler, Gerald*	Die kollisionsrechtliche Behandlung von Urheberrechtsverletzungen im Internet	IPRax 5/2003, 412 (2003)
[Stach]	*Stach, John/Brundage, Trent/Hannigan, Brett/Bradley, Brett/Kirk, Tony/Brunk, Hugh*	On the use of web cameras for watermark detection	http://www.digimarc.com/tech/docs/dmrc_web_cameras.pdf (2002)
[Standard]	derStandard	iTunes-Konkurrenz ohne	derStandard –

		Digitales Rechtemanagement	Pressenachricht vom 15.2.2005 (2005)
[Stomper03-1]	*Stomper, Bettina*	Internet-Tauschbörsen nach der UrhG-Novelle	RdW 7/2003, 368 (2003)
[Stomper03-2]	*Stomper, Bettina*	Das neue Urheberrecht: Mehr Schutz für Rechteinhaber	http://www.fafo.at/download/Anti-Piraterie/News-Urheberr.pdf (2003)
[Strasser]	*Strasser, Mathias*	A&M Records v Napster	medien und recht 2001, 6 (2001)
[Thiele]	*Thiele, Clemens/Laimer, Barbara*	Die Privatkopie nach der Urheberrechtsgesetznovelle 2003	ÖBl 2004, 52 (2004)
[Trybus]	*Trybus, Peter*	Digital Rights Management-Systeme im Spannungsfeld von technischem und rechtlichem Schutz	http://www2.wu-wien.ac.at/informationsrecht/Rechtsinformationen/Seminararbeiten/DRM_Peter_Trybus.pdf (2004)
[Waß]	*Waß, Clemens Matthias*	Digital Rights Management – Die Zukunft des Urheberrechts?	http://www.rechtsprobleme.at/doks/wass-drm.pdf (2002)
[Wayner]	*Wayner, Peter*	Digital Copyright Protection	Academic Press Professional (1997)
[Wiebe03-1]	*Wiebe, Andreas*	Das neue „digitale“ Urheberrecht – Eine erste Bewertung	MR 5/2003, 309 (2003)
[Wiebe03-2]	*Wiebe, Andreas/Leupold, Andreas*	Digital Rights Management	in *Wiebe, Andreas/Leupold, Andreas* (HG), Recht der elektronischen Datenbanken, Teil V/C, C.F. Müller (2003)
[WIPO]	*WIPO standing committee on copyright and related rights*	Current developments in the field of digital rights management (Tenth Session)	http://www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf (2003)
[Worlock]	*Worlock, Kate*	Digital Rights Management: Moving from Theory to Implementation	World Internet Law Report, 06/04, 26 (2004)

8. Abbildungsverzeichnis