Carina Gerstengarbe; Katharina Lang; Anna Schneider

Wasserzeichen. Vom 13. Jahrhundert bis zum Digital Watermarking

2010

https://doi.org/10.25969/mediarep/648

Veröffentlichungsversion / published version
Zeitschriftenartikel / journal article

FAIR PLAY IM DIGITALEN ZEITALTER

Anspruch und Wirklichkeit des Digital Rights Management

VON DANIEL KÖHNE

1. KENNEN SIE DRM?

Sie hören gerne Musik? Sie schauen Filme? Sie spielen gerne mit Ihrer Spielkonsole? Sie benutzen einen Computer? Dann hatten und haben Sie mit an Sicherheit grenzender Wahrscheinlichkeit schon mit *Digital Rights Management* (DRM) zu tun! Falls Sie diesen Begriff dennoch zum ersten Mal hören, dann geht es Ihnen vermutlich nicht viel anders als den meisten anderen Nutzern digitaler Inhalte. Der Umgang mit DRM ist mit der Nutzung digitaler Werke zwar (fast) unvermeidlich geworden, bewusst wird das vielen Verbrauchern allerdings erst in dem Augenblick, wo sie die restriktive Seite dieser Rechteverwaltungssysteme kennenlernen.

Abb. 1: Eine Persiflage von DRM-Gegnern auf die 1980 von der British Phonographic Industry veröffentlichten Kampagne »Home Taping Is Killing Music«.

Drei typische Beispiele: Eine legal erworbene Software lässt sich partout nicht auf dem heimischen Zweit-Computer installieren. Die erst kürzlich erworbenen Filme aus dem Onlineshop können nach der Neuinstallation des Betriebssystems nicht mehr abgespielt werden. Der CD-Player im Auto verweigert die Wiedergabe des neuen Albums Ihrer Lieblingsband.

Vor allem solche *Pannen* haben zu einer großen Zahl von Missverständnissen, Mythen und vor allem jeder Menge Ärger über das sog. Digital Rights Management geführt. Von »elektronischer Leine für Kunden« ist da beispielweise die Rede, von Einschränkungen der Privatsphäre und der Blockade von Kulturgütern durch die Medienindustrie. Ganze Foren im World Wide Web beschäftigen sich ausschließlich mit dem Thema der digitalen Rechteverwaltung, diskutieren über deren (Un)Sinn und Zweck, liefern Tipps, wie man die oft lästige Kontrollinstanz umgehen kann und gelangen oft zu der Überzeugung, dass das *R* in DRM wohl eher für *Restriction* als den Begriff *Rights* stehe.[1] Gerald Fränkl[2] fasst die Ausgangslage knapp aber treffend zusammen: »DRM, ist ein stark polarisierendes Schlagwort der aktuellen Medienlandschaft« (Fränkl 2005: 13; vgl. ebd.: 35ff.).

2. DIGITAL RIGHTS MANAGEMENT – VERSUCH EINER DEFINITION

Was ist und bezweckt DRM überhaupt? Es ist schwer, vielleicht sogar unmöglich, digitale Rechteverwaltungssysteme allgemeingültig zu definieren. Das zeigt sich schon daran, dass selbst dem Gesetzgeber bislang eine solche Definition nicht gelingen will oder vielleicht auch nicht gelingen soll. In der juristischen Literatur wird DRM teilweise synonym zu dem Begriff »technische Schutzmaßnahme« verwendet. Auf den ersten Blick scheint es – vor allem aus Verbrauchersicht – auch leicht zu fallen, DRM-Systeme einer Kopierschutztechnik gleich zu setzen. Immerhin erlangen die meisten Verbraucher erst durch diese Funktion der digitalen Rechteverwaltungssysteme Kenntnis über deren Existenz. Bei einer genaueren Betrachtung muss diese Bewertung jedoch differenzierter ausfallen.

Für eine Konkretisierung ist es wichtig, zwischen Schutzmaßnahmen im Sinne des Urheberrechts auf der einen Seite und DRM-Systemen auf der anderen Seite klar zu unterscheiden. Das ist schon deshalb zwingend erforderlich, da eine »industrielle Massenproduktion von urheberrechtlichen Werken [...] im Urheberrecht nicht vorgesehen« (Höhne 2007: 7) ist, diese aber nun einmal de facto der Realität entspricht.

Festhalten lässt sich in jedem Fall: nicht jede technische Schutzmaßnahme ist zwangsläufig ein DRM-System. Gegen die These, dass es sich bei DRM-Systemen um komplexere Kopierschutzverfahren handelt, spricht auch die Tatsache, dass die Produzenten digitaler Werke ein erhebliches Interesse an der massenhaften Vervielfältigung und Verbreitung ihrer digitalen Inhalte haben und ihnen dabei ein Kopierschutz eher hinderlich sein dürfte. Was also ist unter digitaler Rechteverwaltung zu verstehen?

---

1 Siehe dazu beispielsweise ein kritisches Internetportal unterstützt von der Free Software Foundation Europe: http://drm.info/, 18.12.2009.

2 Neben zwei Buchpublikationen zum Thema digitale Rechteverwaltung, ist Gerald Fränkl u.a. als Autor auf der Internetseite http://www.digital-rights-management.info, 20.06. 2009, aktiv.

Zunächst einmal ist festzuhalten, dass es *das* DRM-System nicht gibt. Der Begriff des Digital Rights Management beschreibt weder eine bestimmte Software noch eine konkrete Handlung, sondern vielmehr ein komplexes System, das auf der Kombination vieler verschiedener Technologien basiert und dessen Zweck die Kontrolle des Zugangs und Steuerung der Nutzung digitaler Inhalte ist (vgl. Fränkl 2005: 35ff.; Zeng 2006). »Es ist das Ziel der Rechteinhaber an Geistigem Eigentum durch ein sogenanntes Digitales Rechtemanagement (DRM) den Verlust der physischen Bindung eines digitalen Produkts zu kompensieren« (Grimm 2009: 27; vgl. Tsolis 2009).

Dieses Zitat zeigt bereits drei wesentliche Kontroversen der digitalen Rechteverwaltung auf: Erstens, die Debatte um das geistige Eigentum. Zweitens, der Umgang mit digitalen Produkten an sich und drittens, die physische Bindung, welche mit dem Siegeszug des Digitalen verloren ging. Aber dazu an späterer Stelle mehr.

Selbst über die typischen Merkmale einer digitalen Rechteverwaltung gibt es unterschiedliche Ansichten. Die Firma Microsoft erklärt ihr DRM beispielsweise wie folgt:

> »Windows Media DRM ist eine bewährte Plattform, die das Schützen und sichere Übermitteln von Inhalten für die Wiedergabe auf einem Computer, einem tragbaren Gerät oder einem Netzwerkgerät ermöglicht. Ihre Flexibilität ermöglicht die Unterstützung einer Reihe von Geschäftsmodellen: von einzelnen Downloads bis hin zur Übertragung in Form physischer Medien. Die neueste Version von Windows Media DRM enthält neue Szenarien und bietet Heimanwendern noch besseren Zugriff auf geschützte Audio- und Videoinhalte.« (Microsoft 2009)

Martin Schippan charakterisiert DRM dagegen schlicht als »ein vollautomatisiertes, elektronisches Vertriebs- und Abrechnungssystem, [welches] [...] digitale Inhalte zu definieren versucht« (Schippan 2004: 190).

Auch wenn eine exakte Definition offenbar schwerfällt, so lassen sich DRM-Systeme allgemein dennoch wie folgt beschreiben: Die digitale Rechteverwaltung identifiziert digitale Werke, regelt den Zugang und die Nutzung dieser und überwacht gleichzeitig die Einhaltung ebendieser Kontrollinstanzen. Letztlich erfüllen DRM-Systeme aber vor allem die Rolle eines anspruchsvollen Vertriebssystems, insbesondere für digitale Angebote im Internet.

Folglich muss man DRM-Systeme weniger als Kopierschutz, sondern eher als Vertriebsinfrastruktur für die Produzenten digitaler Werke einerseits und die Nutzer dieser Inhalte andererseits sehen, da ein wichtiges Ziel von digitaler Rechteverwaltung letztlich auch der Authentizitäts- und Integritätsschutz der zur Verfügung gestellten medialen Inhalte ist. Darüber hinaus lässt sich ein System digitaler Rechteverwaltung durch weitere technische Prozesse wie beispielsweise

Bezahlsysteme und Metainformationen, die Rückschlüsse auf den digitalen Inhalt bzw. dessen Urheber ermöglichen, beliebig erweitern.

Diese technischen Möglichkeiten sind mit Sicherheit nicht allein charakteristisch für DRM-Systeme, allerdings machen sie deutlich, dass die Bezeichnung »Vertriebsinfrastruktur« im Zusammenhang mit digitaler Rechteverwaltung einer allgemeingültigen Definition schon sehr nahe kommt. Denn vereinfacht dargestellt steht bei einfachen digitalen Rechteverwaltungssystemen das Ziel im Vordergrund, potenziellen Kunden einen Zugang zu digitalen Inhalten zu verschaffen. Dieser erfolgt dann in der Regel gegen Bezahlung (vgl. Höhne 2007: 43ff.; Roßnagel 2009: 18f.). Nach dem Kauf eines digitalen Produktes und der damit bestandenen Zugangskontrolle kann der Kunde nun über das erworbene Produkt theoretisch frei verfügen. In der Praxis haben die Produzenten digitaler Inhalte allerdings ein erhebliches Interesse daran, dass ein Kunde die erworbenen Inhalte eben nicht völlig frei verwenden kann, vor allem aber, dass es dem Kunden nicht möglich ist, diesen Content beliebig zu vervielfältigen und weiterzugeben. An dieser Stelle greifen technische Maßnahmen zur Nutzungskontrolle ein, welche zum Ziel haben, den Umgang des Kunden mit den erworbenen Produkten zu steuern bzw. einzuschränken (vgl. Höhne 2007: 43ff.).

Festzuhalten bleibt also zunächst, dass DRM kein klassisches und eindeutiges Verfahren zum Schutz und zur Verwaltung von Rechten oder einen Kopierschutz darstellt, sondern viel mehr eine komplexe Infrastruktur bestehend aus verschiedenen Basistechnologien beschreibt. Zum Verständnis von DRM ist daher zum einen die Kenntnis der entsprechenden Technologien und zum anderen das Wissen um die technischen Entwicklungen der vergangenen Jahrzehnte erforderlich, welche die digitale Rechteverwaltung *nötig*, auf jeden Fall aber erst *möglich* machten.

3. TECHNISCHE ENTWICKLUNGEN ALS GRUNDLAGE FÜR DIGITAL RIGHTS MANAGEMENT

In den vergangenen Jahren fand ein gewaltiger Umbruch bei der Produktion medialer Werke bzw. Inhalte statt, vereinzelt wird sogar von einem Paradigmenwechsel gesprochen: Der Wechsel von analogen zu digitalen Medien wurde vollzogen (vgl. Fränkl 2005: 15). Maßgeblich dazu beigetragen haben technische Entwicklungen im Bereich der Vervielfältigungs- aber auch der Kommunikationsmöglichkeiten innerhalb der letzten Jahrzehnte. Als besonders markante Punkte sind in diesem Zusammenhang sicherlich die Ablösung der Schallplatte durch die Audio-CD zu nennen, sowie die spätere DVD, die ihrerseits den bis dato analogen Standard VHS im Bereich Video und Film verdrängte (vgl. ebd.: 2005: 14ff.; Höhne 2007: 2-6, 19ff.; Schollin 2008: 269ff.).

Die Vervielfältigungstechnologien wurden zunehmend preiswerter und damit – zum ersten Mal – auch für eine breite Masse von Privatpersonen erschwinglich. In diesem Kontext spielt vor allem der – wenn auch noch analoge – Kassettenrekorder eine herausragende Rolle. Mit einem einfachen Rekorder war es plötzlich

auch im privaten Bereich problemlos möglich, die eigene Lieblingsmusik auf MC zu kopieren, neu zu mischen oder weiterzugeben. Durch die massenhafte Verbreitung der VHS-Technik und des VHS-Videorekorders, der um 1980 eingeführt wurde, zeichnete sich darüber hinaus für die Filmindustrie eine ähnliche Entwicklung ab.

Diese Beispiele sind insofern nicht unerheblich, da sie verdeutlichten, dass die Thematik des Kopierschutzes nicht per se eine der neuen *digitalen* Welt ist. Im Gegenteil – insbesondere durch den Siegeszug der MC erkannten die Produzenten medialer Inhalte, dass ihnen die immer leistungsfähigere Technik nicht nur (Kosten-)Vorteile, sondern auch ein neues Problem bescherte: den Kontrollverlust über die Vervielfältigungen im privaten Bereich (vgl. Eggert 2005: 12f.; Fränkl 2005: 14ff., Höhne 2007: 19ff.; Schollin 2008: 269ff.).

So beliebt die neuen Techniken jedoch auch waren, sie hatten einen nicht unerheblichen Makel: Jede analoge Vervielfältigung ging technisch bedingt mit einem deutlichen Qualitätsverlust einher, der zumindest »die Anfertigung der Kopie einer Kopie unattraktiv machen« (Höhne 2007: 3) konnte. Dies allerdings änderte sich schlagartig mit dem Durchbruch der digitalen Medien, der im Audio-Bereich 1981 auf der Internationalen Funkausstellung in Berlin mit der Vorstellung der Audio-CD begann. Das Problem der unerlaubten Vervielfältigung von Software, das bereits seit der 1980er Jahre bestand, wird durch massenhafte Einführung von Heimcomputern ab den frühen 1990er Jahren weiter verschärft. Die wenig später folgenden CD- und DVD-Brenner in modernen Computern ermöglichten plötzlich jedem Privathaushalt in kurzer Zeit, bei geringem Kostenaufwand und vor allem ohne nennenswerte Qualitätsverluste die Vervielfältigung von digitalem Content jeglicher Art. Moderne Computer haben sich so zu einem »Kommunikations- und Unterhaltungszentrum« (Höhne 2007: 5) für Privatanwender entwickelt. Auch in anderen Bereichen, beispielsweise bei der Übertragung von Radio- und insbesondere Fernsehprogrammen, haben sich mittlerweile digitale Standards durchgesetzt – zunächst via Satellit und Kabel, schließlich mit dem *Digital Broadcasting Standard* auch über den terrestrischen Weg.

Beschleunigt wurde dieser Prozess zudem durch leistungsfähigere und preiswertere Kommunikationsmöglichkeiten, insbesondere dem schnellen Breitband-Internet. Während zu Beginn der privaten Nutzung des Internets die langsamen Übertragungsraten von gerade einmal 56 kBit den Austausch größerer Datenmengen noch unattraktiv machten, erhöhten sich diese Raten durch die nahezu flächendeckende Einführung von Breitband-Internet mittels der DSL-Technik bereits um den Faktor 10 und mehr. Durch die Verwendung von Funk-Netzwerktechniken und schnellen Mobilfunknetzen, wie EDGE und insbesondere UMTS, sowie immer leistungsfähigeren und kleineren mobilen Endgeräten, ist ein schneller Zugang zum World Wide Web mittlerweile an nahezu jedem beliebigen Ort möglich. Der Austausch und die Übertragung von Daten jeglicher Art und Größe über das Internet wurde so praktikabel und wird durch immer kostengünstigere Internetzugänge für Privatpersonen kontinuierlich attraktiver.

In diesem Zusammenhang muss sicherlich auch die Entwicklung der sog. Peer-to-Peer-Protokolle (P2P) erwähnt werden, mit denen eine dezentrale Speicherung von Daten auf Servern realisiert werden konnte. Aufgrund dieser neuen Protokolle zum Austausch von Daten im Internet konnten schließlich auch die populären Tauschbörsen entstehen, die es möglich machten, digitale Kopien innerhalb kürzester Zeit weltweit über das Internet zu verbreiten (vgl. Mittenzwei 2006: 10ff.). Technische Fortschritte bei den Kompressionsmöglichkeiten digitaler Inhalte taten ihr Übriges. An dieser Stelle sind vor allem die Entwicklung des JPEG-Formats für Bilder sowie die des MP3-Formats für Audio-Inhalte im Jahr 1992 hervorzuheben; neue Standards die sich rasant verbreiteten, und mit deren Hilfe sich große Datenmenge weitestgehend ohne sicht- oder hörbare Qualitätsverluste erheblich komprimieren ließen und so ohne großen Zeitaufwand über das Internet übertragen und ausgetauscht werden konnten (vgl. Fränkl/Karpf 2004: 21; Fränkl 2005: 14-16, Höhne 2007: 4ff.).

4. KONSEQUENZEN DER TECHNISCHEN ENTWICKLUNG

Vor allem in ihrer Gesamtheit betrachtet haben diese technischen Fortschritte erhebliche Konsequenzen für die Produktion, aber auch die Nutzung von medialen Inhalten. Im Zuge der kompletten Digitalisierung des Medienmarktes sanken für die Urheber der digitalen Inhalte die Herstellungskosten erheblich, so dass diese mittlerweile vernachlässigt werden können. Gleichzeitig entfällt, insbesondere durch die Popularität des Internets, eine Beschränkung auf bestimmte regionale Märkte. In diesem Zusammenhang von einer »Industrialisierung der Werkschöpfung« (Höhne 2007: 7f.) zu sprechen, liegt daher nahe.

Zum anderen stehen die Produzenten digitaler Inhalte vor einem Problem: Genauso simpel und günstig, wie sie ihre eigenen Inhalte produzieren können, ist es nun auch Privatnutzern möglich, einen beliebigen digitalen Content zu vervielfältigen. Das illegale Kopieren von digitalen Daten führt dabei zweifelsohne zu ökonomischen Einbußen der Produzenten (vgl. Kühne 2009: 3ff.). Die unrechtmäßige Vervielfältigung digitaler Inhalte ist praktisch nicht kontrollierbar, die Rückverfolgung nahezu aussichtslos. Qualitätsverluste, wenn es sie denn überhaupt gibt, sind so marginal, dass sie in der Regel komplett vernachlässigt werden können.

Diese Folgen der rasanten technischen Entwicklung haben im Wesentlichen zu zwei Reaktionen der Medienproduzenten und -urheber geführt. Erstens dem vermehrten Einsatz von Schutz- und Kontrollmaßnahmen zur Wahrung der Urheberrechte an medialen Inhalten. Und zweitens, vor allem bedingt durch den mäßigen Erfolg der erwähnten Schutz- und Kontrolltechniken, zu einer Verschärfung der gesetzlichen Rahmenbedingungen, die unter dem entsprechenden Druck der Medienproduzenten politisch umgesetzt worden sind und weiter verschärft zu werden scheinen (vgl. Krempl 1998; Krempl 2001).

Als Konsequenz aus den rasanten technischen Fortschritten der vergangenen Jahrzehnte wurde allerdings auch die digitale Rechteverwaltung mittels DRM erst denkbar und vor allem realisierbar. Eine Tatsache, die nicht unbeachtet bleiben sollte, da sie den Medienproduzenten zunächst einen wesentlichen Vorteil verschaffte: Die lückenlose und vor allem oftmals heimliche Kontrolle darüber, wie, wann und wo digitale Inhalte erworben werden und vor allem die Möglichkeit dazu, die spätere Nutzung dieser Werke zu steuern – Optionen, die im analogen Zeitalter noch undenkbar waren (vgl. Grimm 2009: 27ff.; Grassmuck 2004: 24f.). Als Reaktion auf die neuen Vervielfältigungsmöglichkeiten entwickelten die Produzenten digitaler Inhalte Kopierschutzmaßnahmen für ihre Werke. Techniken, die einen Kopierschutz gewährleisten sollten, wurden für Filme, Musik, Software, also im Grunde alle erdenklichen Varianten digitaler Inhalte, entwickelt.

Ein erster populärer Ansatz solcher Mechanismen, um die unerlaubte Nutzung und Vervielfältigung von Software zu unterbinden, waren sog. »Dongles«. Die Funktionsweise dieser kleinen Geräte, die zusammen mit der entsprechenden Software ausgeliefert wurden, war vergleichsweise simpel: Eine in die Software integrierte Abfrage überprüfte, ob der dazugehörige Dongle ebenfalls an den Computer angeschlossen war. War dies nicht der Fall, wurde das Programm beendet bzw. ließ sich erst gar nicht vollständig starten oder nutzen. Wirklich durchsetzen konnten sich Dongles jedoch nicht. Das hatte verschiedene Gründe: Zum einen gab es häufig Kompatibilitätsprobleme, unter denen zwangsläufig auch die Anwenderfreundlichkeit litt. Zum anderen basierte die Dongle-Variante auf einem relativ einfachen Sicherheitsverfahren, welches dazu führte, dass entweder die in die Software integrierten Abfragen manipuliert oder sogar Dongles selbst illegal kopiert bzw. nachgebaut werden konnten.

Eine weitere eingesetzte Kopierschutzvariante sollte das Kopieren von Software mit einem herkömmlichen Computer bzw. der darauf installierten Software durch eine verschlüsselte Beschriftung der Datenträger verhindern – aber auch dieser Schutz konnte innerhalb kurzer Zeit durch speziell entwickelte Kopiersoftware umgangen werden.

Interessante Ansätze gab es bei der Kombination von Software und der – zumindest noch damals – beiliegenden gedruckten (sic!) Dokumentation. Bei dieser Schutzvariante unterbrach die Software in unregelmäßigen Abständen ihren Nutzer, um von ihm bestimmte Informationen aus dem Handbuch abzufragen. Natürlich war es kein allzu großes Problem, die entsprechenden Fragestellungen bzw. Antworten unerlaubt weiterzugeben. Das erkannten auch die Software-Produzenten und lieferten schließlich in weiter entwickelten Varianten dieser Schutztechnik beispielweise selbst kopiergeschützte Dokumentationen aus. Zumindest als kreativ muss ein Versuch der Produzenten gewertet werden, die Abfragen am Bildschirm bzw. deren Antworten in der Dokumentation nur über die Verwendung von speziellen Farbfolien, die der Software beilagen, zu ermöglichen. Diese ersten Versuche, eine unerlaubte Nutzung oder Vervielfältigung von Software zu unterbinden, muten aus heutiger Sicht zweifelsohne laienhaft an und er-

innern eher an ein Gimmick für junge Detektive aus einem Comic-Heft (vgl. Höhne 2007: 18ff.).

5. DIE GRUNDLAGEN VON DRM-SYSTEMEN

Wie bereits einleitend erwähnt, stellen Systeme der digitalen Rechteverwaltung Infrastrukturen dar, die verschiedene Basistechnologien kombiniert einsetzen, um so den Zugang und die Nutzung digitaler Werke zu kontrollieren und zu steuern.

Dazu ist es erforderlich, dass in einem ersten Schritt digitaler Content vor unberechtigtem Zugang geschützt wird. Dies lässt sich wirkungsvoll durch eine Verschlüsselung realisieren, weshalb auch kryptographische Verfahren zu den wichtigsten Basistechnologien von DRM-Systemen zählen. Auch wenn die Begriffe »Kopierschutz« und das sog. Digital Rights Management – wie bereits erwähnt – nicht gleichzusetzen sind, so hat sich das digitale Rechtemanagement doch aus den klassischen Kopierschutzverfahren, wie sie bereits zuvor kurz beschrieben worden sind, entwickelt. Im Gegensatz zu den meisten altbekannten Kopierschutzverfahren basieren moderne DRM-Systeme allerdings auf deutlich komplexeren Mechanismen, kombinierten Verfahren der Stegano- und Kryptographie[3] (vgl. Abie 2009; Agnew 2008: 295ff.; Höhne 2007: 23ff.; Schollin 2008: 144ff.).

In Form von digitalen Wasserzeichen[4] und Fingerabdrücken, elektronischen Signaturen und Verschlüsselungstechnologien sind diese Kernbestandteile eines jeden DRM-Systems, die jedoch nur auf den ersten Blick absolut sicher gegenüber Manipulationen erscheinen. Seit Beginn der Kryptographie gibt es einen regelrechten Wettbewerb zwischen den Entwicklern neuer Verschlüsselungstechniken auf der einen Seite und den Entwicklern von Methoden, die genau jene Verschlüsselung zu umgehen oder auch aufheben versuchen, auf der anderen Seite (vgl. Eggert 2005: 12ff.). Wobei erste Verfahren dieser Art keine Erscheinungen der digitalen Welt sind, sondern in Form von Geheimschriften bereits im 5. Jahrhundert v. Chr. in Griechenland Verwendung fanden.

Es gibt diverse Formen von Verschlüsselungsmethoden[5], die sich zum Teil erheblich voneinander unterscheiden. Entscheidend für moderne Verfahren der Kryptographie ist allerdings, dass die Sicherheit der angewandten Verschlüsselung nur von der Geheimhaltung des entsprechenden Schlüssels, aber niemals von der Geheimhaltung des eingesetzten Algorithmus abhängen sollte. Dabei wird zwischen symmetrischer, asymmetrischer und hybrider Verschlüsselung sowie dem sog. Hash-Verfahren unterschieden.

---

3 Eine sehr umfangreiche Linksammlung zu den Themen Kryptographie, Steganographie, Datenschutz und -sicherheit findet sich bei Burkhard Schröder: http://www.burks.de/krypto.html, 10.12.2009.

4 Siehe den Beitrag von Carina Gerstengarbe, Katharina Lang und Anna Schneider in diesem Heft.

5 Einen spannenden Einblick in dieses komplexe Thema bietet Singh (2000).

Symmetrische Verschlüsselungsverfahren (Private-Key-Verfahren) verwenden dabei für die Codierung und Decodierung denselben Schlüssel, in dessen Kenntnis oder Besitz logischerweise sowohl der Sender als auch der Empfänger der so codierten Inhalte sein muss. Dieser Schlüssel muss wiederum zwingend über einen sicheren Übertragungskanal übermittelt werden, da ansonsten der Schutz des gesamten Verfahrens nicht mehr gewährleistet ist.

Bei der asymmetrischen Verschlüsselung (Public-Key-Verfahren) wird dagegen ein Schlüssel verwendet, der sowohl aus einem öffentlichen (Public Key) und einem geheimen, privaten Schlüssel (Private Key) besteht. Diese stehen in einem mathematischen Zusammenhang, wodurch sich aus dem privaten Schlüssel der öffentliche Teil ableiten lässt, nicht jedoch umgekehrt. So kann der Sender digitale Inhalte mit dem öffentlichen Schlüssel codieren; die Decodierung ist allerdings nur mit dem privaten Schlüssel des vorgesehenen Empfängers möglich. Asymmetrische Verschlüsselungsverfahren haben jedoch einen Nachteil; sie erfordern einen relativ hohen Rechenaufwand.

Dies hat zur Entwicklung der sog. hybriden Verschlüsselung geführt, welche bis heute Standard ist und die symmetrischen und asymmetrischen Verfahren entsprechend ihrer Vor- und Nachteile nutzt. So werden die eigentlichen Daten oder Informationen zwar symmetrisch verschlüsselt, der Schlüssel zur Decodierung jedoch mittels eines asymmetrischen Verfahrens codiert und über einen öffentlichen Kanal übertragen. Dadurch wird lediglich eine geringe Rechenleistung benötigt, aber gleichzeitig die Sicherheit bei der Schlüsselverteilung gewährleistet. Eine andere Methode verwenden Hash-Verfahren. Mittels eines sog. Hash-Wertes oder digitalen Fingerabdrucks weisen sie beliebigen digitalen Daten einen nahezu eindeutigen Wert fester Länge zu, also sozusagen eine »Kurzfassung« des originalen Contents (vgl. Agnew 2008: 295ff.; Höhne 2007: 30; Mittenzwei 2006: 67ff.; Schollin 2008: 144ff.). Originale Information und Hash-Wert werden dabei abgeglichen; ändert sich die originale Information, führt dies auch zu einem veränderten Hash-Wert. Aufgrund ihrer festgelegten Länge können mehrere identische Hash-Werte kollidieren, da sie jeweils unterschiedlichen Original-Dateien zugeordnet sind. Deshalb ist es erforderlich, dass bei diesem Verfahren Hash-Funktionen eingesetzt werden, mit denen es praktisch – also mit den Rechenleistungen heutiger oder in naher Zukunft verfügbarer Computer – unmöglich ist, zwei verschiedene digitale Dateien mit identischen Hash-Wert zu ermitteln.

In letzter Konsequenz hat jedoch jede – zumindest zweckmäßige – Codierung einen entscheidenden Nachteil: Soll ein verschlüsselter digitaler Inhalt wieder les- und nutzbar sein, muss er sich zwangsläufig mindestens einmal wieder entschlüsseln lassen. Andernfalls wäre schließlich auch jeglicher Inhalt für den Nutzer unbrauchbar. Kurzum: »Im Prinzip [ist] jede Operation, die ein Computer vornimmt, von einem Computer auch wieder rückgängig zu machen, und muss es auch sein, da autorisierte Nutzer das Werk schließlich dafür bezahlt haben, es zu rezipieren« (Grassmuck 2004: 102).

Eine perfekte Codierung digitaler Inhalte kann es allerdings schon deshalb nicht geben, da jede Sicherheitsinstanz spätestens bei der legitimen Nutzung hinfällig oder zumindest angreifbar ist. Und sei es über den Umweg einer – wenn auch mit Qualitätsverlusten einhergehenden – analogen Kopie. Entscheidend für die Funktionalität eines DRM-Systems ist es daher, dass die beiden wichtigen Kontrollfunktionen, also die Zugangs- und Nutzungssteuerung, so verschlüsselt und integriert sind, dass sie nicht beliebig, also z.B. durch den Nutzer selbst, außer Kraft gesetzt werden können. Insbesondere die dem Kauf zeitlich nachgestellte Nutzungskontrolle ist dabei eine technische Herausforderung. Ohne die entstandenen neuen Kommunikationswege, insbesondere dem Internet, wäre eine solche Kontrolle des Anwenders nicht denkbar. Mit ihr und mittels einer speziellen Software kann jedoch eine Kommunikation zwischen Anwender-(Software) und Produzenten über einen zwischengeschalteten Server ermöglicht werden.

6. DAS FUNKTIONSSCHEMA VON DRM-SYSTEMEN

Grundsätzlich lässt sich die Funktionsweise eines DRM-Systems in vier Bereiche gliedern:

Erstens einem sog. »Secure Container«, der das eigentliche digitale Werk enthält und mittels – bereits zuvor erläuterter – verschlüsselter Algorithmen vor unberechtigtem Zugriff schützen soll.

Zweitens definiert eine »Rights Expression Language« die Zugangsberechtigung zu den Inhalten des Secure Containers. Bereits Mitte der 1990er Jahre entwickelte die Firma Xerox die *Digital Rights Property Language*[6], eine spezielle Sprache, die ebendiese Kommunikation zum ersten Mal möglich machte. Mittlerweile haben sich sozusagen zwei Kommunikationsstandards durchgesetzt: die *Open Digital Rights Language*[7] und die *eXtensible rights Markup Language*[8]. Beide Sprachen sind inkompatibel zueinander; die eine wird bevorzugt von der *Open Mobile Alliance*[9] eingesetzt, die andere verwendet zum Beispiel der *Windows Media Rights Manager*. Was machen diese Sprachen im Detail?

6 Für weiterführende Informationen zur *Digital Rights Property Language* (DPRL) siehe u.a.: http://xml.coverpages.org/dprl.html, 11.01.2010.

7 Für weiterführende Informationen zur *Open Digital Rights Language* (ODRL) siehe u.a.: http://odrl.net/, 08.01.2010.

8 Für weiterführende Informationen zur *eXtensible rights Markup Language* (XrML) siehe u.a.: http://www.xrml.org/about.asp, 08.01.2010.

9 Für weiterführende Informationen zur *Open Mobile Alliance* (OMA) siehe: http://www.openmobilealliance.org/, 08.01.2010.

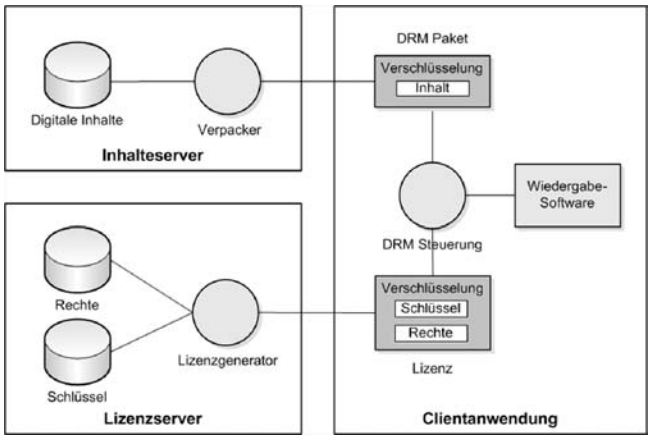

Abb. 2: Die Funktionsweise von DRM-Systemen vereinfacht dargestellt. Quelle: Prussio (CC-Linzenz), http://de.wikipedia.org/w/index.php?title=Datei:DRMS.png&filetimestamp=20050908195600, 08.01.2010

Sie erkennen, welche Lizenzbedingungen erworben worden sind und schränken den Nutzer bei Bedarf dementsprechend ein. So ist es zum Beispiel möglich, bestimmte Funktionen einer Software einzuschränken oder aber auch die Nutzungsdauer von digitalen Inhalten zu begrenzen. Dabei lässt sich im Wesentlichen zwischen inhaltlichen, zeitlichen, räumlichen und persönlichen Beschränkungen, sowie der vorgegebenen Nutzungsart unterscheiden. Beispiele dafür sind die Einschränkung der Exportmöglichkeiten in DRM-freie Formate, die Unterbindung des Anlegens von Sicherheitskopien, die Beschränkung der Gesamtnutzungsdauer, die Bindung an bestimmte Abspielgeräte bzw. Hardware oder auch der Ausschluss der gewerblichen Nutzung von digitalen Inhalten (vgl. Fränkl 2005: 25ff.; Höhne 2007: 45f.; Schollin 2008: 144ff.).

Drittens und ebenso wichtig ist die Identifikation des digitalen Inhaltes, beispielsweise durch eine Seriennummer, sowie die eindeutige Zuordnung der Nutzer.

Und schließlich wird, viertens, im Anschluss an den Verkauf der digitalen Werke und einer erfolgreichen Identifikation durch das System, eine Kontrollinstanz aktiv, die ggf. Nutzungsberichte übermitteln oder auch zur Bezahlung eingesetzt werden kann (vgl. Eggert 2005: 17f.; Höhne 2007: 47ff.). Da eine Manipulation nun aber nicht sicher ausgeschlossen werden kann, setzen die Produzenten digitaler Werke zusätzlich auf spezielle verborgene Kennzeichen, die dem Kunden – zumindest im Optimalfall – verborgen bleiben, dem Urheber der Werke jedoch einen direkten Rückschluss auf den legitimen Nutzer oder Inhaber des entsprechenden Werkes zulassen.[10]

10 Siehe den Beitrag von Carina Gerstengarbe, Katharina Lang und Anna Schneider in diesem Heft.

An dieser Stelle wird klar, dass DRM-Systeme die Persönlichkeitsrechte der Kunden berühren. Transparenz und Zustimmung des Kunden sind daher ein wichtiges Thema für DRM-Funktionen.

7. DIE PRAKTISCHE ANWENDUNG VON DIGITAL RIGHTS MANAGEMENT

DRM-Systeme werden vielfältig eingesetzt. Zu den populärsten Einsatzgebieten zählen aber sicherlich der Vertrieb von digitaler Musik und elektronischen Text-Dokumenten. Zu den bekanntesten Systemen auf dem digitalen Markt zählten (sic!) *Fairplay*, das die Firma Apple in seinem Online-Musikshop *iTunes* einsetzte oder auch der *Windows Media Rights Manager* von Microsoft, der u.a. durch das deutsche Musikportal *Musicload* von T-Online eingesetzt wird (vgl. Grimm 2009: 35f.).

Digitales Rechtemanagement fand und findet also Anwendung in populären Bereichen. Dennoch ist die Kritik an DRM-Systemen laut und vielfältig. Und tatsächlich scheint sich die umfangreiche Kontrolle und Steuerung der Nutzer durch die Medienindustrie nicht durchsetzen zu können. Schlussfolgern lässt sich dies zumindest anhand der Tatsache, dass mittlerweile alle vier großen Musikverleger von DRM-Systemen wieder abgekommen sind. Dafür gibt es mit Sicherheit vielfältige Gründe – entscheidend dürfte aber die mangelnde Akzeptanz der Kunden gewesen sein, welche sich vor allem dadurch erklären lässt, dass es bislang eben *das* DRM-System nicht gibt.

Möglicherweise hätte sich eine digitale Rechteverwaltung gerade im digitalen Musikvertrieb durchsetzen können. Immerhin boomt der Markt der Online-Musikshops, wie nicht nur das Beispiel von Apples *iTunes* zeigt (Grimm 2009: 33). Kurzum: entgegen aller Befürchtungen und – vielleicht auch beabsichtigter – Panikmache in Form diverser Szenarien über den Untergang der Musikindustrie gibt es offenbar nach wie vor zahlreiche Kunden, die bereit sind, für ihre Lieblingsmusik zu bezahlen, anstatt sie – fast genauso bequem – kostenlos, wenn auch illegal, aus dem Internet herunterzuladen. Durch die Vielzahl der eingesetzten Systeme ergibt sich für die Kunden allerdings eine nicht unerhebliche Unsicherheit, insbesondere was die Verfügbarkeit der von ihnen erworbenen digitalen Werke betrifft. Denn so bequem wie die Lizenzen für digitale Musik, Texte und Software über das Internet mittlerweile bezogen werden können, so schnell können genau diese Lizenzen auch wieder erlöschen bzw. ihre Gültigkeit verlieren.

Besonders deutlich wird das an dem Fall *Playsforsure* der Firma Microsoft. Kunden, die Musik über Microsofts Onlineshop *msn music* gekauft hatten, sahen sich ab dem 31. August 2008 mit einem Problem konfrontiert. Wenige Monate zuvor hatte Microsoft lapidar mitgeteilt, dass es sein in *msn music* eingesetztes DRM-System *Playsforsure* nicht weiter unterstützen werde. Das Problem: ohne das entsprechende DRM-System lässt sich die legal erworbene Musik nicht weiter nutzen. Für die Kunden von Microsoft bedeutete das im Klartext, dass sie spätes-

tens mit einem Wechsel des Betriebssystems nicht mehr auf ihre gekauften Musiktitel zurückgreifen konnten. Dieser Vorgang zeigt sehr deutlich, wie flüchtig die Lizenzierung von digitalen Inhalten ausfallen kann. Nebenbei bemerkt: Microsofts Problemlösung für die verständlicherweise aufgebrachten Kunden wirkt vor dem Hintergrund, dass es sich um ein DRM-System handelt, besonders paradox: man empfahl den Kunden kurzerhand die in Deutschland illegale Umgehung des in die Musikwerke eingebundenen Kopierschutzes per Anleitung auf der eigenen Internetseite (vgl. Kreutzer 2007: 103ff., 135ff.; Lischka 2008; Microsoft 2009; Pantalog 2008; Schollin 2008: 147).

Der Fall *Playsforsure* verdeutlicht, neben dem Chaos durch die – zumindest bislang – fehlende Standardisierung, die Defizite im Umgang mit DRM-Systemen sowohl bei den Produzenten digitaler Waren als auch deren Kunden. Letztere gehen beispielsweise völlig selbstverständlich davon aus, dass sie über die von ihnen legal erworbenen digitalen Werke im gleichen Umfang frei verfügen können, wie sie es bislang im Umgang mit *stofflichen* Produkten gewohnt waren (vgl. Kreutzer 2001; Lohoff 2007; Meretz 2007: 52ff.).

Ein einfaches Beispiel soll das Dilemma verdeutlichen: Kein Buchhändler wird sich weder ernsthaft darüber beklagen, noch rechtliche Bedenken äußern, für den nicht ganz ungewöhnlichen Fall, dass ein Kunde das bei ihm erworbene Buch weiter verschenkt, verleiht oder gar verkauft. Viele Kunden wissen jedoch nicht, dass sich der Fall bei digitalen Inhalten meist völlig anders verhält. Nehmen wir also an, derselbe Kunde erwirbt ein digitales E-Book. So schließt beispielweise Amazon, der Anbieter des populären E-Books *Kindle*, eine Weitergabe, einen Weiterverkauf und sogar einen Verleih der digitalen Bücher kategorisch über seine Geschäftsbedingungen aus:

> »Unless specifically indicated otherwise, you may not sell, rent, lease, distribute, broadcast, sublicense or otherwise assign any rights to the Digital Content or any portion of it to any third party, and you may not remove any proprietary notices or labels on the Digital Content. In addition, you may not, and you will not encourage, assist or authorize any other person to, bypass, modify, defeat or circumvent security features that protect the Digital Content.« (Amazon 2009)

Und natürlich sichert sich Amazon darüber hinaus auch für den Fall ab, dass das eigene DRM-System nicht mehr weiter zur Verfügung stehen sollte:

> »Your rights under this Agreement will automatically terminate without notice from Amazon if you fail to comply with any term of this Agreement. In case of such termination, you must cease all use of the Software and Amazon may immediately revoke your access to the Service or to Digital Content without notice to you and without refund of any fees. Amazon's failure to insist upon or enforce your strict

> compliance with this Agreement will not constitute a waiver of any of its rights.« (Amazon 2009)

Häufige Kritik gibt es darüber hinaus für DRM-Systeme im Zusammenspiel mit dem gesetzlich geforderten Datenschutz. Grundsätzlich darf dieser zwar nicht berührt werden, tatsächlich gibt es aber in diesem Bereich teilweise erhebliche Defizite.

Beispielweise codierte Apple in seinem DRM-System *Fairplay* für *iTunes* die Apple-Benutzerkennung eines Kunden – in der Regel also dessen E-Mail-Adresse – direkt und unverschlüsselt (!) in die an ihn verkauften digitalen Werke ein. Obwohl dies gesetzlich zwingend erforderlich gewesen wäre, erfuhr der Verbraucher von dieser Praxis nichts im Rahmen des Kaufvorgangs oder innerhalb der Datenschutzerklärung, welcher der Kunde vorab ausdrücklich zustimmen musste. Die erforderliche Transparenz gegenüber den Kunden bezüglich des Einsatzes und der Verwendung derer persönlicher Daten fehlte also. Nebenbei bemerkt – vor diesem Hintergrund betrachtet scheint die Bezeichnung *Fairplay* für Apples DRM-System mehr als paradox (vgl. Bizer 2009: 95ff.; Kreutzer 2007: 103ff.; 135ff.; Mittenzwei 2006: 23ff.).

Aber auch die Kunden bewegen sich beim Thema Kopierschutz und DRM oft in einer rechtlichen Grauzone. Entgegen der häufigen Annahme gibt es beispielsweise kein gesetzlich eindeutig definiertes Recht auf Privatkopien. Zwar wird das Urheberrecht in Bezug auf private Vervielfältigungen eingeschränkt, allerdings ist es unter keinen Umständen erlaubt zu diesem Zwecke einen Kopierschutz zu umgehen. Selbst die Vorbereitung der Umgehung eines DRM-Systems ist nicht zulässig und strafbar. Grundsätzlich verhalten sich die gesetzlichen Regelungen gerade beim Thema Privatkopie sehr schwammig. So gibt es beispielsweise eindeutige Vorgaben für die Privatvervielfältigungen von Büchern, ob damit aber auch Texte die digital zur Verfügung stehen, gemeint bzw. abgegolten sind, bleibt weitgehend offen (vgl. Fränkl 2004: 49ff.; Kronner 2008: 101ff.; von Diemar 2002: 40ff.).

Das Phänomen der sog. Raubkopien ist dabei in jeder sozialen Schicht und auch unabhängig vom Alter anzutreffen. Dies begründet sich vor allem darin, dass für die Vervielfältigung kein spezielles Verständnis oder Wissen benötigt wird. Grundlegende Kenntnisse im Umgang mit dem Heim-Computer und der entsprechenden Software reichen völlig aus (vgl. Kühne 2009: 32). Die Beweggründe, unberechtigte Kopien zu erstellen, sind dabei durchaus unterschiedlich. Vielen Raubkopierern geht es nicht in erster Linie um die digitalen Inhalte selbst, sondern eher um Anerkennung in einer Art Wettbewerb um digitalen Medien und um deren Neuheit und Menge. Aber natürlich spielen auch finanzielle Interessen eine Rolle, was sich letztlich auch im Umsatzrückgang z.B. der Musikindustrie widerspiegelt. Schließlich, aber sehr wesentlich, führen die neuesten technischen Entwicklungen, die von den Produzenten digitaler Medien angetrieben werden, dazu, dass die Vervielfältigungsmöglichkeiten zunehmend simpler werden und gleichzeitig sinkt die Hemmschwelle der Konsumenten, illegal zu kopieren. In diesem Zu-

sammenhang sind vor allem das MP3-Format und die diversen Onlineshops zu erwähnen, das Video on Demand-Verfahren (VoD) im Filmbereich sowie Hörbücher und E-Books auf dem Literaturmarkt (vgl. ebd.: 36-40).

Die Medienproduzenten setzen deshalb zunehmend auf die Entwicklung von neuen Kopierschutzmechanismen. Das Problem ist nur, dass parallel dazu die entsprechende illegale Kopiersoftware entwickelt wird, bzw. »Hacker« vor allem über das Internet sehr zeitnah Möglichkeiten zur Umgehung solcher Schutzmechanismen preisgeben. Da die Effektivität der Kopierschütze deshalb nur sehr begrenzt ist, setzen vor allem die großen Produzenten parallel dazu auf die Sensibilisierung der Konsumenten durch *Aufklärungskampagnen*, die dem Verbraucher verdeutlichen sollen, dass Raubkopieren eine Straftat darstellt (vgl. ebd. 63ff.; Krempl 2004b).

Eine weitere Maßnahme stellen Urheberrechtserweiterungen des Gesetzgebers dar. Zwar bleiben Privatkopien weiter zulässig, allerdings nur dann, wenn das Originalmedium vorliegt und für eine Kopie nicht ein Kopierschutz umgangen werden muss (vgl. ebd.: 66ff.; Meretz 2007: 77). »Auf der einen Seite sind Privatkopien erlaubt, gleichzeitig ist aber nicht erlaubt, einen Kopierschutz zu umgehen, womit das eine das andere relativiert« (Kühne 2009: 107).[11] Schließlich gibt es heutzutage nahezu kein Medium mehr, das nicht mit einem Kopierschutz versehen ist. Tatsächlich liegt das Problem auf Seiten der Medienproduzenten. Diese haben offensichtlich schlichtweg den Zeitpunkt verpasst, ihren Angebote dem heutigen digitalen Umfeld anzupassen (vgl. ebd.: 108f.; Lodigkeit 2006: 98ff.).

Zusammenfassend lässt sich festhalten, dass DRM-Systeme insbesondere durch die Musikindustrie eingesetzt wurden, aber bereits kurze Zeit später – vor allem auf Grund mangelnder Akzeptanz durch die Verbraucher – wieder vom Markt verschwanden. So bietet beispielsweise Apples *iTunes* seit Anfang 2009 fast sein gesamtes Sortiment DRM-frei an.[12] Auch der Mitbewerber *Musicload* hat nachgezogen.

Beliebt war und ist die digitale Rechteverwaltung verständlicherweise nie beim Verbraucher, da sie ihn einschränkt (Kühne 2009: 98ff.). Allerdings auch deshalb, weil es keinen einheitlichen Standard gibt, der die permanente Verfügbarkeit sichert. Während ein Buch mit relativ hoher Wahrscheinlichkeit auch noch in 100 Jahren gelesen werden kann, verhält sich dies mit einem E-Book anders und setzt zumindest voraus, dass das entsprechende DRM-System noch läuft und die erworbene Lizenz auch noch Gültigkeit besitzt.

11 Vgl. dazu den Beitrag von Martin Senftleben im Heft »Kulturen des Kopierschutzes I«.

12 Siehe dazu auch: http://www.pcwelt.de/it-profi/business-ticker/76271/drm_freie_songs_branche_bejubelt_emi_und_apple/, 05.10.2009.

8. ARGUMENTE GEGEN EINEN KOPIERSCHUTZ DIGITALER INHALTE UND GRÜNDE FÜR DEN MISSERFOLG VON DRM-SYSTEMEN

Technische Entwicklungen der vergangenen Jahrzehnte haben zu tiefgreifenden Veränderungen und Fortschritten bei Vervielfältigungs- und Übermittlungstechniken von Werken aller Art geführt. Auch wenn einzelne technische Entwicklungen für sich alleine genommen keine größeren Auswirkungen hatten, so haben diese in Kombination doch erhebliche Veränderungen bewirkt (vgl. Höhne 2007: 2). DRM stellt kein klassisches und eindeutiges Verfahren zum Schutz und der Verwaltung von Rechten oder der Wahrung eines Kopierschutzes dar, sondern beschreibt vielmehr eine komplexe Infrastruktur, die auf verschiedenen Basistechnologien aus unterschiedlichen Bereichen basiert. Zum technischen Verständnis von DRM ist daher die Kenntnis solcher klassischen Technologien erforderlich.

In der digitalen Zeit ist es in der Regel leicht, Kopien von Daten jeglicher Art anzufertigen.[13] Die Maßnahmen, die unternommen werden, um das Kopieren zu unterbinden oder zumindest zu erschweren, sind enorm aufwendig und kostenintensiv. Allerdings sind sie in der Regel auch bereits nach kurzer Zeit wieder veraltet bzw. können mit vergleichsweise geringem Aufwand umgangen werden (vgl. Kühne 2009: 107ff.). Das Thema wird kontrovers diskutiert.

Insbesondere das »Recht auf Privatkopie« wird in diesem Zusammenhang regelmäßig aufgegriffen. So kritisiert beispielsweise der *Chaos Computer Club* (CCC), dass Konsumenten, insbesondere durch die Kampagnen der Musik- und Filmindustrie, regelrecht zu potenziellen Straftätern abgestempelt werden. Auch das Urheberrecht steht in der Kritik, da es das Grundrecht auf Informationsfreiheit einschränke[14] (vgl. Kühne 2009: 78ff.). Der CCC ruft sogar zum Boykott der Musikindustrie auf, weil der Verein der Industrie unterstellt, die Verkaufserlöse zu einem wesentlichen Teil zur Finanzierung von Klagen und für die Entwicklung neuer Kopierschütze einzusetzen. Die Gründe für die sinkenden Verkaufszahlen sieht der CCC in den zu hohen Preisen für CD und DVD bei gleichzeitig gesunkener Qualität. Außerdem hindere der Kopierschutz oftmals den Konsumenten daran, die legal erworbenen Inhalte auf dem eigenen CD-Player wiederzugeben. Auch die Initiative »Recht auf Privatkopie«[15] setzt sich gegen die Beschränkungen durch das Urheberrecht ein.

Andererseits ist ein ökonomischer Schaden durch unerlaubte Vervielfältigungen nicht zu leugnen.[16] Auch Bibliotheken und Informationszentren, aber auch Vi-

13 Eine Ausnahme stellen hier beispielweise viele strategisch wichtige staatliche Dokumente dar, zu deren Verschlüsselung und Geheimhaltung von Seiten der offiziellen Stellen erheblicher Aufwand betrieben wird. Siehe dazu den Beitrag von Ludwig Andert und Doris Ortinau im Heft »Kulturen des Kopierschutzes I«.

14 Weitere Informationen zum *Chaos Computer Club*: http://www.ccc.de, 27.10.2009.

15 Vgl.: http://www.privatkopie.net, 13.11.2009.

16 Vgl.: http://www.musikindustrie.de/jwb_musikkopien07.html, 13.11.2009.

deotheken leiden unter Raubkopien. Beschränkte sich die illegale Vervielfältigung erst noch auf das Kopieren von Büchern oder Zeitschriften mit einem herkömmlichen Fotokopierer, nehmen nun die Diebstähle digitaler Inhalte zu. Natürlich untersagen die entsprechenden Institutionen diese Nutzung in ihren Allgemeinen Geschäftsbedingungen. Allerdings nimmt der Verkauf solcher Medien parallel über neue Distributionswege zu.[17] Dass der ökonomische Schaden allein auf die Verbreitung entsprechender Kopiersoftware zurückzuführen ist, darf also bezweifelt werden.

Zumindest muss bedacht werden, dass der CCC mit seiner Kritik an der Qualität durchaus nicht Unrecht hat. Zudem sind Online-Musikshops ja durchaus erfolgreich und wären möglicherweise bei einem entsprechend größerem Angebot (wie es beispielsweise von Tauschbörsen angeboten wird) noch wesentlich populärer. Jedenfalls scheint es zu einfach, den Verbrauchern zu unterstellen, dass sie nicht mehr bereit wären, für digitale Inhalte zu bezahlen.

Generell lässt sich feststellen, dass DRM-Systeme zusammen mit einer Ausweitung des Urheberrechts zu einer deutlichen Verschlechterung des Verbraucherschutzes geführt haben, da Nutzungsbedingungen digitaler Werke nun über Vertragswerke und nicht mehr über das Urheberrecht allein geregelt werden (vgl. Strube 2008; Akester 2010). Dies hat zur Folge, dass die Rechteinhaber, also die Produzenten digitaler Werke, sich in einer – entgegen der von ihnen selbst oftmals öffentlich inszenierten Darstellung – sehr starken Position gegenüber dem Nutzer befinden. Auch Bürger- und Datenschutzrechte werden von Rechteverwaltungssystemen tangiert, denn »wenn etwa DRM-Systeme überwachen sollen, dass nur bestimmte, berechtigte Personen einen Inhalt nutzen, heißt das auch, dass sie wissen müssen, wer sie nutzt« (Spielkamp 2005). Darüber hinaus sind die, wie bereits erwähnt, fehlenden Standards bei den derzeit eingesetzten DRM-Systemen alles andere als verbraucherfreundlich. Praktisch muss für jeden digitalen Content ein eigenes DRM-System installiert werden und bei einem Anbieterwechsel wird in der Regel sogar die Anschaffung neuer Abspielgeräte zwingend erforderlich (Höhne 2007: 250ff.).

Schon deshalb scheint es nur konsequent, dass auch über völlig neue Bezahlsysteme für digitale Inhalte diskutiert wird (vgl. Umeh 2007). So gibt es beispielsweise Überlegungen, pauschale Abgaben für Breitbandanschlüsse oder Abspielgeräte einzuführen, ähnlich dem in Deutschland bestehenden Rundfunkgebührensystem (Krempl 2004a; Spielkamp 2004). Allerdings werden auch weiter Alternativen zu den derzeit eingesetzten DRM-Systemen gesucht. So wurden etwa in Deutschland von der Fraunhofer Gesellschaft zwei Systeme entwickelt, die auf unterschiedlichen Konzepten basieren:

Das sog. *Light Weight Digital Rights Management* (LWDRM)[18] implementiert ein DRM-System, welches dem Nutzer mehr Freiheiten insbesondere bei der

17 Vgl.: http://www.ivd-online.de/f_markt.html, 10.11.2009.

18 Vgl.: http://www.emt.iis.fhg.de/de/projekte_themen/ lwdrm.htm, 20.11.2009.

Weitergabe digitaler Inhalte einräumt. Allerdings hat es wieder einen entscheidenden Nachteil, da LWDRM die digitalen Inhalte in einem eigenen Dateiformat verschlüsselt, so dass diese nur auf speziellen Wiedergabegeräten wieder entcodiert werden können.

Das zweite alternative System *Potato*[19] arbeitet dagegen völlig ohne Verschlüsselung und Markierung digitaler Inhalte und versucht deren unberechtigte Weitergabe allein über wirtschaftliche Anreize zu minimieren. So erhalten Nutzer Verkaufsprovisionen, wenn sie ein legal erworbenes digitales Werk anstatt über Tauschbörsen im Rahmen eines speziell zur Verfügung gestellten Reseller-Systems anderen Nutzern zur Verfügung stellen. Letztere müssen dafür allerdings bezahlen. Gerade das Potato-Modell scheint dabei zumindest für populären digitalen Content vielversprechend zu sein, ist derzeit aber nicht besonders praktikabel, da auch für dieses – wie schon für die bereits eingesetzten DRM-Systeme – noch keine einheitlichen Standards existieren. Eine dauerhafte Lösung, die verbraucherfreundlich ist und zugleich Profite einbringt, die also gleichermaßen attraktiv für die Konsumenten als auch die Produzenten digitaler Inhalte ist, scheint jedenfalls in naher Zukunft nicht in Sicht (vgl. Grimm et al 2002; Höhne 2007: 76ff.; Kühne 2009: 83ff., 110ff.; Nützel 2003).

LITERATURVERZEICHNIS

Abie, Habtamu (2009): *Distributed Digital Rights Management: Frameworks, Processes, Procedures and Algorithms*, Saarbrücken: VDM Verlag.

Agnew, Grace (2008): *Digital Rights Management: A Librarian's Guide to Technology and Practise*, Oxford: Chandos Publishing (Oxford) Limited.

Akester, Patricia (2010): »The Impact of Digital Rights Management on Freedom of Expression: the First Empirical Assessment«, in: *IIC: International Review of Intellectual Property and Competition Law,* Bd. 41, Nr. 1, S. 31-58.

Amazon (2009): »Amazon Kindle: License Agreement and Terms of Use«, http://www.amazon.com/gp/help/customer/display.html?nodeId=20014453, 11.09.2009.

Bizer, Johann (2009): »Datenschutzgerechte Rechteverwaltung«, in: Roßnagel, Alexander (Hg.): *Digitale Rechteverwaltung*, Baden-Baden: Nomos, S. 91-104.

Eggert, Denis (2005): *Digital Music Service, Digital Rights Management & Alternativen. Bestandsaufnahme, Analyse und Perspektiven des deutschen Marktes*, Bochum: projektverlag.

Fränkl, Gerald (2005): *Digital Rights Management in der Praxis. Hintergründe, Instrumente, Perspektiven, (und) Mythen,* Berlin: VDM Verlag Dr. Müller.

19 Vgl.: http://www.idmt.fraunhofer.de/de/projekte_themen/ potato.htm, 20.11.2009 sowie http://www.potatosystem.com/de/, 10.01.2010.

Fränkl, Gerald / Karpf, Phlipp (2004): *Digital Rights Management Systeme. Einführung, Technologien, Recht, Ökonomie und Marktanalyse,* München: Pg Medien.

Grassmuck, Volker (2004): *Freie Software. Zwischen Privat- und Gemeineigentum*, Bonn: bpb.

Grimm, Rüdiger (2009): »Digitale Rechteverwaltung als Techniksystem«, in: Roßnagel, Alexander (Hg.): *Digitale Rechteverwaltung*, Baden-Baden: Nomos, S. 27-38.

Grimm, Rüdiger / Nützel, Jürgen (2002): »A Friendly Peer-to-Peer File Sharing System with Profit but without Copy Protection«, in: Unger, Herwig et al. (Hg.): *Innovative Internet Computing Systems*, Berlin: Springer-Verlag, S. 133-142.

Höhne, Sven (2007): *Digital Rights Management System aus Verbrauchersicht. Eine urheberrechtliche Untersuchung der Folgen des Einsatzes von Digital Rights Management Systemen*, Norderstedt: Books on Demand GmbH.

Krempl, Stefan (1998): »Copyright«, http://www.heise.de/tp/r4/artikel/2/2471/1.html, [17.11.1998], 18.12.2009.

Krempl, Stefan (2001): »Kopieren verboten«, http://www.heise.de/tp/r4/artikel/4/4756/1.html, [24.01.2001], 18.11.2009.

Krempl, Stefan (2004a): »Alternatives Kompensationssystem für Künstler verzweifelt gesucht«, http://www.heise.de/newsticker/meldung/Alternatives-Kompensationssystem-fuer-Kuenstler-verzweifelt-gesucht-92745.html, [01.02.2004], 18.12.2009.

Krempl, Stefan (2004b): »Raubkopierer sind immer noch Verbrecher«, http://www.heise.de/tp/r4/artikel/18/18923/1.html, [30.11.2004], 18.12.2009.

Kreutzer, Till (2001): »Selbsthilferecht zum Umgehen von Kopierschutz. Die Zukunft der privaten Nutzung nach der Umsetzung der europäischen Urheberrechts-Richtlinie«, http://www.heise.de/tp/r4/artikel/9/9817/1.html, [18.10.2001], 05.12.2009.

Kreutzer, Till (2007): *Verbraucherschutz bei digitalen Medien*, Berlin: Berliner Wissenschafts-Verlag.

Kronner, Ralf (2008): *Digitaler Werktransfer: Zum Interessengleichgewicht zwischen Verwertern, Nutzern und dem Gemeinwohl*, Berlin: Olaf Gaudig & Peter Veit GbR.

Kühne, Sascha (2009): *Phänomen Raubkopie. Illegale Vervielfältigung von Medien im Digitalen Zeitalter,* Saarbrücken: VDM Verlag Dr. Müller.

Lischka, Konrad (2008): »DRM-Debakel. Bürgerrechtler wüten gegen Microsoft-Musik mit Verfallsdatum«, http://www.spiegel.de/netzwelt/web/0,1518,550686,00.html, [30.04.2008], 20.08.2009.

Lodigkeit, Klaus (2006): *Intellectual Property Rights in Computer Programs in the USA and Germany*, Frankfurt a.M.: Peter Lang GmbH.

Lohoff, Ernst (2007): »Der Wert des Wissens«, http://www.krisis.org/2007/der-wert-des-wissens/print/, 05.12.2009.

Meretz, Stefan (2007): »Der Kampf um die Warenform. Wie Knappheit bei Universalgütern hergestellt wird«, in: *krisis. Beiträge zur Kritik der Warengesellschaft*, Nr. 31.

Microsoft (2009): »Informationen über Windows Media DRM«, http://www.microsoft.com/windows/windowsmedia/de/drm/default.aspx, 26.10.2009.

Mittenzwei, Julius (2006): *Informationen zur Rechtewahrung im Urheberrecht. Der Schutz von Digital Rights Management-Systemen und digitalen Wasserzeichen durch § 95c UrhG*, München: GRIN Verlag.

Nützel, Jürgen (2003): »Wie kann man mit dem Potato-System eine Ware verkaufen, die alle schon haben?«, http://www.4fo.de/download/Tonmeister02_Nuetzel.pdf, [20.05.2003], 10.01.2010.

Pantalog, Frank (2008): »Amazon komplett DRM-frei. Kopierschutz ist tot«, http://www.spiegel.de/netzwelt/web/0,1518,527992,00.html, [11.01.2008], 15.08.2009.

Roßnagel, Alexander (2009): »Digitale Rechteverwaltung - Ein gelungenes Beispiel für die Allianz von Recht und Technik?«, in: Roßnagel, Alexander (Hg.): *Digitale Rechteverwaltung*, Baden-Baden: Nomos, S. 15-26.

Schippan, Martin (2004): »Rechtsfragen bei der Implementierung von Digital Rights Management-Systemen«, in: *Zeitschrift für Urheber- und Medienrecht*, Ausgabe 3/2004, S. 188-198.

Schollin, Kristoffer (2008): *Digital Rights Management. The New Copyright*, Stockholm: Jure Förlag.

Singh, Simon (2000): *Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet*, München.

Spielkamp, Matthias (2004): »Mit Technik allein lässt sich DRM nicht durchsetzen«, http://www.heise.de/tp/r4/artikel/16/16673/1.html, [03.02.2004], 05.01.2010.

Spielkamp, Matthias (2005): »Rechte oder Restriktionen?«, http://irights.info/index.php?id=140, [01.04.2005], 11.01.2010.

Strube, Jochen (2008): »Der Einfluss von Digital Rights Management auf die Zahlungsbereitschaften für Online-Musik: Untersuchung auf Basis einer Conjoint-Analyse«, in: *Medienwirtschaft*, Bd. 5, Nr. 4, S. 6-15.

von Diemar, Undine (2002): »Die digitale Kopie zum privaten Gebrauch«, in: *Schriftenreihe der Stipendiatinnen und Stipendiaten der Friedrich-Ebert-Stiftung*, Band 17.

Tsolis, Dimitrios (2009): *Digital Rights Management for E-commerce Systems*, Hershey u.a.: Information Science Reference.

Umeh, Jude C. (2007): *The World Beyond Digital Rights Management*, Swindon: British Computer Society.

Zeng, Wenjun (2006) (Hg.): *Multimedia Security Technologies for Digital Rights Management*, Amsterdam: Academic Press.