Digital Rights Management – Optionen der Technikgestaltung

von Knud Böhle, ITAS

In diesem Beitrag wird nach Optionen der Gestaltung von DRM-Systemen gefragt und das Thema damit an die Technikfolgenabschätzung und sozialwissenschaftliche Technikforschung angeschlossen. Ausgegangen wird von einer Definition von DRM-Systemen und einer Charakterisierung der zugehörigen Technik. Im nächsten Schritt werden verschiedene Anwendungsfelder aufgezeigt, die mit ganz unterschiedlichen Bewertungen von DRM-Systemen verbunden sind. Es stellt sich dabei heraus, dass sich die politischen Kontroversen an einem spezifischen DRM-Ansatz festmachen lassen. Die Entstehung dieses Ansatzes wird kurz nachgezeichnet, um daran die Erörterung von alternativen Optionen der Technikgestaltung anzuschließen. Die hier vorgestellten durchaus vorläufigen Überlegungen basieren auf Arbeiten, die im Projekt INDICARE durchgeführt wurden (INDICARE 2006).

1 Zur Charakterisierung der DRM-Technik

Es gibt eine Vielzahl von DRM-Definitionen, aber keine allgemein akzeptierte (vgl. INDICARE 2004, S. 1 f.). In der Einleitung zu diesem Schwerpunkt haben wir bereits auf den Charakter von DRM als Kontrolltechnologie und auf die Definition von Armstrong (2006, S. 1) hingewiesen, der DRM-Technologien als solche charakterisiert „that prevent the [digital media] works from being accessed or used except upon conditions the producers themselves specify“. Daran anknüpfend lässt sich der Begriff „DRM-System“ wie folgt definieren:

Digital-Rights-Management-System ist ein Sammelbegriff für jede Kombination von Techniken, die den Zugriff auf und die Nutzung von digitalen Inhalten nach bestimmten Regeln kontrolliert.

Diese Definition ist in mehrerer Hinsicht bewusst unbestimmt. Es bleibt offen, ob die Regeln aus dem Urheberrecht abgeleitet werden, ob sie in Lizenzverträgen enthaltene Bestimmungen umsetzen oder ob es z. B. Regeln sind, die nur innerhalb von Organisationen gelten. Die Definition gilt zudem unabhängig von be-

stimmten Anwendungszwecken und Einsatzgebieten. „Kontrolle“ muss auch nicht in jedem Fall unmittelbare Durchsetzung der Regeln („enforcement“) implizieren – eine Engführung, die sich häufiger in Definitionen von DRM findet (vgl. z. B. Wikipedia 2006a; Bizer et al. 2005, S. 17). Der unschärfere Begriff „Kontrolle“ hat den Vorteil, dass damit eine definitorische Festlegung auf einen bestimmten DRM-Ansatz vermieden wird.

In Anlehnung an Rump (2003, S. 7-10) lassen sich idealtypisch sieben Funktionen von DRM-Systemen unterscheiden, die kombiniert und integriert werden müssen, damit ein voll ausgebautes DRM-System entsteht. Auch wenn in manchen Fällen nicht alle Komponenten zwingend erforderlich sind und in anderen Fällen zusätzliche Funktionen benötigt werden, so kann doch mittels dieser funktionalen Differenzierung verdeutlicht werden, dass wir es bei DRM-Systemen mit einer Kombination von Techniken zu tun haben.

Von einem konkreten digitalen Inhalt ausgehend, der anderen kontrolliert zugänglich gemacht werden soll, kommt es zunächst (1) auf Verfahren der eindeutigen Kennzeichnung und (2) Beschreibung der Inhalte an. Das ist vergleichbar etwa mit der ISBN für Bücher (International Standard Book Number) und den normierten bibliographischen Angaben, nur dass es für digitale Werke andere Standards gibt (zu diesen Standards gehört etwa der Digital Object Identifier, DOI) und die Beschreibung der Inhalte über Metadaten erfolgt, die dem Inhalt mitgegeben werden können. Davon zu unterscheiden sind (3) Kennzeichnungsverfahren, die sich nicht auf das Werk und den Inhalt, sondern abstrakt auf das digitale Objekt (das „Bitmuster“) beziehen und helfen, Kopien davon im digitalen Umfeld aufzuspüren (z. B. „watermarking“ und „fingerprinting“). Außerdem werden (4) in DRM-Systemen für jeden Inhalt die Regeln für den Zugang und die Nutzungsarten festgelegt. Dafür wurden spezielle Computersprachen, die i. d. R. auf XML aufbauen, entwickelt: die so genannten „rights expression languages“ (REL). Kombiniert wird diese Zurichtung des Objekts mit (5) Verfahren der Identifikation von Geräten, Personen oder Organisationen, um den Zugang und die Nutzung auf die Berechtigten einzuschränken. Unautorisierter Zugang und unautorisierte Nut-

zung wird (6) durch kryptographische Verfahren verhindert, die Inhalte in so genannte „secure containers“ wegschließen. Dazu kommen (7) Komponenten, die Daten über die Nutzung erzeugen und zusammenstellen, und die verwendet werden, um die Einhaltung der Lizenzbedingungen (z. B. 7 Kopien, Nutzungsdauer 1 Monat) zu kontrollieren und die als Basis für Abrechnungs-, Zahlungs- und Marketingsysteme dienen. Die eingesetzten technischen Komponenten sind nicht gänzlich neu, müssen für DRM-Systeme aber spezifisch weiterentwickelt und aufeinander abgestimmt werden.

Dieser Schnelldurchgang durch wesentliche technische Funktionen von DRM-Systemen (ausführliche technische Beiträge in Becker et al. 2003) macht bereits deutlich, dass der Einsatz dieser Systeme die ganze Wertschöpfungskette für digitale Güter verändert. Inhalte, die DRM-tauglich sein sollen, müssen nicht nur von Anfang an in bestimmter Weise behandelt werden, es müssen auch die Endgeräte – seien es DVD-Abspielgeräte, PCs oder Mobiltelefone – technisch vorbereitet sein. Des Weiteren wirken sich DRM-Systeme auf den gesamten Produktlebenszyklus aus, weil der technische Schutz dauerhaft an dem Inhalt haftet. Das kann z. B. den Weiterverkauf digitaler Güter oder die Langzeitarchivierung, die auf Umkopieren von einem Format auf ein anderes angewiesen ist, erheblich erschweren. Der Lebenszyklus des Produkts kann auch zu einem vorzeitigen Ende kommen, wenn der geschützte Inhalt nach „Updates“ und „Upgrades“ von Hard- oder Software auf einmal unzugänglich wird (vgl. zu einigen Beispielen Böhle 2004 oder INDICARE 2004, S. 19 ff.).

Zur Kennzeichnung und Problematisierung der DRM-Technologie sind noch drei Hinweise wichtig. *Zum einen* ist von Interesse, inwieweit die DRM-Technologie Infrastrukturcharakter erlangen kann. Eingeführt wurden DRM-Systeme in die Umgebung des Internet als Kontrolltechnologie, um der offenen Architektur des Netzes, offenen Formaten (wie MP3) und offenen Endgeräten (wie dem PC) punktuell etwas entgegenzusetzen, das den kommerziellen Interessen der Rechteinhaber entspricht. Die Frage ist, ob es langfristig eher bei einer Anzahl nicht-kompatibler Spezifikationen und Formate für Inhalte wie für Geräte bleiben wird oder ob Erfordernisse der Interoperabilität Standardisie-

rungsprozesse und einen Umschlag in Infrastrukturtechnologie begünstigen werden.¹

Der zweite Hinweis bezieht sich darauf, dass es keine hundertprozentig effektiven, d. h. sicheren Schutzmaßnahmen im IT-Bereich gibt.² Im Kontext der schnellen Verbreitung von Informationen im Internet bedeutet das zum einen, dass sowohl die ihres DRM-Schutzes beraubten Inhalte als auch das Umgehungsverfahren im Nu weltweit verfügbar gemacht werden können. Daraus folgt zum einen, dass DRM-Systeme eher die Funktion von „speed bumps“ erfüllen, also die Geschwindigkeit des „illegalen“ Gebrauchs legal geschützter Inhalte herabsetzen. Zum anderen haben Nutzer dadurch oft die Wahl zwischen dem Abruf legaler, DRM-geschützter Inhalte und dem gegebenenfalls illegalen Abruf derselben Inhalte. Aus Nutzersicht ist dabei aber nicht nur die prinzipielle Wahlmöglichkeit von Bedeutung; auch der jeweilige Aufwand für die eine oder andere Option und die möglichen (strafrechtlichen) Folgen sind relevant.

Der dritte Hinweis stammt von Bizer et al. (2005), die auf einen Geburtsfehler von DRM hinweisen. Sie heben hervor, dass DRM-Systeme gegen einen Grundsatz der IT-Sicherheit verstoßen: „Derjenige Partner, der einen Vorteil an einer Sache hat, muss auch über die technischen Mittel verfügen, sie durchzusetzen“ (S. 197). Anders gesagt, der Anwender des DRM-Systems muss in der Lage sein, seine „Rechte“ auf dem Endgerät des Nutzers auch durchzusetzen, was nicht trivial ist. Daraus folgt eine spezifische Verletzlichkeit solcher DRM-Systeme.

2 Anwendungskontexte

2.1 DRM-Systeme im Inhaus- und Geschäftsbereich

Die Bewertung von DRM-Systemen hängt sehr stark vom Anwendungszweck und Anwendungskontext ab. Dass Unternehmen den Zugang und die Zugriffsrechte ihrer Mitarbeiter auf elektronische Ressourcen innerhalb ihrer Organisationsgrenzen kontrollieren, ist selbstverständlich und reicht von den frühen „file-sharing“-Systemen zu den heutigen „content-management“-Systemen, die DRM-Technologien verwenden („enterprise DRM“). Für TA sind solche Entwicklungen nicht ganz uninter-

ressant, weil Ansätze und technische Entwicklungen, die für große Unternehmen oder Organisationen entwickelt werden, u. U. avancierter sind und möglicherweise schon vorzeichnen, was in anderen Anwendungsfeldern später zu erwarten ist.

Wenig kontrovers ist der Einsatz von DRM-Systemen im Geschäftsbereich. In diesem Zusammenhang steht an erster Stelle die rationale, computergestützte Verwaltung von „Rechten“ – übrigens nicht nur an digitalen Ressourcen. Ein schönes Beispiel dafür, dass DRM-Systeme die Rechteverwaltung und Rechteerlangung erleichtern kann, gibt Hoeren (2006, S. 212). Für eine CD-ROM, die der Musikverlag Schott zum hundertsten Geburtstag von Carl Orff herausbrachte, waren „mehr als 800 Urheber- und Leistungsschutzrechte“ einzuholen. In dem hier gewählten Beispiel erleichtern die DRM-Systeme den Verwertungsgesellschaften die Aufgabe, die Rechte von Urhebern treuhänderisch wahrzunehmen.

2.2 DRM-Systeme für innovative Dienste

Es zeichnen sich einige innovative Dienstleistungen ab, die durch DRM-Systeme erst ermöglicht werden. Beispiele sind das Ausleihen digitaler Inhalte aus Bibliotheken (Coyle 2005), das private Verleihen an Freunde (Einhorn und Rosenblatt 2005) oder das Weiterverkaufen auf Sekundärmärkten (Niehüser 2005). Ein weiteres interessantes Beispiel bildet „Google Book Search“, wobei wir uns hier auf das „publishers program“ beziehen. Google digitalisiert Verlagspublikationen, indiziert die Daten für seine Suchmaschine und bietet als Antwort auf Suchanfragen Auszüge aus dem betreffenden Buch an. Die Regeln dafür, was und wie viel angezeigt wird und wie das Angezeigte genutzt werden kann, sind zwischen den Verlagen und Google vertraglich festgelegt. Dem Anbieter Google werden als Lizenznehmer bestimmte Rechte eingeräumt, die entsprechend technisch implementiert werden und die Nutzung der Verlagshalte durch die Endnutzer reglementieren. Letztlich haben wir es mit einem DRM-System zu tun. Da in diesem Fall die Kontrolle nicht auf das Endgerät des Kunden ausgedehnt wird und es auch nicht um den Erwerb eines Inhalts geht, sondern um einen Dienst, der das Inspizieren von Büchern erlaubt (wie in der Freihandbiblio-

thek oder im Buchladen), wird diese Art des DRM-Systems nicht als restriktiv empfunden.³

Führt man sich noch einmal die Beispiele des DRM-gestützten Ausleihens, Verleihens (sharing), Weiterverkaufs und Inspizierens vor Augen, wird deutlich, dass hier Möglichkeiten gesucht werden, traditionelle Nutzungsformen von Inhalten in einer digitalen Umgebung kontrolliert zu reproduzieren (vgl. dazu auch Ruikka 2005).

2.3 DRM-Systeme in der Kritik

Massive Kritik an DRM-Systemen wird laut, wenn sie von den Bürgern bzw. Konsumenten als lästig, unfair, ungerechtfertigt, kontraproduktiv oder sogar als rechtsverletzend eingeschätzt oder empfunden werden. An dieser Stelle können wir uns kurz fassen, da ja schon unter der Perspektive der Nebenfolgen in der Einführung zu diesem Schwerpunkt auf einige Probleme hingewiesen wurde. Man kann zwei zentrale Konfliktherde bestimmen. Die den *Bürger* umtreibende Sorge bezieht sich auf das Verhältnis von DRM-Systemen zum Recht. Im Zentrum steht deren Bezug zum Urheberrecht, aber auch andere Bezüge – Schutz der Privatsphäre, Datenschutz, Eigentumsrechte, Vertragsrecht, Verbraucherrechte und Wettbewerbsrecht – sind einschlägig.

Die den *Konsumenten* umtreibende Frage ist die nach dem „value for money“ und einer fairen, vertrauensvollen Business-to-Consumer-(B2C)-Beziehung. Das Problem beginnt damit, dass der gesetzestreue Konsument, der DRM-geschützte Inhalte erwirbt, feststellen muss, dass (a) die Nutzung aufwändiger geworden ist, weil Softwaredownloads und Registrierungen dazu kommen, (b) die erwartete Interoperabilität nicht gegeben ist, wenn eine CD z. B. nicht mehr im Autoradio oder auf dem PC abspielbar ist, und dass (c) auch die Interoperabilität der DRM-Formate nicht gegeben ist und die geschützten Inhalte nur auf den Geräten bestimmter Hersteller genutzt werden können. Diese Nebenfolgen sind vor dem Hintergrund kostenfreier legal wie illegal zu beziehender Inhalte in weiterverwendbaren und weiterverarbeitbaren Formaten zu bewerten, die dem Konsumenten als Alternative zur Verfügung stehen. Das Diktum über die Psychoanalyse abwandeln könnte man sagen, dass solche Art von DRM die Krankheit ist, für

deren Therapie es sich hält. Dem entgegenzuhalten ist freilich, dass der Markt DRM-Systeme mit diesen Kinderkrankheiten kaum auf Dauer akzeptieren dürfte und man zu konsumenten- und nutzerfreundlicheren DRM-Systemen kommen wird.

2.4 DRM-Systeme „von unten“

Die heftige Kritik an DRM-Systemen rührt oft daher, dass es die großen Plattenfirmen, die Filmindustrie oder die großen Verlage sind, die diese Systeme in ihrem Verwertungsinteresse einsetzen. Diese Sichtweise verstellt häufig den Blick auf die Anwendung von DRM-Systemen „von unten“. Damit ist gemeint, dass es im wohlverstandenen Interesse der Künstler oder Autoren liegen kann, die Nutzung der von ihnen erstellten Inhalte in gewissem Rahmen zu kontrollieren. Man kann z. B. die „Creative Commons Lizenzen“ in diesem Zusammenhang als recht erfolgreichen Versuch verstehen, die Urheber in die Lage zu versetzen, die Rechte die sie behalten möchten, und die Nutzungen, die sie freigeben wollen, selbst zu definieren (Dreier 2004).⁴ Ob die Einhaltung der Lizenzbestimmungen durch DRM-Technologien kontrolliert werden sollte, ist bei den Befürwortern der Creative Commons umstritten. Es gibt aber einige Stimmen, die durchaus für eine gewisse technische Kontrolle plädieren, um z. B. in der Lage zu sein, Kopien aufzuspüren, die unter Umgehung der Lizenzbestimmungen gemacht wurden (Hatcher 2005). In der „Open Access Bewegung“ gibt es eine ähnliche Debatte (Friend 2004; Poynder 2005; Fitzgerald, Reid 2005).

3 Gestaltungsoptionen

Aus unserer Sicht sind hauptsächlich drei Gestaltungsoptionen zu diskutieren, die zunächst in knapper Form narrativ eingeführt werden.

Anfangs wird der Bedarf an DRM-Systemen von der Medienindustrie formuliert und entsprechend entstehen zunächst einseitig am Verwertungsinteresse orientierte DRM-Systeme. Im Zuge der deutlich werdenden Schwächen dieses Ansatzes kommt es einerseits zu unterschiedlichen Modifizierungen im Rahmen des ursprünglichen Ansatzes. Zum anderen führt die Kritik an den einseitig auf Verwertung ausge-

richteten Ansätzen, die der grundlegenden Idee des Urheberrechts vom Interessenausgleich zuwider laufen, zu alternativen, am Interessenausgleich orientierten DRM-Ansätzen, die meistens in akademischen Kreisen konzipiert und entwickelt werden und auf eine gewisse Resonanz bei Verbraucherverbänden und zivilgesellschaftlichen Interessengruppen stoßen.

Das Bild wäre allerdings unvollständig ohne eine dritte Option, die den Interessenausgleich über so genannte alternative Kompensationsmechanismen (Alternative Compensation Schemes <ACS>) erreichen möchte, in denen DRM-Systeme bestenfalls als Inhaus-DRM-Systeme (s. o.) eine Rolle spielen. Insbesondere Verwertungsgesellschaften, zivilgesellschaftliche Gruppen und einzelne Forscher engagieren sich für diesen Weg. Im Folgenden gehen wir etwas genauer auf die unterschiedlichen Optionen der Technikgestaltung ein.

3.1 Am Verwertungsinteresse orientierte DRM-Systeme

Der Ursprung der DRM-Technologie ist in den Anfängen der 1990er Jahre zu suchen, als der kommerzielle Vertrieb digitaler Güter über das Internet als Chance und gleichzeitig als Problem erkannt und der Ruf nach Kontrolltechniken laut wurde. Die Schule machende Antwort auf dieses Problem wird in der Regel Mark Stefik zugeschrieben, der zu dieser Zeit am berühmten Palo Alto Research Center von Xerox forschte und einige grundlegende Konzepte entwickelte. Stefik verwendete damals nicht den Terminus DRM, sondern sprach von „usage rights management“ (Stefik 1996, S. 221 zitiert nach Gehring 2006) und konkretisiert dieses Konzept mit Blick auf die zu leistenden technischen Entwicklungsarbeiten in zwei Punkten:

„(1) that the terms and conditions governing the authorized use of a digital work can be expressed in a computer-interpretable language; and (2) that computers and software can be designed to enforce those terms and conditions“ (Stefik 2000, S. 83).

Die Nutzung digitaler Medieninhalte wird also technisch eingeschränkt auf *autorisierte* Nutzungen, deren jeweiliger Umfang computergestützt festgelegt und auch durchgesetzt werden kann. Dieses Leitbild orientiert sich deutlich an den Verwertungsinteressen der Medienindust-

rie, womit jedoch noch nichts darüber ausgesagt ist, ob den Konsumenten eher ein weites oder enges Nutzungsspektrum angeboten wird.

Das Konzept ist inzwischen zehn Jahre alt und darf insbesondere deshalb als erfolgreich eingestuft werden, weil es Einzug in das Urheberrecht gehalten hat – auch wenn es dort unter dem Etikett „Technische Maßnahmen“ auftaucht.⁵

Es zeigte sich nämlich, dass der Ansatz nicht ohne weiteres das leisten kann, was er soll. Insbesondere die Umsetzung des zweiten von Stefik genannten Punkts (enforcement) gestaltete sich schwierig, weil die interessierte Partei letztlich nicht in der Lage ist, die gesetzten Einschränkungen auch tatsächlich durchzusetzen. Entsprechend wurde deshalb versucht, rechtlich und technisch nachzurüsten. Rechtlich ist das mit dem Umgehungsschutz im Urheberrecht bereits geschehen.

Technisch wird auf dem Gebiet der physischen Medien an der Sicherheit gearbeitet. Die DVD etwa, deren derzeitiger Kopierschutz, wie allgemein bekannt, leicht zu umgehen ist, soll abgelöst werden durch neue Datenträger (HD DVD und Blue Ray) und ein damit verbundenes leistungsfähigeres Schutzsystem (Advanced Access Content System <AACS>). Für den Bereich der Online-Medien werden Hoffnungen auf das „Trusted Computing“ (TC) als Kontrollverstärker gesetzt, auch wenn in der heutigen Praxis die Kopplung von DRM und TC noch nicht sehr weit fortgeschritten ist.⁶

Ein anderes Mittel, den Schutz zu erhöhen, besteht darin, eine „*second line of defense*“ aufzubauen. Damit ist gemeint, dass neben dem Schutz des Objekts auch Mechanismen implementiert werden, mit denen – wenn der Schutz gebrochen ist – nicht-autorisierte Nutzungen und deren Verursacher ausfindig gemacht werden können, um sie dann gegebenenfalls strafrechtlich zu belangen (vgl. Bizer et al. 2005, S. 188, 191). Dass diese Strategie tatsächlich verfolgt wird, wurde in der Studie „privacy4DRM“ nachgewiesen (vgl. Möller und Puchta 2006 in diesem Heft).

Ein anderes Verfahren, die Schwächen des Ansatzes zu umgehen, kann man im Ansatz der „Rights Locker Architectures“ erkennen, der wesentlich auf einer Trennung von Lizenz und Inhalt und der Vermeidung von Kopien in der Domäne des Nutzers beruht.⁷ Man kann sich den

Ansatz konkret etwa so vorstellen: Die digitalen Inhalte sind in einer Datenbank auf einem Server des Anbieters gespeichert. Der Kunde erwirbt lediglich eine Lizenz für einen bestimmten Inhalt und kann auf ihn zugreifen und ihn nutzen, entsprechend der Lizenz. Die Rechte des Nutzers werden auf einem Autorisierungs-Server verwaltet. Der Konsument installiert auf seinen Endgeräten nur ein kleines Programm („applet“), mit dem er Nutzungsanfragen an den Autorisierungs-Server schickt. Entspricht die Nutzungsanfrage der Lizenz, wird der Inhalt aus der Datenbank freigegeben und per „streaming“ dem Kunden zur Verfügung gestellt. Entscheidend ist, dass der Inhalt niemals auf dem Endgerät des Kunden gespeichert wird, der Rechteverwerter nicht-autorisierte Nutzungen ausschließen kann und er zudem über die Daten auf dem Autorisierungs-Server genauestens über das Nutzungsverhalten (wann, wie oft, wo) seiner Kunden informiert sein kann. Dem Kunden mit gültiger Lizenz bietet dieser Ansatz z. B. den Vorteil, dass er auf die Inhalte von überall und von verschiedenen Geräten aus zugreifen kann. Außerdem braucht er sich nicht um Sicherungskopien zu kümmern, das Risiko, mit dem Inhalt einen Virus einzuschleppen, ist gering und es muss kein Speicherplatz auf dem lokalen Gerät vorgehalten werden. Dieser DRM-Ansatz, der mit zunehmender Bandbreite attraktiver und relevanter wird, ist als ambivalent zu bewerten (Melzer 2004).

3.2 Am Interessenausgleich orientierte DRM-Systeme

Pauschal gesagt richtet sich die Kritik an den verwertungsorientierten Ansätzen dagegen, dass den im Urheberrecht vorgesehenen Ausnahmen („fair use“, „fair dealing“, „Schrankenbestimmungen“) nicht entsprochen wird und dass darüber hinaus kein Spielraum für legale nicht-autorisierte Nutzungen bleibt. Die Ansätze stehen demnach im Gegensatz zu dem im Urheberrecht vorgesehenen Interessenausgleich zwischen Urhebern und Rechteinhabern einerseits und Nutzern und der Allgemeinheit andererseits. Die Antwort darauf sind am Interessenausgleich orientierte DRM-Systeme.⁸ Stefan Bechtold hat einen ersten Versuch gemacht, die Gestaltungsoffenheit von DRM-Systemen mit Blick auf verschiedene konkrete Forschungsarbeiten zu

belegen und das entstehende Forschungsfeld unter dem Aspekt der wertorientierten Gestaltung zu systematisieren (Bechtold 2006 in diesem Heft). Dabei konnte er an die US-amerikanische Diskussion um „fair use by design“ anknüpfen⁹, die in jüngster Zeit auch von Armstrong (2006) aufgearbeitet wurde. Die wesentliche Herausforderung liegt darin, DRM-Systeme so zu gestalten, dass sie als Hilfsmittel zur Durchsetzung von Verwertungsinteressen dienen und gleichzeitig zur Durchsetzung der Ausnahmeregelungen im Urheberrecht. Das macht die Sache in jedem Fall komplexer. Wir unterscheiden innerhalb dieser Kategorie Ansätze, die a) stärker die Interessen der Nutzer in der B2C-Beziehung berücksichtigen, die b) stärker die Ausnahmen im Urheberrecht durch Einrichtung zusätzlicher Infrastrukturkomponenten berücksichtigen, und c) Ansätze, die darauf aufbauend selbst noch unautorisierte Nutzungen vorsehen. Diese drei genannten Linien werden in den folgenden Passagen genauer betrachtet.¹⁰

a) *Ansätze, die stärker die Interessen der Nutzer berücksichtigen*

Eine „rights expression language“ (REL), darauf wurde schon mehrfach hingewiesen, ist ein Kernelement der meisten DRM-Systeme. Typischerweise werden die zu ermöglichenden Nutzungen einseitig von den Informationsanbietern vorgegeben, entsprechend implementiert und sind danach nicht mehr veränderbar. Dem Nutzer bleibt nur ein „take it or leave it“. Die Gefahr besteht, dass bei diesem Ansatz berechnete Ansprüche der Nutzer nicht mehr geltend gemacht werden können (vgl. Bechtold in diesem Heft). Der konsequente Gegenvorschlag geht dahin, an bi-direktionalen RELs zu arbeiten. Einschlägig sind hier die Arbeiten von Mulligan und Burstein (2004), die ausgehend von einer existierenden REL (XrML) zu zeigen versucht haben, wie auch zusätzlich Nutzerrechte eingebaut werden könnten.¹¹ Die Erweiterung der vorgesehenen Rechte allein reicht nicht aus, sondern es müssen noch Kommunikationsprotokolle und Schnittstellen dazukommen, die die Einweg-REL zur bi-direktionalen REL erweitern. Erst dann können die Rechteinhaber mit den Nutzern darüber verhandeln, welche Rechte zu welchen Bedingungen gewährt werden sollen. Rump und Barlas (2004) sehen in diesem Gewinn an In-

teraktivität und Aushandlungschancen eine Annäherung an die Verhältnisse der „physical world“ und die Möglichkeit, dass aus dem Konsumenten als „couch potato“ ein aktiver Teilnehmer in der Wertschöpfungskette wird. Korba und Kenny (2002) haben vorgeschlagen, den Ansatz der bi-direktionalen REL mit der Idee eines „Privacy Rights Management“ (PRM) zu verbinden, das den Konsumenten gestattet, die Weitergabe persönlicher und nutzungsbezogener Daten als Gut („asset“) zu behandeln, das sie mit in die Verhandlungen über die Nutzungsrechte einbringen könnten.

b) *Ansätze, die stärker die Ausnahmen im Urheberrecht berücksichtigen*

Ein zweiter Gestaltungsansatz führt „Trusted Third Parties“ ein, die Genehmigungen bzw. Autorisierungen erteilen und die technischen Mittel bereitstellen, geschützte Inhalte auf Grund von „fair use“ u. ä. Ansprüchen zu nutzen. Mit diesem Ansatz verbindet sich auch die Erwartung, dass die Privatsphäre besser geschützt werden kann, weil die Konsumenten die Genehmigung nicht direkt beim Inhalteanbieter, sondern bei einer Dritten Partei einholen. Da hier die B2C-Beziehung, anders als bei den bi-direktionalen RELs, verlassen wird und weitere Instanzen hinzukommen, wird in dem Zusammenhang auch von „fair use licensing infrastructures“ gesprochen. Sie sind komplementär zu den verwertungsorientierten DRM-Systemen zu sehen. Erst im Zusammenspiel beider Komponenten konstituiert sich hier das DRM-System. Wie von Bechtold (in diesem Heft) mit Bezug auf die Europäische Urheberrechtsrichtlinie bemerkt, ist eine Lösung dieser Art durchaus vom europäischen Gesetzgeber angedacht, wenn die Inhalteanbieter nicht von sich aus entsprechende Nutzungen ermöglichen. Systeme dieser Art wurden verschiedentlich schon konzipiert (für einen frühen Vorschlag vgl. Burk und Cohen 2001; neuerdings Knopf 2005), und auch schon für die „fair-use“-Ansprüche bestimmter Gruppen konkretisiert – etwa für Blinde und Sehbehinderte (Mann 2005) oder für den Bibliotheksbereich (Tyrväinen 2005a und 2005b).

c) *Ansätze, die selbst noch unautorisierte Nutzungen berücksichtigen*

Einen Schritt weiter geht Armstrong (2006, S. 46-54), der betont, dass das „fair-use“-Prinzip nicht ausschließlich an eine ex-ante-Autorisierung gebunden werden darf, wenn es wie im Offline-Bereich gelten soll. Dazu entwickelt er einen eigenen Vorschlag, in dem bereits vorausgesetzt ist, dass manche „fair-use“-Nutzungen a priori in die REL mit eingehen und andere über spezielle Genehmigungsverfahren gewährt werden. Sein darüber hinausgehender Vorschlag ist von einer niederländischen Forschergruppe inspiriert, die eine auf „Prolog“ basierende Computersprache „LicenseScript“ entwickelte, mit der es den Nutzern möglich ist, nach dem Kauf DRM-geschützter Inhalte noch Ansprüche auf bestimmte Nutzungen einzubringen. Diese Idee greift Armstrong auf und erweitert sie mit Blick auf die „fair-use“-Nutzungen. Damit es nicht zu beliebigen Urheberrechtsverletzungen kommt, werden gleichzeitig persönliche Daten und Nutzungsdaten erzeugt und gesammelt, die aber erst im Streitfall bei Verdacht auf Copyright-Verletzungen von einer Dritten Partei (identity escrow) aufgedeckt bzw. zur Verfügung gestellt werden.

3.3 Am Interessenausgleich orientierte alternative Kompensationsmechanismen

Die Grundidee alternativer Kompensationsmechanismen (Alternative Compensation Schemes – ACS) kam in Deutschland 1965 zum Zuge. Um die Privatsphäre zu schützen (und mangels praktikabler Alternativen) wurde in Zeiten der Kassettenrecorder das Recht auf Privatkopie als Ausnahme im Urhebergesetz eingeführt. Dieser Ansatz ist mit einer pauschalen Abgabe auf Aufnahmegeräte und später auch Leermedien verbunden, die von den Verwertungsgesellschaften eingezogen und nach bestimmten Schlüsseln an die Urheber ausgezahlt wird, um so eine Kompensation für den Ausfall direkter Einnahmen bei Kopieraktionen zu gewähren. Dieses Modell wird derzeit auch für das „file-sharing“ (den freien Austausch von Dateien) vorgeschlagen. Filesharing soll generell erlaubt werden, wenn im Gegenzug eine „flatrate“, also

eine Pauschalabgabe erhoben wird, die z. B. von Internet Service Providern oder deren Kunden zu entrichten wäre, und orientiert an den Downloadzahlen für ein Werk an die Urheber ausgeschüttet werden könnte. Wie diese Modelle konkret in einem globalen Kontext funktionieren könnten, wird seit Jahren diskutiert (siehe dazu Fisher 2004, Bernault, Lebois 2006; Grassmuck 2006; weitere ausführliche Hinweise auch unter <http://crosscommons.org/acs.html>). Wichtig ist an dieser Stelle nur der Hinweis, dass es sich hier um eine eigenständige Option der Technikgestaltung handelt, die nicht von der Diskussion um die Gestaltung von DRM-Systemen getrennt werden sollte. DRM-Systeme tauchen in diesem Ansatz, wenn überhaupt, nur im Sinne der Inhaus-DRM-Systeme auf.

4 Fazit

Der Beitrag sollte die Gestaltungsoffenheit von DRM-Systemen aufzeigen. Dazu bedurfte es einer Definition, die nicht von vornherein den Begriff auf einen bestimmten DRM-Ansatz einschränkt. Die Untersuchung verschiedener Anwendungsfelder führte zum einen zu einer Unterscheidung des Einsatzes im Inhaus- und Geschäftsbereich einerseits und in der Business-to-Consumer-Beziehung andererseits, aber darüber hinaus auch zu einer Unterscheidung von „top-down“ und „bottom-up“-Einsatz, wobei besonders auf die Frage hingewiesen wurde, welche Chancen für Autoren und Künstlern in dieser Aneignung der Technik liegen könnten. Schließlich sollte im dritten Abschnitt der Nachweis geführt werden, dass es tatsächlich alternative Optionen der Technikgestaltung gibt, die unterschiedlichen Orientierung – am „Verwertungsinteresse“, am „Interessenausgleich“ und am „Interessenausgleich bei Verzicht auf DRM-Systeme“ – folgen.

Eine TA, die tatsächlich an Optionen der Technikgestaltung und ihrer Bewertung interessiert ist, könnte sich zur Aufgabe machen, die Ansätze, die hier eher cursorisch und provisorisch eingeführt wurden, einem Assessment zu unterziehen. Dabei wären genauer zu untersuchen die technische Machbarkeit, die Risiken und Nebenwirkungen, die Relevanz der Ansätze für bestimmte technische Kanäle (z. B. Mobilfunk, Digitalfernsehen, Internet) sowie ihre Eignung für bestimmte Anwendungsbereiche

(z. B. Unterhaltung, Wissenschaft, Unterricht). Außerdem wären das Wechselspiel von Technik und Recht und natürlich auch die Interessen, Machtverhältnisse und Anreizstrukturen hinter den Ansätzen zu analysieren.

Für die sozialwissenschaftliche Technikforschung halten wir die abschließend zu nennenden fünf Fragestellungen für besonders relevant:

1. Stehen hinter den hier vorgestellten Ansätzen Leitbilder der Technikentwicklung? Dabei wäre zu klären, was die *Leitbildforschung* (bzw. „vision assessment“) zur Erhellung der DRM-Entwicklung beitragen kann.
2. Welche kommenden Techniken begünstigen die Durchsetzung bestimmter Ansätze (Leitbilder)? Sind neuartige Verfahren in Sicht, die zu weiteren Gestaltungsoptionen für DRM-Systeme führen? Zur Klärung könnten prospektive Methoden (*Foresight*) beitragen.
3. Es wäre nach dem Komplex Technikentwicklung, Patente, Standards zu fragen, der bezogen auf DRM-Systeme relativ schlecht aufbereitet ist. Das gilt insbesondere für das Verhältnis von Standards, die von Industriekonsortien vorangebracht werden (vgl. Anm. 1), zu Projekten und Initiativen, die sich als „grassroot“-Ansätze (z. B. DMP), Open Source (ODRL, DReaMs) verstehen oder sich europäischer Forschungsförderung verdanken (wie z. B. Axmedis).
4. Es wäre nach dem potenziellen Umschlag von DRM-Systemen als Einzeltechnik in Infrastruktur zu fragen – ein Umschlag, der wegen der Interoperabilitätsanforderungen der Märkte, Entwicklungen des Trusted Computing oder auch vermittelt über die so genannten „fair-use“-Infrastrukturen nicht ganz ausgeschlossen werden kann. Diese Perspektive wäre im größeren Kontext der technischen Veränderungen des Internet zu verfolgen.
5. Schließlich wäre die Frage nach den Chancen und Risiken der Rechtsdurchsetzung durch Technik im Fall der DRM-Systeme weiter zu untersuchen (ausgehend etwa von Lessig 2001 und Günnewig 2004).

Anmerkungen

- 1) Aktuell lassen sich zum einen Geschäftsmodelle beobachten, die gerade auf Inkompatibilität beruhen, wie Felten leicht sarkastisch bemerkt hat („Incompatibility isn't an unfortunate side-

effect of deficient DRM systems – it's the goal of DRM" – Felten 2004). Zum anderen sehen wir große branchenweit angelegte Standardisierungsvorhaben wie OMA (Open Mobile Alliance) im Mobilbereich, DVB (Digital Video Broadcasting) im TV- und Videobereich oder das Coral Consortium (<http://www.coral-interop.org/>) im Internetbereich. Für Einzelheiten siehe die diversen Artikel im INDICARE Monitor (<http://www.indicare.org/monitor>).

- 2) Ein oft erwähntes Fallbeispiel sind die vom Industriekonsortium SDMI (Secure Digital Music Initiative) entwickelten Schutzmaßnahmen, die binnen drei Wochen „geknackt“ wurden (Röttgers 2000; Wikipedia 2006b, vgl. dazu und zu anderen Beispielen der erfolgreichen Umgehung von DRM-Systemen auch Armstrong 2006, S. 12 f., Fußnote 46). Aus dem Fall kann jedoch nicht geschlossen werden, dass es nicht auch relativ sichere Vertriebskanäle für geschützte digitale Inhalte gibt und dass sich das Sicherheitsniveau nicht erhöhen ließe.
- 3) Zur Einschätzung von Google Book Search vgl. Rosenblatt 2005 und Redmer 2005. Anzumerken ist, dass das „Google Book Search libraries program“ durchaus kontrovers diskutiert und von Verlagen als gegen das Urheberrecht verstoßend attackiert wird (vgl. aktuell EDRI-gram 2006).
- 4) Im Juni 2006 waren immerhin schon 140 Millionen Webseiten CC-lizenziert; <http://creativecommons.org/weblog/entry/5936>.
- 5) So heißt es im geltenden deutschen Urheberrecht im § 95a Abs. 2: „Technische Maßnahmen im Sinne dieses Gesetzes sind Technologien, Vorrichtungen und Bestandteile, die im normalen Betrieb dazu bestimmt sind, geschützte Werke oder andere nach diesem Gesetz geschützte Schutzgegenstände betreffende Handlungen, die vom Rechtsinhaber nicht genehmigt sind, zu verhindern oder einzuschränken.“ (Bundesministerium der Justiz 2003) – Vgl. auch den Artikel 11 des WIPO Copyright Treaty (WIPO 1995).
- 6) Trusted Computing definiert Gehring (2006) „[a]s a tool for making the behaviour of computer systems more predictable, by enforcing rules on users and processes (i.e., mandatory access control), trusted computing creates ample opportunity for ruling out undesirable effects of software – and software users. At the same time it empowers parties controlling access to the rule-making process to forcing users to comply with their private interests, and to cut out competitors, when attempting to access, and use, system resources“. Zu Trusted Computing im Zusammenhang mit DRM vgl. ausführlich Kuhlmann und Gehring 2003 und den Schwerpunkt

- zu diesem Thema im INDICARE Monitor vom Februar 2006 <http://www.indicare.org/monitor>; zu den rechtlichen Problem des TC siehe Bechtold 2005.
- 7) Vgl. dazu Melzer 2004, Bechtold 2003, S. 600-602, und Bechtold in diesem Heft.
 - 8) Die Idee, anbieterorientierte von nutzerorientierten DRM-Systemen zu unterscheiden, haben wir verworfen, da sowohl der verwertungsorientierte Ansatz auch nutzerorientiert, wie der am Interessenausgleich orientierte Ansatz auch anbieterorientiert sein muss.
 - 9) Vgl. das Sonderheft der Communications of the ACM April 2003 und den Workshop „Fair Use by Design?“ im Rahmen der 12th Conference on Computer, Freedom & Privacy; 16.-19 April 2002 San Francisco; <http://www.cfp2002.org/fairuse/>
 - 10) Wir betrachten „forensisches DRM“ in diesem Artikel nicht als eigenständige Option der Technikgestaltung, geben aber zu, dass unsere Überlegungen dazu noch nicht abgeschlossen sind. Es geht bei „forensischem DRM“ um technische Kontrollmaßnahmen (z. B. „Wasserzeichen“, „Fingerabdrücke“ und „elektronische Signaturen“) mit denen herausgefunden werden soll (u. U. strafrechtlich verwertbar), ob es sich bei einer aufgespürten Kopie um eine berechnete handelt und wer diese in Umlauf gebracht hat. Da „forensisches DRM“ sowohl im Dienst verwertungsorientierter wie am Interessenausgleich orientierter Ansätze stehen kann, ist es nur schwer mit einer eindeutigen Orientierung zu verbinden. Am ehesten noch könnte „forensisches DRM“ als eigenständige Variante den um Interessenausgleich bemühten Optionen zugeordnet werden. Seine leitende Orientierung in diesem Kontext wäre dann möglicherweise über die Maxime „ungehinderte private Nutzung bei Verhinderung massiver Urheberrechtsverletzungen“ zu definieren.
 - 11) Diese Nutzungsrechte müssen sich nicht nur aus dem geltenden Urheberrecht ergeben, sondern können auch darüber hinausgehen, was gerade mit Blick auf neue Nutzungsweisen digitaler Inhalt zunehmend relevant wird. Bechtold kann sich in dem Sinn Regeln für ein fein austariertes Erstellen von Derivaten vorstellen (2003, S. 604).

Literatur

Armstrong, T.K., 2006: Digital Rights Management and the Process of Fair Use. Online verfügbar bei SSRN unter der Adresse <http://ssrn.com/abstract=885371> (demnächst in Harvard Journal of Law & Technology, Vol. 20, No. 1, Herbst 2006)

Bechtold, St., 2003: The Present and Future of Digital Rights Management – Musings on Emerging Legal Problems. In: Becker, E. et al. (eds.): Digital Rights Management – Technological, Economic, Legal and Political Aspects. Berlin: Springer, S. 597-654, online verfügbar unter http://www.jura.uni-tuebingen.de/bechtold/pub/2003/Future_DRM.pdf

Bechtold, St., 2005: Trusted Computing – Rechtliche Probleme einer entstehenden Technologie. In: Computer und Recht (CR), S. 393-404 (leicht überarbeitete Fassung online verfügbar unter http://www.coll.mpg.de/pdf_dat/2005_20online.pdf)

Bechtold, St., 2006: Rechtliche Technikgestaltung von Digital-Rights-Management-Systemen – ein Blick auf ein entstehendes Forschungsgebiet. In: Technikfolgenabschätzung – Theorie und Praxis 15/2 (2006), S. 47-51

Becker, E.; Buhse, W.; Günnewig, D. et al. (Hg.), 2003: Digital Rights Management. Technological, Economic, Legal and Political Aspects. Lecture Notes Computer Science 2770. Berlin: Springer

Bernault, C.; Lebois, A., 2006: Peer-to-peer File Sharing and Literary and Artistic Property – A Feasibility Study regarding a system of compensation for the exchange of works. Englische Version 03.2006; online abrufbar unter http://privatkopie.net/files/Feasibility-Study-p2p-acs_Nantes.pdf

Bizer, J.; Grimm, R.; Möller, J. et al., 2005: privacy4DRM – Datenschutzverträgliches und nutzungsfreundliches Digital Rights Management. Kiel, Ilmenau; online verfügbar unter <http://www.datenschutzzentrum.de/drm/privacy4drm.pdf>

Böhle, K., 2004: Of vanishing media and copyright enforcement by destruction. In: INDICARE Monitor Vol. 1, No 2, July 2004; online verfügbar über http://www.indicare.org/tiki-read_article.php?articleId=29

BmJ – Bundesministerium der Justiz, 2003: Gesetz über Urheberrecht und verwandte Schutzrechte (zuletzt geändert 10.9.2003); online verfügbar über Juris: <http://bundesrecht.juris.de/urhg/BJNR012730965.html>

Burk, D.L.; Cohen, J.E., 2001: Fair Use Infrastructure for Rights Management Systems. In: Harvard Journal of Law & Technology 15 (2001), S. 41-83

Coyle, K., 2005: The role of digital rights management in library lending. In: INDICARE Monitor, Vol. 2, No 2, April 2005; online verfügbar über http://www.indicare.org/tiki-read_article.php?articleId=95

Dreier, Th., 2004: „Some rights reserved“. Creative Commons in between unlimited copyright and copyright anarchy. INDICARE-Interview by Bettina Krings. INDICARE Monitor, Vol. 1, No 4, Septem-

ber 2004; online verfügbar unter http://www.indicare.org/tiki-read_article.php?articleId=40

Dreier, Th., 2006: Steuerung durch Recht. Einige Überlegungen zum rechtlichen Schutz technischer Schutzmaßnahmen im Urheberrecht. In: Technikfolgenabschätzung – Theorie und Praxis 15/2 (2006), S. 13-19

EDRI-gram, 2006: Google's victory in court against German publisher. In: EDRI-gram newsletter – Number 4.13, 5 July 2006; online verfügbar unter <http://www.edri.org/edriagram/number4.13/googlegermany?PHPSESSID=d03811ca1fcb56989aad4e40e14f2610>

Einhorn, M.A.; Rosenblatt, B., 2005: Peer-to-Peer Networking and Digital Rights Management. How Market Tools Can Solve Copyright Problems. Policy Analysis 534. Cato Institute; online verfügbar über <http://www.cato.org/pubs/pas/pa534.pdf>

EUCD, 2001: Directive 2001/29/EC of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society; online verfügbar über http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32001L0029&model=guichett

Felten, E., 2004: A Perfectly Compatible Form of Incompatibility. Freedom to Tinker (Blog) April 15, 2004; online verfügbar über <http://www.freedom-to-tinker.com/index.php?p=578>

Fisher, W.W., 2004: Promises to Keep: Technology, Law, and the Future of Entertainment. Stanford: Stanford University Press; Kapitel 6 zu den Alternative Compensation Schemes ist online verfügbar unter <http://cyber.law.harvard.edu/people/ffisher/PTKChapter6.pdf>

Fitzgerald, B.; Reid, J., 2005: Digital rights management (DRM): managing digital rights for open access. In: Rooney, D.; Hearn, G.; Ninan, A. (Hg.): Handbook on the Knowledge Economy. Cheltenham: Edward Elgar 2005, S. 268-277

Friend, F.J., 2004: Who protects the un-protected? Open access publication needs DRM! INDICARE Monitor, Vol. 1, No. 5, October 2004; online verfügbar unter http://www.indicare.org/tiki-read_article.php?articleId=49

Gehring, R.A., 2006: Trusted computing for digital rights management. INDICARE Monitor, Vol. 2, No. 12, February 2006; online verfügbar unter http://www.indicare.org/tiki-read_article.php?articleId=179

Grassmuck, V., 2006: Of Price Discrimination, Rootkits and Flatrates. Entwurf vom 19. Februar 2006; online verfügbar über <http://edoc.hu-berlin.de/oa/bookchapters/reV3bcUwu4c/PDF/27MmjHeGKpCbE.pdf>

Günnewig, D., 2004: Architecture is Policy? Politische Steuerung durch Technik in digitalen Informations- und Kommunikationsnetzwerken am Beispiel des Einsatzes von Digital-Rights-Management-Systemen. In: Österreichische Zeitschrift für Politikwissenschaft (ÖZP), 33/4 (2004), S. 423-436

Hatcher, J.S., 2005: Can TPMs help create a commons? Looking at whether and how TPMs and Creative Commons licenses can work together. In: INDICARE Monitor, Vol. 2, No. 8, October 2005; online verfügbar über http://www.indicare.org/tiki-read_article.php?articleId=146

Hoeren, Th., 2006: Urheberrecht und Musik in der digitalen Revolution. In: Jacobshagen, A.; Reininghaus, F. (Hg.): Musik und Kulturbetrieb – Medien, Märkte, Institutionen. Laaber: Laaber Verlag, S. 195-217; online verfügbar unter: <http://www.uni-muenster.de/Jura.itm/hoeren/INHALTE/publikationen/UrhRMusik.pdf>

INDICARE, 2004: Digital Rights Management and Consumer Acceptability. A Multi-Disciplinary Discussion of Consumer Concerns and Expectations. State-of-the-Art Report; verfasst von Helberger, N. (ed.), Dufft, N.; van Gompel, S.; Kerényi, K.; Krings, B.-J.; Lambers, R.; Orwat, C.; Riehm, U.; Dezember 2004; online verfügbar unter: http://www.indicare.org/tiki-download_file.php?fileId=60

INDICARE, 2006: Digital Rights Management Systems – A Whiff of Technology Assessment. Second Policy Paper; verfasst von Böhle, K.; Karlsruhe 2006 (unv. Manuskript)

Knopf, D., 2005: How to implement copyright exceptions in DRM systems. In: INDICARE Monitor, Vol. 2, No. 1, March 2005; online verfügbar unter http://www.indicare.org/tiki-read_article.php?articleId=87

Korba, L.; Kenny, S., 2002: Towards Meeting the Privacy Challenge: Adapting DRM. NRC paper number NRC 44956, November 2002; online verfügbar unter <http://iit-iti.nrc-cnrc.gc.ca/iit-publications-iti/docs/NRC-44956.pdf>

Kuhlmann, D.; Gehring, R.A., 2003: trusted Platforms, DRM and beyond. In: Becker, E.; Buhse, W.; Günnewig, D. et al. (Hg.): Digital Rights Management. Technological, Economic, Legal and Political Aspects. Lecture Notes Computer Science 2770, Berlin: Springer, S. 178-205

Lessig, L., 2001: Code und andere Gesetze des Cyberspace. Berlin: Berlin Verlag

Mann, D., 2005: Digital rights management and people with sight loss. In: INDICARE Monitor, Vol. 2, No. 11, January 2006; online verfügbar unter http://www.indicare.org/tiki-read_article.php?articleId=170

Melzer, R., 2004: Rights locker architecture – the next step? Potential and risks of a new approach to digital content delivery. In: INDICARE Monitor, Vol. 1, No. 4, September 2004; http://www.indicare.org/tiki-read_article.php?articleId=44

Mitchell, J.T., 2004: DRM: The Good, the Bad, and the Ugly; online available at http://interactionlaw.com/documentos/DRM_good_bad_ugly.pdf

Möller, J.; Puchta, St., 2006: Privacy4DRM: Nutzer- und datenschutzfreundliches Digital Rights Management. In: Technikfolgenabschätzung – Theorie und Praxis 15/2 (2006), S. 26-32

Mulligan, D.K.; Burstein, A., 2004: Implementing Copyright Limitations in Rights Expression Languages. In: Feigenbaum, J. (Hg.): Security and privacy in Digital Rights Management (LNCS2696). New York: Springer, S. 137-154

Niehüser, L., 2005: Sekundärmärkte für digitale Medien auf Basis des Digital Rights Management. Rechtliche und technologische Voraussetzungen sowie ökonomische Implikationen. Aachen: Shaker

Redmer, J., 2005: Google Book Search: fostering public access in a controlled way. Interview von Knud Böhle mit Jens Redmer. In: INDICARE Monitor, Vol. 2, No. 9, November 2004; http://www.indicare.org/tiki-read_article.php?articleId=153

Poynder, R., 2005: The role of digital rights management in Open Access. In: INDICARE Monitor Vol. 2, No. 2, April 2005; online verfügbar über http://www.indicare.org/tiki-print_article.php?articleId=93

Röttgers, J., 2000: Good bye SDMI! Telepolis (13.10.2000); online verfügbar unter <http://www.heise.de/tp/r4/artikel/3/3578/1.html>

Rosenblatt, B., 2005: Rights Management and the revolution in e-publishing. In: INDICARE Monitor Vol. 2, No. 9, November 2005; online verfügbar unter: http://www.indicare.org/tiki-read_article.php?articleId=152

Rosenblatt, B., 2006: A Short Policy Analysis of Copyright Law and DRM in the United States. In: Technikfolgenabschätzung – Theorie und Praxis 15/2 (2006), S. 19-26

Ruikka, T., 2005: Contractual balance in digital content services. In: INDICARE Monitor, Vol. 2, No. 4, June 2005; http://www.indicare.org/tiki-read_article.php?articleId=113

Rump, N., 2003: Definition, Aspects, and Overview. In: Becker, E. et al. (eds.): Digital Rights Management – Technological, Economic, Legal and Political Aspects. Berlin: Springer, S. 3-15

Rump N.; Barlas, C., 2004: From couch potato to active consumer. In: INDICARE Monitor, Vol. 1, No

4, September 2004; http://www.indicare.org/tiki-read_article.php?articleId=42

Stefik, M., 1996: Letting loose the light: Igniting commerce in electronic publication. In: Stefik, M. (ed): Internet dreams: Archetypes, myths, and metaphors. Cambridge, MA: The MIT Press, 3rd Printing 2001, S. 219-253

Stefik, M., 2000: The Bit and the Pendulum. In: The Internet Edge. Social, technical, and legal Challenges for a networked world. Cambridge, MA: The MIT Press, S. 79-106

Tyrväinen, P., 2005a: Concepts and a Design for Fair Use and Privacy in DRM. In: D-Lib Magazine, Vol. 11, No. 2; <http://www.dlib.org/dlib/february05/tyrvainen/02tyrvainen.html>

Tyrväinen, P., 2005b: Fair use licensing in library context. A privacy-preserving lending service with a revenue sharing business model. In: INDICARE Monitor, Vol. 2, No. 2, April 2005; http://www.indicare.org/tiki-read_article.php?articleId=94

Wikipedia, 2006a: Digital Rights Management; online abrufbar unter http://en.wikipedia.org/wiki/Digital_Rights_Management

Wikipedia, 2006b: Secure Digital Music Initiative; online abrufbar unter http://en.wikipedia.org/wiki/Secure_Digital_Music_Initiative

World Intellectual Property Organization, 1996: WIPO Copyright Treaty Art. 11 (adopted Dec. 20, 1996), available at http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html

Kontakt

Dipl.-Soz. Knud Böhle, M.A.
Forschungszentrum Karlsruhe GmbH
Institut für Technikfolgenabschätzung und Systemanalyse (ITAS)
Postfach 36 40, 76021 Karlsruhe
Tel.: +49 (0) 72 47 / 82 - 29 89
Fax: +49 (0) 72 47 / 82 - 48 06
E-Mail: boehle@itas.fzk.de
Internet: <http://www.itas.fzk.de>

«