Digital Rights Management Systeme:

Implementierungsstrategien und Auswirkungen auf Datenschutz- und Urheberrechte vor dem Hintergrund der Internetkommerzialisierung

Web-Version V 1.0a der

D I P L O M A R B E I T

zur Erlangung des Magistergrades der

Philosophie

an der Fakultät für

Sozialwissenschaften der Universität Wien

eingereicht von

Christian Gossmann

Wien, (Juni, 2006)

Danksagung

Primären Dank möchte ich meinem Diplomarbeitsbetreuer Dr. Michael Latzer für das Beharren auf einem klaren Konzept aussprechen. Ohne dieses wäre die Arbeit im Nachhinein betrachtet wegen der Informationsfülle des verarbeiteten Materials nicht in dieser Form realisierbar gewesen. Dank gilt auch Mag. Florian Saurwein für die anfänglich orientierende Unterstützung zur Durchführung. Informationsrechtsexperte Dr. Nikolaus Forgó gebührt ebenfalls Lob und Anerkennung für die Bereitschaft zu einem aufschlussreichen Interview. Außerdem gilt der Dank Michael Bischoff für seine geleistete Übersetzungsarbeit von Lessigs Werk: „Code and other Laws of Cyberspace“ und allen sonstigen Verfassern literarischer Werke und Fachschriften, die sich schon mit Problemstellungen hinsichtlich des noch jungen Themenbereichs Digital Rights Management auseinandergesetzt haben. Ferner soll noch den Herstellern von Computern und Textverarbeitungssystemen, besonders denen, die für die dortigen Rechtschreib- und Grammatikprüfprogramme verantwortlich waren, gedankt werden[1]. Letztlich gebührt aber auch der Dank den Raubkopierern, die es erst ermöglicht haben, dieses für mich beruflich wie privat interessante Thema zu bearbeiten.

Ich widme dieses Werk meiner Familie.

[1] Sollten Sie diesbezüglich Fehler entdecken, so melden Sie diese bitte an fehler@rechtschreibung.at. Eine fehlerbereinigte Version dieser Arbeit wird dann so schnell wie möglich ins Netz gestellt.

Ehrenwörtliche Erklärung

Hiermit erkläre ich, Christian Gossmann, geb. am 3. Juni 1976, ehrenwörtlich, vorliegende Arbeit eigenständig und ohne fremde Hilfe, mit Ausnahme der angegebenen Literatur und den sonstigen Quellen dazu nach bestem Wissen und Gewissen verfasst zu haben. Die Arbeit wurde bisher noch nirgendwo sonst veröffentlicht und an keiner anderen Universität eingereicht (ausgenommen die Universität Wien, wo sie erstmals eingereicht wird). Sämtliche Hinweise und Verfahren wurden mit größter Sorgfalt recherchiert. Durch die Natur des Themas wird ausdrücklich darauf hingewiesen, dass für Strafverfolgung durch Anwendung einiger erläuterter Verfahren zur Umgehung von Schutzmechanismen für digitales geistiges Eigentum keinerlei Haftung übernommen werden kann (besonders wenn diese Verfahren in Deutschland oder in den USA nachvollzogen werden). Ferner distanziere ich mich ausdrücklich von missbräuchlicher Verwendung der preisgegebenen Verfahren zur Fertigung von Plagiaten und Raubkopien. Alle Hinweise und Verfahren sind daher für rein wissenschaftliche / akademische Zwecke bestimmt.

Vorwort

Diese Arbeit zeigt, warum digitale Inhalte nicht so genutzt werden können, wie man dies eigentlich nach Bezahlung erwartet. Etliche Schutzmechanismen an geistigem Eigentum der Unterhaltungs- und Computerindustrie hindern einen in heutiger Zeit einfach daran, Software auf verschiedenen Endgeräten weiterhin einzusetzen (v.a. dann, wenn die alten defekt werden). Sogar Filme, die man sich aus den USA auf DVDs mitnimmt, werden hier bei der Einreise zwar verzollt, nur um danach festzustellen, dass sie gar nicht abgespielt werden können. Musik-CDs ereilt das gleiche Schicksal im Autoradio. Es werden somit erhebliche Entwicklungsressourcen anstatt in „günstigeres Verfügbarmachen“ von Unterhaltungsmedien und Software in Schutzmechanismen und Allianzen zur Entwicklung von Digital Rights Management-Standards gesteckt. Diese Entwicklungen können dann im Extremfall Systeme unbrauchbar machen und sogar Datenspionage bezüglich des Nutzungsverhaltens betreiben. Die vorliegende Arbeit untersucht die Gründe dafür und soll auch aufzeigen, warum dies vielleicht doch zum größten Teil dem Anwender (Raubkopierer) zu verdanken ist, dass die Industrie sich gegen Verluste durch unbefugte Vervielfältigungen zu wehren versucht.

Christian
www.Gossmann.at

Eisenstadt, Juni 2006

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1. Problemstellung

> Die wirksamen rechtlichen Beschränkungen (des Kopierens) verschwinden im selben Augenblick wie die technischen Beschränkungen. Die technische Bedrohung ist maximal, der vom Gesetz gebotene Schutz dagegen nur noch minimal. Für den Urheberrechtsinhaber vereint der Cyberspace die schlechtesten Eigenschaften beider Welten – die Kopiermöglichkeiten könnten nicht besser und der rechtliche Schutz nicht schlechter sein[2].
>
> Lawrence Lessig

Rechtsprofessor Lawrence Lessig der Stanford Law School erkannte hier schon 2001 treffend, was unmittelbar von diesem Problem Betroffene erst einige Zeit später bemerkten und durch Verzweiflungsrufe bestätigten[3]:

Britney Spears (Sängerin, Schauspielerin)	CDs im Laden klauen oder illegal Musik downloaden – das ist für mich das Gleiche
Missy Elliot (Sängerin)	Tauschbörsen sind eine Bedrohung für das Musikgeschäft.
Frank Farian (Produzent und Labelboss).	Die Scheiben müssen billiger werden. Bei den Preisen darf man sich nicht wundern, wenn die Jugendlichen Raubkopien brennen oder Songs aus dem Netz laden
Smudo (Rapper und Label-Inhaber)	Wir von den Fantastischen Vier haben noch die fetten Jahre erlebt. Jetzt sag´ ich jungen Künstlern: Macht Musik, weil´s Spaß macht, nicht, um Geld zu verdienen
Shakira (Sängerin)	Wenn jemand illegal Musik im Web anbietet und herunterlädt, schadet das nicht nur den Musikern, sondern allen Beteiligten wie Autoren und Produzenten

Dies vor Augen wird in der vorliegenden Arbeit auf die Gefahren für geistiges Eigentum im digitalen Zeitalter eingegangen – o.a. Stimmen standen dabei lediglich für die Musikindustrie (CDs und Online-Musik). Längst sind aber auch Filme von dieser Entwicklung betroffen. Computersoftware und Texte auf Websites runden dabei die wichtigsten Kategorien digitalen geistigen Eigentums ab. Daher sind wo auch immer im Laufe dieser Arbeit von „Content“ die Rede ist sämtliche o.a. digitalen Werke gemeint. Technischer Fortschritt, Breitbandinternetzugänge und höhere Verarbeitungsgeschwindigkeiten von Computeranlagen ermöglichen es geradezu, digitale Güter für jedermann/-frau immer schneller verteilen und v.a. vervielfältigen zu können. Seith drückt dies infolge der Dematerialisierung analoger Güter auf den Punkt getroffen aus: „Das Wandern ist des Werkes Lust.[4]“ Anzumerken wäre hier, den

[2] Zitat: Lessig, 2001, S. 224.
[3] Zitate nach: Kunterding Kathrin: Tauschrausch im Web. Die MP3-Revolution. In: Tomorrow, April 2003, S. 60 ff.
[4] Zitat: Seith, 2003, S. 53.

„Wanderbegriff“ mit „Vervielfältigung“ und damit „Kopieren“ gleichzusetzen. Dann dürfte auch die Problematik, die sich aus der globalen Vernetzung durch das Internet ergibt, erkannt sein. Immerhin sind digitale Daten seit jeher der Grundstoff des Internets und damit von Computeranlagen[5]. Kernpunkt der Untersuchung ist daher folgende:

1.1. Forschungsfrage

Wie und zu welchem Preis in Hinblick auf Datenschutz wird Zugang und Nutzung geistigen Eigentums im digitalen Zeitalter reguliert, um unbefugte Vervielfältigungen zu verhindern und Marktversagen vorzubeugen?

Versagt hier nämlich der Markt (staatliche Regulierung), so ist es durchaus legitim, den Schutz für geistiges Eigentum in die Hände der Betroffenen selbst zu legen (=Implementierung von Digital Rights Management Systemen – im Folgenden DRMS), um o.a. Vervielfältigungsprobleme in den Griff zu bekommen. Zu Grunde liegender theoretischer Ansatz ist dabei, dass digitales geistiges Eigentum (=Content) nur dann kommerziell produziert wird, wenn es sich auch lohnt – konkret also, solange Schutzmöglichkeiten bestehen und Vergütung als Anreizwirkung sichergestellt ist[6]. Als Unterfragen werden die einzelnen betroffenen Bereiche behandelt, d.h. also die eigentliche Implementierung und die Auswirkungen auf die Urheberrechte, konkret also:

1. Welche Implementierungen von DRMS gibt es bereits und reichen deren Schutzmöglichkeiten zur Sicherung kommerzieller Vergütung für Content aus?
2. Ist eben jenes Urheberrecht, bzw. der Regulator „Staat“ den neuen Herausforderungen nicht mehr gewachsen gewesen, wenn DRMS im Sinne einer Transformation von Staatlichkeit implementiert werden konnten? Wie ist dies in Hinblick auf Schrankenbestimmungen in Urheberrechten zu beurteilen?
3. Zu welchem Preis geschieht Regulierung digitalen geistigen Eigentums bezogen auf Datenschutz? Wird Datenschutz durch DRMS-Implementierung eingehalten oder opfert man hier zwecks besserer Schutzmöglichkeiten von Content Privatsphäre durch totale Überwachung der Nutzungshandlungen?

[5] Vgl. Bröcker Klaus Tim: Schutz des Nutzers im Netz: Datenschutz und Datensicherheit. In: Bröcker, 2003, S. 231.

1.2. Methodik

Die Beantwortung erfolgt anhand wissenschaftlicher Literatur und Fachschriften, sowie einem Interview mit Informationsrechtsexperte Dr. Nikolaus Forgó. Dies soll mit Augenmerk auf die vier Regulierungsbereiche Lawrence Lessigs geschehen (Markt, Recht, Architektur / Code, Normen). Beschränkt wird die Darstellung dabei auf die wichtigen IT-Märkte USA und Deutschland[7].

1.3. Gang der Darstellung und Erkenntnisziel

Der Schwerpunkt liegt bei der Behandlung der Implementierung von DRMS für Content im Internet und in abgespeicherter Form auf externen Datenträgern. Im *ersten Teil* wird auf die Schutzerfordernisse geistigen Eigentums und Implementierungsstrategien von DRM eingegangen, ohne dabei zu sehr in technische Details abzuschweifen (dies allein würde ganze Bände füllen) – wo dies allerdings zwecks Verständlichkeit unerlässlich ist, wird dies in Hinblick auf den Schutzmechanismus von Content erläutert. Außerdem werden bereits hier einige Probleme in Hinblick auf deren urheberrechtliche Relevanz erörtert. Generelle Relevanz erlangt das Thema dabei deswegen, da an DRMS nicht etwa erst seit der internationalen rechtlichen Verankerung des Schutzes digitalen geistigen Eigentums durch die Regelungen in den TRIPS-Abkommen gearbeitet wurde, sondern schon seit den Achtzigern des 20. Jhdt[8]. Die Vielfältigkeit der verschiedenen DRMS macht es erforderlich, die Auswahl auf die wichtigsten Systeme zu beschränken – dabei steht vor allem das mit 92% aller Systeme vertretene Windows im Vordergrund, wie folgende Abbildung der verwendeten Betriebssysteme zum Aufruf von Websites zeigt. Dieser ist zu entnehmen, dass Windows XP dabei mit fast 2/3 aller Systeme den Löwenanteil ausmacht, Mac OS dagegen mit 4,3% eine verschwindend geringe Präsenz hat. Für DRMS ist dies bedeutsam, da der zu behandelnde Media Player und die Aktivierung als Schutzmechanismus gerade dort Anwendung finden, was datenschutzrechtlich bedenklich ist.

---

[6] So auch Lessig, 2001, S. 237.
[7] Österreich ließe sich hier schlecht mit der Größenordnung eines Staates wie die USA es sind vergleichen.
[8] Vgl. Bechtold, 2002, S. 21.

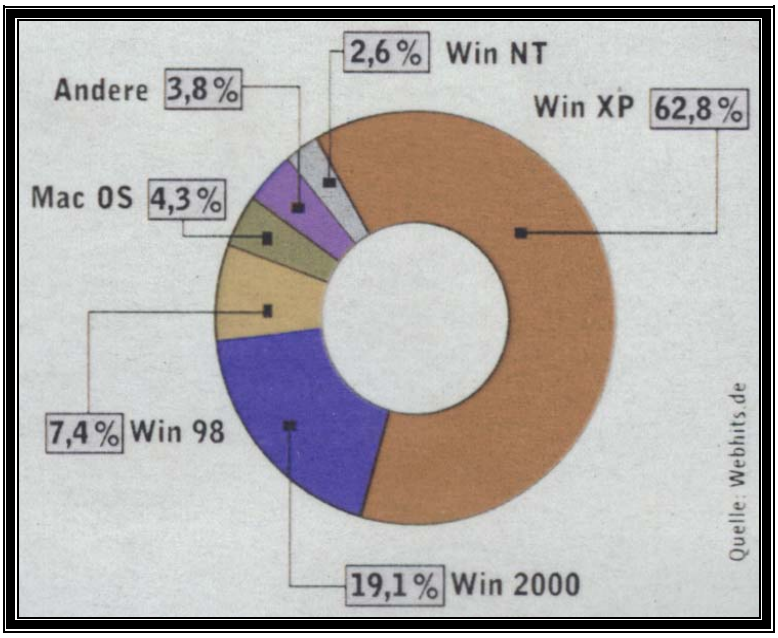

Abbildung 1: Verbreitung von genutzten Computer-Systemen[9]

An Beispielen werden allerdings nicht nur die primären Sicherungsmechanismen und Schwachstellen dieses Systems, sondern derer von DRMS generell aufgezeigt. Im *zweiten Teil* werden dann die eigentlichen Auswirkungen der Implementierungen auf Urheberrechte speziell in Hinblick auf die Unterschiede in den USA und Deutschland, sowie die rechtlichen Reaktionen und Sanktionsbestimmungen des Gesetzgebers behandelt. Dabei soll als Erkenntnisziel deutlich werden, dass hier fundamentale Unterschiede zwischen den US-Auffassungen von Urheberechtsschutz und denen von Deutschland bestehen. Im *dritten Teil* folgt die Fortsetzung der divergierenden Ansichten beider Staaten unter datenschutzrechtlichen Auswirkungen von DRMS, d.h. also vereinfacht ausgedrückt, wie viel Regulierungskompetenz hier noch beim Staat verbleiben soll und wie viel bei Privaten. Ausdrücklich nicht behandelt werden dagegen die Schwierigkeiten, die sich aus patentrechtlichen Ansprüchen auf DRMS und die Bereitstellung von Content über derartige kommerzielle Spezialschnittstellensysteme ergeben. Es steht ausschließlich die Wertschöpfungskette durch den Content im Vordergrund.

[9] Aus: Chip, 06 / 2006, S. 62.

2. Implementierungsstrategien

2.1. Die Definitionsversuche: DRM und DRMS

Bevor die Problembereiche der DRM-Implementierung behandeln werden, ist eine Definition für DRM und DRMS erforderlich. Da hierbei ein junger Technologiebereich tangiert ist, gibt es aber noch keine einheitliche Definition[10]. Rump bietet schon zwei verschiedene Definitionen an, wobei eine auf „whatis.com“ basiert und auf den zu regulierenden Content durch DRM abstellt. Es soll Software entwickelt werden, die *erstens* dessen sichere Verteilung ermöglicht, *zweitens* illegalen Vertrieb unterbindet[11]. Gefragt werden muss nun, welche Verteilung und welcher Vertrieb hier gemeint ist? Dabei kann nur digitaler Content gemeint sein, da das Wort Digital Rights Management schon darauf schließen lässt. Diese Definition ist allerdings etwas eng. Weitaus konkreter und viel offener gehalten ist die zweite Definition. Hier wird davon ausgegangen, dass schlichtweg jegliche auf Content angewandte Handlung, deren Ziel Vermarktung ist, zu DRM gehört. Anzumerken wäre, dass hier eine große Lücke besteht, denn würde man tatsächlich auf dieser Definition beharren, so würde auch jegliche illegale Vermarktung von Content (=Raubkopien) darunter fallen – dies aber soll der ersten Definition folgend verhindert, d.h. also reguliert, werden. Somit basieren im Kern sämtliche DRMS auf Enforcement der Regulierung von Contentnutzung im Sinne der Rechteinhaber, also der Urheber[12]. Hier mag der Einwand angebracht sein, dass die Definitionen alle DRM behandeln – was DRMS sind, blieb bisher offen. Fränkl räumt ein, dass es gar keine geeignete Definition für DRMS gibt. Damit sieht es hier noch schlechter aus, als bei den Definitionsversuchen zu DRM. Es gibt lediglich einen Vorschlag, der da lautet:

> Digital Rights Management Systeme sind technischen Lösungen zur sicheren zugangs- und nutzungskontrollierten Distribution, Abrechnung und Verwaltung von digitalem und physischem Content[13].

[10] Vgl. Fränkl, 2004, S. 25.
[11] Vgl. Rump Niels: Digital Rights Management: Technological Aspects. Definition, Aspects, and Overview. In: Becker, 2003, S. 3.
[12] Vgl. Rump Niels: Digital Rights Management: Technological Aspects. Definition, Aspects, and Overview. In: Becker, 2003, S. 4.
[13] Zitat: Fränkl, 2004, S. 26.

Wohl handelt es sich deshalb bloß um einen Vorschlag, da der eigentlich Kern, nämlich der DRM-Teil ohnehin selbst definiert wurde als:

> Digital Rights Management (DRM) involves the description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets – both in physical and digital form – including management of Rights Holders relationships[14].

Bei der Kombination aus dem Vorschlag und der Definition handelt es sich bei DRMS somit um die hardwaremäßige Implementierung des softwaremäßigen DRM. Damit verwundert es auch nicht mehr, dass eine explizite DRMS-Defintion fehlt. Hat man den Kern der Problematik verstanden, wird diese aber auch nicht mehr gebraucht. Auch Bechtold ist der Ansicht, dass DRMS primär auf die Zugangs- und Nutzungskontrolle abzielen, mit Hauptsicherheitsmerkmal der Verschlüsselung Marks folgend: „Encryption of content is the keystone of current copy protection efforts.[15]“ Problematisch bei DRM-Implementierung ist aber die Vielzahl an unterschiedlichen beteiligten Akteuren. Dies beginnt bei den Contenturhebern, zieht sich über die Hersteller von DRMS und Entwickler von Verschlüsselungsalgorithmen bis zu den Herstellern von Netzinfrastruktur, über die letztlich der Content zuverlässig freigeschaltet oder der Zugriff auf ihn gesperrt wird. D.h. letztlich, dass das gesamte System sicher vor Störungen sein muss. Dr. Sergio Montenegro vom Fraunhofer Institut FIRST stellte dazu treffend fest: „Im sicheren System gilt der Grundsatz: Niemand darf von anderen abhängig sein.[16]“ Damit ist aber die Hauptschwachstelle von DRMS aufgezeigt, denn die Äußerung Montenegros ist klares Wunschdenken, da in einem globalen Markt jeder von jedem abhängig ist. Implementierung durch mehrere beteiligte Stellen zieht nämlich Fehler bei der Kommunikation in Hinblick auf die Interessenlage nach sich, d.h. also, ein ideales DRMS gibt es nicht. Folgt man Bechtold, dürften die Zugangs- und Nutzungskontrollmechanismen in einem idealen DRMS erst gar nicht zum Zuge kommen, da unbefugte Dritte von vornherein den Content gar nicht nutzen könnten. DRM-Nutzungsverträge wirken dabei absolut in dem Sinne, dass es sich hierbei um private Gesetzgebung handelt[17]. Seith liegt in diesem Zusammenhang richtig, wenn er die Frage aufwirft, ob denn nicht nur Konvergenz von Medien, denn

[14] Zitat nach: Fränkl, 2004, S. 29.
[15] Zitat nach: Bechtold, 2002, S. 23
[16] Zitat nach: Flohr Manfred: Programmierter Absturz. Software der Zukunft. In: Chip, 09 / 2004, S. 142 f.

Konvergenz von Urheberrecht und Technologie vorliegt[18]. Die Lösung besteht aber nur darin, Content mit DRM zu kapseln und Rechteverwaltung (Zugang und Nutzung) inkl. Bezahlung sicherzustellen – so jedenfalls lautet von Diemars Definition:

> Grundsätzlich werden daher unter dem Sammelbegriff DRM-System umfassende digitale Vertriebssysteme verstanden, die eine Kombination von technischen Schutzmaßnahmen mit Registrierungs- und Abrechnungsmechanismen darstellen[19].

Freilich räumt auch von Diemar das fehlen einer allgemeingültigen und anerkannten Definition ein. Das Abhängigkeitsgefüge der Wirkungen und Beschränkungen in DRMS wird dabei in folgender Abbildung deutlich – die wichtigsten Einzelpunkte werden im weiteren Verlauf dieser Arbeit noch genauer erläutert. Für das weitere Verständnis der Vorgehensweise ist die grafische Veranschaulichung jedoch hilfreich:

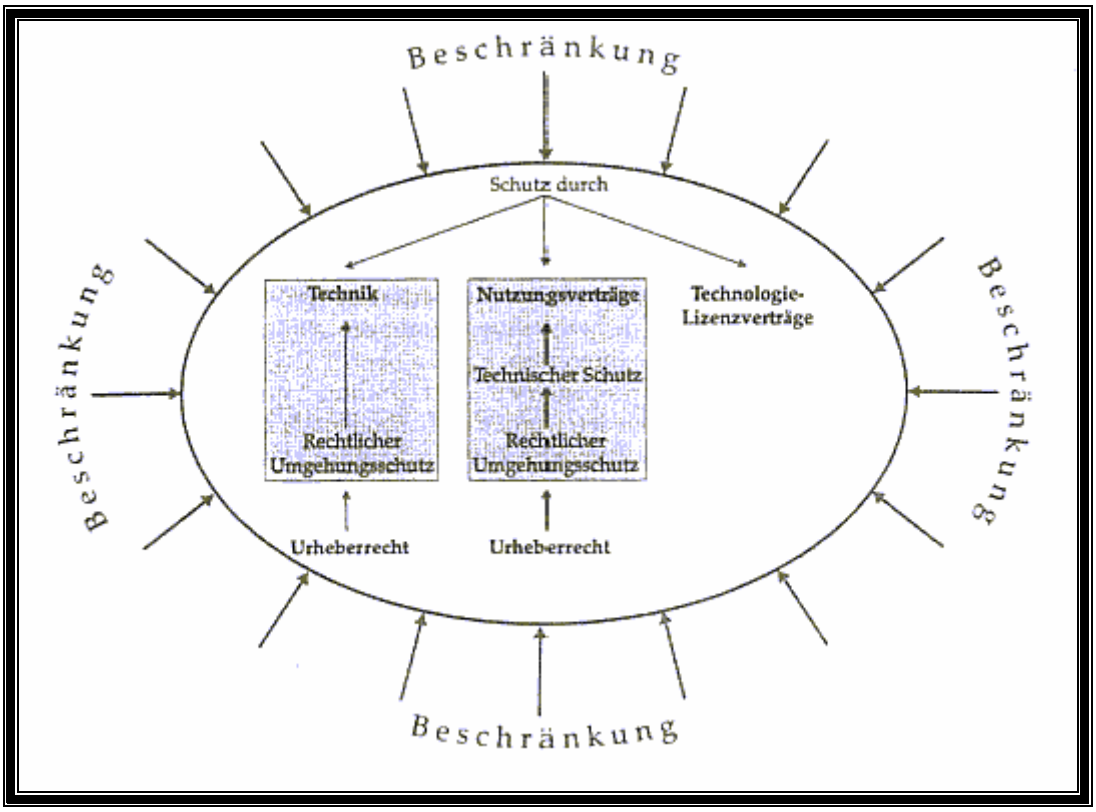

Abbildung 2: Das Wirkungsgefüge des DRM-Schutzes[20]

Anzumerken wäre zu den Beschränkungen, dass diese in Form der Schrankenregelungen durch Beeinflussung einer der vier Regulierungsebenen Lessigs

---

[17] Vgl. Bechtold, 2002, S. 277 f.
[18] Vgl. Seith, 2003, S. 65.
[19] Zitat: von Diemar, 2002, S. 149.
[20] Aus: Bechtold, 2002, S. 384.

verstanden werden können[21]. Ferner ist festzuhalten, dass durch die Vielzahl der beteiligten Subsysteme DRM von der Grundkonzeption her versagensgefährdet ist. Jeder Bereich verlässt sich quasi auf Regulierung in und durch den anderen Bereich. Daher handelt es sich bei den Implementierungsstrategien des gesamten DRM um planungslose Vorgehensweisen ohne einheitliche Standards. Kommen auf diese nun noch gezielte Ein- oder Angriffe durch Kriminelle oder Private dazu, sieht es mit der Sicherheit entsprechend schlecht aus.

2.2. Probleme und Interessenslage bei der Implementierung

Bei der Implementierung von DRMS existieren viele Einschnitte und internationale Probleme beim Versuch, Schutz für geistiges Eigentum im digitalen Zeitalter zu realisieren. Günnewig führt hier sechs Punkte auf[22]. Darunter fallen *erstens* Ausnahmen zur Anfertigung von Kopien, was problematisch in der Technik des DRMS ist – dieses muss hier zwischen legitimen und illegitimen Ansprüchen unterscheiden (ein Problem, das noch nicht gelöst ist). *Zweitens* müssen sich legale Distributionswege (Film- und Musikdownload im Internet) gegen illegale (z.B. Tauschbörsen) behaupten. *Drittens* ist die rechtliche Durchsetzung problematisch (Globalität des Internets). *Viertens* werden erst durch DRMS neue Möglichkeiten der Behandlung geistigen Eigentums geschaffen. *Fünftens* wird das Gleichgewicht der Kräfte zwischen den Beteiligten (Rechteinhaber, DRMS-Hersteller, Nutzer von Content) durch erstmalig auftauchende technische Innovationen in einem Bereich (Schutz im Content selbst, Schutz beim Vertrieb, bzw. im DRMS selbst oder bei einer Umgehungstechnologie) stets zu Ungunsten der anderen verschoben. *Letztlich* sind auch andere Beteiligte von der Implementierung von DRMS betroffen (z.B. Verwertungsgesellschaften oder klassische Wertschöpfungsketten wie der / die Verkäufer[in] im Einzelhandel). So hat der Urheber Interesse an Vergütung und Schutz seines geistigen Eigentums, der DRMS-Hersteller Interesse an der Vermarktung seiner Technologie, der Anwender an freier Werknutzung ohne von Aktivierung und der Gefahr der Profilbildung durch heimlich wirkendes DRM abhängig zu sein. Seith weist dabei auf die mangelnde institutionelle, organisatorische und technische Infrastruktur, sowie deren Zusammenwirken als Hemmnis hin. Besonders

[21] Vgl. Lessig, 2001, S. 162 f.
[22] Vgl. Günnewig Dirk: New Copyright for the Digital Age: Political Conflicts in Germany. In: Becker, 2003, S. 528.

gilt dies für Märkte, die gänzlich noch wenige bis gar keine Bestrebungen in diese Richtung unternommen haben[23]. DRM-Implementierung ist somit zwangsläufig eine internationale Aufgabe und hakt es an nur einer Stelle mit dem Willen oder an finanziellen Mitteln bei der Umsetzung, so hakt es auch mit der Sicherheit innerhalb der DRMS. Mangelnder Umsetzungswille gilt allerdings nicht für Deutschland und die USA, doch hindern die dortigen Gesetze und der „gute Wille zur Umsetzung" niemanden, Content per Laptop am Strand auf den Philippinen zu knacken und Profit durch von dort aus ins Internet eingespeistes fremdes geistiges Eigentum zu ziehen. Rechtliche Grundlage für die Implementierung von DRMS als Schutz für digitales geistiges Eigentum bildet dabei die traditionelle Allmacht von Contenturhebern über ihre Werke, d.h. es zu verwerten (=positives Nutzungsrecht), andere dagegen von jeglicher Einwirkung ohne Erlaubnis davon auszuschließen (=negatives Verbotsrecht)[24]. Anerkannt ist diese Art von Urheberrechten auf internationaler Ebene durch völkerrechtliche Verträge. Vielfach wird DRM auch mit Kopierschutz verwechselt. Mit DRM wird aber der Content selbst, mit Kopierschutz dagegen der Datenträger geschützt[25]. Kopierschutz wird zudem oft synonym mit Nutzungskontrolle verwendet (einem Teilbereich des DRM). Auch dies ist nach Fränkl falsch, denn das Ziel ist nicht, Kopien zu verhindern, sondern deren Anfertigung zu steuern[26]. Einsatz von Schutzmechanismen ist hier geradezu Pflicht, anderenfalls würde wertvolles geistiges Kapital aufs Spiel gesetzt, da es im Internet leicht ist, geistiges Eigentum unerlaubt zu kopieren oder zu übertragen[27]. Ähnliches gilt für Nutzungs- und Verwertungsrechte, die nicht synonym gesehen werden dürfen[28].

2.3. Beamen à la Enterprise: dematerialisierte Güter

Einleitend wurde behauptet, dass digitaler Content so schnell wie nie zuvor verteilt und vervielfältigt werden kann. Hier folgt der Beweis, da sich ein Vergleich geradezu aufdrängt. Ein einzelner PC Baujahr 1998 hätte gereicht, um die gesamte Mondlandung von 1969 zu steuern – die Rechenkapazitäten verdoppeln sich nämlich alle 18 Monate,

[23] Vgl. Seith, 2003, S. 56.
[24] Vgl. Bechtold, 2002, S. 270.
[25] Vgl. Fränkl, 2004, S. 22.
[26] Vgl. Fränkl, 2004, S. 31.
[27] Vgl. Boehme Martin: Wirtschaftliche Bedeutung internetbasierten Handelns und ausgewählte Beispiele. In: Bröcker, 2003, S. 53.
[28] Vgl. Drewes, 2002, S. 50.

aber auch die Forschungs- und Entwicklungskosten (erstes und zweites Moore´sches Gesetz)[29]. Die große Gefahr für den Content ist nun nicht nur die Möglichkeit ihn zu verarbeiten, sondern auch die Schnelligkeit, mit der er bezogen werden kann. So waren Anfang des 21. Jhdt. schon 20 Mio. deutsche Haushalte an TV-Breitbandkabelnetze angeschlossen. Gepaart mit gesteigerten Datenübertragungsraten, die sich alle 12 Monate verdreifachen, ist hier schon abzusehen, wohin die Entwicklung ohne DRM führen würde[30] – zu Wildwuchs und Anarchie der Contentpiraterie. Die von dieser Entwicklung betroffenen Güter sind eben Musik, Filme, gespeicherte Texte und Computerprogramme. Erstere sind dabei das Ergebnis einer Erfindung, die 1983 mit der Veröffentlichung[31] der Audio-CD einsetzte[32]. Diese bot genug Speicherplatz um Musik in höchster Qualität zu speichern und diese nicht schleichend zu verlieren wie es die bis dahin verwendeten Magnetbänder nach Jahren taten. Grund war der sog. regenerative Effekt, wann auch immer digitaler Content vervielfältigt wird[33]. Störrauschen durch sog. Noise oder fehlerhafte Bits wird durch Korrekturalgorithmen beseitigt[34] – zumindest bis zu einem bestimmten Grad. Heute gilt dies auch für die DVD zur Speicherung von Videodaten – das Grundprinzip beider Datenspeicher ist identisch, handelt es sich doch bei beiden um optische Datenträger. Damit ließen sich nun Musik- und Videodaten gleichsam wie Texte festhalten. Der Unterschied liegt im Speicherformat der verschiedenstfarbigen Book-Standards[35] – die Audio-CD hat z.B. den Ursprung im Red Book, verbessert mit der Fehlerkorrektur von 1983 im Yellow Book[36]. Somit war es kein Wunder, dass mit der Verkündung des digitalen Zeitalters durch Nicholas Negroponte sich sämtlicher Content, der vormals auf Papier, Vinyl oder Zelluloid festgehalten wurde, sich in binärer Form von Nullen und Einsen festhalten ließ[37] – ideal für die Verarbeitung mit Computern, die ausschließlich diese beiden Zustände des Stromflusses (ein oder aus) kennen. Die Digitalisierung ermöglicht so

[29] Nach Clement, 2001, S. 15.
[30] Vgl. Clement, 2001, S. 31.
[31] Erfunden wurde die CD schon 1980, allerdings waren dort noch keine Fehlerkorrekturdaten spezifiziert.
[32] Vgl. Seith, 2003, S. 48.
[33] Vgl. Barry, 2004, S. 5.
[34] Vgl. Barry, 2004, S. 571 ff.
[35] Zu den einzelnen CD-Typen vgl. etwa Tischer, 1998, S. 393 ff.
[36] Vgl. Tischer, 1998, S. 295.
[37] Nach Philippi Theresa: Das Filmwerk und sein urheberrechtlicher Schutz im digitalen Zeitalter. In: Forgó, 2003, S. 322 f.

geradezu die Dematerialisierung von analogen Gütern[38]. Die Entwicklung gipfelt dabei im sog. TIME-Sektor, der aus (T)elekommunikation, (I)nformationstechnik, (M)edien und (E)lektronik besteht[39]. Die Dematerialisierung dient damit der Tauglichmachung und die Infrastruktur des TIME-Sektors dem eigentlichen Transport des Contents, womit Lessigs einleitendes Zitat bestätigt wäre. Es kam, was kommen musste:

2.4. Die Problematik mit Raubkopien

Durch Konvergenz verschiedener Medienbereiche ist die Übertragung von Inhalten nicht mehr ausschließlich den Unternehmen der Medienbranche vorbehalten, sondern auch Teil der Telekommunikationsnetze wie dem Internet. Die Folge: es entstehen zusätzliche Leistungsmerkmale von Inhalten[40]. Damit ist die Aufbereitung des Contents gemeint. Dieser kann extrem günstig über Datennetze global und beim Fehlen eines wirksamen Schutzes auch von anderen als den Urhebern selbst vervielfältigt werden. Möglich machen dies die geringen Kosten ab der Zweitkopie. Die hohen Fixkosten bei der Entwicklung entstehen dabei nur für die erste Kopie (=first copy costs)[41]. Dabei werden Ressourcen, Zeit und Mühe investiert – Kosten die als „sunk-costs“ vorfinanziert werden. Als der Netscape Navigator noch kommerziell vertrieben wurde, betrugen dessen Entwicklungskosten 30 Mio. US$, die zweite Kopie dagegen kostete nur einen US$[42]. De Grenzkosten der Produktion einer zusätzlichen Einheit sind somit praktisch Null (z.B. Microsoft bei Betriebssystemsoftware oder Oracle bei Datenbanksoftware)[43]. Um diesen wesentlichen Vorteil der Digitaltechnik wissen aber auch die Raubkopierer Bescheid. Damit profitieren diese von den Investitionen der Hersteller und verfolgen eigene illegale Vertriebsabsichten. Damit wird der Anreiz für die Schaffung weiteren Contents negativ beeinträchtigt. An Hauptbezugsquellen für illegalen Content bieten sich z.B. die Usenet-Newsgruppen an, die mittlerweile sogar erotische Angebote auf den zweiten Platz verwiesen haben und kaum zu kontrollieren sind[44].

---

[38] Vgl. Clement, 2001, S. 14.
[39] Vgl. Clement, 2001, S. 17.
[40] Vgl. Clement, 2001, S. 16 ff.
[41] Vgl. Clement, 2001, S. 76.
[42] Vgl. Clement, 2001, S. 76.
[43] Vgl. Clement, 2001, S. 60.
[44] Vgl. Päff Jochen: Jäger und Sammler. Software, Codes und Filme im Usenet. In: PC-Magazin, 10 / 2002, S. 46 ff.

2.4.1. Vervielfältigungskosten: fast Null, Qualität des Contents: optimal

Das einzige Problem, das vor wenigen Jahren einer Vervielfältigung von Content durch Raubkopierer noch im Wege stand, waren die hohen Herstellungskosten für exakte Digitalkopien und der Speicherplatz dafür. Beides ist mittlerweile mit billigen CD- u. DVD-Brennern, sowie Computer-Festplatten an der Schwelle zum Terabyte-Bereich (=1024 GB, DVD-Typ 9 zum Vergleich: 18 GB) nicht mehr gegeben. Problematisch ist, dass die eingeführten Standards der CD und DVD nicht mehr revidiert werden können (hier 650 MB, dort 18 GB). Aktuelle Musik-Hits oder Kinofilme belegen eben nicht mehr Speicherplatz, sogar bei HDTV wird etwa nur mit 4-fachem Platzbedarf einer DVD gerechnet, was angesichts o.a. Festplattengrößen lächerlich erscheint. Konsequenterweise konnte dematerialisierter Content nun auf Servern im Internet zum Download bereitgehalten werden. Bald darauf setzte auch reger Tauschhandel ein. Problematisch dabei ist, dass infolge der Massenhaftigkeit dieses Phänomens die Anzahl der Rechtsverletzungen nicht überschaubar ist[45]. Qualitätsverluste wie bei analogen Bandüberspielungen gab es hier nicht mehr, und Leerdatenträger (CD- / DVD-Rohlinge) waren mit Kosten um den Bruchteil eines ordnungsgemäß lizenzierten Originaldatenträgers erhältlich. Die geringeren Transaktionskosten der Digital Economy und mehr Komfort dank Individualisierungsmöglichkeiten des Contents zielen dabei geradezu auf den Nutzer. Diese Market-Pull Faktoren versetzen den Rezipient in die Lage, den Informationsfluss exakt auf seine Bedürfnisse abzustimmen[46]. Ohne DRM bezogen auf den Content, würde dies allerdings unkontrolliert geschehen, weshalb DRM somit den Regulator darstellt. Zusätzliche Gefahr geht dabei von hervorragenden Kompressionsalgorithmen aus, wie dem MP3-Format des Fraunhofer-Institutes[47]. Deutlich wird dies, da Ende des 20. Jhdt. 90% des Musikangebotes im Internet aus Raubkopien bestanden[48]. Die amerikanische RIAA spricht von 200.000 Raubkopien am Tag[49]. Die Schäden durch unkontrollierte CD-Brenner-Tätigkeiten belaufen sich dabei auf eine Milliarde bis 3,5 Milliarden € pro Jahr für die Musikindustrie, davon alleine 740 Mio. in Deutschland[50]. Der Grund dafür: sie bieten eben gleichwertige digitale

[45] Vgl. Fränkl, 2004, S. 69.
[46] Vgl. Clement, 2001, S. 20.
[47] Vgl. Schwarz Kai: Musik legal aus dem Netz. In: Computer-Guide, 02 / 2004, S. 38.
[48] Vgl. Hofer, 2000, S. 142.
[49] Vgl. Czychowski Christian: Zusammenhänge und Überblick. In: Bröcker, 2003, S. 17.
[50] Vgl. Gutman, 2003, S. 121.

Qualität wie das Original[51]. Der Hauptgrund für unkontrollierte Vervielfältigung ist, dass man in der vermeintlichen Anonymität und Globalität des Internets mit unterschiedlichen Rechtssystemen untergeht. Folglich ist auch die Angst vor Strafverfolgung gering. Auch Unternehmen scheuen sich vor der Rechtsverfolgung wegen den hohen Rechtsdurchsetzungskosten bei vergleichsweise geringem Streitwert. Somit liegt das Problem nicht am faktisch präsenten rechtlichen Schutz, sondern an dessen Durchsetzungskraft – gesellschaftlich gilt die Raubkopie ja auch noch als Kavaliersdelikt[52]. Daher verwundert es auch nicht, dass sagenhafte 95% der Raubkopierer keine Angst haben, erwischt zu werden[53]. Somit muss gefragt werden:

2.4.2. Warum schaden Raubkopien – „gekauft hätte ich ja eh nicht“?

Unterschieden werden „große“ Raubkopierer in die Gruppen Totalfälscher, die ein Produkt inkl. Verpackung, Echtheitszertifikaten und Datenträgern in Presswerken fälschen, die Übernutzer, die entgegen Lizenzverträgen Software auf mehr als der angegeben Anzahl an Endgeräten einsetzen, Gold-Disk-Piraten, die mehrere Programme auf einer sog. Compilation-CD unter der Hand vertreiben und letztlich die Hard Disk Loader, die Software auf Festplatten zusammen mit PCs ausliefern, jedoch ohne Lizenz. Zu den kleinen Fischen zählen dabei Schulhofpiraten, die jedoch in Summe ebenfalls hohen Schaden anrichten - v.a. für Spielehersteller[54].

[51] Vgl. Gutman, 2003, S. 123.
[52] Vgl. Fränkl, 2004, S. 71.
[53] Vgl. Fischer Jens: Kopieren: Haben Sie Angst, gepackt zu werden? In: PC Praxis, 10 / 2003, S. 12.
[54] Vgl. Stephan Christian: Multiplikatoren. Raubkopierer und Sicherheitsfanatiker. In PC-Magazin, 09 / 2001, S. 68 f.

Abbildung 3: Die „Zusammensetzung“ des Schadens durch Raubkopien[55]

Kopiert wird dabei folgender Content:

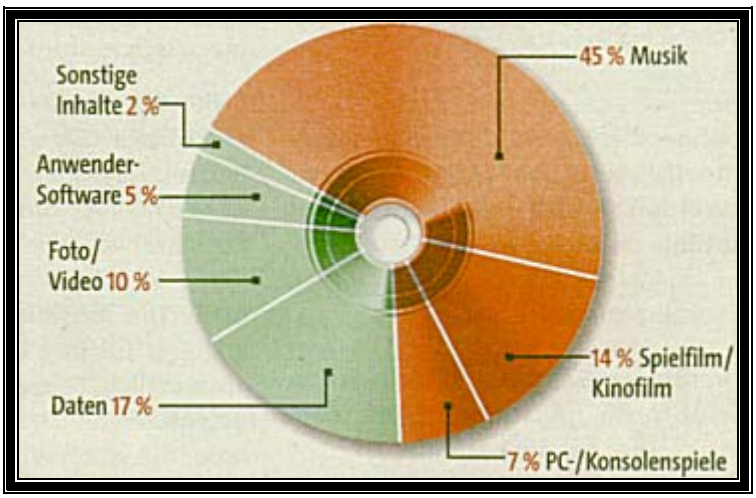

Abbildung 4: Aufschlüsselung der Raubkopien nach Contenttyp[56]

[55] Aus: PC Praxis, 06 / 2002, S. 56.
[56] Aus: Chip, 09 / 2004, S. 115.

Prinzipiell wäre nichts daran auszusetzen, wenn sich Wissen in Form digitaler Güter über Netze vermehrt. Öffentliche Güter sind aber eben nicht mehr geeignet, Gewinn zu schöpfen. Diese Nicht-Exklusivität[57] von Gütern verhindert also Profit. Da DRMS nun zusätzlich zum Urheberrecht Exklusivität sichern - Urheberrecht wurde ja geschaffen, um dem Marktversagen entgegenzuwirken - erhöht sich nun wieder der Anreiz, vermehrt Content zu schaffen[58]. Man weiß hier, dass er vor Vervielfältigung geschützt ist. Das einleitende Zitat Shakiras stimmt somit, denn Nutznießer des Erlöses von CD-Alben sind, wie folgende Grafik zeigt, mehrere Beteiligte, wobei für den Künstler nur 7% bleiben. Sollte der Content nun noch ohne Vergütung illegal kopiert werden, liegt auf der Hand, dass das Interesse schwindet weiteren Content zu produzieren. Auch das Online-Geschäftsmodell mit 1,49 € der Branchenplattform „PhonoLine“ lässt hier nur 9% für den / die Künstler/in übrig.

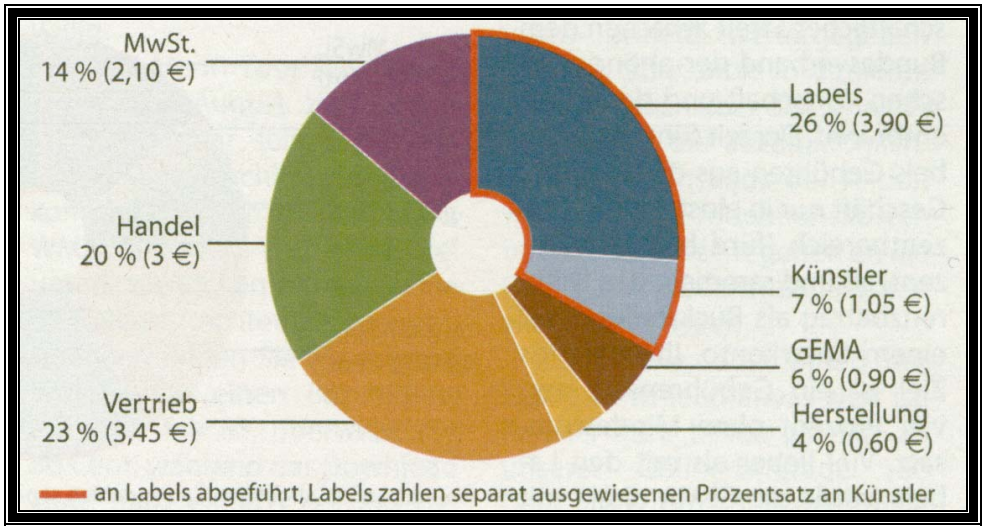

Abbildung 5: So viel (bzw. wenig) bleibt dem/r Künstler/in bei einem 15 €-Album[59]

[57] Vgl. Bechtold, 2002, S. 284 f.
[58] Vgl. Bechtold, 2002, S. 289 f.
[59] Aus: c´t #12, vom 01.06.2004, S. 97.

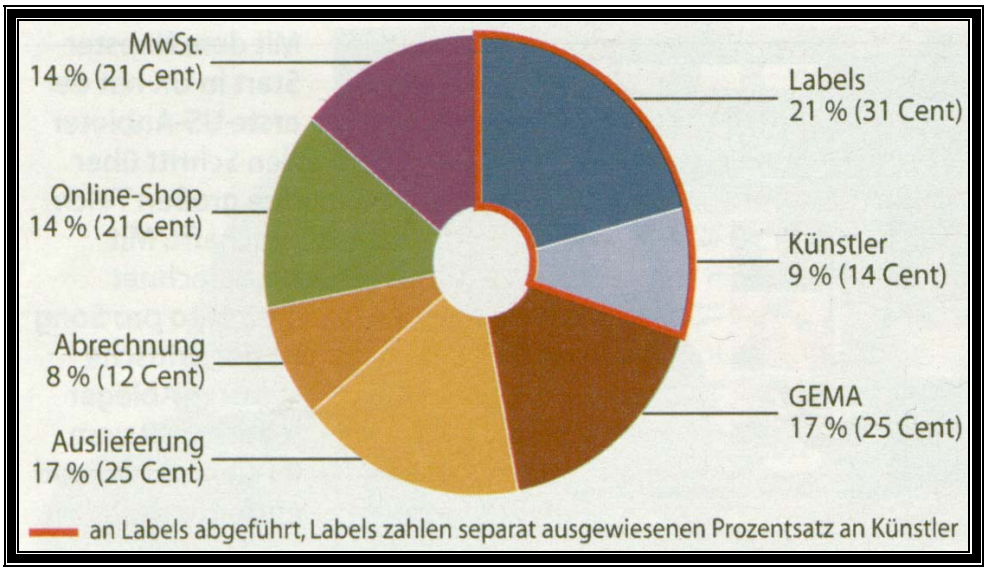

Abbildung 6: So viel (bzw. wenig) bleibt dem/r Künstler/in bei einem Online-Preis von 1,49 € / Titel[60]

Die Auswirkung: Raubkopien schaden damit nicht nur den Labels und dem Künstler, sondern der gesamten Wertschöpfungskette: dies reicht vom Granulathersteller für die Plastikschutzhüllen von CDs / DVDs bis zum LKW-Spediteur, der sie liefert und den Arbeitsplätzen für Verkäufer/innen im Einzelhandel, sowie dem Staat selbst, der keine Umsatzsteuern mehr dafür bekommt, sollte Content nicht mehr „gekauft“ werden. Die Fixkosten werden dann umgelegt auf geringere Stückzahlen der Originale, d.h. deren Preis steigt, womit der Teufelskreis eröffnet ist - denn dann sinkt auch wieder die Nachfrage[61]. Das oft gehörte Argument von Raubkopierern, dass man den Content ohnehin nicht legal erworben hätte und folglich auch kein Schaden entstehen kann, ist daher völlig unzutreffend.

Aber selbst das beste DRMS vermag Exklusivität nicht zu schützen, da AV-Content für den Menschen nur in analoger Form wahrnehmbar ist. Dabei können zufällig anwesende Mitmenschen in der Nähe der Video- oder Schallquellen nicht davon abgehalten werden, den Content mitzukonsumieren. Lessig räumt dies ein, indem er von geteilten Ideen spricht. Ist nämlich das geistige Gut einmal unter das Volk gebracht, so hindert und mindert dies nicht dessen Gebrauch im Sinne von Nutzen. Mit entsprechender Architektur von Schutzmaßnahmen und der „richtigen Technologie“

[60] Aus: c´t #12, vom 01.06.2004, S. 98.
[61] Vgl. Gutman, 2003, S. 124.

kann man andere jedoch fernhalten[62]. DRM leistet nun genau dies, indem Vervielfältigung von geistigem Gut kontrolliert wird und genau darin liegt auch der Wert des Contents. Denn: solange der Hersteller die Kontrolle behält (v.a. der Kopien), solange kann er auch den Wert und damit den Preis bestimmen[63] - zumindest im Rahmen der Schranken wie z.B. zu akademischen Zwecken, der Kritik, Kommentierung und Nachrichten, oder der kulturellen Entwicklung der Gesellschaft (=Fair Use)[64]. Damit die Kontrolle auch behalten wird, gibt es:

2.5. Schutzmaßnahmen von DRM und DRMS

2.5.1. Kryptografie von Content

Zentrale Rolle bei der gesamten DRM-Konzeption spielt Kryptografie. Was die verwendeten Verfahren anbelangt, kommen hier sowohl symmetrische, asymmetrische und hybride zum Einsatz. Wichtig für das Verständnis ohne hier zu sehr ins Detail zu gehen ist, dass dabei Schlüssel unterschiedlicher Bit-Länge zum Einsatz kommen und diese je nach Verfahren zum Ver- als auch Entschlüsseln mittels eines sog. Public Key verwendet werden können[65] – so auch Fränkl[66]. Erzeugt werden dabei sog. Hash-Werte, die Verschlüsselung beliebig großer Datenmengen ermöglichen – damit soll gewährleistet werden, dass nur dazu befugten Personen auf den verschlüsselten Content Zugriff haben[67]. Der Private Key befindet sich dabei ausschließlich im Besitz der Rechteinhaber am verschlüsselten Content, bzw. fest eingebettet in Hardware wie dem TPM-Chip. Verschlüsselung sollte bei schützenswerten Inhalten auch eingesetzt werden[68]. Eine Modifikation des Contents auf dem Weg durchs Netz zwischen Sender und Empfänger ist dann unmöglich[69], da der Content anhand seiner Signatur mittels Public-Key beim Empfänger einer Prüfung auf Konsistenz nicht standhalten würde. Je nach verwendetem Algorithmus (S-Mime oder openPGP) kommen dabei Zertifizierungsstellen ins Spiel, die die Authentizität des Senders gewährleisten, bzw.

[62] Vgl. Lessig, 2001, S. 235 f.
[63] Vgl. Bauckhage Tobias: The Basic Economic Theory of Copying. In: Becker, 2003, S. 236.
[64] Vgl. Bauckhage Tobias: The Basic Economic Theory of Copying. In: Becker, 2003, S. 238.
[65] Vgl. Spenger Gabriele: Authetication, Identification Techniques, and Secure Containers – Baseline Technologies. In: Becker, 2003, S. 62 ff.
[66] Vgl. Fränkl, 2004, S. 39 ff.
[67] Vgl. Clement, 2001, S. 159.
[68] Vgl. Lessig, 2001, S. 80.

Zertifikate in Form von öffentlichen Schlüsseln widerrufen können[70]. Vergleichbar ist diese Vorgehensweise wie die Beiziehung eines Notars im täglichen Leben[71]. Grundlage sind Signaturgesetze[72] sowohl in den USA, als auch Deutschland[73]. In Deutschland war man dabei schon 1997 sogar noch vor der EU-Richtlinie diesbezüglich dabei[74].

Digitaler Content leidet ja generell an der Einfachheit der Manipulation ohne Spuren. Dies betrifft v.a. Textdokumente (Word-Dateien, PDF, HTML). Beweiskräftige Erklärungen im Online-Recht sind daher ausschließlich qualifizierten, d.h. von Zertifizierungsstellen ausgestellten digitalen Signaturen vorbehalten, die bei Empfang anhand des Zertifikates und dieses selbst auf Beschränkungen zu prüfen ist[75]. Gemäß den einleitenden Definitionen sind diese Erklärungen auch Gegenstand des Online-Bezugs von Content, d.h. also, man kann hier ruhigen Gewissens die Signaturen als Teil eines DRMS bezeichnen – und diesen haftet eben der Mangel an, durch deren Umgehungsmöglichkeiten mit einem Restrisiko behaftet zu sein. Anzumerken wäre, dass Verschlüsselung den Content nur während des Transfers, bzw. Downloads oder später in der gefestigten und damit abgespeicherten Form am jeweiligen Datenträger hält. Zur Laufzeit jedoch findet Dekodierung statt. Und genau hier kann man den Content in analoger Form abgreifen – etwas was auch nach den Novellierungen des Urheberrechts und nach dem DMCA noch erlaubt ist, wie im Kapitel zur analogen Lücke gezeigt wird. DRM hindert dabei durch Verschlüsselung somit lediglich die Anfertigung einer digitalen Kopie[76], bzw. zwingt den Nutzer zur analogen Kopie, die dann so lange dauert, wie eben die Spieldauer des Musik-Werks oder des Films beträgt.

---

[69] Unmöglich allerdings nur offiziell, denn wie in den Angriffskapiteln gezeigt wird, gibt es nämlich mehrere Umgehungs- und Knackmöglichkeiten, eine davon mit 100% Erfolgsgarantie gegen jeglichen Widerstand.

[70] Vgl. Bauer Bettina: Konzept für die Implementierung elektronischer Signaturen in einem Unternehmen. In: Forgó, 2003, S. 36.

[71] Vgl. Clement, 2001, S. 156.

[72] Vgl. Rosenblatt, 2002, S. 51.

[73] Vgl. Bröcker Klaus Tim: Schutz des Nutzers im Netz: Datenschutz und Datensicherheit. In: Bröcker, 2003, S. 254

[74] Vgl. Forgó Nikolaus: Code und Kontrolle. In: Gasser, 2002, S. 45.

[75] Vgl. Lapp Thomas: Zivilprozessualer Beweiswert und Beweiskraft digitaler Dokumente. In: Schneider, 2005, S. II / 64.

[76] Wie DeCSS zeigt, leider erfolglos bei DVDs.

2.5.2. Wasserzeichen

Wasserzeichen im Sinne von DRM sind direkt in den Content eingebettet und deren Vorhandensein ist im kommerziellen Verkehr im Gegensatz zur Steganografie Privater meist bekannt. Somit handelt es sich um nicht steganografische Wasserzeichen. Der Sinn dabei ist, festzustellen, wer Content illegal verbreitet. Wasserzeichen verhindern hier den Zugriff auf Content nicht und stellen auch keinerlei eigentliche Schutzmaßnahme dar. Ihr einziger Zweck besteht lediglich in der Markierung[77]. Der Schutz kann aber im Anschluss an eine Rechtsverletzung durch Anwendung von DRMS erfolgen oder durch rechtliche Schritte gegen den Rechtsbrecher. Welche Teile zum Wasserzeichen und welche zum Content gehören, wird erst zur Laufzeit bestimmt. Genau daher ist diese Vorgehensweise auch nicht Einzelschrittsimulationsfest (sog. Debuggen). D.h., man zerlegt hier ein Softwareprogramm, bzw. Content während der Laufzeit in die einzelnen Ablaufschritte, bis man die Stellen gefunden hat, die für das DRM verantwortlich sind. Dann kann man diese eliminieren, indem einfach der reine Content von dem diesen anhaftenden Wasserzeichen separiert wird. Es gibt somit etliche Verfahren, das Debuggen zu erschweren, was an dieser Stelle aber zu technisch zu veranschaulichen wäre[78]. Sichere Wasserzeichen müssen daher den Kriterien Robustheit (D/A-Wandlung, Konvertierung, nicht verlustbehaftete Kompression), und Sicherheit (=Resistenz gegen scannen, verzerren, verlustbehaftete Kompression) entsprechen[79]. Angriffsmethoden existieren aber auch hier, da heutige Wasserzeichenverfahren noch nicht sicher gegenüber gezielten Attacken sind – die Sicherheit hier zu erhöhen ist dabei Aufgabe der Steganoanalyse[80]. Safavi-Naini und Wang weisen zu Recht auf Schwierigkeiten mit modifizierten oder beschädigten Wasserzeichen durch Kürzungen mittels Cut und Paste-Angriffen hin, die komplizierte mathematische Verfahren zur Verfolgung von Contentpiraten erfordern[81].

---

[77] Vgl. von Diemar, 2002, S. 146.
[78] Zu den Details: Bertelsons, 1995, S. 395 ff.
[79] Vgl. Fränkl, 2004, S. 35 ff.
[80] Vgl. Bechtold, 2002, S. 62.
[81] Vgl. Safavi-Naini Reinhaneh / Wang Yejing: Traitor Tracing for Shortened and Corrupted Fingerprints. In: Feigenbaum, 2003, S. 82.

2.5.3. Trusted Systems und der Fritz / TPM–Chip: Die „DRM-Allianz“

Wie bisher erläutert wurde, kann Dematerialisierung von Content dazu führen, dass dieser ohne Vergütung an dessen Urheber vervielfältigt wird. Dank Möglichkeiten von Installationsschlüsseln bei Software und Produktaktivierungstechnologien oder beim Einsatz von Lizenz-Dateien und Wasserzeichen wird hier Schutz für Content realisiert. Einer Verfolgung von Wasserzeichen und dem Abgleich mit einer schwarzen Liste raubkopierter Freischaltschlüsseln steht damit nichts entgegen. Denn dabei wäre eine Nutzung des Contents nach einem Diebstahl von Datenträgern oder der Vervielfältigung aus einer Tauschbörse nicht mehr möglich. All diese Verfahren basieren auf Schlüsseln. Allerdings sind es gerade diese Schlüsseln, die begehrtes Ziel von Angriffen, aber auch mit dem unangenehmen Gefühl der Überwachung verbunden sind. Bisher gibt es ja auch keine zentrale Datenbank, welche Endverkäufer hier über welche Freischaltschlüsseln verfügen, und an welche Nutzer diese verkauft werden, um sie bei Bedarf zu sperren. Die nächste Entwicklung ist hier der erwähnte TPM, bzw. Fritz-Chip, der seinen Namen in Anlehnung an US-Senator Fritz Hollings erhielt[82]. In einem derart ausgerüsteten System soll die gesamte Kommunikation verschlüsselt ablaufen, denn es bringt nichts, wenn einzelne Komponenten eines Systems DRM-geschützt sind, die dann dekodierten Nutzdaten jedoch ohne DRM-Schutz ungesichert übertragen werden (zum Fernseher oder zum Lautsprecher für Video- und Musikausgabe, bzw. auch Texte über das Internet). DRM-kompatible Geräte müssen daher zwingend verschlüsselt kommunizieren[83].

Die einzelnen Komponenten eines TPM-Chip-Systems vertrauen sich dabei gegenseitig. Digitale Signaturen leisten ähnliches für Systeme, die über Netze kommunizieren. Denn nur Systeme, die anderen Systemen vertrauen, würden Informationen und damit Content austauchen können. Diese Trusted Systems sind es somit, die künftig eine zentrale Rolle beim Vervielfältigen von Content und auch beim legalen Erwerb spielen werden, denn nur wenn eine Lizenz dafür als gültig eingestuft wird, lässt sich der Content auch nutzen. Damit lassen sich auch Viren und sonstiger Schadcode[84] nicht mehr verwenden, da es diesen Programmen an der zwingenden

[82] Vgl. Himmelstein Gerald: Der digitale Knebel. In: c´t #15, vom 15.07.2002, S. 18.
[83] Vgl. Bechtold, 2002, S.118.
[84] Logischerweise ist dann auch Open Source wie eben Linux „Schadcode”.

Zertifizierung fehlt[85]. Lessig vergleicht Trusted Systems mit einer Art Kurierdienst, denen man im Gegensatz zur unzuverlässigen Post eher geneigt ist, Wertsachen anzuvertrauen[86]. Der Wert stellt sich dabei jedoch ausschließlich für die Urheber dar, denn das Vertrauen der Nutzer in die Trusted Computing Group schwindet – und das mit Recht, denn Schwachstellen in den TPM-Chips gibt es natürlich jede Menge (z.B. Schlüsselschwächen bei der Umsetzung der Spezifikationen von Key- und Session-Handles und sogar Anfälligkeit für Wörterbuchangriffe, wie die Uni Bochum nachgewiesen hat - mittlerweile haben wir das Jahr 2006 wohlgemerkt, wobei die ersten Spezifikationen um 2002 herum verabschiedet wurden)[87]. Der TCG gehören aber führende Hersteller von Hard- und Software an (u.a. IBM, Intel, AMD, Microsoft, Infineon, HP und Sun Microsystems) – dass sich diese maßgeblich dafür stark machen, einen DRM-Durchsetzungsstandard zu entwickeln, der nicht nur in Computersystemen, sondern auch in Homeelektronik Anwendung findet, mutet hier nach einer globalen Allianz an, das private Leben kontrollieren zu wollen. Nach Willen dieser Allianz soll nämlich in die nächste PC-Architektur ein unverkennbarer individueller Schlüssel implementiert werden, der hier genaue Identifizierung ermöglicht. Damit sollte es der Vergangenheit angehören, von dritter Seite (Zertifizierungsstellen) eine Art Beglaubigung einzuholen, dass hinter einer digitalen Signatur (so wie dies derzeit gehandhabt wird) auch derjenige steckt, der dies vorgibt zu sein – und Signaturen spielen bei Bestellung, Bezahlung, und Identifikation eine zentrale Rolle. Mit auswechselbaren Schlüsseln allerdings wäre dieses Vertrauenssystem wiederum zerstört. In den ersten Entwürfen dazu sollte der Schlüssel konsequenterweise auch nicht auswechselbar sein (sog. Endorsement-Key), neuerdings jedoch schon, wenngleich nicht zwingend[88] - zu problematisch erscheint wohl die Gefahr hier Identitätsklau zu begehen. Gibt es aber keine eindeutigen Schlüssel, ist die Verfolgung von Rechtsverstößen und die genaue Identifizierung von Content einmal mehr nicht gesichert. An dieser Stelle bleibt ungeklärt, was mit der Vielzahl an älteren Systemen geschieht, die die Sprache des DRM noch nicht kennen, da ihnen ein TPM-Chip fehlt.

[85] Vgl. Reinke Stefan: Big Brother Microsoft. In: Chip, 04 / 2004, S. 58 f.
[86] Vgl. Lessig, 2001, S. 230 f.
[87] Vgl. Himmelein Gerald:Sicherheits-Chips auf den Zahn gefühlt. In: c´t #10, vom 02.05.2006, S. 28.
[88] Vgl. Krempl Stefan: Schlüsselfreieheiten. Trusted Computing mit zögerlichen Zugeständnissen. In: c´t #23, vom 03.11.2003, S. 104.

Wie Trusted Computing nach den Vorstellungen des Allianz-Mitglieds Microsoft heute funktionieren sollte[89], zeigt dabei folgendes Schema[90]:

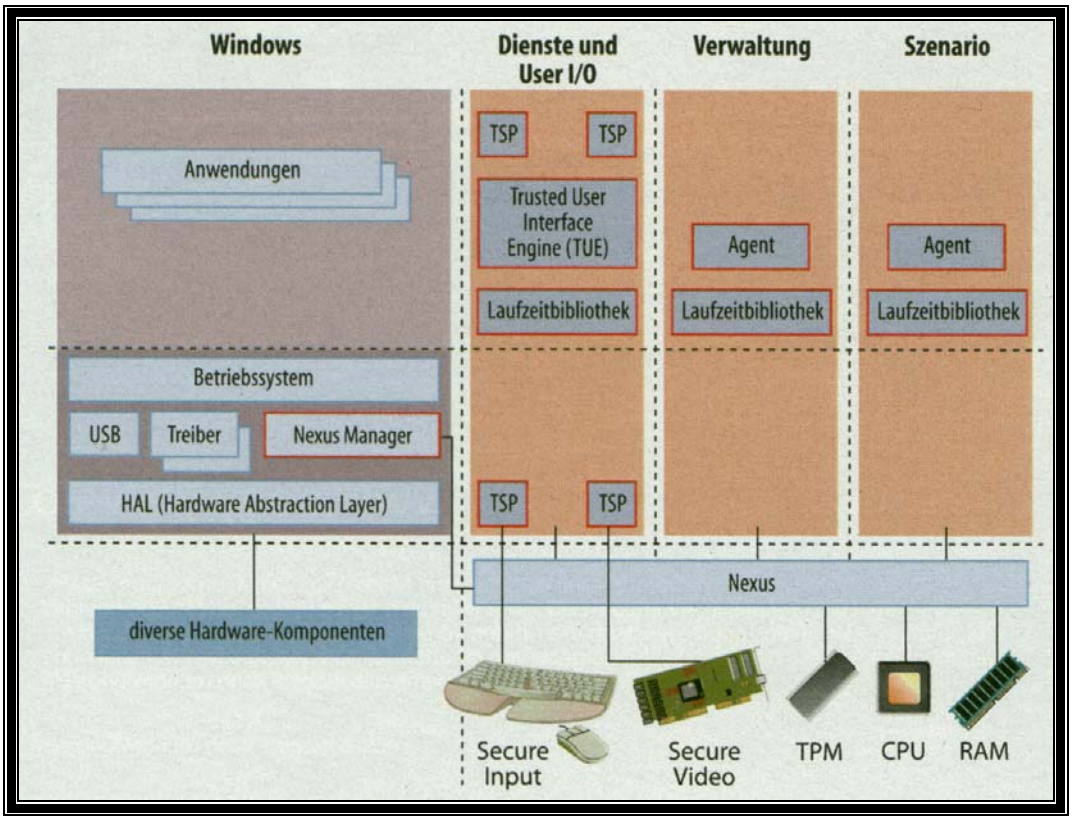

Abbildung 7: So funktioniert Trusted Computing nach DRM-Allianz-Mitglied Microsoft[91]

Deutlich wird, dass ohne die erwähnte verschlüsselte Kommunikation aller Geräte über die Nexus-Schicht nichts funktioniert. Konsequenterweise erblickt Lessig in den Trusted Systems auch eine Alternative zu Urheberrechten. Somit wird der rechtliche Schutz über deren Code sehr viel wirkungsvoller implementiert, d.h. aber auch, dass hier bereits erste Auswirkungen der Transformation von Staatlichkeit vorherrschen. Vieles hängt dabei vom Code des Systems ab. Doch selbst die doppelt verriegelte Wohnungstür, die Lessig als Beispiel anführt, stellt keine Garantie dafür dar, dass nicht trotzdem eingebrochen wird. Der Schutz wird somit lediglich verstärkt – mehr aber

[89] Es gab auch einen älteren Entwurf, der jedoch „eben weil er alt ist“ nicht mehr gebraucht und daher hier auch nicht behandelt wird.
[90] Folgende Grafik zeigt dabei die neuere Architektur und nicht den „alten” Nexus-Kern, wie er sich z.B. noch bei Becker, 2003, S. 199. findet.
[91] Aus: c´t #12, vom 01.06.2004, S. 46.

auch nicht[92]. Dies geht sogar so weit, dass Trusted Systems zwar den gleichen Bereich regeln wie Urheberrechte, allerdings hinsichtlich des öffentlichen Gebrauchs diesem nicht denselben Stellenwert einräumen – der Produzent behält das Höchstmaß an Kontrolle[93]. Denn der TPM-Chip signalisiert erst dann grünes Licht zur Wiedergabe und der Nutzung vertrauenswürdigen Codes, wenn die Lizenzen gültig sind[94] – freilich handelt es sich bei diesem vertrauenswürdigen Code um denjenigen der Rechteinhaber und nicht etwa dem, was der Contentnutzer gerne an Rechten haben möchte. Der Staat kann hier reagieren, indem z.B. Schutzmaßnahmen in urheberrechtlichen Auswirkungen begrenzt werden, sog. Schranken, oder aber er kann versuchen, die unmittelbare Ausgestaltung technischer Schutzmaßnahmen zu beeinflussen[95], wie eben den TPM-Chip - dies wurde derzeit unterlassen. Folgende Abbildung zeigt die Funktion:

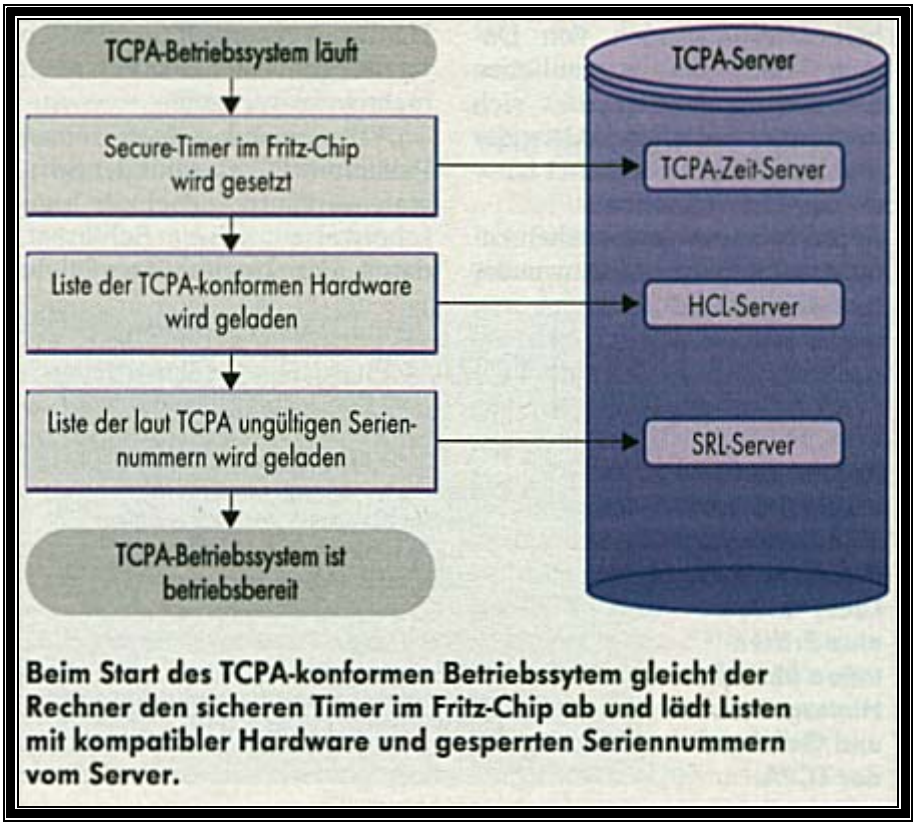

Abbildung 8: Kontrollverlust durch Kontakt zu Schlüssel-Servern beim „Trusted Computing“[96]

[92] Vgl. Lessig, 2001, S. 232.
[93] Vgl. Lessig, 2001, S. 241.
[94] Vgl. Fränkl, 2004, S. 51 f.
[95] Vgl. Bechtold, 2002, S. 407.
[96] Aus: c´t #22, vom 21.10.2002, S. 206.

Hier tritt Kontrollverlust über die eigene Hardware ein. Dies ist auch ein wesentliches Hemmnis in der Digital Economy, da kaum persönliche Interaktion mit Anbietern auftritt. So muss dieses Vertrauen in deren Systeme erst einmal aufgebaut werden[97], v.a. wenn man Content online vertreiben, bzw. zwingend aktivieren muss und besonders dann, wenn sensible Kreditkarteninformationen oder persönliche Dateneingabe unumgänglich ist.

Dank der Medienkonvergenz ist nun der nächste logische Schritt die Ausstattung des Wohnzimmers mit Media-Center-PCs. Damit findet die Implementierung von DRMS in den privaten Lebensbereichen der Menschen ihren Höhepunkt – offensichtlich ist es aber genau das, was die DRM-Allianz im Sinne hat: das private Leben zu kommerziellen Zwecken zu kontrollieren. Konvergenz beteiligter Systeme stellt dabei die Chance für weitere technische Entwicklungen dar – jeglicher Content kann über Netze auf jeglicher Art von Endgerät auf allen Plattformen genutzt werden und zwar ohne Qualitätsverlust[98]. Darin besteht neben der Chance hier neue Märkte zu erschließen auch gleichzeitig das größte Risiko der Digital Economy wegen undurchsichtiger Produkt- und Technologiezyklen, sowie von schwankendem Kundenverhalten[99]. Immerhin weiß heute noch niemand, wie DRM vom Markt aufgenommen wird, da DRMS noch zu kurz dort präsent sind, um hier schlüssige Aussagen treffen zu können. Da die Allianz allerdings fast über eine monopolartige Stellung verfügt, ist dieses Unterfangen des Oktroyierens der Implementierung von DRMS nicht allzu schwer zu realisieren. Was dabei jedoch nicht beachtet wird, ist, dass es auch offene Standards gibt, die zwar die Verwendbarkeit von Content erhöhen, die Vergütungsbereitschaft dafür allerdings verringern, da sich die digitale „dort laufende“ Kopie vom Original eben nicht unterscheidet – hierin liegt die vermutlich einzige Möglichkeit des Verlustes potentieller Kunden[100], sowohl was Vertrauen als auch für Trusted Computing lizenzierten Content anbelangt. Man wendet sich ja genau diesen Alternativen bei Open Source zu, wo man nicht überwacht wird.

---

[97] Vgl. Clement, 2001, S. 73.
[98] Vgl. Seith, 2003, S. 50.
[99] Vgl. Clement, 2001, S. 201 f.
[100] Vgl. Bauckhage Tobias: The Basic Economic Theory of Copying. In: Becker, 2003, S. 243.

2.5.4. Komponenten des DRM und DRMS

Wie in den vorigen Kapiteln gezeigt wurde, spielen Schlüssel und Wasserzeichen bei der Identifizierung von Content eine zentrale Rolle. Die Ahndung von Rechtsverletzungen durch DRM gestaltet sich ohne Verwendung der TPM-Architektur derzeit noch schwierig. Was bei Software durch Aktivierung möglich ist (d.h. natürlich auch Deaktivierung im Falle eines Rechtsverstoßes), wäre für Musik und Film derzeit zu teuer. Immerhin müssten Wasserzeichen in jedem Datenträger individuell unterschiedlich eingebettet sein, was für jede Contentkopie einen individuellen Datenträger erfordern würde und damit eine individuelle Pressung im Presswerk. Bezogen auf Abrechnung ist aber gefordert, dass prinzipiell sämtliche Erlösformen unterstützt werden sollen – somit auch klassische Barzahlung beim klassischen Einkauf. DRM beeinflusst nun zwar die Kopierfähigkeit, bietet aber genau die Möglichkeit der Abrechnungsimplementierung in den Content, bzw. in die Umgebungsplattform (Abspielgeräte, Abspielsoftware)[101]. Fränkl weist dabei auf etliche Forderungen bezüglich des eigentlichen Managements von Rechtsverletzungen hin: was diese anbelangt, sollen diese möglichst verhindert werden. So darf *erstens* der Content nicht von Dritten manipuliert sein, *zweitens* muss sich die Rechtsverletzung ausdrücklich einem Rechtsverletzer zuordnen lassen und *drittens* muss die Strafverfolgung unterstützt werden. Die Kernkomponenten (Funktion und Technologie) von DRM sind daher:

Funktionen	**Technologien**
Zugangskontrolle	Wasserzeichen (incl. Digitalen Fingerabdrücken)
Nutzungskontrolle	Verschlüsselung (incl. Digitale Signatur)
Abrechnung	Rechtedefinitionssprachen
Management Rechteverletzungen: → Integrität → Authentizität → Strafverfolgung	Weitere Technologien
Weitere funktionale Anforderungen	

Tabelle 1: Komponenten eines DRMS - Funktionen und Technologien[102]

[101] Vgl. Gutman, 2003, S. 134.
[102] Quelle: Fränkl, 2004, S. 29.

Unter Zugangskontrolle ist gemeint, Unbefugten den Zugang sicher zu verwehren, wobei die Nutzungskontrolle terminlich und zeitlich, sowie quantitativ und regional beschränkt sein kann. Als Feinheit können noch Endgerätebeschränkungen und Einschränkungen hinsichtlich der Nutzungsqualität getroffen werden (z.B. die Auflösung bei Videos oder Klangqualität bei Musik)[103]. DRM bietet ja die Möglichkeit, Content in schlechter Qualität als Demonstration zu nutzen. Sollte dann das Interesse des Rezipienten geweckt sein, ließe sich höhere Contentqualität freischalten[104]. Mit den weiteren funktionalen Anwendungen dagegen muss z.B. sichergestellt sein, dass das DRM intakt bleibt, so wie es Fetscherin ausdrückte: „as content travels through the value chain from the content creators to consumers, and even from consumer to consumer[105]“. Ferner muss das System viele Standards unterstützen (=Plattformneutralität), sowie unabhängig vom Medientyp und Contentformat sein und zudem einfach bedienbar bleiben. Standards schützen dabei Investitionen durch die vielseitige Verwendbarkeit der Güter[106]. Dieser Satz gilt für digitalen Content umso mehr, da sich dieser auf Fernsehgeräten, DVD-Playern / Recordern, PCs und sogar Handys nutzen lässt, sowohl was Musik- / Videomaterial betrifft, wie auch die Steuerungssoftware der Geräte. Clement hält einer Standardisierung allerdings entgegen, dass dieser Vorgehensweise eine fundamentale Schwäche anhaftet. Werden Standards nämlich zu früh implementiert, ist Unausgereiftheit die Folge, was weitere Entwicklung in diesem Gebiet bremst (so geschehen z.B. bei der DVD mit leicht zu umgehendem CSS), zu späte Implementierung dagegen hätte dazu führen können, dass sich andere Standards anderer Hersteller möglicherweise früher durchgesetzt hätten[107]. Somit führt Konkurrenzdruck unter den DRMS-Herstellern selbst zu unausgereiftem DRM. Zu unterscheiden gilt es hier zwischen BOBE-resistenten (break once, break everywhere) und nicht BOBE-resistenten DRMS. Leider gehören die meisten zu letzterer Kategorie[108]. So ist Umgehung des RC-Codes in einem DVD-Player per Fernbedienung nur an diesem einen Gerät gültig, während die Prozedur zur Umgehung

[103] Vgl. Fränkl, 2004, S. 30 f.
[104] Vgl. Bechtold, 2002, S. 265.
[105] Zitat nach: Fränkl, 2004, S. 33.
[106] Nach Clement, 2001, S. 62.
[107] Vgl. Clement, 2001, S. 63.
[108] Vgl. Biddle Peter (u.a.): The Darknet and the Future of Content Protection. In: Becker, 2003, S. 359.

des CSS-Schutzes am Datenträger DVD überall Wirkung entfaltet[109]. Auch die Corporate-Files von Windows XP und der Generalschlüssel zu Office XP fallen unter letztere Kategorie. Leidtragende sind die Contenturheber, die wegen der schwachen Schutzmechanismen weniger Vergütung erhalten. Aber zur Vorbeugung eines Kunden- und Vertrauensverlusts darf die Sicherheitsstufe des DRM nicht zu hoch sein (Overprotection), sondern muss am Wert des Contents gemessen werden. So ist Bechtold der Auffassung, dass Hyperprotection sogar eine Art zusammengeschustertes Urheberrecht ermöglicht[110]. Letztlich muss DRM zwecks Funktion Data-Mining betreiben und die Contentnutzung muss sich zwangsweise aufzeichnen und analysieren lassen[111]. Dies leuchtet auch ein, denn widrigenfalls könnte die Nutzung am Content niemals reguliert werden, da dieser nicht identifizierbar ist. All diese Forderungen Fränkls spiegeln somit den Wunsch nach der sprichwörtlichen Eier legenden Wollmilchsau wider – und die gibt es bekanntlich nicht. Damit ist auch Montenegros idealistisches Sollzustandsbild von keinerlei wechselseitiger Abhängigkeit widerlegt – warum sonst sollte es eine DRM-Allianz geben, wo schon alleine das Wort Abhängigkeit signalisiert. Im Gegenteil: von der Technologieseite her gibt es noch etliche Schwachpunkte: v.a. die Wasserzeichen und Schlüsseln, die als Identifizierungsmerkmal für DRM eingesetzt werden (ebenso wie Metadaten), da es sich hierbei um gekapselten Content handelt, auf dem Rechtedefinitionssprachen aufbauen. Eben solche Rechtedefinitionssprachen sind dabei nach Fränkl zentraler Punkt eines funktionierenden DRMS. Sie sind weitgehend standardisiert und gehören teilweise sogar zu Open Source. Kernpunkt ist plattformübergreifende Implementierung und das Vorliegen von Rechtearten und deren Attributen – letztere müssen dabei durch den Urheber jederzeit geändert werden können, was dazu geführt hat, dass der Trend dazu geht, den Content von den Rechten zu separieren. So gut diese Idee auch ist, so erhöht dies die Vulnerabilität im Gegensatz zu gekapseltem Content, der die Rechtedaten eingebettet hat[112]. Die erhöhte Content-Vulnerabilität ist von Diemar folgend auch der Grund für die Implementierung technischer Schutzmaßnahmen[113]. An weiteren Technologien finden sich bei Fränkls „unterstützenden Systemen“ noch z.B.

[109] Und dies war leider der wichtigere Schutzmechanismus.
[110] Vgl. Bechtold, 2002, S. 374.
[111] Vgl. Fränkl, 2004, S. 32 ff.
[112] Vgl. Fränkl, 2004, S. 48 ff.
[113] Vgl. von Diemar, 2002, S. 10.

das Sandboxverfahren, das zwar nicht zu DRM gehört, es aber erlaubt in geschützten Bereichen Content und Code auszuführen, ganz so wie der TPM-Chip in Trusted Systems die Trennung zwischen dem uneschützten und geschützten Bereich über die sog. Nexus-Schicht durchführt.

2.5.5. Implementierung bei Software (Schlüssel und Black Lists)

Software wird primär mittels Installationsschlüsseln und neuerdings durch Aktivierung aus daraus erstellten Hash-Werten vor Installation auf mehr als der lizenzierten Anzahl von Systemen geschützt (dies läuft in etwa nach o.a. Verfahren mittels Public-Keys ab). Mittels Update-Funktionen wird in sog. Patches vielfach auch eine Liste mit illegalen Produktschlüsseln mitgeliefert (Black List). Der Sinn: findet der Code des Programms illegale Schlüsseln, so wird die Software in der Regel durch den Hersteller deaktiviert. Somit leuchtet es auch ein, sich im Falle des Verlustes eines Installationsschlüssels, beim Hersteller einen neuen zu besorgen – kostenloser Anspruch auf einen solchen besteht jedoch nicht[114]. Der Einsatz von Schlüssel aus dem Internet ist dabei umstritten – für die Zeit zwischen Erhalt eines neuen Schlüssels vom Hersteller und der Nutzung der Software im Notfall ist es allerdings rechtlich zulässig. Vergleichbar ist dies mit dem „Zutrittverschaffen“ zum eigenen KFZ, von dem man die Schlüsseln verloren hat. Die Weitergabe eines Software-Installationsschlüssels von Freunden oder Bekannten ist dagegen nicht empfehlenswert, da so sehr schnell Black Lists bei den Herstellern entstehen, sollten diese durch Updatefunktionen bemerken, dass diese Schlüsseln mehrfach verwendet werden[115]. Der Primärnutzen von solchen Updates, bzw. Patches, nämlich die Behebung von Sicherheitslücken und Fehler im Code der Software erhält damit den negativen Beigeschmack, Systeme unbrauchbar zu machen[116], was somit nicht ganz im Sinne der geplanten Wirkung von DRMS stehen dürfte, da genau deshalb davon Abstand genommen wird, Sicherheitsfunktionen nachzurüsten. Die Leidtragenden sind ehrliche Anwender, die von ungeschützten Systemen mittels DoS-Attacken betroffen sind[117]. V.a. automatische Updates zum Media Player in Windows,

[114] Vgl. Arnold Arne: Alles wissen. In: PC Welt, 01 / 2005, S. 114.
[115] Vgl. Weidemann Tobias: Seriennummern frei Haus. In: PC Welt, 10 / 2004, S. 78.
[116] Vgl. Eggeling Thorsten / Kroschel Andreas / Löbering Christian: Was weiß Microsoft? In: PC Welt, 06 / 2005, S. 75 f.
[117] Vgl. Busch, 2002, S. 96.

die über Administratorrechte verfügen und unbekannte Patches laden, sind hier verrufen[118]. Mit der neuen TCPA-Architektur wäre es nicht einmal mehr möglich, derartige Updates aus dem System zu entfernen, da schlichtweg ein Programm, wie eben der Media Player ohne Updates nicht mehr als vertrauenswürdig eingestuft wird. Kernbestandteil dieser Architektur sind wieder Schlüssel, wobei einer im PC mit TPM-Chip sitzt, der andere auf einem Lizenzserver irgendwo in der Welt[119]. Eine Reaktivierung von Vorgängerversionen wie sie noch ein Jahr zuvor vorgeschlagen wurde, wäre damit *erstens* nicht mehr möglich, *zweitens* auch gar nicht sinnvoll, da sich neuerer Content (codiert durch neue Codec-Algorithmen) nur auf neuen Versionen nutzen lässt[120]. Die Produktaktivierung für Software und Aktivierung von Content stellt somit eine in letzter Zeit weit verbreitete Methode des DRM zum Schutz geistigen Eigentums dar. Besonders der Nachahmeffekt wirkt hier wie ein Schneeballsystem, da viele Hersteller, wie z.B. Symantec in seinen Antivirenschutz- und Sicherheitsprogrammen[121] seit der Einführung von Windows XP durch Microsoft als erstes Massenprodukt mit Aktivierung ebenfalls auf diese Form des Schutzes setzen. Ohne Freischaltung durch Server im Internet läuft hier nichts[122]. Auch andere Hersteller wie Adobe (PDF-Format) folgen diesem Beispiel nun, da der Bann gebrochen ist[123]. Für Aktivierung allgemein können zur eindeutigen Identifizierung von Endgeräten MAC-Adressen von Netzwerkkarten sowie gebildete Hardware-Hash-Werte aus den Installationsschlüsseln und / oder sog. Dongles zum Einsatz kommen[124], d.h. z.B. USB oder Parallelportstecker, ohne den die Software oder der Content nicht läuft.

---

[118] Vgl. Himmelstein Gerald: Der digitale Knebel. In: c´t #15, vom 15.07.2002, S. 19.
[119] Vgl. Arnold Arne: Droht die totale Überwachung? Big Brother Microsoft. In: PC Welt, 06 / 2003, S. 13.
[120] Vgl. Perband Andreas / Thoma Jörg: Dreister Media Player. In: PC Welt, 09 / 2002, S. 13.
[121] Vgl. Symantec, 2004, S. 31
[122] Telefonische Aktivierung wird teilweise ebenfalls angeboten, allerdings ist dabei noch einfacher festzustellen, wer hier anruft, sofern die Rufnummernanzeige nicht unterdrückt ist. Primär jedoch wird Aktivierung über das Internet forciert, da sich dabei wesentlich mehr Informationen ermitteln lassen, wie im Datenschutzteil noch gezeigt wird.
[123] Vgl. Michl Martin: Front gegen Raubkopierer. Produktaktivierung. In: Chip, 09 / 2003, S. 102.
[124] Vgl. Biddle Peter (u.a.): The Darknet and the Future of Content Protection. In: Becker, 2003, S. 360.

2.5.5.1. Windows XP-Aktivierung und Media Player DRM umgangen

Schwachstellen gibt es in allen DRMS. Gemeinsam ist ihnen aber, dass die Umgehungstechnologie vielfach frei im Internet erhältlich ist, wenn man nur lange genug danach sucht. Somit hat jeder Internet-Nutzer potentiellen Zugang zu solchen Tools, ohne über kompetentes Fachwissen von Programmierung und die Ausnutzung von Sicherheitlücken Bescheid zu wissen (sog. Exploits)[125]. Stellvertretend für die Schwachstellen soll Windows XP hier in doppelter Hinsicht dienen: *erstens* für die Umgehung des Schutzes von AV-Content. *Zweitens* für das Betriebssystem selbst. Zum ersten Punkt lässt sich sagen, dass hierzu der Content für den Media Player vom DRM befreit werden soll. Der Media Player spricht dabei die DRM-Sprache im WMA-Format[126]. Um derartigen Content ohne DRM zu nutzen, gibt es z.B. das Programm „unfuck.exe“. Der Grund dafür ist die schwache Sicherheitsarchitektur des Media Players, der wie auch das System selbst auf DLL-Dateien basiert. Im Gegensatz dazu verwenden z.B. Realplayerdateien und PDF-Texte externe Lizenzen[127]. Der zweite Schwachpunkt bei Windows XP ist die Aktivierung des Systems selbst. Genaue Anleitungen, wie man diese umgehen kann und sich daher sein Recht auf informationelle Selbstbestimmung der beim Aktivierungsprozess übermittelten Daten zurückholt, finden sich z.B. bei Reuscher[128].

Kernbestandteil der verschiedensten Vorgehensweisen sind sowohl legale wie auch rechtlich umstrittene Methoden, da teilweise gegen Urheberrecht verstoßende Eingriffe in das Betriebssystem vorliegen. Die *erste* Möglichkeit besteht in der Sicherung und Wiederherstellung der Datei WPA.DBL, was allerdings schon eine erstmalige Aktivierung voraussetzt. Die *zweite* Möglichkeit dagegen basiert auf einem Russencrack (der sog. SAD-Team Crack), der die Aktivierung wegpatcht. Ob es somit zwecks Erschließung neuer Märkte in Regierungskreisen sinnvoll war, Russland neben den Briten, der Nato und den Chinesen[129] durch Microsoft-Gründer Bill Gates

[125] Vgl. Hauser Tobias / Wenz Christian: DRM Under Attack: Weakness in Existing Systems. In: Becker, 2003, S. 206.
[126] Vgl. Guth Susanne: Rights Expression Languages. In: Becker, 2003, S. 112.
[127] Vgl. Hauser Tobias / Wenz Christian: DRM Under Attack: Weakness in Existing Systems. In: Becker, 2003, S. 207 ff.
[128] Vgl. Reuscher, 2002, S. 40 ff.
[129] Letzteren zur Modifikation von Windows zu Zensurzwecken, um das bisher verwendete Open Source Linux an weiterer Verbreitung in China zu hindern, um somit neue Märkte zu erschließen.

höchstpersönlich autorisierten Einblick[130] in den Windows-Quellcode zu geben, sei dahingestellt[131]. Da allerdings hier Eingriffe in den Code durch urheberrechtliche Verbote der Bearbeitung untersagt sind, wäre hier die Erlaubnis des Urhebers einzuholen[132]. Damit ist ein Crack eindeutig illegal, denn eine Zustimmung zur Umgehung des Schutzmechanismus hätte Bill Gates wohl nicht gegeben[133]. Bemerkenswert ist jedoch, dass sich für Windows-XP die gesellschaftliche Struktur aus Sicht Microsofts erst bei Volume-Lizenzen[134] so richtig zeigt. Diese sind nämlich nicht aktivierungspflichtig und liefern die *dritte* Umgehungsmöglichkeit, denn leider war es genau diese wichtige Zielgruppe der Unternehmenskunden, die die sog. Corporate-Files ins Internet stellten. Damit wurde es nichts mit der WPA, die „vor Softwarepiraterie und dem zufälligen Kopieren von Windows schützen“ soll – so jedenfalls die offizielle technische Referenz dazu[135]. Den Zufall „Unternehmenskunde“ hat man hier offenbar nicht einkalkuliert. Die Corporate-Files lassen sich nämlich auch auf reguläre Windows-Versionen anwenden[136]. Fazit: die Aktivierung ist zahnlos und lediglich für ehrliche Nutzer ärgerlich[137]

---

[130] Sicher ist aber, dass hier ein deutliches Indiz dafür vorliegt, dass die Grenze zwischen privatwirtschaftlichen Unternehmen und staatstragenden Institutionen zusehends verschwindet. Immerhin mutet dies fast schon wie ein Gipfeltreffen großer Staatsmänner an – außerdem hat Hr. Gates schon im Zuge des Anti-Trust-Verfahrens der US-Regierung gegen Microsoft vor dem US-Senat eine Rede gehalten, in der er den Kurs seiner Firma verteidigt hatte.

[131] Vgl. Pyczak Thomas: China darf Windows-Quellcode einsehen. In: Chip, 05 / 2003, S. 14.

[132] Vgl. Wirtz Martin: Urheberrecht und verwandte Schutzrechte. In: Bröcker, 2003, S. 624.

[133] Einen Anwendungsfall gibt es aber dennoch: der Test von Sicherheitsmechanismen. Hier wäre ohne Erlaubnis der Hackversuch ebenfalls strafbar, d.h. in diesem Falle läge durchaus Interesse der Hersteller vor, ihre DRMS einer Sicherheitsüberprüfung zu unterziehen. Vielfach allerdings sind diese Tests nicht umfangreich und aus Konkurrenzdruckgründen werden fertige Programme, bzw. Technologien früher auf den Marktgebracht, als dies eigentlich sicherheitstechnisch vertretbar wäre.

[134] Vgl. Grützmacher Malte: Unternehmens- und Konzernlizenzen. Zur Einräumung urheberrechtlicher Nutzungsrechte an Software bei Unternhemens- und Konzernlizenzen. In: Schneider, 2005, S. II / 204 ff.

[135] Vgl. McKay, 2002, S. 47

[136] Der Einsatz ist dabei umstritten – immerhin (so wird hier vorausgesetzt) verfügt man über eine gültige Windows Lizenz. Wie noch gezeigt wird, ist das Click-Wrap-Agreement zur Akzeptanz der Produktaktivierung vielfach ungültig, d.h. konkret also, dass mit dem Einsatz der Corporate-Files lediglich der „vertragsmäßige Zustand“ der ordnungsgemäßen Softwarenutzung hergestellt wird. Andererseits verfügt man nicht über die Lizenz einer Volume-Edition und muss zur Nutzung der Corporate-Files ohnehin einen Volume-Key zur Installation eingeben. Da allerdings bis heute nicht bekannt ist, wo hier der funktionale Unterschied zwischen aktivierungspflichtigen und aktivierungsfreien Windows-Versionen liegt (eben mit Ausnahme der Aktivierung), erhält man hier sogar „weniger Software“, als eigentlich in aktivierungspflichtigen Versionen – diese sind ja um zusätzlichen Code bereichert, nämlich den, der Aktivierungsprozedur. Ähnlich argumentieren könnte man mit der „Spanischen Panne“ – dabei wurde anstatt einer geplanten zeitlich limitierten Trialversion von Windows 2000 Server irrtümlich eine Vollversion auf die Heft-CD eines spanischen Computer-Magazins gepresst. Nach Bekanntwerden des Irrtums waren die Hefte logischerweise binnen Stunden ausverkauft.

[137] Vgl. Reuscher, 2002, S. 39 ff.

2.5.5.2. Spiele

Bei Spielesoftware wird häufig Zerstörung von Teilbereichen eines Datenträgers[138] als Schutzmechanismus eingesetzt. Spielesoftware prüft nämlich mehrheitlich auf das Vorhandensein einer Original-CD, d.h. auf das Vorliegen der Datenträgerfehler als Erkennungsmerkmal einer originalen CD oder einer Kopie. Verschiedene andere Kopierschutzmechanismen wirken ebenfalls, wie z.B. fehlerhaften TOCs, die auch schon bei Audio-CDs eingesetzt werden oder falschen Angaben über Dateilängen[139], wie folgende Abbildung zeigt:

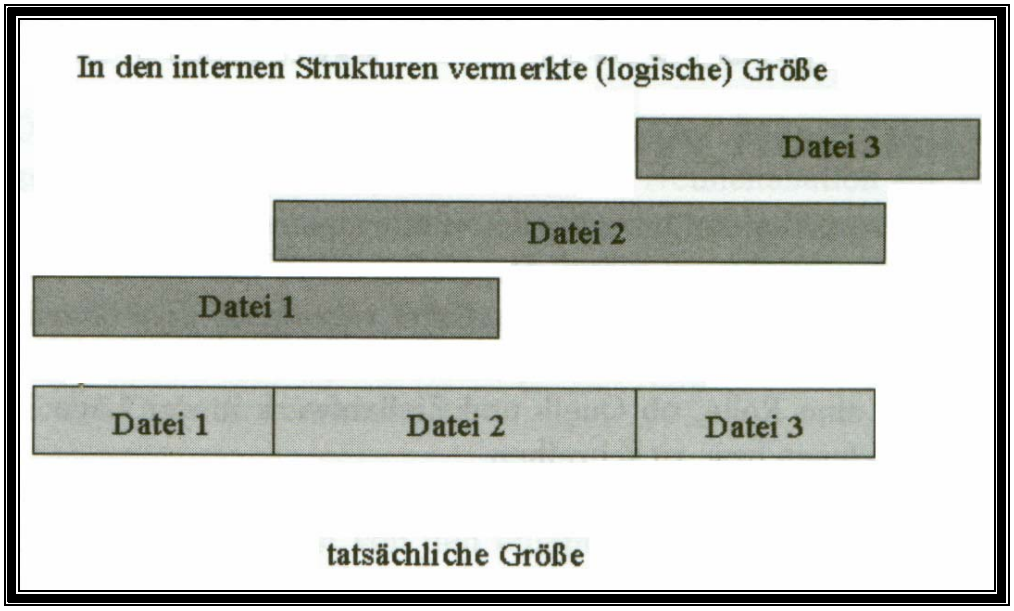

Abbildung 9: Ungültige Dateilängenangaben als Kopierschutzmechanismus[140]

Neueste Schutztechnologien basieren auf DPM (Data Position Measurement). Dabei macht sich der Code der Steuerungssoftware zu Nutze, dass in Presswerken gepresste CDs exakt identische Eigenschaften aufweisen. Gebrannte Rohlinge dagegen weisen Abweichungen bei der Position der Daten auf. Der Kopierschutz erkennt dies, und verweigert so den Zugriff auf den Content. Lediglich durch Kombination von Kopierschutzemulatoren und Images auf virtuellen Laufwerken kann hier noch Abhilfe geschaffen werden[141]. Folgende Abbildung zeigt die Funktionsweise:

---

[138] Vgl. Gutman, 2003, S. 136.
[139] Vgl. Tischer, 1998, S. 366.
[140] Aus: Tischer, 1998, S. 366.
[141] Vgl. Chachulski Frank: Die Allesbrenner. In PC Magazin, 05 / 2003, S. 105.

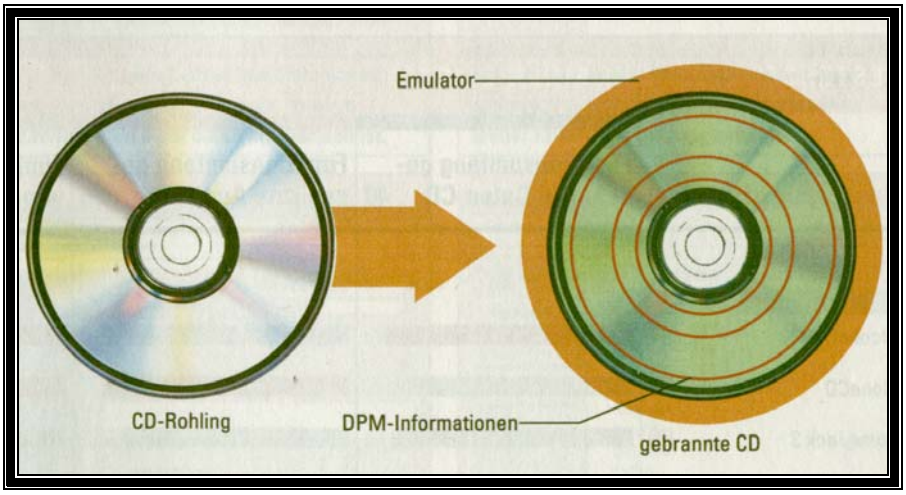

Abbildung 10: Data Position Measurement als Kopierschutzmechanismus[142]

Hacker entschlüsseln auch Zugriffsmuster auf Originaldatenträger mittels Spezialsoftware wie z.B. Bushound[143]. Abhilfe schaffen auch hier Emulatoren wie die Daemon-Tools. Viele davon sind auch in der Lage, Kopierschutzmechanismen zu emulieren, deren legaler Einsatz jedoch umstritten ist – offiziell geht es darum, Hardware zu schonen[144], indem die CD-Laufwerke vor unnötigen Zugriffen auf die originalen Datenträger bewahrt werden, was letztlich auch den Datenträger selbst schont. Vielfach werden auch Schutzmechanismen wie Safe Disc durch Patches unwirksam gemacht, d.h. dass die Prüfung auf den originalen Datenträger einfach deaktiviert wird[145]. Umstritten ist dabei die rechtliche Lage bei Software generell, denn nach herrschender Lehrmeinung ist davon eine Sicherungskopie erlaubt[146], allerdings nur wenn sie für die Sicherung künftiger Benutzung erforderlich ist, so §69d Abs. 2 des deutschen Urheberrechts. Liegt Software jedoch auf CD / DVD vor, so unterliegen diese Medien nicht der Abnutzung, d.h. konkret, dass eine Sicherungskopie nicht erforderlich ist. Dieser Hinweis auf Verschleißfreiheit einer CD / DVD ist aber nach

[142] Aus: PC Magazin, 05 / 2003, S. 105.
[143] Vgl. Kuther Margit / Rau Thomas: Alles Knacken. In: PC Welt, 01 / 2006, S. 108.
[144] Vgl. Wolski David: Gute Tools, böse Tools. In PC Welt, 05 / 2003, S. 71.
[145] Vgl. Schräder Daniel: Kommerzieller Schutz ist kein Hindernis. So manipulieren Cracker jedes Programm. In: PC Direkt, 12 / 2001, S. 66.
[146] Vgl. Mielke Kai: Illegale Datenflut – Risiken und Nebenwirkungen. In: c´t #24, vom 15.11.2004, S. 216.

Aussagen des Philips-Konzerns[147], der ja schließlich die CD erfunden hat, eindeutig falsch[148].

2.5.6. Implementierung bei DVDs

Code stellt nach Lessig die Kontrollarchitektur und damit die Grundlage der Regulierbarkeit von Systemen dar. Seith geht noch weiter, indem dem Code eine Art eigenes Urhebergesetz zugestanden wird – „der Programmiercode als Kodifikation.“[149] Bei DVDs wurde dies jedoch den Contentherstellern zum Verhängnis – der mangelnden Kooperation zwischen Vertretern der Film- und Unterhaltungsindustrie 1996 sei es gedankt[150]. Die Spezifikationen der DVD wurden nämlich zum Zeitpunkt verabschiedet, als deren DRM-Strategie nicht ausgereift war, womit Clement an dieser Stelle bestätigt wäre. Ganze drei Haupt- und insgesamt bis zu zehn (aber weniger wichtigere) Schutzmechanismen wurden bei DVDs implementiert und stellen somit ein Beispiel des Overprotecting[151] von geistigem Eigentum dar. Warum die hervorragende Qualität von DVDs so massiv geschützt werden, ist fraglich, da Filme regelmäßig auch auf VHS erscheinen, die nicht DRM geschützt sind[152].

2.5.6.1. Notwendiger Schutz: Filme gibt es noch vor der Kino-Premiere

Der Grund warum etliche Filme teils vor der Kino-Premiere illegal im Internet zu finden sind, ist schlichtweg, dass es unter den beteiligten Personen bei der Herstellung und den Filmfestival-Juroren schwarze Schafe gibt. Diese wollen z.B. nur ihre Familien damit versorgen und überlassen ihnen eine Vorabkopie. Ist eine solche aber einmal in Umlauf, ist es nicht mehr schwer, diese zu digitalisieren und ins Netz einzuspeisen - damit entstehen die illegale Filmtauschbörsen – und diese sind ebenfalls von schwarzen Administratorschafen bei Providern online geschaltet[153]. Diese Innentäter finden sich

---

[147] Vgl. Kuppek Harald (u.a.): Ich hab´s kopiert. In: Computer Bild, 19 / 2002, S. 133

[148] Wäre dem so, dürfte es mit Ausnahme von schweren mechanischen Beschädigungen und mutwilliger Vernichtung der Datenträger keine defekten CDs geben – die Praxis zeigt aber, dass dies sehr wohl der Fall ist, besonders wenn die Datenträger offen in der Sonne liegen oder schon durch Transportschäden verkrazt sind (dazu reicht es, wenn die CD / DVD aus der Verankerung der Plastikhülle fällt und dadurch „herumrutscht“).

[149] Nach Seith, 2003, S. 57.

[150] Vgl. Bechtold, 2002, S. 102.

[151] Nach Lessig, 2001, S. 204

[152] Vgl. Bechtold, 2002, S. 381.

[153] Vgl. Hosbach Wolf: Schuldig, Euer Ehren! Rechtslage bei Internet-Angeboten. In: PC Magazin, 09 / 2001, S. 55

quasi überall, dass auch das beste DRMS gegen menschliches Versagen machtlos ist[154]. Findet sich jedenfalls einmal der Weg aus dem Internet auf einen DVD-Rohling und dann zu profitgierigen Raubkopieren, erstellen diese im großen Stil daraus echt gepresste DVDs und diese landen dann schneller auf lokalen Hinterhöfen in China und Vietnam als eben auf der Premierenleinwand. Danach ist der Vertriebsweg über einschlägige Kanäle auch nicht mehr weit in andere Staaten. Die weitaus geringeren Beträge, die man für Raubkopien verlangt, rechnen sich dabei schnell, wenn man die gigantische Nachfrage bedenkt – auch illegale Downloads werden vielfach gegen Gebühr angeboten[155]. Legale Alternativen gibt es zu diesem Zeitpunkt nicht, was somit den Sportsgeist weckt, einer der ersten zu sein, die neuesten Blockbuster zu sehen. Immerhin dauert es doch Wochen oder sogar Monate nach der Kino-Verwertung bis erste und wesentlich teurere legale DVDs im Zuge der Zweitverwertung verfügbar sind[156]. Fazit: die dann aufgebrachten Kopierschutzmechanismen kommen zu spät und allfällige Wasserzeichen in Vorabversionen hindern nicht den Filmgenuss im Wohnzimmer für Normalverbraucher, da stand allone DVD-Player im Gegensatz zum Media Player am PC mit Internet (noch) keinen Rückkanal über Datennetze haben.

2.5.6.2. Overprotecting der DVD durch verschiedene Maßnahmen

Im Detail zu nennen wäre ***erstens*** **der Regionalcode** (RC). Dieser sollte die Wiedergabe auf Abspielgeräten nur in einer bestimmten Region der Erde zulassen. Zweck war geradezu die Verhinderung der Wiedergabe von Filmen, die z.B. in den USA bereits zur Zweit- oder Drittverwertung am Markt waren, in Europa jedoch noch im Kino gezeigt wurden. Folgende RCs existieren derzeit:

Regionalcode	**für Land / Region**
0	Alle
1	Kanada, Vereinigte Staaten von Amerika sowie deren Territorien
2	Japan, Europa, Südafrika, Naher Osten (einschließlich Ägypten)
3	Südostasien, Ostasien (einschließlich Hongkong SAR)
4	Australien, Neuseeland, pazifische Inseln, Mittelamerika, Mexiko, Südamerika, Karibik
5	Gebiet der früheren Sowjetunion, indischer Subkontinent, Nordkorea, Mongolei, Afrika
6	China
7	(Reserviert, derzeit nicht verwendet)
8	Besondere internationale Standorte (unter anderem Flugzeuge in der Luft, Kreuzfahrtschiffe, usw.)

Tabelle 2: DVD-Regionalcodes [157]

[154] Vgl. Fuhrberg, 2001, S. 334.
[155] Vgl. Hoffmann Artur: China-Cracker. In: PC Magazin, 06 / 2006, S. 16
[156] Vgl. Eggeling Thorsten: Tauschrausch – illegal im Untergrund. In PC Welt, 12 / 2004, S. 59 ff.
[157] Quelle: McKay, 2002, S. 435 f.

Der RC konnte aber sehr leicht umgangen werden, sei es durch legalen Erwerb und Import eines entsprechenden Abspielgeräts der jeweiligen Region oder durch Freischaltung eines regionsspezifischen Abspielgerätes für alle Regionen. Dies war deswegen so einfach, da die Hersteller durch Konkurrenzkampf und Zeit-, sowie Preisdruck nicht noch die Verwaltungskosten für unterschiedliche Produktionsstraßen übernehmen konnten, in denen dann unterschiedliche Steuerungschips mit hardwaremäßigen RCs implementiert wurden. Stattdessen wurden generalisierte Chips per Einstellung auf den jeweiligen Code gesetzt. So tritt auch Regulierung durch Wettbewerb zwischen den DRMS-Herstellern auf und nicht nur durch gesetzliche Rahmenbedingungen[158]. Die Hersteller von Abspielgeräten ziehen sich dabei aus der Verantwortung, indem Sie offiziell keine Unterstützung für die Freischaltmöglichkeiten von inoffiziellen Zusatzfunktionen bieten. Dadurch sparen sie *erstens* Lizenzgebühren an Philips (um z.B. auch SVCD-Wiedergabe zu ermöglichen) und laufen *zweitens* nicht Gefahr, mit den Interessen der Rechteinhaber an Content in Konflikt zu geraten, sofern die Geräte mit aktivierten Regionalcodesperren ausgeliefert werden. Sämtliche Sperren lassen sich jedoch in fast allen Fällen durch Eintippen von Geheimcodes auf der Fernbedienung umgehen[159]. Die neueste Implementierung ist allerdings der erweiterte Regionalcode RCE (Regional Code Enhancement) – dabei lassen sich DVDs an manipulierten DVD-Playern nicht mehr wiedergeben. Der Trick dabei: RCE-DVDs „fragen“ den Player, welche RCs er verarbeiten kann. Wird mehr als einer unterstützt, handelt es sich um einen modifizierten Player, d.h., dass die Wiedergabe verweigert wird. Allerdings lassen sich die Geräte mittels der Geheimcodes auch wieder „rückmodifizieren“, d.h. dass sie wieder nur einen einzigen RC unterstützen[160].

Der *zweite* Schutzmechanismus bei DVDs stammte vom Hersteller Macrovision und sollte wie schon bei VHS-Bändern die Überspielung auf analoge Aufzeichnungsgeräte verhindern. Dazu wurden Störsignale in den digitalen Datenstrom eingefügt, die den Kommunikationsfluss zwischen Abspielgerät und Recorder durch Farbflackern oder Streifen im Bild beeinträchtigten. Auch hier ließen sich die Steuerungschips der Abspielgeräte freischalten, keine Macrovision-Störsignale

[158] Vgl. Bechtold, 2002, S. 337.
[159] Vgl. Kuppek Harald (u.a.): Geheim-Agent. In: Computer Bild, 14 / 2002, S. 168 ff.
[160] Vgl. Schmelzle Michael: Filme ohne Grenzen. In: PC Welt, 08 / 2003, S. 133.

auszugeben. Der Grund für den Analogschutz ist die Möglichkeit, den Content später neu zu digitalisieren[161]. Dies ist dank heute verfügbarer moderner Mastering-Systeme nur mit einem Minimum an Qualtiätsverlust behaftet und eine qualitativ leicht minderwertige Digitalkopie ohne DRM-Schutz lässt sich besser nutzen als eine optimale Digitalkopie mit DRM-Schutz. Der DRM-Schutz endet ja an analoger Stelle, weshalb analoge Kopierschutzverfahren auch bei digitalem Content sehr wichtig sind und den Beweis dafür liefern, dass eingebettete Wasserzeichen auch konvertierungsfest sein müssen, wie im Wasserzeichenkapitel erläutert wurde.

Übrig bleibt der *dritte* und als effektivster Schutzmechanismus angesehene Content-Scramble-System-Algorithmus (CSS). Dieser sollte den Content verschlüsseln und erst während der Wiedergabe entschlüsseln. Unzulässige Kopien sollten somit verhindert werden. Allerdings verhinderte CSS auch, dass sich legal erworbene DVDs unter dem Open Source Betriebssystem Linux wiedergeben ließen[162]. CSS war bereits bei der Verabschiedung des DVD-Standards schwach und wurde schnell geknackt mittels des DeCSS-Algorithmus[163]. Viele Software-Programme für Computer konnten CSS folglich umgehen. Zu verdanken ist dies u.a. Hackermitgliedern einem 15-jährigen Norweger namens Jon Lech Johansen, der zweitinstanzlich vom Vorwurf der Veröffentlichung von „Reverse-Engineered“ Software freigesprochen wurde[164].

2.5.6.3. Umgehung von CSS

90% aller DVDs am Markt sind mit CSS geschützt[165]. Konsequenterweise heißt dies auch, dass 90% der DVDs mittels des Programms AnyDVD unter Umgehung von CSS durch jegliches Brennprogramm gerippt und anschließend kopiert (=gebrannt) werden können. Zudem lässt sich mittels AnyDVD auch gleichzeitig die Regionalcodeschutzsperre einer DVD entfernen. Ferner ermöglicht das Programm die Wiedergabe von DVDs mit anderen RC-Codes als das Laufwerk eigentlich unterstützt. Dies war auch der Primärzweck des Tools. Damit ist die frühere Vorgehensweise mittels Einspielen einer älteren Firmware ohne RC-Code in das DVD-Laufwerk nicht mehr erforderlich – dies würde auch nicht mehr bei neueren Modellen funktionieren

[161] Vgl. Bechtold, 2002, S. 100.
[162] Vgl. Lessig, 2002, S. 189.
[163] Nach Forgó Nikolaus: Code und Kontrolle. In: Gasser, 2002, S. 45.
[164] Vgl. von Keudell Fabian: Kopierschutz? Na und! In: Chip, 05 / 2006, S. 102.
[165] Vgl. Heidrich Joerg / Himmelreich Gerald: Die Grenzen des Erlaubten. Ratgeber: Privatkopien, Tauschbörsen, Abmahnungen. In: c´t #5, vom 20.02.2005, S. 112.

und Hersteller dürfen konsequenterweise keine Auskunft über die Entfernungsmöglichkeiten geben, sind sie doch von Seiten der Filmindustrie dazu verpflichtet worden[166] – möglich ist aber auch hier auf vielen Brennern mittels entsprechender Geheimcodes oder Zusatzprogrammen die Freischaltung wie bei den o.a. Playern durch die Fernbedienung. Ist nämlich der fünfmalige erlaubte legale Wechsel des RC-Codes eines älteren Laufwerkes ausgeschöpft, so kann man sich mittels Region Killer oder DVD Genie behelfen[167]. Da durch das reine Ändern des Regionlacodes kein Kopierschutz umgangen wird (was neuerdings verboten ist), ist diese Maßnahme auch legal, um DVDs aus anderen Regionen der Welt anzusehen – sie versagt jedoch bei neueren Laufwerken, die den Regionalcode fest implementiert haben – dort wäre wieder AnyDVD angesagt (und dieses auf deutschem Boden zu nutzen, ist verboten). Am Beispiel von Windows XP zeigen folgende Abbildungen sowohl auf reiner Software- wie auf Hardwareebene die Implementierung des Schutzmechanismus.

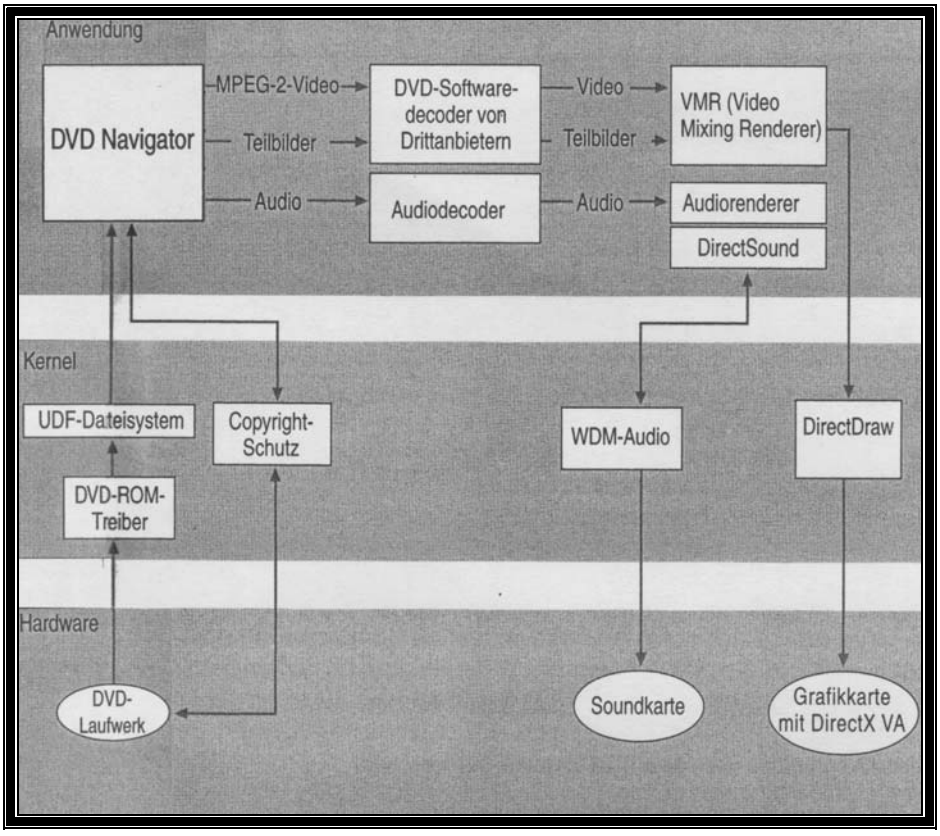

Abbildung 11: Schutz von DVDs durch Software in Windows XP[168]

[166] Vgl. Helmiss Christian / Rau Thomas: Das Duell: Per PC zum Heimkino. In: PC Welt, 11 / 2000 S. 244.
[167] Vgl. Coppala Richard (u.a.): Tipps & Tricks zu Hard- und Software. In PC Welt extra, April / Mai / Juni 2004, S. 53
[168] Aus: McKay, 2002, S. 431.

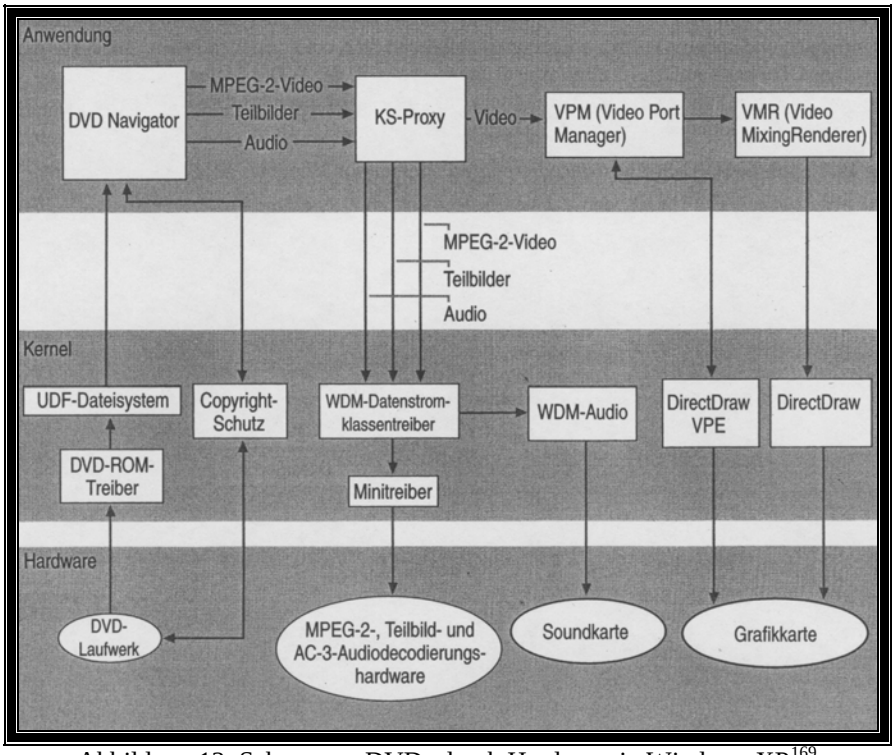

Abbildung 12: Schutz von DVDs durch Hardware in Windows XP[169]

Wegen seines modularen Aufbaus und der „Zwischenschaltung“ in der Architektur verwundert es somit nicht, dass der Schutz sehr anfällig ist, und sich deswegen so leicht umgehen lässt. AnyDVD nutzt dies ja, indem es sich in die Schicht des DRM-Schutzes schaltet. Fazit: alle drei Hauptschutzmechanismen der DVD haben versagt - die anderen sind nur untergeordnet und werden hier nicht behandelt[170] – versagt haben aber auch sie. Der gültige DVD-Standard lässt sich nun nicht mehr revidieren, da einfach zu viele Abspielgeräte am Markt sind, die der Rezipient nicht bereit wäre, zum Zwecke besserer Schutzmechanismen für die Filmindustrie auszutauschen. So muss sich eine gekaufte DVD von heute auch noch am DVD-Player der ersten Generation wiedergeben lassen. Regulierung wäre grundsätzlich durch Änderung der Architektur möglich, allerdings bleibt derzeit aus marktechnischen Gründen lediglich die rechtliche Regulierung durch gesetzlichen Umgehungsschutz wie bei den urheberrechtlichen Auswirkungen noch für Digitalkopien gezeigt wird. Die Contentindustrie scheut hier offenbar den Vertrauensverlust der Nutzer durch zwangsweises Umrüsten auf neue Technologien.

[169] Aus: McKay, 2002, S. 432.
[170] siehe dazu etwa Bechtold, 2002, S. 107 ff.

Lessig spricht für derartige Probleme von bestimmten Kosten in Zusammenhang mit der jeweiligen Regulierungsebene[171]. So ist der CSS-Code von damals Gesetz und bleibt es auch, solange DVDs und Player am Markt sind. Etwas was bei Audio-CDs wie im nächsten Kapitel noch gezeigt wird, nicht der Fall war, da der Yellow Book Standard nicht zu 100% eingehalten wurde. Diese Unsitte kommt allerdings auch schon bei DVDs in Mode, d.h. konkret die Verwendung von absichtlich defekten Sektoren[172].

2.5.7. Implementierung bei sonstigem Content

2.5.7.1. Die Audio-CD

Dank unverblümter Äußerungen von Nutzern, Musik im Internet zu klauen, bzw. von Freunden „zu leihen“ und dann zu brennen, verwundert folgende Entwicklung nicht. Im Jahr 2000 wurde nach einer GfK-Studie erstmals ein Rekord an gebrannten, statt gekauften Musik-Alben gemeldet. Als Konsequenz wurde der erste Audio-Kopierschutz namens Cactus Data Shield durch BMG am Album Razorblade von HIM eingeführt. Angesichts der Raubkopieentwicklung bei CD-Alben (und seit 2003 auch DVDs) leuchtet dies auch ein:

Abbildung 13: Wo man sich neue Musik „holt“[173]

[171] Vgl. Lessig, 2001, S. 161.
[172] Vgl. Krempl Stefan: Ausgebrannt!? In: c´t #24, vom 15.11.2004, S. 67.
[173] Quelle: Tomorrow, März 2006, S. 3.

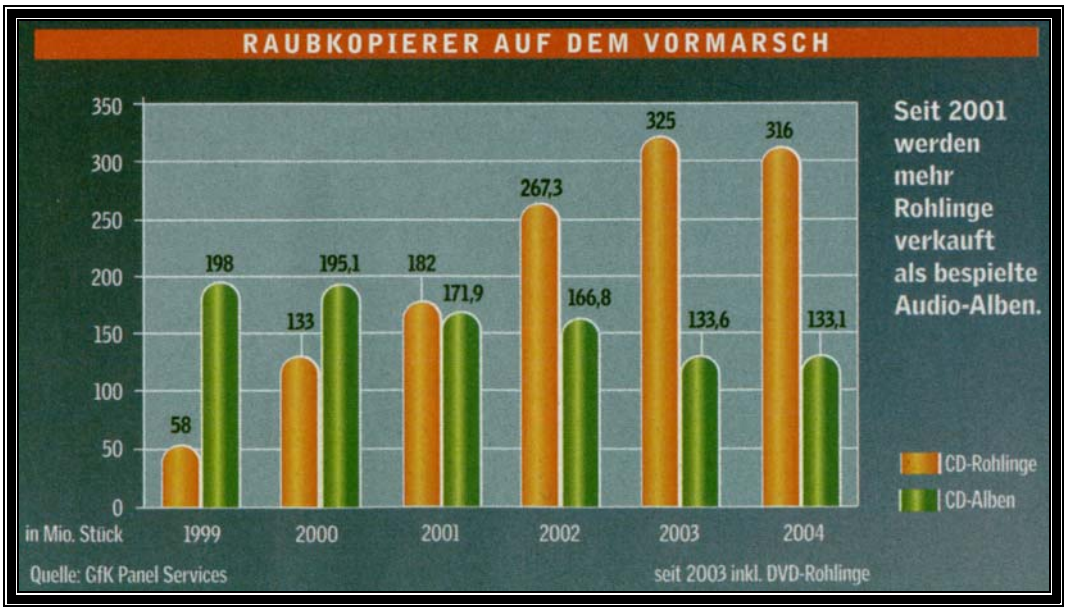

Abbildung 14: Sinkender Absatz bei Alben, dafür steigender bei CD- / DVD-Rohlingen[174]

Der leichte Rückgang von 2004 wäre dadurch erklärbar, dass DVD-Rohlinge berücksichtigt sind, die eine entsprechend höhere Speicherkapazität aufweisen, was automatisch zum Rückgang des Absatzes bei CD-Rohlingen führt. Denn auf DVDs lässt sich etwa die siebenfache Menge an MP3-Dateien speichern, was auch den Vorteil hat, diese auf DVD-Playern zu nutzen (viele unterstützen ja MP3-Wiedergabe). Folgende Abbildung zeigt dabei den direkten Vergleich der Speicherdichte von CD und DVD:

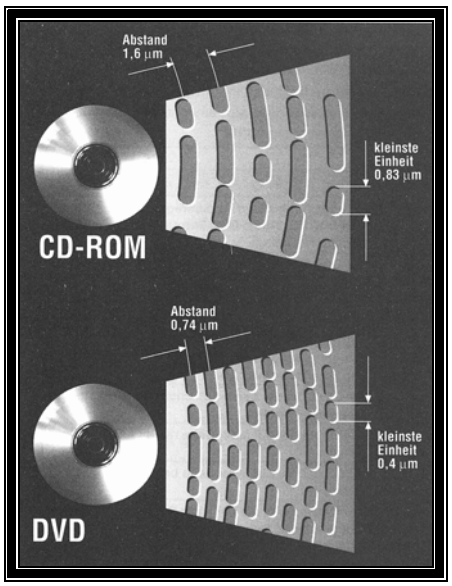

Abbildung 15: Speicherdichte von CD und DVD im direkten Vergleich[175]

[174] Aus: Chip, 05 / 2006, S. 102.
[175] Aus: Tischer, 1998, S. 427.

Cactus Data Shield, was dabei auf Codierung einer fehlerhafter TOC basierte, funktionierte jedoch „so gut“, dass auch viele herkömmliche CD-Abspielgeräte Probleme bei der Wiedergabe hatten[176] - dieser neuartige CD-Typ entsprach eben nicht mehr dem von Philips vorgeschriebenen Yellow Book Standard[177]. Geplant war aber nur, dass Lesegeräte an Computeranlagen am Auslesen[178] der Audio-Informationen zwecks Brennen gehindert werden. Von ihrer Architektur her lesen Audio-CD-Laufwerke nur die sog. erste Session einer CD, wohingegen Computer-Laufwerke alle Sessions einzulesen versuchen[179]. Folgende Abbildung verdeutlicht dies:

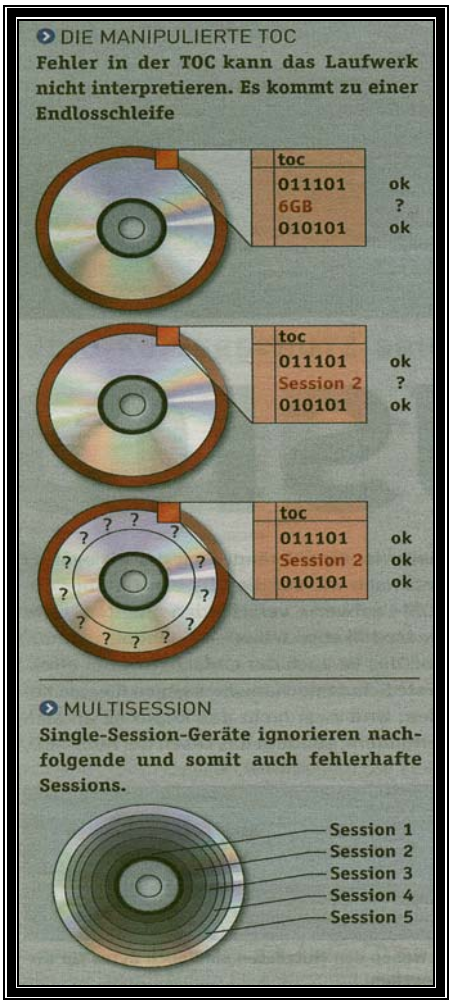

Abbildung 16: Fehler in der TOC einer CD → kein Brennen, da kein Auslesen am PC[180]

[176] Vgl. Kutsal Berk: Copyright Kills Music. Audio-Kopierschutz-Grundlagen. In: PC Magazin, 03 / 2006, S. 28.
[177] Vgl. Tischer, 1998, S. 395.
[178] Vgl. Kutsal Berk: Copyright kills music. Audio-Kopierschutz-Grundlagen. In: PC-Magazin 03 / 2006, S. 28.
[179] Vgl. Halderman John A.: Evaluating New Copy-Prevention Techniques for Audio CDs. In: Feigenbaum, 2003, S. 108 ff.
[180] Aus: PC Magazin, 03 / 2006, S. 28.

Befinden sich in einer nachfolgenden Session somit ungültige Daten, scheitern PC-Laufwerke. Verhalten sich „normale CD-Laufwerke“ dagegen nicht 100% Yellow Book konform (dem erweiterten Audio-CD-Standard), so gibt es auch hier besagte Abspielprobleme – v.a. wenn es sich um MP3-Player handelt, die in Wahrheit Computer-Laufwerke in HiFi-Geräten sind. Es gibt aber auch Ausnahmen, da einige Laufwerke auch kopiergeschütze CDs anstandslos einlesen. Somit wurde durch diese Art des DRM der zahlende Kunde erfolgreich in seinen legal erworbenen Rechten eingeschränkt, während kriminelle Profis mit Spezialprogrammen durch Ausprobieren verschiedenster Leselaufwerke weiterhin kopieren können – eines findet sich nämlich fast immer darunter[181].

2.5.7.2. Online-Musik und Filme

Online erworbene Musik ist durchwegs mittels DRM-Lizenzen und Wasserzeichen geschützt – dabei wird jedoch im Gegensatz zur Gewährleistung bei CDs kein Ersatz geleistet, sollte die Festplatte versagen. Außerdem lässt sich der Content ohne DRM-Umgehung nicht auf anderen PCs nutzen. Diese Umgehung ist neuerdings jedoch nicht gestattet[182]. Wasserzeichen in Musik sollen dabei wie bei sonstigem digitalen Content die Verfolgung in Tauschbörsen erleichtern[183] - v.a. bei MP3-Dateien, da diese es nicht erlauben DRM-Informationen in sie einzubetten[184]. Für Windows XP wird Audio-DRM dabei folgendermaßen realisiert:

> Windows XP Professional verwendet eine DRM-Signatur in den Katalogdateien des Treibers, um ein vertrauenswürdiges Gerät zu identifizieren. Dabei handelt es ich nicht um dieselbe Signatur, die für Windows-Treiber erforderlich ist. WDM-Audioiotreiber und alle damit verknüpften Filterkomponenten müssen DRM-kompatibel sein, um DRM-verschlüsselten Inhalt wiederzugeben, der ein vertrauenswürdiges Audiogerät erfordert[185].

---

[181] Vgl. Masiero Manuel / Schwede Oliver: Hörgenuss mit Hindernissen. In: PC Professionell, 08 / 2003, S. 93 ff.

[182] Vgl. Heidrich Joerg, Himmelreich Gerald: Die Grenzen des Erlaubten. Ratgeber: Privatkopien, Tauschbörsen, Abmahnungen. In: c´t #5, vom 20.02.2005, S. 114. und Metger Christoph: DVDs kopieren. In PC Welt extra, April / Mai / Juni 2004, S. 41

[183] Vgl. Kunterding Kathrin: Tauschrausch im Web. Die MP3-Revolution. In: Tomorrow, April 2003, S. 63.

[184] Vgl. Hentschel Andreas: Musik aus dem Web. In: Chip, 06 / 2006, S. 92.

[185] Zitat: McKay, 2002, S. 388

Ähnlich verhält es sich neuerdings auch mit legalen Film-Downloads. Erste Ansätze hierzu werden bereits in den USA verfolgt[186], ebenso wie E-Books die bereits auch bei Amazon zu beziehen sind[187]. Wesentlich dabei ist die Verschlüsselung durch DRM, wie sie z.B. von T-Online genutzt wird[188]. Folgende Sammelabbildung zeigt die gängigsten DRM-Schutzmechanismen für AV-Content:

CHIP KOMPAKT: DRM-Verfahren

Digitales Rechtemanagement schützt Dateien vor unerlaubtem Abspielen, Kopieren und Brennen. Welche Nutzungsbeschränkungen die Verfahren mit sich bringen, zeigt dieser Überblick.

Quelle	DRM	gleichzeitig Abspielen/PC	Abspielen/mobil	Abspielen/HiFi/Autoradio	Abspielen/DVD-Player	Brennen	geknackt
	Fairplay	5	iPod	als Audio-CD	als Audio-CD	gleiche Playliste 7-mal, sonst beliebig	✓
musicload	per WMA	3	WMA-Player	als Audio-CD	als Audio-CD	3-mal	✓
AOL	per WMA	3	WMA-Player	als Audio-CD	als Audio-CD	3-mal	✓
MTV	per WMA	3	WMA-Player	als Audio-CD	als Audio-CD	3–10-mal	✓
WMV HD	per WMV	1	—	—	—	—	✓
DVD VIDEO	CSS	beliebig oft	mobile DVD-Player	—	als Video-DVD	—	✓
Blu-ray Disc	HD DVD AACS	Spezifikationen noch unklar, Rechtevergabe vom Rechteinhaber abhängig					✗
	Puma/PVP-DPM	DRM für zukünftige Multimedia-Inhalte in Vista, Rechtevergabe vom Rechteinhaber abhängig					✗

Abbildung 17: Gängige DRM-Schutzmechanismen für AV-Content und deren Knackstatus[189]

[186] Vgl. Klumbies Hans: So saugen Sie legal Muisik, Filme und Bücher. In: PC Direkt, 08 / 2002, S. 108.
[187] Vgl. Klumbies Hans: So saugen Sie legal Muisik, Filme und Bücher. In: PC Direkt, 08 / 2002, S. 109.
[188] Vgl. Kunze Andreas: Film-Highlights via Internet. In: Computer Guide, 03 / 2004, S. 37.
[189] Aus: Chip, 05 / 2006, S. 101.

2.5.7.3. Text und Websites

Texte und grafische Elemente auf Webseiten unterliegen ebenfalls Urheberrechten – das Implementieren von fremden Content in eigenen Webseiten ist daher strafbar. Geschützt sind dabei Design (sofern es nicht zahllosen anderen Seiten gleicht), Grafiken (insbesondere fremde Logos) und musikalische Elemente, sowie Bilder von Prominenten die nicht ausdrücklich in Kontext mit zeitgeschichtlichen Ereignissen stehen (z.B. missbräuchliche Verwendung als Werbefoto). Nicht geschützt dagegen sind eigens für Webdesign angebotene Cliparts, zur freien Verwendung überlassene und damit lizenzfreie Fotos, sowie übliche Zitate unter Quellenangabe[190]. Primär finden sich zum Schutz Zungangskontrollen mittels Passwörtern – für das sog. Einloggen ins Internet ist dabei generell ein solcher Schutz vorgesehen. Passwörter lassen sich aber auch mehrfach nutzen, wenn sie z.B. im Internet getauscht werden. Damit ist der Zugang für mehrere Personen zu Content möglich, stellt allerdings nach RA Johannes Richard eine Beihilfe zum Computerbetrug dar. Hier können sich Websites mittels Skripts zur Ermittlung von IP-Adressen[191] behelfen – werden diese gleichzeitig von mehreren Anwendern genutzt, so liegt eindeutig Passwortsharing vor[192] und der Zugang kann gesperrt werden. Letztlich können aber auch bei Texten und Grafiken Wasserzeichen eingesetzt werden. Wie man an dieser Stelle sieht, kristallisieren sich Passwörter und Verschlüsselungsalgorithmen[193] als Dreh- und Angelpunkt des DRM-Schutzes heraus – vielfach werden diese als Restriktionsmethoden angesehen, besonders bei Personen, die ohnehin bereit sind für Content zu bezahlen, sich allerdings nicht in ihren Rechten einschränken lassen wollen. Aus welchen Motiven dies auch immer geschieht: kommerzieller Vertrieb von Raubkopien, (Wieder)herstellung von Rechten bei „Nichtaktivierung“ (Datenschutz) oder Sicherstellung der weiteren Benutzung durch Schonen originaler Datenträger: es gibt

---

[190] Vgl. Schweizer Michael / Vogelsang Andreas: Ist Ihr Content legal? Fallstricke auf der Homepage. In: Chip, 05 / 2003, S. 226 ff.

[191] Hier noch ohne gezielte Verknüpfung von Informationen, wie im datenschutzrechtlichen Teil noch erläutert wird.

[192] Vgl. Arnold Arne / Behrens Daniel / Weidemann Tobias: Exklusiv-Report: Website-Knacker. In: PC Welt, 02 / 2005, S. 63.

[193] Vgl. Auer-Riesdorff, 2003, S. 157.

2.6. Gezielte Angriffsmethoden: Der Krieg gegen DRMS

In o.a. Kapiteln wurden zwar schon einige Schwachstellen von DRMS gezeigt, doch sind diese nichts im Vergleich zu dem, was noch folgt. Vieles basierte ausschließlich auf Sicherheitslücken in der Architektur oder auf menschlichem Versagen (CSS von DVDs, Windows XP-Aktivierung, Filmjuroren mit Vorabversionen, die „aus der Hand gegeben werden"). Hier sollen daher gezielte Angriffsmöglichkeiten dargestellt werden, von denen schon zu Beginn durch Bechtolds Wirkungsgefügeabbildung (v.a. der Schutz durch Technologie) und dem „sich Verlassen auf den Anderen" gewarnt wurde:

2.6.1. Primärziel: Passwörter

Wer über Passwörter verfügt, hat oftmals Zugang zu ganzen Systemen, v.a. wenn es sich dabei um Administrationsrechte handelt. Wie sichere Passwörter aussehen, zeigt Fuhrberg: demnach soll es aus mindestens acht Zeichen bestehen, nicht den eigenen Vornamen oder sonstige Trivialdaten und mehrere Zeichen aus Buchstaben und Zahlenkombinationen enthalten. Natürlich muss es auch geheim gehalten werden und es darf nicht im Klartext gespeichert oder am Bildschirm angezeigt werden[194]. Es empfiehlt sich daher, Passwörter kombiniert aus Ziffern, Buchstaben und Sonderzeichen zu wählen[195]. Die klassischsten Methoden zur Umgehung von Passwörtern sind sog. Brute-Force-Angriffe. Dabei werden alle erdenklichen Zeichenkombinationen ausprobieren, bis man Zugriff erlangt (meist auch durch Wörterbuchlisten, d.h. die sog. Dictionary-Methode → keine sinnvollen Wörter als Passwörter wählen[196]). Vielfach ist aber wegen solcher (menschlicher) Sicherheitslücken ein Angriff gar nicht erforderlich und DRM unwirksam. Das Programm Passwort Decoder XP[197] zeigt z.B. die hinter den Sternen („*") aus Bequemlichkeit gespeicherten Passwörter in Eingabefeldern im Klartext an[198]. Gegen derartiges Fehlverhalten sind dann auch die besten DRMS mit noch so starken Passwortverschlüsselungsalgorithmen machtlos.

Beim echten Brute Force dagegen dauert es je nach Passwortlänge und Anzahl der verwendeten Zeichen unterschiedlich lange, bis die Sperre umgangen ist.

---

[194] Vgl. Fuhrberg, 2001, S. 43 f.
[195] Vgl. Goldmann Stephan (u.a.): So sicher ist Ihr PC wirklich. Hacker-Report 2004. In: Chip, 03 / 2004, S. 60.
[196] Vgl. Baur Thomas / von Keudell Fabian: Passwort-Cracker. In: Chip, 09 / 2003, S. 124.
[197] Das Programm Revelation leistet das Gleiche, ist zudem kostenlos im Internet erhältlich und auch für ältere Systeme tauglich.
[198] Vgl. Weidemann Tobias: PC-Schlüsseldienst. In: PC Welt, 11 / 02, S. 136.

Passwort-Recovery-Tools gibt es dabei für alle möglichen Anwendungen: von ZIP-Dateien über Microsofts Office-Dateiformate bis zu Zugangstools für Betriebssysteme, BIOS-Zugriff, FTP-Sites und Instant-Messanger. Der Einsatz ist legal, sofern man sie nutzt, um Zugang zu eigenen Daten zu erhalten, sollte man versehentlich das Passwort dazu vergessen haben. Im Kern sind DRMS schwach, die lediglich mit 8 Zeichen-Passwörtern und 26 Buchstaben des Alphabets arbeiten (Knackzeit: 24 Tage) – besonders schlimm ist, wenn das System intern nur acht Zeichen akzeptiert, obwohl dies augenscheinlich nicht der Fall ist[199]. Nimmt man nun die 96 standardmäßig druckbaren Zeichen von PCs und eine Passwortlänge von 8 Zeichen, dauerte es mit der Rechenleistung vom Jahr 2002 2287 Jahre, mit 10 Zeichen aber schon 21 Mio. Jahre zum Knacken[200] wie folgende Tabelle zeigt:

Passwortlänge / Zeichensatz (Mittelwert 100.000 Passwörter pro Sekunde)	**26 Zeichen** (ohne Groß- / Kleinschreibung)	**36 Zeichen** (Ziffern und Groß- / Kleinschreibung jedoch berücksichtigt)	**52 Zeichen** (Groß- / Kleinschreibung berücksichtigt)	**96 Zeichen** (alle druckbaren Zeichen)
4	0	0	1 Minute	13 Minuten
5	0	10 Minuten	1 Stunde	22 Stunden
6	50 Minuten	6 Stunden	2,2 Tage	3 Monate
7	22 Stunden	9 Tage	4 Monate	23 Jahre
8	**24 Tage**	10,5 Monate	17 Jahre	**2287 Jahre**
9	21 Monate	32,6 Jahre	881 Jahre	219.000 Jahre
10	45 Jahre	1159 Jahre	45.838 Jahre	**21 Mio. Jahre**

Tabelle 3: Knackgeschwindigkeiten von Passwort-Recovery-Tools Anfang 2002[201]

Ende 2003 sah die Lage schon deutlich anders aus, da sich auch die Passwort-Cracker weiter entwickelten (bessere Algorithmen) [202]:

Passwortlänge	**26 Zeichen**		**128 Zeichen**	
	Kombinationen	**Knackdauer**	**Kombinationen**	**Knackdauer**
4	456976	18 Millisekunden	268.435.456	11 Stunden
8	208.827.064.576	2,3 Stunden	72.057.594.037.927.900	**91 Jahre**
12	95.428.956.661.682.200	121 Jahre	19.342.813.113.834.100.000.000.000	**24,5 Mrd. Jahre**

Tabelle 4: Knackgeschwindigkeiten von Passwort-Recovery-Tools Ende 2003[203]

[199] Vgl. Reischl, 2001, S. 63.
[200] Quelle: Widmann Britta: Die Crack-Methoden. In: PC Professionell, 01 / 2002, S. 146
[201] Quelle: PC Professionell 01 / 2002, S. 146.
[202] Vgl. Baur Thomas / von Keudell Fabian: Passwort-Cracker. Kennwörter auslesen. In: Chip, 09 / 2003, S. 121
[203] Quelle: Chip, 09 / 2003, S. 121

Das Problem des sog. Clusterings ist in den Tabellen aber gänzlich unberücksichtigt, weshalb sich die Knackgeschwindigkeiten relativieren. Es geht nämlich um verteiltes Rechnen mehrerer Systeme, von der jedes nur einen vordefinierten Bereich behandelt. Dies kommt z.B. beim als sicher geltenden PGP oder auch bei neueren Office-Versionen zum Einsatz – als Anbieter des „Services" fungiert dabei Elcomsoft aus Russland[204]. V.a. Videomaterial lässt sich aber auch schneller recodieren - damit ist beweisen, was bei den DVDs gesagt wurde: der Standard bleibt, während die Rechen- und Speicherkapazitäten steigen. Obige Passwörter lassen sich somit auch schneller knacken[205]. Daher bietet nur ein Passwort mit 10-12 Stellen unter Verwendung von allen möglichen Zeichen (noch) ausreichenden Schutz. Bei 24,5 Mrd. Jahren müssten schon 67,2 Mio. Rechner ein ganzes Jahr lang Cluster-Brute-Force Angriffe anstellen. Viele Systeme akzeptieren aber nur acht Stellen, weshalb diese häufige Kombination mit 91 Jahren von Ende 2003 gegenüber den 2287 Jahren Anfang 2002 ein deutlicher Fortschritt war. Passwortschutz ist somit ungeeignet, Content zu schützen. Allenfalls Laien, keineswegs Kriminelle oder Geheimdienste werden davon abgehalten. Verwendet man nämlich für die angeführten 91 Jahre die korrespondierende Anzahl von 91 Rechnern, würde man konsequenterweise nur ein Jahr zum Knacken brauchen, bei knappen 3500 Rechnern dagegen nur 10 Tage (damit ist man auf Universitätsniveau) – Großrechenzentren mit einer noch höheren Anzahl an Computeranlagen und Geheimdienste lachen dagegen über derartige Aufgaben, sollte Clustering dazu eingesetzt werden, Passwörter zu knacken: dies ist vielfach innerhalb von Sekunden, max. einigen Stunden erledigt. Aktuellste Entwicklung sind dabei Rainbow Tables, die es durch mathematische Verfahren noch schneller ermöglichen, die Hash-Werte von Passwörtern relativ schnell zu knacken. Verzögernder Widerstand ist in Windows Systemen kaum möglich, bei Linux mittels zufälliger Erweiterung der Passwörter um Zufallswerte (sog. Salted Passwords) schon[206].

2.6.2. Sekundärziel: Verschlüsselungsalgorithmen

Von Passwortangriffen zu unterscheiden sind die wesentlich wichtigeren aber komplizierteren kryptografischen Verfahren. Dabei geht es um die Schlüsseln (v.a.

[204] Vgl. Bachfeld Daniel: PGP- und Office-Passwörter im Verbund knacken. In: c´t #10, vom 02.05.2006, S. 60.
[205] Vgl. Schraudoplh Markus / Suck Michael: Ihr Heimnetz als Supercomputer. In: Chip, 10 / 2004, S. 44 ff.

Private Keys[207]). Wie bedeutend die Verschlüsselung sein kann, zeigt auch das Wassenaar-Abkommen, in dem die Mitgliedsstaaten keine Beschränkung der Import-Kontrolle und der Verwendung von Kryptografiesoftware vereinbaren. Die USA und die EU-Staaten, also auch Deutschland gehören dazu. Nicht betroffen davon ist jedoch der Export und Meldepflichten für die Verwendung, die den einzelnen Staaten unterliegt[208]. Verschlüsselung von Content ist nämlich sicherer als diesen nur vor dem Zugriff über eine Passwortsperre zu schützen. Immerhin wäre ein 185-Bit-Key mit 2.397.840.682.401.340.000.000 Supercomputern erst in 4,5 Mrd. Jahren geknackt. Folgende Abbildung zeigt dabei die Verdoppelung der Knackzeit pro zusätzlichem Bit in Jahrtausenden:

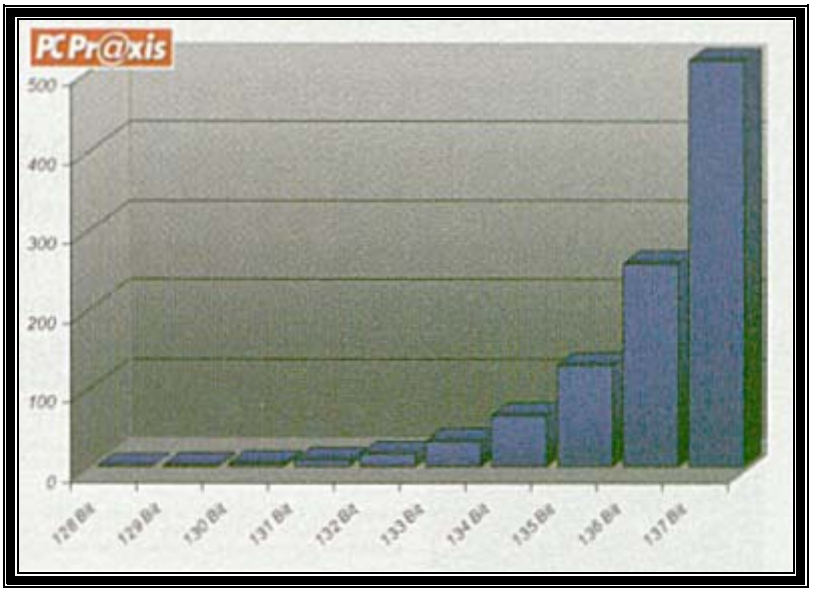

Abbildung 18: Verdoppelte Knackzeit von Algorithmen pro zusätzlichem Bit[209]

Die Schwachstelle von Kryptografie liegt jedoch an anderer Stelle: dem verwendeten Algorithmus. V.a. Geheimdienste könnten Generalschlüssel in Programme einbinden – kriminelle Hacker allerdings auch[210]. Hat man den Algorithmus ermittelt, kann man auch Private Keys wesentlich einfacher errechnen und ohne Brute Force die Entschlüsselung des Contents vornehmen. An die Algorithmen gelangt man wesentlich

---

[206] Vgl. Arnold Arne: Passwort ausgehebelt. In PC Welt, 06 / 2006, S. 54 ff.
[207] Vgl. Marksteiner Peter: Grundbegriffe der Kryptographie. In: Comment, Oktober 2000, S. 20 ff.
[208] Vgl. Backu Frieder: Exportkontrolle bei Kryptographiesoftware. In: Schneider, 2005, S. I / 15 ff.
[209] Aus: PC Praxis 05 / 2005, S. 83.
[210] Vgl. Plura Michael: Geknackt! In: PC Praxis, 05 / 2005, S. 83.

einfacher als gedacht. Es verhält sich hier ähnlich wie bei den Filmjuroren, die Ihre Familien versorgen, nur, dass es sich hier um interne Sicherheitslücken bei den Programmierern von Sicherheitssoftware handelt, wo Firmen Know How im Zuge von Industriespionage weiterverbreitet wird. Wie sonst sollten nämlich Keygeneratoren zum Freischalten von Software mit Zwangsaktivierung schon wenige Tage nach, teilweise sogar noch vor dem eigentlichen Release den Weg ins Internet finden?[211] Software freischalten kann man dagegen auch durch Beobachtung (=Debuggen), was „sich im Speicher des Computers tut" – damit lässt sich der Code ermitteln und modifizieren. Cracks gibt es kurz danach aus dem Internet zu beziehen[212]. Die interessanteste Möglichkeit zum Unwirksammachen jeglichen DRMS ist aber ein:

2.6.3. Vernichtungsschlag gegen DRMS - der Atomangriff

DRMS bestehen wie alles im Universum aus atomaren Strukturen. Dabei sind die Datenträger (CDs und DVDs) wie auch Hardwarekomponenten (Kontrollchips in PCs und Unterhaltungselektronik zur Wiedergabe von Film und Musik) gemeint. Ein Angriff auf diese Strukturen spielt daher die zentralste Rolle bei der DRM-Umgehung. Atomangriff auf DRMS heißt konkret Einsatz von Signalabhörmikrophonen, Rastertunnelelektronenmikroskop, Salpetersäure, Infrarot-Laser und Ionenstrahl[213]. Letztere sind dabei bittere Realität für Contenthersteller und keineswegs Science-Fiction aus Star Trek, denn Sicherheitsexperte Dr. Rüdiger Weis von Cryptolabs Amsterdam ist sicher: „Gegen Angriffe auf atomarer Ebene ist der nur daumennagelgroße Chip wehrlos.[214]" Und tatsächlich gibt es gegen die physikalische schichtweise Zerlegung von Schaltkreisen mittels obiger Methoden kein Gegenmittel, wie man sieht[215]:

---

[211] Vgl. Kaden Jan: Windows-XP-Codes hacktiviert [sic!]. In: PC Magazin, 10 / 2001, S. 42 ff.
[212] Vgl. Hosbach Wolf: Schuldig, Euer Ehren! Rechtslage bei Internet-Angeboten. In: PC Magazin, 09 / 2001, S. 55
[213] Vgl. Flohr Manfred: Die Waffen der Hightech-Hacker. In: Chip, 10 / 2004, S. 122 ff.
[214] Zitat nach: Flohr Manfred: Die Waffen der Hightech-Hacker. In: Chip, 10 / 2004, S. 126.
[215] Hier kämen nur zuverlässige Selbstzerstörungsmechanismen in Betracht, doch müssten diese erst einmal erfunden werden. Gedanken in dieser Richtung gab es mehrfach tatsächlich schon, bei sog. Schokolade-Schallplatten, die man zwar 1x abspielen und danach wirklich nur mehr zum Essen gebrauchen konnte, da die Tonrillen verschlissen waren. Fortgesetzt wurde dies bei CDs, bei denen sich die Datenschicht zersetzte (meist in ein bis zwei Tagen, nachdem man sie aus der luftdichten Verpackungsfolie nahm) – hätte es hier schon CD-Brenner gegeben, hätte 1x auslesen gereicht. Echte Selbstzerstörung von Content gibt es nur durch effektive DRM-Lizenzen, die nach einem Tag ablaufen. Auf Chip-Ebene dagegen gibt es noch keinen effektiven Schutzmechanismus.

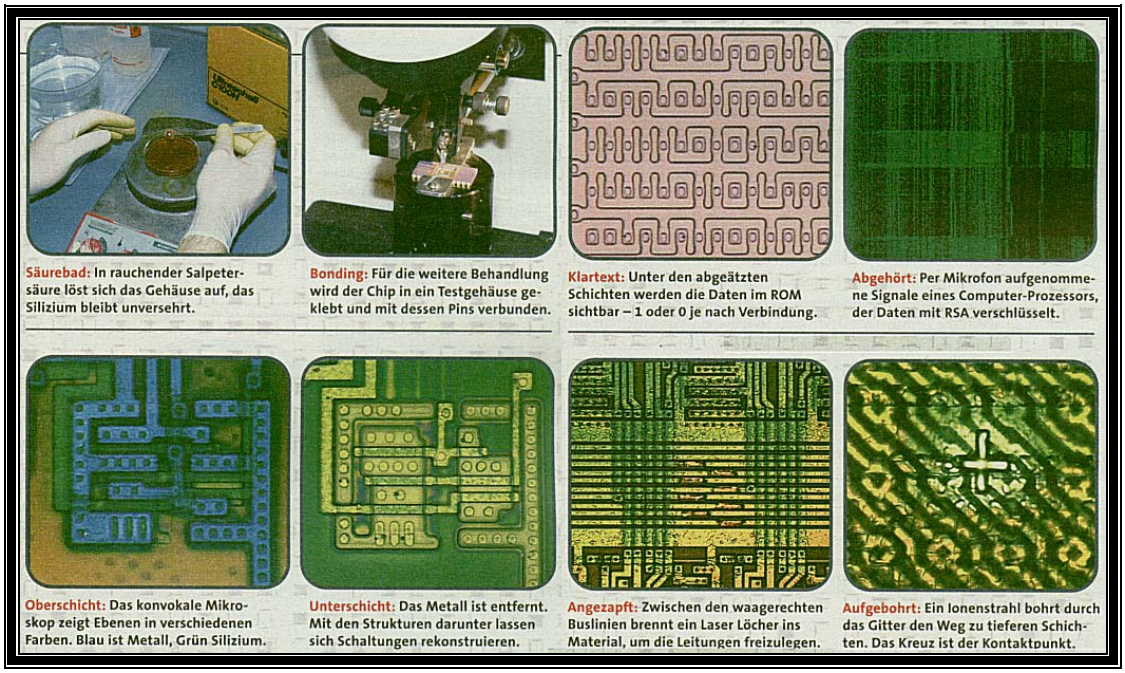

Abbildung 19: Analyse von Schaltungen in Chips durch Angriff auf atomare Strukturen[216]

Die Rede ist hier wieder vom TPM-Chip der Allianz. Als Abwehrversuch gegen Atomanalysen setzen die Hersteller aber auf Dummymaßnahmen, wobei es darum geht, sinnlose Berechnungen im Chip vorzutäuschen und überflüssige Leitungsschichten zu implementieren. Damit erschwert man Atomanalysen, denn verhindern können diese Verzweiflungsakte sie nicht - nur verzögern. Konsequenterweise bekräftigt der Hamburger Informatik-Professor Joachim Posegga: „Die Frage ist nicht, ob ein Hardware-Schutz geknackt werden kann, sondern wie schwierig es ist, ihn zu knacken.[217]“ Und je mehr Schaltkreise im Chip sind, desto länger dauert es natürlich. Damit ist auch klar, dass Heimanwender definitiv nicht mehr an heutige Chips herankommen[218], denn für atomare Strukturanalysen benötigt man Großlaboratorien und teures Equipment. D.h., es kommen nur korrupte Regierungen, terroristische Vereinigungen, bzw. auf Gewinn gerichtete professionelle Raubkopierunternehmen zur Durchführung in Frage. Nebenbei lassen sich dann aber nicht nur Chips, sondern auch Datenträger inkl. aufgebrachter Kopierschutzmechanismen analysieren. Die so ausspionierten Strukturen können dann 1:1 in eigens dafür eingerichteten Presswerken dupliziert werden. Bei Filmen und Musik ist man damit bereits am Ziel. Bei moderner

[216] Aus: Chip, 10 / 2004, S. 125.
[217] Zitat nach: Flohr Manfred: Die Waffen der Hightech-Hacker. In: Chip, 10 / 2004, S. 124.
[218] Vgl. Flohr Manfred: Die Waffen der Hightech-Hacker. In: Chip, 10 / 2004, S. 124.

Software fehlen im Normalfall noch Keygeneratoren und Freischaltcodes des Herstellers, da sich der Code des Freischaltalgorithmus der Scheiben durch exakte Duplizierung im Presswerk ja nicht ändert. Beides kann man durch oben erwähntes Abhören, bzw. Debuggen von Programmen zur Laufzeit ermitteln und so den Algorithmus identifizieren. Debuggen kann man zwar mittels diverser Programmiertechniken verhindern und zu erschweren versuchen, letztlich handelt es sich aber auch hier nur um verzögernde Maßnahmen. So gehört z.B. die Beschlagnahme des gesamten Arbeitsspeichers dazu, um Debugging-Programme nicht laufen zu lassen. Auch das Sperren der Tastatur, um keine Interaktion mehr während der Prüfroutinen für Passwörter zuzulassen und Ausnutzung von Zwischenspeichern (=Stack-Overflow) oder Mechanismen in modernen CPUs zur schnelleren Verarbeitung von Befehlssequenzen – die Prefetchque – fallen in diese Kategorie. Ändert man hier zur Laufzeit bestimmte nahe zusammen liegende Speicherstellen, so wird beim Debugging eine gänzlich andere Anweisung ausgeführt. Bei regulärer Ausführung dagegen wäre die Anweisung (z.B. zum korrekten Decodieren) schon korrekt im Zwischenspeicher der CPU und würde korrekt ausgeführt.[219]

Wenn man nun schon zum Kreis der atomaren Strukturangreifer gehört, dann ist der Weg zur Totalfälschung mit Handbüchern und bedruckten Originalverpackungen, sowie Spezialhologrammen (v.a. bei Software), bzw. Label-Etiketten von Film-DVDs oder Musik-CDs auch nicht mehr weit. Die Erzeuger sind dabei vornehmlich in China, Vietnam oder auf den Philippinen beheimatet und somit für US- und EU-Recht nicht greifbar. Mit den „Produkten“ wird dann der Deutsche und US-Markt mit Totalfälschungen überschwemmt. Folglich wurden im Zuge der Verordnung zur Bekämpfung der Produkt- und Markenpiraterie (in Kraft seit 1. Juli 2004) von der EU die Verfahren zur Vernichtung nachgeahmter und unerlaubt vervielfältigter Waren beschleunigt und erleichtert. Der Zoll erhielt weit reichende Befugnisse, z.B. schon bei der bloßen Vermutung von Rechteverletzungen aktiv zu werden[220].

Als Ergebnis von Atomanalysen lassen sich Geräte auch modifizieren, sich nicht mehr DRM-konform zu verhalten. Und sollte DRM-Code einmal umgangen sein, funktioniert Device-Revocation auch nicht mehr. In welchen konkreten

[219] Hierzu etwa: Bertelsons, 1995, S. 371 ff. und S. 395 ff.
[220] Vgl. Jaschinski Martin: Neue EU-Verordnung zur Produktpiraterie. In: Schneider, 2005, S. I / 213.

Regulierungsbereich Lessigs in diesem Spannungsgefüge die Regulierung durch DRMS fällt, lässt sich nicht eindeutig klären. Bechtold folgend sind ja DRMS geradezu im Schnittfeld zwischen Recht, Technik und Ökonomie zu sehen[221]. Für Lessig dagegen ist das Recht eine Instanz, die auch auf alle anderen Regulierungsebenen stark einwirkt, da es letztlich das Recht ist, das sowohl gesellschaftliche Normen, wie auch den Markt reguliert. Die Architektur, bzw. der Code ist letztlich nur das Ergebnis hiervon – die Frage ist aber, ob hier direkte oder indirekte Eingriffe in den Code nun als Regulierung gesehen werden können, bzw. Atomangriffe eine Art Anti-Regulierung darstellen, da letztlich der Zweck jeder Modifikation eines Teilbereichs Regulierung zum Zwecke hat[222].

2.7. Zwischenbilanz: Reichen die Schutzmechanismen?

Angesichts der angeführten Implementierungsstrategien und deren Schwachstellen, sowie dem 100% Erfolg versprechenden Atomangriffen muss als Zwischenergebnis festgehalten werden, dass DRM-Schutz keinesfalls reicht, Content vor unbefugtem Zugriff zu schützen – allenfalls der Heimanwendungsbereich kann durch DRM reguliert werden, den Profibereich dagegen lassen Schutzmaßnahmen durch DRMS kalt. Gedeckt wird diese Erkenntnis durch Bechtold mit dem Eingeständnis, dass DRMS ausdrücklich auf den Massenmarkt und damit den „normalen Nutzer“ abzielen. Ferner wird eingestanden, dass die Entwicklung von DRMS auch noch nicht abgeschlossen ist, was angesichts der Omnipräsenz in DVD-Playern (tauglich für AV-Content), bei PAY-TV, Windows XP, dem PDF-Dokumentformat und sogar in Videorecordern auch einleuchtet[223]. Fraglich ist aber, warum der Normalnutzer gehindert, die eigentlich Verantwortlichen für unbefugte Vervielfältigung, also Profis, kaum betroffen sind. Erinnert sei nur daran, dass es Unternehmen waren, die die Corporate-Files für Windows XP erhielten und diese auch im Netz verfügbar machten.[224] Setzt man „digitales Gut“ daher mit „Information“ gleich – technisch gesehen ist eine Folge von

[221] Vgl. Bechtold Stefan: Digital Rights Management zwischen Urheber- und Innovationsschutz. In: Zerdick (u.a.), 2004, S. 333.
[222] Vgl. Lessig, 2001, S. 170 ff.
[223] Vgl. Bechtold Stefan: Digital Rights Management zwischen Urheber- und Innovationsschutz. In: Zerdick (u.a.), 2004, S. 335.
[224] Vgl. Apfelböck Hermann / Eggeling Thorsten: Zwangsaktivierung. Aktenzeichen XP ungelöst. In: PC Welt, 03 / 2002, S. 44.

Nullen und Einsen[225] auch nichts anderes, so weist dieses Gut genau die Eigenschaft eines Kollektivgutes auf, d.h. die Nutzung von AV-Content einerorts, hindert nicht dessen Wiedergabe anderenorts[226]. Software, die dabei nicht mittels individualisierten Freischaltschlüsseln in Kombination mit Aktivierung geschützt ist, würde hier auch an vielen Orten gleichzeitig nutzbar sein. Damit wurde mit dem publik werden der Corporate-Files auch Windows XP quasi über Nacht zum Kollektivgut. Rechtlicher Schutz ist folglich zur Sicherheit unumgänglich. Daher gibt es erhebliche:

[225] Vgl. Seith, 2003, S. 49.
[226] Vgl. Clement, 2001, S. 68.

3. Auswirkungen auf Urheberrechte

3.1. Grundsatzprobleme

DRMS erweisen sich bei globaler Durchsetzung von Urheberrechten einfacher als nationale Rechte[227]. So droht der Verlust der staatlichen Autorität, da das Verhältnis zwischen allen Beteiligten Wandlungen unterworfen ist[228]. Hauptargument im Urheberrecht ist Vergütung als Anreiz, Content in Form von Werken der Schrift-, Bild- und Tonkunst zu produzieren. Der Anreiz wäre gering, Werke zu schaffen, die hinterher nicht gekauft werden, nur weil es nicht verhinderbar ist, sie ohne Vergütung zu kopieren[229]. Gestützt wird diese Aussage durch die Schadenssumme infolge unerlaubter Nachahmungen. So verloren US-Firmen 50 Mrd. US$ pro Jahr und in der EU belaufen sich die Verluste aus Piraterie bei Büchern, Software und Unterhaltungsmedien auf 10% des gesamten Export-Volumens[230]. 1993 trat dabei der zivilisationshistorische Wandel ein, da erstmals mehr PCs als PKW verkauft wurden (>100 Mio. Stück)[231]. PCs bedeuten dabei Gefahr für dematerialisierte Güter, deren Krönung in der Auflösung physischer Grenzen besteht. Grund dafür waren globale Möglichkeiten der AV-Wahrnehmung des Contents in Folge der Verbreitung von Kabelnetzen und der Massenproduktion von digitalisierte Werke verkörpernder Datenträger[232]. Weltweit setzte nun die Diskussion darüber ein, wie man adäquaten Rechtsschutz auch für Computerprogramme gewähren konnte, da es sich um erhebliche Wirtschaftsgüter mit hohen Investitionskosten handelt[233]. 1993 war es dann soweit: urheberrechtlicher Schutz wurde für Software anerkannt. Grundsätzlich (als Sprachwerk) schutzfähig angesehen wurden Datenverarbeitungsprogramme in Deutschland schon 1985[234]. Ferner wurde die Begriffswandlung zum „privaten Gebrauch“ von Kopien im Gegensatz zum „persönlichen Gebrauch“ vollzogen[235]. Damit wurde die kommerzielle Unzulässigkeit

[227] Quelle: Interview mit Dr. Forgó vom 17.02.2006.
[228] Vgl. Siegrist Hannes: Geschichte und aktuelle Probleme des geistigen Eigentums (1600-2000). In: Zerdick (u.a.), 2004, S. 331.
[229] Vgl. Lessig, 2001, S. 237.
[230] Vgl. Bayer, 1995, S. 9.
[231] Vgl. Asche, 1998, S. 43 f.
[232] Vgl. Seith, 2003, S. 43 ff.
[233] Vgl. Asche, 1998, S. 73.
[234] Vgl. Asche, 1998, S. 88.
[235] Vgl. von Diemar, 2002, S. 57

von Kopien herausgestrichen. In den USA war man aber für den Schutz von Computerprogrammen etwas schneller. Diese unterlagen dort schon seit 1980 Urheberrechten. Das verwundert auch nicht, da die USA das für den technischen Fortschritt[236] wohl bedeutendste Land ist[237]. Urheberrecht erfüllt aber auch den Zweck des Schutzes vor Verfälschung[238]. Dies ist deswegen wichtig, da man Content einfach kopieren und unter falschen Identifizierungsmerkmalen (Copyrightinformationen) weiter verbreiten kann – für den Nutzer ist dabei nicht ersichtlich, von wem der so erhaltene Content stammt. Historisch betrachtet handelt es sich somit beim Urheberrecht generell um eine Reaktion auf neue Techniken beginnend beim Gutenberg-Buchdruck[239] - bekanntlich um 1440, was massenhafte Herstellung von verkörperten immateriellen Gütern erlaubte und diese in weiterer Folge aus dem raum-zeitlichen Kontext herauslöste[240].

Das Urheberrecht sowohl in den USA als auch in Deutschland in seiner Reaktion auf die technischen Errungenschaften kann somit die in Gesetz gegossene Fassung bereits fester Gegebenheiten zum Schutz digitalen geistigen Eigentums sein (normative Kraft des faktischen DRMS). Dies entspricht damit einem Bottom-up-Ansatz einer Regulierung[241]. Allerdings ist es richtig, dass keine Selbst-, bzw. Ko-Regulierung in diesem sensiblen Bereich des Urheberrechts stattfinden darf, da zur Durchsetzung von finanziellen Interessen die rechtliche Sicherheit benötigt wird – die Eingriffsintensität würde hier sonst zu groß sein[242] - fraglich bleibt aber, warum Eingriffe eines Regulators namens DRM nicht in diese Kategorie fallen. Die Antwort ist der technologische Wandel in Form von Architekturänderung (Code), denn nach Lessig ändert sich der Cyberspace durch den Code und der Cyberspace kann sehr wohl kontrolliert werden[243], indem man seine Architekten (die Autoren des Codes, wie Ethan Katsh es ausdrückte[244]) kontrolliert. Die ausschließlichen Befugnisse

---

[236] Immerhin sitzen dort die Hauptkomponentenhersteller von Computern, Steuerungssoftware und DRM-Chips (AMD, Intel, Apple, Microsoft, IBM, Cisco-Systems, SUN,…).
[237] Vgl. Asche, 1998, S. 94.
[238] Vgl. Siegrist Hannes: Geschichte und aktuelle Probleme des geistigen Eigentums (1600-2000). In: Zerdick (u.a.), 2004, S. 326.
[239] Vgl. Dreier Thomas / Nolte Georg: The German Copyright- Yesterday, Today, Tomorrow. In: Becker, 2003, S. 479.
[240] Vgl. Seith, 2003, S. 43.
[241] Vgl. Latzer, 2002, S. 83.
[242] Vgl. Latzer, 2002, S. 87.
[243] Vgl. Lessig, 2001, S. 115.
[244] Nach Lessig, 2001, S. 164.

(Verwertungsrechte) am Werk verbleiben dabei beim Urheber, sowohl in körperlicher und unkörperlicher Form - auch das Recht des Inverkehrbringens auf Datenträgern. Körperlich heißt dabei, wo und auf welchem Träger es wahrnehmbar gemacht wird, unkörperlich dagegen durch Sendung, Aufführung, bzw. Leitungsübertragung oder Satelliten. Dabei geht es um die potentielle Wahrnehmungsmöglichkeit. Auch das Bearbeitungsrecht ist Teil dieser Befugnisse (Übersetzen, Synchronisieren, Umwandeln und Konvertieren)[245].

3.2. Schutz- und Herkunftslandsprinzipien: welches Recht?

3.2.1. Grundsätzliches

Das Schutzlandprinzip ist territorial begrenzt und bietet nur im Rahmen des Rechtes des jeweiligen Staates Schutz am Content. Sowohl für Urheberrecht, als auch Verwertung und Nutzung sind dabei getrennte Rechtssysteme tangiert, so beide Handlungen nicht im gleichen Land stattfinden. Das Abruflandprinzip dagegen besagt, dass dort wo der Server steht, der Content nach dem Recht des jeweiligen Staates verwertet wird, d.h. aber auch, dass Verwerter Staaten mit geringem Urheberrechtsschutzniveau wählen können, um von dort aus Dritten Nutzungshandlungen gegen Entgelt einzuräumen. Das Ursprungslandprinzip dagegen besagt, dass sämtliche Rechte dem Ursprungsland unterliegen, heißt aber auch, dass der Urheber für jede Nutzungshandlung erst ausfindig gemacht werden müsste und man sich daher nach dortigem ausländischen Recht mit Lizenzbestimmungen vertraut machen müsste[246].

3.2.2. Spezielles zu urheberrechtlichem Schutz an digitalen Werken

Urheberschutz hat stets das Werk zum Ziel. Bei digitalem Content ist dies die digitalisierte Form. Grundsätzlich gilt dabei das Schutzlandprinzip für Content ausländischer Urheberrechteinhaber, der auf deutschem Bundesgebiet bezogen wird[247]. Dies erscheint auch sinnvoll, da so Rechtssicherheit gewahrt bleibt[248]. Fraglich ist aber, ob bei Internet-Angeboten nicht das Herkunftlandprinzip besser wäre. Durch die Verwendung von DRMS ist diese Frage jedoch rhetorisch. Sie lässt sich nämlich mit Nein beantworten – dies in Hinblick darauf, dass Nutzer in einem anderen Staat dann

[245] Vgl. Gutman, 2003, S. 42 ff.
[246] Vgl. Gutman, 2003, S. 118 f.
[247] Vgl. Nordmann-Schiffel Anke: Internet und Internationales Recht. In: Bröcker, 2003, S. 80.
[248] Vgl. Nordmann-Schiffel Anke: Internet und Internationales Recht. In: Bröcker, 2003, S. 85.

das Recht des Herkunftlandes anwenden müssten, was sehr kompliziert und politisch nicht optimal wäre. Außerdem bestünde Gefahr, dass Raubkopien aus sog. Free Havens angeboten werden, d.h. Staaten, die sich wenig bis gar nicht um Urheberrechte scheren[249] - so z.B. Russland wo ein MP3-Anbieter nach dortigem Recht legal offensichtliche illegale Kopien anbietet und sich deutsche Interessenten beim Erwerb strafbar machen[250]. Immerhin gibt es keinen gutgläubigen Erwerb von Nutzungsrechten im Urheberrecht[251]. Beim regulären Abruf rechtmäßiger Werke dagegen aus dem Internet durch einen Nutzer unterwirft sich der Rechteinhaber dessen technischen Gegebenheiten à venire contra factum proprium, d.h. der Nutzer kann sich auf eine konkludente Nutzungsbewilligung stützen. Bei offensichtlich unrechtmäßigem Abruf aus dem Internet (eben von Hackerseiten) dagegen fehlt eine solche - die Unrechtmäßigkeit für den Nutzer muss allerdings eindeutig erkennbar sein[252]. Das reine „illegale Ansurfen“ ist aber nicht strafbar, da erst Anzeigen am Bildschirm, bzw. die Nutzung eine Unterscheidung potentiell ermöglicht[253]. Der Konsum eines Streams von illegalen Inhalten ist dabei legal, da nur der Anbieter strafbar ist[254]. Ein anderes Beispiel ist Umgehungstechnologie für das Kopieren von CDs und DVDs, die aus der Karibik vertrieben wird. So sitzt Slysoft als neuer Rechteinhaber von Clone CD / DVD und AnyDVD in Antigua, nachdem diesem der deutsche Hersteller Elaborate Bytes die Rechte an den Programmen als Reaktion auf das neue Urheberrecht verkauft hatte und in die Schweiz „geflüchtet“ ist. Dies hat der zweifellos meist gehasste Mensch der Unterhaltungsindustrie Oliver Kastl – der Programmierer von Clone CD / DVD - bestätigt[255]. Der Zugriff auf solche im Ausland hergestellten Produkte lässt sich daher nur nach inländischem Recht regulieren, nicht aber die Distribution an sich verhindern, v.a. deshalb, da diese Produkte auch über das Internet bezogen werden können und sich diesbezügliche Verkehrsdaten nicht ohne weiteres speichern lassen, so sie nicht für Verrechnungszwecke gebraucht werden[256]. Weitere Probleme ergeben sich daher durch Anknüpfung an Serverstandorte, sowie, wenn die eigentliche Tathandlung

[249] Vgl. Nordmann-Schiffel Anke: Internet und Internationales Recht. In: Bröcker, 2003, S. 86 f.
[250] Vgl. Hentschel Andreas: Musik aus dem Web. In: Chip, 06 / 2006, S. 93.
[251] Vgl. Auer-Reinsdorff, 2003, S. 60.
[252] Vgl. Gutman, 2003, S. 101 f.
[253] Vgl. Gutman, 2003, S. 107.
[254] Vgl. Gutman, 2003, S. 86.
[255] Vgl. Göhler David: Scharfmacher und Kopiertools. In: PC Magazin, 11 / 2003, S. 17.
[256] Quelle: Interview mit Dr. Forgó vom 17.02.2006.

(Vervielfältigung) an einem anderen Ort (dem sog. Eingriffsort) begangen wird. Nordmann-Schiffel prangert hier folglich Rechtsunsicherheit in diesen Fällen an[257].

3.3. Allgemeine Schutzabkommen zu geistigem Eigentum

Die völkerrechtlich wichtigste Konvention zum Schutz von Urheberrechten ist die Revidierte Berliner Übereinkunft (RBÜ) von 1886. Die USA sind erst mehr als 100 Jahre später: 1989 beigetreten[258] – damit war dann auch der Weg frei für massive Novellierungen durch die TRIPS-Abkommen. Bis dahin und auch heute noch fußen wesentliche Kernbestimmungen in den USA am eigenen Copyright Act von 1976 und in Deutschland auf dem Urheberrechtsgesetz von 1965[259]. Zentrale Bedeutung für DRMS erlangte das TRIPS-Regelwerk v.a. in Hinblick effektive Verfahren zum Schutz geistigen Eigentums zu etablieren[260]. Erweitert wurde darin die Berner Konvention von 1971 um den Schutz von Computerprogrammen und Datenbanken[261]. Ein wohl unbeachteter, aber extrem wichtiger Punkt behandelt den Schutz des Layouts von Schaltkreisen, die ja letztlich die Grundlage moderner Unterhaltungselektronik bilden[262] für mind. 10 Jahre[263] - genau das, was wichtig für rechtliche Verhinderung von Atomangriffen darauf ist. Mit der Umsetzung der WIPO-Verträge wurde im deutschen Recht das „Internet-Recht“ als ausschließliches Recht für die ausübenden Künstler anerkannt – somit bedarf eine Nutzung ihrer Darbietung im Internet deren Zustimmung[264]. Digitaler Content kann und soll dabei durch die WIPO-Verträge mittels DRMS vor unerlaubten Kopien, mitunter aber auch erlaubter Vervielfältigung geschützt werden[265]. Der wesentliche Schutzcharakter von Urheberrechten wird deutlich, wenn man sich die Fristen ansieht, nach deren Ablauf Werke gemeinfrei werden. Diese Frist beträgt für audiovisuelle Werke nach der RL zur Harmonisierung der Schutzdauer des

[257] Vgl. Nordmann-Schiffel Anke: Internet und Internationales Recht. In: Bröcker, 2003, S. 88.
[258] Vgl. Bechtold, 2002, S. 148.
[259] Vgl. Bechtold, 2002, S. 150.
[260] Vgl. Bayer, 1995, S. 17.
[261] Vgl. Bayer, 1995, S. 18.
[262] Vgl. Boehme Martin: Wirtschaftliche Bedeutung internetbasierten Handelns und ausgewählte Beispiele. In: Bröcker, 2003, S. 39.
[263] Vgl. Bayer, 1995, S. 21.
[264] Vgl. Brücker, 2003, S. 617.
[265] Quelle: Interview mit Dr. Forgó vom 17.02.2006.

Urheberrechts der EU von 1993 70 Jahre[266] nach dem Tod der hauptbeteiligten Urheber (Regisseur, Drehbuchautor, Filmmusikkomponist, bzw. Urheber der Dialoge)[267].

Erwähnenswert ist auch die sog. Vergeistigung des Gegenstandsbegriffs, d.h. Werke sind nur dann gemeinsam mit anderen nutzbar, sofern man Kenntnis davon erlangen kann, also die Werke „den Geist verlassen" haben. Hier liegt die Regulierungsfunktion des Staates begründet: dem Urheber Schutz geistiger Schöpfungen einzuräumen, um das in die Nähe zum öffentlichen Gut gerückte Werk vor Marktversagen zu bewahren[268]. Charakteristisch dabei ist, dass hier sowohl ein Markt für Lizenzgebühren zahlende Nutzer geschaffen und gleichzeitig der Zugang für unbefugte Dritte reguliert wird[269]. Die Regulierungsmacht des Staates endet aber dort, wo Schranken zwar erlaubnisfreie Werknutzung vorsehen, DRM dies aber verhindert. Immerhin wäre dabei keinerlei Verständigung oder Vergütung zwischen Urheber und Nutzungswilligen erforderlich[270]. So sind z.B. definitive Schranken für Behinderte vorgesehen, für die Privatkopie dagegen wurde dies von den WIPO-Verträgen explizit für die Mitgliedstaaten offen gelassen – folglich ist diese Schranke nicht durchsetzbar[271]. Durchsetzbar wären Schranken z.B. durch den Key Escrow-Ansatz für Europa[272]. Reichweiten von Schranken sind letztlich aber ohnehin von Transaktionskosten abhängig. Sind diese geringer als die für eine Kopie, kann man sich gleich eine legale Lizenz kaufen[273]. Ferner dienen Schranken aber auch den Urhebern selbst, eben für Kritiken, Zitate oder Ausschnitte, bzw. für Unterrichtszwecke[274]. Letztlich wird ja auch Bekanntheit im Sinne eines „follow the free"-Ansatzes gefördert, bei dem man für gewisse Zeit zwecks schneller Marktdurchsetzung kostenlose Güter

[266] Verschiedentlich merkt man sogar, dass die teilweise hohen Schutzfristen bevor Copyrights auslaufen oder Werke gemeinfrei werden, mit 50-70 Jahren auch vielfach zu kurz waren. So sind bereits einige Rechte an ersten Elvis Presley Tonaufnahmen der 50er-Jahre erloschen, aber auch Mickey Mouse wäre bald schutzlos dagestanden, wenn nicht der sog. Mickey Mouse Extension Act hier zusätzliche 20 Jahre Schutzfrist gewährt hätte. Angesichts dieser ausgeprägten Politik der schützenden Hand auf geistiges Eigentum und offensichtlichem Lobbytum der Hersteller stellt sich die Frage, ob denn hier überhaupt eine Chance besteht, wertvollen, da sehr bekannten Content, jemals gemeinfrei zu stellen.
[267] Vgl. Philippi Theresa: Das Filmwerk und sein urheberrechtlicher Schutz im digitalen Zeitalter. In: Forgó, 2003, S. 341.
[268] Vgl. Seith, 2003, S. 19 f.
[269] Vgl. Seith, 2003, S. 24.
[270] Vgl. Seith, 2003, S. 39.
[271] Quelle: Interview mit Dr. Forgó vom 17.02.2006.
[272] Vgl. Bechtold, 2002, S. 423.
[273] Vgl. Bechtold, 2002, S. 315.
[274] Vgl. Bechtold, 2002, S. 330 ff.

verteilt (z.B. wurde auch der Internet Explorer so unter das Volk gebracht) und um die nötige Publizitätswirkung, bzw. Werbung zu erzielen[275].

3.4. Wann entsteht Werkschutz?

Urheberrechtlichen Schutz können Werke in den USA und Deutschland nur genießen, wenn sie geschaffen sind. Nach deutschem Recht ist dies bereits dann der Fall, sobald es sinnlich wahrnehmbar ist. In den USA dagegen hat es zwingend in verkörperter Form darzuliegen. Dazu genügt es, dieses auf einem Datenträger vorrätig zu halten. Damit wird nach dem Preemption Clause des Copyright Acts bundesstaatliches Recht wirksam und nicht Common Law, das traditionell seit 1790 auf die Erstveröffentlichung abzielte[276]. Dieser Ansatz wäre für digitalen Content auch nicht haltbar gewesen – würde dieser nämlich durch die Fehleranfälligkeit des Zugriffsschutzes von DRMS über Netze gestohlen und erstmals durch Diebe veröffentlicht, so wären diese nach dem Common Law Urheber – hier schütz somit das deutsche Urheberrecht mit einer zentralen Bindung des Urhebers an das Werk besser. Denn der Urheberpersönlichkeitsschutz ist eine entsprechende Ausweitung des grundrechtlichen allgemeinen Persönlichkeitsschutzes[277].

3.5. Lizenzproblematik – wird Content lizenziert oder verkauft?

Frühere meist lebenslängliche Lizenzmodelle (Software, klassische CDs, Zugriff auf Online-Texte) gehören dank DRMS bei digitalem geistigen Eigentum der Vergangenheit an[278] So ging man einfach zum Händler, bezahlte und nutzte den „am Datenträger mitgenommenen“ digitalen Content – wenn man ohne zu bezahlen ging, lag Diebstahl vor – das „Raubgut“ ließ sich aber dennoch ohne Einschränkung nutzen – weder Zugang noch Nutzung wurde reguliert – somit hatte man faktisches Sacheigentum in der Hand. Heute lassen sich zudem sämtliche Contentformen mehrheitlich auf Computern nutzen, d.h. Text, Musik, Video und Software. Man kann hier durchaus von Contentkonvergenz sprechen, denn es liegt nun ein einheitliches Endgeräteformat, nicht aber ein DRM-Standard dafür vor. Dieser ist ständigen Neuerungen, ebenso wie der Einführung neuer Format-Standards für Content in der

[275] Vgl. Clement, 2001, S. 80 f.
[276] Vgl. Asche, 1998, S. 100 f.
[277] Vgl. Fränkl, 2004, S. 67.
[278] Vgl. von Diemar, 2002, S. 149 f.

Computertechnologie unterworfen. Da zur Nutzung von digitalem Content zwingend Kopien (im Arbeitsspeicher oder in Form von Ausgabesignalen an entsprechenden Endgeräteanschlüssen) vorliegen, braucht man dazu aber die Befugnis in Form einer Nutzungslizenz[279]. Problematisch ist nämlich, dass RAM-Speicher Werknutzung ermöglicht, selbst wenn andere Kopien bereits gelöscht sind[280]. Probleme, die sich dabei mit Zwischenspeichern ergeben (Cache, Proxy,...), können aus wirtschaftlichen Gründen nicht als urheberrechtliche Vervielfältigung angesehen werden – denn dann würde das Internet zusammenbrechen[281]. Der Unterschied ist nun, dass bei analogem Content die Verfügungsgewalt mit dem Erhalt des Datenträgers einherging (z.B. Musikkassette). Für digitale Musik aus einer Downloadplattform gilt dies z.B. nicht mehr uneingeschränkt, da Lizenzen mit DRM gekapselt sein können, bzw. zur Nutzung in separaten Lizenzdateien vorhanden sind. Das DRM von digitalem Content wirkt somit über den eigentlichen Kauf weiter, d.h. DRM-geschützter Content lässt sich nicht ohne weiteres weiterveräußern (wie eine Musikkassette) geht es nach den Vorstellungen der Urheber. Hier kann aber dennoch nicht vom Aushöhlen des sog. Erschöpfungsgrundsatzes gesprochen werden, da dieser für körperliche Werkstücke gilt – konkret unterliegt ihm das eigentlich geistige in digitaler Form vorliegende Werk auf welchem Datenträger auch immer nicht[282], da nur das Recht des mit Willen des Urhebers in Verkehr gebrachten einen Datenträgers, aber nicht die sonstigen Rechte des Contents erschöpft sind (wie z.B. Vermiet- und Verleihrechte)[283].

Besitz ist somit lediglich im Sinne der Sachgewaltherrschaft darüber aufzufassen. Mit bloßer Sachgewalt über ein konkretes verkörpertes Werkstück auf einem Datenträger leuchtet aber auch ein, hier keine weitergehenden Rechtsbefugnisse über den eigentlichen Content darauf zu haben[284]. Auch die WIPO-Verträge unterscheiden zwischen körperlicher und unkörperlicher Vervielfältigung – demnach darf zwar ein berechtigter Nutzer auch online bezogenen Content weiterveräußern,

---

[279] Die Schrift eines Buches z.B. kann dagegen sofort rezipiert werden, ohne erst den digitalen Code zu verarbeiten und für Ausgabe tauglich zu machen, d.h. hier gibt es nur eine Kopie, während zur Nutzung von digitalem Content mehrfache Kopien zur Laufzeit vorliegen können (auch in Zwischenspeichern – sog. Cache – von Computern oder auch in den Videochips von Fernsehgeräten, etc...).
[280] Vgl. Gutman, 2003, S. 94.
[281] Vgl. Gutman, 2003, S. 111.
[282] Vgl. von Diemar, 2002, S. 91.
[283] Quelle: Interview mit Dr. Forgó vom 17.02.2006.
[284] Vgl. Hoeren Thomas: Copyright Dilemma: Access Right as a Postmodern Symbol of Copyright Deconstruction? In: Becker, 2003, S. 578 f.

sofern er selbst kein Exemplar mehr zurückbehält[285], leider verhindern aber genau dies viele DRMS, die z.B. auf sog. gekapseltem Content[286] basieren und an das jeweilige Endgerät gekoppelt sind.

Auch bei aktivierungspflichtigem Content ist eine genaue Beschreibung, wann diese Aktivierung erstmals, bzw. neuerlich geschehen muss, anzuraten, um keine allfälligen Sachmängel- / Gewährleistungsansprüche zu begründen[287]. Allerdings ist im Zweifel eine Abwägung der Interessenlage erforderlich, da die Theorie vom Sacheigentum am Datenträger sehr wohl durch absolut wirkendes Urheberrecht beschränkt werden kann[288]. So lässt sich aktivierungserforderlicher Content, wie eben Windows XP, nur für die Nutzung auf einem einzelnen Gerät freischalten. Der Hersteller Microsoft gewährt hier unbegrenzte Aktivierungen, sollte sich die Hardware nicht oder nur geringfügig ändern, sowie viermalige Aktivierung pro Jahr. Bei großen Modifikationen wäre ein Kaufnachweis erforderlich[289]. Und das ist das Problem: wie soll jeder noch so kleine Händler „ums Eck“ der vielleicht selbst bei Großhändlern einkauft und daher nicht Kunde von Microsoft ist, in der Datenbank des Konzerns als legitimer Reseller aufscheinen? Noch problematischer ist, wenn die Software von Privat zu Privat ohne Rechnungslegung weiterveräußert wurde. Die Aktivierung steht dabei sogar im Widerspruch zum bestimmungsgemäßen Gebrauch der Software sog. Multiboot-Systeme zu unterstützen - damit sollte es zulässig sein, mehrere Windows-Kopien auf einem System zu installieren. Nach Ansicht von RA Til Jaeger ist dies durchaus legal[290]. RA Helmut Redeker dagegen geht davon aus, dass dieser Anspruch nicht besteht[291]. Somit ist vieles strittig.

Die Durchsetzung von DRM-Lizenzen generell unterliegt dabei keiner gesetzlichen Kontrolle, lediglich der Kontrolle auf Verkehrsfähigkeit unter kartellrechtlichen Gesichtspunkten[292]. Dabei ist die EU gehalten, zu große Marktmacht

---

[285] Vgl. von Diemar, 2002, S. 94 f.
[286] Vgl. Fränkl, 2004, S. 48
[287] Vgl. Schneider Jochen: Die Beschreibung des Vertragsgegenstandes bei Standardsoftware-Beschaffung. Schutz vor unliebsamen Überrasschungen durch Sperren oder Beschränkungen? In: Schneider, 2005, S. II / 41 ff.
[288] Nach von Diemar, 2002, S. 91 f.
[289] Vgl. Mergard Heiko: Aktivierungsfinale. In: PC Professionell, 11 / 2001, S. 82.
[290] Vgl. Schmidts Rudolf (u.a.): Ein PC – 4x Windows. In: com!, 11 / 2004, S. 27.
[291] Vgl. Perband Andreas: Ihr gutes Recht. In: PC Welt, 05 / 2001, S. 80.
[292] Vgl. Ulmer Detlef: Softwareüberlassung: Formulierung eines Lizenzvertrags. In: Schneider, 2005, S. II / 215

zu regulieren. Denkbar wären Strafzahlungen und Inverkehrbringverbote[293]. Erste Aktionen in dieser Richtung gab es bereits gegen das Bundeling von Zusatzprogrammen mit dem Betriebssystem Windows und damit verbundener Auflagen zur Offenlegung der diesbezüglichen Quellcodes für Mitbewerber. Die aktuelle in Entwicklung befindliche neue Windows Vista Version soll nun ebenfalls Gegenstand einer formellen EU-Untersuchung werden[294]. In den USA (der Microsoft-Heimat) dagegen wurde ein derartiges Kartellverfahren abgeschmettert[295]. Probleme ergeben sich beim Contentbezug ferner bei der Wahl des anwendbaren Rechts (je nachdem in welchem Land dies geschieht, oder wo der Server steht), sowie unbilligen und verbotenen Klauseln in Lizenzverträgen[296]. Festzuhalten bleibt nun, dass Online-Content tatsächlich nur lizenziert, ein körperlicher Datenträger dagegen verkauft wird.

3.6. US-Click-Wrap und Shrinkwrap Lizenzen

Die USA als maßgeblicher Hersteller von DRMS und AV-Content haben hohes Interesse am Schutz dieser Güter. Das US-Urheberrecht ist dabei zweigeteilt in das Contract- und Copyright Law. Die Preemption Doctrine versucht dabei Anwendungsvorrang zwischen Bundes- und einzelstaatlichem Recht zu regeln, sorgte aber für viele Auslegungsprobleme und folglich für mehr Verwirrung denn Ordnung[297]. Außerdem gibt es von Staat zu Staat unterschiedliche Rechte, die sich dann in den dem Content beigefügten Click-Wrap und Shrinkwrap Lizenzen bemerkbar machen, indem sie „dem Recht des Staates XYZ“ unterliegen. Derartige Lizenzen werden in den USA durch das Case Law Systems seit dem sog. ProCD-Fall als wirksam erachtet. Dabei ging es darum, dass dem einzelstaatlichen Contract Law der Nutzungslizenz zu einem Programm infolge der bundesstaatlichen Preemption Doctrine vorerst Unwirksamkeit zugebilligt wurde. Richter Eastbrook dagegen sah zweitinstanzlich eine scharfe Trennung zwischen dem Contract und Copyright Law. Das Contract Law der Nutzungslizenz entfaltete hier sehr wohl Gültigkeit, da Urheberrechte absolute

[293] So hat die EU schon ein kartellrechtliches Verfahren gegen Microsoft geführt mit dem Ergebnis, mehr Freiheit bei der Auswahl von Software durch Dritthersteller zuzulassen (v.a. beim Media Player und Internet Explorer, die in Windows integriert sind).
[294] Vgl. Fischer Jens: Kein Vista in Europa? In: PC Praxis 06 / 2006, S. 25.
[295] Vgl. Fischer Jens: Kartell-Prozess: Microsoft siegt. In: PC Praxis, 01 / 2003, S. 37.
[296] Vgl. Karger Michael: Download im Rahmen bestehender Softwareüberlassungs- und Pfelgeverträge. Probleme mit Click-Wrap-Agreements. In: Schneider, 2005, S. I / 134 ff.
[297] Vgl. Bechtold, 2002, S. 394 ff.

Wirksamkeit gegen jeden, Vertragsrecht dabei speziell zwischen den Beteiligten wirkt (also ergänzende Bestimmung)[298]. Generell ist aber das Verhältnis Copyright und Contract in den USA nicht eindeutig bestimmt, da Gerichtsentscheidungen immer noch Einzelfallentscheidungen sind[299]. Lessig räumt ein, dass Lizenzen weit weniger schlimm, als der eigentliche Code sind. Code lässt sich im Gegensatz zu Verträgen nämlich nicht kraft Willens ignorieren[300]. Will man sich an eine Lizenzbestimmung nicht halten, so konnte man sie in Zeiten vor DRM einfach ignorieren. Den Code zu ignorieren, funktioniert aber nicht. Bemerkenswert dazu sind Pop-Up-Fenster, die Nutzern Lizenzverträge anbieten können, die diese möglicherweise nicht annehmen möchten. Pop-Ups, die einen Nutzer auf einer Website halten wollen, verstoßen dabei zumindest in Deutschland gegen die guten Sitten[301]. In den USA ist die Gültigkeit derartig aufgenötigter Lizenzen lediglich umstritten, hat doch der Nutzer selbst entschieden, die Seite, bzw. den jeweiligen Content nutzen zu wollen. Ähnliche Probleme gibt es für „tear me open"-Verträge, wonach sich Nutzer mit „innenliegenden" Vertragsbedingungen durch Aufreißen der Verpackung einverstanden erklären. Da die Konditionen des Vertrages somit überhaupt nicht eingesehen werden können, ist die Gültigkeit derartiger US-typischer Verträge in Deutschland anzuzweifeln[302]. Die größte Gefahr bleibt auch hier der Code, wenn er an die Stelle des Gesetzes tritt. Lessig wirft hier die Frage auf, bei welcher Instanz dieser denn angefochten werden könnte, wenn er ohne staatlichen Rückhalt geschaffen wurde[303]. Eine eindeutige Antwort darauf bleibt er aber schuldig[304].

3.7. Der Digital Millenium Copyright Act in den USA

Der DMCA von 1998 unterscheidet zwischen Access Control und Usage Control zu geistigen Eigentum. Ob Ex-US-Präsident Clinton vergessen hatte, noch 1997 zu fordern, das Internet nicht zu regulieren und lieber dessen Potential zum Aufbau einer Freihandelszone zu nutzen, als er den DMCA unterzeichnete, ist nicht bekannt[305]. Im

[298] Vgl. Bechtold, 2002, S. 397 ff.
[299] Vgl. Bechtold, 2002, S. 154 ff.
[300] Vgl. Lessig, 2001, S. 242.
[301] Vgl. Laucken Fabian: Sittenwidrigkeit von Pop-up-Fenstern. In: Schneider, 2005, S. I / 146 f.
[302] Vgl. Asche, 1998, S. 87.
[303] Vgl. Lessig, 2001, S. 242.
[304] Beim lokalen Salzamt möglicherweise?
[305] Vgl. Rastl Peter: Illegale Inhalte im Internet. In: Comment, September 1997, S. 32.

DMCA geregelt sind im Kern Verbote von Umgehungstechnologien für technische Schutzmaßnahmen (also DRM). Dies umschließt Herstellung zu kommerziellen Zwecken, sowie Einfuhr, Vertrieb und die Zugänglichmachung für die Öffentlichkeit. Umgehungstechnologie ist dabei nach dem DMCA eine Vorrichtung, mit der sich verschlüsselter Content entschlüsseln oder auf andere Art vermeiden, umgehen, entfernen oder gänzlich ohne Zustimmung des Rechteinhabers deaktivieren lässt. Ferner finden sich genaue Definitionen, was eine technische Schutzmaßnahme nach dem DMCA ist[306]. Dabei handelt es sich um eine effektive Kontrolle über ein Werk, wenn die Maßnahme in ihrem normalen Funktionsablauf erforderlich ist, um den eigentlichen Zugriff auf das Werk durch entsprechende Information, Bearbeitung oder Behandlung erst zu ermöglichen[307]. Unterschieden wird ferner noch zwischen Umgehung des Zugangsschutzes einerseits und der unbefugten Kopie andererseits. Wobei technische Maßnahmen bei ersterem generell nicht umgangen werden dürfen, dürfen zu Zwecken des Fair Use Umgehungstechniken sehr wohl dazu eingesetzt werden, Kopien anzufertigen. Zu Recht wendet Simons hier ein, dass eine derartige Kopie nutzlos wäre, wenn man keinen Zugriff auf den Content nehmen darf, indem die Zugangssperren des DRM nach dem DMCA nicht umgangen werden dürfen[308]. Dies wäre allenfalls dann gegeben, wenn eine technische Schutzmaßnahme zu weit gehen würde, d.h. konkret, dass dem Nutzer hier ein sog. „right to hack“ zusteht, konkret also, dass Umgehungstechnologie durch den Staat in gewissen Grenzen toleriert wird[309].

Genau daher finden sich im US-Code des DMCA §1201 Absatz f bis j verschiedene Ausnahmen. Darunter fallen wichtige Bestimmungen wie Herstellung der Interoperabilität mit Systemen, d.h. sollten Schutzmaßnahmen diese beeinträchtigen oder generell hindern, dürfen sie umgangen werden (Reverse Engineering §1201 Abs. f). Ebenfalls erlaubt ist die Suche nach Schwachstellen in kryptografischen

[306] In Deutschland dagegen wird lediglich in abstrakter Weise von „wirksamen technischen Maßnahmen“ im novellierten Urheberrechtsgesetz gesprochen – genaue Definitionen fehlen, weshalb sich etliche Auslegungsprobleme im Zusammenhang mit Umgehungstechnologien ergeben (so z.B. ob ein Kopierschutz schon „wirksam“ ist, wenn die Autostartfunktion von CDs / DVDs in Windows deaktiviert ist, und daher Schutzprogramme nicht automatisch beim Einlegen starten, oder ob ein „Filzstift“ Umgehungstechnologie darstellt).

[307] Vgl. Simons Barbara: The Copyright Wars – A Computer Scientist’s View of Copyright in the U.S. In: Becker, 2003, S. 388.

[308] Vgl. Simons Barbara: The Copyright Wars – A Computer Scientist’s View of Copyright in the U.S. In: Becker, 2003, S. 384.

[309] Vgl. Bechtold, 2002, S. 411.

Algorithmen, hier die Sicherheit von Systemen zu gewährleisten (Encryption Research §1201 Abs. g). Zum Zwecke des Schutzes Minderjähriger dürfen zusätzliche Schutzmechanismen unter Umgehung vorhandener implementiert werden (Exceptions regarding minors §1201 Abs. h). Auch Umgehung zwecks Wahrung von Persönlichkeitsrechten, wenn unberechtigterweise Daten gesammelt werden, ist erlaubt (Personal Privacy §1201 Abs. i). Letztlich ist zu Zwecken von Sicherheitstests mit Zustimmung des Eigentümers eines attackierten Computersystems die Umgehung von Schutzmechanismen gestattet (Security Testing §1201 Abs. j)[310].

Ein weiterer Punkt behandelt Metadaten als die Parameter von DRM. Der DMCA reagiert darauf mit Vorschriften zum Schutz der Änderung oder Entfernung, sowie zur Bereitstellung falscher Metadaten und untersagt hier sogar vorbereitende Handlungen[311]. Nicht voll umfänglich erfasst vom Umgehungsverbot ist die reine Usage Control – hier greifen Schrankenbestimmungen[312]. Zur Umgehungshandlung nach den Schranken ist aber Know How erforderlich. Durchschnittsnutzer sind damit faktisch überfordert, d.h. konkret, dass auch die US-Schranken zahnlos sind – immerhin müsste Umgehungstechnologie nach dem DMCA § 1201 Abs. i im Normalfall selbst entwickelt werden, d.h. Durchschnittsnutzer können dies i.d.R. nicht[313]. Ferner funktioniert die Electronic Self Help in beide Richtungen, d.h., dass hier auch Lizenzgeber Programmsperren implementieren dürfen, um die Einhaltung der Lizenz sicherzustellen. Strittig ist aber, ob dies auch für Massenmarktlizenzen gilt[314]. Eigentlich vorbereitende Handlungen im Bereich der Nutzungskontrolle sind ja untersagt, d.h. Herstellung und Vertrieb von Umgehungsvorrichtungen[315]. Inwieweit hier Fair Use noch praktikabel ist, ist strittig, denn dieser wurde ja entwickelt, um die monopolartige Urheberstellung zu schwächen, wenn Transaktionskosten bei Aushandlung von Lizenzen höher wären, als das Interesse neue Werke zu entwickeln und öffentliche Diskussion oder Information[316] hier behindert würde[317]. So würden

[310] Vgl. Lejeune Mathias: Protection under US Copyright Law. In: Becker, 2003, S. 369 ff.
[311] Vgl. Bechtold, 2002, S. 239
[312] Vgl. Bechtold, 2002, S. 207 ff.
[313] Vgl. Bechtold, 2002, S. 433.
[314] Vgl. Bechtold, 2002, S. 420 ff.
[315] Vgl. Bechtold, 2002, S. 225.
[316] D.h. also die gesellschaftliche Weiterentwicklung
[317] Vgl. Fränkl, 2004, S. 61.

nach Bechtold auch Bücher nicht mehr kopiert werden, wenn man dafür stets eine Erlaubnis bräuchte[318].

3.8. Die Situation in Deutschland

Ein großer Unterschied nach US- und deutschem Recht besteht in der Wirkung von Click- / Shrinkwrap Verträgen. Zwar gilt in Deutschland auch freies Vertragsrecht und niemand wird gehindert solche Klauseln zu akzeptieren, doch stellt dies AGB dar, die besonderen Vorschriften zur Wirksamkeit unterliegen. Folglich wird die Gültigkeit mehrheitlich bezweifelt[319], ausgenommen sie waren bei Lizenzierung (=dem „Kauf" des Contents) bereits bekannt, bzw. dass ausdrücklich darauf hingewiesen wurde. Im Privatrecht im Supermarkt ist dies faktisch nicht der Fall, im Geschäftsverkehr dagegen haben derartige Bestimmungen mehrheitlich Gültigkeit, allerdings mit erheblichen Einschränkungen im Gegensatz zu den USA. So dürfen Urheber nicht gegen die guten Sitten verstoßen, oder sich unbilliger und völlig überraschender gröblich benachteiligender Klauseln bedienen. Ein Notebook mit Word z.B. darf wegen der Waffenexportgesetze der USA nicht nach Kuba mitgenommen werden, nach deutschem Recht schon, so RA Helmut Redeker[320]. Ferner existieren für Deutschland im Gegensatz zur USA keine speziellen Vorschriften gegen Bereitstellung falscher Metadaten – damit ließen sich Werke bei denen keine angegeben wurden, einfach fälschen – z.B. digitalisieren herkömmlicher und ungeschützter CDs[321]. Damit gibt es auch diesbezüglich eine Hintertür, DRMS auszuhebeln, indem man die Parameter ändert. Das heißt aber noch lange nicht, dass man nicht nach anderen Vorschriften des deutschen Rechts wie Computersabotage (§303b StGB) oder Computerbetrug (§263a StGB) strafbar wäre[322].

3.8.1. Die „Intoleranz der tolerierten neun statt sieben" Privatkopien

Vor Inkrafttreten der Urheberrechtsnovelle in Deutschland konnten nach einer Bundesgerichtshofentscheidung von 1978 fünf bis sieben Privatkopien von Content[323] gefertigt werden. Heute sollen es nach Ansicht der derzeitigen Bundesjustizministerin

[318] Vgl. Bechtold, 2002, S. 314.
[319] Vgl. Bechtold, 2002, S. 160 ff.
[320] Vgl. Perband Andreas: Ihr gutes Recht. In: PC Welt, 05 / 2001, S. 78.
[321] Vgl. Bechtold, 2002, S. 236 f.
[322] Vgl. Tinnefeld, 1998, S. 458.
[323] Ausnahme: Software, da hier lediglich eine einzelne sog. Sicherungskopie gestattet ist.

Zypries bis zu neun Stück sein[324]. Es sind aber zahnlose Forderungen, da weitere Verschärfungen des Urheberrechts geplant sind. Schon jetzt wird nach §93 des deutschen Urheberrechts durch den Begriff der „wirksamen technischen Maßnahmen“ zum urheberrechtlichen Schutz von Werken die Privatkopie erfolgreich verhindert[325]. Da die Privatkopie generell in keinem Gesetz als Recht formuliert wurde, war sie bisher lediglich toleriert, denn „das Recht“ auf Privatkopie gibt es somit nicht, so RA Niclas Vilma. Der Unterschied: nun ist auch die Toleranz weg, denn die Fertigung von digitalen Privatkopien DRM-geschützten Contents ohne straffällig zu werden, ist unmöglich[326]. Auch Dr. Forgó vertritt die Ansicht, dass Privatkopien ohne Zustimmung der Urheber in einem Spannungsverhältnis mit DRMS stehen[327] - so auch Bechtold[328]. Somit ist der Wunsch von Fr. Zypries ein Widerspruch in sich. Wie sonst lässt sich eine Ausweitung der Anzahl zulässiger Privatkopien bei gleichzeitiger Verschärfung des Urheberrechts durch Schutzmaßnahmen (=keine Bagatellklausel[329]) werten?[330] Die Duldung der Privatkopie für Deutschland ist durch die Urheberrechtsnovelle somit zum Verbot geworden. Dem hält die Firma S.A.D. als Hersteller von Movie Jack und Game Jack[331] entgegen, dass dieses Recht sehr wohl Privatpersonen zustehen würde[332]. Allerdings können Urheber das Anfertigen von Privatkopien ihrer Werke untersagen, unabhängig davon, ob dies zu Wohlfahrtsverlust, Unterproduktion oder Unternutzung führen kann[333]. Private Gebrauchsschranken sind, wenn DRM eingesetzt wird, wirkungslos, da dessen Schutzmassnahmen dann nicht mehr umgangen werden dürfen[334].

---

[324] Nach Brüggen-Freye Claudia: Wer knackt, wird verknackt. In Computer Bild, 08 / 2006, S. 6

[325] Vgl. Heidrich Joerg / Himmelreich Gerald: Die Grenzen des Erlaubten. Ratgeber: Privatkopien, Tauschbörsen, Abmahnungen. In: c´t #5, vom 20.02.2005, S. 116.

[326] Vgl. Heidrich Joerg / Himmelreich Gerald: Die Grenzen des Erlaubten. Ratgeber: Privatkopien, Tauschbörsen, Abmahnungen. In: c´t #5, vom 20.02.2005, S. 110.

[327] Quelle: Interview mit Dr. Forgó vom 17.02.2006.

[328] Vgl. Bechtold, 2002, S. 377.

[329] Vgl. Pilzweger Markus: Urheberrecht: Ein bisschen schwanger. In: PC Welt, 05 / 2006, S. 18.

[330] Allenfalls als Witz des Tages oder als Zeichen der Inkompetenz des Gesetzgebers um das Wirken von DRM-Schutzmaßnahmen Bescheid zu wissen.

[331] Dabei handelt es sich um Spezialprogramme für Film-DVDs und Computerspiele zum Erzeugen von Kopien kopiergeschützter Datenträger

[332] Nach Knitter Jörg: Neverending Copy. Neue Tricks und Ansichten zum Thema Kopieren. In: PC Magazin, 07 / 2004, S. 10 ff.

[333] Vgl. Bechtold, 2002, S. 328.

[334] Vgl. Gutman, 2003, S. 149.

3.8.2. US-typische Klauseln und deren (Un)wirksamkeit in Deutschland

In Nutzungsverträge finden sich Beschränkungen bei AV-Content und Software hinsichtlich Weiterveräußerung (auch OEM-Klauseln, d.h. Content nicht getrennt von Hardware zu veräußern), Nutzungsanzahl der eingesetzten CPUs, bzw. Vereinbarungen zur Beschränkung regionaler Nutzung oder Nutzung nur auf best. Endgeräten (v.a. DVDs). Ferner können Verfügungen über das DRMS getroffen werden, besonders dieses nicht zu umgehen und zu dekompilieren, also kein Reverse Engineering durchzuführen[335]. Software wurde ja bis 1970 fast ausschließlich nur zusammen mit Hardware verkauft, da beides durch einen einzigen Hersteller geschaffen wurde[336]. Sowohl in den USA wie Deutschland sind entsprechende Klauseln unwirksam – in den USA wurde dies durch die First Sale Doctrine verankert[337], in Deutschland durch ein Bundesgerichtshofurteil (Aktenzahl: I ZR 244/97) vom Jahr 2000 bestätigt[338]. Bei OEM-Lizenzen, die in der Regel an Hardware gebunden sind, wäre ja Content an die technische Lebensdauer des Rechners, bzw. der Hardware gebunden. Damit wären Investitionen in Content mit einem Verfalldatum behaftet, ebenso wie dies durch die Verwendung von Produktaktivierungstechnologien, die auch auf spezielle Hardware abstellen, herbeigeführt würde[339]. Ausdrücklich nicht betroffen von OEM-Klauseln ist dagegen der erstmalige Vertrieb von gebundeltem Content, bei dem der Distributor mit dem Hersteller entsprechende Vereinbarungen trifft und daher an diese gebunden ist, die Hardware nur in Verbindung mit dem Content zu verkaufen[340]. OEM-Software, die dabei mehrfache Nutzbarkeit auf verschiedenen Computern verhindern soll, ist somit nicht vom Partizipationsinteresse des Urhebers gedeckt. Wichtig ist, dass die Software der Lizenz entsprechend auf einem einzelnen Rechner angewendet wird, auf welchem dagegen ist uninteressant[341]. CPU-Klauseln sind nur in Ausnahmefällen zulässig, etwa bei Softwaremiete für bestimmte Zeiträume oder bei Individualsoftware, die auf

---

[335] Vgl. Bechtold, 2002, S. 154.
[336] Vgl. Asche, 1998, S. 41 f.
[337] Vgl. Fränkl, 2004, S. 61.
[338] Vgl. Bechtold, 2002, S. 392.
[339] Vgl. Grützmacher Malte: Das Recht des Softwarevertriebs. Eine Gegenüberstellung verschiedener Vertriebsformen. In: Schneider, 2005, S. I / 199 ff.
[340] Vgl. Beninca Jürgen / Seffer Adi: OEM-Klauseln unter dem Gesichtspunkt des europäischen Kartellrechts. In: Schneider, 2005, S. II / 210 ff.
[341] Nach. Asche, 1998, S. 122.

bestimmte Hardware angewiesen ist – nicht aber bei Standardsoftware[342]. Unter Standardsoftware versteht man, dass diese für gleiche Anwendungsbereiche für eine Vielzahl an Benutzern, Individualsoftware dagegen erst bei Bedarf im Einzelfall entwickelt wird[343]. Problematisch ist dabei, dass versucht wird, den eigentlichen Nutzungsvertrag über das DRMS erst nachträglich mit dem Urheber abzuschließen, und nur der weniger wichtigere[344] Überlassungsvertrag des Contents mit dem jeweiligen Händler[345]. Nach dem US-Modellgesetz UCITA, das noch nicht in allen Bundesstaaten umgesetzt wurde, steht dem US-Nutzer lediglich ein Rückgabeanspruch zu[346] – somit gibt es keinen Schadenersatz wie in Deutschland, bzw. gänzliche Unwirksamkeit einzelner oder aller Bestimmungen in Click- / Shrinkwrap Verträgen.

Faktisch ist allerdings diese Rechtspraxis auch in Deutschland durch DRMS zahnlos geworden, denn ein wirksamer Schutzmechanismus darf nicht mehr umgangen werden. Somit schützt nicht mehr das Recht, sondern das DRMS. Es kommen allenfalls noch Sachmängelvorschriften des deutschen BGB und eben Schadenersatzpflichten zum Tragen[347]. Ist eine Musik-CD infolge technischer Schutzmaßnahmen auf einem Endgerät nicht abspielbar, liegt ein Sachmangel vor. Kann der Content dagegen nicht wegen DRM-Schutzmechanismen auf die Festplatte kopiert werden (absichtlich defekte Sektoren, ungültige TOC, etc...[348]) liegt kein Sachmangel vor, sofern man über die Auswirkungen und die Präsenz des Schutzes im Vorfeld informiert wurde (=Kennzeichnungspflicht kopiergeschützter Datenträger)[349]. Da künftig aber davon auszugehen ist, dass solche Vorgehensweisen den allgemeinen Verkehrssitten entsprechen werden, wandeln sich folglich urheberrechtliche Nutzungsverträge vielfach zu Verträgen über die Nutzung des DRMS. Wird der Vertrag nicht abgeschlossen, kann der Nutzer erfolgreich an der Contentnutzung gehindert werden. Dies geht sogar so weit, dass das DRM auch noch nach Erlöschen gesetzlicher Schutzfristen für

---

[342] Martens Silke: Softwareüberlassung: Verwendungsbeschränkung in Verträgen. In: Schneider, 2005, S. I / 260. und Dieselhorst Jochen (u.a): Wirksamkeit von CPU-Klauseln. In Schneider, 2005, S. I / 262
[343] Vgl. Asche, 1998, S. 38 f.
[344] Aus Nutzersicht ist dagegen gerade dieser der weitaus wichtiger Vertrag, da er schließlich dafür i.d.R. das Geld hinlegt, ohne im Vorfeld zu wissen, was das DRMS später für Regelungen beinhaltet.
[345] Vgl. Bechtold, 2002, S. 162.
[346] Vgl. Bechtold, 2002, S. 175.
[347] Vgl. Perband Andreas: Ihr gutes Recht. In: PC Welt, 05 / 2001, S. 84.
[348] Vgl. Arnold Arne: Kopierschutz geknackt. Warum jeder Kopierschutz zu umgehen ist. In: PC Welt, 08 / 2001, S. 47.
[349] Vgl. von Diemar, 2002, S. 153.

Urheberrechte weiterwirkt[350]. Strittig ist auch, ob der Freischaltschlüssel für Office XP verwendet werden kann, der keine Zwangsaktivierung nach max. 50 Starts erfordert. Fest steht nur, dass Cracks, also Programme die Veränderungen am Code vornehmen, nicht genutzt werden dürfen[351], denn das sog. patchen ist nur durch originale Patches des Herstellers gedeckt[352], da ansonsten Eingriffe in Urheberrechte vorliegen (Änderung, bzw. Bearbeitung durch Modifikation des Codes)[353]. Aufsplitten von Programmpaketen ist allerdings nach herrschender Lehrmeinung erlaubt, so z.B. aus einem kommerziellen Büropaket die Textverarbeitung und Tabellenkalkulation auf getrennten Rechnern eingesetzt wird[354].

Eine weitere Spezialität des US-Rechts findet dagegen in Deutschland auch keine Anwendung: die Geldrückgabe. Sehen US-Lizenzen im Falle ihrer Ablehnung vor, das Produkt (v.a. Software) an den Händler gegen Kaufpreisrückerstattung zurückzugeben, so liegt in Deutschland im Normalfall gar keine Vertragsbeziehung zwischen Urheber und Käufer vor, d.h. Urheber können in ihren Lizenzen keinen Händlern vorschreiben, hier aus Kulanz eine Wandlung durchzuführen, so RA Helmut Redeker. Auch für Minderjährige ergeben sich ähnliche Probleme, sind sie doch geschäftsunfähig[355], d.h. können sie doch niemals wirksam einen Contentüberlassungsvertrag, geschweige denn eine derartig nachträglich untergeschobene Lizenz eines DRMS annehmen[356] - v.a. wenn dies wie beim Online-Kauf von Content vielfach automatisch ohne Rückfrage geschieht[357]. Es darf sehr daran gezweifelt werden, ob Eltern hier immer und überall für alles haftbar gemacht werden können[358]. Vielfach finden sich auch Bestimmungen in Click-Wrap Verträgen, den

---

[350] Vgl. Bechtold, 2002, S. 259 f.
[351] Vgl. Perband Andreas: Registrieren unnötig. In: PC Welt, 09 / 2001, S. 57.
[352] Die Corporate-Files von Windows XP stammen ja von Microsoft selbst und wie im Implementierungsteil gezeigt wurde, lassen sich diese ja dazu nutzen, Windows XP um das Aktivierungserfordernis zu erleichtern.
[353] Vgl. Himmelsbach Gero / Pursche Olaf: User am Rande der Legalität. In: PC Professionell, 02 / 2003, S. 73.
[354] Vgl. Himmelsbach Gero / Pursche Olaf: User am Rande der Legalität. In: PC Professionell, 02 / 2003, S. 74.
[355] Nach Perband Andreas: Ihr gutes Recht. In: PC Welt, 05 / 2001, S. 79.
[356] So wären alle Minderjährigen, die aktivierungspflichtigem Content nutzen wollen, gar nicht dazu befugt.
[357] Vgl. Reuscher, 2002, S. 361.
[358] Bemerkenswert ist auch, dass Käufer hier von Fall zu Fall selbst entscheiden müssten, wann denn welche Lizenzbestimmung unwirksam und daher gefahrlos ignoriert, bzw. wann das Risiko eingegangen wird, sich im Falle des Irrtums darüber strafbar zu machen. Contentkauf im digitalen Zeitalter wird somit mehr und mehr zur riskanten Sache, mit dem Gesetz in Konflikt zu geraten.

Content nicht kommerziell zu nutzen - etwas was bei Unternehmen auch keinen Sinn hat. Ferner finden sich weitgehende Haftungsausschlüsse und die Übertragung der Gefahr von allfälligen Störungen eines Downloads auf den Kunden. Abgerundet wird dies durch Exportkontrollbestimmungen, mit denen Durchschnittsanwender überfordert sind. In Deutschland wurde daher mit Recht die Gültigkeit derartige Bestimmungen in Verträgen in Zweifel gezogen[359].

3.9. Metadaten und Metadatenschutz

Gewährleistet kann DRM-Schutz nur durch Metadaten werden, d.h. das DRMS muss diese interpretieren können und am Stand der Technik bleiben. Möglich wird dies durch Technologie-Lizenzverträge zwischen Contentherstellern und DRMS-Herstellern, wie in der Wirkungsgefügegrafik Bechtolds zu Beginn dargestellt wurde. Vorgeschrieben ist darin, welche anderen DRM-Maßnahmen beachtet und mit welchen diese gekoppelt werden können, bzw. müssen. Betroffen von solchen Verträgen sind primär Endgerätehersteller - faktisch ist der Abschluss jedoch erzwungen, da ansonsten kein Content wiedergegeben werden kann und das Gerät nicht unterstützt werden würde (Device Revocation, bzw. keine Vergabe von Entschlüsselungscodes / -algorithmen)[360]. Die Metadaten definieren dabei, wie DRM wirken soll, welcher Content wann und wie geschützt wird, bzw. wie oft und von wem was wohin kopiert werden darf, bzw. welche Endgeräte befugt sind, den Content zu nutzen. Kurzum: Metadaten steuern das DRM und Inhalte, Rechte und Nutzungsmöglichkeiten müssen dabei immer und dauerhaft identifizierbar bleiben[361]. Damit wird auch klar, dass sich Angriffe zur Umgehung des DRM-Schutzes nicht unbedingt gegen das DRMS richten müssen, sondern es ausreicht, die weitaus ungeschützteren Parameter anzugreifen. Bedeutsam ist diese Parameterisierung v.a. bei Software. Werden dabei Einstellungen vorgenommen, stellen diese keinerlei urheberrechtliche Handlung dar[362]. Auch die RC-Sperre bei DVD-Playern fällt unter diesen Begriff. Hier wird ja auch nicht das DRM selbst attackiert. Aus technischer Sicht wird lediglich die Einstellung des Endgerätes geändert

[359] Vgl. Karger Michael: Fallstricke in Clickwrap-Agreements. Software-Download im Unternehmen. In: Schneider, 2005, S. II / 110 ff.
[360] Vgl. Bechtold, 2002, S. 262.
[361] Vgl. Bechtold, 2002, S. 231.
[362] Vgl. Bauer Ines M., Bischof Elke: Nutzungsrechtsklauseln. Die Einräumung von Nutzungsrechten an Computerprogrammen. In: Schneider, 2005, S. I / 258.

(normalerweise auf RC 0, also für alle Regionen) – ähnliches gilt für Aufhebung von SIM-Locks bei Handys. Dies stellt dabei zwar eine Markenverletzung dar, nicht aber in jedem Fall einen Eingriff in Urheberrechte, da die Marke des Netzbetreibers geschädigt wird, nicht aber der Hersteller der Handysoftware[363]. Ähnlich argumentieren könnte man beim echten Freischalten von zusätzlichen Funktionen in ordnungsgemäß lizenzierter Software mittels undokumentierter Einstellungsmöglichkeiten. Dem:

3.10. Tuning

Mittels Tuning kann man vielfach Inhalte nutzen, für die man kein Entgelt zahlt. Beim Tunen von Software mit Spezialprogrammen, um versteckte Funktionen freizuschalten ist strittig, was erlaubt und verboten ist. So tobte über Monate hinweg ein Streit zwischen Microsoft und dem Fachmagazin PC Welt. Kernpunkt war der vermeintliche Verrat von Geschäftsgeheimnissen durch das Fachmagazin, indem hochbrisante Tipps geliefert wurden, wie man ohne zusätzliche Software-Produkte des Herstellers vergleichbare Leistung durch Eingriffe in die Einstellungsmöglichkeiten erreichen kann[364]. Noch heute lassen sich durch Tricks viele Funktionen aus Windows XP Professional in der günstigeren Home-Version freischalten[365]. Sicher ist lediglich, dass man durch Installationsschlüsseln keine Funktionen freischalten darf[366], die man nicht erworben, also lizenziert hat[367]. Ob Tuning-Maßnahmen nach der eigentlichen Installation davon betroffen sind, ist noch nicht ausjudiziert.

3.11. DRMS-Probleme in der Verwertung

3.11.1. Viele Urheber = viele Lizenzen = viele Probleme

Mit der Digitaltechnik entstanden neue Miturheber an Werken, wie Sampler, Programmierer (z.B. von DVD-Menüs) oder Designer der Bild- u. Toneffekte[368] – auch

---

[363] Vgl. Elteste Thomas: Entfernen der SIM-Lock-Sperre als Markenverletzung. In: Schneider, 2005, S. I / 27 f.

[364] Hier verhält es sich in etwa so, wie wenn man einem KFZ durch Modifikationen in der Fahrzeugelektronik zu einer höherer PS-Leistung verhilft. Wobei bei Kraftfahrzeugen versicherungstechnische und steuerrechtliche Gesetze im Wege stehen, sind aus urheberrechtlicher Sicht Tuningmaßnahmen bei Software dagegen unbedenklich - es handelt sich nämlich um Parameterisierung.

[365] Vgl. Reuscher, 2002, S. 21 ff.

[366] Bei Office XP wird durch Eingabe eines speziellen Installationsschlüssels z.B. die Aktivierungspflicht ausser Kraft gesetzt – darum ist es strittig, ob dies gestattet ist, oder nicht. Es wird ja keine zusätzliche Funktion „freigeschaltet“, sondern im Gegenteil, noch etwas weggeschaltet.

[367] Vgl. Arne Arnold: Alles wissen. In: PC Welt, 01 / 2002, S. 114.

[368] Vgl. Plate, 2003, S. 234.

diese Personen steht Vergütung zu. Damit verwandt ist auch das Synchronisationsrecht in dem Sinne, ein Werk multimedial mit anderen zu verbinden[369] (z.B. Sammelausgaben von DVDs auf Computer-Fachheften oder Literatur-CDs / DVDs, Lexika). Daher steigt die Nachfrage nach geschütztem Content wegen neuer digitaler Verwertungs- und Kommerzialisierungschancen[370]. So verwundern die Definitionsversuchen zu Beginn dieser Abhandlung auch nicht, schwingt doch der kommerzielle Aspekt als primäre Existenzberechtigung für die Implementierung von DRMS geradezu mit. Eine Verleugnung des Zusammenhangs zwischen E-Commerce und DRMS ist daher unangebracht, denn Content, der keine Vergütung zum Ziel hat, braucht i.d.R. auch keinen Schutz durch DRM. DRM setzt somit auf den Schnittstellen des E-Commerce auf und bedient sich dieser Strukturen[371].

Das Problem ist aber, dass Content nur dann lizenzierbar ist, wenn man die Zustimmungsrechte aller Urheber eingeholt hat. Wenn nun Hunderte von Einzelrechten eingeholt werden müssten, würden sich mit individuellen Nutzungsverträgen Schwierigkeiten ergeben. Die digitale Werkform war ja bei alten Verwertungslizenzen vielfach noch nicht bekannt, d.h. es war wirtschaftlich besser, das Risiko einzugehen, einzelne Rechte zu verletzen, als ewig nach allen Urhebern und Miturhebern zu suchen – Lizenzabgaben in der Verwertung wurden daher nur gezahlt, wenn sich die Urheber selber meldeten[372]. Deshalb ergeben sich Schwierigkeiten bei unauffindbaren Miteigentümern des Contents. Der Grund: digitale Werke werden kaum durch Einzelpersonen, sondern durch Teamwork geschaffen. Filme und Software fallen mehrheitlich darunter. Musik kann zwar darunter fallen, ist aber im Normalfall auch nicht immer ein Solostück - lediglich bei Texten kann man vielfach nur einen einzigen Urheber als Autor betrachten.

Zwecks Wahrung von Rechtssicherheit gab es damit nur die Möglichkeit, Urheberrechte teilweise aufzuheben, was aber internationalen Vereinbarungen widersprochen hätte, oder in Anlehnung an US-Recht ein fiktives Urheberrecht für

---

[369] Vgl. Plate, 2003, S. 237.
[370] Vgl. Plate, 2003, S. 244.
[371] Allenfalls wären DRMS im entferntesten Sinne denkbar, die Content ausschließlich regional überwachen und dafür sorgen, dass z.B. Waffenexportgesetze der USA eingehalten werden, oder jugendgefährdende Inhalte erst per DRM ab 21 oder 18 Jahren freigeschaltet werden können. Diese Art von DRM findet sich aber in den in dieser Abhandlung verwendeten Definitionen nicht, weshalb diese Möglichkeiten auch unberücksichtigt bleiben. Verstecktes Machtpotential steckt dennoch dahinter.
[372] Vgl. Plate, 2003, S. 247 f.

Auftragswerke eines Arbeitgebers an diesem anzunehmen. Da das deutsche Urheberrecht jedoch den starken Charakter des Schöpfers betont (allenfalls Abspaltung einzelner Nutzungsrechte kommt in Frage[373]) und weniger auf Wirtschaftsinteressen wie das US-Recht abzielt, war dies jedoch nicht durchführbar[374]. Die Abspaltung von Einzelrechten und nicht eine gänzliche Urheberrechtsübertragung resultiert aus der vernachlässigten (physischen) Bindung des Urhebers an sein Werk, wie in der Theorie vom geistigen Eigentum schlechthin. Von Gierke griff diese Lehre auf und stellte die individuelle Leistung in den Mittelpunkt – aus dieser Erkenntnis resultierte dann die deutsche Unübertragbarkeit des Urheberrechts[375]. Die Ablösung des Privilegiensystems, wonach Urheber nur die Rechte an ihrer geistigen Schöpfung hätten, die ihnen gesetzlich zugebilligt wurden, wurde durch das „Droit d´auteur“ in Deutschland vollständig verdrängt. Dadurch wurde die zentrale Bindung des Urhebers an das Werk mit allen ausschließlichen Rechten verknüpft[376] Dieser Auffassung folgt auch Fränkl, da die Bindung an das Werk schon fast so stark wie an einer Sache im materiellen Sinne zu verstehen ist[377]. Genau dieser Ansatz ist für digitalen Content aber nicht haltbar, da er niemals körperlich, sondern nur in verkörperter Form vorliegen kann (auf Datenträgern) - hieraus resultiert auch der Vervielfältigungsbegriff[378]. Urheber haben dabei wenig Interesse, Persönlichkeitsrechte im Sinne des „Droit d´auteur“ durchzusetzen – die kommerzielle Verwertung würde darunter leiden. So ist die eigentliche persönliche Bindung zum Werk eines Teams wesentlich lockerer[379], die Verwertung aber wesentlich komplizierter wahrzunehmen, sollten sich Streitigkeiten untereinander ergeben. Somit ist das deutsche Urheberrecht weniger gut auf die ökonomischen Herausforderungen des Informationszeitalters vorbereitet, denn das US-Recht – man kann durchaus an dieser Stelle davon sprechen, dass man sich in Deutschland und Europa generell für „das falsche Urheberrechtsmodell“ entschieden hat, nämlich einem pauschalen Verwertungsabgabensystem, denn:

[373] Vgl. Bechtold, 2002, S. 167 f.
[374] Vgl. Plate, 2003, S. 250 f.
[375] Vgl. Drewes, 2002, S. 25.
[376] Vgl. Berking, 2002, S. 20 f.
[377] Nach Fränkl, 2004, S. 66.
[378] Vgl. von Diemar, 2002, S. 19 f.
[379] Vgl. Berking, 2002, S. 46.

> Schließlich stellt die mittelbare Erfassung aufgrund der damit zwangsläufig zusammenhängenden pauschalisierenden Vergütungsweise gegenüber der unmittelbaren Erfassung der Nutzungsvorgänge, die eine individuelle Vergütung gewährleisten kann, immer nur die zweitbeste Lösung dar[380].

An dieser Stelle treten DRMS in Aktion und beheben genau diesen Mangel im deutschen Urheberrecht, da die Rechteinhaber nun selbst entscheiden, wann und wem welche Lizenz erteilt wird. Das US-Recht dagegen war schon von Grund auf stets auf diese Wirtschaftlichkeit ausgerichtet, was genau dem Leitgedanken des DRM entgegenkommt: der kommerziellen Verwertung. Die USA zählen im Gegensatz zu den Droit d´auteur-Ländern wie Deutschland eben zu den Copyright-Ländern – und genau das ist ja, wie bereits erläutert, Sinn und Zweck von DRM: die Vervielfältigungshandlungen zu steuern[381]. Zwischengeschaltete Verwertungssysteme- und -gesellschaften stören hier nur.

Asche weist ausdrücklich auf das Konsumentenwohl infolge der totalen Ausrichtung des Urheberrechts in den USA als Vermögensrecht hin. Jeder kann am Profit der Gesellschaft teilhaben – moralische Rechte, wie die Bindung des Autors an das Werk sind dem US-Recht dagegen fremd. Allerdings können ausschließlich Vervielfältigungen verhindert werden[382], was jedoch nur dann im Interesse des Urhebers ist, wenn es ohne Vergütung geschieht. Darin liegt auch bereits der fundamentalste kommerzielle Unterschied zwischen den beiden Urheberrechtssystemen. Die Anreizfunktionen sind somit stärker ausgeprägt Content zu entwickeln, als in Deutschland. Dort ist es nämlich staatlicherseits nicht ausschließliches Ziel Profit erlangen zu lassen wie im US-Recht und somit „nur“ Marktversagen zu korrigieren[383], sondern eben auch die Kulturförderung[384]. So wäre z.B. die GEMA in Deutschland bei reinem Online-Vertrieb[385] überflüssig[386].

---

[380] Zitat: von Diemar, 2002, S. 49.
[381] Vgl. Fränkl, 2004, S. 31.
[382] Vgl. Asche, 1998, S. 99.
[383] Vgl. Dreier Thomas / Nolte Georg: The German Copyright- Yesterday, Today, Tomorrow. In: Becker, 2003, S. 489.
[384] Vgl. Berking, 2002, S. 44 f.
[385] Sicherlich wäre noch zu untersuchen, ob denn der Enderlös für die Künstler hier insgesamt höher ausfallen würde, als bei den beiden Modellen, die im ersten Kapitel gezeigt wurden. So blieben dort beim 15 €-Album 1,05 € für den Künstler, beim 1,49 €-Download / Titel. 14 Cent, was sich aber schon ab dem 11. Titel eines Albums positiv bemerkbar machen würde. Beim 50-Cent-Download muss berücksichtigt werden, dass dabei die Nachfrage steigen würde, was angesichts der nur 10 Cent noch höhere Erlöse für den Künstler erwarten ließe. Den genauen Gewinnmaximierungsmodellen soll an dieser Stelle jedoch nicht weiter nachgegangen werden, da die Preisgestaltung von Content kein Problem des DRM mehr ist.

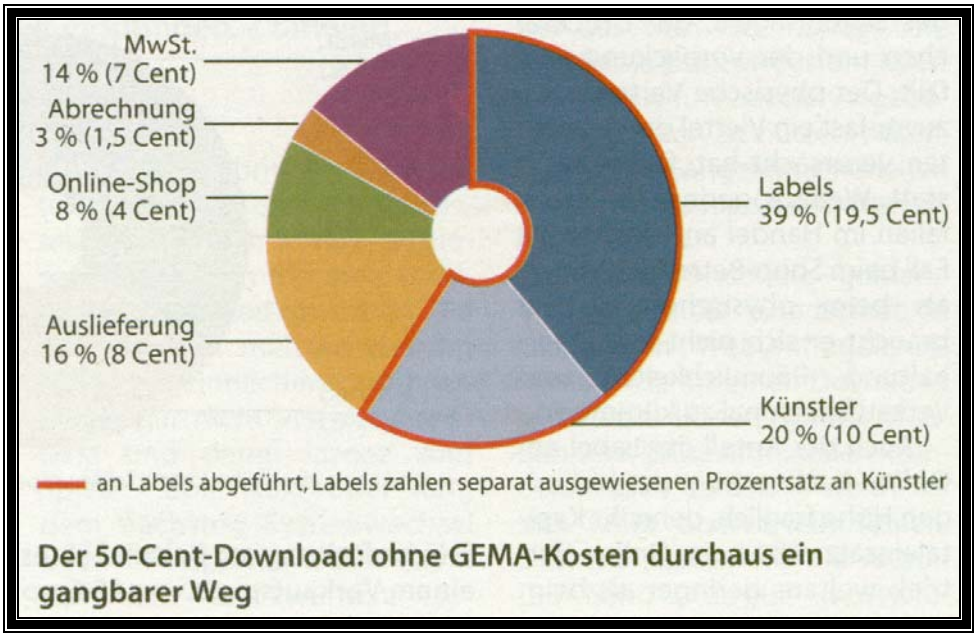

Abbildung 20: Bekämen Künstler/innen mehr, wenn die GEMA nicht wär´[387]?

Für US-Content verwundert es aber nicht, dass DRM-Lizenzen präzise Regelungen betreffend Copyrights beinhalten. Für Deutschland verwundert es dagegen nicht, dass der Tradition folgend ein massives Ausgestalten von Verwertungsrechten und -gesellschaften eingesetzt hat. Dieses Modell ist dabei in Europa generell[388] verbreitet[389]. Davon zeugt schon die Anzahl der Gesellschaften: in den USA gibt es nur wenige Clearing Stellen, bei denen Rechte angefragt werden können, sowie „das" Copyright Clearing Center, das kollektive Rechte für Texte und literarische Werke wahrnimmt, neuerdings auch für Textpublikationen im Internet. Daneben gibt es zwei große Musikorganisationen (ASCAP und BMI), sowie zwei für Film (MPA und MPAA) mit kleineren Untergruppen. Letztlich gibt es eine Vielzahl von kommerziellen Musik- und Filmstudios, die allerdings die Verwertung selbst übernehmen und nicht verwerten lassen[390]. In Deutschland dagegen sind es von Grund auf schon elf verschiedene kollektive Verwertungsgesellschaften. Probleme ergeben sich schon

[386] Vgl. Hansen Sven: Fair, fairer, fünfzig. Der richtige Preis für den legalen Musik-Download. In: c´t #12, vom 01.06.2004, S. 98.
[387] Aus: c´t #12, vom 01.06.2004, S. 98.
[388] Ausgenommen Großbritannien
[389] Vgl. Lejeune Mathias: Protection under US Copyright Law. In: Becker, 2003, S. 380.
[390] Vgl. Rosenblatt, 2002, S. 7 ff.

deshalb, da es nicht immer eindeutig ist, wem welcher Content zugeschrieben wird. Wichtige Funktionen bekleiden dabei die GEMA, die VG Wort und die VG Bild-Kunst.

Bemerkenswert ist, dass dabei alle wahrgenommenen Verwertungsrechte durch Private ausgeübt werden, was einen vollständigen Rückzug des Staates aus diesem Bereich bedeutet[391]. Der Vorteil eines Verwertungssystem ist jedoch, hier zentral die Funktion der Vergütung für die Werknutzung zu übernehmen, ohne dass Nutzer mit allen Beteiligten am Schöpfungsprozess individuelle Nutzungsverträge abschließen müssen – somit erspart man sich Suchkosten bei deren Ausfindigmachung[392]. „Genutzt" wird dabei genau so viel, wie man für die Verwertung braucht – nicht mehr und nicht weniger. Hier liegt die Zweckübertragungstheorie Goldbaums zu Grunde, d.h. genau so viel Recht zu erwerben, wie zur Erfüllung der Zwecke gebraucht wird[393]. Und solche Zwecke sind jedenfalls dann gegeben, wenn neue Nutzungsarten vorliegen. Klarerweise verändern sich mittels DRM die Wertschöpfungsketten des digitalen Contents. So werden Urheber in hohem Maße von Vertriebspartnern unabhängig, können sie doch nun auf eigenen Websites den Content direkt vermarkten ganz ohne Verträge z.B. mit Musiklabels[394].

3.11.2. Die Vergütungspauschale für Geräte und Leerdatenträger

Historisch reagierte Deutschland erstmals 1985 mit einer Vergütungspauschale für die Betreiber von Kopiergeräten durch die massenhaft einsetzende Kopienerstellung von Büchern und Zeitschriften.[395] Damit soll die Vergütung Schrankenregelungen (wis. Arbeiten, Kritiken, Zitate, privater Gebrauch, Kirchen, Schul- und Unterrichtszwecke) beim Erstellen von einzelnen Kopien eines Werkes abfedern. Eingehoben wird dabei die Leerkassettenabgabe, bzw. Geräteabgaben[396]. Folgende Tabelle zeigt die Vergütungstarife mit Stand 2003:

[391] Vgl. Günnewig. Dirk: New Copyright for the Digital Age: Political Conflicts in Germany. In: Becker, 2003, S. 535.
[392] Vgl. Plate, 2003, S. 252.
[393] Nach Drewes, 2002, S. 26.
[394] Vgl. Hofer, 2000, S. 142.
[395] Vgl. Bechtold, 2002, S. 253
[396] Vgl. Gutman, 2003, S. 51.

Artikel	Pauschale Abgabe (ohne Mwst.)
PC	voraussichtlich bis zu 12 € pro Gerät
Drucker	Voraussichtlich 10,- bis 300,- € je nach Leistung
CD-Brenner	7,50 € pro Gerät
DVD-Brenner & CD-/DVD-Combobrenner	9,21 € pro Gerät
Videorecorder	9,21 € pro Gerät
Kassettenrecorder	1,28 € pro Gerät
Kopierer, Faxgerät, Scanner	8,18 bis 306,78 € je nach Leistung
Leerkassette, Tonbänder, DATs, MiniDisc	0,0614 € pro Stunde Spieldauer
CD-R/RW	0,072 € pro angefangene Stunde Spieldauer
Videokassette, DVD	0,087 € pro Stunde Spieldauer

Tabelle 5: Abgaben auf diverse Geräte und Datenträger 2003[397]

Neuerdings (2005) sind für Leer-DVDs schon 17,40 Cent pro Spielstunde[398] fällig[399]. Auch für Komplett-PCs gibt es schon konkrete Pläne für die 12 €-Abgabe[400]. Strittig ist, auf welche Gerätekomponenten und ob Generalabgaben auf ganze PCs zulässig sind – damit wäre Doppel-, bzw. Dreifachvergütung für Content gegeben (PC als Ganzes und Einzelkomponenten wie CD- / DVD-Brenner, sowie Festplatten und Rohlinge). Die deutsche Rechtsprechung geht jedoch davon aus, dass solange es keine umfassende Möglichkeit gibt, digitale Kopien zu verhindern, mit den Pauschalabgaben ein adäquater Interessenausgleich für die Rechteinhaber gegeben ist[401]. Diese Pauschalabgabe ist somit in jedem Falle nach herrschender Lehrmeinung für Leerdatenträger gegeben[402], auch wenn Content bereits durch DRM geschützt wird und vergütet wurde. Allerdings fordern Vertreter der Gerätehersteller ein rechtliches Verbot digitaler Privatkopien generell und den verstärkten Einsatz von DRMS zur wirksamen Kontrolle der Einhaltung – davon versprechen sie sich eine Befreiung von den Pauschalabgaben und damit günstigere Endpreise[403]. Fraglich ist aber, wozu dann noch die Geräte gebraucht werden würden, da sie ja geradezu eingesetzt werden, Kopien anzufertigen[404]. Würde ein generelles Vervielfältigungsverbot für digitalen Content gelten, müssten die Geräte 100% Sicherheit in der Interpretation des DRM

[397] Quelle: Chip, 10 / 2003, S. 18.
[398] Dies ist allerdings verwirrend, da bei digitalem Content je nach Kompressionsgrad eine Spieldauer von einer bis 32 Stunden für DVD-Rohlinge auf neusten Recordern möglich ist.
[399] Vgl. Nuthmann Thomas: Vergütungssätze für Daten-CDs und DVDs neu festgelegt. In: Schneider, 2005, S. I / 45.
[400] Vgl. Burchard Daniel: Urheberrechtsabgabe: DPMA-Schiedsstelle schlägt 12 Euro pro PC vor. In: Schneider, 2005, S. I / 45.
[401] Vgl. Burchard Daniel: Urheberrechtsabgabe für den PC? In: Schneider, 2005, S. I / 57 ff.
[402] Vgl. von Diemar, 2002, S. 126.
[403] Vgl. von Diemar, 2002, S. 179.
[404] Vgl. Broecheler Kirsten: Urheberrecht: Sie dürfen zahlen, aber nicht kopieren. In: Chip, 10 / 2003, S. 18.

gewährleisten. Tauglich wären sie dann nur noch zur privaten Datenspeicherung, d.h. das Interesse an Vervielfältigungsgeräten, die man nicht mehr nutzen kann, würde schwinden, da digitaler Content ja mehrheitlich DRM-geschützt ist[405].

3.11.3. neue Nutzungsarten - neue Vergütungen - neue Probleme

Eine Problematik anderer Natur sind sog. neue Nutzungsarten. Diese behandeln primär Verträge mit Verwertern und Herstellern, die für Anfertigung neuer Datenträger, bzw. der Zurverfügungstellung von Content als neue Nutzungsart Lizenzgebühren bezahlen müssen. Wie Bechtold anführt, kann ein gesamter Markt anhand von Nutzungsverträgen erschlossen werden, ohne mit den einzelnen Käufern in Beziehung zu stehen. Möglich macht dies eine Art Vertragsnetz mehrstufiger DRM-Ketten, das sämtliche Zwischenstationen umschließt, also Urheber, Zwischenhändler und Nutzer[406]. Es ist offensichtlich, dass der Zwischenhändler hierbei leicht umgangen werden kann, denn durch DRM kann dem Umstand einer neuen Nutzungsart künftig ein Ende gesetzt werden, sollte der Urheber selbst die Vervielfältigungshandlungen steuern. Außerdem könnte ein Händler niemals mehr Rechte am Content übertragen als er selber hat[407]. Als Rechteinhaber ist man daher gehalten, sich ständig über neue technische Entwicklungen am Laufenden zu halten. Immerhin wurde die DVD als neue Nutzungsart nicht anerkannt - in einem entsprechenden Fall hatte es eine Filmmusikrechteinhaberin verabsäumt, 1998 im Zuge der letzten Freigabe zur bereits bekannten CD-Verwertung die DVD als Nutzungsart auszuklammern. Das Gericht sah es hierbei als erwiesen an, dass die DVD 1998 bereits bekannt war (1997 wurde der erste DVD-Player auf der internationalen Funkausstellung gezeigt und es gab immerhin schon 40.000 verkaufte Geräte[408]).

Schon 1901 wurde das deutsche Urheberrechtsgesetz erlassen, um die Berner Übereinkunft umzusetzen. Urheber sollten vor nicht gestatteter Verwertung geschützt werden. Die damalige Formulierung der „mechanisch-optischen“ Werkvorführung von Filmen durch den Kinematograph wurde aber in „mechanische und optische“

[405] Dieses Verhalten der Gerätehersteller ist daher faktisch nur so zu interpretieren, dass diese sehr wohl wissen, dass ihre Geräte gängige Kopierschutzmechanismen ignorieren – Treibende Kraft ist hier der Profit aus dem Geräteerlös – aus dem gleichen Grund sind Hersteller von Rohlingen daran interessiert, dass DRMS in Brennern mühelos überwunden werden können, um Absatz und Umsatz zu machen.
[406] Vgl. Bechtold, 2002, S. 259.
[407] Vgl. Bechtold, 2002, S. 136.
[408] Vgl. Dieselhorst Jochen (u.a.): DVD als „neue“ Nutzungsart. In: Schneider, 2005, S. I / 270.

Einrichtungen geändert, was in weiser Voraussicht geschah, hier künftige technische Entwicklungen zu erfassen[409]. Für die Frage gerechtfertigter Vergütungen durch alte Lizenzen mit Verwertungsgesellschaften ist die Klärung der Frage einer neuen Nutzungsart essentiell. Eine CD stellt dabei keine solche dar, ist sie doch durch Verträge zur Verwertung von Schallaufnahmen abgedeckt[410] - so auch Drewes[411]. Die CD bietet nur qualitative Verbesserungen und solche führen nicht zur Annahme einer neuen Nutzungsart[412]. Aus gleichen Erwäggründen ist ja auch die DVD keine solche[413]. Für Text-CDs gilt dies nur insoweit, als hier keinerlei Recherchetools zur Verfügung stehen. Gibt es solche, liegt eine neue Nutzungsart vor, wobei bei der On-Demand Nutzung im Online-Bereich generell von solchen gesprochen werden kann[414]. Der Schlüssel zur Klassifikation als neue Nutzungsart liegt in der Beantwortung der Frage, ob eine wirtschaftliche Veränderung oder Verbesserungen in der Auswertung einer bestehenden bekannten Nutzungsart liegt - konkret, ob somit der Werkgenuss durch eine ursprüngliche Auswertungstechnik befriedigt wird. Ist hier mit „Ja“ zu antworten, liegt keine neue Nutzungsart vor, bei „Nein“ dagegen schon[415]. Davon abhängig ist, ob Urhebern Lizenzgebühren für neue Nutzungsarten zustehen, bzw., ob der Einsatz von DRM im Content hier gerechtfertigt ist. Drewes drückt dies folgendermaßen aus:

> Schon unter der Rechtsprechung des Reichsgerichts war anerkannt, daß [sic!] eine einfache technische Fortentwicklung nicht als eine neue, eigenständige Nutzungsart angesehen werden kann, da sie an die Stelle der alten Befugnis tritt und diese ersetzt. Anderenfalls könnte der Verwerter, der aufgrund der ursprünglich erteilten Befugnis Produkte herstellt, diese nicht mehr absetzen, weil sie nicht dem technischen Standard entsprächen. Die ihm erteilte Lizenz würde wertlos, und er hätte die Lizenzgebühr vergebens bezahlt. Der Urheber hingegen könnte die Befugnis zur Herstellung der Produkte gemäß dem neuen technischen Standard einem Dritten erteilen und erhielte erneut eine Lizenzgebühr. Er könnte auf Kosten seines bisherigen Vetragspartners einen ungerechtfertigten Gewinn erzielen[416].

In den USA ergeben sich im Gegensatz zu Deutschland keine Probleme bei neuen Nutzungsarten, da dort nur der Gewinn im Vordergrund steht. Bis zum Copyright Act von 1976 – dieser ist bundesstaatliche Aufgabe[417] - konnte man Urheberrechte nur nach dem Copyright Act von 1909 als Ganzes übertragen – beim CA 1976 wurde der

---

[409] Vgl. Drewes, 2002, S. 18 f.
[410] Vgl. Günther Andreas: Einwilligung in neue Nutzungsarten. In: Schneider, 2005, S. I / 100 f.
[411] Vgl. Drewes, 2002, S. 118.
[412] Vgl. Drewes, 2002, S. 38.
[413] Vgl. Drewes, 2002, S. 120.
[414] Vgl. Drewes, 2002, S. 132.
[415] Vgl. Drewes, 2002, S. 58.
[416] Zitat: Drewes, 2002, S. 59
[417] Vgl. Fränkl, 2004, S. 60.

Wirtschaftsfaktor Content dagegen noch bedeutsamer eingestuft. Nach §106 wurden alle derzeitigen und künftigen Verwertungsformen erfasst. Somit liegt hier eine offenkundig intelligentere Lösung als beim deutschen Ansatz vor. In den USA hatte man aber Probleme anderer Natur die heute bei DRMS Schwierigkeiten bereiten: die Ausrichtung des gesamten Urheberrechts auf Copyright wurde beim DRM-Einsatz zum Verhängnis. Wird das Copyright nämlich einmal auf einen Dritten übertragen, gebühren diesem sämtliche, also auch die künftigen Nutzungsmöglichkeiten[418], d.h. einmal auf Datenträgern materialisierter Content, muss damit auf anderen Endgeräten nutzbar bleiben. Jegliches DRM beim Hindern künftiger Nutzungsmöglichkeiten durch den Urheber wäre somit untersagt. Daher kann man die Übertragung auf die „derzeit bekannten Nutzungsarten“ beschränken (Beschränkungsklausel)[419], d.h. aber auch, dass digital verwerteter Content auf andere Art als ursprünglich lizenziert, ein Rechtsverstoß wäre[420].

Für Deutschland ist für die eigentliche Nutzungshandlung der Vergütungspflichtige nicht der Nutzer, sondern der, der die Möglichkeiten zur Vornahme der urheberrechtlich relevanten Handlung anbietet - somit Hersteller von Endgeräten und Datenträgern. Diese wälzen die Vergütungen natürlich auf die Nutzer ab[421]. Relevante Handlungen sind dabei das Kopieren der Daten auf Festplatten über das Internet[422] und nicht Zwischenspeicherung im Cache, sowie das Laden und Anzeigen, da es sich hier lediglich um eine vorübergehende Speicherung handelt[423]. Internationale Regelungen sind lediglich bezüglich wechselseitiger Anerkennungen von Leistungsschutzrechten von Künstlern vorhanden, wie im ROM-Abkommen von 1961[424]. D.h. konkret, dass wenn Nutzungspräferenzen unberücksichtigt bleiben, ein Wettbewerb der Konditionen eintritt und sich bestimmte DRMS-Nutzungsverträge einfach nicht durchsetzen[425]. Damit schafft das Internet für digitales geistiges Eigentum eine neuartige Macht des Marktes dessen Ziel es ist, Güter zu tauschen und dadurch

[418] Vgl. Drewes, 2002, S. 77 f.
[419] Vgl. Drewes, 2002, S. 81.
[420] Z.B. als Klingelton für ein Handy. Außerdem darf man auf die Beschränkungsklausel nicht vergessen. Fehlt sie, liegt kein Rechtsverstoß vor.
[421] Vgl. Seith, 2003, S. 12 f.
[422] Dies aber könnte zur Verschiebung des Wettbewerbs beim Bezug von Content führen, dorthin wo er günstiger ist, z.B. in die USA wegen dem Fehlen von Pauschalabgaben und dem generellen Verwertungsabgabensystem.
[423] Vgl. Gutman, 2003, S. 86.
[424] Vgl. Fränkl, 2004, S. 59.

wohlhabende Mitglieder der Gesellschaft zu werden[426]. Auch die Frage nach Zusatzleistungen wird bedeutsamer, da Raubkopierer i.d.R. auf Zusatzmaterial, Handbücher und Support verzichten müssen - ansonsten würde Content nicht mehr gekauft werden, da Raubkopien infolge von Netzeffekten den Nutzen auch für nicht Zahlende erhöhen würden[427]. Genau die Leistungsschutzrechte stellen aber das große Manko für Verwertungsgesellschaften in der Wahrnehmung der Rechte für Urheber dar. DRM ermöglicht hier den Verzicht auf Verwertungsgesellschaften und die Wahrnehmung selbst in die Hand zu nehmen (eben wie dies die US-Rechteinhaber für ihre geistigen Erzeugnisse tun) – damit wäre das komplizierte Verwertungssystem in Deutschland gestorben. Immerhin gibt es Gegenseitigkeitsverträge mit ausländischen Verwertungsgesellschaften. Verboten ist den Verwertungsgesellschaften dabei generell, Gewinn zu erwirtschaften (abzüglich ihrer Deckungskosten) – die Erlöse sind an die jeweiligen Künstler auszuschütten[428]:

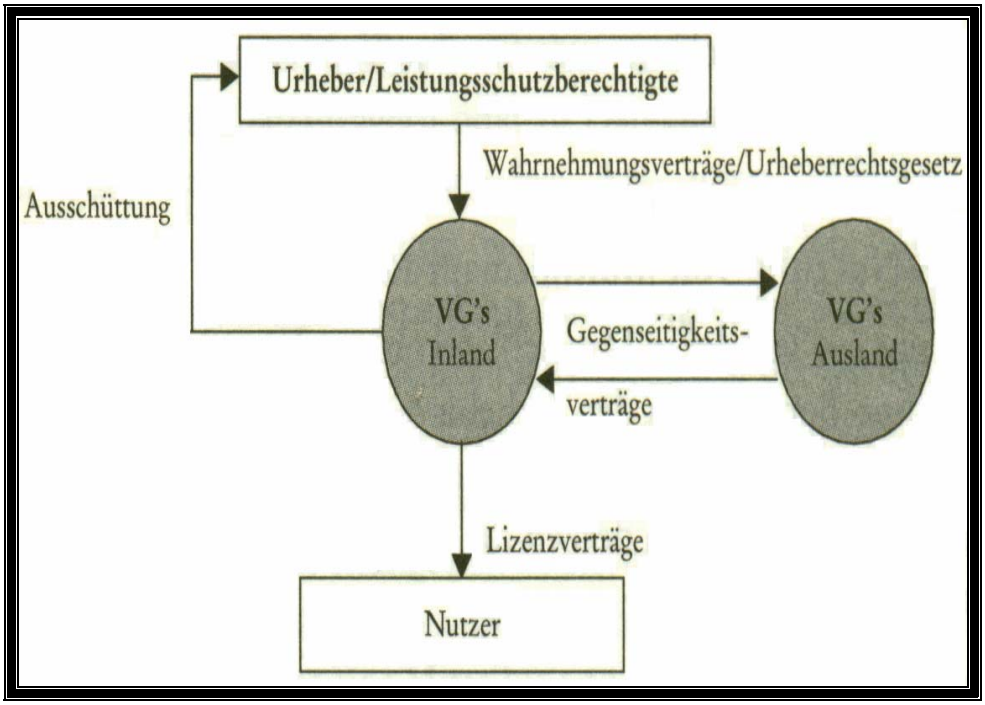

Abbildung 21: So arbeiten Verwertungsgesellschaften[429]

[425] Vgl. Bechtold, 2002, S. 338 f.
[426] Vgl. Czychowski Christian: Zusammenhänge und Überblick. In: Bröcker, 2003, S. 16.
[427] Vgl. Bechtold, 2002, S. 360.
[428] Vgl. Auer-Reinsdorff, 2003, S. 141.
[429] Aus: Auer-Reinsdorff, 2003, S. 141.

Es gibt aber auch Zwangslizenzen im deutschen Recht für den Fall, dass Musik-Urheber einem Tonträgerhersteller Nutzungsrechte und keiner Verwertungsgesellschaft einräumen. Damit sind sie verpflichtet, auch Anderen diese Rechte zu ähnlichen Konditionen einzuräumen. Deshalb handelt es sich faktisch um teilweise erzwungene Abschlusspflicht mit Verwertungsgesellschaften, denn dank dieser wird es nur in den seltensten Fällen zu Zwangslizenzen kommen[430] – hier besteht somit trotz DRM der Hoffnungsschimmer, dass Verwertungssysteme für digitalen Content nicht so schnell zum Auslaufmodell werden. Auf analoger Seite sind Pauschalabgaben und die Wahrnehmung von Verwertungsrechten, sowie der rechtliche Urheberschutz ohnehin die einzigen Möglichkeiten Herr des Contents zu bleiben – eine Abschaffung ist daher bei Marktdurchsetzung von DRMS nicht erforderlich[431], da Vergütungen für Analogkopien von digitalen Datenträgern weiterhin einzuheben wären[432].

Festgehalten werden kann somit, dass beide Systeme in den USA und Deutschland für eine Übergangszeit nebeneinander existieren müssen[433]. Welches System sich letztlich durchsetzen wird, wird erst die Zukunft zeigen. DRM spricht dabei eher die Bedürfnisse des US-Marktes an und stört nur die deutschen Verhältnisse - DRM kann aber ein zusätzliches Sicherheitsinstrument sein. Allerdings widersprechen individuelle durch DRM gesteuerte neue Nutzungsarten von Content einer kollektiven Verwertung – genau diese individuelle Nutzung wird ja geradezu durch DRM reguliert[434]. Fraglich ist somit, wie ein System von Verwertungsrechten in Deutschland mit dem Profitsystem im Sinne des Copyrights einzelner Gruppierungen in den USA (Plattenlabels, Filmstudios, Softwarehersteller) und deren Vorstellungen von DRMS kompatibel sein kann. Derzeit prallen hier Welten aufeinander, aber:

3.12. Online-DRM-Content ist günstiger und weniger riskant

Beim Bezug von Online-Content fallen viele Zwischenstationen weg (=Transaktionskosten). Die Steuern der Internet-Transaktionen bilden dabei noch Handlungsbedarf, denn klassischerweise gilt für reguläre Waren das Bestimmungslandprinzip für die Besteuerung (Softwarepakete, CD- / DVD-

[430] Vgl. von Diemar, 2002, S. 87.
[431] Vgl. von Diemar, 2002, S. 185.
[432] Solange analoge Aufzeichnungs- und Wiedergabegeräte existieren.
[433] Vgl. Goldmann Bettina: Copy Protection by DRM in the EU and Germany: Legal Aspects. In: Becker, 2003, S. 517 f.

Lieferungen). Würde dies auch für Online-Content angewendet werden, könnten immaterielle Güter kaum mehr durch das Netz distribuiert werden[435]. Das Ursprungslandprinzip dagegen angenommen, würde Steuereinnahmen in Staaten mit einer „negativen digitalen Handelsbilanz“ bedeuten. Konsequenterweise wurde daher schon 1998 eine „Bit-Steuer“ vorgeschlagen, die nach der Datenmenge zu entrichten gewesen wäre. Denn der Content wird dort bezogen, wo er am günstigsten ist. Dabei kommen einem geringe Suchkosten im Internet entgegen und wo der Server mit dem Content steht, ist letztlich egal[436]. Durch DRM lassen sich drei, der vier Transaktionskostentheoriepunkte regulieren. Außer den Suchkosten sind dies Kosten für den eigentlichen Abschluss des Nutzungsvertrages, die Kosten der Einhaltung zur Überwachung des Vertrages und allfällige Kosten für Anpassungen im Laufe der Zeit. Während DRM bei der Contentsuche kaum hilfreich sein kann, können o.a. Punkte durch den DRM-Code bestimmt sein. Die eigentlichen Abschlusskosten durch Click-Wrap sind praktisch null, ebenso wie Überwachungskosten zur Urheberrechtseinhaltung durch permanente DRM-Präsenz, abgesehen von den Entwicklungskosten des DRMS und Anpassungen z.B. durch Updates, Device Revocation, etc..., was aber nur im Rahmen der Investitionen in diesem Bereich geschieht[437]. D.h. also, man schließt online den Vertrag nach dem Recht des Ursprungslandes ab und unterliegt damit dessen Urheberrecht und damit dem DRM – nicht dem Schutzlandprinzip für Datenträger, wenn man sich z.B. Content direkt auf solchen liefern lässt, bei dem später festgestellt wird, dass etliche DRM-Mechanismen gar nicht mit dem nationalen Recht vereinbar sind. Für reine Online-Contentanbieter ist DRM-Schutz somit günstiger und weniger riskant. Für Nutzer freilich wäre nicht DRM-geschützter Offline-Content besser[438].

3.13. Das Dilemma mit Umgehungstechnologien

DRMS stellen große Probleme dar, da es sowohl staatliche und gesellschaftliche Interessen gibt, Urheberrechte zu beschränken. (=die Schrankenregelungen). Das Dilemma beim DRMS-Einsatz ist ja, dass Urheberrechtsschranken zahnlos werden – so auch Bechtold, der einen Schritt weiter geht und generell ein stimmiges Konzept

---

[434] Vgl. Auer-Riesdorff, 2003, S. 155.
[435] Es gibt eben (noch!) keinen Zoll in Routern des Internets.
[436] Vgl. Clement, 2001, S. 210 f.
[437] Vgl. Wigand Rolf T.: Facing the Music: Value—Driven Electronic Markets, Networks and Value Webs in Economic Integration of Digital Products. In: Becker, 2003, S. 258 f.

vermisst, wie DRMS mit Schranken in Einklang zu bringen sind[439]. Da Deutschland keinen Unterschied zwischen Zugangsschutz und Kopien macht, ist Umgehungstechnologieeinsatz in beiden Fällen illegal. Schrankenbestimmungen könnten hier infolge ihrer Zahnlosigkeit nur gerichtlich durchgesetzt werden[440]. Lessigs regulierender Code ist hier fehl am Platz, da er nicht zwischen rechtlich gestattetem Zugang und dem Schutzzweck des DRM unterscheiden kann[441]. Koelman bringt dies auf den Punkt:

> However, as with technological measures, circumvention devices cannot distinguish between infringing and non-infringing uses. Therefore, if circumvention devices are freely available, anybody can obtain them to engage in infringing activities and the protection of technological measures will supposedly not have a large impact in practice[442].

Dem ist zuzustimmen, denn damit sind die Rechtsordnungen der USA und Deutschland überfordert, zu klären, wann Umgehungstechnologie eingesetzt werden darf. Nach Bechtold ist die grundsätzliche Sichtweise der Lage in beiden Staaten identisch. Geschützt werden viele DRM-Komponenten, d.h. Verschlüsselungsverfahren zur Zugangs- und Nutzungskontrolle, Kopierkontrollsysteme und Passwörter, Systeme zum Schutz von Authentizität und Integrität, manipulationssichere Systeme zum Schutz von Hard- und Software, sowie Metadaten (letztere jedoch nicht in Deutschland)[443]. Die Gefahr ist nicht vereinzelte Umgehung durch Private, sondern kommerzieller Vertrieb der Umgehungstechnologie[444]. Die WIPO-Verträge waren schon darauf vorbereitet und sahen auch Mindestrechte für Urheber bei Leistungsrebringungen im Internet vor (Digitalisierung, Up- und Download, sowie Laden in den Arbeitsspeicher eines Computers)[445]. Wegen ihrer Internationalität sind die beiden WIPO-Verträge auch für

---

[438] Solche Vorstellungen gehören aber der Vergangenheit an.
[439] Vgl. Bechtold Stefan: Digital Rights Management zwischen Urheber- und Innovationsschutz. In: Zerdick (u.a.), 2004, S. 339.
[440] Vgl. Lejeune Mathias: Protection under US Copyright Law. In: Becker, 2003, S. 381
[441] Würde er das können, müsste es sich um künstliche Intelligenz handeln, die selbständig denken und entscheiden kann, wann z.B. ein Behinderter, ein staatlicher Ermittlungsbeamter, ein Journalist oder ein unberechtigter Nutzer Zugang zum Content erlangen möchte. Derzeit funktioniert dies aber noch nicht, da dafür noch keine Gedankenschnittstellen mit Systemen existieren. Andere Identifizierungsmethoden mit Fingerabdrücken, Signaturen oder Zugriffspasswörtern würden aber selbst wiederum den einleitenden Definitionen folgend DRMS-Abwandlungen darstellen und sind daher untauglich.
[442] Zitat: Koelman Kamiel J.: The protection of technological measures vs. the copyright limitations. In: Gasser, 2002, S. 27.
[443] Nach Bechtold, 2002, S. 197.
[444] Vgl. Bechtold, 2002, S. 198.
[445] Vgl. Czychowski Christian: Zusammenhänge und Überblick. In: Bröcker, 2003, S. 21 f.

die USA bedeutsam, die sie im DMCA 1998 umgesetzt haben[446]. Dies ist auch Ausdruck dafür, dass die transnationale Regulierungsaktivität zunimmt, nationale dagegen abnimmt, was aber infolge der Globalität des Problems der schnellen Vervielfältigung von digitalen Gütern auch nicht verwundert[447]. Deutschland folgte durch Umsetzung der Richtlinie der EU zum Urheberrecht in der Informationsgesellschaft[448], wenngleich dies am 11.04.2003 vom Deutschen Bundestag mit leichter Verspätung geschah. In Kraft trat sie am 13.09.2003[449]. Damit blieb genug Zeit für das Volk, sich noch vorher mit Umgehungstechnologie einzudecken. Denn Kernbestandteil ist ja nun ein Verbot von Umgehungstechnologie, die wirksame technische Schutzmaßnahmen umgehen kann.

Wirksam sind Maßnahmen dann, wenn ein Durchschnittsbenutzer sie nicht umgehen kann[450]. Eine exakte Definition was unter „wirksam“ zu verstehen ist, fehlt aber in Deutschland im Gegensatz zum DMCA[451]. Das „wirksam“ kann daher nur im Sinne faktischer Präsenz eines Schutzes verstanden werden, wenngleich objektiv unwirksam, da zu schwach oder bereits geknackt. Einer der lächerlichsten Schutzmechanismen diesbezüglich waren Cactus Data Shield 100 / 200 und Key2audio. Diese konnten durch einen einfachen „Strich“ mit einem handelsüblichen Filzstift „als Umgehungstechnologie“ im Außenringbereich der so geschützten Musik-CD eingesetzt und dadurch „weggemalt“ werden[452]. Nach der Info-RL fallen vorbereitende Handlungen (Einfuhr, Verbreitung und Besitz zu kommerziellen Zwecken) von Umgehungserzeugnissen deswegen unter Verbot, da Umgehungstechnologien die Anzahl der potentiellen gefährlichen Nutzer erhöhen würde, die ansonsten kein entsprechendes Know How hätten[453]. Einzelne Privatpersonen werden dabei nicht als Gefahr eingestuft, sondern die Umgehungstechnologie[454]. D.h. aber auch, Nutzer vom Vorhandensein von Schutzmechanismen nach §95d des deutschen Urheberrechts deutlich sichtbar mit Angaben über die Eigenschaften der technischen Maßnahmen in Kenntnis zu setzen, wodurch erst die Geltendmachung von Ansprüchen resultiert. Sollte

[446] Vgl. Bechtold, 2002, S. 207.
[447] Vgl. Latzer, 2002, S. 23.
[448] Vgl. Bechtold, 2002, S. 199 ff.
[449] Vgl. Nuthmann Thomas: In-Kraft-Treten des neuen Urheberrechts. In: Schneider, 2005, S. I / 237.
[450] Vgl. Gutman, 2003, S. 143.
[451] Siehe hierzu die Ausführungen im Kapitel dort.
[452] Vgl. Schmelzle Michael: Musik-CDs kopieren. In: PC Welt, 08 / 2002, S. 98 f.
[453] Vgl. Gutman, 2003, S. 144.

nämlich Umgehungstechnologie unbewusst eingesetzt werden (die aus Zeiten vor dem Verbot stammt) oder durch Fehlfunktion eines DRMS dieses ineffektiv sein, würde man sich mangels Aufklärung nicht strafbar machen. Es ist künftig aber auch hier damit zu rechnen, dass es den allgemeinen Verkehrssitten entsprechen wird, grundsätzlich von technischen Schutzmechanismen im Content auszugehen, d.h. also, das bereits jetzt nicht existente „Recht auf Privatkopie“ wird noch weiter eingeschränkt[455].

Dass dabei Fehler in den verantwortlichen Systemen sehr häufig vorkommen, zeigt folgende Tabelle. Wie gut und sicher Code eines Systems ist, sieht man anhand der Fehler pro 1000 Zeilen. Prof. Thomas Huckle der TU-München prophezeit durch die immer höher werdende Anzahl an Codezeilen einen massiven Anstieg der Gesamtfehleranzahl in Systemen. Da nämlich in durchschnittlichen Anwendungen fünf Fehler pro 1000 Zeilen auftreten, würde sich durch Verzehnfachung des Programmcodes trotz einer fiktiven Senkung durch bessere Tests auf vier Fehler pro 1000 Zeilen immer noch eine Verachtfachung der Fehler ergeben[456], was nicht verwundert: „Zum Testen nehmen sich die Software-Entwickler immer weniger Zeit.[457]“ DRMS selbst sind dabei mehrheitlich softwarecodierte Implementierungen in Betriebssystemen wie Windows[458]:

	allgemeine Anwendungen					**Windows als Betriebssystem für DRMS**			
	Standard-Handy	Hubble-Teleskop	Luftraum-Überwachung	Space-Shuttle	B2-Stealth-Bomber	95	NT	2000	XP
Code-zeilen in Mio.	0,2	1	2	3	4	10	16	27	45
Fehler pro 1000 Zeilen	7	2	2	<0,1	2	7	7	7	7

Tabelle 6: Fehler im Code diverser Anwendungen im Vergleich zu Windows als DRMS-Basis[459]

---

[454] Vgl. Bechtold, 2002, S. 198.
[455] Vgl. von Diemar, 2002, S. 151.
[456] In der Praxis sind es deutlich mehr.
[457] Zitat nach: Flohr Manfred: Programmierter Absturz. Software der Zukunft. In: Chip 09 / 2004, S. 138.
[458] Dass es auch anders geht, davon zeugen wichtigere Systeme, wie Space-Shuttles – dort liegt die Fehlerquote bei weniger als 0,1 Fehler pro 1000 Zeilen, was somit von der Zuverlässigkeit zeugt. Die Challenger ging immerhin 1986 wegen eines defekten Treibstoffventils und die Columbia wegen einer defekten Hitzekachel verloren → keine Softwarefehlfunktion und der Beweis, dass es durchaus möglich ist, effektiven Code zu schreiben. Da ein Space-Shuttle allerdings einige 100 Mio. US$ mehr kostet als sich mit Standardsoftware und AV-Content im Normalfall verdienen lässt, würde hier die Verhältnismäßigkeit der erforderlichen Tests nicht stimmen. Außerdem betreibt die Raumfahrt hauptsächlich der Staat, wohingegen die auf Gewinn gerichtete Unterhaltungsindustrie privatwirtschaftlich tätig ist.
[459] Quelle: Chip, 09 / 2004, S. 140.

3.13.1. Der DeCSS-Fall

Der erste brisante Umgehungstechnologiefall nach dem DMCA war das Programm DeCSS zur CSS-Umgehung. Norwegische Hacker knackten ja 1999 den CSS-Schutz von DVDs und boten US-Bürgern den Quellcode an. Acht US-Filmstudios führten gegen diese nun Anklage und erstinstanzlich wurde tatsächlich eine Verletzung der Zugangskontrollvorschriften festgestellt. Nach kalifornischer Rechtsauffassung[460] lag sogar ein Verstoß gegen Geschäftsgeheimnisse vor, trotz fehlenden einheitlichen Schutzes dafür auf Bundesebene[461]. Letztlich siegte aber das Verfassungsrecht auf freie Meinungsäußerung[462], denn man kam zum Schluss, dass DeCSS auch in Kalifornien rechtmäßig veröffentlich wurde. Zum Veröffentlichungszeitpunkt konnte nämlich nicht mehr von einem Geschäftsgeheimnis ausgegangen werden. Diese Meinungsäußerung in Form von Liedern, Texten, Büchern, o.ä. leistete schon bei der Veröffentlichung von PGP als Quellcode gute Dienste, um die Waffenexportgesetze der USA zu umgehen[463]. Daher ist es im Zuge „freier Meinungsäußerung“ auch möglich, weiterhin Umgehungstechnologie zu beziehen. Dr. Forgó räumt ein, dass es ohnehin schwer ist, den Zugriff auf Umgehungstechnologie zu verhindern und rechtlich gegen die Hersteller vorzugehen – daher verwundert es auch nicht, dass Erfinder von Umgehungstools und Hersteller von DRMS in einen regen Wettstreit zueinander stehen: „In Summe liegt hier eine ungünstige Entwicklung für das Recht vor“, so Dr. Forgó weiter.[464] Wie Lessig dazu festhält, kommt es aber nicht auf den Erfolg oder Misserfolg rechtlicher Schritte gegen Contentpiraterie an, sondern einzig und allein darauf, ein Signal zu senden: „Any system that threatens its control will be threatened with an army of Hollywood lawyers.[465]“ – eine Armee Hollywoods aus Rechtsanwälten richtet allerdings nur auf US-Boden nach dem DMCA des US-Rechts etwas aus[466].

---

[460] Ob Hollywood dabei nur zufällig in Kalifornien liegt oder ob Lobbytum im Spiel war, ist nicht bekannt.
[461] Vgl. Bechtold, 2002, S. 229 f.
[462] Vgl. Nuthmann Thomas: Kalifornien: Rechtmäßige Veröffentlichung des DeCSS-Codes. In: Schneider, 2005, S. II / 97.
[463] Vgl. Plura Michael / Teetz Tobias: Geknackt! In: PC Praxis, 05 / 2005, S. 83.
[464] Quelle: Interview mit Dr. Forgó vom 17.02.2006.
[465] Vgl. Lessig, 2002, S. 190.
[466] Gegen eingeschmuggelte Chinesenplagiate müsste aber der Eingriffsbefehl vom amtierenden Präsident George Bush jr. an seine Zollbeamten kommen.

3.13.2. DeCSS in Deutschland

Für Deutschland stellt sich das DeCSS-Problem wie in den USA nicht mehr, da die Einfuhr, der Erwerb und der Besitz derartiger Tools zu kommerziellen Zwecken nach der Urheberrechtsnovelle verboten und jegliche Umgehung untersagt ist[467]. D.h. konkret, dass auch der Handel mit Knackprogrammen strafbar ist – darunter fallen älteren Versionen von Clone-CD / -DVD, AnyDVD oder DVD Shrink, das doppelschichtige Film-DVDs des Typs 9 auf einschichtige DVDs des Typs 5[468] durch Datenkompression brennen kann[469]). Auch wenn man sich solche Tools aus dem Ausland schenken lässt (=Einfuhr), ist man bereits strafbar[470]. Damit lohnt sich der nur mehr geduldete private Besitz aus Zeiten vor der Urheberrechtsnovelle kaum mehr[471] - hier soll lediglich Kriminalisierung verhindert werden. Sogar Anleitungen zur Umgehung in einschlägigen Fachschriften sind strafbar. Die Praxis zeigt aber, dass Tipps und Tricks dennoch fast überall zu finden sind. RA Schumacher-Deutzmann prangert dies folgendermaßen an: „Zwar zeigen sich Verbandsvertreter erbost, doch sehen sie im Ergebnis bisher entweder `keine Strafbarkeit´ oder sind langfristig mit der Prüfung befasst“[472]. Bei geringen Streitwerten unterlassen es diverse Verwerter sogar, Verfolgungshandlungen zu setzen und tolerieren sogar Raubkopien[473] – vielfach auch, weil sie gar nicht wissen, wer eigentlich für private Kleinstmengen in Hinblick auf die Rechteerteilung an Kopien zuständig ist[474]. Umstritten ist jedenfalls auch der Patch zu Movie Jack, mit dem sich drei Kopien einer DVD anfertigen lassen, auch wenn die Datenträger kopiergeschützt sind – damit soll die Privatkopie ermöglicht werden, die beim Wirken von Kopierschutzmechanismen eigentlich verboten ist. Argumentiert wird, dass „echte wirksame“ DRMS noch fehlen und der Hersteller S.A.D. sich nicht mit der Filmindustrie einigen konnte wenigstens private Kopien wieder zu erlauben[475]. Gestützt wurde diese Ansicht auch von einem in Auftrag gegebenen

[467] Vgl. Bechtold, 2002, S. 213 f.
[468] Zu den verschiedenen DVD-Typen siehe Tischer, 1998, S. 428.
[469] Vgl. Schmelzle Michael: 1:1 oder individuell. DVD-Filme auf DVD kopieren. In PC Welt, 07 / 2003, S. 83 f.
[470] Vgl. Metger Christoph: DVDs kopieren. In PC Welt extra, April / Mai / Juni 2004, S. 41
[471] Dies geht sogar soweit, dass man derartige „gebrauchte“ Umgehungstechnologie z.B. nicht über die deutsche eBay-Plattform anbieten darf – Abmahnungen und hohe Strafen können die Folge sein.
[472] Nach Matthiesen Nils: So einfach ist das Kopieren von CDs und DVDs. In PC Praxis, 08 / 2004, S. 44
[473] Dies dürfte eindeutig ein falsches Signal sein, hier mit zweierlei Maß zu messen.
[474] Vgl. Mansmann Urs: Von einem, der auszog, eine legale CD zu brennen. In: c´t #05, vom 20.02.2006, S. 118.
[475] Vgl. Fischer Jens: Kopieren wieder erlaubt? In: PC-Praxis, 03 / 2004, S. 22 f.

Verfassungsgutachten[476] laut S.A.D.-Pressesprecher Christian Trögele[477].[478] Mit doppelschichtigen DVD-Rohlingen und Brennern wurde die Filmindustrie jedenfalls um eine weitere Gefahr der „illegalen optimaleren“ Vervielfältigung reicher[479]. Es gibt bisher nur eine legale Alternative zur digitalen Kopie: die

3.13.3. Analoge Lücke - aber nicht in HDTV

Der Grund für die Existenz der analogen Lücke in den USA und Deutschland liegt in der Regulierung durch Code / Architektur. Dabei ist derzeit noch keine generelle verschlüsselte Kommunikation beteiligter Endgeräte vorgesehen, so wie in der Allianz-Architektur des DRM mit TPM-Chip. Solange dies aber nicht der Fall ist, bieten analoge Ausgabesignale Schlupflöcher decodierten digitalen Content (Musik und Film) abzugreifen und sofort wieder zu redigitalisieren. Sofern man den Ursprungscontent lizenziert hat, fertigt man damit lediglich eine geduldete Privatkopie. Der Clou: analoge Signale sind i.d.R. um digitale Kopierschutzverfahren befreit, d.h. konkret, ein wirksamer Kopierschutz wird nicht mehr umgangen – damit ist dieses Verfahren völlig legal[480]. Tatsächlich praktizierte Möglichkeiten, wie Rundfunkaufnahmen oder Webradio könnten damit zu einer Verteuerung der Abgaben auf Leermedien und der Gebühren zur eigentlichen Programmausstrahlung führen, geht es nach dem Willen der GVL. Konkret soll das Mitschneiden generell verhindert werden – praktisch ist dies aber nicht realisierbar[481]. Nach Aussagen der GEMA ist es ja geradezu legal Sendungen mitzuschneiden[482]. Hier sieht man, dass sogar Verwertungsgesellschaften unterschiedliche Ansichten vertreten, welcher Content geschützt und welcher pauschal vergütet werden soll (=Leerkassettenabgabe). Die Zukunft sorgt jedenfalls auch hier mit dem HDCP-Schutz vor, da digitale Satellitenübertragungen in HDTV-Qualität und HDTV-Endgeräte (TV, Notebooks, DVD-Player oder PC) über entsprechende Schutzmechanismen verfügen müssen, um ein Abgreifen der Signale verhindern zu können:

---

[476] Vgl. Perband Andreas: Abzocke per Gesetz. In: PC Welt, 07 / 2003, S. 13.
[477] Vgl. Fischer Jens: Geknackt: DVD-Tools. In: PC-Praxis, 02 / 2004, S. 103.
[478] Daraus wurde aber dennoch nichts, da im folgenden Verfahren der Streitwert durch das Gericht mit einer Million € festgesetzt wurde, was die wirtschaftlichen Möglichkeiten von S.A.D überstieg → es wurde kein Verfahren durchgeführt.
[479] Vgl. Masiero Manuel: Doppelter Speicherplatz. In: PC-Professionell, 12 / 2003, S. 202.
[480] Vgl. Kuther MArgit / Rau Thomas: Alles Knacken. In: PC Welt 01 / 2006, S. 103ff.
[481] Vgl. Weidemann Tobias: MP3 gratis. In PC, Welt, 07 / 2005, S. 130.
[482] Vgl. Behrens Daniel: Web-Recorder. In: PC Welt, 07 / 2003, S. 205.

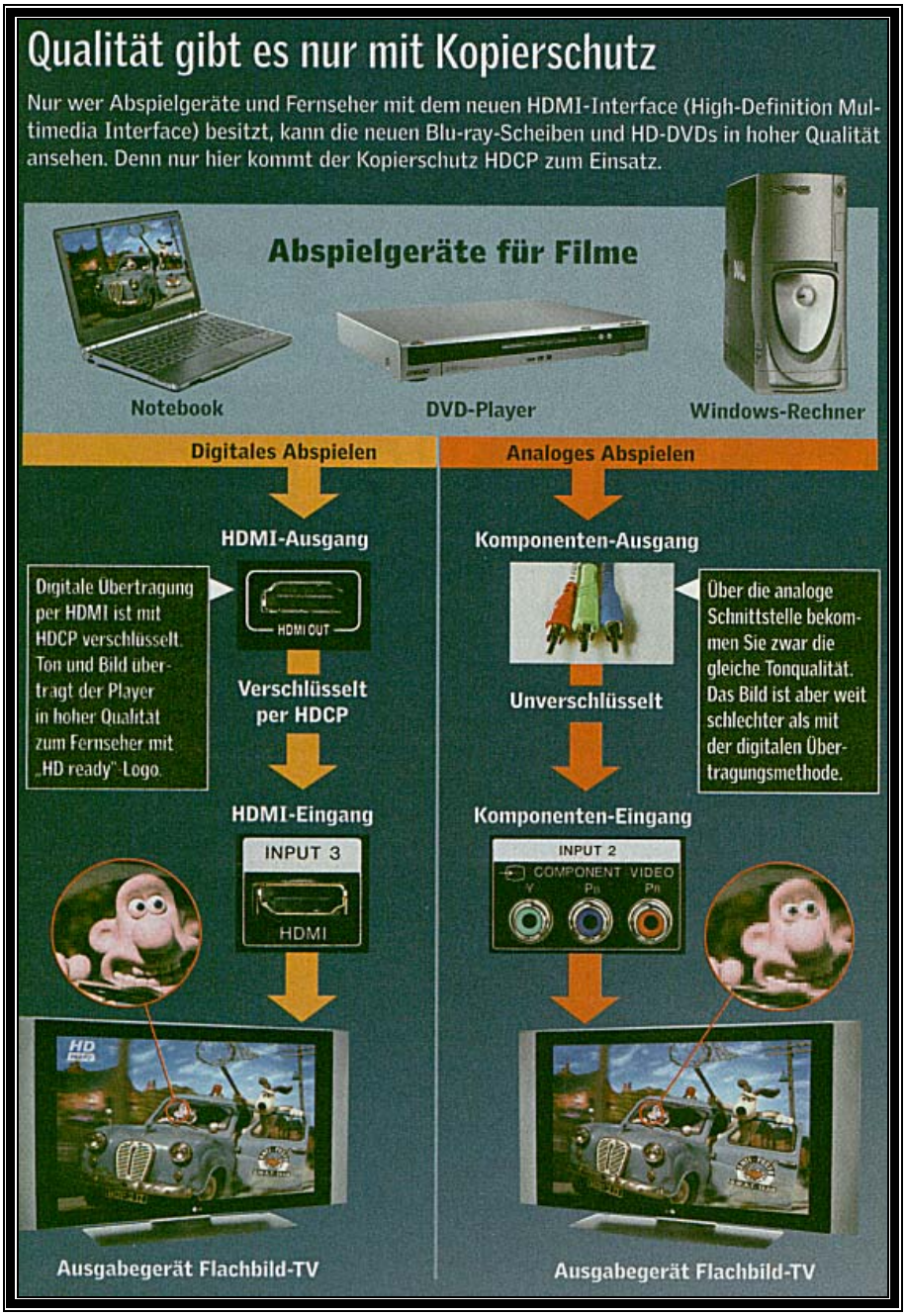

Abbildung 22: Der HDCP-Kopierschutz von HDTV in Aktion[483]

Sicherungsmittel dazu sind einmal mehr die von Bechtold angeführten Technologie-Lizenzverträge. Der Grund: DRMS sind nur solange effektiv, wie die Endgeräte die DRMS-Sprache interpretieren. Daher verpflichten Hersteller von DRMS die Lizenznehmer (v.a. Endgerätehersteller), gewisse Schutzstandards einzuhalten. Das

[483] Aus: Chip, 05 / 2006, S. 104.

Interesse liegt auf der Hand: sichere DRMS veranlassen auch Contenthersteller diese Schutztechnologie zu lizenzieren, was letztlich Geld für die Hersteller bringt. Dagegen würde es Verluste bringen, wenn ein DRMS geknackt wird (=verlorenes Vertrauen) - genau deshalb wird Contentanbietern auch das Recht in die Hand gegeben, best. Endgeräte von weiterer Nutzung auszuschließen (eben Device Revocation[484]). Ob dadurch das Sicherheitsniveau hoch gehalten werden kann, darf bezweifelt werden, da Privatanwender nicht alljährlich die gesamte Heimelektronik vom TV über DVD-Recorder bis zu Sat-Receiver auswechseln, um neuen Standards zu entsprechen[485], v.a. dann nicht, wenn dies zu ihren Ungunsten geschieht. Somit schützen Technologielizenzverträge nur begrenzt. Außerdem kostet die Entwicklung der DRMS Geld und DRM-geschützter Content wird beim Nutzer als weniger wertvoll eingestuft als Content, der nicht DRM-geschützt ist[486]. Dabei dürfte der Faktor der Unannehmlichkeiten, bzw. Nicht-Akzeptanz am Markt ins Spiel kommen. Immerhin ist der Frustfaktor bei Nutzern groß genug, Piraterie zu forcieren, sollte Content, der eigentlich „gekauft wurde“, nicht frei genutzt werden können, so wie Content der nicht DRM-geschützt ist[487]. Lessig räumt ein, dass nicht einmal der Staat Standards durchsetzen kann, von denen sich Anwender in unerwünschter Weise eingeschränkt fühlen. Chancen, diese Einschränkungen zu umgehen, bietet der offene Code, denn dabei handelt es sich letztlich um offene Kontrolle, der man aus dem Weg gehen kann. Die Regulierungsmacht des Staates wird zwar auch hier nicht beseitigt, allerdings verändert[488].

3.14. Ist Open Source oder Closed Source besser?

Der Grund warum dieses Kapitel zu DRM gehört, ist schlichtweg, dass auf Computeranlagen neben Windows Open Source Systeme laufen können z.B. Linux. Im Zuge möglicher offener Regulierung könnte Open Source eine Alternative zu Closed Source darstellen – so sind auch viele Verschlüsselungsalgorithmen offen gelegt und

[484] Vgl. Bechtold, 2002, S. 191.
[485] Die diesjährige Fußball-WM hätte ja den Durchbruch bei HDTV in Europa bringen sollen. Bisher merkt man rein subjektiv betrachtet aber nicht viel davon. HDTV-Geräte bleiben in Europa rar und die Industrie hat sich hier grob verspekuliert. Möglicherweise ist dies auch ein Indiz dafür, dass der PAL-Standard den Qualitätsbedürfnissen von „Normalanwendern“ noch die nächsten Jahre lang vollauf genügen wird.
[486] Vgl. Haber Stuart: If Piracy Is the Problem, Is DRM the Answer? In: Becker, 2003, S. 232.
[487] Vgl. Fetscherin Marc: Evaluating Consumer Acceptance for Protected Digital Content. In: Becker, 2003, S. 315.

lizenzfrei[489]. Grundvoraussetzung ist aber, dass Nutzungsrechte an offenem Code ebenfalls eingeräumt werden müssen und dieser als solcher identifizierbar ist. Dabei ist die treuhändische Bündelung von Rechten wie in der Free Software Foundation Europe zu erwähnen, um Rechte an Code aus anderen Staaten (wie eben den USA) einfacher zu übertragen. Ansonsten müsste wieder jeder beteiligte Entwickler infolge der zersplitterten Bearbeitungsrechte gesondert kontaktiert werden. Daher steht eine standardisierte Rechteübertragungsmethode an offenem Code zur Verfügung: die GNU General Public License (GPL)[490]. Eine Unterlassung des Hinweises, Quellcode von unter GNU-Lizenz bearbeitetem Code weiterhin kostenlos zu veröffentlichen, stellt einen durchsetzbaren Verstoß dar[491]. Daher ist das Schutzlandprinzip wichtig, da Open Source sonst keinerlei Rechten eines Staates unterworfen wäre. Hier gelten allgemeine Grundsätze zum Schutz von Software, Schutz der aber ohnehin nur in der Weiterveröffentlichungspflicht des Quellcodes besteht, da Open Source ja jederzeit durch jeden modifiziert werden kann[492].

Genau dies aber ist bei Closed Source strittig: ohne Quellcode ist dies kaum möglich. Bei Standardsoftware ist dessen Herausgabe generell unangebracht, bei Individualsoftware nach Vereinbarung – vieles hängt dabei vom Einzelfall ab. Wichtig ist daher, genaue Regelungen über Quellcode bereits im Vorfeld einer Softwareüberlassung zu treffen[493], klarerweise nur für kommerziell entwickelte Software. Dies deshalb, da der Auftraggeber i.d.R. erhebliche finanzielle Ressourcen investiert hat. Bei Standardsoftware dagegen liegt das primäre Interesse beim Urheber auf Geheimhaltung seines Know Hows[494]. Genau hier sollte klar werden, was das ganze mit DRM zu tun hat. Denn wenn Umgehungstechnologien erforderlich sind, um DVDs auch unter dem Open Source System Linux anzusehen[495], bzw. dieses Betriebssystem auch auf künftigen DRM-Architekturen (der Allianz) laufen soll, muss der Ansteuerungscode und damit die Schnittstelle des DRMS offen gelegt werden. Daraus

---

[488] Vgl. Lessig, 2001, S. 193 ff.
[489] Vgl. Fränkl, 2004, S. 45.
[490] Vgl. Brexl Oliver: Treuhandvertrag in Open Source Software vorgestellt. In: Schneider, 2005, S. I / 69
[491] Vgl. Ernst Stefan: Geltung einer GPL. In: Schneider, 2005, S. II / 242.
[492] Vgl. Lejeune Mathias: Rechtsprobleme bei der Lizenzierung von Open Source Software nach der GNU GPL. In: Schneider, 2005, S. 10 f.
[493] Vgl. Burkart Axel: Softwareerstellung – Anspurch auf Herausgabe des Quellcodes. In: Schneider, 2005, S. I / 53 ff.
[494] Vgl. Rössel Markus: Zulässigkeit einer Quellcode-Klausel. In: Schneider, 2005, S. I / 238 f.
[495] Vgl. Lessig, 2002, S. 189.

ließe sich aber Wissen ableiten, wie man das DRMS wieder umgehen könnte, denn einerseits ist man gezwungen, den Quellcode zu veröffentlichen, andererseits könnten strafrechtliche Tatbestände in bestimmten Staaten vorliegen (Geheimnisschutz, vorbereitende Handlung zur Umgehung).

Strittig ist auch, ob Unternehmen für den Insolvenzfall, Zugangsdaten zu Software, Quellcodes und Lizenzen bei Escrow-Agents hinterlegen müssen, um allfällige Vollstreckungen gegen derartige Ressourcen zu dulden[496]. Ähnliches gilt für Mitarbeiter in Unternehmen, die an ihren Werken alleinige Urheberrechtsbefugnisse hätten, wenn Arbeits- und Dienstverträge nicht ausdrücklich Gegenteiliges vorsehen würden – kommerzielle Verwertung durch den Dienstgeber und im Auftrag erstellten Contents wäre ohne solche Vereinbarungen faktisch ausgeschlossen[497]. Für diese sog. Works Made For Hire gibt es auch hier einen Unterschied zwischen US- und deutschem Recht. Ist in Deutschland der Arbeitnehmer in jedem Fall der Urheber, ist der Arbeitgeber nur zur Ausübung der Vermögensrechte am Content berechtigt. In den USA dagegen kann auch eine juristische Person, also i.d.R. die Firma des Arbeitnehmers Urheber sein[498].

Fallweise ist auch vollständige freie Verwendung von Content erlaubt (Public Domain). Da in Deutschland das Urheberrecht es aber nicht erlaubt, Content in den Public Domain Bereich „zu entlassen“, bestehen hier noch Schwierigkeiten - anders das US-Recht, wo Urheberrechte aufgegeben werden können[499]. Damit bietet Open Source Code weltweit die Möglichkeit zentral kontrollierte Regulierungsinteressen durch den Staat und die DRM-Allianz zu reduzieren. Wie Lessig ja treffend feststellte, findet ja die staatliche Macht Grenzen im offenen Code. Freilich ändert dies nichts an der potentiellen Regulierbarkeit des offenen Codes durch Änderung der Rahmenbedingungen in den drei anderen Bereichen (Recht, Normen oder Markt). Entscheidend ist letztlich, dass diese Regulierung nur innerstaatlich greift, weil wie Lessig es weiter formuliert hat: „die Autoren des Codes kontrolliert werden können[500].“ Was nun wirklich besser ist, lässt sich nicht eindeutig sagen – ob geschlossener Code

[496] Vgl. Martens Silke: Insolvenzrecht und Escrow-Agents. In: Schneider, 2005, S. I / 139.
[497] Vgl. Auer-Reinsdorff Astrid: IT-Arbeitsverhältnisse. Regelungsbedarf in Arbeitsverträgen mit Programmierern und Urhebern. In: Schneider, 2005, S. II / 116 ff.
[498] Vgl. Asche, 1998, S. 102.
[499] Vgl. Jaeger Till: Lizenzierungsplattform für Open Content. In: Schneider, 2005, S. I / 21 ff.
[500] Vgl. Lessig, 2001, S. 191.

eines privaten auf Gewinn gerichteten Unternehmens oder offener Code zur allgemeinen Verfügung.

3.15. Verliert das Urheberrecht dank DRMS an Bedeutung?

Die aufgezeigten DRM-Schwachstellen sind vergleichbar mit Einbruchsgelegenheiten, allerdings ohne sich an den eigentlichen Ort, wo der Content vorrätig gehalten wird, begeben zu müssen – damit stellen sie eine Existenzbedrohung für die Rechteinhaber dar[501]. Da DRMS-Schutz aber außerhalb des Urheberrechts ansetzt, unterliegt dieser der Wandlung der Technik und den daraus resultierenden modifizierten Nutzungs- und Technologie-Lizenzverträgen diesbezüglich[502] - das Recht agiert hier nicht, sondern reagiert nur auf diesen Wandel, weshalb festzuhalten bleibt, dass erst technische Novitäten die Entwicklung des Urheberrechts vorantrieben[503]. Wie in den Angriffskapiteln auf DRM gezeigt wurde, gibt es keinen effektiven Schutz durch DRMS. Das Beharren der Contenthersteller darauf ist daher nur so zu deuten, einen „präsent wirkenden“ Kopierschutz zu haben[504], um wenigstens nach den Urheberrechtsnovellen in den USA (DMCA) und Deutschland (EU-Richtlinie) strafrechtliche Sanktionsmittel in der Hand zu haben. D.h. konkret, dass hier ein Beispiel für das „Sicherheitsnetz Urheberrecht“ vorliegt, wenn DRM versagt.

Zudem wird in der postindustriellen Informationsgesellschaft wie von Diemar feststellte wegen des rasanten Anstiegs des Bedarfs an schöpferischen Leistungen, wesentlich mehr geistig als körperlich gearbeitet[505]. Bedeutungsverlust erlangt das Urheberrecht daher keinesfalls, denn wenn individueller, vertraglicher oder rechtlicher Schutz versagt, bzw. einzelne Bestimmungen in Nutzungsverträgen unwirksam sein sollten, greift dennoch das absolut wirkende Urheberrecht zum Schutz der schöpferischen Tätigkeit[506] - im Gegenteil noch: das Urheberrecht ist angesichts der mehrheitlich geistigen Schöpfungen wichtiger denn je. Denn: technischer Schutz alleine reicht ohne verfassungsrechtliche oder sonstige gesetzliche Unterstützung nicht aus, um

[501] Vgl. Jaeger Till: Gutachten zu „Datenpiraterie im Internet“. In: Schneider, 2005, S. I / 22.
[502] Vgl. Bechtold, 2002, S. 280 f.
[503] Vgl. Plate, 2003, S. 207.
[504] Vgl. Bechtold, 2002, S. 204.
[505] Vgl. von Diemar, 2002, S. 5.
[506] Vgl. Bechtold, 2002, S. 371 ff.

Content effektiv zu schützen[507]. So vermag zwar ein DRMS durch Zwang die Interessen des Urhebers auch gegen gesellschaftliche Nichtakzeptanz durchzusetzen, das Urheberrecht dagegen kommt dann zum Zug, wenn die Schutzmechanismen des DRMS umgangen werden[508]. Hier liegt somit eindeutig Regulierung durch Architektur im Sinne von Code und Recht vor - allerdings gibt es auch Kritik an Lessigs regulativer Kräfte. Wie Tuomi anführt, fehlt der Bezug zur gesellschaftlichen Praxis (also z.B. eben die Nichtakzeptanz). Ferner kann der regulierende Code bereits innerstaatlich unterschiedliche Umsetzung erfahren[509] Damit kann das eigentliche Regulierungsziel vielfach nicht so erreicht werden, wie geplant: Schutz geistigen Eigentums. Dennoch ist nach Art. 1 Abs. 8 Satz 8 der US-Verfassung das Urheberrecht als Zielbestimmung definiert[510], in Deutschland dagegen als zersplitterte Auffassung einzeln auszugestaltender Grundrechte – eine Stellung des Urheberrechts in den Verfassungsrang fehlt aber auch hier[511].

Man kann dennoch festhalten, dass die verfassungsmäßige Wichtigkeit von Urheberrechten (an)erkannt wurde und diese somit „fast im Verfassungsrang“ einzustufen ist. De jure ist dies natürlich nicht der Fall, denn das geistige Eigentum muss sich in bestimmten legitimen Fällen (Schrankenregelungen) auch ohne Einverständnis des Urhebers nutzen lassen[512] und damit „verletzbar“ sein. Problematisch ist hier auch die Hinterlegung von Schlüsseln (sog. Key Escrow-Ansatz), denn diese müssen hier bei vertrauenswürdigen Institutionen sicher verwahrt und der Zugriff auf diese durch sie reguliert werden. Bechtold spricht hier von mühsamen und langwierigen Unterfangen, besonders wenn Fehlentscheidungen der Akteure

[507] Dies ergibt sich schon aus der Natur des geistigen Eigentums – da es flüchtig ist, kann es nur auf Datenträgern festgehalten werden – somit resultiert Schutz geistigen Eigentums auch im Schutz vor unbefugter Nutzung, d.h. der „Wahrnehmung in den Geist“ des Nutzers. Ist dies einmal unvergütet geschehen, wäre nur die Liquidierung des Nutzers möglich, um den „Geist zu löschen“ – dem vorzubeugen dienen somit DRMS. Der Satz: „Wissen ist das einzige Gut, das sich vermehrt, wenn man es teilt.“, entwickelt im Informationszeitalter auf digitalen Content bezogen eine fragwürdige Tragweite. Die Teilung (=hier Vervielfältigung durch Digitalkopie) ist bei kommerziellem Content nur dann erwünscht, wenn für diese „Vermehrung“ angemessene Vergütung für den Urheber gesichert ist.
[508] Vgl. Fränkl, 2004, S. 78 f.
[509] Vgl. Tuomi Ilkka: De-Regulierung und Re-Regulierung. In: Zerdick (u.a.), 2004, S. 309.
[510] Vgl. Berking, 2002, S. 38.
[511] Vgl. Seith, 2003, S. 89.
[512] Vgl. Dreier Thomas / Nolte Georg: The German Copyright- Yesterday, Today, Tomorrow. In: Becker, 2003, S. 480.

vorliegen[513]. Die Wichtigkeit des Urheberrechts bleibt jedenfalls bestehen, um „strafen zu können“:

3.16. Die drohenden Strafen

Rechtlicher Umgehungsschutz von DRMS würde nichts bringen, wenn keine Sanktionen vorgesehen wären. Daher wird durch Geld- und / oder Haftstrafen Anreiz geschaffen, Urheberrechte zu respektieren. Nach dem Schutzlandprinzip ist dies aber nur dort möglich, wo auch entsprechende Regelungen vorhanden sind. In den USA und Deutschland ist dies jedenfalls der Fall. Die Strafen für gewerbliche Raubkopierer nach deutschem Recht erstrecken sich auf bis zu fünf Jahre Haft, Privatpersonen dagegen sind hauptsächlich zivilrechtlich schadenersatzpflichtig, beim rechtswidrigen Angebot in Tauschbörsen dagegen liegt der Strafrahmen bei Geldstrafen oder Freiheitsstrafen bis zu drei Jahren[514]. Die zivilen Schadenersatzforderungen können dabei nach Ansicht von Urheberrechtsexperte RA Christian Czirnich sogar noch höher sein, als die übliche zwei- bis dreifache Lizenzgebühr, so der höhere Schaden nachgewiesen wird – beim illegalen Angebot von mehreren Tausend Dateien in Tauschbörsen kommen so schnell Summen im sechs- bis siebenstelligen €-Bereich zusammen[515]. In den USA sind die Strafen noch höher. Beim ersten Verstoß gegen den DMCA droht eine Geldstrafe bis zu 500.000 US$ oder fünf Jahren Haft - für Folgeverstöße bis zu 1 Mio. US$ oder zehn Jahre[516]. Damit dürfte bewiesen sein, dass Raubkopierer tatsächlich als Verbrecher einzustufen sind[517] und nicht als Kleinkriminelle, die Kavaliersdelikte begehen.

Weitere zivilrechtliche Schutzmöglichkeiten sind neben Schadenersatz, Unterlassungsansprüche, Urteilsveröffentlichungen, Beseitigungsansprüche und Entgeltsnachzahlung[518]. Außerdem können die Gegenstände zur Vervielfältigung verfallen (=beschlagnahmt werden)[519]. Gemeinhin wird bei der Streitwertfestsetzung

---

[513] Vgl. Bechtold, 2002, S. 412 ff.
[514] Heidrich Joerg / Himmelreich Gerald: Die Grenzen des Erlaubten. Ratgeber: Privatkopien, Tauschbörsen, Abmahnungen. In: c´t #5, vom 20.02.2005, S. 111.
[515] Vgl. Jannot Thomas (u.a.): So kopieren Profis Kinohits aus dem Internet. In: PC Direkt, 05 / 2002, S. 79
[516] Vgl. Lejeune Mathias: Protection under US Copyright Law. In: Becker, 2003, S. 371.
[517] So tönt es zumindest aus verschiedensten Kampagnen im Kino oder beim Vorspann zu DVDs (z.B. der DVD: Babylon 5: Legende der Ranger) – v.a. im Kino ist aber fraglich, was dies bewirken soll, denn die Zuseher dort haben ja ohnehin Eintritt bezahlt. Mehr Wirkung verspricht da schon die illegale digitale Kopie einer DVD.
[518] Vgl. Gutman, 2003, S. 127.
[519] Vgl. Gutman, 2003, S. 132.

auch auf den Faktor Abschreckung gesetzt. Damit soll Generalprävention betrieben werden, um zu zeigen, dass Urheberrechtsverletzungen sehr kostspielig sein können[520]. So wurde z.B. für eine ungefragte und unbefugte Kopiergerätewerbung eine Lizenzgebühr von 70.000 € für die 1992 verstorbenen Marlene Dietrich an deren Tochter fällig[521]. Dass jedoch das alleinige Anbieten von „Möglichkeiten“ der Vervielfältigung keine urheberrechtlich relevante Handlung darstellt, zeigt sich im Fall von Münzkopierautomaten zur Herstellung von CD-Kopien. Die Vervielfältigung selbst wird nämlich nicht durch den Anbieter, sondern durch den Nutzer des Gerätes herbeigeführt[522]. Dies kann im Analogieschluss auch für interne CD- und DVD-Brenner in Computeranlagen angenommen werden. Für Umgehung von Smart-Cards bei PAY-TV dagegen wurde anders entschieden. Da der verkehrsübliche Zweck von programmierbaren Smart-Cards eben in der Decodierung von verschlüsselten Fernsehprogrammen liegt, lag hier konsequenterweise ein Unterlassungsanspruch durch den Anbieter „Premiere“ gegenüber Herstellern von Samrt-Cards und Geräten, diese zu programmieren vor.

Hier resultierte der Anspruch aber nicht aus urheberrechtlichen sondern aus zugangskontrolltechnischen Gründen, die ebenfalls die Herstellung, Einfuhr und Verbreitung von Umgehungsvorrichtungen untersagt. Denn im Gegensatz zum bloßen Besitz von Umgehungstechnologie des Urheberrechts ist der Besitz von Umgehungstechnologie des deutschen Zugangskontrollgesetzes sehr wohl strafbar (bis zu 50.000 €)[523]. In den USA läuft zudem eine ständige Diskussion, ob der DMCA noch weiter verschärft werden könnte und sollte[524]. Allerdings ist die bloße Nutzung von raubkopiertem Material noch keine urheberrechtlich relevante Nutzungshandlung – es fehlt am Vervielfältigungsbegriff des US-Rechts. Das Werk ist ja lediglich wahrnehmbar (Musik, Film, gelesener Text im Internet). Lediglich bei Software ist eine bewusste Vornahme der Vervielfältigung durch Laden in den Arbeitsspeicher erforderlich. Daher liegt eine urheberechtlich relevante und strafbare Vervielfältigungshandlung vor[525].

---

[520] Vgl. Gebler Alexander: Streitwertfestsetzung zur Abschreckung von Urheberrechtsverletzungen. In: Schneider, 2005, S. II / 273.
[521] Vgl. Elteste Thomas: Angemessene Linzenzgebühr – „Blauer Engel“. In Schneider, 2005, S. I / 198.
[522] Vgl. Schmid Grgor: Vertrieb von CD-Münzkopierautomaten. In: Schneider, 2005, S. 214 ff.
[523] Vgl. Rössel Markus: Zugangskontrolldiensteschutz. In: Schneider, 2005, S. I / 220.
[524] Vgl. Nuthmann Thomas: USA: Verschärfung des DMCA geplant. In: Schneider, 2005, S. I / 166.
[525] Vgl. Asche, 1998, S. 112.

4. Auswirkungen auf den Datenschutz

4.1. Warum wirkt DRM generell auf Datenschutz?

Da künftig sämtliche Formen der Kommunikation über Internet, bzw. zumindest computergestützt ablaufen werden[526], liegt auf der Hand, dass auch digitaler Content mehr und mehr online zu beziehen sein wird. Die von Fröhle festgestellten zu Grunde liegenden Identifikationsmerkmale[527] klassischer Webnutzung lassen sich daher uneingeschränkt 1:1 auf DRMS übertragen, mehr noch, stellen sie geradezu das Paradebeispiel erzwungener Profilbildung und Verknüpfung mit Daten dar. Immerhin ist ohne Contentfreischaltung keine Nutzung möglich, so Schutzmechanismen des DRM zur Urheberrechtseinhaltung wirken. Der Nebeneffekt und Motivationsgrund für die gleichzeitigen Verknüpfungsmöglichkeiten von Daten durch Auswertung kommerziellen Nutzungsverhaltens von Menschen ist dabei die Verbesserung von Geschäften[528] – damit hat man Wettbewerbsvorteile gegenüber Konkurrenten. Eine Contentfreischaltung setzt Kontakt zum DRMS je nach Vertriebsmodell der beteiligten Urheber und Miturheber voraus. Für den Media Player z.B. wird hier auch bei Streaming-Angeboten auf Lizenzserver zurückgegriffen, wie folgende Abbildung zeigt:

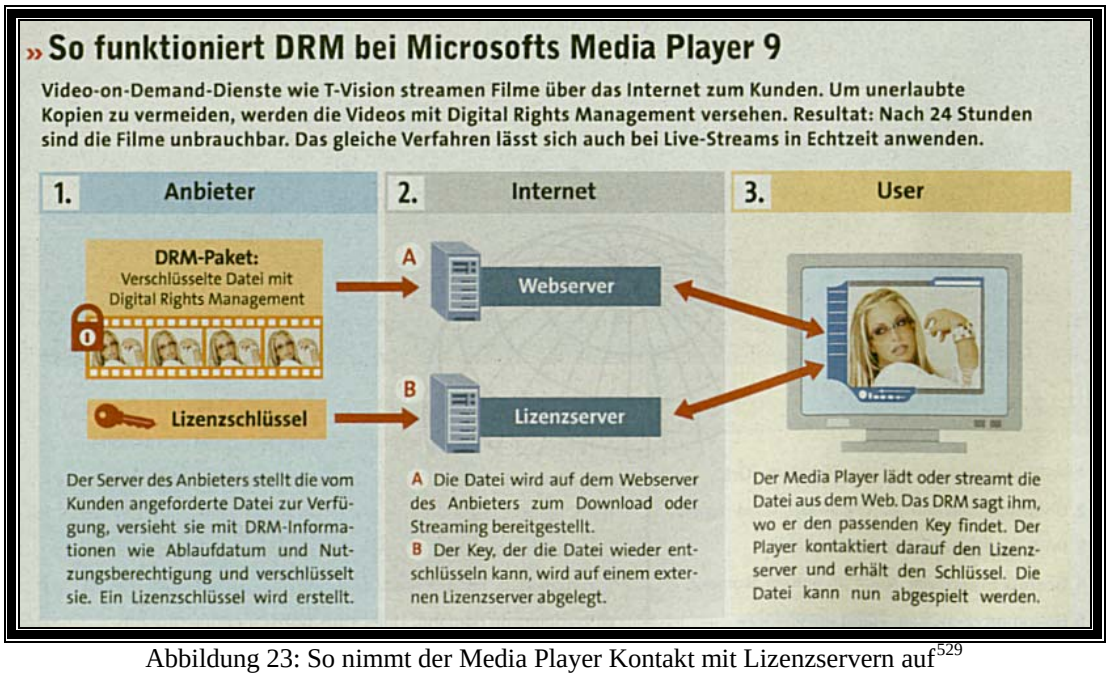

Abbildung 23: So nimmt der Media Player Kontakt mit Lizenzservern auf[529]

[526] Vgl. Bäumler, 2003, S. 72.
[527] Vgl. Fröhle, 2003, S. 40 ff.
[528] Vgl. Roßnagel, 2003, S. 55.
[529] Aus: Chip, 04 / 2004, S. 64.

Dabei besteht das Problem, dass ohne Datenspuren im Internet nichts läuft. Alleine der Aufruf einer Website kann Logprotokolle am lokalen System hinterlassen, sowie die IP-Adresse beim Provider oder beim Host-Rechner der abgerufenen Seite. Dies alles passiert im Hintergrund, noch ohne dass ein spezielles DRMS wirkt. Kommt nun zielgerichtete Contentfreischaltung dazu, ist nicht absehbar, welche Daten durch die Urheber noch abgefragt, geschweige denn gespeichert werden. Somit handelt es sich um verdeckte Datenerhebung. Offene Datenerhebung wäre nur das, was offensichtlich vom Nutzer zum Bezug des Contents anfällt (Name, Kreditkartennummer, Zieladresse, Geburtsdatum als Altersverifikation, etc…). Angereichert werden können diese Daten aber schon hier um freiwillige Zusatzinformationen, die nichts mit dem Bezug des Contents zu tun haben[530]. Im Gegensatz zum Urheberrecht müssen sich Rechteinhaber beim Datenschutz aber noch einem Top-down-Ansatz der Regulierung durch den Gesetzgeber beugen[531], wenngleich hier durch die EU bereits Selbstregulierung wie in den USA forciert wird[532].

4.2. Privatsphäre

Um nun konkret zu wissen, welche Auswirkungen DRMS auf den Datenschutz haben, muss zuerst definiert werden, was der Datenschutz bewirken soll, d.h. also was die zu schützende Privatsphäre ist. International und kulturübergreifend fußt Datenschutz dabei auf der Achtung des privaten Lebens - eben der Privatsphäre[533]. Die Möglichkeiten geistige Erkundungen nach Gutdünken anzustellen und ohne ständige Beobachtung z.B. ungestört lesen zu können, stellen Julie Cohen zufolge Werte dar[534]. David Brin geht dabei so weit die Privatsphäre zu definieren als das Bedürfnis, Produktion und Verbreitung von Daten über andere zu verhindern, gleichzeitig auch die Unterbindung von Gegenspionage des Überwachten zu fordern[535]. Ethan Katsh dagegen

[530] Vgl. Bröcker Klaus Tim: Schutz des Nutzers im Netz: Datenschutz und Datensicherheit. In: Bröcker, 2003, S. 232 ff.
[531] Vgl. Latzer, 2002, S. 83.
[532] Vgl. Latzer, 2002, S. 87.
[533] Vgl. Genz, S. 7.
[534] Nach Lessig, 2001, S. 247.
[535] Nach Lessig, 2001, S. 271.

definiert sie als die Macht, das zu kontrollieren, was andere über jemanden (=Sie) wissen[536]. Moderne DRMS bieten nun beide Möglichkeiten: *erstens* weiß man nicht, dass man überwacht wird - folglich ist Gegenspionage kaum möglich und *zweitens* wird „die Macht“ nach Katsh aus der Hand gegeben. Diese Macht, die die Privatsphäre kontrolliert, ist transformiert zu Code des DRMS. Dies geht faktisch so weit, dass vergleichbar von echten Hausdurchsuchungen des Staates Schnüffelprogramme von Contentherstellern ebenfalls solche durchführen, bezogen auf Daten in PCs. Werden sie fündig, wird dies gleich an zentrale Stellen gemeldet – damit soll die Nutzung von Raubkopien aufgedeckt werden[537]. Dies wäre zwar ok, sofern ein richterlicher Beschluss von Seiten des Staates vorläge, ansonsten aber sind Persönlichkeitsrechte tangiert. Die Verhältnismäßigkeit wird dabei nur selten gewahrt, da die Architektur der digitalen Welt es ist, die im Gegensatz zu offenen Übergriffen des Staates bei Hausdurchsuchungen oder Abhören von Telefonen der totalen Überwachung entgegenkommt. Die „Belastungskosten“ an Mensch und Material sind hier sehr gering[538]. Daher ist Datenverschlüsselung geradezu Pflicht. Der Entwickler des E-Mail-Verschlüsselungsprogrammes PGP Phil Zimmerman hat zur Gefahr unverschlüsselter Kommunikation bereits festgestellt:

> Je weiter das Informationszeitalter voranschreitet, desto mehr verlieren wir unsere Privatsphäre. Regierungen können heute mit automatischen Systemen den Telefonverkehr fast lückenlos überwachen und nach Schlüsselwörtern oder Stimmen einzelner Personen durchstöbern. Sie können den Datenverkehr im Internet überwachen. Dieses System widerspricht den historischen Grundlagen der Demokratie. Nur durch Verschlüsselungstechnik können wir einen Teil der verlorenen Privatsphäre wieder zurückgewinnen[539].

Zimmerman hatte hierbei staatliche Überwachung im Sinn. Er sollte sich irren: mittels DRMS schlüpfen nun private Contenthersteller in die Rolle des Staates und verwenden ihrerseits Verschlüsselung, nicht aber um den Contentnutzern dienlich zu sein, sondern um eigene Interessen (=urheberrechtlichen Schutz, Profilbildung zur Erlangung von Wettbewerbsvorteilen) im Zuge eigenmächtiger Handlung zu verfolgen. Dass damit zwangsläufig Datenerhebungen einhergehen und der Datenschutz auf der Strecke bleibt, kümmert viele Hersteller nicht. Die technologische Entwicklung spielt geradezu dem Identifizieren von Content, der über DRMS freigeschaltet wird in die Hände. Denn:

---

[536] Nach Lessig, 2001, S. 255.
[537] Vgl. Lessig, 2001, S. 256.
[538] Vgl. Lessig, 2001, S. 260.

4.3. Datenschutz war nicht auf DRMS vorbereitet

Schon 1980 setze Computerisierung ein, was zur Folge hatte, dass Datensammlungen entstanden und die OECD Leitlinien zum Schutz personenbezogener Daten vorgeben musste. Das Ziel: Persönlichkeitsrechte zwar innerstaatlich zu achten, aber auch ungerechtfertigte Hemmnisse beim Transfer grenzüberschreitender Daten abzubauen. Primäre Sorge waren dabei negative ökonomische Effekte durch verschiedene internationale Datenschutzgesetze[540]. Mehr Bedeutung hatte die verbindliche Konvention 108 des Europarates, die im Kern vier Punkte beinhaltete: allgemeine Datenschutzgrundsätze, Regelungen zum grenzüberschreitenden Datenverkehr, Maßnahmen zur gegenseitigen Hilfe und Zusammenarbeit, sowie die Einrichtung eines ständig beratenden Ausschusses. Damit war die Konvention das erste supranationale Datenschutzabkommen für europäische Staaten[541]. Erste Ansätze zur Vereinheitlichung wurden aber erst mit der EG-Datenschutzrichtlinie unternommen, die auch die Charta der Grundrechte der europäischen Union beinhaltete. Darunter ist die Zweckbindung von erhobenen Daten, ein Auskunftsrecht dazu, sowie die Überwachung der Einhaltung durch unabhängige Stellen vorgesehen. Da man bereits die Gefahr der Überwachungsmöglichkeiten durch die Technik erkannte, war der für DRM essentielle Punkt[542] die universelle und technologieneutrale Ausgestaltung[543].

Für Deutschland hat dabei Auskunft nach dem Teledienstegesetz §7 unentgeltlich über zu einer Person oder zu deren Pseudonym gespeicherten Daten zu erfolgen. Genau dies verweigerte man wegen der Aktivierung von Windows XP durch Microsoft. Ein Rostocker Student klagte daher auf Erteilung der Auskunft - zum Urteil kam es nicht, da wohl aus Furcht vor der Justiz die Auskunft dennoch erteilt wurde[544]. Auch ist nicht bekannt, dass im Vorfeld eine Unterrichtung nach §3 Abs. 5 im Vorfeld bezüglich Art, Umfang und Ort der Erhebung erfolgte[545]. Brisant für aktivierungspflichtigen Content ist dabei, dass v.a. Löschverpflichtungen nicht wahrgenommen werden könnten, soll das DRMS korrekt funktionieren. Würde man die

---

[539] Zitat nach: Reischl, 2001, S. 89.
[540] Vgl. Genz, S. 12 ff.
[541] Vgl. Genz, S. 14 ff.
[542] Wenngleich damals DRM, bzw. DRMS noch unbekannte Wörter waren.
[543] Vgl. Genz, S. 17 ff.
[544] Vgl. Arnold Arne: Windows abgeriegelt. In: PC Welt, 02 / 2002, S. 55.
[545] Vgl. Reuscher, 2002, S. 390.

Daten löschen (egal ob pseudonymisiert oder namentlich), dann müssten nutzungsberechtigte Personen jederzeit neue Aktivierungen veranlassen können, was dem Sinne von DRM widerspricht. Kopiervorgänge könnten nicht mehr gesteuert werden. D.h. auch, dass das Transfermedium Internet durch die damit verbundene Globalität ausgenutzt wird, DRMS-transferierte Daten in Drittstaaten speichern zu können. Daher ist Vorsicht geboten, im Vorfeld einen genauen Blick auf das DRMS zu werfen, um zu sehen, ob hier lediglich abstrakte Daten übermittelt werden, die keinerlei Rückschluss auf die Person, sondern nur auf den Content zulassen. Eine Rückführbarkeit auf die Person darf nicht gegeben sein. Werden jedoch, wie Dr. Forgó einräumt in der Mehrzahl der Fälle anstelle abstrakter Daten personalisierte Informationen verlangt, hat dies sehr wohl Implikationen auf die Privatsphäre und den Datenschutz[546]. Somit waren durch das rasante Wachstum in diesem Bereich zwingend Schutzmaßnahmen erforderlich und die Richtlinie erlangte international Bedeutung [547]. Wie lange nun ein Privater die vom DRMS erhaltenen Daten speichern kann, ist noch ungeklärt. Da die Lizenz zur Nutzung von Content ja im Normalfall durch „Kauf“ unbefristet ist, wäre auch der Zweck der Datenspeicherung unbefristet zur Sicherung der Einhaltung der Lizenz. Dieses ewige Speichern von Daten ist sogar länger, als die Vorratsdatenspeicherung für Verkehrsdaten der EU mit Entschließung C6-0293/2005-2005/0182 vorsieht (24 Monate), was bei etlichen Providern Datenmengen von 20.000-40.000 Terabyte verursachen würde – deren Durchsuchung mit derzeitigen technischen Mitteln nähme alleine 50-100 Jahre in Anspruch[548].[549]

4.4. Strategien für den Datenschutz unter DRMS

Lessig fordert einen klaren Regulator für den Cyberspace. Dieser soll nach den US-Gründungsvätern eine Verfassung darstellen, allerdings kein Gesetzestext sein. Was sich kompliziert anhört, wird deutlich, wenn man sich die Architektur vorstellt, aus der der Cyberspace und damit das Internet geschaffen ist – nämlich aus Protokollen. Daraus resultiert eine mächtige Kontrollinstanz: der dahinter steckende Code – und der Code ist

[546] Quelle: Interview mit Dr. Forgó vom 17.02.2006.
[547] Vgl. Genz, S. 22.
[548] Vgl. Störing Marc: Vorratsdatenspeicherung – Beschlossene Sache. In: WCM, Februar 2006, S. 40.
[549] Angesichts dieser Zahlen wundert man sich wirklich, warum DRMS ausgebaut werden, anstatt die Kosten dafür zu sparen und lieber in Vergünstigung des Contents zu investieren. Dies hätte zur Folge, dass gemäß dem klassischen Spiel von Angebot und Nachfrage, die Nachfrage bei günstigerem Preis

auch hier das Gesetz[550]. Dieser Code ist dabei so stark, dass sogar staatliche Institutionen es nicht vermögen, seine Architektur zu modifizieren und damit zu regulieren, allerdings nur, wenn dies vor dem Hintergrund einer weltweiten Architektur des Cyberspace zutrifft. Denn im eigenen Land können sehr wohl gesetzliche Änderungen in diesem Code vorgeschrieben werden – damit ist das Internet auch regulierbar[551] - China praktiziert dies z.B. hervorragend, zeigt aber auch, dass dann etliche Bereiche des Netzes nicht funktionieren. DRMS können nun genau dieser Code sein, denn resultierend aus Lessigs Erkenntnis des starken Codes stellt sich die Frage, ob denn Privatsphäre im Cyberspace beachtet wird[552]. Wesentlich dabei ist, dass hier Konvergenz von bisher zwei getrennten Bereichen im Internet stattfindet, nämlich Fernsehen und Telefon[553] – und genau durch diesen Rückkanal kann der Content interaktiv seine eigene Regulierung überwachen. Beim reinen Fernsehen (oder Radio und gelesenen Texten) war dies bisher nicht der Fall – auch nicht bei Software. DRMS aber erzwingen Datenübermittlung bei Nutzung (Media Player) oder zur Sicherung der Nutzung (Freischaltung von Content).

Sogar banaler Hilfscode in Form von Druckertreibern sendet personenbezogene Daten wie Tintenverbrauch und Anzahl der Druckjobs an Server ins Ausland, was eben nicht datenschutzkonform und geradezu Ausdruck der Mächtigkeit von Code ist[554]. Wie das Magazin PC Welt feststellte, wurden hier auch Daten wie CPU-Typ, Betriebssystem und Grafikkarte mit übertragen – an einer wirksamen Einwilligung und Transparenz für Nutzer mangelt es hier zweifellos[555], besonders dann, wenn Drucker geheime Codemarkierungen mitdrucken, die lediglich für das Mikroskop zu entdecken sind, aber Rückschlüsse auf den Nutzer zulassen[556]. Auch durch „Trap Doors“ in Software lassen sich DRM Profile ohne Wissen des Anwenders erstellen und ermöglichen auch hier Datenrückführbarkeit[557]. Wie das Magazin PC Welt schon im Jahr 2000 erfolgreich

---

steigen würde und die Notwendigkeit zur Raubkopie wegen des dazu erforderlichen Aufwands mit Rippen und Brennen sinken könnte.

[550] Vgl. Lessig, 2001, S. 23 f.
[551] Vgl. Lessig, 2001, S. 100.
[552] Vgl. Lessig, 2001, S. 26.
[553] Vgl. Clement, 2001, S. 29.
[554] Vgl. Nuthmann Thomas: Datenschutzverletzung durch Druckertriber. In: Schneider, 2005, S. I / 117 f.
[555] Vgl. Coppola Richard / Walke-Chomjakov Ines: Spionagetreiben. In: PC Welt, 03 / 2005, S. 118 f.
[556] Vgl. Pilzweger Markus: Drucker-Spionage: Code geknackt. In: PC Welt, 12 / 2005, S. 16.
[557] Vgl. Schneider Jochen: Die Beschreibung des Vertragsgegenstandes bei Standardsoftware-Beschaffung. Schutz vor unliebsamen Überrasschungen durch Sperren oder Beschränkungen? In: Schneider, 2005, S. II / 43.

demonstrierte, ließen sich in verschiedenen Bereichen des Internets eingegebene Daten von Personen zu genauen Profilen verknüpfen. So konnte man Namen wie Telefonnummern ermitteln, gleichsam Beruf und Finanzdaten und sogar Aussagen über den Gesundheitszustand, sexuelle Vorlieben und das Alter machen. Schlimm ist dabei, dass seither immer noch die Transferprotokolle des Internets von damals gelten (TCP / IP)[558]. Noch schlimmer ist, dass beim nächsten Test 2003 nichts daraus gelernt wurde – es fanden sich immer noch Daten und Verknüpfungsmöglichkeiten anhand der Spuren im Internet und diese sind es auch derer sich DRMS bedienen[559]. Nutzungdaten sind dabei geradezu die Bewegungsdaten im Internet (z.B. Sesseion-IDs, temporäre URL, Referrer[560]). Es gilt daher:

4.5. Anonymität ist im Internet nicht möglich

Die Überschrift dieses Kapitels ist eigentlich falsch gewählt: denn Anonymität im Internet gab es schon, allerdings nur, wenn man Zugang zum Netz hatte, ohne personenbezogene Daten bekannt zu geben. Dies war nur mittels Wertkartentelefonen möglich, die man unbeobachtet benützte. Solche anonymen Internet-Zugänge gibt es dank des Telekommunikationsgesetzes (in Kraft seit 26.06.2004) nicht mehr. Telekommunikationsanbieter werden darin gehalten, Kundendaten verpflichtend zu erheben, was letztlich auch der Strafverfolgung aller Art dient (nicht nur Urheberrechtsverletzungen im Online-Bereich)[561]. Im Visier stehen dabei die Provider. Diese sind es ja, die sämtlichen Datenverkehr über ihre Zugangssysteme kontrollieren müssen, um einerseits Abrechnungen der Leistungen durchführen zu können und zwar je nach Zeit oder Datenvolumen[562]. Genau daher liegt es für Contentanbieter auf der Hand, die Nutzungsdaten der Provider zur Verfolgung von Urheberrechtsverletzungen heranzuziehen. DRMS liefern dabei Datensammlungen über Rechtsverstöße, Strafanzeigen und angeordnete Herausgabe der Providerdaten die dahinter stehenden realen Personen.

Da somit je nach Datenschutzbestimmungen des Staates, in dem der Provider seinen Sitz hat, mit mehr oder weniger schwieriger Auskunftserteilung über die

[558] Vgl. Maier Ulrich: Wir wissen alles über Sie. In: PC Welt, 11 / 2000, S. 58 ff.
[559] Vgl. Behrens Daniel: Anti-Spionage-Tipps. Das erfährt man über Sie im Internet. In: PC Welt, 08 / 2003, S. 196 ff.
[560] Vgl. Roßnagel, 2003, S. 153
[561] Vgl. Nuthmann Thomas: Inkrafttreten des neuen TKG. In: Schneider, 2005, S. 169.

jeweiligen Benutzer zu rechnen ist, bieten DRMS auch hier eine ideale Lösungsmethode. Denn die Providerkompetenz im Sinne einer Datenverarbeitung ist immer dann nicht mehr gegeben (und somit auch nicht mehr der nationalen Rechtsprechung unterworfen), wenn der Benutzer einen „Dienst“ aus dem Internet nutzt, der anderenorts angesiedelt ist[563]. D.h. also, man „ködert“ hier Nutzer mit verschiedensten Dienstleistungen, um ihnen reale Personendaten zu entlocken, wie beim Media Player. Der Dienst verbirgt dabei konsequenterweise eine Art Freischaltungssystem des Contentanbieters in einem Staat in dem die Datenschutzgesetze keinen, bzw. wenig effektiven Schutz vor Zugriffen durch Private bieten (also eben die USA). Damit sind die ursprünglichen Vertragsbeziehungen zum (deutschen) Internet-Provider und dessen nationale Datenschutzbestimmungen erfolgreich durch DRM unterwandert. Zu nennen wären hier ferner die Produktaktivierungen von Software, bzw. die Nutzung von US-Downloadportalen im Internet für Musik und Film.

Da das Recht im Internet hier immer den Datenschutz tangiert, hat dies die EU relativ früh erkannt[564]. Fallweise ist aber dennoch anonyme Nutzung möglich, so man z.B. über einen offenen WLAN-Hotspot[565] einsteigt, und dabei die MAC-Adresse der Netzwerkkarte[566], die eigentlich weltweit wie eine IMEI-Nummer eines Handys eindeutig sein sollte, fälscht, was prinzipiell möglich ist[567]. Wirklich anonyme Daten im digitalen Zeitalter wird es aber kaum mehr geben können. Wie Roßnagel anführt, ist dabei auf die Wahrscheinlichkeit abzustimmen, die dabei so gering zu sein hat, dass es nach der Lebenserfahrung oder dem Stand der Wissenschaft praktisch ausscheidet, hier Daten einer Person zuordnen zu können[568].

---

[562] Vgl. Grindl, 1999, S. 67.
[563] Vgl. Grindl, 1999, S. 69.
[564] Vgl. Czychowski Christian: Zusammenhänge und Überblick. In: Bröcker, 2003, S. 27.
[565] Vgl. Bachfeld Daniel: Per Anhalter durchs Internet. In: c´t #13, vom 14.06.2004, S. 92 ff.
[566] Das fälschen der MAC dient dabei lediglich „Sicherheitsgründen“, falls man doch von der Polizei erwischt wird – in allfälligen LOG-Files scheint dann nämlich die gefälschte (sog. gspoofte MAC) auf. Profis konfigurieren Systeme (durch Firewalls oder TCP / IP-Protokolleinstellungen) auch so um, dass sie andere Webbrowser und Betriebssysteme beim Aufruf von Websites melden (natürlich handelt es sich um Seiten, mit brisanten Inhalten wie raubkopiertem Material). Verantwortlich ist dabei dann primär der WLAN-Betreiber und nicht der Hacker. Selbstverständlich sollten die Änderungen am System (falsche MAC, falsch gemeldeter Browser und Betriebssystem) nach jedem erfolgreichen WLAN-Einbruch wieder rückgängig gemacht werden, um hier tatsächlich keine Rücksschlüsse auf den verwendeten Laptop ziehen zu können (die Primärwaffe beim Suchen von offenen WLANs).
[567] Vgl.Mizgalski Markus / Teetz Tobias: Filme & MP3s unerkannt laden. In: PC Praxis, 06 / 2006, S. 70.
[568] Vgl. Roßnagel, 2003, S. 150.

4.6. Datenschutz in Deutschland

Konkret verankert ist in Deutschland die Privatsphäre im Grundgesetz. Für DRM ist besonders die Unverletzlichkeit der Wohnung, das Brief-, Post- und Fernmeldegeheimnis relevant[569], da in der Regel vom PC in der Wohnung über öffentliche Netze Daten übertragen werden. Richtungsweisend war dabei das Volkszählungsurteil, aus der sich die informationelle Selbstbstimmung herleitet[570]. Man hat zwar keine grundsätzliche Herrschaft über „seine“ Daten, allerdings eben die Entscheidungsfreiheit über vorzunehmende und zu unterlassende Handlungen – somit wird hier durch die Verfassung ein eigentumähnliches Informationsbeherrschungsrecht konstruiert[571]. Bereits hier steckt der Widerspruch zu DRMS. Denn durch diese wird genau dieses Recht ausgehöhlt – nicht der Nutzer daheim, sondern der Urheber in der Ferne bestimmt, welche Informationen er erhalten will – das DRMS sendet sie ihm. Wichtige Gesetze zur Wahrung des Datenschutzes sind dabei das Bundesdatenschutz-, das Teledienstedatenschutz-, das Telekommunikationsgesetz und der Mediendienstestaatsvertrag, sowie diverse Verordnungen dazu[572]. Die wichtigsten Regelungen finden sich in beiden Ersteren. Für das Internet bedeutsamer ist dabei das TDDSG, da der MDStV für Mediendienste unter Benutzung elektromagnetischer Schwingungen gilt (also vornehmlich Rundfunk). Im Kern enthalten beide Gesetze allerdings nahezu wortgleiche Regelungen[573].

In Deutschland ist die Zweckbindung von Datenerhebungen im TDDSG vorgesehen. Prinzipiell ist somit vor einer Datenerhebung die Einwilligung des Nutzers erforderlich. Diese kann auch über elektronische Signaturen erfolgen, darf aber nicht damit gekoppelt sein, Daten zwecks Zugangserlangung zu einem Dienst zu Werbe- und Marketingzwecken zur Verfügung zu stellen [574] - genau dies ist bei DRM regelmäßig nicht möglich. Da die Signatur einer handschriftlichen Unterschrift gleichzustellen und in Gerichtsverfahren Beweiskraft hat[575], birgt deren Manipulation etliche Gefahren –

[569] Vgl. Genz, S. 8.
[570] Vgl.Bröcker Klaus Tim: Schutz des Nutzers im Netz: Datenschutz und Datensicherheit. In: Bröcker, 2003, S. 236.
[571] Vgl. Born, 2001, S. 62.
[572] Vgl. Bröcker Klaus Tim: Schutz des Nutzers im Netz: Datenschutz und Datensicherheit. In: Bröcker, 2003, S. 235.
[573] Vgl. Roßnagel, 2003, S. 125 f.
[574] Vgl. Roßnagel, 2003, S. 160 ff.
[575] Vgl. Reischl, 2001, S. 80.

eine digitale Signatur ist ja technisch betrachtet nichts anderes als digitaler Content[576]. Genau die Einwilligung ist bei der Mehrzahl an bezogenem US-Content in Deutschland infolge der US-Click-Wrap Agreements nicht gegeben, da sie nach deutschem Recht unwirksam sind. Somit mangelt es auch an einer Rechtsgrundlage für solcherart automatisierter Datenerhebungen[577]. Beheben lässt sich diese Unwirksamkeit noch über Ankreuzen einer entsprechenden Einwilligung auf der Website, was allerdings schon an Nötigung grenzt, da es ansonsten keine Contentfreischaltung gibt. Weiters dürfen Daten nicht über den Zweck der Erhebung hinausgehen (z.B. ist es nicht erforderlich, Hobbys und Anzahl der Kinder eines Nutzers zu erfragen, wenn dieser nur Musik downloaden möchte). Lediglich peseudonymisierte Nutzerprofile dürfen dabei verwendet werden, bei denen Personenbezug nicht hergestellt werden kann und letztlich ist bei der Verarbeitung von Daten ein Widerspruchsrecht vorzusehen, auf das im Vorfeld hinzuweisen ist[578].

Diese Rechte zielten allerdings mehrheitlich auf staatliche Stellen und Telediensteanbieter, nicht jedoch auf Contenthersteller, besonders durch das Aufkommen von Großrechenzentren aus der Furcht vor dem allmächtigen Staat. Diese Abwehrrechte haben sich nun gewandelt, da Abwehrrechte gegen Private bedeutsamer wurden, denn es fand und findet immer noch die Transformation hin zu privaten Serverrechnern mit privaten Datensammlungen statt. Die Datenschutzgesetze der ersten Generation waren auf diese Herausforderungen nicht vorbereitet, wenn Daten privat organisiert werden. Somit ist die heutige Auffassung von Datenschutz erweitert um den Schutz vor privaten Datensammlungen[579]. Damit kollidieren aber zwei unterschiedliche Verfassungsinteressen: der Schutz geistigen Eigentums als Quasiverfassungsrecht - der vermögensrechtliche Aspekt ist dabei vollständig durch Art. 14 des deutschen GG gedeckt - und das Recht auf informationelle Selbstbestimmung des allgemeinen Persönlichkeitsrechts. Die große Frage dabei ist, wie viel man von dem einen beschneidet, um den anderen Bereich zu stärken. Anders ausgedrückt: reguliert man

[576] Und damit unterliegt die digitale Signatur sämtlichen Angriffsmethoden auf DRMS, die im Implementierungsteil gezeigt wurden.
[577] Vgl. Bröcker Klaus Tim: Schutz des Nutzers im Netz: Datenschutz und Datensicherheit. In: Bröcker, 2003, S. 242.
[578] Vgl. Bröcker Klaus Tim: Schutz des Nutzers im Netz: Datenschutz und Datensicherheit. In: Bröcker, 2003, S. 244.
[579] Vgl. Bröcker Klaus Tim: Schutz des Nutzers im Netz: Datenschutz und Datensicherheit. In: Bröcker, 2003, S. 236 f.

hier an einer Stelle mehr, unterreguliert man den anderen Bereich – ein Dilemma in dem sich der Gesetzgeber ständig befindet[580]. Eine Art Interessenausgleich ist bisher nicht geschaffen. Das BDSG ermöglicht es allerdings auf freiwilliger Basis durch staatlich zugelassene Prüfer die Datenverarbeitungsanlagen entsprechender Stellen und das zugehörige Konzept zur Verarbeitung von Daten einer Überprüfung zu unterziehen[581]. DRMS verstärken dabei in doppelter Hinsicht beide Rechtsgebiete zu Ungunsten der Nutzer. Beim Urheberrecht werden sie um die Schrankenbestimmungen beschnitten, beim Datenschutz in ihren Grundrechten verletzt. Abwehrrechte können kaum geltend gemacht werden, da die Datensammler hauptsächlich in Staaten angesiedelt sind, die nicht vom deutschen Datenschutzrecht betroffen sind – eben vornehmlich die USA (Windows, Hollywood, internationale große Plattenlabels) als eine Folge der Amerikanisierung der Gesellschaft.

Einen Versuch zur Regulierung diesbezüglich stellen die sog. Safe Harbour Priciples als Antwort zur Einhaltung von Datenschutzbestimmungen der EU in Staaten dar, wo diese Standards niedriger sind. So soll EU-Datenschutzniveau in den USA für übermittelte Daten aus Europa gelten, ganz so, als ob diese Daten innerhalb Europas transferiert werden[582]. US-Unternehmen – so der Wunsch – unterwerfen sich dabei durch „Selbstzertifizierung“ den Bestimmungen des Safe Harbours[583]. Fraglich ist allerdings, wie sich das liberale US-Wirtschaftssystem mit geforderter Zurückhaltung staatlicher Eingriffe mit den Ansichten der EU bezüglich Datenschutz verträgt. Hingewiesen werden soll hier auf die Tatsache, dass international weniger Verfahren bezüglich Datenschutz- denn Urheberrechtsverletzungen anhängig sind. Für die „Transferleistungserbringung“ von Providern gilt dabei das TDDSG. Dieses enthält weltweit als einziges Gesetz spezielle Vorschriften bezüglich Nutzerprofilen[584]. Konkret werden unter Telediensten sämtliche elektronischen Informations- und Kommunikationsdienste verstanden, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bildern oder Tönen bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt – so die Def. des § 2 Abs. 1 TDG – daher gilt dies auch für Content-Freischaltung über DRMS durch Private. In

[580] Vgl. von Diemar, 2002, S. 48 f.
[581] Vgl. Genz, 2004, S. 113.
[582] Quelle: Interview mit Dr. Forgó vom 17.02.2006.
[583] Vgl. Genz, 2004, S. 152.
[584] Vgl. Fröhle, 2003, S. 71.

Summe gesehen existieren somit in Deutschland weit ausgestaltete Regelungen von Seiten des Gesetzgebers, d.h. also, es herrscht keine Selbstregulierung vor, allerdings nur für Deutschland. So verwundert es nicht, dass die Mehrzahl an DRMS trotzdem Profile sammeln und verknüpfen können, weil die Daten eben nicht in Deutschland gespeichert werden.

4.7. Gütesiegelprogramme und Safe Harbour Principles

Um mangelnden Datenschutz abzufedern und Vertrauen von Nutzern in ihre DRMS zu erhalten, gehen Hersteller verschiedene Wege. So ließ Microsoft z.B. sein Windows XP vom TÜV in Hinblick auf die Produktaktivierung überprüfen, wohlgemerkt allerdings mit selbst entwickelten Diagnosetools. Wichtiger aber sind echte Gütesiegel, wie die Safe Harbour Principles, die für Übermittlung personenbezogener Daten in Drittstaaten nach Art. 25 Abs. 1 der EG-Datenschutzrichtlinie angemessenes Schutzniveau gewährleisten sollen. Die Übernahme der SHPs erfolgte dabei ins Gemeinschaftsrecht durch die Entscheidung der Kommission [2000/520/EG] vom 26.07.2000. Dies ist insofern brisant, als bis zu diesem Zeitpunkt schon fleißig durch Windows-XP und Media Player Datenprofile auf US-Servern gesammelt werden konnten. Insofern war der Schritt Deutschlands verständlich, die Bundeswehr auf Einsatz von US-Software zwangsverzichten zu lassen. Der Grund: der sog. NSA-Key, bei dem es sich um einen bis heute nicht geklärten Verschlüsselungsalgorithmus der US-National Securty Agency in Windows handelt. Befürchtet wird, dass dieser dazu dient, sämtliche gesammelten Daten zu protokollieren und für US-Interessen zu nutzen[585].

Das Vertrauen in DRMS in Deutschland ist somit genau wie in Europa generell nicht so hoch, wie in den USA[586]. Die Angst liegt hier zweifellos in der omnipräsenten Überwachung. Strafverfolgung ist nämlich auf zwei Arten möglich: reaktiv und präventiv[587]. Bisherige DRMS waren bloß reaktiv, d.h. also, erst bei einem konkreten Verstoß wurden sie aktiv. Neuere DRMS dagegen arbeiten permanent und führen ständige Überwachungen der Aktivitäten eines Endgerätes, bzw. PCs durch (=z.B. Rootkits) – genau im Sinne der TCPA-Architektur. Hier können zwar staatliche Stellen die Herausgabe von Generalschlüsseln erzwingen, allerdings ist der einzelne Nutzer

[585] Vgl. Reuscher, 2002, S. 388.
[586] Vgl. Lejeune Mathias: Protection under US Copyright Law. In: Becker, 2003, S. 381.
[587] Vgl. Lessig, 2001, S. 279.

nicht vor Datenschutzverstößen sicher. Lessig hat dies korrekt erkannt, da Verschlüsselung das Problem somit nicht löst[588] – im Gegenteil: es wäre sogar geradezu verlockend, hier trügerische Sicherheit anzunehmen und möglicherweise mehr Daten preiszugeben, als eigentlich erforderlich wären. Dr. Forgó räumt hier auch ein, dass es trotz SHPs eine sehr große Anzahl an Unternehmen gibt und die Hauptschwierigkeit darin besteht, ob deren Verständnis von Datenschutz mit dem der EU kompatibel ist. Zudem bestehen noch zu wenige Erfahrungen mit der Einhaltung des Datenschutzes nach den SHPs – allerdings sind die SHPs zumindest besser als nichts[589].

Konkret gehört nun zu Datenschutzgütesiegeln adäquate Betriebsorganisation und Beachtung von Verbraucherbestimmungen[590]. Mehr Vertrauen in SHPs lässt sich über zusätzliche Gütesiegelprogramme erreichen. Deren Ziel ist es, Drittstellen zur Zertifizierung und Zusicherung der Einhaltung von Datenschutzstandards heranzuziehen. Da die SHPs diese Funktion jedoch auch übernehmen, kann zumindest von einem Grundgütesiegel in den USA gesprochen werden, deren Name jedoch EU-Datenschutzgütesiegel hätte sein sollen. Der Lohn der freiwilligen Unterwerfung unter SHPs ist die Aufhebung der Beschränkung des Datentransfers. Fraglich bleibt dabei, wie dies zu kontrollieren wäre, denn Safe Harbour ist nicht verbindlich[591], so auch Dr. Forgó, da bei weitem nicht alle Unternehmen Mitglied der SHPs sind[592]. Genz folgend ist zudem auch das Enforcement nicht sichergestellt[593]. Andere Gütesiegelprogramme werden dabei in den USA auf freiwilliger Basis unabhängig von SHPs auch untereinander betrieben. Arbeitet man hier nach einem dieser Verfahren, so kann sich das jeweilige Unternehmen mit einem entsprechenden Etikett (sog. Trustmark) auf der Website schmücken. Dem Nutzer bleibt allerdings vorbehalten, wie glaubhaft ein derartiges Etikett ist. Allerdings kann auch unter den SHPs die Angemessenheit nicht hinreichend bestimmt werden – da es US-Unternehmen nur im Zuge der Selbstverpflichtung obliegt, was konkret Bestandteil ihrer Privacy Policy ist. Und nur dann, wenn diese Grundsätze gegenüber den Betroffenen bekannt gemacht werden, ist die Selbstverpflichtung auch wirksam[594].

---

[588] Vgl. Lessig, 2001, S. 278.
[589] Quelle: Interview mit Dr. Forgó vom 17.02.2006.
[590] Vgl. Nuthmann Thomas: Datenschutzzertifikat für Online-Dienste. In: Schneider, 2005, S. I / 69.
[591] Vgl. Genz, 2004, S. 162.
[592] Quelle: Interview mit Dr. Forgó vom 17.02.2006.
[593] Vgl. Genz, 2004, S. 167 ff.
[594] Vgl. Genz, 2004, S. 166.

Einen Interessenabgleich zwischen den Praktiken des jeweiligen Unternehmens und den Nutzern soll der Standard Platform for Privacy Preferences (P3P) wahren[595]. Die P3P-Architektur ist prinzipiell genau das, was Lessig auch fordert: einen starken Code als Regulator für Datenschutz – aber jetzt kommt der Pferdefuß: nicht im Moment, da Lessig einräumt, dass es bisher ungelöste Probleme gibt. Denn hier läge sowohl Urheberrecht wie Datenschutz wieder in einer Hand (dem Code). Ob Lessigs Wunsch nach Wahlfreiheit über den Umgang von Daten somit jemals vertretbar sein wird, sei angezweifelt[596]. Daher kommt er zum Ergebnis, dass Selbstregulierung im Datenschutzbereich letztlich fehl am Platze ist[597]. Dem wäre jedoch insoweit zu widersprechen, als staatliche Regulierung in diesem Bereich wie bei den Urheberrechten gezeigt wurde nur eine Reaktion auf technische Entwicklungen sein kann und der Staat selbst Interesse an Daten zur Strafverfolgung hat. Selbstregulierung durch unabhängige Datenschutzorganisationen, bzw. Open Source könnte somit besser sein, würde aber erst einmal die Überwindung der Dominanz der derzeitigen DRMS am Markt erfordern. Es ist somit auch hier etliches strittig und ungelöst.

4.8. Datenschutz in den USA

In den USA hat sich der Begriff „Privacy“ für ein Konglomerat an gebündelten Rechten der US-Verfassung durchgesetzt. Zwar ist der Datenschutz basierend auf dem vierten Verfassungszusatz der USA von 1791 auch ein Grundrecht, der sich aus dem Recht auf Sicherheit der Person, Häuser, Unterlagen und Eigentum herleitet, dieser Grundrechtsschutz trifft aber nur staatliches Handeln vor willkürlicher Verletzung der Privatsphäre. Abgestimmt wird dabei auf einen rechtfertigenden Grund zur Verletzung von Eigentumsrechten[598]. Private sind generell nicht erfasst, was in der Konzeption der US-Verfassung begründet liegt[599]. Interessant ist der internationale Pakt über bürgerliche und politische Rechte von 1966 – besonders Artikel 17, der die Erklärung der Menschenrechte über willkürliche Eingriffe in das Privatleben konkretisiert und dem Gesetzgeber rechtliche Schutzpflichten auferlegt. Sowohl in den USA wie Deutschland findet der Pakt Anwendung, wobei allerdings die USA von umfassenden

[595] Vgl. Roßnagel, 2003, S. 105.
[596] Vgl. Lessig, 2001, S. 282 f.
[597] Vgl. Lessig, 2001, S. 288.
[598] Vgl. Genz, S. 44 ff.
[599] Vgl. Genz, S. 49.

Beschränkungsmöglichkeiten Gebrauch machten[600]. Die US-Regierung stellt Rahmenbedingungen für Datenschutz durch einen sog. Verhaltenskodex zur Verfügung[601]. Diese Codes of Conduct sind dabei im Gegensatz zu deutschen Gesetzen aber nicht verbindlich – im Gegenteil sie untermauern das liberale Prinzip der Selbstregulierung in den USA[602]. Dies verwundert aber nicht: „Industry in the United States has long argued strenuously for self regulation of information practices.[603]“ Somit hat die US-Industrie selbst Zurückhaltung von Seiten des Staates gefordert. Im Zeitalter von DRMS ist diese Forderung jedoch nicht mehr haltbar, da es abgesehen von z.B. Wahlwerbespots für politische Parteien und im Auftrag der US-Regierung geschaffener (kostenloser) Computerspiele[604], hauptsächlich Private sind, die Content jeglicher Art schaffen.

Private spionieren aber auch vielfach mit staatlicher Erlaubnis. Gegen (geringe) Geldbeträge erfährt man in den USA durch die State Licensed Private Investigators alles, wie z.B. Kontostände von Konkurrenten, Kennzeichenhalter zu Fahrzeugen, Verwaltungsstrafen oder Geheimnummern[605]. Benachrichtigungs-, Auskunfts- und Berichtigungsansprüche, sowie Schadenersatzrechte gegenüber Behörden und den Schutz vor Zweckentfremdung von Daten gibt es prinzipiell auch in den USA seit dem Privacy Act 1974, allerdings hat dieses Thema in den USA an Aktualität verloren[606]. Dies umso mehr, als nach den Terroranschlägen vom 11.09.2001 Oracels CEO Larry Ellison an Justizminister John Ashcroft herantrat und ihm Software zur Erstellung einer eindeutigen Amerikanischen National-ID anbot. Allerdings war dies eher als Sensibilisierung der Öffentlichkeit für massive Einschränkungen beim Datenschutz zu werten, die faktisch schon durch Führerschein- und Sozialversicherungsnummern gegeben war und damit Ausdruck reinster Kommerzialisierungsinteressen durch Datenverarbeitungsanlagen samt Software ist[607]. Nach dem 11.09.2001 wurden die bereits bis dahin kaum bestehenden Datenschutzgesetze weiter beschnitten, was auch von etwa 2/3 der Amerikaner so befürchtet wurde: Bürgerrechte zum Preis erhöhter

[600] Vgl. Genz, S. 10 f.
[601] Vgl. Lessig, 2001, S. 281 f.
[602] Vgl. Genz, 2004, S. 90.
[603] Zitat nach: Schwartz, 1996, S. 216.
[604] Z.B. America´s Army.
[605] Vgl. Reischl, 2001, S. 93.
[606] Vgl. Tinnefeld, 1998, S. 39.
[607] Vgl. Parenti, 2003, S.84 f.

Sicherheit auszuhöhlen[608]. 2001 war aber genau das Jahr in dem Windows XP erschien und DRMS ihre massenhafte Verbreitung fanden. Deutlich wird somit, dass beim Datenschutz neben den Urheberrechten (Umsatzsteuer am Content, gesellschaftliche Weiterentwicklung) auch großes Interesse staatlicher Seite vorliegt und daher kaum Entspannung beim Sammeln von Daten zu erwarten ist.

Die Interessen und mangelnden Datenschutzbestimmungen der USA merkt man z.B. auch beim Online-Auktionshaus eBay. Hier wird in den AGB geregelt, dass Nutzer der Verarbeitung von Daten ausdrücklich zustimmen. In den USA hat somit das FBI unter dem Deckmantel der Terrorbekämpfung uneingeschränkten Zugriff auf sämtliche Geschäftstätigkeiten aller weltweit über eBay abgeschlossenen Transaktionen, was nach US-Recht auch völlig legal ist[609]. Dennoch gehörte neben dem hessischen Landesdatenschutzrecht für Deutschland der US-Privacy-Act von 1974 zu den weltweit ersten Datenschutzbestimmungen. Damit wurden erstmals gesamtstaatliche Regelungen für den Privacyschutz als Abwehr staatlicher Eingriffe zur Abwehr unbegründet durchgeführter Datensammlungen von Personen geschaffen[610]. Schutz für die Probleme durch DRM war damals aber noch ein Fremdwort. Sogar heute ist die im zehnten Zusatzartikel der Verfassung geregelte Gesetzgebungskompetenz bei der Vereinheitlichung bundesstaatlicher Datenschutzvorschriften immer noch hinderlich – sie fehlen nach wie vor. Das Ergebnis ist, dass die Bundesstaaten unterschiedliche Datenschutzvorstellungen von Privat zu Privat haben und die Entwicklung von Schutzbestimmungen bisher schleppend bis überhaupt nicht lief[611]. Daher konnte sich mehr und mehr Selbstregulierung etablieren, was aber auch daran liegen mag, dass Datenschutz durch Verrechtlichung umständlich und unhandlich würde. Dann wäre er sowohl von Datenverarbeitern als auch den Betroffenen mehr als Belastung denn als Gewinn gesehen[612].

Auch hier vermögen DRMS Abhilfe schaffen, da eine Verrechtlichung dabei zwar fehlt, allerdings die Transformation von Staatlichkeit hin zum Contentanbieter stattfindet. Die Regulierungsmacht wird nämlich diesem in die Hand gegeben. Dabei entsteht durch Kommunikation bei Aktivierungen und Registrierung von Content eine

---

[608] Vgl. Parenti, 2003, S.184.
[609] Vgl. Kranz Kim: FBI spioniert bei eBay. In: Chip, 05 / 2003, S. 200
[610] Vgl. Genz, 2004, S. 50.
[611] Vgl. Genz, 2004, S. 57 f.
[612] Vgl. Genz, 2004, S. 183.

Datensammlungsgefahr, die neben klassischen personenbezogenen Daten auch pseudonymisierte E-Mail-Adressen beinhaltet[613]. Genau solche lassen sich dann durch Verknüpfung anhand der von Fröhle genannten Identifizierungsmerkmale einer Person zuordnen. Aggressive Vorgehensweisen in diesem Bereich durch US-Unternehmen bei der Vermarktung von Content führt dabei schon dazu, dass in der Bevölkerung in dieser Hinsicht Angst vor dem Verarbeiten ihrer Daten durch die Industrie vorherrscht: „A significant portion of the Amrican public no longer has confidence in the way industry treats personal information." Tatsächlich sind 40% der Amerikaner der Meinung, kommerzielle Interessen gefährden deren Daten mehr, als die Regierung[614]. Untermauert wird dies durch sehr wenige Spezialvorschriften wie z.B. den Video Privacy- oder den Drivers Privacy Protection Act. Damit sind dann Videoverleih- oder Führerscheindaten der KFZ-Zulassung geschützt, aber sensible Bereiche wie Gehaltsdaten, Daten zum Gesundheitswesen oder auch Telekommunikationsdaten nicht[615] – und genau letztere zählen zum Bereich der bekannten Netzinfrastruktur, auf die die Internet-Webtechnologie aufsetzt und die sich für das Funktionieren von Online-Freischaltungen von Content via DRMS verantwortlich zeichnet. Daher gilt:

4.9. Bekannte Webtechnologien: (aus)genutzt durch DRMS

Das Überwachungspotential heutiger Technik drückt Lessig folgendermaßen aus: „Damals verzeichnete man nur Ungewöhnliches, heute alles.[616]" Somit verwundert es nicht, dass 92% von kommerziellen Websites Datenprofile ihrer Nutzer sammeln[617]. Durch DRM muss sich der Contentrezipient nicht einmal mehr bewusst auf der jeweiligen Website des Urhebers einloggen, da das DRMS dies ohne Wissen vollautomatisch erledigt. Besonders bei Aktivierung von Software bei sonstiger Programmsperre ist dies nur unter ausdrücklicher vertraglicher Vereinbarung gestattet. Somit muss der Hersteller auf eine Programmsperrfunktionen vor Erwerb der Nutzungsberechtigung deutlich hinweisen[618]. Wenn aber eine Sperre unter diesem Gesichtspunkt aktiv werden sollte, so tritt diese vielfach nach Ausnutzung der

[613] Vgl. Genz, 2004, S. 69 f.
[614] Zitat nach: Schwartz, 1996, S. 215 f.
[615] Vgl. Genz, 2004, S. 126.
[616] Zitat: Lessig, 2001, S. 267.
[617] Vgl. Lessig, 2001, S. 272.
[618] Vgl. Martens Silke: Produktaktivierung als Sachmangel. In: Schneider, 2005, S. I / 20.

klassischen Transferinfrastruktur des Internets in Kraft (z.B. illegalen Content entdeckt), aber auch durch Zeitablauf, d.h. sollte man zwecks Freischaltung innerhalb einer vorgegebener Zeitspanne diese (technischen) Strukturen zu beanspruchen verweigern[619]. Somit muss man sie zwangsweise nutzen. Gängige DRMS verstoßen daher in fast allen Punkten gegen das von Hansen angeführte Datenschutz 1x1 (Zulässigkeit, Erforderlichkeit und Datensparsamkeit, Zweckbindung, Betroffenenrechte, Datensicherheit, sowie Transparenz). In folgender Tabelle werden einige Möglichkeiten gezeigt, wie DRMS i.d.R. mit den einzelnen Punkten umgehen. Lediglich im Bereich der Datensicherheit herrscht volle Unterstützung, da dies geradezu den eigenen Interessen der Contentanbieter dient[620].

was	**soll eigentlich was bewirken**	**DRMS dagegen bewirkt**
Zulässigkeit	Datenverarbeitung wenn gesetzlich vorgeschrieben oder Betroffene/r einwilligt	DRMS stehen in keinem Gesetz / vieles geschieht automatisch und ohne Rückfrage
Erforderlichkeit und Datensparsamkeit	Daten nur auf erforderliches Maß beschränken	Mehr Daten übertragen als erforderlich (z.B. Aktivierungsdaten, Media Player, diverse Windows XP-Funktionen wie Fehlerberichterstattung, Zeitsynchronisation, o.ä.)
Zweckbindung	Personenbezogene Daten dürfen nur für den erhobenen Zweck verwendet werden	Wiedererkennung bei Rechtsverstößen und Contentsperre → kein Gericht involviert
Betroffenenrechte	Unterrichtungs-/ Einwilligungs- / Widerspruchs- / Auskunfts- / Richtstellung- / Sperr- / Löschrechte	Übertragung in andere Staaten, bzw. zu anderen Servern → nationales Recht greift nicht – kaum Hinweise auf Ansprechpartner und Speicherorte von Daten
Datensicherheit	Für personenbezogene Daten angemessene Sicherheitsmaßnahmen für Verarbeitungsverfahren treffen	wird im eigenen Interesse erfüllt, damit Daten zu kommerziellen Zwecken genutzt werden können, aber auch zur Verfolgung von Urheberrechtsverstößen
Transparenz	nur informierte Einwilligung wirksam / Datenverarbeitungsverfahren darstellen (=offen legen)	selten / Datenverarbeitungsverfahren offen legen würde Quellcode, bzw. Contentoffenlegung bedeuten oder zu viele technische Details beinhalten

Tabelle 7: Unterminierung des Datenschutzes durch DRMS[621]

[619] Vgl. Bechtold, 2002, S. 259.
[620] Vgl. Hansen Martin: Auf dem Weg zum Identitätsmanagement –von der rechtlichen Basis bis zur Realisierung. In: Bäumler, 2003, S. 198 f.
[621] Eigene tabellarische Darstellung der von Hansen erläuterten Probleme - Spalte drei wurde diesen um die bisherigen Erkenntnisse dieser Arbeit hinzugefügt.

Wie folgende Abbildung zeigt, fallen nun für Nutzerdaten im Internet erhebliche Möglichkeiten der Profilbildung an. Diese Art des Ausspionierens von Konsumverhalten gab es zwar schon früher, gepaart mit DRM muss man sich hier jedoch vorstellen, dass nicht der Nutzer es ist, der den Datenfluss im Internet steuert, sondern das heimlich operierende DRMS die Rolle des Nutzers übernimmt.

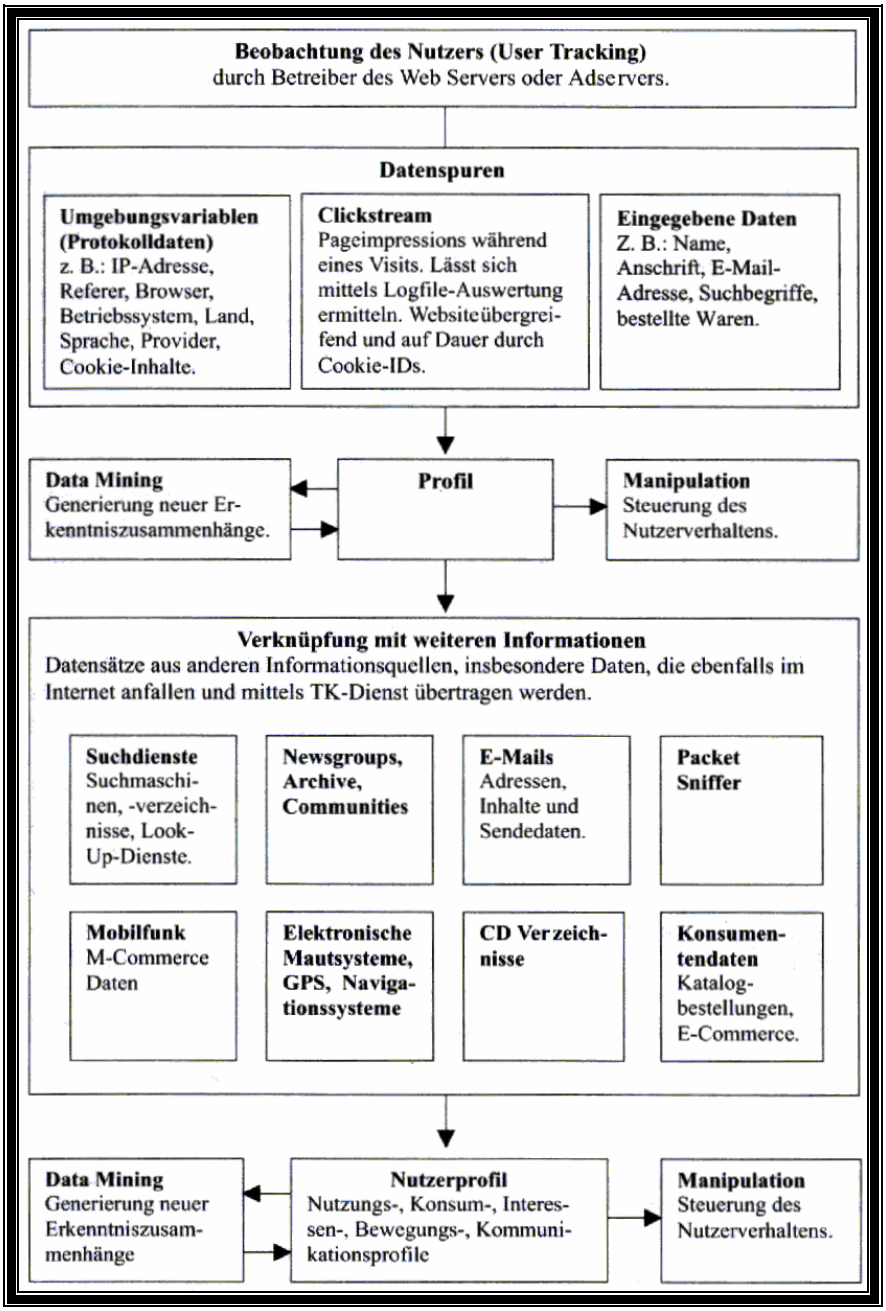

Abbildung 24: Klassische Spuren im Internet als Datensammlungsgrundlage für „wirkende DRMS“[622]

[622] Aus: Fröhle, 2003, S. 65.

Nachfolgend werden die wichtigsten Punkte behandelt und gezeigt, warum DRMS „davon profitieren“:

4.9.1. IPv4 ermöglichen sie, IPv6 sind sie: GUIDs

Da das Internet derzeit mit dynamischen IP-Adressen arbeitet, sind eindeutige Nutzerprofile noch nicht möglich. Dynamische IP-Adressen können ja von mehreren Personen geteilt werden. Der Grund ist, dass das Internet auf dem IPv4-Prtokoll basiert, d.h. es stehen nicht genug Adressen für alle Erdbewohner zur Verfügung. Daher werden diese Adressen dynamisch beim Einloggen zugewiesen. Kernstück der Datenermittlung ist die IP-Adresse über die jeder teilnehmende Internet-Rechner verfügt. Sie funktioniert somit ähnlich einer Telefonnummer anhand derer sich ein Anschluss ausforschen lassen[623]. Somit ist zwecks Personenbezug eine Auskunft der Provider über dessen Logfiles erforderlich, will man einen Nutzer identifizieren. Ohne Auskunft kann ein Diensteanbieter, sofern es sich nicht um den Provider selbst handelt, anhand einer dynamischen IP-Adresse nicht einmal einen Rechnerbezug[624] herstellen und die Person dahinter schon gar nicht identifizieren[625]. Mit dem neuen IPv6-Protokoll soll sich dies ändern – jedem Erdbewohner kann dann eine eigene IP-Adresse auf Lebenszeit zugewiesen werden so wie ein Personalausweis. Werden diese Daten dann wie derzeit in der RIPE-Datenbank Domaininhaberdaten gespeichert, ist jeder Internet-Teilnehmer identifizierbar.

Technischer Hintergrund war bei IPv4, dass die IP aus 32 Bit gebildet wurde, was somit 2^{32}, also etwa 4,3 Mrd. Adressen ermöglichte – und das reicht nun einmal nicht mehr aus. Mit den geplanten 128 Bit des IPv6 und 2^{128}, also 3,402823669209384634633746074317e+38 Möglichkeiten der Adressvergabe dürfte für den Rest der Existenz der Menschheit ausgesorgt sein – es ist sogar möglich jeden Erdbewohner mit einer Vielzahl an IP-Adressen zu versorgen[626]. Fröhle spricht in diesem Zusammenhang davon, dass die Ablösung der ehemaligen dynamischen IP-Adressen die Funktion eines GUIDs (Globally Unique Identifiers) übernehmen

[623] Vgl. Antoine Ludwig (u.a.): IP-Adresse als „andere Kennung“ eines TK-Anschlusses. In: Schneider, 2005, S. II / 56.
[624] V.a. wenn der Nutzer hinter einem sog. Proxy-Server des Providers „sitzt“.
[625] Vgl. Bröcker Klaus Tim: Schutz des Nutzers im Netz: Datenschutz und Datensicherheit. In: Bröcker, 2003, S. 241.
[626] Vgl. Fröhle, 2003, S. 99.

könnte[627]. Sicherlich wäre noch abzuwarten, wie dies im Detail gelöst wird, da es eine Vielzahl an Providern gibt, die nur über einen begrenzt zugewiesenen Adresspool verfügen, d.h. ob denn die neue IPv6-Adresse sich beim Providerwechsel ändert, oder wie bei der bereits jetzt möglichen Rufnummernmitnahme beim Telefon dem Nutzer weiterhin erhalten bleibt. Sicher ist aber, dass man mit IPv6 einfach im Internet zu identifizieren ist, sollte eine namentliche Registrierung von Content, bzw. eine Aktivierung erfolgen. D.h. also, mit IPv4 konnte man bei Bedarf identifiziert werden, mit IPv6 ist man dagegen automatisch identifiziert. Profile lassen sich dann eindeutig einer Person zuordnen - eine Lösung wäre lediglich die Beibehaltung von dynamischer IP-Vergabe auch unter IPv6, bzw. die Nutzung von IPv6-Adressen durch mehrere Personen, so wie auch bei KFZ-Kennzeichen die Person des Lenkers nicht mit dem Fahrzeughalter identisch sein muss. Ob sich dieser Vorschlag durchsetzt, darf angesichts der Cyber-Straftaten bezweifelt werden. So kann entweder der hinter einer IP-Adresse steckende Domain-Name oder Abteilungsname in Firmen Aufschluss darüber geben, wer sich tatsächlich hinter einer IP verbirgt. Gibt der Nutzer dann noch irgendwo seinen realen Namen ein, kann keinesfalls mehr von pseudonymisierten Daten gesprochen werden[628].

Die Identifizierungsmöglichkeit beginnt hier bei den Schnittstellen eines durch DRM genutzten E-Commerce-Systems, das IP-Adressen speichert. Dadurch lässt sich der Provider ermitteln. Dieser könnte nun den Nutzer ausforschen und anhand seiner Zahlung für die Dienste des Providers (Entgelt) durch das Geldinstitut eindeutig zuordnen (anonyme Konten sind in Deutschland nicht gestattet)[629], oder auf allfällige Ausweisdaten bei der Diensteanmeldung zurückgreifen. Somit ist anonymer Online-Bezug von Content ein Widerspruch in sich. Lediglich der rechtliche Datenschutz hindert Provider noch daran, Auskünfte über hinter IP-Adressen steckenden Personen zu geben. Somit müssen sich Contentanbieter auf ihre DRMS verlassen, die Profile sammeln. Die gewonnenen Daten werden dann eben im Anschluss verknüpft. Zur allfälligen Strafverfolgung ist zwecks Überwachung und Auskunft ja ein Richterbeschluss zur Herausgabe von Verbindungs- und Nutzungsdaten erforderlich[630].

---

[627] Vgl. Fröhle, 2003, S. 42.
[628] Vgl. Roßnagel, 2003, S. 155.
[629] Vgl. Bizer Johann: Das Recht auf Anonymität in der Zange gesetzlicher Identifizierungspflichten. In: Bäumler, 2003, S. 93.
[630] Vgl. Golembiewski Claudia: Anonymität im Recht der Multimediadienste. In: Bäumler, 2003, S. 115.

Da dies derzeit allerdings nur für Strafverfolgungsbehörden und nicht zivilrechtliche Schadenersatzansprüche durch Contenturheber vorgesehen ist, brauchen Tauschbörsennutzer derzeit noch nicht allzu große Angst haben – mit den geplanten weiteren Reformen in Urheber- und Datenschutzgesetzen soll sich dies ändern[631]. Dies ist weitgehend auch schon das einzige Hindernis bei der Bekämpfung von Urheber- und sonstigen Strafdelikten (außer, dass das Recht noch an den Landesgrenzen endet)[632].

Was Tauschbörsen anbelangt, so beläuft sich die Menge an zur Verfügung gestelltem Content z.B. im KaZaA-Netzwerk bei etwa 3 Mio. Nutzern auf 300 - 400 Mio. Dateien. Eine Identifizierung der Nutzer ist nun anhand der IP-Adresse möglich, d.h. anonym ist man in Tauschbörsen keinesfalls[633]. Befindet sich dabei rechtswidriges Material auf Servern von Internet-Providern, so haften diese erst bei nachweislicher Kenntnis davon[634] – und jemandem nachzuweisen, er habe Kenntnis davon gehabt, ist nicht so einfach. Besonders trifft dies zu, wenn es sich um den Provider, bzw. dessen Angestellten handelt, die Logskripte selber löschen können. Für Firmen gilt allgemein, dass diese für ihre Mitarbeiter haften – im Extremfall drohen Vernichtungsansprüche gegen die Ausrüstung zur Herstellung von illegalen Kopien und damit die Beschlagnahme der gesamten IT-Ausrüstung eines Betriebs, so Server zum Tauschen illegaler Daten oder eben Equipment zur Herstellung solcher genutzt wurde – damit dürfte dessen Existenzgrundlage beendet sein, was angesichts der Strafen von bis zu fünf Jahren Haft in Deutschland für gewerblichen Handel mit Raubkopien die noch weitaus härtere Strafe sein dürfte – abgesehen vom Imageverlust[635].

4.9.2. GUIDs in Hardware und Software

CPUs, wie der P3-Prozessor von Intel verfügen über eine individuelle Seriennummer und ermöglichen damit eine Identifizierung[636]. Diese Personal Serial Number im P3-Prozessor wurde erstmals 1999 eingeführt und verkörpert somit die Hardwareimplementierung eines Wiedererkennungsmerkmales. 1999 ist auch die GUID in Software entdeckt worden. So werden z.B. schon unter Windows 98 (also vier Jahre

---

[631] Vgl. Sietmann Richard: „Elektronischer Hausfriedensbruch“. In c´t #06, vom 08.03.2004, S. 58.
[632] Und immer mehr Plattenlabels und Filmverleiher gehen auch mittels Anzeigen gegen die sog. kleinen Fische vor.
[633] Vgl. Behrens Daniel: Geheim, gratis, illegal. In: PC Welt, 12 / 2002, S. 70 f.
[634] Vgl. Laucken Fabian: Beweislast bei Haftung des Internet-Providers. In: Schneider, 2005, S. II / 28 f.
[635] Vgl. Pursche Olaf: Brisante Downloads. In: PC Professionell, 05 / 2002, S. 80.
[636] Vgl. Bechtold, 2002, S. 69.

vor XP) erzeugte Dokumente mit einer eindeutigen Kennung versehen, die bei einer allfälligen Registrierung online übermittelt wird. Anhand dieser Informationen lassen sich auch Aussagen über registrierte und unregistrierte Programme anhand ihrer erzeugten Dokumente treffen, sowie der Nutzer im Internet eindeutig identifizieren – sogar nicht nur für Microsoft, sondern für alle Interessierten[637].

4.9.3. Webbrowser

Da auf IP-Adressen und den Basisprotokollen des Internets mehrere Anwendungen aufsetzen, fallen neben den Klassikern E-Mail, FTP, Chat und Webbrowser letztlich auch DRMS als neuer Client für Internet-Zugriffe darunter. I.d.R. wird aber weiterhin der Webbrowser zur Freischaltungsoperation und zum Contentbezug (Bestellen) genutzt, sofern nicht Aktivierungssoftwaremodule oder Rootkits diese Aufgabe übernehmen. Browser verraten dabei neben der IP-Adresse des Anwenders die ursprünglich besuchte Website (Referrer) und natürlich, welcher Browsertyp verwendet wird – i.d.R. auch, unter welchem Betriebssystem[638] (sog. Header Daten)[639]. Was ein ausschließlicher DRMS-Client hier verraten würde, weiß dagegen nur dessen Hersteller. Das DRMS selbst „weiß“ aber im Vorfeld leider nicht, welche Daten Nutzer auf ihren PCs speichern und was es daher möglicherweise zufällig „mitüberträgt“. Zu Recht weist Reischl auf die Gefahr der digitalen Assistenten hin, wie z.B. durch Entwicklungen von Motorola namens Mya (=My Assistant) – dabei ist das Problem, dass Menschen den Maschinen zu viele Informationen anvertrauen[640] – und digitalisierte Informationen können über Netze abgefragt werden[641].

4.9.4. Cookies

Dass Cookies der Personalisierung von Informationen auf Websites dienen, davon zeugt, dass Microsoft das Patent dazu am 14.10.2003 erhalten hat. Innerhalb des EU-Parlaments hingegen ist Patentschutz für reine Software am 24.09.2003 abgelehnt worden[642]. Cookies, die nicht zur Steuerung einer Session dienen, unterliegen in

---

[637] Vgl. Fröhle, 2003, S. 47.
[638] Außer man hindert sie durch Firewalls daran, sich gegenüber der aufgerufenen Website zu identifizieren, was aber oftmals mit unzureichender Darstellung oder Systemfehlern in Steuerungsskripts verbunden ist.
[639] Vgl. Behrens Daniel: Dirty Online-Tricks. In: PC-Welt, 11 / 2005, S. 72.
[640] Vgl. Reischl, 2001, S. 75.
[641] Übrigens finden Motorola-CPUs in Apple-Computern Anwendung, neuerdings werden allerdings auch Intel-CPUs eingesetzt.
[642] Vgl. Jaschinski Martin: USA: Patent für „Cookies“. In Schneider, 2005, S. II / 2.

Deutschland jedoch der Unterrichtungspflicht des TDDSG. In Kombination mit den SHPs für die USA stellt sich jedoch die Frage, wie US-Websites hier auf deutsches Recht reagieren könnten. Immerhin muss man grundsätzlich davon ausgehen, dass deutsche Nutzer auch US-Seiten nutzen, sollte ein DRMS dies vorsehen. Cookies speichern hier zwar im Normalfall nur belanglose Daten, die lediglich der Vereinfachung der Kommunikationsprozesse zwischen Hersteller und Nutzer dienen. So könnte z.B. eine individuelle Begrüßung stattfinden oder das gewünschte Seitenlayout für den Nutzer angepasst werden. Leider gibt es aber auch gefährlichere Funktionen, wie den virtuellen Einkaufskorb, über den Bestellungen realisiert werden. Dabei sind die Persistentcookies, d.h. solche, die auch nach Beendigung der Session mit dem Webbrowser erhalten bleiben, gemeint. Problematisch ist nun, dass gängige Webbrowser in den Standardeinstellungen nicht auf diesen Umstand hinweisen, hier Daten ohne Rückfrage und Einverständniserklärung beim Nutzer zu speichern. Die Cookies bleiben dann erhalten, bis ihr Verfalldatum erreicht oder diese durch den Nutzer gelöscht werden. Somit lassen sich anhand mehrerer Cookies Wege des Nutzers durch das Internet nachvollziehen[643].

4.9.5. Daten die man noch nicht hat werden zugekauft, dann verknüpft

Problematisch ist durch DRM die Möglichkeit, Nutzerprofile über die Art der digitalen Informationen anzulegen. Somit ist zweifelsfrei der genutzte Content identifizierbar. Was dabei die unterschiedlichen Arten anbelangt, fallen derzeit bei multimedialen Inhalten auch unterschiedliche Verwertungsmöglichkeit an. Diese reichen dabei von zielgerichtet eingeblendeter Werbung für den vermeintlich potentiellen und v.a. zahlungskräftigen Rezipientenkreis bis zur Weiterveräußerung angelegter Nutzerprofile. Bei Musiknutzung lässt sich z.B. bei Besuch einer potentiellen Website mit Schwerpunkt digitalem Vertrieb von Audio-Dateien, sogleich als Hintergrundmusik ein Appetizer mit Auszügen aus den Rezipienten vermutlich interessierenden Inhalten wiedergeben. Es bieten sich somit im Internet weitaus exzellentere Auswertungsmöglichkeiten als diese klassische Statistiken im Sinne von Umfragen und Feedback jemals liefern könnten. Ziel dieses sog. Data-Minings ist es, Prognosen über die Zukunft anzustellen, d.h. Zahlungs- und Konsumverhalten zu eruieren. Der

[643] Vgl. Fröhle, 2003, S. 43 ff.

Computer ermittelt diese Muster und Trends dabei völlig selbständig[644]. US-Anwalt Friedmann spricht in diesem Zusammenhang angesichts einer Auseinandersetzung zwischen dem Suchdienst Yahoo und Universal Image über die Lieferung von Nutzerprofilen treffend von einer „Internet-Währung“. Die Tendenz zur Kommerzialisierung personenbezogener Daten wird somit klar erkennbar[645]. Dazu ist anzumerken, dass durch DRM diese Art elektronischen Handelns wesentlich erleichtert wird, da nicht der am Content interessierte Rezipient entscheidet, welche Daten er im Laufe der Geschäftsabwicklung (von der Lizenzierung, über Aktivierung und kontrollierte Nutzung) dem jeweiligen Unternehmen zur Verfügung stellt, sondern der Anbieter. Zum Preis seiner Privatsphäre erhält der Rezipient so teilweise auch unentgeltlichen Zugriff auf verschiedene Dienste - v.a. die Nutzung von Medienangeboten, wie z.B. werbefinanzierte Internetzugänge fallen darunter[646].

So hatte man beim Marktführer der Cookienutzung Doubleclick.net 1999 für 1,8 Mrd. € Abacus gekauft – eine Firma die von 88 Mio. Haushalten Einkaufsgewohnheiten gesammelt hat. Doubleclick dagegen hatte beim Suchen von Musik-CDs über die Suchmaschinen Altavista oder über alle Seiten mit Doubleclick-Bannern die Profile der Surfer ermittelt und gespeichert. Diese „ehemaligen“ anonymen Verhaltensdaten konnten nun namentlich mit den Einkaufsdaten abgeglichen werden – damit hatte man in kürzester Zeit, ohne aktiv gegen Datenschutzgesetze zu verstoßen, detaillierte personenbezogene Profile[647]. Genau solche Arten von Datenschutzverstößen sind es aber auch, die am häufigsten (neben der bloßen rechtswidrigen Übermittlung von Daten) vorkommen: Adresshandel – leider ist der alleinige Handel damit aber nicht illegal und betrifft gleich eine große Anzahl an Personen, da kommerzielle Datenbanken i.d.R. eine Vielzahl an Datensätzen aufweisen[648]. Somit liegt auf der Hand, dass es absolut nichts bringt, gegen Sammlungsgewohnheiten von DRMS punktuell per Gesetz vorzugehen. Denn: Anbieter beschaffen sich ja per Zukauf oder Übernahme anderer Anbieter fehlendes Datenmaterial und verhalten sich somit legal. Sogar die BSA nutzt Adresshandel, um an Daten von potentiellen Raubkopierern zu gelangen und diese dann durch spekulative Drohbriefe aufzufordern, ihre Softwarebestände ordnungsgemäß zu

[644] Vgl. Fröhle, 2003, S. 62.
[645] Nach Born, 2001, S. 35.
[646] Vgl. Born, 2001, S. 35.
[647] Vgl. Reischl, 2001, S. 48.
[648] Vgl. Born, 2001, S. 99.

lizenzieren[649]. Man merkt auch, dass diese Art Data-Mining[650] abgesehen vom Informationswert für den Rezipienten dem Anbieter weitaus mehr nützt - wenn nicht sofort, dann eben später bei der Aushandlung eines Verkaufspreises für die gesammelten Daten zwecks Verknüpfung mit gesammelten Daten anderer Anbieter anderen Contents. So lassen sich durch Verkauf von mittels Data-Mining ermittelten Profilen an Dritte gute Erlöse erzielen[651] Außerdem wird deutlich, dass neben dem Vertrieb von Content mit DRMS auch die Online-Werbung und klassische Adresssammlung Hand in Hand geht. Völlig zu Recht prangert hier Parenti das US-Data-Mining durch Cookies an, da nun sogar das sog „Window-Shopping“ aufgezeichnet werden kann[652].

4.9.6. Cookies im Media Player

Echte Anwendung finden Cookies im Media Player von Microsoft, der in neueren Windows Betriebssystemen standardmäßig implementiert ist. Trotz Dementi hier private Datenprofile zu sammeln wird bei jeder wiedergegebenen Scheibe (CD / DVD) die GUID des Players verschickt, um weiterführende Informationen darüber zu erhalten (wie Künstler und Titelangaben) oder allgemeine Lizenzanfragen zu stellen, ob denn der Rezipient überhaupt über alle zur Nutzung erforderlichen Rechte verfügt, wie folgende Abbildung zeigt:

[649] Vgl. Götz Birgit: Raubkopierer? In: PC Welt, 08 / 2002, S. 41.
[650] Vgl. Born, 2001, S. 33.
[651] Vgl. Clement, 2001, S. 79.
[652] Vgl. Parenti, 2003, S.100.

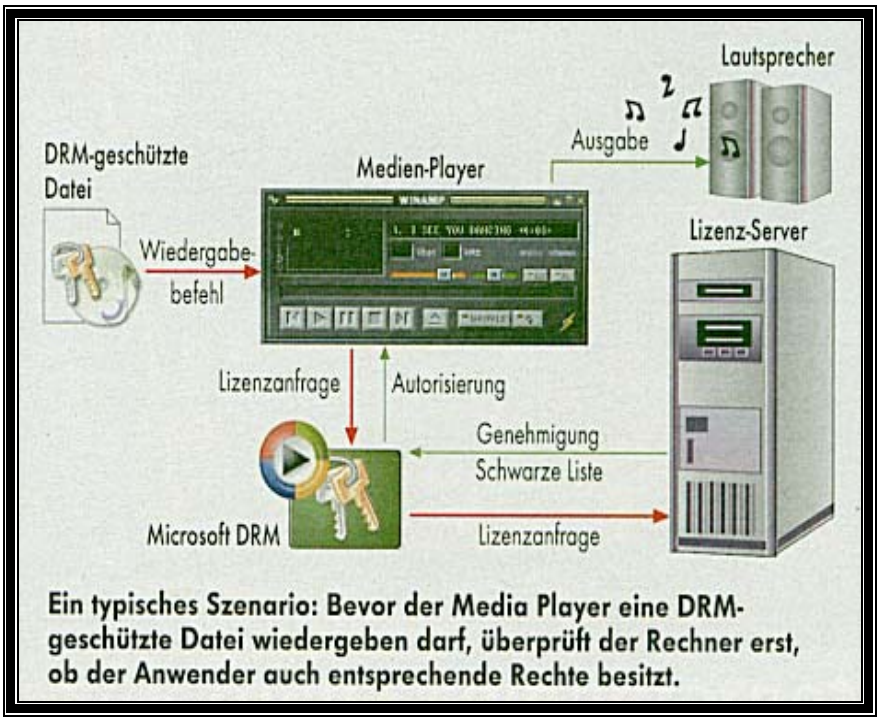

Abbildung 25: allgemeine Lizenzanfrage des Media Players zur Wiedergabe von DRM-Content[653]

Mit diesen Lizenzanfragen lassen sich aber nicht nur Lizenzen freischalten, sondern auch abändern, bzw. gleich gänzlich deaktivieren – auch wenn der Content ordnungsgemäß vergütet wurde. Damit ließe sich dann weitere Content-Nutzung verbieten[654]. Gepaart mit dem Windows Media Newsletter lassen sich auch eindeutig Personenprofile zuordnen. Bewiesen wurde dies durch einen Netzwerksniffertest, der von dem Magazin PC Welt durchgeführt wurde[655]. Da dieser Test schon 2002 stattfand und damals DRMS sich gerade durchzusetzen begannen, bleibt an dieser Stelle jedem selbst überlassen, zu vermuten, wie viele Daten Microsoft schon gesammelt hat. Da Cookies sich mit früheren Besuchen von Websites verknüpfen lassen, kann hier ebenfalls Personenbezug hergestellt werden, so früher unter Bekanntgabe von realen Abrechnungsdaten schon einmal Content online bezogen wurde[656]. Wie folgende Abbildung zeigt, liegt heimliches Spionieren nicht nur durch den Media Player allein vor, sondern auch durch die Aktivierung und Übertragung von Daten ohne Wissen des Nutzers durch verschiedene andere Funktionen in Windows:

[653] Aus: c´t #15, vom 15.07.2002, S. 18.
[654] Vgl. Himmelstein Gerald: Der digitale Knebel. In: c´t #15, vom 15.07.2002, S. 18 f.
[655] Vgl. Löbering Christian / Apfelböck Hermann: Spioniert Microsoft? In: PC-Welt, 05 / 2002, S. 12.
[656] Vgl. Roßnagel, 2003, S. 157.

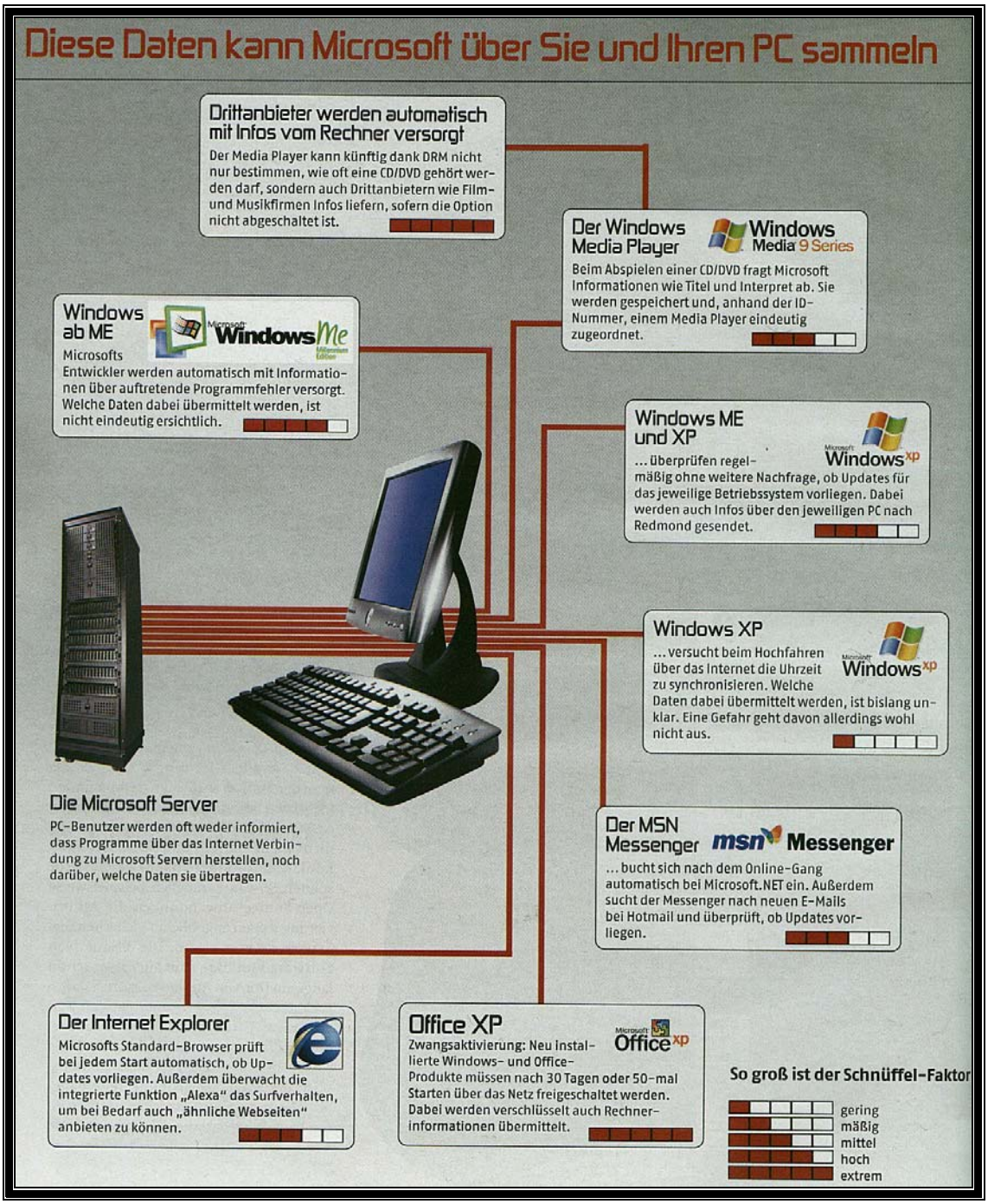

Abbildung 26: Spionage durch Windows, Office, Internet Explorer und Media Player im Überblick[657]

Deutlich zu sehen ist, dass die Gefahr der Profilbildung gerade durch die Aktivierung und den Media Player sehr hoch einzustufen ist. Noch bemerkenswerter ist, dass gerade Letzterer für die AV-Wiedergabe zuständig ist, was ganz im Sinne von Medienkonvergenz ermöglicht, an einem zentralen Punkt DRM einzusetzen. Daten über

[657] Aus: Tomorrow, Juli 2003, S. 30.

die bevorzugten Filme oder CDs im Wohnzimmer lassen sich somit einfach sammeln. Immerhin ist ja dank Media-Center-PCs mittelfristig die Ära des Videorecorders, bzw. modernerer DVD-Recorder beendet. Dann stehen alle Möglichkeiten der Abfrage von Nutzungsverhalten über Online-Netze zur Verfügung, da ja keinerlei Freischaltung des Contents ohne gültige Lizenz erfolgt. Die genauen Listen sämtlicher wiedergegebenen CDs / DVDs werden dabei durch sog. ID-Nummern an den Hersteller übermittelt. In Lizenzverträgen zu neuen Media Player Versionen heißt es sogar ganz offen, dass Microsoft dann „möglicherweise“ automatisch verhindern kann[658], sicheren Content wiederzugeben[659]. Mit diesem sicheren Content ist aber auch Content für Konkurrenzprodukte gemeint. Damit wird der Nutzer in seiner Wahl der Bezugsquellen erheblich eingeschränkt und mehr noch, es können durch derartige automatische Updates Sicherheitslücken im System geöffnet werden, die Schadcode enthalten - dieser kann dann PCs zu Spamsendern umfunktionieren, ohne dass der Anwender etwas bemerkt, oder es lassen sich ungefragt Programme installieren, die dazu dienen, das zu tauschen, was DRM eigentlich verhindern soll: illegalen und unlizenzierten, bzw. gecrackten Content[660].

Auch der Internet-Explorer ist durch das sog. Alexa-Plugin dafür berüchtigt, heimlich das Surfverhalten auszuspionieren und möglicherweise sogar Kennwörter zu versenden[661]. Wie man es loswird, erklärt z.B. Reuscher, ebenso wie man die Uhrzeitsynchronisation abstellt[662]. Festzuhalten bleibt an dieser Stelle, dass es gefährlich ist, wenn Hersteller von Hard- und Software eine monopolartige Stellung ihrer Produkte genießen[663] – so wird eben die IT- und Endgerätewelt für Contentbezug und dessen Nutzung fast ausschließlich von spionagefreudigen Herstellern[664] dominiert, d.h. von CISCO-Systems bei Internet-Netzwerktechnologie (wo Hintertüren in Routern des Internets vorgesehen sind, um bei „staatlichem Bedarf[665]“ Verschlüsselung zu

[658] Vgl. Reuscher, 2002, S. 358.
[659] Der „sichere Content” ist dabei in dem Sinne zu verstehen, durch DRM-Lizenzen geschützt zu sein.
[660] Vgl. Reuscher, 2002, S. 357 ff.
[661] Vgl. Pyczak Thomas: Internet Explorer verschickt Passwörter. In: Chip, 09 / 2003, S. 192.
[662] Vgl. Reuscher, 2002, S. 370 f.
[663] Vgl. Picot Arnold / Fiedler Marina: Impacts of DRM on Internet Based Innovations. In: Becker, 2003, S. 295.
[664] Die hier genannten sind jedoch nicht die Einzigen, sondern lediglich die Bekanntesten. Es würde den Rahmen sprengen, sämtliche DRM-Methoden anderer Hersteller hier zu behandeln – es gibt sie aber.
[665] Es ist offensichtlich, dass dies auch durch Entscheidungen von Providern, bzw. Betreiber derartiger Geräte geschehen kann.

deaktivieren[666]), Microsoft bei Software (flächendeckendes DRM in Windows XP und TCPA-Mitglied) und Intel bei der Herstellung von CPUs (P3-Prozessor GUID). Auch Apple-Rechner werden neuerdings mit Intel-CPUs ausgerüstet, d.h. auch, dass Windows XP nun ebenfalls dort läuft[667]. Hier kann durchaus davon gesprochen werden, dass ein Transformationsprozess von Staatlichkeit schon abgeschlossen ist.

Die Macht liegt bei großen Konzernen, die dann über das Schicksal von Daten entscheiden. Nicht einmal Nazi-Deutschland unter Adolf Hitler hatte so viel Machtpotential durch Gleichschaltung der Medien in der Hand, wie es sich durch DRMS insbesondere durch Freischaltgremien der TCPA realisieren lässt[668]. Sollten nämlich die noch vorhandenen Sicherheitslücken in DRMS beseitigt werden, dass ausschließlich nur mehr wie bei den Atomanalysen finanziell starke Staaten oder Konkurrenzkonzerne Umgehungsmöglichkeiten finden können, so ist es mit der Privatsphäre der Allgemeinheit vorbei – das Modell des TPM-Chips wird früher oder später siegen. Daraus resultiert geradezu eine Verpflichtung des Staates, hier Bürger vor datenschutzrelevanten Eingriffen Privater zu schützen[669], doch freilich müsste dann auch der Staat erhebliches Ressourcenkapital dazu aufwenden. Somit bleiben auch an dieser Stelle viele Probleme ungelöst und im Dunkeln.

4.9.7. Dank DRM: Computerwürmer und Rootkits

In dieser Arbeit sind sie bereits angeklungen: die Sicherheitslücken und Möglichkeiten, Spionageprogramme, wie z.B. Computerwürmer auf Festplatten loszulassen, die ohne Wissen Betroffener nach verdächtigem Content suchen. Was davon datenschutzrechtlich zu halten ist, ist strittig. So ist, wie Lessig hier anführt, fraglich, was der vierte US-Verfassungszusatz noch schützt, bzw. überhaupt zu schützen vermag (immerhin weiß man ja im Gegensatz zur vor der Tür stehenden Polizei nicht, dass eine Durchsuchung stattfindet)[670]. Die Gefahr dabei ist, dass dank DRM jeder Private Daten ausspionieren kann. Als Lieferant fungieren dabei die eigentlich als nützliche Programme getarnten Wiedergabeprogramme für Content. Erste Vorschubarbeit zur

[666] Vgl. Lessig, 2001, S. 203.
[667] Vgl. Benz Benjamin / Schnurer Georg: Einfach besser? Showdown: Apples Intel-Macs gegen den Rest der PC-Welt. In: c´t #10, vom 02.05.2006, S. 116 ff.
[668] Vgl. Kranz Kim: TCPA: Der Große Bruder am PC. In: Chip, 05 / 2003, S. 13.
[669] Vgl.Bröcker Klaus Tim: Schutz des Nutzers im Netz: Datenschutz und Datensicherheit. In: Bröcker, 2003, S. 237.

vollständigen Aushöhlung der Privatsphäre leistet ja auch die DRM-Allianz durch vollständig abgeschottete und verschlüsselte Kommunikation. Da dies ohne Möglichkeit der Interaktion des Benutzers geschieht, ist hier völlig unklar, welche Daten dabei transferiert werden. Das Urheberrecht wäre hier zum Preis der völligen Aufgabe der Privatsphäre effektiver als je zuvor. Allerdings nutzen auch populäre Tauschbörsenprogramme wie E-Donkey sog. Spyware, d.h. Programme die das Surfverhalten und Nutzergewohnheiten ausspionieren und somit ebenfalls zwielichtige Funktionen haben[671].

Die Krönung der Missachtung von Persönlichkeitsrechten sind aber Rootkits. Das sind Programme, die sich in die Kommunikation zwischen Anwendungen und dem Betriebssystem versteckt einnisten[672]. Sie übernehmen verschiedenste Aufgaben, wie die Überwachung der Wiedergabe von geschütztem Content, bzw. liefern eine spezielle Software mit, mit der sich Content, der für Homeelektronik gedacht ist (DVD-Player oder CD-Spieler) auch am PC wiedergeben lässt. So ist von der DVD „Mr. und Mrs. Smith“ eine Art Rootkit[673] zu installieren, wenn man die DVD auf PCs wiedergeben möchte – das kuriose daran: der Hersteller der DVD wusste gar nicht, dass der aus Südkorea von Settec zugekaufte Kopierschutz Datenveränderungen am System vornahm und Sicherheitslücken öffnete, sowie ohne Rückfrage Ressourcen verbrauchte[674]. Das zentrale Problem dabei ist, dass dies einmal mehr heimlich geschah, da Aktivitäten bewusst verschleiert wurden und Prozesse, Dateien, Benutzer und offene Ports eines Systems verborgen werden[675]. Sogar Microsoft selbst demonstrierte anhand eines eigenen Rootkits, wie man hier sogar das gesamte Betriebssystem „als Anwendung“ des Rootkits ablaufen lassen kann – eine Entdeckung durch Virenscanner oder Firewalls ist damit ausgeschlossen und der Datenspionage Tür und Tor geöffnet, wie folgende Abbildung zeigt:

---

[670] Vgl. Lessig, 2001, S. 264 f.
[671] Vgl. Apfelböck Hermann: So gefährlich ist Spyware. Sie werden bespitzelt. In: PC Welt, 08 / 2002, S. 12 f.
[672] Vgl. Arnold Arne / Ziemann Frank: Rootkits: Versteckte Gefahr. In: PC Welt, 02 / 2006, S. 11.
[673] Vgl. Schmidt Jürgen / Himmelein Gerald: Sicherheitsrisiko durch DVD-Kopiersperre. In: c´t #05, vom 20.02.2006, S. 37.
[674] Quelle: TV-Sendung: Planetopia online, Sat 1, 21.04.2006 - 22:15h
[675] Vgl. Busch, 2002, S. 242 f.

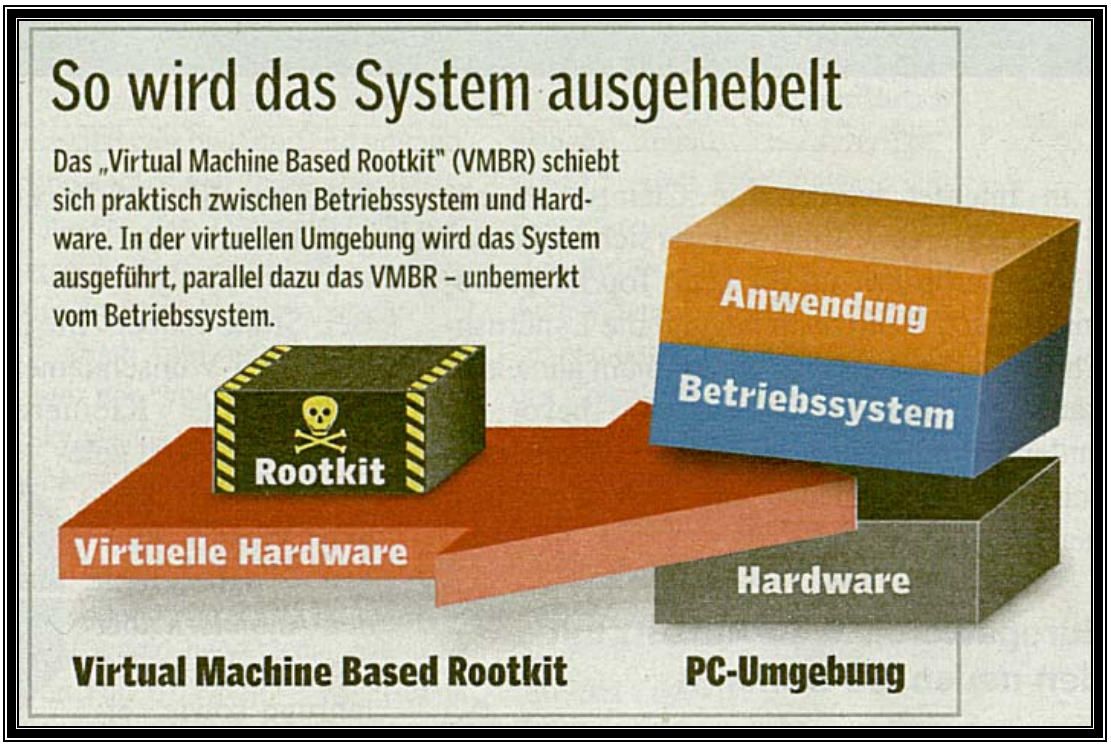

Abbildung 27: Microsoft selbst demonstriert die Funktion eines Rootkits[676]

Damit liegt ein klarer Eingriff in EDV-Anlagen vor, was nach deutschem Recht Computersabotage (§303b StGB) gleicht. Ein anderer aktueller Fall ist das Rootkit von Sony BMG, das ähnliche Funktionen für Audio-CDs beinhaltete und Album-Id, IP-Adresse und Uhrzeit bei aktiver Internet-Verbindung an Sony über den XCP-Kopierschutz sendet[677].

Gleichzeitig wird auch die Problematik von zugekauften DRM-Technologien deutlich: Contenthersteller und Urheber wissen oftmals nicht, dass hier Rechte verletzt werden. Damit stellt sich nach Rosenblatt die Frage, ob denn DRM-Technologie nicht selbst entwickelt denn zugekauft werden soll. Auch Outsourcing stellt eine Alternative dar. Welcher Weg optimal ist, kann leider nicht beantwortet werden, da dies vom Wert des Contents und dem Know How der Hersteller, sowie dem Willen zur Finanzierung eines Schutzmechanismus abhängt[678]. Es gibt aber auch Tools zur Realisierung von Datenschutz gegen DRMS-Mechanismen analog den Umgehungstools für den Schutz technischer Maßnahmen im Urheberrecht. Krause zählt hier intelligente Firewalls,

[676] Aus: Chip 05 / 2006, S. 22.
[677] Vgl. Schmelzle Michael: Übler Kopierschutz. In: PC Welt, 01 / 2006, S. 13.
[678] Vgl. Rosenblatt, 2002, S. 191 ff.

Anonymitätstools, die auf sog. Proxy-Servern basieren (dabei wird eine Schar von Anwendern hinter nur einer IP-Adresse „versteckt“), sowie Programme zur automatischen Löschung von Surfspuren und Cookies auf. Letztlich allerdings kann auch hier der Faktor Mensch versagen, d.h. Daten blindlings aus der Hand geben (z.B. in Webformularen mehr Angaben als zwingend erforderlich machen)[679]. Was die Rootkits betrifft, so wurden diese in Anti-Viren-Software dagegen schon als Schadcode eingestuft und mehrere Sammelklagen auf Schadenersatz sind in den USA bereits gegen Sony anhängig[680]. Dies ist auch verständlich, da Schadenersatz durch heimliche Eingriffe und Sabotageakte weitaus höher ausfallen kann, als:

4.10. Strafen für Datenschutzverletzungen

In den USA gibt es wie auch in Deutschland kaum Strafen für Datenschutzverletzungen, da erst der eigentliche Missbrauch von Daten, wie z.B. Verwertung für SPAM-Mails strafbar wäre. So hat US-Präsident Bush erst am 16.12.2003 ein bundesweites SPAM-Verbotsgesetz unterzeichnet[681]. Nun gibt es für Spammer hohe Strafen und auch Berufsverbote[682], besonders seit dem In-Kraft-Treten des CAN-SPAM-Aktes – dieser sieht Haft bis zu fünf Jahren und Geldstrafen bis sechs Mio. US$ vor[683], allerdings ist die eigentliche Datenschutzverletzung durch DRMS nicht sanktioniert. Es ist jedoch ohnehin schwer, zu beweisen, welche Unternehmen im Missbrauchsfall dahinter stecken würden. Somit bleiben lediglich die freiwilligen SHPs als Garant für EU-Datenschutzniveau oder noch schlimmer, die freiwilligen Datenschutzerklärungen von Unternehmen, ohne Mitglied von SHPs zu sein – diese haben dann dementsprechenden Wert.

Für Deutschland gibt es aber auch nur Ordnungs- und Bußgelder, die für Firmen lächerliche Höhen haben. Die Gewinne aus dem Sammeln von Profilen werden hier bewusst höher eingeschätzt, als die Strafzahlungen – so ist im BDSG ein Bußgeld bis 50.000 € vorgesehen, Haftstrafen dagegen überhaupt nur für nicht offenkundigen personenbezogenen Datenmissbrauch von bis zu zwei Jahren. Diese Daten sind aber für

[679] Vgl. Krause Christian: Tools für die Anonymität. In: Bäumler, 2003, S. 158 ff.
[680] Vgl. Schmelzle Michael: Übler Kopierschutz. In: PC Welt, 01 / 2006, S. 14.
[681] Vgl. Nuthmann Thomas: USA: Präsident unterzeichnet Anti-Spam-Gesetz. In: Schneider, 2005, S. II / 25.
[682] Vgl. Biere Sebastian: Millionenstrafe für Spammer. In: Schneider, 2005, S. II / 2.
[683] Vgl. Nuthmann Thomas: USA: Präsident unterzeichnet Anti-Spam-Gesetz. In: Schneider, 2005, S. II / 25.

DRMS ohnehin nicht zugänglich, da medizinische Daten und Strafregisterauszüge nicht Gegenstand von DRM sind und auch von keinem bekannten System abgefragt werden. Dagegen nehmen weniger schutzwürdige offenkundige Daten, also solche, die ohne große Anstrengung zu erlangen sind (Adressen und Hobbys) erst gar nicht am strafrechtlichen Schutz teil. Somit wird deutlich, dass es sich größtenteils nur um Ordnungswidrigkeitsdelikte handelt. Allerdings verpflichtet das BDSG Dienstleister - egal welche Daten verarbeitet werden - zur Absicherung der Verarbeitungsanlagen gegenüber unberechtigter Zugriffe von Seiten Dritter[684]. Damit ist die Implementierung von Sicherheitsstandards in Unternehmensnetzwerken gemeint. Datenschutzverletzungen fallen in diesem Bereich jedoch weniger auf und werden folglich kaum bis gar nicht zur Kenntnis genommen und noch weniger vor Gericht gebracht[685]. Dies verwundert auch nicht, geht es hier um „uninteressante Dinge", wie missbrauchte Mailadressen oder auch reale Adressdaten, was aber lediglich in Zusendung von unverlangter Werbung endet (Spam). Der so entstandene Schaden an privater Stelle hält sich regelmäßig in Grenzen, da die ökonomischen Auswirkungen im Einzellfall gering sind, sieht man von massenhaften Spam-Zusendungen ab, die durchaus ganze Telekommunikationseinrichtungen überlasten können. Dies mag auch der Grund dafür sein, dass Urheberrechtsdelikten wesentlich mehr Aufmerksamkeit als dem Datenschutz gewidmet wird, ist doch hier die Wertschöpfungskette stärker tangiert.

Bei Datenschutzverletzungen in Deutschland gibt es das Rechtsinstrument der strafbewehrten Unterlassungserklärung zur Unterbindung von weiterer Zusendung unverlangter Werbung (SPAM).[686] Für geringfügige Eingriffe in die Persönlichkeitsrechte dagegen, was in der Mehrzahl der Fälle auch so ist, gibt es dagegen keine Ansprüche auf Geldentschädigung – und genau damit sind leider die meisten Eingriffe durch DRMS abgedeckt. Die Schäden unter Ausnutzung von erlangten Daten zwecks Spam-Zusendung und aggressiven Marketings, bzw. Werbe-Pop-Ups dürften sich dabei allenfalls auf einige Sekunden für die Löschung, bzw. das Annehmen eines Telefonats bei Direktmarketing belaufen. Immerhin liegt hier keine derart schwerwiegende Beeinträchtigung oder schweres Verschulden der Schädiger vor (=Anwender von DRMS, also den Rechteinhabern von Content). Die

[684] Vgl. Busch, 2002, S. 46.
[685] Vgl. Born, 2001, S. 133 f.
[686] Vgl. Antoine Ludwig: Unterlassungsanspruch gegen Spam. In: Schneider, 2005, S. II / 11.

Tatsache, dass diese Phänomene in der Informationsgesellschaft durch mehrere Anbieter kumuliert auftreten sind für den Einzelfall dagegen unbedeutend – denn genau auf den Einzelfall ist ja bei Datenschutzverletzungen abzustimmen. So begründen z.B. nur rufschädigende Verwertung, preisgegebene Daten aus der Intimsphäre oder Informationen aus der Privatsphäre, bei denen schutzwürdige Interessen vorliegen (Geschäfts-, Beichtgeheimnisse, Rechtsanwaltskanzleidaten, medizinische Daten,...), Haftungsansprüche[687].

4.11. Bester Datenschutzmechanismus: Die Wirtschaftlichkeit

An Erkenntnis lässt sich somit festhalten: DRMS sichern nicht nur technisch Zugangs- und Nutzungskontrolle zu digitalem Content neben dem Urheberrecht, sondern lassen sich auch dazu (aus)nutzen, Nutzungsprofile zu Marketingzwecken zu sammeln – mehr Interesse ist nach derzeitigem Stand der Dinge im Datenschutzbereich nicht gegeben. Dies ist schon alleine aus wirtschaftlichen Erwäggründen geboten, da die Verarbeitung und Kombination von gesammelten Daten einen nicht unerheblichen Verwaltungsaufwand bedeutet. Als gutes Beispiel dazu läuft bekanntlich staatliche Verwaltung durch Behörden schleppend. Wohingegen „staatliches Data-Mining“ Sicherheit und Ahndung von Straftaten zum Ziel hat, hat privatwirtschaftliches Data-Mining nur solange Sinn, solange es Gewinn erwarten lässt. Der kostspieligen Sammlung aller Datenspuren aus dem Internet ist daher durch das Gebot der Wirtschaftlichkeit eine Grenze gesetzt[688]. Geld ist somit auch hier der beste Anreizfaktor, sowohl Daten durch DRMS sammeln zu lassen, gleichzeitig aber auch der effektivste Schutzmechanismus vor nicht mehr zu bewältigenden Datenfluten.

Andere Lösungsmöglichkeiten würden sich Dr. Forgó folgend in Hinblick auf sog. Flatrates in der Internet-Nutzung ergeben, wobei man keine individuelle Vergütung für Werke und daher auch keine entsprechenden Überwachungsmaßnahmen bräuchte – dies hätte aber den Nachteil für Wenignutzer, die sehr wenig Content lizenzieren. Man könnte daher auch mit Treuhandstellen operieren, wobei noch geklärt werden müsste wie hier die Finanzierung der Leistungen und die Leitung (staatlich oder nicht staatlich) erfolgen sollte. Dieser Auffassung folgt auch Fränkl, indem hier Trennung von

[687] Vgl. Born, 2001, S. 70 f.
[688] Vgl. Born, 2001, S. 31.

Kundendaten und DRMS gefordert wird[689]. Letztlich wäre auch griffigere Ausgestaltung des Datenschutzes möglich, d.h. konkret für bessere Einhaltung zu sorgen oder aber gänzlich zu kapitulieren und den Datenschutz hinsichtlich der Lizenzierungsproblematiken von Content durch DRMS zu vergessen[690].

[689] Vgl. Fränkl, 2004, S. 97.
[690] Quelle: Interview mit Dr. Forgó vom 17.02.2006.

5. Zusammenfassung und Schlussfolgerungen

Die im Sinne dieser Arbeit optimalste Definition von DRMS konnte nur in jeglicher auf Content angewandter Handlung mit dem Ziel kommerzieller Verwertung gefunden werden. Nebeneffekte von DRMS sind dabei datenschutzrechtliche Auswirkungen, d.h. konkret, dass hier oft ohne Wissen von Contentnutzern personenbezogene Datenprofile durch Verknüpfungsmöglichkeiten entstehen. Dies deshalb, da einzelne DRM-Mechanismen in der Tat keine personenbezogenen Daten abfragen – wohl aber das Gesamtpaket der Maßnahmen. DRMS setzen derzeit noch lediglich auf Tricks[691], da veraltete Protokolle und Architekturen es nicht vermögen, Content wirklich effektiv zu schützen.

Regulierung wurde deswegen erforderlich, da die Anzahl an Raubkopien jeglicher Art dramatische Ausmaße annahmen. Vorherrschende Regulierbarkeit soll erst durch die nächste PC-Generation im Sinne des TPM-Chips (Fritz-Chip) erfolgen, der somit auf Ebene des zu Grunde liegenden Codes ansetzt. Dabei kommt der Regulierung zu Gute, dass durch Medienkonvergenz mittelfristig in jedem Wohnzimmer ein Media-Center-PC stehen wird, was der TPM-Architektur sehr entgegen kommt. Diese Architektur ist es auch, der führende Hersteller angehören und für einen Durchsetzungsstandard des DRM sorgen wollen – denn bisher fehlt ein solcher. Bis dahin muss man sich mit wechselseitiger Abhängigkeit von Technik, Nutzungsverträgen und Technologie-Lizenzverträgen begnügen. Folglich wurden bisher verschiedenste „andere“ Arten der Implementierung von DRMS durchgeführt, wie Installationsschlüsseln, Verschlüsselungen, Passwörter und defekte Sektoren bei CDs / DVDs als Kopierschutz. Auch Softwareaktivierungen kamen zu Beginn des 21. Jhdt. in Mode, wobei das erste diesbezügliche Massenprodukt Windows XP war. Nutzung von Content ist nur auf Geräten, die „zum Entschlüsseln befugt“ sind, möglich. Sicherungsmittel dazu sind Technologielizenzverträge und Device Revocation-Rechte. Problematisch ist aber die unklare Lage am Markt, der derartige Entwicklungen nicht annehmen könnte, so wie Clement es erläutert hat.

Angesichts der dramatischen Entwicklung von raubkopierten Inhalten kann aber keinesfalls mehr davon gesprochen werden, dass hier der Staat mit Urheberrechten als

[691] Vgl. Biddle Peter (u.a.): The Darknet and the Future of Content Protection. In: Becker, 2003, S. 359.

Sicherungsinstrument ausreich hat. Die Aktivierung von Content jeglicher Art wird so künftig bei der Verfolgung von Rechtsverletzungen eine erhebliche Rolle spielen, gleichsam wie der zwangsläufige Schutz durch ein trotz allem erforderliches „Sicherheitsnetz Urheberrecht“. Genau dies sind auch die primären Auswirkungen auf Urheberrechte in den USA und Deutschland, denn seitens der Industrie wurde sehr wohl erkannt, dass staatliche Regulierung weiterhin erforderlich ist – immerhin ist man bisher nicht fähig gewesen, Sicherheitslücken in der DRM-Architektur zu stopfen, was auch für die künftige TCPA-Architektur gelten wird. Angriffe gegen DRMS sind immer möglich, sowohl technischer wie menschlicher Natur, wobei beim Angriff auf deren atomare Strukturen nur Konkurrenzfirmen, Profiraubkopierer und korrupte Regierungen in Frage kommen. Als dessen Ergebnis wird so jedes System früher oder später geknackt, d.h., dass auch die Umgehungstechnologie (oder Anleitung) dafür früher oder später im Internet auftaucht. Somit waren Kernbestandteile der staatlichen Regulierung Umgehungstechnologieverbote durch den DMCA in den USA und die Umsetzung der EU-Richtlinie zum Urheberrecht in der Informationsgesellschaft in Deutschland. Damit hatte man weiterhin Sanktionsmittel gegen Rechtsbrecher in der Hand (Geld und Freiheitsstrafen).

Der Schutz ist vielfach aber derart weltfremd gestaltet, dass auch Schrankenbestimmungen der Urheberrechte zahnlos wurden, weil DRMS sie erfolgreich unterminieren können. Einige Schranken sind dabei von den WIPO-Verträgen her generell nicht unterminierbar (z.B. Zugang für Behinderte), andere dagegen wurden offen gelassen (z.B. Privatkopie). In den USA käme hier das Prinzip der sog. Electronic Self Help zur Durchsetzung von gestatteten Ausnahmen im DMCA zu tragen, wobei dieses in beide Richtungen funktioniert: einerseits darf der Lizenznehmer seine Rechte durchsetzen, indem DRMS umgangen werden, andererseits darf der Lizenzgeber wirksame elektronische Sperren nutzen, um die Einhaltung des Lizenzvertrages zu erzwingen. In Deutschland dagegen ist generell keine Umgehung von „wirksamen technischen Schutzmaßnahmen“ gestattet ist, v.a. für das „nicht existierende Recht“ auf Privatkopie. Wirksam ist dabei im Sinne von „präsent“ zu verstehen und nicht tatsächlich effektiv. Vielfach werden auch Nutzungsverträge von US-Content mit speziellen Regelungen über DRMS ausgeliefert und auch teilweisen Beschränkungen unterzogen. Etliche Bestimmungen des US-Rechts, v.a. bei üblichen

Click- und Shrinkwrap Lizenzen sind dabei in Deutschland privatrechtlich unwirksam, in den USA dagegen gültig, wodurch sich neue Probleme ergeben, da DRMS keinen Unterschied zwischen legal gestatteter Umgehung, bzw. erforderlicher Contentsperre treffen können.

Weitere Probleme bestehen bei AV-Content auch durch die analoge Welt wie Screenshots oder dem Abfilmen und neuem Recodieren, was auch heute noch möglich ist, trotz Verbot der Umgehung von wirksamen technischen Schutzmaßnahmen[692]. Generell gilt dabei, dass Datenträger und Endgeräte in Deutschland einem Verwertungssystem unterliegen, das Pauschalvergütung für die Urheber ermöglicht und somit u.a. die „Privatkopie“ vergütet wird. In den USA dagegen wird die Verwertung durch die Filmstudios und Plattenlabels selbst durchgeführt. Genau deshalb zeichnen sich DRMS dadurch aus, genaue Regelungen zum Copyright zu treffen, da das gesamte US-Urheberrecht auf den Profit, das Deutsche dagegen an die zentrale Stellung des Urhebers in Hinblick auf kulturelle Aspekte anknüpft. Strittige Punkte in Deutschland ergeben sich vielfach in Hinblick auf doppelte und dreifache Vergütung von DRM-geschütztem Content (Lizenzgebühr, Endgeräteabgabe, Rohlingabgabe) – das Urheberrecht wird einfach als antiquiert erachtet, so RA Niclas Vilma, da für digitale Privatkopien und Rohlinge einerseits Pauschalgebühren verlangt, andererseits diese faktisch nicht mehr durchführbar ist[693]. Außerdem steht nicht fest, was passiert, wenn ein Hersteller in Konkurs geht, seine DRMS aber weiter wirken und daher der Content nicht mehr genutzt werden kann, da die Freischaltserver fehlen, so es keinen Rechtsnachfolger gibt.

Das Urheberrecht verlor trotz aller Probleme im digitalen Zeitalter keineswegs an Bedeutung – im Gegenteil: sie erhöht sich sogar, da wegen neuer Nutzungsarten und Nutzungsmöglichkeiten von Content noch mehr geistige Schöpfungen nachgefragt werden, womit die einleitende Theorie bestätigt wäre. DRMS steuern hier die Kopier- und Nutzungsvorgänge, wenngleich noch unausgereift und daher nicht optimal. Einer der Hauptgründe dafür sind unterschiedliche Implementierungsstrategien, wo viel zu viele wechselseitige Interessen sowie Abhängigkeit unter den Contentherstellern und denen der Technologie bestehen. Wenn es schon der Gesetzgeber (Fr. Zypries) nicht

[692] Vgl. Gutman, 2003, S. 141.
[693] Nach Stelzel-Morawitz Peter: Kopieren trotz Kopierschutz. In: PC go, 06 / 2002, S. 30.

schafft, zu wissen, was eigentlich reguliert werden soll (Stichwort: Privatkopie), dann vewundert es auch nicht, dass viele Auslegungsprobleme im Urheberrecht bestehen.

Aus dem gleichen Grund ist vieles auch beim Datenschutz strittig, dabei jedoch v.a. bezüglich der unterschiedlichen Ansichten in den USA und Deutschland, sowie dem Interesse der Nutzer, hier nicht überwacht zu werden. Schwachpunkte bestehen hier bei allen Formen von DRMS hinsichtlich der Wahrung des Datenschutzes. Da Content vornehmlich aus den USA kommt und dort Datenschutz eher ein Fremdwort ist, liegen hier lediglich freiwillige Zusagen in Form von Gütesiegelprogrammen vor. Forcierte Safe Harbour Principles gewähren hier wenigstens dem Papier nach die Einhaltung europäisches Datenschutzniveaus auch bei Datenverarbeitern in den USA. Problematisch ist aber, dass man hier kaum Kontrollmöglichkeiten hat. Hinderlich erweisen sich v.a. die freiwilligen und unverbindlichen Selbstzertifizierungen, sowie mangelnde Aufklärung der Datenerhebung und –verarbeitung im Vorfeld. Allen DRMS, die das Internet nutzen ist auch hier gemein, dass sie auf bekannten und veralteten Protokollen, bzw. Architekturen aufsetzen. Diese ermöglichen es geradezu, eine Überwachung sämtlicher Aktivitäten eines Nutzers im Internet zurückzuverfolgen. Der Hauptzweck der Contentfreischaltung wird so mitgenutzt, um als Nebeneffekt kommerzielles Data-Mining zu betreiben – dies geschieht auf Kosten ahnungsloser Nutzer, die mit verschiedenen DRMS teilweise gefährlichen Code auf ihren Rechner bekommen. Dieser Schadcode verhindert nicht nur zum Preis der besseren Einhaltung von Urheberrechten und Aufgabe der Privatsphäre unbefugte Kopien, sondern öffnet teilweise gravierende Sicherheitslücken in den Systemen, die dann als Spam-Sender fungieren oder zur totalen Überwachung sämtlichen wiedergegebenen Contents dienen, nicht nur der o.a. Überwachung von Spuren im Internet.

Was den Staat anbelangt, so hat dieser wie auch die Rechteinhaber Interesse daran, Profit zu machen und für die gesellschaftliche Weiterentwicklung zu sorgen, bzw. auch in gewissem Umfang Umgehungstechnologie zuzulassen (Schranken für Bildungszwecke, Nachrichten, Kritik an Werken oder auch zu Zwecken des zwangsweisen Datenschutzes, so wie im DMCA in den USA vorgesehen). Problematisch ist dabei, dass man hierbei erst einmal wissen muss, wie man an die Umgehungstechnologie gelangt (entweder Electronic Self Help oder die Hinterlegung bei Escrow-Agents), wobei strittig ist, wer den Zugriff darauf verwalten soll. In

Hinblick auf Datenschutz besteht hier generell das Interesse bei den Nutzern von Content auf Einhaltung, d.h. nicht überwacht zu werden, gleichzeitig auch durch den Staat gegenüber den privaten Datensammlungen der Rechteinhaber geschützt zu werden.

Durch die Natur des Phänomens DRM(S) konnten abschließend nicht alle diesbezüglichen Probleme erschöpfend behandelt werden. So ergeben sich noch hinreichende Forschungsfelder – v.a. was marken-, muster- und patentrechtrechtliche Angelegenheiten betrifft. Völlig ungeklärt ist auch, wie Lessig treffend festgestellt hat, wo man DRMS, bezogen auf den Code wirkungsvoll bekämpfen kann. Diese Arbeit soll daher auch mit einer denkwürdigen Metapher Lessigs schließen:

> Gesetze sind auf Polizei, Staatsanwaltschaft und Gerichte angewiesen, ein Schloss nicht[694].

Lawrence Lessig

[694] Zitat: Lessig, 2001, S. 410.

6. Literaturverzeichnis

6.1. Bücher

- Asche Henning: Zwangsvollstreckung in Software. Wiesmoor / Ostfriesland, 1998
- Auer-Reinsdorff Astrid / Brandenburg Andrea: Urheberrecht und Multimedia. Berlin, 2003
- Bäumler Helmut / von Albert Mutius (Hrsg.): Anonymität im Internet. Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts. Wiesbaden, 2003
- Barry John R. (u.a.): Digital Communication. Boston / Dordrecht / London, 2004[3]
- Bayer Kurt: Die neuen Welthandelsregeln zum Schutz geistigen Eigentums (TRIPS). Analyse und Auswirkungen. Wien, 1995
- Bechtold Stefan: Vom Urheber zum Informationsrecht. Implikationen des Digital Rights Management. München, 2002
- Becker Eberhard / Buhse Willms (u.a.): Digital Rights Management. Technological, Economic, Legal and Political Aspects. Berlin / Heidelberg / New York, 2003
- Berking Christina: Die Unterscheidung von Inhalt und Form im Urheberrecht. Baden-Baden, 2002
- Bertelsons Boris (u.a.): PC Underground. Enthüllt die geheimen Tricks der Profi-Programmierer. Düsseldorf, 1995
- Bröcker Tim / Czychowski Christian / Schäfer Detmar (Hrsg.): Praxishandbuch. Geistiges Eigentum im Internet. München, 2003
- Busch Christoph / Wolthusen Stephen D.: Netzwerksicherheit. Heidelberg / Berlin, 2002
- Drewes Stefan: Neue Nutzungsarten im Urheberrecht. Baden-Baden, 2002
- Feigenbaum Joan (Hrsg.): Digital Rights Management. Berlin / Heidelberg, 2003
- Forgó Nikolaus (u.a. Hrsg.): Probleme des Informationsrechts. Wien, 2003

- Fränkl Gerald / Karpf Philipp: Digital Rights Management Systeme. Einführung, Technologie, Recht, Ökonomie und Marktanalyse. München, 2004
- Fröhle Jens: Web Advertising, Nutzerprofile und Teledienstedatenschutz. München, 2003
- Fuhrberg Kai (u.a.): Internet-Sicherheit: Browser, Firewalls und Verschlüsselung. München / Wien, 2001[3]
- Gasser Urs (Hrsg.): Informationsrecht in „e"-Umgebungen. Baden-Baden, 2002
- Genz Alexander: Datenschutz in Europa und den USA. Eine rechtsvergleichende Untersuchung unter besonderer Berücksichtigung der Safe-Harbour-Lösung. Wiesbaden, 2004
- Grindl Rudolf: Datenschutz in globalen Telekommunikationssystemen. Baden-Baden, 1999
- Gutman Daniel: Urheberrecht im Internet in Österreich, Deutschland und der EU. Missbrauch, technische Schutzmöglichkeiten und rechtliche Flankierungen. Wien / Graz, 2003
- Hofer Michael: Medienökonomie des Interent. Münster, 2000
- Latzer Michael (u.a.): Selbst- und Ko-Regulierung im Mediamatiksektor. Alternative Regulierungsformen zwischen Staat und Markt. Wiesbaden, 2002
- Lessig Lawrence: Code und andere Gesetze des Cyberspace. Aus dem Amerikanischen von Michael Bischoff. Berlin, 2001
- Lessig Lawrence: The Future of Ideas. New York, 2002
- McKay Paulette (u.a.): Microsoft Windows XP Professional. Die technische Referenz. Kempten, 2002
- Plate John-Christian: Die Verwertungsgesellschaftspflicht für urheberrechtliche Vergütungsansprüche und ausschließliche Verwertungsrechte. Berlin, 2003
- Reischl Gerald: Gefährliche Netze. Wien, 2001
- Reuscher Dominik / von Heyl Julian: Windows XP. Dirty Tricks. Düsseldorf, 2002
- Roßnagel Alexander (u.a): Datenschutz im Electronic Commerce. Heidelberg, 2003
- Schwartz Paul M. / Reidenberg Joel R.: Data Privacy Law. A Study of United States Data Protection. Charlottesville, 1996

- Seith Sebastian: Wie kommt der Urheber zu seinem Recht. Zu den verfassungsrechtlichen Rahmenbedingungen staatlicher Politik zum Schutz des Urheberrechts im digitalen Zeitalter. Heidelberg, 2003
- Symantec Corporation: Norten System Works 2005 Premier Benutzerhandbuch, Cupertino, 2004
- Tinnefeld Marie-Therese / Ehmann Eugen: Einführung in das Datenschutzrecht. München / Wien / Oldenburg, 1998[3]
- Tischer Michael / Jennrich Bruno: CD-Brenner. Düsseldorf, 1998
- von Diemar Undine: Die digitale Kopie zum privaten Gebrauch. Münster, 2002
- Zerdick Axel (u.a.): E-Merging Media. Berlin / Heidelberg, 2004

6.2. Fachmagazine und Zeitschriften

c´t

- #15, vom 15.07.2002
- #22, vom 21.10.2002
- #23, vom 03.11.2003
- #06, vom 08.03.2004
- #12, vom 01.06.2004
- #13, vom 14.06.2004
- #24, vom 15.11.2004
- #05, vom 20.02.2005
- #05, vom 20.02.2006
- #10, vom 02.05.2006

Chip

- 05 / 2003
- 09 / 2003
- 10 / 2003
- 09 / 2004
- 10 / 2004
- 03 / 2004
- 04 / 2004
- 09 / 2004
- 05 / 2006
- 06 / 2006

Comment

- September 1997
- Oktober 2000

Computer Bild

- 14 / 2002
- 19 / 2002
- 08 / 2006

Computer Guide

- 02 / 2004
- 03 / 2004

PC Direkt

- 12 / 2001
- 05 / 2002
- 08 / 2002

PC Magazin

- 09 / 2001
- 10 / 2001
- 10 / 2002
- 05 / 2003
- 11 / 2003
- 07 / 2004
- 03 / 2006
- 06 / 2006

PC Praxis

- 06 / 2002
- 01 / 2003
- 10 / 2003
- 02 / 2004
- 03 / 2004
- 08 / 2004
- 05 / 2005
- 06 / 2006

PC Professionell

- 11 / 2001
- 01 / 2002

- 05 / 2002
- 02 / 2003
- 08 / 2003
- 12 / 2003

PC Welt

- 11 / 2000
- 05 / 2001
- 08 / 2001
- 09 / 2001
- 02 / 2002
- 03 / 2002
- 05 / 2002
- 08 / 2002
- 09 / 2002
- 11 / 2002
- 12 / 2002
- 05 / 2003
- 07 / 2003
- 08 / 2003
- extra, April / Mai / Juni 2004
- 10 / 2004
- 12 / 2004
- 01 / 2005
- 02 / 2005
- 03 / 2005
- 06 / 2005
- 07 / 2005
- 11 / 2005
- 12 / 2005
- 01 / 2006
- 02 / 2006
- 05 / 2006
- 06 / 2006

Tomorrow

- April 2003
- Juli 2003
- März 2006

sonstige Fachzeitschriften

- com!, 11 / 2004
- PC go, 06 / 2006

- WCM, Februar 2006

7. Anhang

7.1. Abkürzungsverzeichnis

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
Art.	Artikel
ASCAP	American Society of Composers, Authors, and Publishers
AV	audio / visuell, audio / visuellem, audio / visueller
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
Bit	Binary Digit (=kleinste digitale Informationseinheit)
BMI	Broadcast Music International
BSA	Business Software Alliance
CA	Copyright Act
CAN-SPAM	Controllig the Assault of Non-Solicited Pornography and Marketing Act
CD	Compact Disc
CEO	Chief Executive Officer
CPU	Central Processing Unit
CSS	Content Scramble System
D/A	digital / analog
Def.	Definition
DLL	Dynamic Link Library
DoS	Denial of Service
Dr.	Doktor
DMCA	Digital Millenium Copyright Act
DPM	Data Position Measurement
DPMA	Deutsches Patent- und Markenamt
DRM	Digital Rights Management
DRMS	Digital Rights Management System/e
DVD	Digital Versatile Disc
f.	folgende
ff.	fortfolgende
Fr.	Frau
GEMA	Gesellschaft für musikalische Aufführungs- und mechanischer Vervielfältigungsrechte
GUID	Globally Unique Identifiers
HDCP	High Bandwith Digital Content Protection
HDMI	High Definition Multimedia Interface
HDTV	High Definition Television
Hr.	Herr
Hrsg.	Herausgeber
i.d.R.	in der Regel
inkl.	inklusive
IT	Internet und Telekommunikations-Technologie
Jhdt.	Jahrhundert

KFZ	Kraftfahrzeug
LKW	Lastkraftwagen
MDStV	Mediendienstestaatsvertrag
MP3	MPEG Audio Layer-3
MPA	Motion Picture Association
MPAA	Motion Picture Association of America
MPEG	Moving Pictures Expert Group
Mwst.	Mehrwertsteuer
NSA	National Security Agency
o.a.	oben angeführt/e/r/em/en
o.ä.	oder ähnlichem
PDF	Portable Document Format
PGP	Pretty Good Privacy
RA	Rechtsanwalt / Rechtsanwältin
RL	Richtlinie
RBÜ	Revidierte Berliner Übereinkunft
SHPs	Safe Harbour Principles
sog.	sogenannte/r
TCG	Trusted Computing Group
TCPA	Trusted Computing Platform Alliance
TDG	Teledienstegesetz
TDDSG	Teledienstedatenschutzgesetz
TK	Telekommunikation
TOC	Table Of Contents
TPM	Trusted Platform Module
TRIPS	Trade Related Intellectual Property Rights
UCITA	Uniform Computer Information Transactions Act
u.a.	und andere / unter anderem / unter anderen
US	United States
USA	United States of America
v.a.	vor allem
VG	Verwertungsgesellschaft
Vgl.	Vergleiche
VHS	Video Home System
WMA	Windows Media Audio
WMV	Windows Media Video
WIPO	World Intellectual Property Organization
wis.	wissenschaftliche
WPA	Windows Product Activation
Z.B. / z.B.	zum Beispiel

7.2. sonstige Quellen

- DVD-Vorspann der DVD: Babylon 5: Legende der Ranger, (RC2)
- Interview mit Informationsrechtsexperte Dr. Nikolaus Forgó, vom 17.02.2006
- TV-Sendung: Planetopia online, Sat 1, 21.04.2006 - 22:15h