# Rechtliche Technikgestaltung von Digital-Rights-Management-Systemen – ein Blick auf ein entstehendes Forschungsgebiet

von Stefan Bechtold, Max-Planck-Institut zur Erforschung von Gemeinschaftsgütern

Digital-Rights-Management-Systeme (DRM-Systeme) werden häufig als gegebene Größen betrachtet. Ein derzeit entstehendes interdisziplinäres Forschungsgebiet untersucht DRM-Systeme dagegen nicht mehr als unveränderliche, sondern als der rechtlichen Technikgestaltung zugängliche Systeme. Es wird untersucht, wie DRM-Systeme in einem wertorientierten Gestaltungsprozess verändert werden können, so dass wichtige rechtliche und politische Wertvorstellungen in solchen Systemen gewahrt bleiben. Der vorliegende Beitrag bietet einen kurzen Überblick über dieses Forschungsgebiet und liefert einige Beispiele konkreter Forschungsarbeiten im Schnittfeld von Technik, Urheberrecht, Datenschutzrecht und Wettbewerbspolitik.1

# 1 Einleitung

In den letzten Jahren ist viel darüber geschrieben worden, wie DRM das Urheberrecht privatisiert und ersetzt, urheberrechtliche Schrankenbestimmungen unterläuft, die Interessen von Nutzern und der Allgemeinheit insgesamt bedroht sowie Kreativität und Innovation durch die ungerechtfertigte Ausweitung des immaterialgüterrechtlichen Schutzes behindert. Auch wenn der Verfasser dieser Zeilen viele dieser Besorgnisse teilt, sollte beachtet werden, dass DRM-Technik viel flexibler und gestaltbarer ist, als dies von manchen DRM-Kritikern dargestellt wird.

Zunehmend werden DRM-Systeme nicht als unveränderliche Systeme verstanden, die dem rechtspolitischen Gestaltungsprozess nicht zugänglich wären. Die Frage lautet vielmehr, wie sie in einem wertbezogenen Gestaltungsprozess so verändert werden können, dass wichtige rechtliche und politische Wertvorstellungen in solchen Systemen gewahrt bleiben. Der Gedanke, Technikgestaltung an solchen Wertvorstellungen auszurichten, ist nicht neu,

wird jedoch erst seit jüngster Zeit auf DRM-Systeme angewendet.

#### 2 DRM und urheberrechtliche Schranken

DRM-Systeme sind in das Kreuzfeuer der Kritik geraten, weil durch sie urheberrechtliche Schrankenbestimmungen umgangen werden können und der Schutz von Inhalteanbietern zu Lasten der berechtigten Interessen von Nutzern und der Allgemeinheit erhöht wird. Diese Kritik mag derzeit auf viele kommerzielle DRM-Systeme zutreffen. Unbeantwortet ist jedoch die Frage, ob diese Kritik für DRM-Systeme generell gilt oder ob sie lediglich auf eine bestimmte Klasse von DRM-Systemen zutrifft. Diese Überlegung soll anhand von vier Beispielen illustriert werden.

# 2.1 Rights Expression Languages und Rights Messaging Protocols

Ob in einem DRM-System urheberrechtliche Schrankenbestimmungen gewahrt werden oder nicht, hängt von der Gestaltung der "rights expression languages" (REL) und der sie unterstützenden "rights messaging protocols" (RMP) ab. Mit Hilfe einer "rights expression language" kann ein DRM-System eine Vielzahl an Nutzungsbedingungen in maschinenlesbaren Metadaten ausdrücken, die mit dem geschützten Inhalt verbunden werden können. Mit Hilfe einer REL (wie z. B. XrML) lassen sich etwa die Berechtigung zum Kopieren, Löschen, Ändern, Einbetten, Ausführen, Exportieren, Extrahieren, Annotieren, Anmerken, Installieren, Sichern, Verleihen, Verkaufen, Weitergeben, Vermieten, Abspielen, Drucken, Anzeigen, Lesen, Wiederherstellen, Übertragen, Deinstallieren, Verifizieren, Sichern, Erhalten, Herausgeben, Besitzen und Zurückholen des Inhalts in maschinenlesbarer Form ausdrücken. Wenn sich Nutzungsarten, die unter einer urheberrechtlichen Schrankenbestimmung erlaubt sind, nicht in einer REL ausdrücken lassen, existieren diese Interessen einfach nicht im DRM-System. Deshalb ist es von größter Bedeutung, dass "rights expression languages" entsprechende Semantiken enthalten und so abgefasst werden, dass damit nicht nur die Interessen von Rechteinhabern, sondern auch von Nutzern und der Allgemeinheit ausgedrückt werden können. In einem Aufsatz aus dem Jahr 2002 skizzieren Deirdre Mulligan und Aaron Burstein von der University of California Berkeley Änderungen an XrML, die zu einer solchen "symmetrischen" REL führen würden (Mulligan, Burstein 2002). Ähnliche Ansätze finden sich unter anderem bei Arnab, Hutchison 2005 und im von Sun Microsystems initiierten "Open Media Commons"-Projekt.<sup>2</sup>

Nach Mulligan und Burstein muss ein DRM-System nicht nur in der Lage sein, eine große Vielfalt an Nutzungsbedingungen in seiner REL auszudrücken. Um bidirektionale-Verhandlungsprozesse zwischen Rechteinhabern und Nutzern darüber zu ermöglichen, welche Nutzungsrechte unter welchen Bedingungen zu gewähren sind, muss ein DRM-System auch über RMPs verfügen, die solche Prozesse unterstützen. Die meisten heutigen DRM-Systeme bieten Nutzern keine nennenswerte Möglichkeit, hinsichtlich der Nutzungsrechte in einen bilateralen Verhandlungsprozess zu treten. Obwohl in eCommerce-Systemen schon seit längerer Zeit an entsprechenden Verfahren gearbeitet wird, hat die Forschung erst in jüngster Zeit damit begonnen, solche Verfahren für DRM-Systeme zu entwickeln.

Bislang ist nicht klar, wie die technischen Komponenten, die für solche symmetrischen DRM-Systeme erforderlich sind, zwischen der REL und dem RMP eines DRM-Systems aufzuteilen sind. Manche Forscher versuchen, die erforderliche Funktionalität möglichst in die REL zu integrieren, während andere sie ausschließlich im RMP ansiedeln wollen. Allgemein ist festzustellen, dass die Forschung auf diesem Gebiet noch sehr lückenhaft ist. Sie wird außerdem durch ihre Interdisziplinarität erschwert, erfordert sie doch einen intensiven Austausch zwischen Technikern und Juristen

# 2.2 "Fair-use"-Infrastrukturen

In einem Aufsatz aus dem Jahr 2001 regen Dan Burk von der University of Minnesota und Julie Cohen von der Georgetown University unter anderem die Schaffung einer "Fair-use-Infrastruktur" an (Burk, Cohen 2001). Nach ihrem Vorschlag einer so genannten "key escrow" (etwa: treuhänderische Schlüsselhinterlegung) können sich Berechtigte urheberrechtlicher

Schrankenbestimmungen an eine dritte Instanz wenden, um Dechiffrier-Schlüssel für DRMgeschützte Inhalte zu erhalten und damit von der Schrankenbestimmung Gebrauch machen zu können. Dieser Vorschlag ist ein weiteres Beispiel, wie die Gestaltung von DRM-Systemen modifiziert werden kann, um das Spannungsverhältnis zwischen DRM-Systemen und urheberrechtlichen Schrankenbestimmungen schon auf technischer Ebene zu entschärfen. Interessant ist dabei, dass dieser Vorschlag gewisse Ähnlichkeiten mit der rechtlichen Regelung zum Verhältnis zwischen technischen Schutzmaßnahmen und urheberrechtlichen Schrankenbestimmungen aufweist, wie sie in Artikel 6 Absatz 4 der Europäischen Urheberrechtsrichtlinie aus dem Jahr 2001 (Richtlinie 2001/29/EG 2001) sowie in § 95b des deutschen Urheberrechtsgesetzes geregelt ist.

# 2.3 Architekturen für die Authorized Domain

DRM-Systeme berücksichtigen zunehmend so genannte "authorized domains", mitunter auch "family domains" genannt.<sup>3</sup> Diesen Architekturen liegt die Vorstellung zugrunde, dass der Konsument auf den Inhalt nicht nur mit einem bestimmten Gerät zugreifen will. Vielmehr will er den Inhalt auf unterschiedlichen Geräten, die ihm gehören, nutzen. Erwirbt ein Konsument beispielsweise eine Musikdatei, so will er diese Musik nicht nur auf seinem MP3-Player anhören, sondern will sie auch auf seine Stereoanlage, sein Autoradio oder sein Mobiltelefon kopieren. Der Ansatz der "authorized domain" besagt, dass Inhalte, die der Konsument rechtmäßig erworben hat, auf allen Geräten, die ihm gehören, abgespielt werden können. Bei einer derartigen Architektur sind digitale Rechte zwischen verschiedenen Geräten übertragbar, da Genehmigungen zur Nutzung von Inhalten nicht mehr an ein bestimmtes Gerät, sondern an den Konsumenten selbst gebunden sind.

"Authorized domain"-Architekturen sind ein Versuch, die Ausgestaltung von DRM-Systemen an urheberrechtliche Schrankenbestimmungen anzunähern. Sie sind auch ein Beispiel dafür, wie Techniker auf Konsumentenpräferenzen und im Urheberrecht niedergelegte Wertvorstellungen eingehen. Natürlich haben "authorized domain"-Architekturen ihre

eigenen Probleme und sind keine Patentlösungen für die Implementierung urheberrechtlicher Schrankenbestimmungen in einer digitalen Welt. Sie sind jedoch ein Beispiel für eine rechtliche Technikgestaltung, wird hier doch schon bei der Entwicklung der DRM-Architektur versucht, Wertvorstellungen zu berücksichtigen, die dem technischen Entwicklungsprozess eigentlich fremd sind.

# 2.4 Das Digital Media Project

Das "Digital Media Project", von Leonardo Chiariglione im Sommer 2003 ins Leben gerufen, will die technischen Grundlagen einer Umgebung für digitale Medien schaffen, in der die Interessen von Urhebern, Rechteinhabern, Nutzern und weiteren an der Wertschöpfungskette beteiligten Akteuren berücksichtigt werden und digitale Medienangebote gleichzeitig kommerziell erfolgreich vertrieben werden können. Zu diesem Vorhaben gehört auch die Identifizierung und Spezifizierung von Rechten und Nutzungsarten, die dem Nutzer bei den analogen Medienangeboten offen standen und die auch in DRM-Umgebungen zur Verfügung stehen sollen ("traditional rights and usages"). Ähnliche Ansätze finden sich auch im "Open Media Commons"-Projekt von Sun Microsystems. Obwohl sich diese Projekte noch in der Entwicklungsphase befinden, könnten sie die Entwicklung und Implementierung von DRM-Systemen, die sich an einer rechtlichen Technikgestaltung orientieren, erheblich weiterbringen.<sup>4</sup>

# 3 DRM-Systeme und der Datenschutz

DRM-Systeme bedienen sich verschiedener Mechanismen, um Nutzer innerhalb des Systems zu identifizieren und zu verfolgen. So kann potentiell nachvollzogen werden, welche Medienangebote Nutzer lesen, hören oder ansehen. Obwohl das Spannungsverhältnis zwischen DRM-Systemen und dem Datenschutz seit langem bekannt ist, gibt es bis heute keinen klaren Ansatz, wie dieses Spannungsverhältnis zu lösen wäre. Julie Cohen von der Georgetown University argumentiert, ein Teil der Lösung sei in einer rechtlichen Technikgestaltung zu suchen (Cohen 2003). Sie schlägt vor, in bestimmten Fällen die Funktionalität von DRM-Systemen

technisch derart zu beschränken, dass ein gewisser Spielraum für datenschutzfreundliche Nutzungen (wie dem Erstellen von Kopien zum privaten Gebrauch) entstünde, während gleichzeitig die Informationsanbieter weiterhin vor Raubkopiertätigkeit in kommerziellem Umfang geschützt blieben. Für eine solche rechtliche Technikgestaltung wären auch Verfahren zu entwickeln, mit denen die Erstellung und Nutzung von Nutzungs- und Persönlichkeitsprofilen beschränkt werden kann. Schließlich wäre zu erwägen, ob die Schutzmaßnahmen, mit denen Rechteinhaber ihre Interessen schützen, nicht auf technischer Ebene begrenzt werden sollten. Ein solcher Design-Ansatz sollte nicht als Einschränkung der Funktionalität von DRM-Systemen, sondern als Chance aufgefasst werden, konkurrierende Wertvorstellungen - unter anderem die Interessen von Urhebern, Rechteinhabern und Nutzern - auf technischer Ebene miteinander zu vereinen.

# 4 Trusted Computing und Owner Override

In den letzten Jahren ist so genannten "Trusted Computing Platforms" (wie etwa der "Trusted Computing Group" und dem Microsoft-Projekt "Next Generation Secure Computing Base") von Technikern, Juristen, Ökonomen und "Cyberpolicy"-Aktivisten viel Aufmerksamkeit zuteil geworden. "Trusted Computing"-Architekturen versuchen, durch technische Lösungen das allgemeine Vertrauen in unsere IT-Umgebung zu erhöhen. Nach dem "Trusted Computing"-Ansatz kann einer Systemkomponente nur vertraut werden, wenn sie sich stets in der erwarteten Weise hinsichtlich des verfolgten Zwecks verhält. Teilt ein bestimmtes Softwareprogramm einem Anwender mit, was es gerade macht, so soll der Anwender durch Trusted Computing dieser Aussage auch tatsächlich vertrauen können. Um dieses Vertrauen in Softwareprogramme zu ermöglichen, fügen "Trusted Computing"-Architekturen spezielle Hardware-Bausteine in die herkömmliche Computerarchitektur ein, die die Grundlage für ein solches Vertrauen legen sollen. Dadurch bieten Trusted Computing-Architekturen sowohl dem Eigentümer einer Plattform wie auch beliebigen Dritten den Nachweis der Integrität und Authentizität der Plattform. Viele Beobachter haben darauf hingewiesen, dass "Trusted Computing"-Architekturen von Dienste- und Softwareanbietern verwendet werden könnten, um Wettbewerb auf Endkundenmärkten zu behindern und "Lockin"-Effekte zu erzielen. Vor einiger Zeit hat Seth Schoen (2003) von der "Electronic Frontier Foundation" (EFF) vorgeschlagen, Benutzern von "Trusted Platforms" die Möglichkeit einzuräumen, falsche Integritätsangaben an Diensteund Softwareanbieter zu senden (die "Owner-Override"-Funktion). Dann könnte der Anbieter solche Angaben nicht mehr zur Grundlage wettbewerbsschädlicher Verhaltensweisen machen.

Die Beziehung zwischen "Trusted-Computing"-Architekturen und DRM-Systemen ist kompliziert und geht über den Rahmen des vorliegenden Beitrags hinaus. Obwohl der Verfasser aus verschiedenen Gründen vom Vorschlag der EFF nicht überzeugt ist, stellt dieser ein weiteres Beispiel dar, wie technische Architekturen schon im Entwurfsstadium beeinflusst werden können, damit rechtliche und politische Wertvorstellungen gewahrt bleiben.

# 5 Schlussfolgerung

Die Vorstellung einer wertorientierten und rechtlichen Technikgestaltung ist alt. Sie wird aber erst seit kurzem im Bereich der DRM-Entwicklung angewendet. Verschiedene Forschungsprojekte loten die Möglichkeiten und Grenzen dieses Ansatzes aus. Ein übergreifendes Forschungskonzept existiert bisher nicht. Rechtliche Technikgestaltung im DRM-Bereich wird dadurch erschwert, dass eine enge wechselseitige Beziehung zwischen Technikern, Juristen und Ökonomen erforderlich ist - mit den üblichen Vorteilen und Grenzen interdisziplinärer Forschung. Techniker müssen sich mit rechtlichen Grundlagen auseinandersetzen. Wie Barbara Fox und Brian LaMacchia von Microsoft ausgeführt haben, benötigen Techniker außerdem angemessene Anreize, damit sie sich überhaupt auf eine solche rechtliche Technikgestaltung einlassen (Fox, LaMacchia 2003). Juristen und Ökonomen müssen lernen, technische Konzepte und ihre Konsequenzen zu verstehen.

Rechtliche Technikgestaltung stößt bei DRM-Systemen auch an inhärente Grenzen. Viele rechtliche Probleme lassen sich nicht auf einer technischen Ebene lösen. Manche Rechtssätze sind offen formuliert und machen eine technische Umsetzung nahezu unmöglich. Außerdem kommt es bei den rechtlichen Problemen von DRM immer auf den Ausgleich unterschiedlicher Interessen an. Wertorientierte Gestaltungsprozesse können ein nützliches Hilfsmittel sein, um einen bestimmten Interessenausgleich zu implementieren. Sie bieten aber keinen Anhaltspunkt dafür, wie dieser Ausgleich grundsätzlich herbeigeführt werden kann. Schließlich hat die Automatisierung der Rechtsdurchsetzung durch technische Systeme grundlegende Nachteile, da die Systeme eine Reduzierung der rechtlichen Fragen auf einfache Ja- / Nein-Fragen erzwingen, was nicht in allen Fällen angemessen ist (Erickson, Mulligan 2004; Erickson 2003).

Rechtliche Technikgestaltung im DRM-Bereich ist ein viel versprechender Ansatz, der noch weitgehend unerforscht ist. Letztlich weiß derzeit niemand, ob ein ausgewogenes DRM-System, das die Interessen von Rechteinhabern, Nutzern und der Allgemeinheit schützt, technisch realisierbar und wirtschaftlich tragfähig wäre. Wie jedes technische System sind auch DRM-Systeme gestaltungsfähig. Daher sollte man die Gelegenheit einer rechtlichen Technikgestaltung von DRM-Systemen nicht versäumen.

### Anmerkungen

- Der vorliegende Beitrag ist die autorisierte Übersetzung eines für den INDICARE Monitor verfassten Beitrags (Bechtold 2004), der für die vorliegende Veröffentlichung geringfügig überarbeitet und den redaktionellen Vorgaben der TATuP angepasst wurde. Weitere einschlägige Veröffentlichungen des Autors zu DRM sind Bechtold 2002 und 2003; außerdem sei auf den "Trusted Computing Blog" des Autors unter http://cyberlaw.stanford.edu/blogs/bechtold/tcb log.shtml hingewiesen. (Anm. d. Red.)
- 2) http://www.openmediacommons.org
- 3) Ein verwandtes Konzept ist die so genannte "rights locker architecture".
- 4) Weitere Informationen zum Digital Media Project sind zu finden unter <a href="http://www.dmpf.org">http://www.dmpf.org</a>.

#### Literatur

Arnab, A.; Hutchison, A., 2005: Fairer Usage Contracts For DRM. 5th ACM Workshop on Digital Rights Management, Alexandria V.A. USA, November 7, Manuskript online verfügbar unter http://pubs.cs.uct.ac.za/archive/00000231/01/fair\_use acm.pdf (download am 18.7.2006)

Bechtold, St., 2002: Vom Urheber- zum Informationsrecht. München: Beck; online verfügbar unter http://www.jura.uni-tuebingen.de/bechtold/pub/2002/DRM\_Diss.pdf (download am 18.7.2006)

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 (download am 18.7.2006)

Bechtold, St., 2004: Value-centered design of Digital Rights Management – Perspectives on an Emerging Scholarship. In: INDICARE Monitor, Vol. 1, No. 4, September 2004; online verfügbar unter: http://www.indicare.org/tiki-read\_article.php?articleId=39 (download am 18.7.2006)

*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

Cohen, J.E., 2003: DRM and Privacy. In: Berkeley Technology Law Journal 18 (2003), S. 575-617

*Erickson, J.S.*, 2003: Fair Use, DRM, and Trusted Computing. In: Communications of the ACM 46/4 (2003), S. 34-39

*Erickson, J.S.; Mulligan, D.K.*, 2004: The Technical and Legal Dangers of Code-Based Fair Use Enforcement. Proceedings of the IEEE. Vol. 92, No. 6, June 2004, S. 985-996

Fox, B.L.; LaMacchia, B.A., 2003: Encouraging Recognition of Fair Uses in DRM Systems. In: Communications of the ACM 46/4 (2003), S. 61-63

Mulligan, D.K.; Burstein, A., 2003: Implementing Copyright Limitations in Rights Expression Languages. In: Feigenbaum, J. (ed.): Security and Privacy in Digital Rights Management. New York: Springer, S. 137-154; online verfügbar unter: http://crypto.stanford.edu/DRM2002/mulligan\_burste in acm drm 2002.doc (download am 18.7.2006)

Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft. In: Amtsblatt der Europäischen Gemeinschaften Nr. L 167 vom 22. 6. 2001, S. 10-19

Schoen, S., 2003: Trusted Computing: Promise and Risk; online verfügbar unter: http://www.eff.org/Infrastructure/trusted\_computing/20031001\_tc.pdf (download am 18.7.2006)

#### Kontakt

Dr. Stefan Bechtold, J.S.M. (Stanford) Max-Planck-Institut zur Erforschung von Gemeinschaftsgütern Kurt-Schumacher-Straße 10, 53113 Bonn

Tel.: +49 (0) 228 / 914 16 - 71 Fax: +49 (0) 228 / 914 16 - 55 E-Mail: stef@n-bechtold.com Internet: http://www.bechtold.name

**«**