Identifikationszwecken, d.h. zur Feststellung, ob ein digitales Multimediawerk bestimmten Rechten Dritter unterliegt, wem diese Rechte zustehen und welchen Umfang diese Rechte haben, vorwiegend sogenannte „rights expression languages" eingesetzt.[125] Im Zusammenhang mit der Verhinderung des unerlaubten Zugriffs und der unerlaubten Nutzung eines digitalisierten Multimediawerks spielen hingegen Verschlüsselungstechnologien eine wichtige Rolle.[126]

In der nachfolgenden Darstellung ist unter dem Begriff DRM bzw. DRM-Systeme durchweg die technologisch gesteuerte Verwaltung und Sicherung von Rechten und Nutzungsbedingungen im Zusammenhang mit digitalen Multimediawerken zu verstehen, d.h. DRM im engeren Sinne. Darüber hinaus bezieht sich der Begriff vor allem im Rahmen der Ausführungen zum Scheitern von DRM-Systemen im Zusammenhang mit dem Vertrieb von Musikdownloads[127] in erster Linie auf DRM-Systeme der ersten Generation, d.h. auf Technologien, die vorwiegend auf die Einschränkung der Möglichkeit der Vervielfältigung sowie der Übertragbarkeit von digitalen Multimediawerken gerichtet sind. Solche DRM-Systeme werden nachfolgend verkürzt auch als Kopierschutztechnologien bezeichnet.[128]

B. Technischer Hintergrund

Im folgenden Abschnitt werden der Aufbau von DRM-Systemen sowie die Technologien, die hierbei typischerweise eine Rolle spielen, in Grundzügen dargestellt.[129] Grundsätzlich gibt es nicht „die eine" DRM-Technologie im Sinne einer identischen, fest gefügten technologischen Einheit. Vielmehr setzt sich jedes einzelne DRM-System aus einer Vielzahl unterschiedlicher Komponenten zusammen, die im Gesamtsystem des jeweiligen DRM-Systems eine bestimmte Funktion erfüllen.[130]

I. Grundstruktur von DRM-Systemen

Im Rahmen eines durch ein DRM-System betreuten Prozesses zur Lieferung eines digitalen Multimediawerks (im Rahmen dieses Kapitels nachfolgend als „Inhalt"

125 *Ünlü*, Content Protection, 2005, S. 47.
126 *Ünlü* s.o.
127 Vgl. 5. Kapitel, Teil A.
128 *Flechsig*, in: FS. *Nordemann*, 2004, S. 313, 317.
129 Weiterführend vgl. die sehr ausführliche Darstellung bei *Bechtold*, DRM, 2002, S. 23-101; *Fränkl/Karpf*, DRMS, 2004, S. 29-55; *Ünlü*, Content Protection, 2005, S. 60-84.
130 *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007, S. 34-35; *Arlt*, DRMS, 2006, S. 13; *ders*., GRUR 2004, S. 548, 549.

bezeichnet) an einen Nutzer lassen sich – bei allen Unterschieden zwischen verschiedenen DRM-Systemen im Detail – im Wesentlichen drei Phasen unterscheiden: die Verpackung des Inhalts zusammen mit wesentlichen, darauf bezogenen Informationen auf Ebene des „content server", die Hinzufügung von Informationen über den Umfang der erlaubten Nutzung durch den „license server" sowie die Anforderung und Lieferung des Inhalts über den Computer des Nutzers, den „client".[131]

Auf der Ebene des *content servers* wird der Inhalt durch eine Software, den „content packager", mit bestimmten Informationen[132] versehen und in einer Datei verpackt. Diese Datei wird mit Hilfe einer vom Rechtsinhaber gewählten Technologie verschlüsselt.[133] Dieses durch den *content packager* geschnürte Paket wird auf Ebene des *license server* mit Hilfe einer weitere Software, dem „DRM license generator", mit Informationen über die Nutzungsrechte versehen, die einem Nutzer an dem Inhalt seitens des Rechtsinhabers eingeräumt werden. Diesem Datenpaket wird aus einer Datenbank ein Schlüssel zugeordnet, mit dessen Hilfe die Datei wieder entschlüsselt werden kann.

Auf der Ebene des *client* sorgt eine Software, der „DRM controller",[134] dafür, dass der Computer des Nutzers mit dem *license server* bzw. dem *content server* kommunizieren kann. Der *DRM controller* ist gleichzeitig Ausgangs- und Endpunkt des Kommunikationsprozesses zwischen *content server*, *license server* und *client*. Über ihn wird dieser Kommunikationsprozess zunächst angestoßen, indem der Nutzer mit seiner Hilfe beispielsweise den Download einer bestimmten Tonaufnahme beim *content server* abfragt. Daraufhin führen *content* und *license server* die oben dargestellten Prozesse durch. Bevor jedoch der *DRM license generator* die Informationen betreffend die Nutzungsrechte und die Entschlüsselung an den *client* überträgt, verifiziert er zuvor über den *DRM controller* die Identität des Nutzers.

Weiterhin findet vor der Lieferung in der Regel ein Zahlungsvorgang statt. Dessen genauer Zeitpunkt hängt von dem einzelnen Geschäftsmodell ab, innerhalb dessen das jeweilige DRM-System eingesetzt wird. Bei einem sogenannten „direct download"-Modell findet beispielsweise die einmalige Zahlung regelmäßig vor der Lieferung des Download an den *client* statt. Im Falle eines Abonnement-Modells wird hingegen sowohl nach der ersten Registrierung des Nutzers im Voraus für die

131 Die nachfolgende Darstellung basiert im Wesentlichen auf den Ausführungen bei *Montagnani*, 26 Cardozo Arts & Ent. L.J. 719, S. 742-744; s.a. *Ünlü*, Content Protection, 2005, S. 41.

132 Wie beispielsweise die Identität des Rechtsinhabers.

133 Handelt es sich nicht um ein Download- sondern ein Streaming-Angebot, das ebenfalls mit DRMS verknüpft werden kann, so wird nur die Information über den Inhalt in der Datei verpackt und bereitgestellt, da der Inhalt selbst im Gegensatz zum Download nicht an den Nutzer ausgeliefert wird.

134 Beispielsweise die Abspielsoftware „Windows Media Player" von Microsoft.

Bereitstellung der durch das Abonnements gewährten Nutzungsmöglichkeiten für einen bestimmten Zeitraum gezahlt, sowie im Anschluss daran in regelmäßigen Intervallen abhängig von der Laufzeit des Abonnements.

II. Technologien

Nachfolgend wird die Funktionsweise von Verschlüsselungstechnologien sowie von Metadaten, Rights Expression Languages und Wasserzeichen kurz skizziert.

1. Verschlüsselungstechnologien

Diese Technologien spielen im Zusammenhang mit dem Schutz von digitalen Multimediawerken vor unberechtigtem Zugriff und vor unerlaubten Nutzungshandlungen eine wichtige Rolle. Denn durch Verschlüsselungsalgorithmen wird sichergestellt, dass nur ein Nutzer, der über eine entsprechende Berechtigung verfügt, eine Multimediawerk nutzen kann.[135] Denn ein verschlüsselter Inhalt ist ohne den entsprechenden Schlüssel für den Empfänger nutzlos.[136] Diese sogenannten „kryptographischen Technologien" stellen die am weitesten entwickelte Gruppe von DRM-Technologien dar, die daher ein relativ hohes Schutzniveau gewähren.[137]

Es ist zu unterscheiden zwischen symmetrischen, asymmetrischen und hybriden Verschlüsselungsverfahren. Im Falle eines symmetrischen Algorithmus (sogenannte „private key"-Kryptographie) verwenden sowohl der Absender als auch der Empfänger denselben Schlüssel, um die das digitale Multimediawerk enthaltende Datei zu ver- bzw. entschlüsseln.[138] Der Nachteil des symmetrischen Algorithmus besteht in der Notwendigkeit, den „private key" zusammen mit der verschlüsselten Datei an den Adressaten zu übermitteln. Denn zum einen sind mit der Generierung und Übermittlung eines eigenen Schlüssels an jeden Adressaten Kosten verbunden, und zum anderen geht mit der Übermittlung des Schlüssels ein Sicherheitsrisiko einher, da, wenn das Multimediawerk mitsamt dem Schlüssel während der Übermittlung über das Internet von einem Dritten abgefangen wird, dieser das Multimediawerk ohne weiteres decodieren und nutzen kann.[139]

135 *Ünlü*, Content Protection, 2005, S. 68.
136 *Bechtold*, DRM, 2002, S. 23.
137 *Ünlü*, Content Protection, 2005, S. 69; *Bechtold*, DRM, 2002, S. 33.
138 *Ünlü*, Content Protection, 2005, S. 69; bekannte *private-key*-Verfahren sind der Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard und International Data Encryption Standard (IDEA); *Bechtold*, DRM, 2002, S. 23 m.w.N.
139 *Bechtold*, DRM, 2002, S. 24; *Ünlü*, Content Protection, 2005, S. 69.

Hingegen kommen bei einer Technologie, die einen asymmetrischen Algorithmus verwendet (sogenannte „public key"-Kryptographie), in Bezug auf die Ver- und Entschlüsselung jeweils unterschiedliche Schlüssel zum Einsatz. Zum einen im Rahmen der Verschlüsselung ein „public key", der öffentlich bekannt und in einer Datenbank abgelegt ist, und weiterhin zur Entschlüsselung ein *private key*, der nur dem Empfänger bekannt ist und bei diesem verbleibt.[140] Das *public-key*-Verfahren ist computertechnisch komplexer – und damit langsamer – als das *private-key*-Verfahren und erfordert zudem die Errichtung einer Infrastruktur, über die der öffentlich verfügbare Schlüssel verwaltet wird.[141]

Im Rahmen des dritten, hybriden Verschlüsselungsverfahrens werden symmetrische und asymmetrische Algorithmen miteinander kombiniert.[142] Dabei wird die das Multimediawerk enthaltende Datei mit Hilfe eines symmetrischen Algorithmus verschlüsselt, der für die Codierung verwendete Schlüssel hingegen asymmetrisch codiert, bevor Datei und Schlüssel gemeinsam an den Adressaten übermittelt werden. Aufgrund der asymmetrischen Codierung des Schlüssels ist es nur dem berechtigten Empfänger möglich, diesen mit Hilfe des bei ihm deponierten *private key* zu entschlüsseln, wodurch eine Minimierung des Risikos der Übermittlung des Schlüssels zur Dekodierung der Datei über das Internet erreicht wird. Da jedoch nicht für die Datei, sondern nur für den zur Decodierung notwendigen Schlüssel, der wesentlich kleiner als die Datei ist, ein asymmetrischer Algorithmus eingesetzt wird, hält sich die computertechnische Komplexität des Übermittlungsvorgangs in Grenzen.

2. Metadaten, Rights Expression Languages und Wasserzeichen

Zum Zweck der Identifizierung und Verwaltung von Rechten durch DRM-Systeme kommen vor allem Metadaten, Rights Expression Languages und Wasserzeichen zum Einsatz.

Durch Metadaten werden „Informationen über Informationen" in standardisierter Form weitergegeben, so dass sie automatisiert verarbeitet und ausgelesen werden können.[143] Die mitgeteilten Informationen können in einer Beschreibung der charakteristischen Merkmale eines digitalisierten Inhalts, der Nutzungsbedingungen, denen ein solcher Inhalt unterliegt, oder aber in Informationen über den Nutzer bestehen, an den ein solcher Inhalt übermittelt wird.

140 *Ünlü*, Content Protection, 2005, S. 69; Beispiele für das *public-key*-Verfahren sind RSA und El Gamal; *Bechtold*, DRM, 2002, S. 24.
141 *Ünlü*, Content Protection, 2005, S. 70; *Bechtold*, DRM, 2002, S. 25.
142 *Bechtold*, DRM, 2002, S. 26.
143 *Bechtold*, DRM, 2002, S. 35 ff.

Eigens zur standardisierten Beschreibung von Nutzungsbedingungen wurden spezielle formalisierte sogenannte „rights expression languages" („REL") entwickelt, anhand derer diese Bedingungen in für Computer verständlicher Form einheitlich ausgedrückt werden können. [144] Mit Hilfe von REL ist es möglich, den Umfang der einem Nutzer in Bezug auf ein digitalisiertes Multimediawerk gewährten Rechte festzuhalten, wie beispielsweise Dauer und Häufigkeit der Nutzung, Qualität der Wiedergabe, die dem Nutzer erlaubten Handlungen sowie das vom Nutzer für die Vornahme einer solchen Handlung jeweils zu entrichtende Entgelt.[145] Die beiden bekanntesten REL-Standards sind die „eXtensible rights Markup Language" (XrML) sowie die „Open Digital Rights Language" (ODRL).[146]

Um Metadaten möglichst untrennbar mit einem digitalen Multimediawerk zu verbinden, werden Wasserzeichen-Technologien eingesetzt, die diese Informationen unmittelbar mit der digitalen Kopie des Multimediawerks verweben.[147] Eine qualitativ hochwertige Wasserzeichen-Technologie zeichnet sich dadurch aus, dass sie den jeweiligen digitalen Inhalt, dem sie Metadaten hinzufügt, nur geringfügig verändert, so dass diese Veränderung vom Nutzer nicht sinnlich wahrgenommen werden kann. Zudem darf ein Wasserzeichen nicht entfernt werden können, ohne dass der Inhalt, dem es hinzugefügt wurde, dadurch beschädigt wird.[148] Wasserzeichen-Technologien werden auch dazu eingesetzt, um digitale Multimediawerke im Internet nachzuverfolgen. Dadurch wird nachvollzogen, aus welcher Quelle ein digitales Multimediawerk ursprünglich stammt und auf welchem Weg es an den Ort gelangt ist, an dem es vom Rechtsinhaber letztlich aufgefunden wurde – beispielsweise in einem illegalen Filesharing-Netzwerk.

III. Beispiele für in der Multimediaindustrie eingesetzte DRM-Systeme

1. CDs

Mit Beginn des neuen Jahrtausends kamen in der Musikindustrie zunehmend DRM-Systeme zur Verhinderung der Auslesbarkeit von Musik-CDs über Computer zum Einsatz, um die illegale Vervielfältigung und Verbreitung von digitalen Tonaufnahmen zu verhindern.[149] Allerdings kam es seitens der Käufer solcher ko-

144 *Bechtold*, DRM, 2002, S. 46; *Ünlü*, Content Protection, 2005, S. 79.
145 *Ünlü*, Content Protection, 2005, S. 79.
146 Weiterführend vgl. *Bechtold*, DRM, 2002, S. 47 ff. (XrML), 50 ff. (ODRL).
147 *Ünlü*, Content Protection, 2005, S. 71.
148 *Bechtold*, DRM, 2002, S. 54 ff.
149 Vgl. bzgl. der Details der unterschiedlichen, konkret verwendeten Technologien den Üblick bei *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007, S. 35-37.

piergeschützter CDs bald zu massiven Beschwerden, da der Einsatz dieser Kopierschutztechnologien oftmals zu Problemen bei der Abspielbarkeit der Tonaufnahmen über ältere CD-Player führte.[150] Die bereits aus diesem Grund unter den Nutzern weit verbreitete Ablehnung[151] von Kopierschutztechnologien wurde weiterhin durch den Rootkit-Skandal[152] angeheizt. Daraufhin erklärten die Major Labels zwischen 2004 und 2007 sukzessive den Verzicht auf den Einsatz von Kopierschutztechnologien auf CDs.[153] Musik-CDs sind somit gegenwärtig wieder weitgehend frei von DRM-Systemen habbar.[154]

2. Onlineshops und Abonnementdienste

Weiterhin werden bzw. wurden DRM-Systeme im Rahmen von Internetdiensten, die digitale Tonaufnahmen als herunterladbare Dateien („Musikdownloads") über das Internet zum Kauf anbieten („Onlineshops") und zeitlich befristeten Abonnements zur Nutzung von Musik („Abonnementdienste") eingesetzt.

150 *CDT*, Evaluating DRM, 2006, S. 7; *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007, S. 36.

151 Man gebe nur die Stichworte „CD" und „kein Kopierschutz" bei Google ein, worauf man jede Menge Links zu Einträgen und Webseiten erhält, die deutliche Kritik an sowie Anleitungen und Tipps zur Umgehung von Kopierschutztechnologien zum Gegenstand haben.

152 Vgl. 5. Kapitel, Teil B.II.3.

153 Vgl. *Theurer*, Die Musikindustrie zweifelt am Kopierschutz, FAZ.NET, 04.06.2004, http://www.faz.net/s/RubE2C6E0BCC2F04DD787CDC274993E94C1/Doc~EC158B-DE6F1404D6D8A8BAD5AA28D1357~ATpl~Ecommon~Scontent.html (zuletzt abgerufen am 01.07.2010); *Heise Online*, Sony Music Japan verzichtet auf Kopierschutz, 03.10.2004, http://www.heise.de/newsticker/meldung/Sony-Music-Japan-verzichtet-auf-Kopierschutz-106635.html (zuletzt abgerufen am 01.07.2010); *gullinews*, EMI beendet die Ära kopiergeschützter CDs, 08.01.2007, http://www.gulli.com/news/emi-beendet-die-ra-kopiergesch-2007-01-08/ (zuletzt abgerufen am 01.07.2010). Allerdings war die Wirksamkeit des Einsatzes solcher Kopierschutztechnologien bereits vor diesem Schritt höchst fraglich geworden, da jede Kopierschutztechnologie innerhalb kürzester Zeit durch Hacker „geknackt" und die entsprechende Umgehungssoftware im Internet veröffentlicht worden war. Auch war der auf CDs enthaltene Kopierschutz anders als bei DVDs nicht zusätzlich mit einem entsprechenden Schutz auf den CD-Abspielgeräten kombiniert, was die Effektivität des Kopierschutzes weiter einschränkte. Vgl. hierzu *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007, S. 36.

154 Vgl. hierzu die Webseite des Bundesverbandes der Musikindustrie zum Thema Kopierschutz, http://www.musikindustrie.de/kopierschutz/ (zuletzt abgerufen am 01.07.2010); s.a. *Jobs,* Thoughts on Music, 06.02.2007, http://www.apple.com/hotnews/thoughtsonmusic/ (zuletzt abgerufen am 01.07.2010): *„In 2006, under 2 billion DRM-protected songs were sold worldwide by online stores, while over 20 billion songs were sold completely DRM-free and unprotected on CDs by the music companies themselves. The music companies sell the vast majority of their music DRM-free, and show no signs of changing this behavior, since the overwhelming majority of their revenues depend on selling CDs which must play in CD players that support no DRM system"*. Dementsprechend wird auch vermutet, dass der weit überwiegende Anteil, digitaler Tonaufnahmen, die auf iPods enthalten sind, von „gerippten" CDs stammt, vgl. *Krasilovsky/Shemel*, Music Business, 2007, S. 429.

Das Geschäftsmodell, auf dem Onlineshops basieren, überträgt das tradierte, im analogen Zeitalter dominierende Vertriebsmodell der Tonträgerunternehmen ins Internet.[155] Der hauptsächliche Unterschied zum Offline-Vertrieb besteht darin, dass die Tonaufnahmen in rein digitaler Form als Datei anstatt in Form eines physischen Datenträgers erworben werden und unmittelbar auf den Computer des Nutzers heruntergeladen werden können.[156] Der iTunes-Store war der erste Onlineshop, der seinen Nutzern einen sogenannten „à la carte" oder „pay-per-download"-Service anbot, d.h. die Möglichkeit, sich eine einzelne digitale Tonaufnahme oder ein „bundle", d.h. eine Kombination mehrerer Tonaufnahmen in Form eines Albums, im Internet auszusuchen und eine digitale Kopie dieser Tonaufnahme dauerhaft zu Eigentum zu erwerben. Durch den Einsatz von DRM-Systemen wurde bis vor kurzem[157] sichergestellt, dass ein Musikdownload nur bei Vorhandensein einer bestimmten Software auf dem Computer des Nutzers und/oder nur im Zusammenhang mit der Verwendung eines vom jeweiligen Anbieter vertriebenen digitalen Endgerätes genutzt werden konnte, worüber die Einhaltung der vom Rechtsinhaber vorgegebenen Beschränkungen der Nutzbarkeit der erworbenen Dateien kontrolliert werden sollte.[158] Auch wurden nutzerseitige Handlungen in Bezug auf den Musikdownload weitgehend eingeschränkt, insbesondere die Möglichkeit der Vervielfältigung, der Bearbeitung sowie der Übertragbarkeit auf andere Computer als denjenigen, auf den die Datei ursprünglich heruntergeladen wurde.[159] Bekanntestes Beispiel für ein solches im Rahmen eines Onlineshop genutztes DRM-System ist die im Rahmen des iTunes-Store eingesetzte „Fair Play"-Technologie des Unternehmens Apple.[160]

Im Gegensatz zu Onlineshops wird im Rahmen von Abonnementdiensten nicht der dauerhafte Erwerb einzelner Tonaufnahmen oder *bundles* angeboten, sondern erhält der Nutzer gegen Zahlung einer monatlichen Gebühr einen zeitlich begrenzten Zugang zu einer Musikbibliothek, deren Inhalte er bis zum Ablauf des Abonnements jederzeit nutzen kann.[161] Der Nutzer zahlt bei diesem Modell somit nicht dafür, Eigentümer einer erlaubten Kopie einer digitalen Tonaufnahme zu werden und diese auf unbegrenzte Dauer nutzen zu können, sondern für die vorübergehend gewährte Möglichkeit der Nutzung von digitalen Tonaufnahmen. Die vom Nutzer aus der Bibliothek abgerufene Tonaufnahme wird auf den Computer des Nutzers in Form eines Live-Streams (nachfolgend „Stream" oder „Streaming-Angebot")

155 *CDT*, Evaluating DRM, 2006, S. 8; *Bernstein/Sekine/Weissman*, Global Music Industry, 2007, S. 17.
156 *Montagnani*, 26 Cardozo Arts & Ent. L.J. 719, 756 (2009).
157 Vgl. 5. Kapitel, Teil A.
158 *Perritt*, 16 Mich. St. J. Int'l Law 113, 122 (2007); *CDT*, Evaluating DRM, 2006, S. 9.
159 *CDT*, Evaluating DRM, 2006, S. 8, 9.
160 *Perritt*, 16 Mich. St. J. Int'l Law 113, 123 (2007).
161 *Montagnani*, 26 Cardozo Arts & Ent. L.J. 719, S. 757 (2009); CDT, Evaluating DRM, 2006, S. 9.

übertragen. Unter einem Stream versteht man das Empfangen und die gleichzeitige Wiedergabe von Audio- und/oder Videodateien aus einem Rechnernetz,[162] wobei die dauerhafte lokale Speicherung der Datei auf dem empfangenden Computer nicht vorgesehen ist.[163] Im Rahmen von Abonnementdiensten wird mit Hilfe von DRM-Systemen vor allem die Zugriffsberechtigung des Nutzers verifiziert. Dafür wird ein verschlüsselter Token-Code durch den Computer des Nutzers bei dem Internetdienst abgerufen, der verweigert wird, sofern keine Berechtigung seitens des jeweiligen Nutzers besteht oder sobald eine bisher bestehende Berechtigung abgelaufen ist.[164]

3. Filmbereich

Bereits im Zeitalter von Videokassetten wurden auch seitens der Filmindustrie Kopierschutztechnologien zur Verhinderung der Herstellung von Raubkopien eingesetzt. Dieser Schutz gegen die illegale Anfertigung von analogen Kopien wurde auch auf die DVD übertragen, durch die die Videokassette seit dem Jahr 1996 sukzessive ersetzt wurde, und zu diesem Zweck die Kodierungssoftware „Content Scrambling System" („CSS-Technologie") entwickelt.[165] Über diese Technologie wird der gesamte auf einer DVD gespeicherte Inhalt verschlüsselt, so dass er grundsätzlich nur von einem DVD-Player ausgelesen werden kann, der durch die „DVD Copy Control Association" lizenziert wurde und daher über die zur Entschlüsselung erforderliche Software verfügt.[166] Durch diese Verschlüsselung soll insbesondere das Auslesen von DVDs über reguläre CD-Rom-Computerlaufwerke, sowie die anschließende Recodierung des digitalen Inhalts zum Zwecke der Abspeicherung und Verbreitung des Inhaltes über CD-Rom oder über das Internet verhindert werden.[167] Für die neuste Generation an Trägermedien für Film- und Videowerke, der sogenannten „Blu-ray"-Disc,[168] wird ebenfalls ein der CSS-Kodierungssoftware vergleichbares DRM-System namens „Advanced Access Content System" eingesetzt.[169]

162 Vgl. *Wikipedia*, Stichwort „Streaming Media", Version vom 25.4.2010, 16:48 h, http://de.*Wikipedia*.org/w/index.php?title=Streaming_Media&oldid=73585843 (zuletzt abgerufen am 27.04.2010).
163 *CDT*, Evaluating DRM, 2006, S. 9-10.
164 *Perritt*, 16 Mich. St. J. Int'l Law 113, 122 (2007); *CDT*, Evaluating DRM, 2006, S. 10.
165 *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007, S. 37.
166 *CDT*, Evaluating DRM, 2006, S. 5; *Ünlü*, DRM, 2005, S. 70.
167 *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007, S. 37.
168 Die Blue-ray Disk hat sich im Februar 2008 gegen den Konkurrenten HD DVD als im Bereich *optical discs* als Nachfolgemedium der DVD durchgesetzt.
169 Vgl. *Wikipedia*, Stichwort „Advanced Acess Content System", Version vom 22.04.2010, 22:31 h, http://en.*Wikipedia*.org/w/index.php?title=Advanced_Access_Content_System&oldid=357711069 (zuletzt abgerufen am 27.04.2010).

Trotz des zweistufigen Ansatzes der CSS-Technologie, wonach bereits die DVD-Rohlinge mit dieser Software kodiert werden und weiterhin das Auslesen der DVDs an die Nutzung eines mit CSS ausgestatteten digitalen Endgeräts geknüpft ist, wurde auch dieses DRM-System zwischenzeitlich von Hackern „geknackt".[170] Dennoch stellt die CSS-Technologie, die nach wie vor beim Vertrieb von DVDs eingesetzt wird, ein relativ erfolgreiches DRM-System dar,[171] insbesondere im Vergleich mit den zahlreichen erfolglosen Versuche der Musikindustrie, einen vergleichbaren Schutz für CDs zu etablieren. Der Hauptgrund hierfür dürfte darin liegen, dass DVDs anders als CDs von Anfang an mit diesem DRM-System versehen waren und daher alle Hersteller von DVD-Abspielgeräten diese CSS-kompatibel ausstatten mussten, wodurch von Anfang an ein geschlossenes, DRM-gestütztes Schutzniveau für auf DVD veröffentlichte Filme erreicht wurde.

C. Ökonomischer Hintergrund

Vor Anbruch der Digitalisierung wurden Multimediawerke, die dem Oberbegriff der „Informationsgüter" zuzuordnen sind,[172] in der Wirtschaftstheorie als Mischgüter („impure public goods")[173] oder gar als private Güter („private goods")[174] eingeordnet, da sie aus technischen Gründen, nämlich der für den Vertrieb notwendigen Verbindung mit einem physischen Datenträger, nicht die für ein reines öffentliches Gut typischen Merkmale der Nichtrivalität („non-rivalness") und Nichtausschließbarkeit („non-excludability") aufwiesen.[175] *Non-rivalness* bedeutet, dass ein Gut von einer unbegrenzten Anzahl an Personen genutzt werden kann, ohne dass die individuelle Nutzbarkeit des Guts davon beeinträchtigt wird. Das Gut ist somit ohne Anstieg der Grenzkosten von einer Vielzahl von Personen nutzbar und damit nicht knapp („scarce").[176] Demgegenüber bedeutet *non-excludability*, dass von den Vorteilen der Nutzung des Guts niemand ausgeschlossen werden kann.[177] Da im analogen Zeitalter Multimediawerke jedoch auf physischen Datenträgern vertrieben wurden, konnten sie sich zum einen bei vielfacher Beanspruchung abnutzen. Zum anderen waren Personen, die nicht im Besitz eines solchen Datenträgers waren, von der Nutzung des Multimediaprodukts weitgehend ausgeschlossen, auch weil die illegale, d.h. außerhalb des durch die Rechtsinhaber au-

170 *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007, S. 37.
171 *Biddle/England/Peinado/Willman*, The Darknet and the Future of Content Distribution, S. 1, 11, http://msl1.mit.edu/ESD10/docs/darknet5.pdf (zuletzt abgerufen am 01.07.2010).
172 *Ünlü*, Content Protection, 2005, S. 26.
173 *Ünlü*, Content Protection, 2005, S. 36-37.
174 *Bechtold*, DRM, 2002, S. 285.
175 *Ünlü*, Content Protection, 2005, S. 37.
176 *Bechtold*, DRM, 2002, S. 284; *Ünlü*, Content Protection, 2005, S. 36.
177 *Bechtold*, DRM, 2002, S. 284-285; *Ünlü*, Content Protection, 2005, S. 36.