

[ivirbumaconference.org/docs/thefutureofdigitalrightsmanagementformusic1.doc](http://ivirbumaconference.org/docs/thefutureofdigitalrightsmanagementformusic1.doc) [last visit 23.06.2006]

Rosenblatt, B., 2005: Meltdown Continues over First4Internet's CD Copy Protection. In: DRM Watch, November 17, 2005; available at: <http://www.drmwatch.com/drmtech/article.php/3565106> [last visit 23.06.2006]

Sony, 1984: Supreme Court decision in Sony vs. Universal; available at: <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=464&invol=417> [last visit 23.06.2006]

USC 17: United States copyright law; available at: <http://www.law.cornell.edu/uscode/17/> [last visit 23.06.2006]

USC 35: United States patent law; available at: [http://www.law.cornell.edu/uscode/html/uscode35/usc\\_sup\\_01\\_35.html](http://www.law.cornell.edu/uscode/html/uscode35/usc_sup_01_35.html) [last visit 23.06.2006]

USCA, 2005: DC circuit Court of Appeals decision to strike down Broadcast Flag regulation; available at: <http://pacer.cadc.uscourts.gov/docs/common/opinion/s/200505/04-1037b.pdf> [last visit 23.06.2006]

WIPO, 1996: WIPO international copyright treaty; available at: [http://www.wipo.int/treaties/en/ip/wct/trtdocs\\_wo033.html](http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html) [last visit 23.06.2006]

## Contact

Bill Rosenblatt  
President  
GiantSteps Media Technology Strategies  
1841 Broadway, Suite 200, New York, NY 10023,  
USA  
Tel.: +1 - 212 - 956 10 45  
Fax: +1 - 212 - 258 32 86

»

## Privacy4DRM: Nutzer- und datenschutzfreundliches Digital Rights Management

von Jan Möller, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, und Stefan Puchta, Fraunhofer-Institut für Digitale Medientechnologie

**Ziel dieses Artikels ist es, einen Überblick über Inhalt und Ergebnisse der Studie „Privacy4DRM“ zu geben, die vom Bundesministerium für Bildung und Forschung (BMBF) gefördert wurde. Dabei werden zunächst Eigenschaften und Einsatzumfeld von klassischen Systemen des Digital Rights Managements (DRM) näher beleuchtet; anschließend wird die datenschutzrechtlich geprägte Untersuchungsmethode erläutert, gefolgt von der Darstellung der konkreten rechtlichen Anforderungen an DRM-Systeme. Abschließend werden Handlungsempfehlungen und Forschungsbedarf in diesem Zusammenhang vorgestellt.**

### 1 Einleitung

Virtuelle Güter in digitaler Form (kurz: digitale Inhalte) spielen eine zentrale Rolle in der Informationsgesellschaft. Dabei kommt dem Schutz und dem Management der Urheber- und Verwertungsrechte einerseits und der Wahrung von Kunden- und Nutzerrechten andererseits eine wichtige Bedeutung zu. Die seit einiger Zeit geführten Debatten zielen dabei besonders auf den Sinn und die Einsatzmöglichkeiten so genannter digitaler Rechtemanagement-Systeme (DRM-Systeme) ab. Dabei zeigt sich, dass die Verwendung von DRM-Technik in aktuellen eCommerce-Anwendungen nicht nur technische sondern auch vielfältige rechtliche Probleme aufwirft – insbesondere, wenn es um den Schutz der Privatsphäre des einzelnen Nutzers geht. Eine datenschutzkonforme, das informationelle Selbstbestimmungsrecht des Kunden respektierende Gestaltung von DRM-Systemen ist aber nicht nur unter Compliance-Gesichtspunkten<sup>1</sup> geboten, sondern ist für das einsetzende Unternehmen auch eine Frage der Beziehung zum und des Umgangs mit dem Kunden.

In der Studie „Privacy4DRM“, die das Fraunhofer Institut für digitale Medientechnologie (IDMT) Ilmenau zusammen mit dem Unab-

hängigen Landeszentrum für Datenschutz in Kiel (ULD) und dem Institut für Medien- und Kommunikationswissenschaft der TU Ilmenau (IfMK) im Auftrag des BMBF durchgeführt hat, wurden aktuelle DRM-Systeme anhand zentraler Prinzipien des Datenschutzes analysiert (Bizer, Grimm, Will et al. 2005). Das Projekt wurde im Rahmen des Teilnahmewettbewerbs „Innovationspotenziale der Informationstechnik“ gefördert. Als Projektträger agierte die Innovations- und Technikanalyse (ITA) des BMBF.<sup>2</sup> In der Durchführung wurde interdisziplinär vorgegangen und eine entsprechende Untersuchungsmethodik entworfen und angewendet, innerhalb derer das IDMT den technischen, das ULD den rechtlichen und das IfMK den ökonomischen Projektteil bearbeitete. Anschließend wurden gemeinsam mögliche Handlungsempfehlungen zur datenschutz- und nutzerfreundlichen Gestaltung und Implementierung von DRM-Techniken entwickelt.

## 2 DRM-Systeme

### 2.1 Das klassische DRM-Modell

Das derzeit häufig anzutreffende DRM-Modell geht über den lange bekannten einfachen Kopierschutz hinaus. Es trennt Nutzungslizenzen vom Medieninhalt (Content) mit dem Ergebnis, dass nur der (rechtmäßige) Inhaber einer zum Content gehörenden Lizenz diesen auch nutzen kann. Technisch unterscheidet man „Contentserver“ und „Lizenzserver“, die ihrer Funktion entsprechend Inhalte und zugehörige Lizenzen bereitstellen und an den Nutzer ausliefern. Der eigentliche Inhalt ist dabei meist verschlüsselt und kann erst mittels des mit der Lizenz gelieferten Schlüssels freigeschaltet und benutzt werden. Die Lizenz enthält die möglichen Nutzungsrechte und wird durch kryptografische Mechanismen an den Nutzer bzw. an seinen PC gebunden. Die Trennung von Lizenz und Inhalt ermöglicht grundsätzlich die Superdistribution digitaler Inhalte, d. h. die Verbreitung der Inhalte von Nutzer zu Nutzer, wobei die Inhalte von jedem Nutzer erst wieder erneut „freigeschaltet“ werden müssen. Also auch der jeweils neu adressierte Nutzer muss eine entsprechende Lizenz erwerben (Chip 2006, Secor 2004, Kawahara 2006). Im Gegensatz zu der grundsätzlichen Möglichkeit, Inhalte schnell und einfach zu

verbreiten, erschweren fast alle aktuellen DRM-Systeme den Weiterverkauf einmal erworbener Medieninhalte. Die Schwierigkeit, Inhalte von einem Nutzer an den nächsten weiterzuverkaufen, wie es bisher mit CDs möglich ist, besteht vor allem darin, dass Inhalte fest mit Nutzersystemen verbunden sind und es mit vielen DRM-Systemen faktisch nicht oder nur schwer möglich ist, diese Regeln zu umgehen. Darüber hinaus verbieten häufig auch Lizenzbestimmungen die Weiterveräußerung von Inhalten.

### 2.2 Das „DRM-Dilemma“

Bei klassischen DRM-Systemen spricht man auch von Digital Rights Enforcement (DRE), da Verwertungsrechte durch auf dem Nutzergerät installierte Systeme (oftmals gegen den Willen des Nutzers) organisiert und durchgesetzt werden. Darin liegt ein erhebliches Problem: Nutzerinteressen an freier und uneingeschränkter Verwendung werden durch Technik beschnitten oder gar komplett verhindert, die im Einflussbereich des Nutzers angesiedelt ist. Werden legitime Erwartungen möglicher Nutzungen („fair use“) und Abspielemöglichkeiten („Interoperabilität“) enttäuscht, öffnet diese Konstellation dem Nutzer die Möglichkeit, die ungeliebte Technik anzugreifen und Beschränkungen aufzuheben (Aichroth, Hasselbach 2003; Merrit, Chin 2006). Das dazu erforderliche Know-how ist leicht über das Internet zu beschaffen, so dass DRM-Umgehung keinem exklusiven Club von Wissenden vorbehalten bleibt. Klassische DRM-Systeme lassen insofern ein grundlegendes IT-Security-Prinzip außer Acht: Danach sollte derjenige, der ein Interesse an einer Sache hat, auch die Mittel zu ihrer Durchsetzung in seiner Hand halten. Neben dieser Missachtung grundlegender IT-Security-Prinzipien ist ein weiterer Gesichtspunkt von besonderer Bedeutung. Eine Vielzahl verschiedener DRM-Systeme führt zu Inkompatibilitäten von Inhalten mit Abspielgeräten, die den Nutzen geschützter digitaler Inhalte einschränken. Der Anreiz, nicht geschützte Inhalte aus möglicherweise nicht legaler Quelle zu verwenden, steigt, weil damit Kompatibilitätsprobleme entfallen.

Den Einsatz von DRM-Technik ergänzt die Strategie der Rechtheverwerter, auf die Etablierung moralischer Standards für geistige Eigentumsrechte einerseits und auf die straf- und zi-

vilrechtliche Verfolgung von Urheber- und Verwertungsrechtsverstößen andererseits zu setzen. Insbesondere letztere richtet sich als abschreckende Maßnahme gegen alle Nutzer. Sie werden durch diese Strategie zu potentiellen „Rechteverletzern“; damit wird das Vertrauen der eigenen Kunden und folglich die ökonomisch anstrebenswerte vertrauensvolle Kundenbeziehung zerstört. Beispielhaft sei die „Hart-aber-gerecht“-Kampagne der deutschen Filmwirtschaft angeführt, die mit zum Teil drastischen Mitteln versucht, Nutzer von Raubkopien zu kriminalisieren (<http://www.hartabergerecht.de>).

### 2.3 Nutzeridentifikation und -kontrolle

Zusätzlich zur Sicherung von Verwertungsrechten durch DRM-Systeme werden oftmals auch ohne Wissen und Kontrollmöglichkeiten des Nutzers personenbezogene Informationen in Inhalte eingebracht. Dieses erfolgt z. B. durch einfaches Speichern von Zusatzdaten in den Content oder in die Lizenz – meist mittels Wasserzeichentechnologien oder anderer steganographischer Techniken (Bizer, Grimm, Will et al. 2005, S. 18 ff.). Solche Informationen ermöglichen beispielsweise das Auffinden des Ersterwerbers eines Inhalts, ohne auf Auskunftsansprüche gegenüber Dritten (z. B. Internet Providern) angewiesen zu sein. So können Lizenzverstöße (z. B. die Weitergabe von Inhalten an Dritte), die aufgrund der Schutzlücken von DRM-Technik auftreten, der rechtlichen Ahndung zugeführt werden. Sie können insofern als „second line of defense“ hinter der DRM-Technik, die als first line zu betrachten ist, angesehen werden. Der Einsatz dieser Mittel kann dabei naturgemäß nicht zwischen „legal“ und „potentiell illegal“ handelnden Nutzern differenzieren. Das Misstrauen der Verwerter bezahlen damit letztlich alle Kunden mit der Verwendung personenbezogener Informationen zur Verfolgung potentiell nicht rechtstreuen Verhaltens und der Verhinderung eines legalen „Gebrauchsmarktes“ für digitale Inhalte. Dies schädigt letztendlich das Vertrauen der Kunden in die Shopbetreiber und Inhalteanbieter. Darüber hinaus können Inhalteanbieter auch noch zu einem späteren Zeitpunkt personenbezogene Daten mit eingebrachten Nutzerkennungen verbinden und damit weitere Rückschlüsse auf das Nutzerverhalten ziehen. Sol-

che Maßnahmen setzen den Kunden unter Überwachungsdruck und bringen ihn möglicherweise dazu, sich von Online-Märkten mit DRM-Systemen zurückzuziehen.

### 2.4 Datenschutzrechtliche Vorgaben für DRM-Systeme

Die Bindung eines digitalen Inhalts an einen konkreten Nutzer und bestimmte Endgeräte lässt bereits erkennen, dass derzeitige DRM-Techniken eine ganze Reihe personenbezogener Daten verarbeiten. Dabei sind die bestehenden datenschutzrechtlichen Vorgaben auf europäischer und nationaler Ebene zu beachten und einzuhalten.

In einer datenschutzrechtlichen Analyse von Technik, wie sie in dem Projekt „Privacy4DRM“ vorgenommen wurde, sind zunächst die Informationen aus den technischen Systemen zu extrahieren, die für die Rechtsprüfung erforderlich sind (Bizer, Grimm, Will et al. 2005, S. 30 ff.; Möller, Bizer, 2006, S. 81; Grimm, Puchta, 2006, S. 75 f.). Im Bereich des Datenschutzrechts sind dies insbesondere Informationen über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sowie Kontextinformationen, aus denen sich z. B. der Zweck der Datenverarbeitung, die Empfänger personenbezogener Daten, die Erfüllung von Transparenzanforderungen oder die Umsetzung von Betroffenenrechten ergeben. Diese Informationen können mittels einer Datenfluss-Analyse ermittelt werden. Dazu wird die Technik in einem konkreten oder wahrscheinlichen Anwendungsumfeld platziert. Derzeit eingesetzte DRM-Techniken sind in der Regel in Distributionsplattformen für digitale Inhalte (Onlineshops) eingebunden. In diesem Kontext wird dann analysiert, welche personenbezogenen Daten – im Rahmen der im Geschäftsmodell vorgesehenen Aktionen – erhoben, gespeichert oder genutzt werden. Diese Datenspuren lassen sich für DRM-Systeme in folgende Kategorien einteilen:

- Datenfluss vor Vertragsschluss,
- Datenfluss bei Vertragsschluss,
- Datenfluss, der bei der Rechteüberprüfung durch DRM-Systeme generiert wird,
- Datenfluss für andere Zwecke,
- Datenfluss durch verborgene Schnittstellen und Verkettung verschiedener Funktionen.

Die genannten Kategorien bereiten die rechtliche Analyse der personenbezogenen Datenverarbeitung insofern vor, als hier nach Zwecken differenziert wird, für die bestimmte Erlaubnistatbestände eine personenbezogene Datenverarbeitung zulassen können bzw. für die explizit eine Einwilligung des Betroffenen vorliegen muss, um rechtmäßig zu sein. Ergänzt wird diese am Zulässigkeitsprinzip und am Zweckbindungsgrundsatz des Datenschutzrechts orientierte Aufbereitung der Datenspuren durch das „Transparenzprinzip“. Gegen dieses wird verstoßen, wenn Datenflüsse oder Verarbeitungen für den Betroffenen nicht sichtbar sind, er hierüber nicht informiert wird und / oder die Auflösbarkeit von Pseudonymen erst durch später hinzutretendes Zusatzwissen möglich oder tatsächlich umgesetzt wird. Probleme dieser Art treten insbesondere bei Techniken in stark vernetzten technischen Umfeldern auf. Sie schränken die Fähigkeit des Betroffenen ein, von seinem informationellen Selbstbestimmungsrecht Gebrauch zu machen.

Vor dem Hintergrund des so genannten Selbst Datenschutzes<sup>3</sup>, also den Maßnahmen, die der Nutzer treffen kann, um die Kontrolle über seine personenbezogenen Daten zu behalten, macht es darüber hinaus Sinn, zwischen verschiedenen Datenspuren zu unterscheiden. Dazu gehören Datenspuren, die vom Anbieter erzeugt oder erhoben wurden, solche, die vom Nutzer erzeugt oder erhoben wurden, und solche, die in das Produkt vom Anbieter oder Dritten einkodiert wurden. Der entsprechend informierte und möglicherweise auch technisch ausgestattete Nutzer kann zumindest das Anlegen bestimmter Datenspuren vermeiden (z. B. wenn weitere Informationen zur Auflösung von Pseudonymen nicht preisgegeben werden). Mit diesem theoretischen Rüstzeug wurden in dem hier dargestellten Projekt die rechtlichen Anforderungen an DRM-Systeme anhand des geltenden Rechts geprüft und Defizite festgestellt.

### 3 Rechtliche Anforderungen an DRM-Systeme

Die Datenschutzrichtlinien der EU sowie das sie national umsetzende Datenschutzrecht enthalten einschlägige datenschutzrechtliche Anforderungen auch für DRM-Systeme. Zusammenfassend betrachtet bilden die Rechtsnor-

men des Datenschutzrechts die datenschutzrechtlichen Grundprinzipien ab, die in der Gestaltung der Technologie wie auch in der späteren Implementierung in der Praxis zu berücksichtigen sind. Hierzu gehören:

- die *Zulässigkeit personenbezogener Datenverarbeitung*: Personenbezogene Daten dürfen nur erhoben, verarbeitet oder genutzt werden, wenn eine informierte, freiwillige Einwilligung des Betroffenen vorliegt oder eine Rechtsvorschrift die Verarbeitung explizit erlaubt. Eine solche Erlaubnisvorschrift existiert unter anderem für personenbezogene Datenverarbeitungen, die zur Zweckbestimmung eines Vertrages, also insbesondere auch dessen Durchführung erforderlich sind (Möller, Bizer, 2006, S. 81; Bizer, Grimm, Will et al. 2005, S. 33).
- die *Zweckbindung*: Nach dem allgemeinen Zweckbindungsgrundsatz dürfen personenbezogene Daten nur zu vorher konkret festgelegten Zwecken (Primärzweck) erhoben, verarbeitet oder genutzt werden; eine Vorratsdatenspeicherung ohne konkreten Zweck ist damit unzulässig. Zweckänderungen sind unter bestimmten, die Rechte des Betroffenen währenden Voraussetzungen möglich (Möller, Bizer, 2006, S. 82; Bizer, Grimm, Will et al. 2005, S. 34).
- die *Erforderlichkeit*: Personenbezogene Daten dürfen nur insoweit verarbeitet werden, wie dies für die Zweckerreichung erforderlich und von der Einwilligung oder erlaubenden Rechtsvorschrift abgedeckt ist. Darüber hinaus ist auf eine datenvermeidende und datensparsame Gestaltung von Datenverarbeitungssystemen zu achten (Möller, Bizer, 2006, S. 82; Bizer, Grimm, Will et al. 2005, S. 34).
- die *Transparenz*: Um dem datenschutzrechtlichen Leitbild des informationellen Selbstbestimmungsrechts<sup>4</sup> entsprechen zu können, muss beim Betroffenen ein Wissensfundament über die Art, grundlegende Funktionsweise und Zweck personenbezogener Datenverarbeitung im Rahmen der eingesetzten Technik bestehen. Dieses wird vornehmlich durch eine Reihe von Informationspflichten der verantwortlichen Datenverarbeiter und Auskunftsrechte der Betroffenen erreicht (Möller, Bizer, 2006, S. 83; Bizer, Grimm, Will et al. 2005, S. 35).

- *die Qualität der Daten*: Bestände personenbezogener Daten, die zu bestimmten Zwecken auch im Rahmen von DRM-Systemen vorgehalten werden, müssen aktuell und inhaltlich korrekt sein. Dies schützt den Betroffenen u. a. vor Diskriminierungen aufgrund von falschen oder überholten zu seiner Person gespeicherten Daten (Möller, Bizer 2006, S. 83; Bizer, Grimm, Will et al. 2005, S. 35).
- *die Sicherheit der Daten*: Ein Schutz personenbezogener Daten lässt sich insbesondere in Datenverarbeitungsanlagen nur sicherstellen, wenn die verantwortliche Stelle die vollständige und alleinige Verfügungsgewalt über diese Daten hat. Dies ist nur zu gewährleisten, wenn ein angemessenes Maß an IT-Sicherheit durch entsprechende technische und organisatorische Maßnahmen sichergestellt werden kann (Möller, Bizer, 2006, S. 81; Bizer, Grimm, Will et al. 2005, S. 36).

#### 4 Ergebnisse der Studie und Handlungsempfehlungen

In der Studie „Privacy4DRM“ wurden beispielhaft „iTunes“ von Apple, „Musicload“ von T-Online in Verbindung mit „Windows Media Rights Manager“, „Sony Connect“, das „PotatoSystem“ von 4FO und Fraunhofer IDMT sowie „Adobes Media Store“ untersucht. Dabei wurde die Einkodierung verschiedener personenbezogener oder nutzersystembezogener Daten festgestellt, die ihrerseits Möglichkeiten zur Verbindung mit Nutzeraktivitäten eröffnen. Beispielsweise werden sowohl bei „iTunes“ als auch bei „Musicload“ so genannte System-IDs verwendet, die eindeutige Zuordnungen zum Nutzersystem ermöglichen. In den iTunes-Dateien wird zusätzlich die E-Mail-Adresse des Nutzers<sup>5</sup> eingebracht. Im Gegensatz zu den eben erwähnten Systemen verwendet das „PotatoSystem“ keinerlei DRM-Maßnahmen, um Rechte an Inhalten durchzusetzen.<sup>6</sup>

Die datenschutzrechtliche Analyse verschiedener DRM-Techniken und der sie einsetzenden Verkaufsplattformen hat eine Reihe datenschutzrechtlicher Defizite aufgezeigt. Bei den Verkaufsplattformen traten dabei vor allem eCommerce-typische Datenschutzmängel auf. Personenbezogene Datenerhebungen gehen über das für die Vertragserfüllung erforderliche Maß

hinaus und sind aufgrund unwirksamer Einwilligungen rechtswidrig. Die mit der DRM-Technik verbundene personenbezogene Datenverarbeitung kann als Vertragsbestandteil zur Durchsetzung der Lizenzrechte zulässig sein. Dies setzt jedoch voraus, dass die Datenverarbeitung nicht über das erforderliche Maß hinausgeht, dem Kunden die Verarbeitung zu diesem Zweck als Vertragsbestandteil bewusst und die strikte Zweckbindung der Datenverarbeitung sichergestellt ist. Diese Anforderungen konnten die untersuchten Anbieter nur teilweise erfüllen (Bizer, Grimm, Will et al. 2005, S. 7). Insbesondere hinreichende Transparenz und eine datensparsame Technikgestaltung weisen die aktuell im Einsatz befindliche DRM-Techniken nicht auf. Als Beispiel dieser Problematik sei die Einkodierung einer E-Mail-Adresse des Erwerbers in den erworbenen Inhalt genannt, die von jedem ausgelesen werden kann. Diese Einkodierung wird dem Kunden nicht mitgeteilt und lässt gleichzeitig als „second line of defense“ die Ermittlung von (Erst-)Erwerbern von in rechtlich zweifelhaften Quellen gefundenen Inhalten zu. Ob eine solche Nutzung einkodierter personenbezogener Daten zu Zwecken der Rechtsverfolgung beabsichtigt ist, lässt sich im konkreten Fall mangels Kommunikation der Tatsache der Einkodierung an sich nur vermuten. Das starke Bestreben der Rechteinhaber, einen Auskunftsanspruch zur Verfolgung von Urheberrechtsverletzungen gegenüber Internet Providern auch gesetzlich festschreiben zu lassen, deutet jedoch darauf hin, dass ein solcher Nutzungszweck zumindest in der Praxis wahrscheinlich ist. Die Realisierung einer Rückverfolgungsmöglichkeit ohne einen solchen Anspruch dürfte zwar im Interesse der Verwerter liegen, gleichwohl würde sie datenschutzrechtlich nur durch Transparenz und die Einwilligung des Kunden legal umzusetzen sein. Eine Legitimation auf Basis einer Rechtsvorschrift dagegen kommt nicht in Betracht, da sich die Verarbeitung gegenüber allen Kunden als nicht erforderlich und unverhältnismäßig darstellt.

Gesellschaftlich könnten kombinierte Formen von technischem DRM und Rückverfolgungsmöglichkeiten gemeinsam mit entsprechenden vertraglichen Regelungen und der zivilrechtlichen Durchsetzung (smöglichkeit) derselben zum Ende eines Gebrauchsmarktes für Musik- und andere Medieninhalte führen.

Aktuelle DRM-Systeme regeln den Konflikt zwischen der Wahrung der geistigen Eigentums- und Verwertungsrechte sowie den Nutzungsinteressen der Konsumenten nicht in ausgewogener Weise. Der derzeitige Lösungsansatz führt vielmehr zu einer Benachteiligung der ehrlichen Kunden, die geschützte digitale Inhalte erwerben. Einer solchen Lösung wird wirtschaftlich nur wenig Erfolg beschieden sein, wenn der Kunde eine einfache und zudem noch kostengünstigere Möglichkeit hat, der Benachteiligung auszuweichen (z. B. Download über „peer-to-peer“-Tauschbörsen). Die mögliche Illegalität solcher Lösungen stellt dabei kaum ein Hindernis dar, weil ein Unrechtsbewusstsein gegenüber geistigen Eigentumsverletzungen mangels eigener Erfahrung bei vielen Menschen weniger ausgeprägt ist. Außerdem scheint das Gefühl, als Kunde ungerecht von der Musikindustrie behandelt zu werden, ein solches Verhalten als Selbstschutz zu rechtfertigen. Aktuelle DRM-Systeme untergraben so nachhaltig das Nutzervertrauen in digitale Vertriebskanäle.

Ob der Zwang technischer Entwicklungen und der Marketingerfolg einzelner Anbieter das fehlende Nutzervertrauen in die Technik überlagern und in der Akzeptanzfrage positiv beeinflussen können, bleibt abzuwarten. Neue Systeme müssen den Nutzer und nicht das „Datenobjekt“ in das Zentrum ihrer Gestaltung rücken. Geistiger Eigentumsschutz wird z. B. dort für Nutzer attraktiv, wo er in ihrem eigenen Interesse stattfindet, weil sie z. B. finanziell an der Weiterverbreitung lizenzierter Inhalte partizipieren. Die Entwicklung dieser und anderer Formen eines echten Vorteils des lizenzierten Inhalts und damit eines gesteigerten Eigeninteresses des Kunden wird den Kern der Entwicklung neuer Formen von geistigem Eigentumsschutz für digitale Inhalte ausmachen müssen. Wer nur das geschützte Datenobjekt in seinem Nutzen einschränkt, reduziert das Eigeninteresse des Kunden an dem digitalen Inhalt.

Der Nutzer muss sich im Geschäftsmodell als Partner, nicht als Gegner des Künstlers / Verwerters verstehen. Neben der Akzeptanz des geistigen Eigentums durch den Nutzer sollten Mehrwerte ehrlichen Kunden und nicht den Nutzern illegaler Kopien zufließen. Solche Anreize sollten sich dabei möglichst nicht nur als Zugaben für Fans präsentieren, sondern einen tatsächlichen z. B. monetären Anreiz

bieten, mit dem dann die als für den Verkaufserfolg wichtig erachtete „Mundpropaganda“ des Nutzers in gewisser Weise entlohnt würde.

Ein partnerschaftliches Verhältnis, wie oben beschrieben, erfordert Kundenvertrauen in den Anbieter und die eingesetzte Technologie. Dieses sollte auch durch transparentes und die Rechte des Nutzers berücksichtigendes Verhalten „zurückgewonnen“ werden. Kommuniziert werden könnte dies gegenüber den Kunden z. B. durch Datenschutzgütesiegel für DRM-Produkte.<sup>7</sup> Das setzt jedoch voraus, dass Kundenrechte als wichtiger Bestandteil der Kundenbeziehung ernst genommen und systematisch beim Design der Angebote (dies betrifft sowohl die rechtlichen Rahmenbedingungen, das Design technischer Komponenten wie auch die Ausgestaltung von Mechanismen zum Rechtesschutz) berücksichtigt werden. Die Kommunikation einer solchen Ausrichtung kann mit datenschutzrechtlicher Transparenz und marktwirtschaftlichen Instrumenten (wie freiwilligen Gütesiegeln) stattfinden.

## 5 Ausblick

Für neue DRM-Strukturen wird eine Reihe weiterer Themenfelder genauerer Betrachtung bedürfen. Hierzu zählen unter anderem die Infrastrukturen und Verteilungsprotokolle – insbesondere auch die Verteilungsmodelle für Bildungsgüter (Bizer, Grimm, Will et al. 2005, S. 205 ff.). Neben traditionellen Vertriebssystemen für Online-Shopangebote existieren für andere Geschäftsumgebungen (wie Bibliotheken, Konferenzen und eLearning-Angebote) keine oder wenige vergleichbare Protokolle. Die Unterstützung vorhandener Institutionen und Vorbereitung neuer Dienstleistungsangebote werden im größeren Maßstab als bisher Aufgabe des Bildungsstandortes Deutschlands sein. Besondere Geschäftsfelder für Bildungsgüter bilden die Produktion und das Angebot an Lehrmaterial als Alternative / Ergänzung zum Lehrbuchverlagswesen sowie das Veröffentlichungswesen für Forschungsergebnisse. In allen angesprochenen Bereichen wird umfangreiche Forschungsarbeit geleistet werden müssen.

Für die erfolgreiche Einbettung in Geschäftsmodelle werden insbesondere ein ökonomisches Studium der Verteilmodelle, die Entwicklung neuer Konzepte für ein tragfähiges

ges (rechtliches) Risikomanagement und eine Analyse der Einsatzmöglichkeiten von Pseudonymitätskonzepten für weitere Forschungen empfohlen.

### Anmerkungen

- 1) Der Begriff „Compliance“ beschreibt die Einhaltung von Gesetzen und Richtlinien, aber auch freiwillige Kodices in Unternehmen.
- 2) Siehe <http://www.innovationsanalysen.de/de/ita.html>. Der Teilnahmewettbewerb „Innovationspotenziale der Informationstechnik“ war vom BMBF im Mai 2004 ausgeschrieben worden.
- 3) Ausführlichere Informationen zum Selbstschutz sind zu finden unter <http://www.datenschutzzentrum.de/selbstschutz/>.
- 4) Sehr instruktiv hierzu ist das Volkszählungsurteil des Bundesverfassungsgerichts (BVerfGE 65, S. 1 ff.).
- 5) Diese wird auch als „Apple-ID“ bezeichnet.
- 6) Das „PotatoSystem“ verwendet IDs z. B. in Dateinamen, die für den Nutzer offensichtlich sind und der Provisionsbeteiligung dienen (vgl. Nützel, Grimm 2005). Sie können vergleichsweise einfach entfernt werden. Allerdings entfällt dann die Möglichkeit der Provisionsbeteiligung (Bizer, Grimm, Will et al. 2005, S. 142 ff). Weitere alternative Distributionsmodelle sind beschrieben in Aichroth, Puchta, Hasselbach 2004.
- 7) Ausführlichere Informationen zu Datenschutzgütesiegeln unter <http://www.datenschutzzentrum.de/guetesiegel>.

### Literatur

Aichroth, P.; Hasselbach, J., 2003: Incentive Management for Virtual Goods: About Copyright and Creative Production in the Digital Domain; [http://virtualgoods.tu-ilmenau.de/2003/incentive\\_management.pdf](http://virtualgoods.tu-ilmenau.de/2003/incentive_management.pdf); download 30.4.2006

Aichroth, P.; Puchta, S.; Hasselbach, J., 2004: Personalized Previews: An Alternative Concept of Virtual Goods Marketing; [http://virtualgoods.tu-ilmenau.de/2004/personalized\\_previews.pdf](http://virtualgoods.tu-ilmenau.de/2004/personalized_previews.pdf); download 30.4.2006

Bizer, J.; Grimm, R.; Will, A. et al., 2005: Privacy4DRM – Datenschutzverträgliches und nutzungsfreundliches Digital Rights Management. Studie im Auftrag des Bundesministeriums für Bildung und Forschung (BMBF); [http://www.bmbf.de/pub/privacy4drm\\_studie.pdf](http://www.bmbf.de/pub/privacy4drm_studie.pdf); download 20.4.2006

Bizer, J.; Grimm, R.; Will, A., 2006: Privacy4DRM, Nutzer- und Datenschutzfreundliches Digital Rights Management. Datenschutz und Datensicherheit

2/2006, S. 69-73; <http://www.datenschutzzentrum.de/drm/kurzfassungen.htm>

Chip, 2006: The Superdistribution Times; <http://superdistributiontimes.blogspot.com>; download 20.4.2006

Grimm, R.; Puchta, S., 2006: Datenspuren bei der Nutzung von Digital Rights Management-Systemen (DRM). Datenschutz und Datensicherheit 2/2006, S. 74-79; <http://www.datenschutzzentrum.de/drm/kurzfassungen.htm>

Kawahara, M., 2006: The Superdistribution Resource Page; <http://sda.k.tsukuba-tech.ac.jp/SdA>; download 20.4.2006

Merrit, R.; Chin, S., 2006: CES: Gordischer Knoten Interoperabilität; <http://www.eetimes.de/at/news/showArticle.jhtml?articleID=175800635>; download 30.4.2006

Möller, J.; Bizer, J., 2006: Datenschutzerfordernungen an Digital Rights Management. Datenschutz und Datensicherheit 2/2006, S. 80-84; <http://www.datenschutzzentrum.de/drm/kurzfassungen.htm>

Nützel, J.; Grimm, R., 2005: Musikvertrieb mit Potato Web Services. Datenschutz und Datensicherheit 3/2005, S. 125-129

Secor, G., 2004: The Gilbane Report: Volume 12, Number 5, Compliance: Make „DRM“ A Part of the Solution; [http://gilbane.com/gilbane\\_report.pl/99/Compliance\\_Make\\_DRM\\_A\\_Part\\_of\\_the\\_Solution.html](http://gilbane.com/gilbane_report.pl/99/Compliance_Make_DRM_A_Part_of_the_Solution.html); download 20.4.2006

### Kontakt

Jan Möller  
 Unabhängiges Landeszentrum für Datenschutz  
 Schleswig-Holstein (ULD)  
 Holstenstr. 98, 24103 Kiel  
 E-Mail: [moeller@privacy-law.eu](mailto:moeller@privacy-law.eu)  
 Internet: <http://www.datenschutzzentrum.de>

Stefan Puchta  
 Fraunhofer-Institut für Digitale Medientechnologie  
 (IDMT)  
 Ernst-Abbe-Zentrum  
 Ehrenbergstraße 29, 98693 Ilmenau  
 E-Mail: [stefan.puchta@idmt.fraunhofer.de](mailto:stefan.puchta@idmt.fraunhofer.de)  
 Internet: <http://www.idmt.fraunhofer.de>

«