Information und Recht

Band 33

Schriftenreihe
Information und Recht

Herausgegeben von
Prof. Dr. Thomas Hoeren
Prof. Dr. Gerald Spindler
Prof. Dr. Bernd Holznagel, LL.M.
Prof. Dr. Georgios Gounalakis
PD Dr. Herbert Burkert

Band 33

Verlag C.H. Beck München 2002

Vom Urheber- zum Informationsrecht

Implikationen des Digital Rights Management

von
Dr. jur. Stefan Bechtold

Verlag C.H. Beck München 2002

ISBN 3 406 48717 3

Druck: Nomos Verlagsgesellschaft
In den Lissen 12, 76547 Sinzheim

Gedruckt auf säurefreiem, alterungsbeständigem Papier
(hergestellt aus chlorfrei gebleichtem Zellstoff)

We shape our tools,
and thereafter our tools shape us.

Marshall McLuhan,
Understanding Media, 1964

Vorwort

Die vorliegende Arbeit ist zwischen Oktober 1999 und Juni 2001 entstanden und wurde im Sommersemester 2001 von der Juristischen Fakultät der Eberhard-Karls-Universität Tübingen als Dissertation angenommen. Bei der Untersuchung der neuen EU-Richtlinie zum Urheberrecht in der Informationsgesellschaft legt die Arbeit die endgültige, Ende Juni 2001 im Amtsblatt veröffentlichte Fassung zugrunde.

Mein besonderer Dank gilt meinem verehrten Doktorvater, Herrn Prof. Dr. *Wernhard Möschel*. Er hat meinen Blick für ordnungspolitische Grundprobleme und übergreifende Fragestellungen geschärft und mir als Mitarbeiter an seinem Lehrstuhl große Freiräume und optimale Arbeitsbedingungen gewährt. Für die vorliegende Arbeit hat er mich immer ermutigt, einmal eingeschlagene Pfade konsequent zu beschreiten und vor ungewohnten Analyseansätzen und Ergebnissen nicht zurückzuschrecken. Ohne diese Rahmenbedingungen wäre die Arbeit in der vorliegenden Form niemals entstanden. Ihm und Herrn Prof. Dr. *Ulrich Bälz* danke ich weiterhin für die überaus sachkundige Erstellung der beiden Gutachten. Herrn Prof. Dr. *Thomas Hoeren* danke ich für die Aufnahme der Arbeit in die vorliegende Schriftenreihe. Der Arbeitskreis Wirtschaft und Recht im Stifterverband für die Deutsche Wissenschaft hat die Erstellung dieser Arbeit durch ein Promotionsstipendium und einen Druckkostenzuschuß großzügig unterstützt, wofür ich mich stellvertretend beim Vorsitzenden, Herrn Prof. Dr. *Harm Peter Westermann*, herzlich bedanke.

Zahllose wichtige Anregungen habe ich während zweier Forschungsaufenthalte erhalten, die ich von Oktober bis Dezember 1999 sowie von März bis Mai 2000 als „Visiting Scholar" an der Law School der University of California at Berkeley verbringen konnte. Neben traumhaften Arbeitsbedingungen und einer beeindruckenden Bibliotheksausstattung habe ich insbesondere von zahlreichen Gesprächen sehr profitiert. Diesbezüglich gilt mein herzlicher Dank den Damen und Herren Professoren *Pamela Samuelson*, *Robert P. Merges* und *Mark A. Lemley*. Mein ganz besonderer Dank gilt ferner Professor *Lawrence Lessig*, von dem ich nicht nur durch seine Schriften, sondern auch durch mehrere Gespräche außerordentlich viel gelernt habe.

Die Erstellung des ausführlichen technischen Teils dieser Arbeit wäre unmöglich gewesen, wenn sich nicht intensive Kontakte zu Technikern ergeben hätten, die im „Digital Rights Management" oder verwandten Bereichen tätig sind. Mein besonderer Dank gilt den Herren Dr. rer. nat.

Tomas Sander (InterTrust Technologies Corp., Santa Clara, USA), Dr.-Ing. *Hannes Federrath* (Technische Universität Dresden) und Dipl.-Inf. *Niels Rump* (Rightscom Ltd., London). Sie haben mir – mit einem weit über das Übliche hinausreichenden Einsatz – nicht nur zahlreiche Literaturhinweise gegeben, sondern in vielen Gesprächen mit bewundernswerter Geduld meine zahllosen technischen Fragen beantwortet. Zusätzlich haben sie jeweils umfangreiche Abschnitte des technischen Teils dieser Arbeit sorgfältig durchgeschaut und mich auf inhaltliche Fehler hingewiesen.

Weiterhin möchte ich Herrn Dr. *Albrecht Haller* und Herrn *Kamiel Koelman* danken, die für mich seit langem im Urheberrecht zu wichtigen Gesprächspartnern geworden sind und mir für die Arbeit viele Informationen und Anregungen gegeben haben. Herrn Dr. *Michael Paulweber*, LL.M. (Berkeley), danke ich für viele Gespräche und Anregungen in unterschiedlichen Stadien der Arbeit. Herr Prof. Dr. *Christoph Engel* versorgte mich dankenswerterweise monatelang per E-Mail mit unzähligen interessanten Literaturhinweisen.

Ganz herzlich bedanken möchte ich mich bei meinem Lehrstuhlkollegen Herrn *Florian Wagner* für zahllose Diskussionen und Anregungen zu fast allen Aspekten der Arbeit sowie für die sorgfältige Durchsicht des Manuskripts. Ebenfalls Dank gebührt meinem Kollegen Herrn Dr. *Markus Müller* für viele Gespräche zu den rechtsökonomischen Aspekten der Arbeit. Mein Dank gilt auch Herrn Dr. *Patrick Mayer*, der tragischerweise vor kurzem viel zu früh verstorben ist. Wie wenige Internetrechtler vereinte er juristische Fachkompetenz mit Detailkenntnissen der technischen Grundlagen des Netzes sowie der Hacker-Kultur. Darin war er mir immer ein Vorbild gewesen.

Schließlich hat eine Arbeit, die sich mit Rechtsfragen des Internets auseinandersetzt, auch vielen Nutzern des Internets zu danken. Ich habe auf den Mailinglisten Cyberia-L, CNI-Copyright, DVD-Discuss, Fitug-Debate, Netlaw-L und Politech, auf der Community-Seite Slashdot, auf *John Young*'s Cryptome.org sowie von der Electronic Frontier Foundation unzählige Anregungen, Ideen, Informationen und Dokumente erhalten, von denen die vorliegende Arbeit wesentlich profitiert hat.

Der größte Dank gebührt jedoch meinen Eltern, die mich in den unterschiedlichen Phasen meiner Ausbildung, bei der Erstellung dieser Arbeit und bei meinen sonstigen Interessen stets in jeder Hinsicht unterstützt und gefördert haben. Beiden danke ich auch für die sorgfältige Durchsicht des Manuskripts. Ihnen ist die Arbeit gewidmet.

Allen Genannten verdankt die vorliegende Arbeit viel. Hingegen sind alle Fehler und Ungenauigkeiten von mir allein zu vertreten.

Tübingen, im August 2001 *Stefan Bechtold*

Inhaltsübersicht

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

Neben den üblichen juristischen Abkürzungen verwendet die vorliegende Arbeit spezielle Abkürzungen, die im folgenden aufgeführt werden.

ACM	Association for Computing Machinery
AGICOA	Association de Gestion Internationale Collective des Œuvres Audiovisuelles
AHRA	Audio Home Recording Act
ALI	American Law Institute
Am. Jur. 2d	American Jurisprudence (Second)
ANSI	American National Standards Institute
API	Application Programming Interface
CAE	Compositeur, Auteur, Editeur
CGMS	Copy Generation Management System
CIS	Common Information System
CISAC	Confédération Internationale des Sociétés d'Auteurs et Compositeurs
CMMV	Clearingstelle Multimedia für Verwertungsgesellschaften von Urheber- und Leistungsschutzrechten
Comm. ACM	Communications of the ACM
COREPER	Comité des Représentants Permanents
CPPM	Content Protection for Pre-Recorded Media
CPRM	Content Protection for Recordable Media
CPSA	Content Protection System Architecture
CPTWG	Copy Protection Technical Working Group
CSS	Content Scramble System
DHCP	Dynamic Host Configuration Protocol
DMCA	Digital Millennium Copyright Act
DOI	Digital Object Identifier
DPRL	Digital Property Rights Language
DRM	Digital Rights Management
DTCP	Digital Transmission Content Protection
DTD	Document Type Definition
DVB	Digital Video Broadcasting
DVD	Digital Versatile Disc
DVD CCA	DVD Copy Control Association, Inc.
EBX	Electronic Book Exchange
ECM	Entitlement Control Message
EDI	Electronic Data Interchange
EEPROM	Electrically Erasable Programmable Read-Only Memory
EFF	Electronic Frontier Foundation
EMM	Entitlement Management Message
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FernAbsG	Fernabsatzgesetz
FIAPF	Fédération Internationale des Associations de Producteurs de Films

FIPA	Foundation for Intelligent Physical Agents
FÜG	Fernsehsignalübertragungs-Gesetz
Gema	Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte
GÜFA	Gesellschaft zur Übernahme und Wahrung von Filmaufführungsrechten
GVL	Gesellschaft zur Verwertung von Leistungsschutzrechten
GVO	Gruppenfreistellungsverordnung
GWFF	Gesellschaft zur Wahrnehmung von Film- und Fernsehrechten
HDCP	High-bandwidth Digital Content Protection System
HDTV	High-Definition Television
HTML	Hypertext Markup Language
IETF	Internet Engineering Task Force
IFPI	International Federation of the Phonographic Industry
IOTP	Internet Open Trading Protocol
IP	Internet Protocol
IPMP	Intellectual Property Management & Protection
ISBN	International Standard Book Number
ISO	International Orgnization for Standardization
ISP	Internet Service Provider
ISRC	International Standard Recording Number
ISSN	International Standard Serial Number
ISWC	International Standard Work Code
MAC	Media Access Control Message Authentication Code
MMP	Multimedia Protection Protocol
MMRCS	Multimedia Rights Clearance System
MP3	MPEG-1 Audio Layer III
MPAA	Motion Picture Association of America
MPEG	Moving Pictures Expert Grouop
MR	Medien und Recht
NAFTA	North American Free Trade Agreement
NCCUSL	National Conference of Commissioners for Uniform Laws
NISO	National Information Standards Organization
OASIS	Organization for the Advancement of Structured Information Standards
ODRL	Open Digital Rights Language
OEB	Open eBook Forum
OPIMA	Open Platform Initiative for Multimedia Access
P2P	Peer-to-Peer
P3P	Platform for Privacy Preferences Project
PCI	Peripheral Component Interconnect
PCMCIA	Personal Computer Memory Card International Association
PET	Privacy-Enhancing Technology
PICS	Platform for Internet Content Selection
PIN	Personal Identification Number
PKI	Public Key Infrastructure
Proc. IEEE	Proceedings of the IEEE
RAM	Random Access Memory
RBÜ	Revidierte Berner Übereinkunft
RDF	Resource Description Framework
RFC	Request for Comments
RIAA	Recording Industry Association of America

RID	Recorder Identification Code
RPS	Rights Protection System
SCMS	Serial Copy Management System
SDMI	Secure Digital Music Initiative
SET	Secure Electronic Transaction
SID	Source Identification Code
SMPTE	Society of Motion Picture and Television Engineers
TCPA	Trusted Computing Platform Alliance
TDG	Teledienstegesetz
UCC	Uniform Commercial Code
UCITA	Uniform Computer Information Transactions Act
UDRP	Uniform Dispute Resolution Policy
UETA	Uniform Electronic Transactions Act
UN/CEFACT	United Nations Centre for the Facilitation of Procedures and Practices for Administration, Commerce and Transport
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UTSA	Uniform Trade Secret Act
VERDI	Very Extensive Rights Data Information
VFF	Verwertungsgesellschaft der Film- und Fernsehproduzenten
VG Bild-Kunst	Verwertungsgesellschaft Bild-Kunst
VG Wort	Verwertungsgesellschaft Wort
VGF	Verwertungsgesellschaft für Nutzungsrechte an Filmwerken
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WCT	WIPO Copyright Treaty
WIPO	World Intellectual Property Organization
WL	Westlaw
WPPT	WIPO Performances and Phonograms Treaty
WWW	World Wide Web
Xerox PARC	Xerox Palo Alto Research Center
XML	eXtensible Markup Language
XrML	eXtensible rights Markup Language

Literaturverzeichnis

Dokumente, die nur im Internet erhältlich sind, werden unter Verwendung von Seitenzahlen zitiert, sofern das Dokument selbst Seitenzahlen enthält. Ist dies nicht der Fall, so wird nach Abschnitten oder Absätzen zitiert. Fehlen in dem Dokument auch Abschnitte oder Absätze, wird es mit den Seitenzahlen zitiert, die sich beim Ausdruck mit einem handelsüblichen Drucker ergeben. Die Zitierung U.S.-amerikanischer rechtswissenschaftlicher Literatur orientiert sich am Blue Book, A Uniform System of Citation, 17. Auflage, Cambridge 2000.

Abdalla, Michel/Shavitt, Yuval/Wool, Avishai, Towards Making Broadcast Encryption Practical. In: Franklin (Hrsg.), Financial Cryptography. Third International Conference. 22.–25. 2. 1999, Anguilla, British West Indies – Proceedings. Berlin, 1999. S. 140 ff.

Abrams, Howard B., Copyright, Misappropriation, and Preemption: Constitutional and Statutory Limits. 11 Supreme Court Review 509 ff. (1983)

Adams, Carlisle/Cain, Pat/Pinkas, Denis/Zuccherato, Robert, Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP). Internet Draft (work in progress), aft-ietf-pkix-time-stamp-13.txt, Januar 2001. <http://www.watersprings.org/pub/id/draft-ietf-pkix-time-stamp-13.txt>

Adams, Michael, Ökonomische Analyse des Gesetzes zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen (AGB-Gesetz). In: Neumann (Hrsg.): Ansprüche, Eigentums- und Verfügungsrechte. Berlin, 1984. S. 655 ff.

ders., Ökonomische Begründung des AGB-Gesetzes. Verträge bei asymmetrischer Information. Betriebsberater 1989, 781 ff.

Ahrens, Claus, Napster, Gnutella, FreeNet & Co. – die immaterialgüterrechtliche Beurteilung von Internet-Musiktauschbörsen. Zeitschrift für Urheber- und Medienrecht 2000, 1029 ff

Ahronheim, Judith R., Descriptive Metadata: Emerging Standards. 24 The Journal of Academic Librarianship 395 ff. (1998)

Akerlof, George A., The Market for Lemons: Qualitative Uncertainty and the Market Mechanism. 84 Quarterly Journal of Economics 488 ff. (1970)

Allemann, Alex, Manifestation of an AHRA Malfunction: The Uncertain Status of MP3 Under Recording Industry Association of America v. Diamond Multimedia Systems, Inc. 79 Texas Law Review 189 ff. (2000)

Allen, Tom/Widdison, Robin, Can Computers Make Contracts? 9 Harvard Journal of Law & Technology 25 ff. (1996)

Altin-Sieber, Inci, Joint Ventures, Technologietransfer und sschutz. Heidelberg, 1996

Anderson, Ross J. , Security Engineering – A Guide to Building Dependable Distributed Systems. New York, 2001

Anderson, Ross J./Kuhn, Markus G., Low Cost Attacks on Tamper Resistant Devices. In: Christianson/Crispo/Lomas/Roe (Hrsg.), Security Protocols. 5th International Workshop on Security Protocols. 7.–9. 4. 1997, Paris. Berlin, 1998. S. 125 ff.

dies., Tamper Resistance – a Cautionary Note. In: Proceedings of the Second USENIX Workshop on Electronic Commerce. 18.–21. 11. 1996, Oakland, USA. S. 1 ff.

Anderson, Ross J./Petitcolas, Fabien A. P., On the Limits of Steganography. 16 (4) IEEE Journal of Selected Areas in Communications 474 ff. (1998)

Arlein, Robert M./Jai, Ben/Jakobsson, Markus/Monrose, Fabian/Reiter, Michael K., Privacy-Preserving Global Customization. In: Proceedings of the 2nd ACM Conference on Electronic Commerce. 17.–20. 10. 2000, Minneapolis, USA. New York, 2000. S. 176 ff.

Asokan, N./Schunter, Matthias/Waidner, Michael, Optimistic Protocols for Fair Exchange. IBM Research Report RZ 2858 (#90806). Zürich, 1996. Erhältlich unter <http://www.zurich.ibm.com/pub/cca/infosec/publications/1996/ASW96.ps.gz>

Association of American Publishers, Inc., Digital Rights Management for Ebooks: Publisher Requirements. Version 1.0; 27. 11. 2000. <http://www.publishers.org/home/drm.pdf>

dies., Metadata Standards for Ebooks. Version 1.0; 27. 11. 2000. <http://www.publishers.org/home/metadata.pdf>

dies., Numbering Standards for Ebooks. Version 1.0; 27. 11. 2000. <http://www.publishers.org/home/numbering.pdf>

Aucsmith, David, Tamper Resistant Software: An Implementation. In: Anderson (Hrsg.), Information Hiding – First International Workshop. 30. 5. – 1. 6. 1996, Cambridge, UK. Berlin, 1996. S. 317 ff.

Augot, Daniel/Boucqueau, Jean-Marc/Delaigle, Jean-François/Fontaine, Caroline/Goray, Eddy, Secure Delivery of Images over Open Networks. 87 Proceedings of the IEEE 1251 ff. (1999)

Aura, Tuomas, Practical Invisibility in Digital Communication. In: Anderson (Hrsg.), Information Hiding – First International Workshop. 30.5.–1.6. 1996, Cambridge, UK. Berlin, 1996. S. 265 ff.

Ayres, Ian/Talley, Eric, Solomonic Bargaining: Dividing a Legal Entitlement To Facilitate Coasean Trade. 104 Yale Law Journal 1027 ff. (1995)

Baca, Murtha (Hrsg.), Introduction to Metadata – Pathways to Digital Information. Getty Information Institute, 1998

Bailey, Joseph P., Intermediation and Electronic Markets: Aggregation and Pricing in Internet Commerce. Ph.D. dissertation, Massachusetts Institute of Technology, Mai 1998. Online erhältlich unter <http://www.rhsmith.umd.edu/tbpp/jbailey/pub/phdthesis.pdf>

Baker, Darren C., ProCD v. Zeidenberg: Commercial Reality, Flexibility in Contract Formation, And Notions of Manifested Assent in the Arena of Shrinkwrap Licenses. 92 Northwestern University Law Review 379 ff. (1997)

Bakos, Yannis, The Emerging Role of Electronic Marketplaces on the Internet. 41 (8) Communications of the ACM 35 ff. (August 1998)

Bakos, Yannis/Brynjolfsson, Erik, Aggregation and Disaggregation of Information Goods: Implications for Bundling, Site Licensing, and Micropayment Systems. In: Kahin/Varian (Hrsg.), Internet Publishing and Beyond. The Economics of Digital Information and Intellectual Property. Cambridge, 2000. S. 114 ff.

Baldonado, Michelle/Chang, Chen-Chuan K./Gravano, Luis/Paepcke, Andreas, The Stanford Digital Library Metadata Architecture. 1 International Journal on Digital Libraries 108 ff. (1997)

Balenson, David/McGrew, David A./Sherman, Alan T., Key Management for Large Dynamic Groups: One-Way Function Trees and Amortized Initialization. Internet-Draft (work in progress), <draft-irtf-smug-groupkeymagmt-oft-00.txt>, 25. 8. 2000. <http://www.watersprings.org/pub/id/draft-irtf-smug-groupkeymgmt-oft-00.txt>

Ballardie, Tony, Scalable Multicast Key Distribution. Request for Comments 1949, Mai 1996. <http://www.rfc-editor.org/rfc/rfc1949.txt>

Band, Jonathan, The Digital Millenium Copyright Act: A Balanced Result. European Intellectual Property Review 1999, 92 ff.

Barlas, Chris, The IMRPIMATUR Project. In: Brunnstein/Sint (Hrsg.), Intellectual Property Rights and New Technologies. Proceedings of the KnowRight '95 Conference. 21.–25. 8. 1995, Wien. Wien, 1995. S. 264 ff.

Barlow, John Perry, A Declaration of the Independence of Cyberspace. 8. 2. 1996. <http://www.eff. org/~barlow/Declaration-Final.html>

ders., The Economy of Ideas. A Framework for Rethinking Patents and Copyrights in the Digital Age (Everything you know about intellectual property is wrong). Wired 2.03, S. 84-86, 88-90, 126-129 (März 1994). Online erhältlich unter <http://www.wired.com/wired/archive/2.03/economy.ideas.html>

ders., The Next Economy of Ideas. Will Copyright Survive the Napster Bomb? Nope, But Creativity Will. Wired 8.10, S. 240-242, 252 (Oktober 2000). Online erhältlich unter <http://www.wired.com/wired/archive/8.10/download.html>

Bartolini, Franco/Bini, G./Cappellini, Vito/Fringuelli, A./Meucci, G./Piva, Alessandro/Barni, Mauro, Enforcement of Copyright Laws for Multimedia through Blind, Detectable, Reversible Watermarking. In: Proceedings of the IEEE International Conference on Multimedia Computing & Systems (ICMCS). 7.–11. 6. 1999, Florenz. Los Alamitos, 1999. Band 2, S. 199 ff.

Bartolini, Franco/Cappellini, Vito/Piva, Alessandro/Fringuelli, A./Barni, Mauro, Electronic Copyright Management Systems: Requirements, Players and Technologies. In: Cammelli/Tjoa/Wagner (Hrsg.), Tenth International Workshop on Database and Expert Systems Applications (DEXA 1999). 1.–3. 9. 1999, Florenz – Proceedings. Los Alamitos, 1999. S. 896 ff.

Basho, Kalinda, The Licensing of Our Personal Information: Is It a Solution to Internet Privacy? 88 California Law Review 1507 ff. (2000)

Bauer, Friedrich L., Entzifferte Geheimnisse – Methoden und Maximen der Kryptologie, 2. Auflage, Berlin 1997

Baur, Jürgen F./Stürner, Rolf, Sachenrecht. 17. Auflage, München 1999

Baylin, Frank/McCormac, John/Maddox, Richard, World Satellite TV and Scrambling Methods. The Technicians' Handbook. 3. Auflage, 1993

Bearman, David/Miller, Eric/Rust, Godfrey/Trant, Jennifer/Weibel, Stuart W., A Common Model to Support Interoperable Metadata – Progress Report on Reconciling Metadata Requirements From the Dublin Core and INDECS/DOI Communities. 5 (1) D-Lib (Januar 1999), erhältlich unter <http://www.dlib.org/dlib/january99/bearman/01bearman.html>

Bechtold, Rainer, Anmerkung zu EuGH EuZW 1995, 339 – Magill. Zeitschrift für Europäisches Wirtschaftsrecht 1995, 345 ff.

Bechtold, Stefan, Der Schutz des Anbieters von Information – Urheberrecht und Gewerblicher Rechtsschutz im Internet. Zeitschrift für Urheber- und Medienrecht 1997, 427 ff.

ders., Multimedia und das Urheberrecht, 1997. Erhältlich unter <http://www.jura.uni-tuebingen.de/~s-bes1/sem97/bechtold.pdf>

ders., Multimedia und Urheberrecht – einige grundsätzliche Anmerkungen. GRUR 1998, 18 ff.

ders., Schutz und Identifizierung durch technische Maßnahmen. In: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht. München. Stand: 2. Ergänzungslieferung, Dezember 2000. Teil 7.11

ders., The Link Controversy Page, 1997-2001. <http://www.jura.uni-tuebingen.de/~s-bes1/lcp.html>

ders., USA: Der Kampf um das Urheberrecht im Internet. Multimedia und Recht Heft 9/2000, S. XXI-XXII (MMR aktuell)

Beese, Dietrich/Merkt, Jutta, Europäische Union zwischen Konvergenz und Re-Regulierung. Die neuen Richtlinienentwürfe der Kommission. Multimedia und Recht 2000, 532 ff.

Behrens, Peter, Die ökonomischen Grundlagen des Rechts. Politische Ökonomie als rationale Jurisprudenz. Tübingen, 1986

Bell, Tom W., Escape from Copyright: Market Success vs. Statutory Failure in the Protection of Expressive Works. Unveröffentlichtes Manuskript vom 29. 3. 2001. Erscheint in 69 University of Cincinatti Law Review 741 ff. (2001)

ders., Fair Use vs. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine. 76 North Carolina Law Review 557 ff. (1998)

Benkler, Yochai, An Unhurried View of Private Ordering Information Transactions. 53 Vanderbilt Law Review 2063 ff. (2000)

ders., Constitutional Bounds of Database Protection: The Role of Judicial Review in the Creation and Definition of Private Rights in Information. 15 Berkeley Technology Law Journal 535 ff. (2000)

ders., Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain. 74 New York University Law Review 354 ff. (1999)

ders., Net Regulation: Taking Stock and Looking Forward. 71 University of Colorado Law Review 1203 ff. (2000)

ders., Overcoming Agoraphobia: Building the Commons of the Digitally Networked Environment. 11 Harvard Journal of Law & Technology 287 ff. (1998)

Benkler, Yochai (Hrsg.), Digital Video Panel. 11 Fordham Intellectual Property Media and Entertainment Law Journal 317 ff. (2001)

Bergh, Roger van den, The Role and Social Justification of Copyright: A „Law and Economics" Approach. Intellectual Property Quarterly 1998, 17 ff.

Berman, Paul Schiff, Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to „Private" Regulation. 71 University of Colorado Law Review 1263 ff. (2000)

Berners-Lee, Tim, Universal Resource Identifiers in WWW – A Unifying Syntax for the Expression of Names and Addresses of Objekts on the Network as used in the World-Wide Web. Request for Comments 1630, Juni 1994. <http://www.rfc-editor.org/rfc/rfc1630.txt>

Berners-Lee, Tim/Fielding, Roy T./Masinter, Larry, Uniform Resource Identifiers (URI): Generic Syntax. Request for Comments 2396, August 1998. <http://www.rfc-editor.org/rfc/rfc2396.txt>

Berschadsky, Ariel, RIAA v. Napster: A Window Onto the Future of Copyright Law in the Internet Age. 18 John Marshall Journal Computer & Information Law 755 ff. (2000)

Besen, Stanley M./Kirby, Sheila N./Salop, Steven C., An Economic Analysis of Copyright Collectives. 78 Virginia Law Review 383 ff. (1992)

Bettinger, Torsten, ICANN's Uniform Domain Name Dispute Resolution Policy. Neue außergerichtliche Konfliktlösungsverfahren im Kampf gegen mißbräuchliche Domainregistrierungen. Computer und Recht 2000, 234 ff.

Beucher, Klaus/Engels, Stefan, Harmonisierung des Rechtsschutzes verschlüsselter Pay-TV-Dienste gegen Piraterieakte. Computer und Recht 1998, 101 ff.

Beucher, Klaus/Leyendecker, Ludwig/Rosenberg, Oliver von, Mediengesetze – Rundfunk, Mediendienste, Teledienste. Kommentar zum Rundfunkstaatsvertrag, Mediendienste-Staatsvertrag, Teledienstegesetz und Teledienstedatenschutzgesetz. München, 1999

Bing, Jon, The Contribution of Technology to the Identification of Rights, Especially in Sound and Audio-Visual Works: An Overview. 4 International Journal of Law and Information Technology 234 ff. (1996)

Blinov, Mikhail/Bessonov, Mikhail/Clissman, Ciaran, Architecture for Information Brokerage in the ACTS Project GAIA. Request for Comments 2552, April 1999. <http://www.rfc-editor.org/rfc/rfc2552.txt>

Bloom, Jeffrey A./Cox, Ingemar J./Kalker, Ton/Linnartz, Jean-Paul M. G./Miller, Matthew/Traw, C./Brendran, S., Copy Protection for DVD Video. 87 Proceedings of the IEEE 1267 ff. (1999)

Bodewig, Theo, USA – Urhebervertragsrecht in ausgewählten Ländern. In: Beier/Götting/Lehmann/Moufang (Hrsg.), Urhebervertragsrecht. Festgabe für Gerhard Schricker zum 60. Geburtstag. München, 1995. S. 833 ff.

Bögeholz, Harald, Datentresor. Hardware-Kopierschutz für Festplatten. c't Heft 2/2001, S. 24 f.

Bohorquez, Fernando A., The Price of PICS: The Privatization of Internet Censorship. 43 New York Law School Law Review 523 ff. (1999)

Bone, Robert G., A New Look at Trade Secret Law: Doctrine in Search of Justification. 86 California Law Review 241 ff. (1998)

Boneh, Dan/Franklin, Matt, An Efficient Public Key Traitor Tracing Scheme. In: Wiener (Hrsg.), Advances in Cryptology – Crypto 1999. 19th Annual International Cryptology Conference. 15.–19. 8. 1999, Santa Barbara, USA – Proceedings. Berlin, 1999. S. 338 ff.

Boneh, Dan/Shaw, James, Collusion-Secure Fingerprinting for Digital Data. In: Coppersmith (Hrsg.), Advances in Cryptology – Crypto 1995. 15th Annual International Cryptology Conference. 27.–31. 8. 1995, Santa Barbara, USA – Proceedings. Berlin, 1995. S. 452 ff.

Bonus, Holger, Öffentliche Güter und Gefangenendilemma. In: Dettling (Hrsg.): Die Zähmung des Leviathan. Neue Wege der Ordnungspolitik. Baden-Baden, 1980. S. 129 ff.

Borrmann, Jörg/Finsinger, Jörg, Markt und Regulierung. München, 1999

Bortloff, Nils, Erfahrungen mit der Bekämpfung der elektronischen Musikpiraterie im Internet. GRUR Int. 2000, 665 ff.

Bott, Cynthia M., Protection of Information Products: Balancing Commercial Reality and the Public Domain. 67 University of Cincinnati Law Review 237 ff. (1998)

Boyle, James, Cruel, Mean, or Lavish? Economic Analysis, Price Discrimination and Digital Intellectual Property. 53 Vanderbilt Law Review 2007 ff. (2000)

Brand, Stewart, The Media Lab. Inventing the Future at MIT. New York, 1988

Brands, Stefan A., Rethinking Public Key Infrastructures and Digital Certificates. Building in Privacy. Cambridge, 2001

Brassil, Jack T./Low, Steven/Maxemchuk, Nicholas F., Copyright Protection for the Electronic Distribution of Text Documents. 87 Proceedings of the IEEE 1181 ff. (1999)

Brassil, Jack T./Low, Steven/Maxemchuk, Nicolas F./O'Gorman, Lawrence, Electronic Marking and Identification Techniques to Discourage Document Copying. 13 IEEE Journal on Selected Areas in Communications 1495 ff. (1995)

Breitbach, Markus/Imai, Hideki, On Channel Capacity and Modulation of Watermarks in Digital Still Images. In: Franklin (Hrsg.), Financial Cryptography. Third International Conference, 22.–25. 3. 1999, Anguilla, British West Indies – Proceedings. Berlin, 1999. S. 125 ff.

Brenn, Christoph, Richtlinie über Informations- und Kommunikationsdienste mit Zugangskontrolle und Überlegungen zur innerstaatlichen Umsetzung. Österreichische Juristen-Zeitung 1999, 81 ff.

Brennan, Lorin, The Public Policy of Information Licensing. 36 Houston Law Review 61 ff. (1999)

dies., Through the Telescope: „UCITA" and the Future of E-Commerce. 20 Mississippi College Law Review 27 ff. (1999)

Brenner, Walter/Zarnekow, Rüdiger/Wittig, Hartmut, Intelligente Softwareagenten. Grundlagen und Anwendungen. Berlin, 1998

Breyer, Stephen, The Uneasy Case for Copyright: A Study of Copyright in Books, Photocopies, and Computer Programs. 84 Harvard Law Review 281 ff. (1970)

Brickley, Dan/Guha, R. V., Resource Description Framework (RDF) Schema Specification 1.0. W3C Candidate Recommendation, 27. 3. 2000. <http://www.w3.org/TR/2000/CR-rdf-schema>

Briem, Stephan L., Tagung der Technischen Kommission der CISAC in London (13.–14. 10. 1997). Medien und Recht 1997, 260 ff.

Bröchler, Stephan/Simonis, Georg/Sundermann, Karsten (Hrsg.), Handbuch Technikfolgenabschätzung. 3 Bände. Berlin, 1999

Bröcker, Klaus T./Neun, Andreas, Fußballweltmeisterschaft zwingend im Free-TV? Rechtsprobleme der gesetzlichen Gewährleistung uneingeschränkter Fernsehempfangbarkeit von bestimmten Ereignissen mit erheblicher gesellschaftlicher Bedeutung. Zeitschrift für Urheber und Medienrecht 1998, 766 ff.

Bruin, Ronald de, Conditional Access. In: de Bruin/Smits (Hrsg.), Digital Video Broadcasting. Technology, Standards, and Regulations. Norwood, 1999. S. 203 ff.

Brynjolfsson, Erik/Smith, Michael D., Frictionless Commerce? A Comparison of Internet and Conventional Retailers. 46 Management Science 563 ff. (2000)

Bundesamt für Sicherheit in der Informationstechnik , Sicherheitsaspekte beim Electronic Commerce. Schriftenreihe zur IT-Sicherheit, Band 10. Bonn, 1999

Burdett, David, Internet Open Trading Protocol – IOTP Version 1.0. Request for Comments 2801, April 2000. <http://www.rfc-editor.org/rfc/rfc2801.txt>

Burdett, David/Eastlake, Donald E./Goncalves, Marcus, Internet Open Trading Protocol. New York, 2000

Burk, Dan L., Muddy Rules for Cyberspace. 21 Cardozo Law Review 121 ff. (1999)

ders., The Trouble With Trespass. 4 Journal of Small and Emerging Business Law 27 ff. (2000)

ders., Virtual Exit in the Global Information Economy. 73 Chicago-Kent Law Review 943 ff. (1998)

Burk, Dan L./Cohen, Julie E., Fair Use Infrastructure for Copyright Management Systems. Erscheint in 11 Harvard Journal of Law & Technology (2002). Entwurf vom 18. 8. 2000 erhältlich unter <http://papers.ssrn.com/abstract=239731>

Burkert, Herbert, Privacy-Enhancing Technologies: Typology, Critique, Vision. In: Agre/Rotenberg (Hrsg.), Technology and Privacy: The New Landscape. Cambridge, 1998. S. 125 ff.

Burnett, Kathleen/Bor Ng, Kwong/Park, Soyeon, A Comparison of the Two Traditions of Metadata Development. 50 Journal of the American Society for Information Science 1209 ff. (1999)

Bush, Vannevar, As We May Think. 176 (1) The Atlantic Monthly 101 ff. (1945). Online erhältlich unter <http://www.theatlantic.com/unbound/flashbks/computer/bushf.htm>

Bydlinski, Peter, Der Sachbegriff im elektronischen Zeitalter: zeitlos oder anpassungsbedürftig? Archiv für die civilistische Praxis 198 (1998), 287 ff.

Bygrave, Lee A./Koelman, Kamiel J., Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems. In: Hugenholtz (Hrsg)., Copyright and Electronic Commerce. London, 2000. S. 59 ff.

Calabresi, Guido/Melamed, A. Douglas, Property Rules, Liability Rules, and Inalienability: One View of the Cathedral. 85 Harvard Law Review 1089 ff. (1972)

Camenisch, Jan, Efficient Anonymous Fingerprinting with Group Signatures. In: Okamoto (Hrs.g), Advances in Cryptology – ASIACRYPT 2000. 6th International Conference on the Theory and Application of Cryptology and Information Security. 3.–7. 12. 2000, Kyoto, Japan – Proceedings. Berlin, 2000. S. 415 ff.

Canaris, Claus-Wilhelm, Die Verdinglichung obligatorischer Rechte. In: Jakobs/Knobbe-Keuk/Picker/Wilhelm (Hrsg.), Festschrift für Werner Flume zum 70. Geburtstag am 12. 9. 1978. Köln, 1978. Band I, S. 371 ff.

Canetti, Ran/Malkin, Tal/Nissim, Kobbi, Efficient Communication-Storage Tradeoffs for Multicast Encryption. In: Stern (Hrsg.), Advances in Cryptology – Eurocrypt 1999. International Conference on the Theory and Application of Cryptographic Techniques. 2.–6. 5. 1999, Prag – Proceedings. Berlin, 1999. S. 459 ff.

Canetti, Ran/Pinkas, Benny, A Taxonomy of Multicast Security Issues (updated version). Internet-Draft (work in progress), <draft-irtf-smug-taxonomy-01.txt>, August 2000. <http://www.watersprings.org/pub/id/draft-irtf-smug-taxonomy-01.txt>

Carlson, Steven C., Patent Pools and the Antitrust Dilemma. 16 Yale Journal on Regulation 359 ff. (1999)

Castells, Manuel, The Rise of the Network Society. 2. Auflage, Oxford 2000

Cavoukian, Ann/Gurski, Michael/Mulligan, Deirdre/Schwartz, Ari, P3P und Datenschutz. Ein Update für die Datenschutzgemeinde. Datenschutz und Datensicherheit 2000, 475 ff.

Cawkell, Tony, Electronic Books. 51 (2) Aslib Proceedings 54 ff. (Februar 1999)

Chang, Ai-Mei/Kannan, P. K./Whinston, Andrew B., The Economics of Freebies in Exchange for Consumer Information on the Internet: An Exploratory Study. 4 International Journal of Electronic Commerce 85 ff. (1999)

Chaum, David, Achieving Electronic Privacy. Scientific American August 1992, 76 ff.

ders., Security Without Identification: Transaction Systems to Make Big Brother Obsolete. 28 Communications of the ACM 1030 ff. (1985)

Chavez, Anthony/Maes, Pattie, Kasbah: An Agent Marketplace for Buying and Selling Goods. In: Crabtree (Hrsg.), First International Conference on the Practical Application of Intelligent Agents and Multi-Agent Technology (PAAM). 22.–24. 4. 1996, London – Proceedings. Lancashire, 1996. S. 75 ff.

Chiariglione, Leonardo, MPEG: Achievements and Current Work. Oktober 2000. <http://www.cselt.it/mpeg/mpeg_general.htm>

Chircu, Alina M./Kauffman, Robert J., Reintermediation Strategies in Business-to-Business Electronic Commerce. 4 (4) International Journal of Electornic Commerce 7 ff. (2000)

Chor, Benny/Fiat, Amos/Naor, Moni , Tracing Traitors. In: Desmedt (Hrsg.), Advances in Cryptology – Crypto 1994. 21.–15. 8. 1994, Santa Barbara, USA – Proceedings. Berlin, 1994. S. 257 ff.

Chrocziel, Peter, Anmerkung zu BGH, Urteil vom 6. 7. 2000, Az. I ZR 244/97 – OEM-Version. Computer und Recht 2000, 738 ff.

Chu, Ha-hua/Qiao, Lintian/Nahrstedt, Klara, A Secure Multicast Protocol with Copyright Protection. in: Wong/Delp (Hrsg.), SPIE International Conference on Security and Watermarking of Multimedia Contents. 25.–27. 1. 1999, San Jose, USA – Proceedings. Bellingham, 1999. S. 460 ff.

Chuang, Trees-Juen/Lin, Ja-Chen, A New Multiresolutional Approach to Still Image Encryption. 9 Pattern Recognition and Image Analysis 431 ff. (1999)

Cichon, Caroline, Internetverträge. Verträge über Internet-Leistungen und Ecommerce. Köln, 2000

Ciciora, Walter/Farmer, James/Large, David, Modern Cable Television Technology. Video, Voide, and Data Communications. San Francisco, 1999

Clark, Charles, The Answer to the Machine is in the Machine. In: Hugenholtz (Hrsg.), The Future of Copyright in a Digital Environment. Amsterdam, 1996. S. 139 ff.

Clay, Karen/Krishnan, Ramayya/Wolff, Eric, Pricing Strategies on the Web: Evidence from the Online Book Industry. In: Proceedings of the 2nd ACM Conference on Electronic Commerce. 17.–20. 10. 2000, Minneapolis. New York, 2000. S. 44 ff.

Clay, Karen/Krishnan, Ramayya/Wolff, Eric/Fernandes, Danny, Retail Strategies on the Web: Price and Non-Price Competition in the Online Book Industry. Ohne Datum. <http://www.heinz.cmu.edu/~kclay/retailstrategies.pdf>

Clemens, Rudolf, Die elektronische Willenserklärung – Chancen und Gefahren. Neue Juristische Wochenschrift 1985, 1998 ff.

Coase, Ronald, The Problem of Social Cost. 3 Journal of Law and Economics 1 ff. (1960)

Cohen, Julie E., A Right to Read Anonymously: A Closer Look at „Copyright Management" in Cyberspace. 28 Connecticut Law Review 981 ff. (1996)

dies., Copyright and the Jurisprudence of Self-Help. 13 Berkeley Technology Law Journal 1089 ff. (1998)

dies., Copyright and the Perfect Curve. 53 Vanderbilt Law Review 1799 ff. (2000)

dies., Lochner in Cyberspace: The New Economic Orthodoxy of „Rights Management". 97 Michigan Law Review 462 ff. (1998)

dies., Some Reflections on Copyright Management Systems and Laws Designed to Protect Them. 12 Berkeley Technology Law Journal 161 ff. (1997)

dies., WIPO Copyright Treaty Implementation in the United States: Will Fair Use Survive? European Intellectual Property Review 1999, 236 ff.

Collberg, Christian S./Thomborson, Clark, Software Watermarking: Models and Dynamic Embeddings. In: Proceedings of the Symposium on Principles of Programming Languages (POPL) 1999. 20.–22. 1. 1999, San Antonio, USA. New York, 1999. S. 311 ff.

dies., Watermarking, Tamper-Proofing, and Obfuscation – Tools for Software Protection. University of Arizona Computer Science Technical Report 2000-03/University of Auckland Computer Science Technical Report #170. 10. 2. 2000. <http://www.cs.arizona.edu/~collberg/Research/Publications/CollbergThomborson2000a>

Collberg, Christian S./Thomborson, Clark/Low, Douglas, A Taxonomy of Obfuscating Transformations. University of Auckland Computer Science Technical Report #148. Juli 1997. <http://www.cs.arizona. edu/~collberg/Research/Publications/CollbergThomborsonLow97a>

Conner, Kathleen Reavis/Rumelt, Richard P., Software Piracy: An Analysis of Protection Strategies. 37 Management Science 125 ff. (1991)

Contreras, Jorge L./Slade, Kenneth H., Click-Wrap Agreements: Background and Guidelines for Enforceability. Computer und Recht international 2000, 104 ff.

Cooter, Robert/Ulen, Thomas, Law and Economics. 3. Auflage, Reading 2000

Cornelius, Herbert, Die Intel Pentium III Prozessor-Seriennummer. Datenschutz und Datensicherheit 1999, 529 ff.

Corradi, Antonio/Cremonini, Marco/Manotanari, Rebecca/Stefanelli, Cesare, Mobile Agents Integrity for Electronic Commerce Applications. 24 Information Systems 519 ff. (1999)

Covotta, Brian/Sergeef, Pamela, ProCD, Inc. v. Zeidenberg. 13 Berkeley Technology Law Journal 35 ff. (1998)

Cox, Brad, Superdistribution. Objects as Property on the Electronic Frontier. Reading, 1996

Cox, Ingemar J./Kilian, Joe/Leighton, Frank Thomson/Shamoon, Talal, A Secure, Robust Watermark for Multimedia. In: Aucsmith (Hrsg.), Information Hiding. Second International Workshop. 14.–17. 4. 1998, Portland, USA – Proceedings. Berlin, 1998. S. 185 ff.

Cox, Ingemar J./Linnartz, Jean-Paul M. G., Some General Methods for Tampering with Watermarking. 16 IEEE Journal on Selected Areas in Communications 587 ff. (1998)

Cranor, Lorrie Faith, Platform for Privacy Preferences – P3P. Datenschutz und Datensicherheit 2000, 479

Craver, Scott/Memon, Nasir/Yeo, Boon-Lock/Yeung, Minerva M., Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limiations, Attacks, and Implications. 16 IEEE Journal on Selected Areas in Communications 573 ff. (1998)

Craver, Scott/Perrig, Adrian/Petitcolas, Fabien A. P., Robustness of Copyright Marking Systems. In: Katzenbeisser/Petitcolas (Hrsg.), Information Hiding Techniques for Steganography and Digital Watermarking. Norwood, 2000. S. 149 ff.

Cromwell-Kessler, Willy, Crosswalks, Metadata Mapping, and Interoperability: What Does It All Mean? In: Baca (Hrsg.), Introduction to Metadata – Pathways to Digital Information. Getty Information Institute, 1998. S. 19 ff.

Cruellas, Juan Carlos/Kesterson, Hoyt L./Medina, Manual/Rubia, Montse, EDI and Digital Signatures for Business to Business Electronic Commerce. 38 Jurimetrics Journal 497 ff. (1998)

Culhane, Marianne B., The UCC Revision Process: Legislation You Should See in the Making. 26 Creighton Law Review 29 ff. (1992)

Cutts, David, DVB Conditional Access. 9 Electronics & Communication Engineering Journal 21 ff. (Februar 1997)

Daigle, Leslie L./Guilik, Dirk-Willem van/Iannella, Renato/Faltstrom, Patrik, URN Namespace Definition Mechanisms. Request for Comments 2611, Juni 1999. <http://www.rfc-editor.org/rfc/rfc2611.txt>

Dam, Kenneth W., Some Economic Considerations in the Intellectual Property Protection of Software. 24 Journal of Legal Studies 321 ff. (1995)

Datta, Tapas, Content Protection. Juli 1998. <http://www.enthink.com/documents/content1.html>

Davidson, Kent M./Kawatsura, Yoshiaki, Digital Signatures for the v1.0 Internet Open Trading Protocol (IOTP). Request for Comments 2802, April 2000. <http://www.rfc-editor.org/rfc/rfc2802.txt>

Davies, Gillian, Copyright and the Public Interest. Weinheim, 1994

Davis, James Raymond, On Self-Enforcing Contracts, the Right to Hack, and Willfully Ignorant Agents. 13 Berkeley Technology Law Journal 1144 ff. (1998)

Day, Michael/Heery, Rachel/Powell, Andy, National Bibliographic Records in the Digital Information Environment: Metadata, Links an Standards. 55 Journal of Documentation 16 ff. (1999)

DeBaun, Steven, The Piracy of Subscription TV – A Marketplace Solution to the Unauthorized Interception of MDS Transmissions. 34 UCLA Law Review 445 ff. (1986)

Debbasch, Charles, Droit de l'audiovisuel. 4. Auflage, Paris 1995

Dellebeke, Marcel (Hrsg.), Copyright in Cyberspace. Copyright and the Global Information Infrastructure. ALAI Study Days, Amsterdam, 4.–8. 6. 1996. Amsterdam, 1997

DeLong, J. Bradford/Froomkin, A. Michael, Speculative Microeconomics for Tomorrow's Economy. In: Kahin/Varian (Hrsg.), Internet Publishing and Beyond. The Economics of Digital Information and Intellectual Property. Cambridge, 2000. S. 6 ff.

Dembowski, Klaus, Feuerdraht. Firewire und andere serielle Bussysteme. c't Heft 2/1997, S. 284 ff.

Dempsey, Lorcan/Heery, Rachel, Metadata: A Current View of Practice and Issues. 54 Journal of Documentation 145 ff. (1998)

Demsetz, Harold, The Private Production of Public Goods. 13 Journal of Law and Economics 293 ff. (1970)

ders., Toward a Theory of Property Rights. 57 American Economic Review Papers & Proceedings 347 ff. (1967)

Denicola, Robert C., Mostly Dead? Copyright Law in the New Millennium. 47 Journal of the Copyright Society of the U.S.A. 193 ff. (2000)

Depoorter, Ben/Parisi, Francesco, Fair Use and Copyright Protection: A Price Theory Explanation. George Mason University School of Law, Law and Economics Working Paper No. 01-03, 2001. Erhältlich utner <http://papers.ssrn.com/abstract=259298>

Detering, Dietmar, Ökonomie der Medieninhalte. Allokative Effizienz und soziale Chancengleichheit in den Neuen Medien. Münster, 2001

Diedrich, Frank, Geistiges Eigentum und Vertragsrecht im neuen Entwurf des Article 2B UCC. Multimedia und Recht 1998, 513 ff.

Dierks, Tim/Allen, Chistopher, The TLS Protocol Version 1.0. Request for Comments 2246, Januar 1999. <http://www.rfc-editor.org/rfc/rfc2246.txt>

Dietz, Adolf, Die EU-Richtlinie zum Urheberrecht und zu den Leistungsschutzrechten in der Informationsgesellschaft. Vorstoß in den Kernbereich des Urheberrechts- und Leistungsschutzes und seine Folgen. Zeitschrift für Urheber- und Medienrecht 1998, 438 ff.

Diffie, Whitfield/Hellman, Martin E., New Directions in Cryptography. 22 IEEE Transactions on Information Theory 644 ff. (1976)

Dinant, Jean-Marc, Law and Technology Convergence in the Data Protection Field? Electronic Threats on Personal Data and Electronic Data Protection on the Internet. ECLIP (Esprit Project 27028) Deliverable 2.2.3; ohne Datum. <http://www.eclip.org/documents/deliverable_2_2_3_privacy.pdf>

Diot, Christophe/Levine, Brian Neil/Lyles, Bryan/Kassem, Hassan/Balensiefen, Doug, Deployment Issues for the IP Multicast Service and Architecture. 14 (1) IEEE Network 78 ff. (Januar/Februar 2000)

Dittmann, Jana, Digitale Wasserzeichen. Berlin, 2000

Dittmann, Jana/Steinebach, Martin, Manipulationserkennung bei digitalem Bildmaterial mit fragilen Wasserzeichen. Datenschutz und Datensicherheit 2000, 593 ff.

Dively, Mary Jo Howard/Ring, Carlyle C., Overview of Uniform Computer Information Transactions Act. Ohne Datum. Erhältlich unter <http://www.ucitaonline.com/docs/ring.pdf>

Dodd, Jeff C., Time and Assent in the Formation of Information Contracts: The Mischief of Applying Article 2 to Information Contracts. 36 Houston Law Review 195 ff. (1999)

Dolly, Craig, The Electronic Self-Help Provisions of UCITA: A Virtual Repo Man? 33 John Marshall Law Review 663 ff. (2000)

Doraswamy, Naganand/Harkins, Dan, IPSec. Der neue Sicherheitsstandard für das Internet, Intranets und virtuelle private Netze. München, 2000

Dowell, Jonathan, Bytes and Pieces: Fragmented Copies, Licensing, and Fair Use in a Digital World. 86 California Law Review 843 ff. (1998)

Dreier, Thomas, Balancing Proprietary and Public Domain Interests: Inside or Outside of Proprietary Rights? In: Dreyfuss/Zimmerman/First (Hrsg.): Expanding the Boundaries of Intellectual Property. Oxford, 2001. S. 295 ff.

ders., Urheberrecht an der Schwelle des 3. Jahrtausends. Einige Gedanken zur Zukunft des Urheberrechts. Computer und Recht 2000, 45 ff.

Dressel, Christian, Strafbarkeit von Piraterie-Angriffen gegen Zugangsberechtigungssysteme von Pay-TV-Anbietern. Multimedia und Recht 1999, 390 ff.

Dreyfuss, Rochelle Cooper, Games Economics Play. 53 Vanderbilt Law Review 1821 ff. (2000)

Dugelay, Jean-Luc/Roche, Stéphane, A Survey of Current Watermarking Techniques. In: Katzenbeisser/Petitcolas (Hrsg.), Information Hiding Techniques for Steganography and Digital Watermarking. Norwood, 2000. S. 121 ff.

Durand, Julian, Nokia – Position Paper. W3C Workshop on Digital Rights Management. Januar 2001. <http://www.w3.org/2000/12/drm-ws/pp/nokia-durand.html>

Durfee, Glenn/Franklin, Matt, Distribution Chain Security. In: Jajodia (Hrsg.), 7th ACM Conference on Computer and Communications Security (CCS). 1.–4. 11. 2000, Athen – Proceedings. New York, 2000. S. 63 ff.

Dusollier, Séverine, Electrifying the Fence: The Legal Protection of Technological Measures for Protecting Copyright. European Intellectual Property Review 1999, 285 ff.

dies., Anti Circumvention Protection Outside Copyright. Situating Legal Protections for Copyright-Related Technological Measures in the Broader Legal Landscape. General Report to the ALAI 2001 Congress, New York, Juni 2001. Erhältlich unter <http://www.law.columbia.edu/conferences/2001/Reports/GenRep_ic_en.doc>

Dwork, Cynthia/Lotspiech, Jeffrey/Naor, Moni, Digital Signets: Self-Enforcing Protection of Digital Information. In: Proceedings of the 28th Annual ACM Symposium on the Theory of Computing (STOC). 22.–24. 5. 1996, Pennsylvania, USA. New York, 1996. S. 489 ff.

Easterbrook, Frank H., Cyberspace and the Law of the Horse. 1996 University of Chicago Legal Forum 207 ff.

ders., Cyberspace versus Property Law? 4 Texas Review of Law & Politics 103 ff. (1999)

ders., Intellectual Property Is Still Property. 13 Harvard Journal of Law & Public Policy 108 ff. (1990)

Eastlake, Donald E./Reagle, Joseph M./Solo, David, XML-Signature Syntax and Processing. Internet Draft (work in progress), <draft-ietf-xmldsig-core-11.txt>, Oktober 2000. <http://www.watersprings.org/pub/id/draft-ietf-xmldsig-core-11.txt>

Ebel, Hans Rudolf, EG-Gruppenfreistellungsverordnung für Technologietransfer-Vereinbarungen. Wirtschaft und Wettbewerb 1996, 779 ff.

Economides, Nicholas, The Microsoft Antitrust Case. New York University, Center for Law and Business, Working Paper #CLB-01-003. 3. 4. 2001. Erhältlich unter <http://papers.ssrn.com/abstract=253083>

Edgar, Laura, Electronic Payment Systems. ECLIP (Esprit Project 27028) Deliverable 2.1.6; 21. 10. 1999. <http://www.eclip.org/documents/deliverable_2_1_6_electronic_ payments.pdf>

Edwards, Gary J., Self-Help Repossession of Software: Should Repossession Be Available in Article 2B of the UCC? 58 University of Pittsburgh Law Review 763 ff. (1997)

Eichler, Hermann, Institutionen des Sachenrechts – Ein Lehrbuch. Erster Band: Allgemeiner Teil, Grundlagen des Sachenrechts. Berlin, 1954

Eidenmüller, Horst, Effizienz als Rechtsprinzip. Möglichkeiten und Grenzen der ökonomischen Analyse des Rechts. 2. Auflage, Tübingen 1998

Eisenach, Jeffrey A./Lenard, Thomas M. (Hrsg.), Competition, Innovation and the Microsoft Monopoly: Antitrust in the Digital Marketplace. Boston, 1999

Eisenberg, Melvin Aron, The Limits of Cognition and the Limits of Contract. 47 Stanford Law Review 211 ff. (1995)

Electronic Privacy Information Center, Filters & Freedom. Free Speech Perspectives on Internet Content Controls. Washington, 1999

Elkin-Koren, Niva, A Public-Regarding Approach to Contracting Over Copyrights. In: Dreyfuss/Zimmerman/First (Hrsg.): Expanding the Boundaries of Intellectual Property. Oxford, 2001. S. 191 ff.

dies., Copyright Policy and the Limits of Freedom of Contract. 12 Berkeley Technology Law Journal 93 ff. (1997)

dies., Copyrights in Cyberspace – Rights Without Laws? 73 Chicago-Kent Law Review 1155 ff. (1998)

Elkin-Koren, Niva/Salzberger, Eli M., Law and Economics in Cyberspace. 19 International Review of Law and Economics 553 ff. (1999)

Ellickson, Robert C., Order Without Law – How Neighbors Settle Disputes. Cambridge, 1991

Elsing, Siegfried H./Van Alstine, Michael P., US-amerikanisches Handels- und Wirtschaftsrecht. 2. Auflage, Heidelberg 1999

Emmerich, Volker, Kartellrecht. 8. Auflage, München 1999

Endres, Albert/Fellner, Dieter W., Digitale Bibliotheken. Informatik-Lösungen für globale Wissensmärkte. Heidelberg, 2000

Engel, Christoph, A Constitutional Framework for Private Governance. Preprint 2001/4 der Max-Planck-Projektgruppe „Recht der Gemeinschaftsgüter". 2001. Online erhältlich unter <http://www.mpp-rdg.mpg.de/pdf_dat/001_4.pdf>

Enzmann, Matthias, Introducing Privacy to the Internet User. How P3P meets the European Data Protection Directive. Datenschutz und Datensicherheit 2000, 535 ff.

Ercegovac, Zorana, Introduction. 50 Journal of the American Society for Information Science 1165 ff. (1999)

Ergun, Funda/Kilian, Joe/Rumar, Ravi, A Note on the Limits of Collusion-Resistant Watermarks. In: Stern (Hrsg.), Advances in Cryptology – Eurocrypt 1999. International Conference on the Theory and Application of Cryptographic Techniques. 2.–6. 5. 1999, Prag – Proceedings. Berlin, 1999. S. 140 ff.

Erickson, John S., Information Objects and Rights Management. A Mediation-based Approach to DRM Interoperability. 7 (4) D-Lib Magazine (April 2001), erhältlich unter <http://www.dlib. org/dlib/april01/erickson/04erickson.html>

Ermer, Dieter J., Systemdatenschutz und Chipkarte. Computer und Recht 2000, 126 ff.

European Communication Council (Hrsg.), Die Internet-Ökonomie – Strategien für die digitale Wirtschaft. 3. Auflage, Berlin 2001

Fabricius, Fritz, Zur Theorie des stückelosen Effektengiroverkehrs mit Wertrechten aus Staatsanleihen. Zugleich ein Beitrag zur Frage der Abgrenzung von Schuldrecht und Sachenrecht. Archiv für die civilistische Praxis 162 (1963), 456 ff.

Farag, Neveen I./Van Alstyne, Marshall W., Information Technology – A Source of Friction? An Analytical model of How Firms Combat Price Competition Online. In: Proceedings of the 2nd ACM Conference on Electronic Commerce. 17.–20. 10. 2000, Minneapolis. New York, 2000. S. 135 ff.

Farnsworth, Edward Allan, Farnsworth on Contracts. 3 Bände. 2. Auflage, New York 1998

Farrell, Joseph, Arguments for Weaker Intellectual Property Protection in Network Industries. In: Kahin/Abbate (Hrsg.), Standards Policy for Information Infrastructure, Cambridge, 1995. S. 368 ff.

Fechner, Frank, Geistiges Eigentum und Verfassung. Tübingen, 1999

Federrath, Hannes, Multimediale Inhalte und technischer Urheberrechtsschutz im Internet. Zeitschrift für Urheber- und Medienrecht 2000, 804 ff.

Federrath, Hannes/Pfitzmann, Andreas, Anonymität, Authentizität und Identifizierung im Internet. In: Bartsch/Lutterbeck (Hrsg.), Neues Recht für neue Medien. Köln, 1998. S. 319 ff.

dies., Gliederung und Systematisierung von Schutzzielen in IT-Systemen. Datenschutz und Datensicherheit 2000, 704 ff.

Ferris, Charles D./Lloyd, Frank W., Telecommunications Regulation: Cable, Broadcasting, Satellite and the Internet. Loseblatt-Sammlung. Stand: 35. Ergänzungslieferung, Dezember 1999

Fiat, Amos/Naor, Moni, Broadcast Encryption. In: Stinson (Hrsg.), Advances in Cryptology – Crypto 1993. 13th Annual International Cryptology Conference. 22.–26. 8. 1993, Santa Barbara, USA – Proceedings. Berlin, 1994. S. 480 ff.

Fiat, Amos/Tassa, Tamir, Dynamic Traitor Tracing. In: Wiener (Hrsg.), Advances in Cryptology – Crypto 1999. 19th Annual International Cryptology Conference. 15.–19. 8. 1999, Santa Barbara, USA – Proceedings. Berlin, 1999. S. 354 ff.

Fikentscher, Wolfgang, Wirtschaftsrecht. Band I: Weltwirtschaftsrecht, Europäisches Wirtschaftsrecht. München, 1983

Fishburn, Peter C./Odlyzko, Andrew M., Competitive Pricing of Information Goods: Subscription Pricing Versus Pay-Per-Use. 13 Economic Theory 447 ff. (1999)

Fishburn, Peter C./Odlyzko, Andrew M./Siders, Ryan C., Fixed-Fee versus Unit Pricing for Information Goods: Competition, Equilibria, and Price Wars. In: Kahin/Varian (Hrsg.), Internet Publishing and Beyond. The Economics of Digital Information and Intellectual Property. Cambridge, 2000. S. 167 ff.

Fisher, William W., Property and Contract on the Internet. 73 Chicago-Kent Law Review 1203 ff. (1998)

ders., Reconstructing the Fair Use Doctrine. 101 Harvard Law Review 1661 ff. (1988)

Fitzpatrick, Simon, Copyright Imbalance: U.S. and Australian Responses to the WIPO Digital Copyright Treaty. European Intellectual Property Review 2000, 214 ff.

Flechsig, Norbert P., EU-Harmonisierung des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft. Zeitschrift für Urheber- und Medienrecht 1998, 139 ff.

Fox, Dirk, Extensible Markup Language (XML). Datenschutz und Datensicherheit 2000, 609

Freytag, Stefan, Digital Millennium Copyright Act und europäisches Urheberrecht für die Informationsgesellschaft. Multimedia und Recht 1998, 207 ff.

ders., Haftung im Netz. Verantwortlichkeit für Urheber-, Marken- und Wettbewerbsrechtsverletzungen nach § 5 TDG und § 5 MDStV. München, 1999

Fridrich, Jiri, Imager Watermarking for Tamper Detection. In: Proceedings of the International Conference on Image Processing (ICIP). 4.–7. 10. 1998, Chicago. Piscataway, 1998. Band 2, S. 404 ff.

ders., Methods for Detecting Changes in Digital Images. In: Proceedings of the 6th IEEE International Workshop on Intelligent Signal Processing and Communication Systems (ISPACS). 4.–6. 11. 1998, Melbourne. S. 173 ff.

ders., Methods for Tamper Detection in Digital Images. In: Dittmann/Nahrstedt/Wohlmacher (Hrsg.), Multimedia and Security. Workshop at ACM Multimedia '99. 30. 10. - 5. 11. 1999, Orlando, USA. GMD Report 85. Sankt Augustin, 2000. Online erhältlich unter <http://www.gmd.de/publications/report/0085/Text.pdf>. S. 41 ff.

Fridrich, Jiri/Goljan, Miroslav, Robust Hash Functions for Digital Watermarking. In: International Conference on Information Technology: Coding and Computing (ITCC). 27.–29. 3. 2000, Las Vegas – Proceedings. Los Alamitos, 2000. S. 178 ff.

Fried, Charles, Perfect Freedom or Perfect Control? Book Review of Code, and Other Laws of Cyberspace by Lawrence Lessig. 114 Harvard Law Review 606 ff. (2000)

Friedman, David D., In Defense of Private Orderings: Comments on Julie Cohen's „Copyright and the Jurisprudence of Self-Help". 13 Berkeley Technology Law Journal 1151 ff. (1998)

Friedman, Gary L., The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image. 39 IEEE Transactions on Consumer Electronics 905 ff. (1993)

Frischmann, Brett/Moylan, Dan, The Evolving Common Law Doctrine of Copyright Misuse: A Unified Theory and Its Application to Software. 15 Berkeley Technology Law Journal 865 ff. (2000)

Fromm, Friedrich Karl/Nordemann, Wilhelm (Hrsg.), Urheberrecht. Kommentar zum Urheberrechtsgesetz und zum Urheberrechtswahrnehmungsgesetz. 9. Auflage, Stuttgart 1998

Froomkin, Michael A., It Came From Planet Clipper: The Battle Over Cryptographic Key „Escrow". 1996 University of Chicago Legal Forum 15 ff.

ders., The Death of Privacy? 52 Stanford Law Review 1462 ff. (2000)

ders., Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution. 50 Duke Law Journal 17 ff. (2000)

Fujii, Hiroshi/Abe, Takehito/Nishihara, Yuichi/Kushima, Kazuhiko, Partial-scrambling of Information. 11 (1) NTT Review 116 ff. (Januar 1999)

Fujimara, Ko, Requirements for Generic Rights Trading. Internet Draft (work in progress), <draft-ietf-trade-drt-requirements-01.txt>, Dezember 2000. <http://www.watersprings.org/pub/id/draft-ietf-trade-drt-requirements-01.txt>

Furon, Teddy/Duhamel, Pierre, An Asymmetric Public Detection Watermarking Technique. In: Pfitzmann (Hrsg.), Information Hiding – Third International Workshop. 29. 9. – 1. 10. 1999. Berlin, 2000. S. 88 ff.

Gafni, Eli/Staddon, Jessica/Yin, Yiqun Lisa, Efficient Methods for Integrating Traceability and Broadcast Encryption. In: Wiener (Hrsg.), Advances in Cryptology – Crypto 1999. 19th Annual International Cryptology Conference. 15.–19. 8. 1999, Santa Barbara, USA – Proceedings. Berlin, 1999. S. 372 ff.

Gallego, Isabel/Delgado, Jaime/Garcia, Roberto, Use of Mobile Agents for IPR Management and Negotiation. In: Horlait (Hrsg.), Mobile Agents for Telecommunication Applications. Second International Workshop. 18.–20. 9. 2000, Paris – Proceedings. Berlin, 2000. S. 205 ff.

Gamm, Otto-Friedrich Freiherr von, Urheberrechtsgesetz. Kommentar. München, 1968

Garcia-Molina, Hector/Ketchpel, Steven P./Shivakumar, Narayanan, Safeguarding and Charging for Information on the Internet. In: Proceedings of the 14th International Conference on Data Engineering (ICDE). 23.–27. 2. 1998, Orlando, USA. Los Alamitos, 1999. S. 182 ff.

Garnett, Kevin, The Music Industry. In: World Intellectual Property Organization (Hrsg.), WIPO Worldwide Symposium on the Impact of Digital Technology in Copyright and Neighbouring Rights. 31. 3. – 2. 4. 1993, Harvard University. Genf, 1993. S. 101 ff.

Garnett, Kevin/James, Jonathan Rayner/Davies, Gillian, Copinger and Skone James on Copyright. 14. Auflage, London 1999

Garon, Jon M., Media & Monopoly in the Information Age: Slowing the Convergence at the Marketplace of Ideas. 17 Cardozo Arts & Entertainment Law Journal 491 ff. (1999)

Garrett, John R./Lyons, Patrice, A., Toward an Electronic Copyright Management System. 44 (8) Journal of the American Society for Information Science 468 ff. (1993)

Gass, Wolfram, Digitale Wasserzeichen als urheberrechtlicher Schutz digitaler Werke? Zeitschrift für Urheber- und Medienrecht 1999, 815 ff.

Gaster, Jens, Die draft U.S. database legislation und die EU-Datenbankrichtlinie – ein Vergleich. Computer und Recht 1999, 669-679

ders., Urheberrecht und verwandte Schutzrechte in der Informationgesellschaft. Anmerkungen zum Grünbuch der Europäischen Kommission. Zeitschrift für Urheber- und Medienrecht 1995, 740 ff.

Gentz, Wolfgang, Elektronische Geldbörsen in Deutschland. GeldKarte und PayCard. Datenschutz und Datensicherheit 1999, 18 ff.

Gervais, Daniel, Electronic Commerce and Copyright: A Key Role for WIPO. In: Koskinen-Olsson/Gervais (Hrsg.), Electronic Commerce and Copyright: A Key Role for WIPO. Advisory Committee on Management of Copyright and Related Rights in Global Information Networks, Genf, 8.–9. 12. 1999. WIPO-Dokument ACMC/2/1 vom 17. 11. 1999, erhältlich unter <http://www.wipo.int/eng/meetings/1999/acmc/pdf/acmc_1.pdf>. S. 6 ff.

Giaglis, George M./Klein, Stefan/O'Keefe, Robert, Disintermediation, Reintermediation, or Cybermediation? The Future of Intermediaries in Electronic Marketplaces. April 1999. <http://www.brunel.ac.uk/depts/cs/reports/InterVersion2.pdf>

Gill, Tony, Metadata and the World Wide Web. In: Baca (Hrsg.), Introduction to Metadata – Pathways to Digital Information. Getty Information Institute, 1998. S. 9 ff.

Gilmont, Tanguy/Legat, Jean-Didier/Quisquater, Jean-Jacques, An Architecture of Security Management Unit for Safe Hosting of Multiple Agents. In: Wong/Delp (Hrsg.), SPIE International Conference on Security and Watermarking of Multimedia Contents. 25.–27. 1. 1999, San Jose, USA – Proceedings. Bellingham, 1999. S. 472 ff.

Gilmore, John, Was falsch ist am Kopierschutz. 16. 2. 2001. c't Heft 4/2001, S. 64 ff. Online unter <http://www.heise.de/ct/copyright>, englische Original-Fassung unter <http://www.toad.com/gnu/whatswrong.html>

Gimbel, Mark, Some Thoughts on the Implications of Trusted Systems for Intellectual Property Law. 50 Stanford Law Review 1671 ff. (1998)

Ginsburg, Jane C., Copyright Legislation for the „Digital Millenium", 23 Columbia-VLA Journal of Law & the Arts 137 ff. (1999)

dies., Copyright Use and Excuse on the Internet. 24 Columbia-VLA Journal of Law & the Arts 1 ff. (2000)

dies., Copyright Without Walls?: Speculations on Literary Property in the Library of the Future. 42 Representations 53 ff. (1993)

dies., From Having Copies to Experiencing Works: the Development of an Access Rights in U.S. Copyright Law, 2000. Online erhältlich unter <http://papers.ssrn.com/abstract=222493>

Gladney, Henry M./Mintzer, Fred/Schiattarella, Fabio, Safeguarding Digital Libary Contents and Users – Digital Images of Treasured Antiquities. 3 (7) D-Lib Magazine (Juli 1997), erhältlich unter <http://www.dlib.org/dlib/july97/vatican/07gladney.html>

Glushko, Robert J./Tenenbaum, Jay M./Meltzer, Bart, An XML Framework for Agent-based E-commerce. 42 (3) Communciations of the ACM 106 ff. (März 1999)

Goldsmith, Jack L., Against Cyberanarchy. 65 University of Chicago Law Review 1199 ff. (1998)

Goldstein, Paul, Copyright and Its Substitutes. 45 Journal of the Copyright Society of the USA 151 ff. (1997)

ders., Copyright. Loseblatt-Sammlung. 2. Auflage, Gaithersburg. Stand: 2000 Supplement (November 1999)

ders., Copyright's Highway. From Gutenberg to the Celestial Jukebox. New York, 1994

Goldstone, David J., A Funny Thing Happened on the Way to the Cyber Forum: Public vs. Private in Cyberspace Speech. 69 University of Colorado Law Review 1 ff. (1998)

Gomulkiewicz, Robert W., The License is the Product: Comments on the Promise of Article 2B for Software and Information Licensing. 13 Berkeley Technology Law Journal 891 ff. (1998)

Gonzalez, Ines G., Recording Industry Association of America, Inc. v. Diamond Multimedia Systems, Inc. 15 Berkeley Technology Law Journal 67 ff. (2000)

Goolsby, Sharan Leslie, Protection of Intellectual Property Rights under NAFTA. 4 NAFTA: Law and Business Review of the Americas 5 ff. (Autumn 1998)

Gordon, Wendy J., An Inquiry into the Merits of Copyright: The Challenges of Consitency, Consent, and Encouragement Theory. 41 Stanford Law Review 1343 ff. (1989)

dies., Asymmetric Market Failure and Prisoner's Dilemma in Intellectual Property. 17 University of Dayton Law Review 853 ff. (1992)

dies., Fair Use as Market Failure: A Structural and Economic Analysis of the Betamax Case and Its Predecessors. 82 Columbia Law Review 1600 ff. (1982)

dies., Intellectual Property as Price Discrimination: Implications for Contract. 73 Chicago-Kent Law Review 1367 ff. (1998)

dies., Systemische und fallbezogene Lösungsansätze für Marktversagen bei Immaterialgütern. In: Ott/Schäfer (Hrsg.), Ökonomische Analyse der rechtlichen Organisation von Innovationen. Tübingen, 1994. S. 328 ff.

Gordon, Wendy J./Bone, Robert G., Copyright. In: Bouckaert/De Geest (Hrsg.), Encyclopedia of Law and Economics. – Volume II: Civil Law and Economics. Cheltenham, 2000. Kapitel 1610, S. 189 ff.

Götting, Horst-Peter, Anmerkung zu EuGH, JZ 1996, 304 – Magill. Juristen-Zeitung 1996, 307 ff.

Götting, Horst-Peter/Fikentscher, Adrian, Gewerblicher Rechtsschutz und Urheberrecht. In: Assmann/Bungert (Hrsg.), Handbuch des US-amerikanischen Handels-, Gesellschafts- und Wirtschaftsrechts. Band 1. München, 2001. Kapitel 7, S. 393 ff.

Green, Brian/Bide, Mark, Unique Identifiers: a Brief Introduction, 1997. <http://www.bic.org.uk/uniquid.html>

Greenleaf, Graham, „IP, Phone Home" – ECMS, -Tech, and Protecting Privacy Against Surveillance by Digital Works. Beitrag zur 21st International Conference on Privacy and Personal Data Protection, Hong Kong, 13.–15. 9. 1999. Fassung vom 26. 5. 1999. <http://www2.austlii.edu.au/~graham/publications/ip_privacy>

ders., An Endnote on Regulating Cyberspace: Architecture vs Law? 21 University of New South Wales Law Journal 593 ff. (1998)

Greenwald, Amy R./Kephart, Jeffrey O., Shopbots and Pricebots. In: Dean (Hrsg.), Sixteenth International Joint Conference on Artificial Intelligence. 31. 7. – 6. 8. 1999, Stockholm – Proceedings. San Francisco, 1999. Band 1, S. 506 ff.

Gröhn, Andreas, Netzwerkeffekte und Wettbewerbspolitik. Eine ökonomische Analyse des Softwaremarkts. Tübingen, 1999

Grover, Derrick, Program Identification. In: Grover (Hrsg.), The Protection of Computer Software – Its Technology and Applications. 2. Auflage, Cambridge 1992. S. 122 ff.

ders., Review of Methods of Software Protection. In: Grover (Hrsg.), The Protection of Computer Software – Its Technology and Applications. 2. Auflage, Cambridge 1992. S. 1 ff.

Grunsky, Wolfgang, Allgemeine Geschäftsbedingungen und Wettbewerbswirtschaft. Betriebsberater 1971, 1113 ff.

Grünwald, Andreas, Analoger Switch-Off. Auf dem Weg zur Digitalisierung des terrestrischen Fernsehens. Multimedia und Recht 2001, 89 ff.

Grusd, Brandon L., Contracting Beyond Copyright: ProCD. Inc. v. Zeidenberg. 10 Harvard Journal of Law and Technology 353 ff. (1997)

Guibault, Lucie M.C.R., Contracts and Copyright Exemptions. In: Hugenholtz (Hrsg.), Copyright and Electronic Commerce – Legal Aspects of Electronic Copyright Management. London, 2000. S.125 ff.

Gunter, Carl/Weeks, Stephen/Wright, Andrew, Models and Languages for Digital Rights. InterTrust StarLab Technical Report STAR-TR-01-04, März 2001. <http://www.star-lab.com/tr/star-tr-01-04.pdf>

Gupta, Sachin/Jain, Dipak C./Sawhney, Mohanbir S., Modeling the Evolution of Markets with Indirect Network Externalities: An Application to Digital Television. 18 Marketing Science 396 ff. (1999)

Guttman, Robert/Moukas, Alexandros/Maes, Pattie, Agents as Mediators in Electronic Commerce. In: Klusch (Hrsg.), Intelligent Information Agents. Agent-Based Information Discovery and Management on the Internet. Berlin, 1999. S. 131 ff.

Haedicke, Maximilan, Einführung in das internationale Urheberrecht: Die Grundprinzipien und der institutionelle Rahmen nach Abschluß der GATT-Uruguay-Runde. Jura 1996, 64 ff.

Hagemann, Hagen/Schaup, Sonja/Schneider, Markus, Sicherheit und Perspektiven elektronischer Zahlungssysteme. Datenschutz und Datensicherheit 1999, 5 ff.

Hakala, Juha/Walravens, Hartmut, Using International Standard Book Numbers as Uniform Resource Names. Internet Draft (work in progress), <draft-hakala-isbn-01.txt>, 25. 1. 2001. <http://www.watersprings.org/pub/id/draft-hakala-isbn-01.txt>

Haller, Albrecht, Music on demand. Internet, Abrufdienste und Urheberrecht. Wien, 2001

ders., Zum EG-Richtlinienvorschlag betreffend Urheberrecht in der Informationsgesellschaft. Medien und Recht 1998, 61 ff.

Hallgren, Martyne M./McAdam, Alan K., The Economic Efficiency of Internet Public Goods. In: McKnight/Bailey (Hrsg.), Internet Economics. Cambridge, 1997. S. 455 ff.

Halpern, Marcelo/Mehrotra, Ajay K., From International Treaties to Internet Norms: The Evolution of International Trademark Disputes in the Internet Age. 21 University of Pennsylvania Journal of International Economic Law 523 ff. (2000)

Hammer, Volker, Die 2. Dimension der IT-Sicherheit. Verletzlichkeitsreduzierende Technikgestaltung am Beispiel von Public Key Infrastrukturen. Braunschweig, 1999

ders., Verletzlichkeitsreduzierende Technikgestaltung. Datenschutz und Datensicherheit 2001, 137 ff.

Hans, Werner/Beykirch, Hans-Bernhard/Hiroya, Masaaki/Kawatsura, Yoshiaki, Payment API for v1.0 Internet Open Trading Protocol (IOTP). Internet Draft (work

in progress), <draft-ietf-trade-iotp-v1.0-papi-03.txt>, November 2000. <http://www.watersprings.org/pub/id/draft-ietf-trade-iotp-v1.0-papi-03.txt>

Hansmann, Henry/Santilli, Marina, Authors' and Artists' Moral rights: A Comparative Legal and Economic Analysis. 26 Journal of Legal Studies 95 ff. (1997)

Hardy, Trotter, Property (and Copyright) in Cyberspace. 1996 University of Chicago Legal Forum 217 ff. (1996)

Harney, Hugh/Muckenhirn, Carl, Group Key Management Protocol (GKMP) Architecture. Request for Comments 2094, Juli 1997. <http://www.rfc-editor.org/rfc/rfc2094.txt>

Hartung, Frank/Girod, Bernd , Fast Public-Key Watermarking of Compressed Video. In: Proceedings of the International Conference on Image Processing (ICIP). 26.–29. 10. 1997, Santa Barbara, USA. Piscataway, 1997. Band 1, S. 528 ff.

Hartung, Frank/Kutter, Martin, Multimedia Watermarking Techniques. 87 Proceedings of the IEEE 1079 ff. (1999)

Hartung, Frank/Ramme, Friedhelm, Digital Rights Management and Watermarking of Multimedia Content for M-Commerce Applications. IEEE Communications Magazine 78 ff. (November 2000)

Hauwe, Ludwig Van den, Public Choice, Constitutional Political Economy and Law and Economics. In: Bouckaert/De Geest (Hrsg.), Encyclopedia of Law and Economics. Volume II: The History and Methodology of Law and Economics. Cheltenham, 2000. Kapitel 0610, S. 603 ff.

Haymer, Robert D., Who Owns the Air? Unscrambling the Satellite Viewing Rights Dilemma. Loyola of Los Angeles Law Review 145 ff. (1986)

Heal, Geoffrey, New Strategies for the Provision of Global Public Goods. Learning from Itnernational Environmental Challenges. In: Kaul/Grunberg/Stern (Hrsg.), Global Public Goods. New York, 1999. S. 220 ff.

Heaton, Timothy P., Electronic Self-Help Software Repossession: A Proposal to Protect Small Software Development Companies. 6 Boston University Journal of Science and Technology Law 8 (2000). Online erhältlich unter <http://www.bu.edu/law/scitech/volume6/Heaton.htm>

Hefermehl, Wolfgang, Wettbewerbsrecht. Kommentar. 22. Auflage, München 2001

Hegyi, Gabor, Das neue ungarische Urheberrechtsgesetz (Gesetz LXXVI/1999). GRUR Int. 2000, 325 ff.

Heide, Thomas, Access Control and Innovation under the Emerging EU Electronic Commerce Framework. 15 Berkeley Technology Law Journal 993 ff. (2000)

ders. , The Approach to Innovation under the Proposed Copyright Directive: Time for Mandatory Exceptions. Intellectual Property Quarterly 2000, 215 ff.

Heil, Helmut, Datenschutz durch Selbstregulung – Der europäische Ansatz. Datenschutz und Datensicherheit 2001, 129 ff.

Helberger, Natali, Hacken von Premiere bald europaweit verboten? Der rechtliche Schutz von Pay-TV Programmen nach europäischem Recht. Zeitschrift für Urheber- und Medienrecht 1999, 295 ff.

Heller, James S., The Uniform Computer Informations Transactions Act (UCITA): Still Not Ready for Prime Time. 7 Richmond Journal of Law & Technology 14 (Symposium 2000). Erhältlich unter <http://www.richmond.edu/jolt/v7i2/heller.html>

Heller, Michael A., The Tragedy of the Anticommons: Property in the Transition from Marx to Markets. 111 Harvard Law Review 622 ff. (1998)

Heller, Michael A./Eisenberg, Rebecca S., Can Patents Deter Innovation? Anticommons in Biomedical Research. 280 Science 698 ff. (1998)

Hemnes, Thomas M. S., Restraints on Alienation, Equitable Servitudes, and the Feudal Nature of Computer Software Licensing. 71 Denver University Law Review 577 ff. (1994)

Herpel, Carsten/Eleftheriadis, Alexandros, MPEG-4 Systems: Elementary Stream Management. 15 Signal Processing: Image Communciations 299 ff. (2000)

Herrigel, Alexander, Digitale Wasserzeichen als Urheberschutz. Datenschutz und Datensicherheit 1998, 254 ff.

Hes, Ronald/Borking, John (Hrsg.), Privacy-Enhancing Technologies: The Path to Anonymity. Revised Edition. Den Haag (Registratiekamer), August 2000

Hetcher, Steven, Climbing the Walls of Your Electronic Cage. 98 Michigan Law Review 1916 ff. (2000)

Heun, Sven-Erik, Die elektronische Willenserklärung. Rechtliche Einordnung, Anfechtung und Zugang. Computer und Recht 1994, 595 ff.

Hill, Jennett M., The State of Copyright Protection for Electronic Databases Beyond ProCD v. Zeidenberg: Are Shrinkwrap Licenses a Viable Alternative for Database Protection? 31 Indiana Law Review 143 ff. (1998)

Hill, Keith, A Perspective: The Role of Identifiers in Managing and Protecting Intellectual Property in the Digital Age. 87 Proceedings of the IEEE 1228 ff. (1999)

Hiltzik, Michael, Dealers of Lightning. Xerox PARC and the Dawn of the Computer Age. New York, 1999

Hoeren, Thomas, Bringt Bücher nach Brüssel – Überlegungen zur Informationskultur bei den Europäischen Institutionen. Neue Juristische Wochenschrift 2000, 3112 ff.

ders., Buchbesprechung von Dittmann: Digitale Wasserzeichen, Heidelberg 2000. Multimedia und Recht Heft 11/2000, S. XVIII

ders., Entwurf einer EU-Richtlinie zum Urheberrecht in der Informationsgesellschaft. Überlegungen zum Zwischenstand der Diskussion. Multimedia und Recht 2000, 515 ff.

ders., Internet und Recht – Neue Paradigmen des Informationsrechts. Neue Juristische Wochenschrift 1998, 2849 ff.

ders., Kollisionsrechtliche Anknüpfungen in internationalen Datenbanken. In: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht. München. Stand: 2. Ergänzungslieferung, Dezember 2000. Teil 7.10

ders., Softwareüberlassung als Sachkauf. Ausgewählte Rechtsprobleme des Erwerbs von Standardsoftware. München, 1989

ders., Urheberrecht 2000 – Thesen für eine Reform des Urheberrechts. Multimedia und Recht 2000, 3 ff.

Hoeren, Thomas/Schuhmacher, Dirk, Verwendungsbeschränkungen im Softwarevertrag. Überlegungen zum Umfang des Benutzungsrechts für Standardsoftware. Computer und Recht 2000, 137 ff.

Hoeren, Thomas/Sieber, Ulrich (Hrsg.), Handbuch Multimedia-Recht. Loseblatt-Sammlung, München. Stand: 2. Ergänzungslieferung, Dezember 2000

Hoffmann-Riem, Wolfgang, Informationelle Selbstbestimmung in der Informationsgesellschaft – Auf dem Wege zu einem neuen Konzept des Datenschutzes. Archiv für öffentliches Recht 32 (1998), S. 513 ff.

ders., Innovation durch Recht und im Recht. In: Schulte (Hrsg.), Technische Innovation und Recht – Antrieb oder Hemmnis? Heidelberg, 1997. S. 3 ff.

ders., Modernisierung von Recht und Justiz. Frankfurt/M., 2001

ders., Öffentliches Recht und Privatrecht als wechselweistige Auffangordnungen – Systematisierung und Entwicklungsperspektiven. In: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen. Baden-Baden, 1996. S. 261 ff.

Hoffmann-Riem, Wolfgang/Eifert, Martin, Regelungskonzepte des Telekommunikationsrechts und der Telekommunikationspolitik: Innovativ und innovationsgeeignet? In: Hoffmann-Riem (Hrsg.), Innovation und Telekommunikation. Rechtliche Steuerung von Innovationsprozessen in der Telekommunikation. Baden-Baden, 2000. S. 9 ff.

Hoffmann-Riem, Wolfgang/Schulz, Wolfgang/Held, Thorsten, Konvergenz und Regulierung. Optionen für rechtliche Regelungen und Aufsichtsstrukturen im Bereich Information, Kommunikation und Medien. Baden-Baden, 2000

Holitscher, Marc, Global Internet Governance and the Rise of the Private Sector. Schweizerische Zeitschrift für Politikwissenschaft 5 (2), S. 134 ff. (Sommer 1999)

Holznagel, Bernd, Weiterverbreitung und Zugangssicherung beim digitalen Fernsehen. Aufgaben der Landesmedienanstalten bei der Umsetzung der §§ 52, 53 RStV. Multimedia und Recht 2000, 480 ff.

Hubmann, Heinrich, Die Zulässigkeit der Ausleihe von Videokassetten in öffentlichen Bibliotheken. Film und Recht 1984, 495 ff.

Hugenholtz, P. Bernt, Code as Code, Or the End of Intellectual Property as We Know It. 6 Maastricht Journal of European and Comparative Law 308 ff. (1999)

ders., Copyright, Contract and Code: What Will Remain of the Public Domain? 26 Brooklyn Journal of International Law 77 ff. (2000)

ders., Copyright and Freedom of Expression in Europe. In: Dreyfuss/Zimmerman/First (Hrsg.): Expanding the Boundaries of Intellectual Property. Oxford, 2001. S. 343 ff.

ders., Why the Copyright Directive is Unimportant, and Possibly Invalid. European Intellectual Property Review 2000, 499 ff.

Hugenholtz, P. Bernt (Hrsg.), Copyright and Electronic Commerce. Legal Aspects of Electornic Copyright Management. Den Haag, 2000

Huhns, Michael N./Stephens, Larry M., Multiagent Systems and Societies of Agents. In: Weiss (Hrsg.), Multiagent Systems. A Modern Approach to Distributed Artificial Intelligence. Cambridge, 1999. S. 79 ff.

Hunter, Jane/Iannella, Renato, The Application of Metadata Standards to Video Indexing. In: Nikolaou/Stephanidis (Hrsg.), Research and Advanced Technology for Digital Libraries. Second European Conference (ECDL). 21.–23. 9. 1998, Heraklion, Kreta – Proceedings. Berlin, 1998. S. 135 ff.

Ihde, Rainer, Cookies – Datenschutz als Rahmenbedingung der Internetökonomie. Computer und Recht 2000, 413 ff.

Immenga, Ulrich/Mestmäcker, Ernst-Joachim (Hrsg.), EG-Wettbewerbsrecht. Kommentar. Band I. München 1997

dies. (Hrsg.), Gesetz gegen Wettbewerbsbeschränkungen (GWB). Kommentar zum Kartellgesetz. 3. Auflage, München 2001

Information and Privacy Commissioner, Ontario, Canada/Registratiekamer, The Netherlands, Intelligent Software Agents. Turning a Privacy Threat into a Privacy Protector. Den Haag, April 1999. Online erhältlich unter <http://www.ipc.on.ca/english/pubpres/sum_pap/papers/isat.pdf>. Ebenfalls veröffentlicht unter dem Titel „Software Agents and Privacy" von den Autoren Verhaar/Luiijf/Struik am

TNO Physics and Electronic Laboratory, TNO Report FEL-98-C213, Den Haag 1998.

Intveen, Carsten, Internationales Urheberrecht und Internet. Zur Frage des anzuwendenden Urheberrechts bei grenzüberschreitenden Datenübertragungen. Baden-Baden, 1999

Jaeger, Till, Die Erschöpfung des Verbreitungsrechts bei OEM-Software. Anmerkung zu den Urteilen des BGH vom 6.7.2000 – I ZR 244/97 (ZUM 2000, 1079) und des OLG Frankfurt am Main vom 18.5.2000 – 6 U 63/99 (ZUM 2000, 763). Zeitschrift für Urheber- und Medienrecht 2000, 1070 ff.

Jasay, Anthony de, Prisoners' Dilemma and the Theory of the State. In: Newman (Hrsg.), The New Palgrave Dictionary of Economics and the Law. London, 1998. Band 3, S. 95 ff.

Jiles, JeanAne Marie, Copyright Protection in the New Millennium: Amending the Digital Millennium Copyright Act to Prevent Constitutional Challenges. 52 Administrative Law Review 443 ff. (2000)

Johnson, David R./Post, David, Law and Borders – The Rise of Law in Cyberspace. 48 Stanford Law Review 1367 ff. (1996)

Johnson, Neil F., Steganalysis. In: Katzenbeisser/Petitcolas (Hrsg.), Information Hiding Techniques for Steganography and Digital Watermarking. Norwood, 2000. S. 79 ff.

Johnson, Neil F./Duric, Zoran/Jajodia, Sushil, Information Hiding: Steganography and Watermarking – Attacks and Countermeasures. Boston, 2001

Johnson, Neil F./Jajodia, Sushil, Exploring Steganography: Seeing the Unseen. IEEE Computer Februar 1998, 26 ff. Erhältlich unter <http://isse.gmu.edu/~njohnson/pub/r2026a.pdf>

Johnson, Neil F./Katzenbeisser, Stefan C., A Survey of Steganographic Techniques. In: Katzenbeisser/Petitcolas (Hrsg.), Information Hiding Techniques for Steganography and Digital Watermarking. Norwood, 2000. S. 43 ff.

Johnston, Jason Scott, Bargaining Under Rules Versus Standards. 11 Journal of Law, Economics, and Organization 256 ff. (1995)

Jolls, Christine/Sunstein, Cass R./Thaler, Richard, A Behavioral Approach to Law and Economics. 50 Stanford Law Review 1471 ff. (1998)

Junger, Peter D., The Illusion Vanishes. Draft Version 1.0; 8. 5. 2001. Online erhältlich unter <http://samsara.law.cwru.edu/dmca/qq.pdf>

Kaestner, Jan, Law and Technology Convergence: Intellectual Property Rights. ECLIP (Esprit Project 27028) Deliverable 2.2.2; 16. 12. 1999. <http://www.eclip.org/documents/deliverable_2_2_2_copyright.pdf>

Kahan, Marcel/Klausner, Michael, Standardization and Innovation in Corporate Contracting (Or „The Economics of Boilerplate"). 83 Virginia Law Review 713 ff. (1997)

Kahn, David, Cryptology and the origins of spread spectrum. 21 (9) IEEE Spectrum 70 ff. (1984)

Kaiser, Andreas/Voigt, Dennis, Vertragsabschluß und Abwicklung des Electronic Commerce im Internet – Chancen und Risiken. Kommunikation & Recht 1999, 445 ff.

Kaplow, Louis/Shavell, Steven, Do Liability Rules Facilitate Bargaining? A Reply to Ayres and Talley. 105 Yale Law Journal 221 ff. (1995)

dies., Property Rules and Liability Rules: An Economic Analysis. 109 Harvard Law Review 317 ff. (1996)

Karjala, Dennis S., Federal Preemption of Shrinkwrap and On-Line Licenses. 22 University of Dayton Law Review 511 ff. (1997)

Katz, Avery Wiener, Standard Form Contracts. In: Newman (Hrsg.), The New Palgrave Dictionary of Economics and the Law. London, 1998. Band 3. S. 502 ff.

Katz, Michael L./Shapiro, Carl, Network Externalities, Competition, and Compatibility. 75 American Economic Review 424 ff. (1985)

dies., Systems Competition and Network Effects. 8 (2) Journal of Economic Perspectives 93 ff. (1994)

Katzenbeisser, Stefan C., Principles of Steganography. In: Katzenbeisser/Petitcolas (Hrsg.), Information Hiding Techniques for Steganography and Digital Watermarking. Norwood, 2000. S. 17 ff.

Katzenbeisser, Stefan C./Petitcolas, Fabien A. P. (Hrsg.), Information Hiding Techniques for Steganography and Digital Watermarking. Norwood, 2000

Katzenberger, Paul, Elektronische Printmedien und Urheberrecht. Archiv für Presserecht 1997, 434 ff.

Kay, Alan/Goldberg, Adele, Personal Dynamic Media. 10 (3) IEEE Computer 31 ff. (March 1977)

Kelsey, John/Schneier, Bruce, Electronic Commerce and the Street Performer Protocol. 1998. Erhältlich unter <http://www.counterpane.com/street_performer.pdf>

Kent, Stephen/Atkinson, Randall, Security Architecture for the Internet Protocol. Request for Comments 2401, November 1998. <http://www.rfc-editor.org/rfc/rfc2401.txt>

Kephart, Jeffrey O./Hanson, James E./Greenwald, Amy R., Dynamic Pricing by Software Agents. 32 Computer Networks 731 ff. (2000)

Kesan, Jay P./Shah, Rajiv C., Fool Us Once Shame On You – Fool Us Twice Shame On Us: What We Can Learn From the Privitizations Of The Internet Backbone Network and the Domain Name System. University of Illinois Law & Economics Research Paper No. 00-18. 2001. Erhältlich unter <http://papers.ssrn.com/abstract=260834>. Erscheint in Washington University Law Quarterly (2001)

Kilian, Wolfgang, Elektronischer Datenaustausch. In: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch. Computertechnologie in der Rechts- und Wirtschaftspraxis. München, Loseblatt-Sammlung, Stand: 14. Ergänzungslieferung, September 1999. Kapitel 23

Kilian, Wolfgang/Picot, Arnold/Neuburger, Rahild/Niggl, Johann/Scholtes, Kay-Larsen/Seiler, Wolfgang, Electronic Data Interchange (EDI). Aus ökonomischer und juristischer Sicht. Forschungsbereicht zu dem von der Volkswagen-Stiftung geförderten Forschungsprojekt ELTRADO (Elektronische Transaktionen von Dokumenten zwischen Organisationen). Baden-Baden, 1994

Kirk, Ewan, Encryption and Competition in the Information Society. Intellectual Property Quarterly 1999, 37 ff.

Kirsch, Guy, Neue Politische Ökonomie. 4. Auflage, Düsseldorf 1997

Kitch, Edmund W., Elementary and Persistent Errors in the Economic Analysis of Intellectual Property. 53 Vanderbilt Law Review 1727 ff. (2000)

ders., The Nature and Function of the Patent System. 20 Journal of Law and Economics 265 ff. (1977)

Klausner, Michael, Corporations, Corporate Law, and Networks off Contracts. 81 Virginia Law Review 757 ff. (1995)

Kleinwächter, Wolfgang, ICANN als United Nations der Informationsgesellschaft? Der lange Weg zur Selbstregulierung des Internet. Multimedia und Recht 1999, 452 ff.

Klett, Alexander, Urheberrecht im Internet aus deutscher und amerikanischer Sicht. Baden-Baden, 1998

Kliege, Helmut, Rechtsprobleme der allgemeinen Geschäftsbedingungen in wirtschaftswissenschaftlicher Analyse unter besonderer Berücksichtigung der Freizeichnungsklauseln. Göttingen, 1966

Klusch, Matthias (Hrsg.), Intelligent Information Agents. Agent-Based Information Discovery and Management on the Internet. Berlin, 1999

Knorr, Michael/Schläger, Uwe, Datenschutz bei elektronischem Geld. Ist das Bezahlen im Internet anonym? Datenschutz und Datensicherheit 1997, 396 ff.

Koboldt, Christian, Property Rights und Urheberschutz. In: Ott/Schäfer (Hrsg.), Ökonomische Analyse der rechtlichen Organisation von Innovationen. Tübingen, 1994. S. 69 ff.

Koboldt, Christian/Schmidtchen, Dieter, Copyright: A und O in Literatur und Musik? Ordo 42 (1991), 295 ff.

Kocher, Paul C., Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: Koblitz (Hrsg.), Advances in Cryptology – Crypto 1998. 16th Annual International Cryptology Conference. 18.–22. 8. 1996, Santa Barbara, USA – Proceedings. Berlin, 1996. S. 104 ff.

Kocher, Paul C./Jaffe, Joshua/Jun, Benjamin, Differential Power Analysis. In: Wiener (Hrsg.), Advances in Cryptology – Crypto 1999. 19th Annual International Cryptology Conference. 15.–19. 8. 1999, Santa Barbara, USA – Proceedings. Berlin, 1999. S. 388 ff.

Kochinke, Clemens/Geiger, Matthias, Trend im US-Computer- und Internetrecht. Kommunikation & Recht 2000, 594 ff.

Kochinke, Clemens/Günther, Andreas, Shrinkwrap-Lizenzen und Datenbankschutz in den USA. Aktuelle Rechtsentwicklungen und UCC-Ergänzung. Computer und Recht 1997, 129 ff.

Koehler, Philipp, Der Erschöpfungsgrundsatz des Urheberrechts im Online-Bereich. München, 2000

Koelman, Kamiel J., A Hard Nut to Crack: The Protection of Technological Measures. European Intellectual Property Review 2000, 272 ff.

ders., The Protection of Technological Measures vs. the Copyright Limitations. Paper presented at the ALAI Congress, New York, 15. 6. 2001. Erhältlich unter <http://www.law.columbia.edu/conferences/2001/pres_koelman.doc>

Koelman, Kamiel J./Helberger, Natali, Protection of Technological Measures. In: Hugenholtz (Hrsg.), Copyright and Electronic Commerce. London, 2000. S. 165 ff.

Koenen, Rob, Intellectual Property Management and Protection in MPEG Standards. Dezember 2000. <http://www.w3.org/2000/12/drm-ws/pp/koenen.pdf>

ders., Multimedia for Our Time. IEEE Spectrum 26 ff. (Februar 1999)

Köhntopp, Marit/Kristian Köhntopp, Datenspuren im Internet. Computer und Recht 2000, 248 ff.

Koller, Ingo, Frachtenregelungen in Konditionenkartellen. Zeitschrift für das gesamte Handelsrecht und Wirtschaftsrecht 136 (1972), S. 139 ff.

Köndgen, Johannes, Grund und Grenzen des Transparenzgebots im AGB-Recht. Bemerkungen zum „Hypothekenzins-“ und zum „Wertstellungs-Urteil“ des BGH. Neue Juristische Wochenschrift 1989, 943 ff.

Kone, Mamadou Tadiou/Shimazu, Akira/Nakajima, Tatsuo, The State of the Art in Agent Communication Languages. 2 Knowledge and Information Systems 259 ff. (2000)

König, Michael, Zur Zulässigkeit der Umgehung von Software-Schutzmechanismen. Neue Juristische Wochenschrift 1995, 3293 ff.

Korobkin, Russell B./Ulen, Thomas S., Law and Behavioral Science: Removing the Rationality Assumption From Law and Economics. 88 California Law Review 1051 ff. (2000)

Koskinen-Olsson, Tanja, Rights Management Organizations in the Digital Era. In: Koskinen-Olsson/Gervais (Hrsg.), Electronic Commerce and Copyright: A Key Role for WIPO. Advisory Committee on Management of Copyright and Related Rights in Global Information Networks, Genf, 8.–9. 12. 1999. WIPO-Dokument ACMC/2/1 vom 17. 11. 1999, erhältlich unter <http://www.wipo.int/eng/meetings/1999/acmc/pdf/acmc_1.pdf>. S. 29 ff.

Kötz, Hein, Die ökonomische Analyse des Rechts. Zeitschrift für die gesamte Versicherungswissenschaft 1993, 57 ff.

ders., Welche gesetzgeberischen Maßnahmen empfehlen sich zum Schutze des Endverbrauchers gegenüber Allgemeinen Geschäftsbedingungen und Formularverträgen? (dargestellt an Beispielen aus dem Kauf- und Werkvertrags- sowie dem Maklerrecht). Gutachten für den 50. Deutschen Juristentag. In: Verhandlungen des Fünfzigsten Deutschen Juristentages, Hamburg 1974. Band I, Teil A. München, 1974

Kravitz, David/Goldschlag, David, Conditional Access Concepts and Principles. In: Franklin (Hrsg.), Financial Cryptography. Third International Conference, 22.–25. 3. 1999, Anguilla, British West Indies – Proceedings. Berlin, 1999. S. 158 ff.

Kravtsova, Natasha/Meyer, Andre, Searching for Music with Agents. In: Horlait (Hrsg.), Mobile Agents for Telecommunication Applications. Second International Workshop. 18.–20. 9. 2000, Paris – Proceedings. Berlin, 2000. S. 195 ff.

Kreile, Reinhold/Becker, Jürgen, Multimedia und die Praxis der Lizenzierung von Urheberrechten. GRUR Int. 1996, 677 ff.

Kreutzer, Till, Napster, Gnutella & Co.: Rechtsfragen zu Filesharing-Netzen aus der Sicht des deutschen Urheberrechts de lege lata und de lege ferenda. Teil 1: GRUR 2001, 193 ff. Teil 2: GRUR 2001, 307 ff.

Kröger, Detlef, Die Urheberrechtsrichtlinie für die Informationsgesellschaft – Bestandsaufnahme und kritische Bewertung. Computer und Recht 2001, 636 ff.

Kroon, Annemique M. E. de, Protection of Copyright Management Information. In: Hugenholtz (Hrsg.), Copyright and Electronic Commerce – Legal Aspects of Electronic Copyright Management. London, 2000. S. 229 ff.

Ku, Raymond, Open Internet Access and Freedom of Speech: A First Amendment Catch-22. 75 Tulane Law Review 87 ff. (2000)

Kuhlmann, Jan, Kein Rechtsschutz für den Kopierschutz? Standardsoftware in rechtlicher Sicht. Computer und Recht 1989, 177 ff.

Kuhn, Markus G./Anderson, Ross J., Soft Tempest: Hidden Data Transmission Using Electromagentic Emanations. In: Aucsmith (Hrsg.), Information Hiding. Second International Workshop. 14.–17. 4. 1998, Portland, USA – Proceedings. Berlin, 1998. S. 124 ff.

Kuhn, Matthias, Rechtshandlungen mittels EDV und Telekommunikation. Zurechenbarkeit und Haftung. München, 1991

Kühne, Eberhard, Verprechungen und Gegenstand. Ein Beitrag zum System der Belastung. Archiv für die civilistische Praxis 140 (1935), 1 ff.

Kulle, Jürgen, Ökonomie der Musikindustrie. Eine Analyse der körperlichen und unkörperlichen Musikverwertung mit Hilfe von Tonträgern und Netzen. Frankfurt, 1998

Kumazawa, Masayuki/Kamada, Hironori/Yamada, Atsushu/Hoshino, Hiroshi/Kambayashi, Yahiko/Mohania, Mukesh, Relationship among Copyright Holders for Use and Reuse of Digital Contents. In: Proceedings of the Fifth ACM Conference on Digital Libraries. 2.–7. 6. 2000, San Antonio, USA – Proceedings. New York, 2000. S. 254 ff.

Kuner, Christopher, Rechtsprobleme der Kryptographie. In: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht. München. Stand: 2. Ergänzungslieferung, Dezember 2000. Teil 17

Kunze, John A., Encoding Dublin Core Metadata in HTML. Request for Comments 2731, Dezember 1999. <http://www.rfc-editor.org/rfc/rfc2731.txt>

Kur, Annette, Metatags – pauschale Verurteilung oder differenzierende Betrachtung? Zugleich eine Stellungnahme zur „kennzeichenmäßigen Benutzung" im Lichte der EuGH-Rechtsprechung. Computer und Recht 2000, 448 ff.

Kurak, Charles/McHughes, John, A Cautionary Note On Image Downgrading. In: Proceedings of the Eighth IEEE Computer Security Applications Conference 1992. S. 153 ff.

Kutter, Martin/Hartung, Frank, Introduction to Watermarking Techniques. In: Katzenbeisser/Petitcolas (Hrsg.), Information Hiding Techniques for Steganography and Digital Watermarking. Norwood, 2000. S. 97 ff.

Lacoste, Gérard/Pfitzmann, Birgit/Steiner, Michael/Waidner, Michael (Hrsg.), SEMPER – Secure Electronic Marketplace for Europe. Berlin, 2000

Lacy, Jack/Rump, Niels/Kudumakis, Panos, MPEG-4 Intellectual Property Management & Protection (IPMP): Overview & Applications Document. Dokument ISO/IEC JTC1/SC29/WG11/N2614. Dezember 1998. <http://www.cselt.it/mpeg/public/mpeg-4_ipmp.zip>

Laddie, Hugh, Copyright: Over-Strength, Over-Regulated, Over-Rated. European Intellectual Property Review 1996, 253 ff.

Ladeur, Karl-Heinz, Datenverarbeitung und Datenschutz bei neuartigen Programmführern in „virtuellen Videotheken" – Zur Zulässigkeit der Erstellung von Nutzerprofilen. Multimedia und Recht 2000, 715 ff.

ders., Rechtliche Regulierung von Informationstechnologien und Standardsetzung. Das Beispiel der Set-Top-Box im digitalen Fernsehen. Computer und Recht 1999, 395 ff.

ders., Zur Notwendigkeit einer flexiblen Abstimmung von Bundes- und Landeskompetenzen auf den Gebieten des Telekommunikations- und des Rundfunkrechts. Das Beispiel des Fernsehsignalübertragungsgesetzes (FÜG) von 1997. Zeitschrift für Urheber- und Medienrecht 1998, 261 ff.

Lagoze, Carl, Keeping Dublin Core Simple. Cross-Domain Discovery or Resource Description? 7 (1) D-Lib Magazine (Januar 2001), erhältlich unter <http://www.dlib.org/dlib/january01/lagoze/01lagoze.html>

Lahore, James, Intellectual Property Rights and Unfair Copying: Old Concepts, New Ideas. European Intellectual Property Review 1992, 428 ff.

Lai, Stanley, Digital Copyright and Watermarking. European Intellectual Property Review 1999, 171 ff.

ders., The Impact of the Recent WIPO Copyright Treaty and Other Initiatives on Software Copyright in the United Kingkom. Intellectual Property Quarterly 1998, 35 ff.

Lai, Stanley/Buonaiuti, Fabrizio Marongiu, Copyright on the Internet and watermarking. In: Katzenbeisser/Petitcolas (Hrsg.), Information Hiding Techniques for Steganography and Digital Watermarking. Norwood, 2000. S. 191 ff.

Landes, William M./Posner, Richard A., An Economic Analysis of Copyright Law. 18 Journal of Legal Studies 325 ff.(1989)

Langelaar, Gerhard C./Setyawan, Iwan/Lagendijk, Reginald L., Watermarking Digital Image and Video Data. A State-of-the-Art Overview. IEEE Signal Processing Magazine September 2000, 20 ff.

Larenz, Karl, Methodenlehre der Rechtswissenschaft. 6. Auflage, Berlin 1991

Larenz, Karl/Wolf, Manfred, Allgemeiner Teil des Bürgerlichen Rechts. 8. Auflage, München 1997

Lassila, Ora, Web Metadata: A Matter of Semantics. IEEE Internet Computing Juli/August 1998, S. 30 ff.

Lassila, Ora/Swick, Ralph R., Resource Description Framework (RDF) Model and Syntax Specification. W3C Recommendation, 22 2. 1999. <http://www.w3.org/TR/REC-rdf-syntax>.

Lastowka, F. Gregory, Search Engines, HTML, and Trademarks: What's the Meta For? 86 Virginia Law Review 835 ff. (2000)

Lauktien, Annette-Tabea/Varadinek, Brigitta, Der Vertragsabschluss im Internet. Zeitschrift für Urheber- und Medienrecht 2000, 466 ff.

Lee, Jong-Hyeon, Fingerprinting. In: Katzenbeisser/Petitcolas (Hrsg.), Information Hiding Techniques for Steganography and Digital Watermarking. Norwood, 2000. S. 175 ff.

Lee, Narn-Yih/Chang, Chi-Chao/Lin, Chun-Li/Hwang, Tzonelih, Privacy and Non-Repudation on Pay-TV Systems. 46 IEEE Transactions on Consumer Electronics 20 ff. (2000)

Lehmann, Michael, Das neue Software-Vertragsrecht – Verkauf und Lizenzierung von Computerprogrammen. Neue Juristische Wochenschrift 1993, 1822 ff.

ders., Das Urhebervertragsrecht der Softwareüberlassung. In: Beier/Götting/Lehmann/Moufang Hrsg.), Urhebervertragsrecht. Festgabe für Gerhard Schricker zum 60. Geburtstag. München, 1995. S. 543 ff.

ders., Eigentum, geistiges Eigentum, gewerbliche Schutzrechte. Property Rights als Wettbewerbsbeschränkungen zur Förderung des Wettbewerbs. GRUR Int. 1983, 356 ff.

ders., Theorie der Property Rights und Schutz des geistigen und gewerblichen Eigentums – Wettbewerbsbeschränkungen zur Förderung des Wettbewerbs. In: Neumann (Hrsg.): Ansprüche, Eigentums- und Verfügungsrechte. Berlin, 1984. S. 519 ff.

Leinemann, Felix, Die Sozialbindung des „Geistigen Eigentums". Zu den Grundlagen der Schranken des Urheberrechts zugunsten der Allgemeinheit. Baden-Baden, 1998

Leistner, Matthias/Klein, Michèle, Anmerkung zu BGH, Urteil vom 6. 7. 2000, Az. I ZR 244/97 – OEM-Version. Multimedia und Recht 2000, 761 ff.

Lejeune, Mathias, UCITA – Recht der Informationsverträge. Computer und Recht 2000, 265 ff.

ders., UCITA – Vertragsrecht für „geistiges Eigentum" im E-Commerce-Zeitalter. Computer und Recht 2000, 201 ff.

ders., US-amerikanisches Vertragsrecht zur Lizenzierung „geistigen Eigentums". Kommunikation & Recht 1999, 210 ff.

Lemley, Mark A., Antitrust and the Internet Standardization Problem. 28 Connecticut Law Review 1041 ff. (1996)

ders., Beyond Preemption: The Law and Policy of Intellectual Property Licensing. 87 California Law Review 111 ff. (1999)

ders., Dealing with Overlapping Copyrights on the Internet. 22 University of Dayton Law Review 547 ff. (1997)

ders., Intellectual Property and Shrinkwrap Licenses. 68 Southern California Law Review 1239 ff. (1995)

ders., Private Property. 52 Stanford Law Review 1545 ff. (2000)

ders., Romantic Authorship and the Rhetoric of Property. Book Review of „Shamans, Software, and Spleens: Law and the Construction of the Information Society" by James Boyle. 75 Texas Law Review 873 ff. (1997)

ders., Shrinkwraps in Cyberspace. 35 Jurimetrics Journal 311 ff. (1995)

ders., The Economics of Improvement in Intellectual Property Law. 75 Texas Law Review 989 ff. (1997)

ders., The Law and Economics of Internet Norms. 73 Chicago-Kent Law Review 1257 ff. (1998)

Lemley, Mark A./Lessig, Lawrence, The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era. 48 UCLA Law Review 925 ff. (2001)

Lemley, Mark A./McGowan, David, Legal Implications of Network Economic Effects. 86 California Law Review 479 ff. (1998)

Lerouge, Jean-François, The Use of Electronic Agents Questioned Under Contractual Law: Suggested Solutions on a European and American Level. 18 John Marshall Journal of Computer and Information Law 403 ff. (1999)

Lessig, Lawrence, Code and Other Laws of Cyberspace. New York, 1999

ders., Commons and Code. 9 Fordham Intellectual Poperty Media & Entertainment Law Journal 405 ff. (1999)

ders., Expert Report im Fall A&M Records, Inc., v. Napster, Inc. Juni 2000. <http://cyberlaw.stanford.edu/lessig/content/works/napd3.pdf> und <http://dl.napster.com/lessig.pdf>

ders., Intellectual Property and Code. 11 St. John's Journal of Legal Commentary 635 ff. (1996)

ders., Reading the Constitution in Cyberspace. 45 Emory Law Journal 869 ff. (1996)

ders., The Law of the Horse: What Cyberlaw Might Teach. 113 Harvard Law Review 501 ff. (1999)

ders., The Limits in Open Code: Regulatory Standards and the Future of the Net. 14 Berkeley Technology Law Journal 759 ff. (1999)

ders., The New Chicago School. 27 Journal of Legal Studies 661 ff. (1998)

ders., The Path of Cyberlaw. 104 Yale Law Journal 1743 ff. (1995)

ders., What Things Regulate Speech. 38 Jurimetrics Journal 629 ff. (1998)

Levy, Daniel/Bergen, Mark/Dutta, Shantanu/Venable, Robert, The Magnitude of Menu Costs: Direct Evidence From Large U.S. Supermarket Chains. 112 The Quarterly Journal of Economics 791 ff. (1997)

Levy, Nichelle Nicholes, Method to Their Madness: The Secure Digital Music Initiative, a Law and Economics Perspective. 5 Virginia Journal of Law and Technology 12 ff. (2000)

Lewinski, Silke von, Der EG-Richtlinienvorschlag zum Urheberrecht und zu verwandten Schutzrechten in der Informationsgesellschaft. GRUR Int. 1998, 637 ff.

dies., Die diplomatische Konferenz der WIPO 1996 zum Urheberrecht und den verwandten Schutzrechten. GRUR Int. 1997, 667 ff.

dies., Die diplomatische Konferenz der WIPO 2000 zum Schutz der audiovisuellen Darbietungen. GRUR Int. 2001, 529 ff.

dies., WIPO-Verträge von 1996 und neuere europäische Entwicklungen. In: Hoeren/Sieber (Hrsg.), Handbuch Multimediarecht, München. Stand: 2. Ergänzungslieferung, Juli 2000. Teil 7.9

Lewinski, Silke von/Gaster, Jens. L., Die Diplomatische Konferenz der WIPO 1996 zum Urheberrecht und zu verwandten Schutzrechten. Zeitschrift für Urheber- und Medienrecht 1997, 607 ff.

Li, Xue/Ammar, Mostafa H./Paul, Sanjoy, Video Multicast over the Internet. IEEE Network März/April 1999, S. 46 ff.

Lieberman, Henry, Personal Assistants for the Web: A MIT Perspective. In: Klusch (Hrsg.), Intelligent Information Agents. Agent-Based Information Discovery and Management on the Internet. Berlin, 1999. S. 279 ff.

Liebowitz, Stan J., The Impact of Reprography on the Copyright System. Kanada, 1981. Online erhältlich unter <http://papers.ssrn.com/abstract= 250082>

Liebowitz, Stan J./Margolis, Stephen E., Network Externality: An Uncommon Tragedy. 8 (2) Journal of Economic Perspectives 133-150 (1994)

dies., Winners, Losers & Microsoft. Competition and Antitrust in High Technology. Oakland, 1999

Lin, Ching-Yung/Chang, Shih-Fu, Generating Robust Digital Signature for Image/Video Authentication. In: Dittmann/Wohlmacher/Horster/Steinmetz (Hrsg.), Multimedia and Security. Workshop at ACM Multimedia '98. September 12-13, 1998, Bristol, UK. GMD Report 41. Sankt Augustin, 1998. Online unter <http://www.gmd.de/publications/report/0041/Text.pdf>. S. 49 ff.

dies., Semi-Fragile Watermarking for Authenticating JPEG Visual Content. In: Wong/Delp (Hrsg.), SPIE International Conference on Security and Watermarking of Multimedia Contents II. 24.–26. 1. 2000, San Jose, USA – Proceedings. Bellingham, 2000. S. 140 ff.

Lin, Eugene T./Delp, Edward J., A Review of Fragile Image Watermarks. In: Dittmann/Nahrstedt/Wohlmacher (Hrsg.), Multimedia and Security. Workshop at ACM Multimedia '99. 30. 10.–5. 11. 1999, Orlando, USA. GMD Report 85. Sankt Augustin 2000. Online erhältlich unter <http://www.gmd.de/publications/report/0085/Text.pdf>. S. 47 ff.

Linnartz, Jean-Paul M. G., The „Ticket" Concept for Copy Control Based on Embedded Signalling. In: Quisquater/Deswarte/Meadows/Gollmann (Hrsg.), Computer Security – ESORICS 98. 5th European Symposium on Research in Computer Security. 16.–18. 8., 1998, Louvain-la-Neuve, Belgien – Proceedings. Berlin, 1998. S. 257 ff.

Lippert, Pascal, Filtersysteme zur Verhinderung von Urheberrechtsverletzungen im Internet. Funktionsweise, Anknüpfungspunkte, rechtliche Rahmenbedingungen. Computer und Recht 2001, 478 ff.

Litman, Jessica, Information Privacy/Information Property. 52 Stanford Law Review 1283 ff. (2000)

dies., The Exclusive Right to Read. 13 Cardozo Arts & Entertainment Law Journal 29 ff. (1994)

dies., The Tales that Article 2B Tells. 13 Berkeley Technology Law Journal 931 ff. (1998)

Loewenheim, Ulrich, Reichweite gesetzlicher Lizenzen bei Online-Produkten nach § 53 UrhG. In: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht. München. Stand: 2. Ergänzungslieferung, Dezember 2000. Teil 7.4

Lohse, Christina/Janetzko, Dietmar, Technische und juristische Regulationsmodelle des Datenschutzes am Beispiel von P3P. Computer und Recht 2001, 55 ff.

Loren, Lydia Pallas, Redefining the Market Failure Approach to Fair Use in an Era of Copyright Permission Systems. 5 Journal of Intellectual Property Law 1 ff. (1997)

Loshin, Pete, TCP/IP Clearly Explained. 3. Auflage, San Diego 1999

Lotspiech, Jeffrey, Copy Protection Feature Proposal. T13-Dokument E00148R3; 22. 1. 2001. <ftp://t13:$tandard$@ftp.t13.org/technical/e00148r3.pdf>

Lou, Stephen H./Maxemchuk, Nicholas F., Performance Comparison of Two Text Marking Methods. 16 IEEE Journal on Selected Areas in Communications 561 ff. (1998)

Luetteke, Georg, The DVB Multimedia Home Platform. 183 ABU Technical Review 183, 3 ff. (Juli/August 1999)

Lunney, Glynn S., Protecting Digital Works: Copyright or Contract. 1 Tulane Journal of Technology & Intellectual Property 1 (1999). Erhältlich unter <http://www.law.tulane.edu/JOURNALS/jtip/V1I1/copycon.htm>

dies., Reexamining Copyright's Incentives-Access Paradigm. 49 Vanderbilt Law Review 483 ff. (1996)

Lutzker, Gary S., DAT's All Folks: Cahn v. Sony and the Audio Home Recording Act of 1991 – Merrie Melodies or Looney Tunes? 11 Cardozo Arts & Entertainment Law Journal 145 ff. (1992)

Lynch, Clifford/Preston, Cecilia/Daniel, Ron Jr., Using Existing Bibliographic Identifiers as Uniform Resource Names. Request for Comments 2288, Februar 1998. <http://www.rfc-editor.org/rfc/rfc2288.txt>

Macq, Benoît M./Quisquater, Jean-Jacques, Cryptology for Digital TV Broadcasting. 83 Proceedings of the IEEE 944 ff. (1995)

Madison, Michael J., Legal-Ware: Contract and Copyright in the Digital Age. 67 Fordham Law Review 1025 ff. (1998)

Maes, Maurice/Klaker, Ton/Linnartz, Jean-Paul M. G./Talstra, Joop/Depovere, Geert F. G./Haitsma, Jaap, Digital Watermarking for DVD Video Copy Protection. What Issues Play a Role in Designing an Effective System? 17 (5) IEEE Signal Processing Magazine 47 ff. (September 2000)

Mahajan, Anthony J., Intellectual Property, Contracts, and Reverse Engineering After ProCD: A Proposed Compromise for Computer Software. 67 Fordham Law Review 3297 ff. (1999)

Major, April Mara, Norm Origin and Development in Cyberspace: Models of Cybernorm Evolution. 78 Washington University Law Quarterly 59 ff. (2000)

Mambo, Masahiro/Murayama, Takanori/Okamoto, Eiji , A Tentative Approach to Constructing Tamper-Resistant Software. In: Proceedings of the New Security Paradigms Workshop. 23.–26. 9. 1997, Langdale, UK. New York, 1998. S. 23 ff.

Manasse, Mark S., Why Rights Management is Wrong (and What to Do Instead). 2001. <http://www.w3.org/2000/12/drm-ws/pp/compaq.html>

Marchiori, Massimo, The Limits of Web Metadata, and Beyond. 30 Computer Networks and ISDN Systems 1 ff. (1998)

Margolis, Stephen E./Liebowitz, Stan J., Path Dependence. In: Newman (Hrsg.), The New Palgrave Dictionary of Economics and the Law. London, 1998. Band 3, S. 17 ff.

Marks, Dean S./Turnbull, Bruce H., Technical Protection Measures: The Intersection of Technology, Law and Commercial Licenses. European Intellectual Property Review 2000, 198 ff.

Marly, Jochen, Rechtsschutz für technische Schutzmechanismen geistiger Leistungen. Kommunikation & Recht 1999, 106 ff.

ders., Softwareüberlassungsverträge. 3. Auflage, München 2000

ders., Urheberrechtsschutz für Computersoftware in der Europäischen Union. Abschied vom überkommenen Urheberrechtsverständnis. München, 1995

Martinek, Michael, Moderne Vertragstypen. Band II: Franchising, Know-how-Verträge, Management- und Consultingverträge. München, 1992

Marvel, Lisa M./Hartwig, George W./Boncelet, Charles, Compression-Compatible Fragile and Semi-Fragile Tamper Detection. In: Wong/Delp (Hrsg.), SPIE International Conference on Security and Watermarking of Multimedia Contents II. 24.–26. 1. 2000, San Jose, USA – Proceedings. Bellingham, 2000. S. 131 ff.

Mashima, Rieko, Examination of the Interrelationship Among Japanese I.P. Protection for Software, the Software Industry, and Keiretsu. Part II. 82 Journal of the Patent and Trademark Office Society 203 ff. (2000)

dies., Examination of the Interrelationship Among the Software Industry Structure, Keiretsu, and Japanese Intellectual Property Protection for Software. 33 International Lawyer 119 ff. (1999)

Masson, Douglas J., Fixation on Fixation: Why Imposing Old Copyright Law on New Technology Will Not Work. 71 Indiana Law Journal 1049 ff. (1996)

Matheson, Lesley R./Mitchell, Stephen G./Shamoon, Talal/Tarjan, Robert Endre/Zane, Francis, Robustness and Security of Digital Watermarks. In: Hirschfeld (Hrsg.), Financial Cryptography. Second International Conference, 23.–25. 2. 1998, Anguilla, British West Indies. Berlin, 1998. S. 226 ff.

Matsui, Tatsuya/Takashima, Youichi, Technique for Searching Pirated Data. 11 NTT Review 134 ff. (1999)

Matsumoto, Tsuneo, Article 2B and Mass Market License Contracts: A Japanese Perspective. 13 Berkeley Technology Law Journal 1283 ff. (1998)

Matsuyama, Kazuo/Fujimura, Ko, Distributed Digital-Ticket Management for Rights Trading System. In: Proceedings of the First ACM Conference on Electronic Commerce. 3.–5. 11. 1999, Denver, USA. New York, 1999. S. 110 ff.

Mayer, Patrick G., Das Internet im öffentlichen Recht – unter Berücksichtigung europarechtlicher und völkerrechtlicher Vorgaben. Berlin, 1999

ders., Selbstregulierung im Internet: Institutionen und Verfahren zur Setzung technischer Standards. Kommunikation und Recht 2000, 13 ff.

McCuaig, Dan, Halve the Baby: An Obvious Solution to the Troubling Use of Trademarks as Metatags. 18 John Marshall Journal of Computer & Information Law 643 ff. (2000)

McKuin, Joel L., Home Audio Taping of Copyrighted Works and the Audio Home Recording Act of 1992: A Critical Analysis. 16 Hastings Communications and Entertainment Law Journal 311 ff. (1994)

McManis, Charles R., The Privatization (or „Shrink-Wrapping") of American Copyright Law. 87 California Law Review 173 ff. (1999)

McNutt, Patrick, Public Goods and Club Goods. In: Bouckaert/De Geest (Hrsg.), Encyclopedia of Law and Economics. Volume I: The History and Methodology of Law and Economics. Cheltenham, 2000. Kapitel 0750, S. 927 ff.

Mealling, Michael/Daniel, Ron, The Naming Authority Pointer (NAPTR) DNS Resource Record. Request for Comments 2915, September 2000. <http://www.rfc-editor.org/rfc/rfc2915.txt>

Medicus, Dieter, Allgemeiner Teil des BGB. Ein Lehrbuch. 7. Auflage, Heidelberg 1997

Mehrings, Josef, Vertragsabschluß im Internet. In: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht. München. Stand: 2. Ergänzungslieferung, Dezember 2000. Teil 13.1

Meier-Wahl, Marc/Wrobel, Ralph Michael, Wettbewerbsregulierung in einem dynamischen Markt – Der Fall Microsoft. Wirtschaft und Wettbewerb 1999, 28 ff.

Melichar, Ferdinand, Verwertungsgesellschaften und Multimedia. In: Lehmann (Hrsg.), Internet- und Multimediarecht (Cyberlaw). Stuttgart, 1997. S. 205 ff.

Menke, Burkhart, Die Verwendung fremder Kennzeichen in Meta-Tags: Ein Fall für das Kennzeichen- und/oder das Wettbewerbsrecht? Wettbewerb in Recht und Praxis 1999, 982 ff.

Mercer, Kell Corrigan, Consumer Shrink-wrap Licenses and Public Domain Materials; Copyright Preemption and Uniform Commercial Code Validity in ProCD v. Zeidenberg. 30 Creighton Law Review 1287 ff. (1997)

Merges, Robert P., A Comparative Look at Property Rights and the Software Industry. In: Mowery (Hrsg.), The International Computer Software Industry. A Comparative Study of Industry Evolution and Structure. New York, 1996. S. 272 ff.

ders., Are You Making Fun Of Me?: Notes on Market Failure and the Parody Defense in Copyright. 21 AIPLA Quarterly Journal 305 ff. (1993)

ders., Contracting into Liability Rules: Intellectual Property Rights and Collective Rights Organizations. 84 California Law Review 1293 ff. (1996)

ders., Intellectual Property and the Costs of Commercial Exchange: A Review Essay. 93 Michigan Law Review 1570 ff. (1995)

ders., Intellectual Property Rights and the New Institutional Economics. 53 Vanderbilt Law Review 1857 ff. (2000)

ders., The End of Friction? Property Rights and Contract in the „Newtonian" World of On-Line Commerce. 12 Berkeley Technology Law Journal 115 ff. (1997)

Mertes, Paul/Zeuner, Volker, Digitale Signatur und Signaturgesetz. In: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht. München. Stand: 2. Ergänzungslieferung, Dezember 2000. Teil 13.3

Messerschmitt, David G./Szyperski, Clemens, Industrial and Economic Properties of Software. Technology, Processes, and Value. 2000. <ftp://ftp.research.microsoft.com/pub/tr/tr-2001-11.pdf>

Mestmäcker, Ernst-Joachim, Unternehmenskonzentration und Urheberrechte in der alten und „neuen" Musikwirtschaft. Zeitschrift für Urheber- und Medienrecht 2001, 185 ff.

Metzger, Axel, Erschöpfung des urheberrechtlichen Verbreitungsrechts bei vertikalen Vertriebsbindungen. GRUR 2001, 210 ff.

Meurer, Michael J., Copyright Law and Price Discrimination. Erscheint in 22 Cardozo Law Review (2001). Erhältlich unter <http://papers.ssrn.com/abstract=274729>

ders., Price Discrimination, Personal Use and Piracy: Copyright Protection of Digital Works. 45 Buffalo Law Review 845 ff. (1997)

Meyer, Andreas, Die EG-Gruppenfreistellungsverordnung zum Technologietransfer. GRUR Int. 1997, 498 ff.

Meyerson, Michael I., The Efficient Consumer Form Contract: Law and Economics Meet the Real World. 24 Georgia Law Review 583 ff. (1990)

Middlebrook, Stephen T./Muller, John, Thoughts on Bots: The Emerging Law of Electronic Agents. 56 Business Lawyer 341 ff. (2000)

Minard, Nathalie, Copysmart: a Trusted Monitoring System for Electronic Works and Document. In: Rowland/Meadows (Hrsg.), Electronic Publishing '97 – New Models and Opportunities. Proceedings of an ICCC/IFIP Conference held at the University of Kent at Canterbury, England, 14-16 April 1997. S. 283 ff.

Minassian, Apik, The Death of Copyright: Enforceability of Shrinkwrap Licensing Agreements. 45 UCLA Law Review 569 ff. (1997)

Mintzer, Fred/Braudaway, Gordon W./Bell, Alan E., Opportunities for Watermarking Standards. 41 Communications of the ACM 57 ff. (Juli 1998)

Mitchell, William J., City of Bits: Space, Place, and the Infobahn. Cambridge, 1995

Mittra, Suvo, Iolus: A Framework for Scalable Secure Multicasting. In: Proceedings of the ACM SIGCOMM '97 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication. 14.–18. 9. 1997, Cannes, Frankreich. New York, 1997. S. 277 ff.

Moats, Ryan, URN Syntax. Request for Comments 2141, Mai 1997. <http://www.rfc-editor.org/rfc/rfc2141.txt>

Möhring, Philipp/Nicolini, Käte (Hrsg.), Urheberrechtsgesetz. Kommentar. 2. Auflage, München 2000

Möller, Erik, Schöner tauschen. Juni – August 2000. <http://www.telepolis.de/deutsch/inhalt/te/8449/1.html>

Monopolkommission, Marktöffnung umfassend verwirklichen. XII. Hauptgutachten 1996/1997. Baden-Baden, 1998

dies., Systemwettbewerb. Sondergutachten 27 der Monopolkommission gemäß § 24 b Abs. 5 Satz 4 GWB. Baden-Baden, 1998

dies., Wettbewerbspolitik in Netzstrukturen. XIII. Hauptgutachten 1998/1999. Baden-Baden, 2000

dies., Wettbewerbspolitik in Zeiten des Umbruchs. XI. Hauptgutachten 1994/1995. Baden-Baden, 1996

dies., Wettbewerbspolitik oder Industriepolitik. IX. Hauptgutachten 1990/1991. Baden-Baden, 1992

Monroe, Jerry David, ProCD, Inv. c. Zeidenberg: An Emerging Trend in Shrinkwrap Licensing? 1 Marquette Intellectual Property Law Review 143 ff. (1997)

Mooney, Stephen P., Interoperability – Digital Rights Management and the Emerging EBook Environment. 7 (1) D-Lib Magazine (January 2001), erhältlich unter <http://www.dlib.org/dlib/january01/mooney/01mooney.html>

Mori, Ryoichi/Kawahara, Masaji, Superdistribution: An Electronic Infrastructure for the Economy of the Future. 38 Transactions of the Information Processing Society of Japan 1465 ff. (1997)

dies., Superdistribution: The Concept and the Architecture. E 73 Transactions of the IEICE 1133 ff. (1990)

Moritz, Hans-Werner, Mängelgewährleistung bei Hard-/Software. In: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch. Loseblatt-Sammlung, München. Stand: 16. Ergänzungslieferung, Januar 2001

Möschel, Wernhard, Dogmatische Strukturen des bargeldlosen Zahlungsverkehrs. Archiv für die civilistische Praxis 186 (1986), 187 ff.

ders., Recht der Wettbewerbsbeschränkungen. Köln, 1983

Möschel, Wernhard/Bechtold, Stefan, Copyright-Management im Netz. Multimedia und Recht 1998, 571 ff.

dies., Digital Rights Management aus juristischer Sicht. Erscheint in: Pfitzmann/Roßnagel (Hrsg.), Urheberschutz und Nutzerschutz für die Informationsgesellschaft. Stuttgart, 2001

Mueller, Milton, Rough Justice – An Analysis of ICANN's Uniform Dispute Resolution Policy. Version 2.1; November 2000. <http://dcc.syr.edu/roughjustice.pdf>

Müller, Markus, Systemwettbewerb, Harmonisierung und Wettbewerbsverzerrung. Europa zwischen einem Wettbewerb der Gesetzgeber und vollständiger Harmonisierung. Baden-Baden, 2000

Mummenthey, Hinrich, US Guidelines für die Lizenzierung von geistigem Eigentum. Computer und Recht 1998, 113 ff.

Münch, Isabel, Sicherheitsanforderungen für Chipkartensysteme. In: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), Mit Sicherheit in die Informationsgesellschaft. 5. Deutscher IT-Sicherheitskongreß des BSI 1997 – Tagungsband. Ingelheim, 1997. S. 215 ff.

Münchener Kommentar , Münchener Kommentar zum Bürgerlichen Gesetzbuch. Band 1: Allgemeiner Teil (§§ 1-240), AGB-Gesetz. 4. Auflage, München 2001, Band 6: Sachenrecht (§§ 854-1296). 3. Auflage, München 1997

N. N., Developments in the Law – The Law of Cyberspace. 112 Harvard Law Review 1574 ff. (1999)

N. N., Franklin Pierce Law Center's Seventh Biennial Intellectual Property System Major Problems Conference – Digital Technology and Copyright: A Threat or a Promise? 39 IDEA: The Journal of Law & Technology 291 ff. (1999)

Nack, Frank/Lindsay, Adam T., Everything You Wanted to Know About MPEG-7: Part 1. IEEE Multimedia 65 ff. (Juli/September 1999)

Nadel, Mark S., Computer Code Vs. Legal Code: Setting the Rules in Cyberspace. 52 Federal Communications Law Journal 821 ff. (2000)

ders., The First Amendment's Limitations on the Use of Internet Filtering in Public and School Libraries: What Content Can Librarians Exclude? Fassung vom 24. 4. 2001. Online erhältlich unter <http://papers.ssrn.com/abstract=230834>. Frühere Fassung erschienen in 78 Texas Law Review 1117 ff. (2000)

Nakamura, Takao/Ogawa, Hiroshi/Takashima, Youichi, A Watermarking Technique for Still Images. 11 NTT Review 124 ff. (1999)

Naor, Moni/Pinkas, Benny, Threshold Traitor Tracing. In: Krawczyk (Hrsg.), Advances in Cryptology – Crypto 1998. 18th Annual International Cryptology Conference. 23.–27. 8. 1998, Santa Barbara, USA – Proceedings. Berlin, 1998. S. 502 ff.

National Research Council, The Digital Dilemma. Intellectual Property in the Information Age. Washington, 2000

Neff, Richard E./Smallson, Fran, NAFTA: Protecting and Enforcing Intellectual Property Rights in North America. New York, 1994

Negroponte, Nicholas, Being Digital. New York, 1995

Nelson, Theodor Holm, Literary Machines 93.1. Sausalito, 1993

ders., Transcopyright. Dealing with the Dilemma of Digital Copyright. 32 (1) Educom Review 32 ff. (1997)

Netanel, Neil Weinstock, Copyright and a Democratic Civil Society. 106 Yale Law Journal 283 ff. (1996)

ders., Cyberspace 2.0. 79 Texas Law Review 447 ff. (2000)

ders., Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory. 88 California Law Review 395 ff. (2000)

ders., From the Dead Sea Scrolls to the Digital Millenium – Recent Developments in Copyright Law. 9 Texas Intellectual Property Law Journal 19 ff. (2000)

Neumann, Danua, Die Rechtsnatur des Netzgeldes. Internetzahlungsmittel ecash. München, 2000

Nimmer, David, A Riff on Fair Use in the Digital Millenium Copyright Act. 148 University of Pennsylvania Lew Review 673 ff. (2000)

ders., Aus der Neuen Welt. 93 Northwestern University Law Review 195 ff. (1998)

ders., Puzzles of the Digital Millenium Copyright Act. 16 Journal of the Copyright Society of the U.S.A. 401 ff. (1999)

Nimmer, David/Brown, Elliot/Frischling, Gary N., The Metamorphosis of Contract into Expand. 87 California Law Review 17 ff. (1999)

Nimmer, Nelville B./Nimmer, David, Nimmer on Copyright. Loseblatt-Sammlung. Stand: 50. Ergänzungslieferung, Dezember 1999

Nimmer, Raymond T., Electronic Commerce Fundamentals. The U.S. Perspective. Computer und Recht international 2000, 97 ff.

ders., Images and Contract Law – What Law Applies to Transactions in Information. 36 Houston Law Review 1 ff. (1999)

ders., Information Law. Loseblatt-Sammlung, Boston. Stand: 2000 Cumulative Supplement Nr. 3

Nordemann, Axel/Goddar, Heinz/Tönhardt, Marion/Czychowski, Christian, Gewerblicher Rechtsschutz und Urheberrecht im Internet. Computer und Recht 1996, 645 ff.

Noriega, Pablo/Sierra, Carles, Auctions and Multi-agent Systems. In: Klusch (Hrsg.), Intelligent Information Agents. Agent-Based Information Discovery and Management on the Internet. Berlin, 1999. S. 153 ff.

Northeast Consulting, Digital Rights Management Technologies. Oktober 1995. Früher erhältlich unter <http://www.ncri.com/articles/rights_management/ifrro95.html>

Nunziato, Dawn C., Exit, Voice, and Values on the Net. 15 Berkeley Technology Law Journal 753 ff. (2000)

Nwana, Hyacinth S./Ndumu, Divine T., A Perspective on Software Agents Research. 14 (2) The Knowledge Engineering Review 1 ff. (1999)

O'Mahoney, Donal/Peirce, Michael/Tewari, Hitesh, Electronic Payment Systems. Boston, 1997

O'Rourke, Maureen A., Copyright Preemption after the ProCD Case: A Market-Based Approach. 12 Berkeley Technology Law Journal 53 ff. (1997)

dies., Drawing the Boundary Between Copyright and Contract: Copyright Preemption of Software License Terms. 45 Duke Law Journal 479 ff. (1995)

dies., Fencing Cyberspace: Drawing Borders in a Virtual World. 82 Minnesota Law Review 609 ff. (1998)

dies., Progressing Towards a Uniform Commercial Code for Electronic Commerce or Racing Towards Nonuniformity? 14 Berkeley Technology Law Journal 635 ff. (1999)

dies., Shaping Competition on the Internet: Who Owns Product and Pricing Information? 53 Vanderbilt Law Review 1965 ff. (2000)

Ohbuchi, Ryutarou/Masudo, Hiroshi/Aono, Masaki, Watermarking Three-Dimensional Polygonal Models Through Geometric and Topological Modifications. 16 IEEE Jounal on Selected Areas in Communications 551 ff. (1998)

Olswang, Simon, Accessright: An Evolutionary Path for Copyright into the Digital Era? European Intellectual Property Review 1995, 215 ff.

Oram, Andy, Gnutella and Freenet Represent True Technological Innovation. Mai 2000. <http://www.oreillynet.com/pub/a/network/2000/05/12/magazine/gnutella.html>

Oram, Andy (Hrsg.), Peer-to-Peer. Harnessing the Benefits of a Disruptive Technology. Sebastopol, 2001

Pahud, Eric, Zur Begrenzung des Urheberrechts im Interesse Dritter und der Allgemeinheit. UFITA 2000, 99 ff.

Palandt, Otto (Begr.), Bürgerliches Gesetzbuch. Kommentar. 59. Auflage, München 2000

Palmer, Tom G., Intellectual Property: A Non-Posnerian Law and Economics Approach. 12 Hamline Law Review 261 ff. (1989)

Papaioannou, Todd, Mobile Information Agents for Cyberspace – State of the Art and Visions. In: Klusch/Kerschberg (Hrsg.), Cooperative Information Agents IV (CIA 2000). The Future of Information Agents in Cyberspace. Fourth International Workshop. 7.–9. 7. 2000, Boston, USA – Proceedings. Berlin, 2000. S. 247 ff.

Parisi, Francesco/Depoorter, Ben/Schulz, Norbert, Duality in Property: Commons and Anticommons. 2000. Erhältlich unter <http://papers.ssrn.com/abstract=224844>

Parker, Geoffrey G./Van Alstyne, Marshall W., InterNetwork Externalities and Free Information Goods. In: Proceedings of the 2nd ACM Conference on Electronic Commerce. 17.–20. 10. 2000, Minneapolis. New York, 2000. S. 107 ff.

Paskin, Norman, The DOI Handbook. Version 0.5.1; 11. 8. 2000. <http://www.doi.org/handbook_2000/DOIHandbookv0.5.1.pdf>

ders., Toward Unique Identifiers. 87 Proceedings of the IEEE 1208 ff. (1999)

Patterson, L. Ray/Lindberg, Stanley W., The Nature of Copyright: A Law of Users' Rights. Athens, 1991

Patterson, Mark R., On the Impossibility of Information Intermediaries. Fordham University School of Law, Law and Economics Research Paper No. 13, Juli 2001. Erhältlich unter <http://papers.ssrn.com/abstract=276968>

Paylago, Stanley U., Search Engine Manipulation: Creative Use of Metatags or Trademark Infringement? 40 IDEA: The Journal of Law & Technology 451 ff. (2000)

Pereira, Fernando, MPEG-4: Why, what, how and when? 15 Signal Processing: Image Communications 271 ff. (2000)

ders., MPEG-7 Requirements Document V.12. Dokument ISO/IEC JTC1/SC29/WG11/n3548.Juli 2000. <http://www.cselt.it/mpeg/public/mpeg-7_requirements.zip>

Perlman, Harvey S., Taking the Protection-Access Tradeoff Seriously. 53 Vanderbilt Law Review 1831 ff. (2000)

Perritt, Henry H., Hybrid International Institutions for Regulation Electronic Commerce and Political Discourse on the Internet. Multimedia und Recht, Beilage zu Heft 7/2000, S. 1 ff.

ders., Property and Innovation in the Global Information Infrastructure. 1996 University of Chicago Legal Forum 261 ff.

Petersen, Holger, Anonymes elektronisches Geld. Der Einfluß der blinden Signatur. Datenschutz und Datensicherheit 1997, 403 ff.

Peterson, Roger L./Ziemer, Rodger E./Borth, David E., Introduction to Spread-Spectrum Communications. Upper Saddle River, 1995

Pethig, Rüdiger, Copyrights and Copying Costs: A New Price-Theoretic Approach. 144 Journal of Institutional and Theoretical Economics 462 ff. (1988)

Petitcolas, Fabien A. P., Introduction to Information Hiding. In: Katzenbeisser/Petitcolas (Hrsg.), Information Hiding Techniques for Steganography and Digital Watermarking. Norwood, 2000. S. 1 ff.

Petitcolas, Fabien A. P./Anderson, Ross J., Evaluation of Copyright Marking Systems. In: Proceedings of the IEEE International Conference on Multimedia Computing & Systems (ICMCS). 7.–11. 6. 1999, Florenz. Los Alamitos, 1999. Band 1, S. 574 ff.

Petitcolas, Fabien A. P./Anderson, Ross J./Kuhn, Markus G., Information Hiding – A Survey. 87 Proceedings of the IEEE 1062 ff. (1999)

dies., Attacks on Copyright Marking Systems. In: Aucsmith (Hrsg.), Information Hiding. Second International Workshop. 14.–17. 4. 1998, Portland, USA – Proceedings. Berlin, 1998. S. 218 ff.

Pfitzmann, Andreas, Datenschutz durch Technik. Vorschlag für eine Systematik. Datenschutz und Datensicherheit 1999, 405 ff.

Pfitzmann, Birgit, Trials of Traced Traitors. In: Anderson (Hrsg.), Information Hiding – First International Workshop. 30. 5. – 1. 6. 1996, Cambridge, UK. Berlin, 1996. S. 49 ff.

Pfitzmann, Birgit/Sadeghi, Ahmad-Reza, Anonymous Fingerprinting with Direct Nonrepudiation. In: Okamoto (Hrs.g), Advances in Cryptology – ASIACRYPT 2000. 6th International Conference on the Theory and Application of Cryptology and Information Security. 3.–7. 12. 2000, Kyoto, Japan – Proceedings. Berlin, 2000. S. 404 ff.

dies., Coin-Based Anonymous Fingerprinting. In: Stern (Hrsg.), Advances in Cryptology – Eurocrypt '99. International Conference on the Theory and Application of Cryptographic Techniques. 2.–6. 5. 1999, Prag – Proceedings. Berlin, 1999. S. 150 ff.

Pfitzmann, Birgit/Schunter, Matthias, Asymmetric Fingerprinting. In: Maurer (Hrsg.), Advances in Cryptology. Eurocrypt 1996: International Conference on the Theory and Application of Cryptographic Techniques. 12.–16. 5. 1996, Saragossa, Spanien – Proceedings. Berlin, 1996. S. 84 ff.

Pfitzmann, Birgit/Waidner, Michael, Anonymous Fingerprinting. In: Fumy (Hrsg.,) Advances in Cryptology – Eurocrypt 1997. International Conference on the Theory and Application of Cryptographic Techniques. 11.–15. 5. 1997, Konstanz – Proceedings. Berlin, 1997. S. 88 ff.

dies., Kopierschutz durch asymmetrisches Fingerprinting. Datenschutz und Datensicherheit 1998, 258 ff.

Pfitzmann, Birgit/Waidner, Michael/Pfitzmann, Andreas, Rechtssicherheit trotz Anonymität in offenen digitalen Systemen. Teil 1: Datenschutz und Datensicherheit 1990, 243 ff. Teil 2: Datenschutz und Datensicherheit 1990, 305 ff.

Phipps, John, Physical Protection Devices. In: Grover (Hrsg.), The Protection of Computer Software – Its Technology and Applications. 2. Auflage, Cambridge 1992. S. 66 ff.

Pichler, Rufus, Rechtsnatur, Rechtsbeziehungen und zivilrechtliche Haftung beim elektronischen Zahlungsverkehr im Internet. Münster, 1998

Piepenbrock, Hermann-Josef/Schmitz, Peter, Fernabsatzgesetz: Neuer Rechtsrahmen für E-Commerce. Kommunikation & Recht 2000, 378 ff.

Pieprzyk, Josef, Fingerprints for Copyright Software Protection. In: Mambo/Zheng (Hrsg.), Information Security. Second International Workshop. 6.–7. 11. 1999, Kuala Lumpur – Proceedings. Berlin, 1999. S. 178 ff.

Pindyck, Robert S./Rubinfeld, Daniel L., Microeconomics. 5. Auflage, Upper Saddle River 2001

Piscitelli, Michael, Home Satellite Viewing: A Free Ticket to the Movies? 35 Federal Communications Law Journal 1 ff. (1983)

Poggi, Christopher T., Electronic Commerce Legislation: An Analysis of European and American Approaches to Contract Formation. 41 Virginia Journal of International Law 224 ff. (2000)

Pohlmann, Ken C., Principles of Digital Audio. 4. Auflage, New York 2000

Pollack, Malla, The Right to Know?: Delimiting Database Protection at the Juncture of the Commerce Clause, the Intellectual Property Clause, and the First Amendment. 17 Cardozo Arts & Entertainment Law Journal 47 ff. (1999)

Polley, Romina, Verwendungsbeschränkungen in Softwareüberlassungsverträgen. Computer und Recht 1999, 345 ff.

Portin, Susan C., Pay TV-Piracy and the Law: It's Time to Clear up the Confusion. 33 Emory Law Journal 825 ff. (1984)

Posner, Richard A., Antitrust in the New Economy. 2001. <http://papers.ssrn.com/abstract=249316>

ders., Economic Analysis of Law. 5. Auflage, New York, 1998

ders., When is Parody Fair Use? 21 Journal of Legal Studies 67 ff. (1992)

Post, David G., What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace. 52 Stanford Law Review 1439 ff. (2000)

Pres, Andreas, Gestaltungsformen urheberrechtlicher Softwarelizenzverträge. Eine juristische und ökonomische Untersuchung unter besonderer Berücksichtigung des Zweiten Gesetzes zur Änderung des Urheberrechtsgesetzes vom 9. Juni 1993. Köln, 1994

Prescott, Peter, Was Autocad Wrongly Decided? European Intellectual Property Review 1992, 191 ff.

PricewaterhouseCoopers, Metadata Watch Report #1. SCHEMAS Deliverable D22. Juni 2000. <http://www.schemas-forum.org/metadata-watch/1.pdf>

dass., Metadata Watch Report #2. SCHEMAS Deliverable D23. September 2000. <http://www.schemas-forum.org/metadata-watch/2.pdf>.

dass., Standards Framework Report 1. SCHEMAS Deliverable D32. September 2000. <http://www.schemas-forum.org/stds-framework/1.pdf>

Radin, Margeret Jane, Humans, Computers, and Binding Commitment. 75 Indiana Law Journal 1125 ff. (2000)

Radin, Margeret Jane/Wagner, R. Polk, The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace. 73 Chicago-Kent Law Review 1295 ff. (1998)

Raiser, Thomas, Das lebende Recht. Rechtssoziologie in Deutschland. 3. Auflage, Baden-Baden 1999

Ramanujapuram, Arun/Ram, Prasad, Digital Content & Intellectual Property Rights. Dr. Dobb's Journal, Dezember 1998, S. 20 ff.

Rankl, Wolfgang/Effing, Wolfgang, Handbuch der Chipkarten. Aufbau – Funktionsweise – Einsatz von Smart Cards. 3. Auflage, München 1999

Raubenheimer, Andreas, Beseitigung/Umgehung eines technischen Programmschutzes nach UrhG und UWG. Computer und Recht 1996, 96 ff.

ders., Die jüngste Rechtsprechung zur Umgehung/Beseitigung eines Dongles. Zugleich eine Analyse des Urteils des OLG Karlsruhe (6 U 40/95) vom 10. 1. 1996. NJW-Computerreport 1996, 174 ff.

ders., Softwareschutz nach den Vorschriften des UWG. Computer und Recht 1994, 264 ff.

ders., Vernichtungsanspruch gemäß § 69 f UrhG. Computer und Recht 1994, 129 ff.

Raue, Peter/Hegemann, Jan, Sonstige gesetzliche Lizenzen bei Online-Produkten. In: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht. München. Stand: 2. Ergänzungslieferung, Dezember 2000. Teil 7.5

Reagle, Joseph M., XML Signature Requirements. Request for Comments 2807, July 2000. <http://www.rfc-editor.org/rfc/rfc2807.txt>

Rehbinder, Manfred, Urheberrecht. Ein Studienbuch. 11. Auflage, München 2001

Rehbinder, Manfred/Schmaus, Stefan, Rechtsprobleme beim Vertragsschluß im Internet. UFITA 2000, 313-351

Reichman, J. H./Samuelson, Pamela, Intellectual Property Rights in Data? 50 Vanderbilt Law Review 51 ff. (1997)

Reichman, Jerome H./Franklin, Jonathan A., Privately Legislated Intellectual Property Rights: Reconciling Freedom of Contract with Public Good Uses of Information. 87 California Law Review 875 ff. (1999)

Reidenberg, Joel R., Governing Networks and Rule-Making in Cyberspace. 45 Emory Law Journal 911 ff. (1996)

ders., Lex Informatica: The Formulation of Information Policy Rules Through Technology. 76 Texas Law Review 553 ff. (1998)

Reimann, Mathias, Einführung in das US-amerikanische Privatrecht. München, 1997

Reimers, Ulrich, Ein Führer durch die Welt der DVB-Spezifikationen und Normen. Fernseh- und Kino-Technik 52 (1998), 82 ff.

Reinbothe, Jörg, Geistiges Eigentum und die Europäische Gemeinschaft. Zeitschrift für Europäisches Privatrecht 2000, 5 ff.

Rice, David A., Digital Information as Property and Product: U.C.C. Article 2B. 22 University of Dayton Law Review 622 ff. (1997)

ders., Public Goods, Private Contract and Public Policy: Federal Preemption of Software License Prohibitions Against Reverse Engineering. 53 University of Pittsburgh Law Review 543 ff. (1992)

Richter, Rudolf/Furubotn, Eirik G., Neue Institutionenökonomik. 2. Auflage, Tübingen 1999

Rieder, Christian, Copyrightverletzungen in der Online-Kommunikation nach US-amerikanischem Recht. Köln, 2000

Roche, Stéphane/Dugelay, Jean-Luc/Molva, Refik, Multi-Resolution Access Control Algorithm Based on Fractal Coding. In: Proceedings of the International Conference on Image Processing (ICIP). 16.–19. 9. 1996, Lausanne. Piscataway, 1996. Band 3, S. 235 ff.

Roditti, Esther C., Is Self-Help a Lawful Contractual Remedy? 21 Rutgers Computer and Technology Law Journal 431 ff. (1995)

Ronit, Karsten/Schneider, Volker, Global Governance through Private Organizations. 12 Governance 243 ff. (1999)

Rosenschein, Jeffrey S./Zlotkin, Gilad, Rules of Encounter. Designing Conventions for Automated Negotiation among Computers. Cambridge, 1994

Rosenthal, Michael, Der aktuelle Rechtsrahmen für digitales Fernsehen in den USA. RTkom 2000, 182 ff.

Roßnagel, Alexander, Globale Datennetze: Ohnmacht des Staates – Selbstschutz der Bürger. Zeitschrift für Rechtspolitik 1997, 26 ff.

ders., Rechtswissenschaftliche Technikfolgenforschung – am Beispiel der Informations- und Kommunikationstechniken. In: Schulte (Hrsg.), Technische Innovation und Recht – Antrieb oder Hemmnis? Heidelberg, 1997. S. 139 ff.

ders., Regulierung und Selbstregulierung im Datenschutz. In: Kubicek/Braczyk/Klumpp/Roßnagel: Global@home – Informations- und Dienstleistungsstrukturen der Zukunft. Jahrbuch der Telekommunikation und Gesellschaft 2000. Heidelberg, 2000. S. 385 ff.

Roßnagel, Alexander/Scholz, Philip, Datenschutz durch Anonymität und Pseudonymität. Rechtsfolgen der Verwendung anonymer und pseudonymer Daten. Multimedia und Recht 2000, 721 ff.

Roth, Wulf-Henning, Das Allgemeininteresse im europäischen Internationalen Versicherungsvertragsrecht. Versicherungsrecht 1993, 129 ff.

Rubin, Aviel A., Trusted Distribution of Software Over the Internet. In: Proceedings of the Internet Society Symposium on Network and Distributed System Security. 16.–17. 2. 1995, San Diego, USA. Los Alamitos, 1995. S. 47 ff.

Rubinfeld, Daniel, Wettbewerb, Innovation und die Durchsetzung des Kartellrechts in dynamischen, vernetzten Industrien. GRUR Int. 1999, 479 ff.

Rudin, John F., E-Business, E-Commerce & the Law. 7 Richmond Journal of Law & Technology 13 (Symposium 2000). Erhältlich unter <http://www.richmond.edu/jolt/v7i2/rudin.html>

Rump, Niels, Copyright Protection of Multimedia Data: The „Multimedia Protection Protocol" (MMP). Unveröffentlichtes Manuskript, 27. November 1997

Rust, Godfrey/Bide, Mark, The <indecs> metadata framework. Principles, model and data dictionary. Juni 2000. <http://www.indecs.org/pdf/schema.pdf>

Saarela, Janne, The Role of Metadata in Electronic Publishing. Acta Polytechnica Scandinavica – Mathematics and Computing Series No. 102, Espoo, Finnland 1999; zugleich: Diss. Helsinki, 1999

Sahasrabuddhe, Laxman H./Mukherjee, Biswanath, Multicast Routing Algorithms and Protocols: A Tutorial. 14 (1) IEEE Network 90 ff. (Januar/Februar 2000)

Salter, Liora, The Standards Regime for Communication and Information Technologies. In: Cutler/Haufler/Porter (Hrsg.), Private Authority and International Affairs. Albany, 1999. S. 97 ff.

Samuelson, Pamela, Intellectual Property and Contract Law for the Information age: Foreword to a Symposium. 87 California Law Review 1 ff. (1999)

dies., Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised. 14 Berkeley Technology Law Journal 504 ff. (1999)

dies., Privacy as Intellectual Property? 52 Stanford Law Review 1125 ff. (2000)

dies, The U.S. Digital Agenda at WIPO. 37 Virginia Journal of International Law 358 ff. (1997)

Samuelson, Pamela/Glushko, Robert J., Intellectual Property Rights for Digital Library and Hypertext Publishing Systems. 6 Harvard Journal of Law & Technology 237 ff. (1993)

Sander, Tomas, Golden Times for Digital Rights Management? Unveröffentlichtes Manuskript, 2001. Erscheint in gekürzter Fassung in den Proceedings zur Finanial Cryptography, Fifth International Conference, 19.–22. 2. 2001, Grand Cayman, British West Indies

Sander, Tomas/Tschudin, Christian F., On Software Protection via Function Hiding. In: Aucsmith (Hrsg.), Information Hiding. Second International Workshop. 14.–17. 4. 1998, Portland, USA – Proceedings. Berlin, 1998. S. 111 ff.

dies., Towards Mobile Cryptography. In: Proceedings of the IEEE Symposium on Security and Privacy 1998. 3.–6. 5. 1998, Oakland, USA. Los Alamitos, 1998. S. 215 ff.

Sandholm, Tuomas, Agents in Electronic Commerce: Component Technologies for Automated Negotiation and Colation Formation. In: Klusch/Weiß (Hrsg.), Cooperative Information Agents II (CIA 1998). Learning, Mobility and Electronic Commerce for Information Discovery on the Internet. Second International Workshop. 4.–7. 6. 1998, Paris – Proceedings. Berlin, 1998. S. 113 ff.

Sather, Robert, Disk-Based Protection Methods. In: Grover (Hrsg.), The Protection of Computer Software – Its Technology and Applications. 2. Auflage, Cambridge 1992. S. 26 ff.

Sayood, Khalid, Introduction to Data Compression. 2. Auflage, San Francisco 2000

Schack, Haimo, Europäisches Urheberrecht im Werden. Zeitschrift für Europäisches Privatrecht 2000, 799 ff.

ders., Neue Techniken und Geistiges Eigentum. Juristen-Zeitung 1998, 753 ff.

ders., Urheber- und Urhebervertragsrecht. 2. Auflage, Tübingen 2001

Schäfer, Hans-Bernd/Ott, Claus, Lehrbuch der ökonomischen Analyse des Zivilrechts. 3. Auflage, Berlin 2000

Schallop, Michael J., The IPR Paradox: Leveraging Intellectual Property Rights to Encourage Interoperability in the Network Computing Age. 28 AIPLA Quarterly Journal 195 ff. (2000)

Schechter, Stuart E./Parnell, Todd C./Hartemink, Alexander J., Anonymous Authentication of Membership in Dynamic Groups. In: Franklin (Hrsg.), Financial Cryptography. Third International Conference, 22.–25. 3. 1999, Anguilla, Britisch West Indies – Proceedings. Berlin, 1999. S. 184 ff.

Scheffler, Hauke/Dressel, Christian, Die Insuffizienz des Computerstrafrechts. Schleppende Gesetzgebungsverfahren als Störfaktor für die E-Commerce-Wirtschaft. Zeitschrift für Rechtspolitik 2000, 514 ff.

Schindler, Werner, Kryptographie bei Chipkartensystemen – Einfälle und Reinfälle. In: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), Mit Sicherheit in die Informationsgesellschaft. 5. Deutscher IT-Sicherheitskongreß des BSI 1997 – Tagungsband. Ingelheim, 1997. S. 241 ff.

Schippan, Martin, Die Harmonisierung des Urheberrechts in Europa im Zeitalter von Internet und digitaler Technologie. Eine Betrachtung aus deutscher Sicht. Baden-Baden, 1999

ders., Die Klärung von „Multimediarechten" in Europa – das VERDI-Projekt und andere von der EU-Kommission unterstütze MMRCS-Projekte. Zeitschrift für Urheber- und Medienrecht 1999, 135 ff.

ders., Purchase and Licensing of Digital Rights: The VERDI Project and the Clearing of Multimedia Rights in Europe. European Intellectual Property Review 2000, 24 ff.

Schlachter, Eric, The Intellectual Property Renaissance in Cyberspace: Why Copyright Law Could Be Unimportant on the Internet. 12 Berkeley Technology Law Journal 15 ff. (1997)

Schmidt, Ingo, Wettbewerbspolitik und Kartellrecht. 6. Auflage, Stuttgart 1999

Schneck, Paul B., Persistent Access Control to Prevent Piracy of Digital Inforation. 87 Proceedings of the IEEE 1239 ff. (1999)

Schneider, Doris Annette, Vertragsschluß bei Schutzhüllenverträgen. Computer und Recht 1996, 657 ff.

Schneider, Marc/Chang, Shih-Fu, A Robust Content Based Digital Signature for Image Authentication. In: Proceedings of the International Conference on Image Proceesing (ICIP). 16.–19. 9. 1996, Lausanne. Piscataway, 1996. Band 3, S. 227 ff.

Schneier, Bruce, Applied Cryptography. 2. Auflage, New York 1996

Schöfisch, Volker, Konsequenzen aus der EU-Richtlinie zum Urheberrecht für die innerstaatliche Umsetzung. In: Prütting/Reinbothe/Schöfisch/Becker/Junker/Gerth/Schaefer, Die Entwicklung des Urheberrechts im europäischen Rahmen. München, 1999. S. 23 ff.

Schönherr, Fritz, Zur Begriffsbildung im Immaterialgüterrecht. In: Brügger (Hrsg.), Homo Creator. Festschrift für Alois Troller. Basel, 1976. S. 57 ff.

Schricker, Gerhard, Urheberrecht zwischen Industrie- und Kulturpolitik. GRUR 1992, 242 ff.

ders., Verlagsrecht. Kommentar zum Gesetz über das Verlagsrecht vom 19. 6. 1901. 3. Auflage, München 2001

ders. (Hrsg.), Urheberrecht auf dem Weg zur Informationsgesellschaft. Baden-Baden, 1997

ders. (Hrsg.), Urheberrecht. Kommentar. 1. Auflage, München 1987 (zit.: Schricker (Hrsg.), UrhG-Kommentar, 1. Aufl.)

ders. (Hrsg.), Urheberrecht. Kommentar. 2. Auflage, München 1999 (zit.: Schricker (Hrsg.), UrhG-Kommentar)

Schuhmacher, Dirk, Wirksamkeit von typischen Klauseln in Softwareüberlassungsverträgen. Computer und Recht 2000, 641 ff.

Schulz, Wolfgang/Leopoldt, Swaantje, Horizontale Regulierung? Im Blickpunkt: Inhaltedienste- und Infrastruktur-Regulierung in den Richtlinienvorschlägend er Kommission zum Rechtsrahmen für elektronische Kommunikationsnetze und dienste. Kommunikation und Recht 2000, 439 ff.

Schwartz, Paul M., Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices. 2000 Wisconsin Law Review 743 ff.

Schwartz, Paul M./Reidenberg, Joel R., Data Privacy Law – A Study of United States Data Protection. Charlottesville, 1996

Schwarz, Mathias, Urheberrecht und unkörperliche Verbreitung multimedialer Werke. GRUR 1996, 836 ff.

Schwenk, Jörg, „Conditional Access" oder Wie kann man den Zugriff auf Rundfunksendungen kontrollieren? In: Seiler (Hrsg.), Taschenbuch der Telekom Praxis 1996. Berlin, 1996. S. 163 ff.

Sciorra, Nicholas E., Self-Help & Contributory Infringement: The Law and Legal Thought Behind a Little „Black-Box". 11 Cardozo Arts & Entertainment Law Journal 905 ff. (1993)

Scott, Robert E., The Limits of Behavioral Theories of Law and Social Norms. 86 Virgina Law Review 1603 ff. (2000)

Seemann, Bruno, Ein Denkmalschutz für Prominenz? Gedanken zum droit de non-paternité. UFITA 128 (1995), 31 ff.

Selke, Gisbert W., Kryptographie. Verfahren, Ziele, Einsatzmöglichkeiten. Köln, 2000

Shah, Pratik A., The Uniform Computer Information Transactions Act. 15 Berkeley Technology Law Journal 85 ff. (2000)

Shapiro, Andrew L., The Disappearance of Cyberspace and the Rise of Code. 8 Seton Hall Constitutional Law Journal 703 ff. (1998)

Shapiro, Carl, Setting Compatibility Standards: Cooperation or Collusion? In: Dreyfuss/Zimmerman/First (Hrsg.): Expanding the Boundaries of Intellectual Property. Oxford, 2001. S. 81 ff.

Shapiro, Carl/Varian, Hal R., Information Rules. A Strategic Guide to the Network Economy. Boston, 1998

Shavell, Steven/Ypersele, Tanguy van, Rewards Versus Intellectual Property Rights. National Bureau of Economic Research Working Paper 6956, Februar 1999. Erhältlich unter <http://www. nber.org/papers/w6956>

Shear, Victor, Testimony of Victor Shear, Founder and CEO, InterTrust Technologies Corporation, Before United States Senate Judiciary Committee, Hearing on „Online Entertainment and Copyright Law". 3. 4. 2001. Erhältlich unter <http://www.intertrust.com/main/pressroom/pressreleases/2001/010403-uss-testimony.pdf> sowie unter 2001 WL 2006823 und 2001 WL 323735 (F.D.C.H.)

Shelanski, Howard A./Sidak, J. Gregory, Antitrust Divestiture in Network Industries. 68 University of Chicago Law Review 1 ff. (2001)

Shy, Oz, The Economics of Copy Protection in Software and Other Media. In: Kahin/Varian (Hrsg.), Internet Publishing and Beyond. The Economics of Digital Information and Intellectual Property. Cambridge, 2000. S. 97 ff.

ders., The Economics of Network Industries. Cambridge, 2001

Shy, Oz/Thisse, Jacques-François, A Strategic Approach to Software Protection. 8 (2) Journal of Economics & Management Strategy 163 ff. (1999)

Sieber, Ulrich, Strafrecht und Strafprozeßrecht. In: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht. München. Stand: 2. Ergänzungslieferung, Dezember 2000. Teil 19

Simon, Marvin K./Omura, Jim K./Scholtz, Robert A./Levitt, Barry K., Spread Spectrum Communications Handbook. Revised edition, New York, 1994

Smith, Michael D./Baily, Joseph/Brynjolfsson, Erik, Understanding Digital Markets: Review and Assessment. In: Brynjolfsson/Kahin (Hrsg.), Understanding the Digital Economy. Data, Tools, and Research. Cambridge, 2000. S. 99 ff.

Smith, Sean W./Palmer, Elaine R./Weingart, Steve, Using a High-Performance, Programmable Secure Coprocessor. In: Hirschfeld (Hrsg.), Financial Cryptography. Second International Conference, 23.–25. 2. 1998, Anguilla, British West Indies. Berlin, 1998. S. 73 ff.

Smith, Sean W./Weingart, Steve, Building a High-Performance, Programmable Secure Coprocessor. 31 Computer Networks 831 ff. (1999)

Sollins, Karen, Architectural Principles of Uniform Resource Name Resolution. Request for Comments 2276, Januar 1998. <http://www.rfc-editor.org/rfc/rfc2276.txt>

Sollins, Karen/Masinter, Larry, Functional Requirements for Uniform Resource Names. Request for Comments 1717, Dezember 1994. <http://www.rfc-editor.org/rfc/rfc1737.txt>

Sommer, Joseph H., Against Cyberlaw. 15 Berkeley Technology Law Journal 1145 ff.(2000)

Sorkin, David E., Technical and Legal Approaches to Unsolicited Electronic Mail. 35 University of San Francisco Law Review 325 ff. (2001)

Spar, Debora L., Lost in (Cyber)space: The Private Rules of Online Commerce. In: Cutler/Haufler/Porter (Hrsg.), Private Authority and Internaitional Affairs. Albany, 1999. S. 31 ff.

Sparks, Shaun, Busting the Code: The Anti-Trafficking Provision of the Digital Millenium Copyright Act and Free Expression in Digital Media. 6 International Journal of Communications Law and Policy (Winter 2000/2001). Erhältlich unter <http://www.ijclp.org/6_2001/pdf/ijclp_webdoc_13_6_2001.pdf>

Spindler, Gerald, Deliktsrechtliche Haftung im Internet – nationale und internationale Rechtsprobleme. Zeitschrift für Urheber- und Medienrecht 1996, 533 ff.

ders., E-Commerce in Europa. Die E-Commerce-Richtlinie in ihrer endgültigen Fassung. Multimedia und Recht, Beilage zu Heft 7/2000, 4 ff.

ders., Urheberrecht und Haftung der Provider – ein Drama ohne Ende? Zugleich Anmerkung zu OLG München v. 8. 3. 2001 – 29 U 3282/00. Computer und Recht 2001, 324 ff.

Spooner, Scott J., The Validation of Shrink-Wrap and Click-Wrap Licenses by Virginia's Uniform Computer Information Transactions Act. 7 Richmond Journal of Law & Technology 27 (Winter 2001). Erhältlich unter <http://www.richmond.edu/jolt/v7i3/article1.html>

Stallings, William, IP Security. 3 (1) Internet Protocol Journal 1 ff. (März 2000)

Staudinger, Julius von, Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen. 13. Bearbeitung, Berlin
Einleitung zu §§ 241 ff; §§ 241-243: 1995
Einleitung zu §§ 854 ff., §§ 854-882: 1995
§§ 903-924: 1996
Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen (AGBG): 1998

Stefik, Mark, Internet Dreams. Archetypes, Myths, and Metaphors. Cambridge, 1996

ders., Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing. 12 Berkeley Technology Law Journal 137 ff. (1997)

ders., The Internet Edge. Social, Legal, and Technological Challenges for a Networked World. Cambridge, 1999

Sterk, Stewart E., Rhetoric and Reality in Copyright Law. 94 Michigan Law Review 1197 ff. (1996)

Stolpmann, Markus, Elektronisches Geld im Internet. Grundlagen, Konzepte, Perspektiven. Köln, 1997

Strömer, Tobias H., Das ICANN-Schiedsverfahren – Königsweg bei Domainstreitigkeiten. Kommunikation und Recht 2000, 587 ff.

Sunstein, Cass R., On the Expressive Function of Law. 144 University of Pennsylvania Law Review 2021 ff. (1996)

ders., Social Norms and Social Roles. 96 Columbia Law Review 903 ff. (1996)

Sutter, Gavin, Law & Technology Convergence: Electronic Payment Systems. ECLIP (Esprit Procet 27028) Deliverable 2.2.6; 16. 12. 1999. <http://www.eclip.org/documents/deliverable_2_2_6_payments.pdf>

Taylor, Jim, DVD Demystified. 2. Auflage, New York 2000

ders., DVD Frequently Asked Questions (and Answers). Stand: 3. 2. 2001. <http://www.dvddemystified.com/dvdfaq.html>

Terada, Masayuki/Kuno, Hiroshi/Hanadate, Masayuki/Fujimura, Ko, Copy Prevention Scheme for Rights Trading Infrastructure. In: Domingo-Ferrer/Chan/Watson (Hrsg.), Smart Card Research and Advanced Applications. IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications. 20.–22. 9. 2000, Bristol, UK. S. 51 ff.

Tettenborn, Alexander, Die Novelle des Signaturgesetzes. Computer und Recht 2000, 683 ff.

Tewari, Gaurav/Maes, Pattie, Beyond Passive Bids and Asks: Mutual Buyer and Seller Discrimination Through Integrative Negotiation in Agent Based Electronic Markets. In: Finin/Grosof (Hrsg.), Knowledge-Based Electronic Markets. AAAI Workshop 2000 (KBE). 31. 7. 2000, Austin, USA. S. 70 ff.

dies., Design and Implementation of an Agent-Based Intermediary Infrastructure for Electronic Markets. In: Proceedings of the 2nd ACM Conference on Electronic Commerce. 17.–20. 10. 2000, Minneapolis, USA. New York, 2000. S. 86 ff.

Thierfelder, Jörg, Zugangsfragen digitaler Fernsehverbreitung. München, 1999

Thornburg, Elizabeth G., Going Private: Technology, Due Process, and Internet Dispute Resolution. 34 U. C. Davis Law Review 151 ff. (2000)

Thorne, John/Huber, Peter W./Kellogg, Michael K., Federal Broadband Law. Boston, 1995

Thot, Norman B., Elektronischer Vertragsschluß – Ablauf und Konsequenzen. Ein Rechtsvergleich zwischen dem amerikanischen und dem deutschen Recht. Frankfurt, 1999

Tietzel, Manfred/Weber, Marion, Urheberrechte im Zeitalter der Fotokopie. Zur Ökonomik von Verwertungsgesellschaften am Beispiel der VG Wort. In: Ott/Schäfer (Hrsg.), Ökonomische Analyse der rechtlichen Organisation von Innovationen. Tübingen, 1994. S. 128 ff.

Tolman, Brett L., ProCD, Inc. v. Zeidenberg: The End Does Not Justify the Means in Federal Copyright Analysis. 1998 Brigham Young University Law Review 303 ff. (1998)

Torunoglu, Ilhami/Charbon, Edoardo, Watermarking-Based Copyright Protection of Sequential Functions. 35 IEEE Journal of Solid-State Circuits 434 ff. (2000)

Towle, Holly K., The Politics of Licensing Law. 36 Houston Law Review 121 ff. (1999)

Trute, Hans-Heinrich, Der Schutz personenbezogener Informationen in der Informationsgesellschaft. Juristen-Zeitung 1998, 822 ff.

Tschudin, Christian F., Mobile Agent Security. In: Klusch (Hrsg.), Intelligent Information Agents. Agent-Based Information Discovery and Management on the Internet. Berlin, 1999. S. 431 ff.

Tuck, Bill, Electronic Copyright Management Systems. Final Report of a Scoping Study for eLib. Juli 1996. <http://www.sbu.ac.uk/litc/copyright/ecms.html>

Tushnet, Mark, „Everything Old is New Again": Early Reflections on the „New Chicago School". 1998 Wisconsin Law Review 579 ff.

Ulmer, Detlef, Der Bundesgerichtshof und der moderne Vertragstyp „Softwareüberlassung". Computer und Recht 2000, 493 ff.

Ulmer, Peter/Brandner, Hans Erich/Hensen, Horst-Dieter (Hrsg.) , AGB-Gesetz. Kommentar zum Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen. 9. Auflage, Köln 2001

Varian, Hal R., Grundzüge der Mikroökonomie. 5. Auflage, München 2001

ders., Versioning Information Goods. In: Kahin/Varian (Hrsg.), Internet Publishing and Beyond. The Economics of Digital Information and Intellectual Property. Cambridge, 2000. S. 190 ff.

Vellucci, Sherry L., Metadata. 33 Annual Review of Information Science and Technology 187ff. (1998)

Viefhues, Martin, Internet und Kennzeichenrecht: Meta-Tags. Multimedia und Recht 1999, 336 ff.

Vinje, Thomas C., A Brave New World of Technical Protection Systems: Will There Still Be Room For Copyright? European Intellectual Property Review 1996, 431 ff.

ders., Copyright Imperilled? European Intellectual Property Review 1999, 192 ff.

ders., Should We Begin Digging Copyright's Grave? European Intellectual Property Review 2000, 551 ff.

ders., The New WIPO Copyright Treaty: A Happy Result in Geneva. European Intellectual Property Review 1997, 230 ff.

Vogt, Carsten, Die DVB-Spezifikation für die Multimedia Home Platform. Fernseh- und Kino-Technik 53 (1999), 21 ff.

Volkmann, Uwe, Der dezente Staat – Verhaltenssteuerung im Umweltrecht. Juristische Schulung 2001, 521 ff.

Vora, Poorvi/Reynolds, Dave/Dickinson, Ian/Erickson, John/Banks, Dave, Privacy and Digital Rights Management. A Position Paper for the W3C Workshop on Digital Rights Management. Januar 2001. <http://www.w3.org/2000/12/drm-ws/pp/hp-poorvi2.html>

Waldenberger, Arthur, Verbraucherschutz im Internet. In: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht. München. Stand: 2. Ergänzungslieferung, Dezember 2000. Teil 13.4

Walker, Luke A., ICANN's Uniform Domain Name Dispute Resolution Policy. 15 Berkeley Technology Law Journal 289 ff. (2000)

Wallner, Debby M./Harder, Erice J./Agee, Ryan C., Key Management for Multicast: Issues and Architectures. Request for Comments 2627, Juni 1999. <http://www.rfc-editor.org/rfc/rfc2627.txt>

Walter, Michel M. (Hrsg.), Europäisches Urheberrecht – Kommentar. Wien, 2001

Wand, Peter, Dreifach genäht hält besser! – Technische Identifizierungs- und Schutzsysteme. GRUR Int. 1996, 897 ff.

ders., Technische Identifizierungs- und Schutzsysteme – Urheber- und Wettbewerbsrecht. In: Lehmann (Hrsg.), Internet- und Multimediarecht (Cyberlaw). Stuttgart, 1997. S. 35 ff.

ders., Technische Schutzmaßnahmen und Urheberrecht. Vergleich des internationalen, europäischen, deutschen und US-amerikanischen Rechts. München, 2001

Wandtke, Artur/Schäfer, Oliver, Music on Demand – Neue Nutzungsarten im Internet? GRUR 2000, 187 ff.

Wang, Joseph C., ProCD, Inc. v. Zeidenberg and Article 2B: Finally, the Validation of Shrink-Wrap Licenses. 15 John Marshall Journal of Computer & Information Law 439 ff. (1997)

Warlick, J. Thomas, A Wolf in Sheep's Clothing? Information Licensing and De Facto Copyright Legislation in UCC 2B. 45 Journal of the Copyright Society of the U.S.A 158 ff. (1997)

Wasserman, Hal/Blum, Manuel, Software Reliability via Run-Time Result-Checking. 44 Journal of the ACM 826 ff. (1997)

Waterman, David, Digital Television and Program Pricing. In: Gerbard (Hrsg.), The Economics, Technology and Content of Digital TV. Boston, 1998. S. 181 ff.

Watkins, Judy, COPEARMS and ERMS: Safeguarding Intellectual Property Rights in the Digital Age. 30 Computer Networks and ISDN Systems 1589 ff. (1998)

Watt, Richard, Copyright and Economic Theory. Friends or Foes? Cheltenham, 2000

Wayner, Peter, Digital Cash. Commerce on the Net. 2. Auflage, Boston 1997

ders., Digital Copyright Protection. Chestnut Hill, 1997

Webb, Stephen W., RIAA v. Diamond Multimedia Systems: The Recording Industry Attempts to Slow the MP3 Revolution – Taking Aim at the Jogger Friendly Diamond Rio. 7 Richmond Journal of Law and Technology 5 (2000). Erhältlich unter <http://www.richmond.edu/jolt/v7i1/note2.html>

Weibel, Stuart W., The Evolving Metadata Architecture for the World Wide Web: Bringing Together the Semantics, Structure and Syntax of Resource Description. In: Proceedings of the International Symposium on Research, Development and Practice in Digital Libraries. 18.–21. 11. 1997, Tsukuba, Japan. S. 16 ff.

Weibel, Stuart W./Kunze, John A./Lagoze, Carl/Wolf, Misha, Dublin Core Metadata for Resource Discovery. Request for Comments 2413, September 1998. <http://www.rfc-editor.org/rfc/rfc2413.txt>

Wein, Thomas, Versicherungsmarkt, asymmetrische Information und asymmetrischer Regulierung. Zeitschrift für die gesamte Versicherungswissenschaft 86 (1997), 103 ff.

Weinberg, Jonathan, Hardware-Based ID, Rights Management, and Trusted Systems. 52 Stanford Law Review 1251 ff. (2000)

ders., ICANN and the Problem of Legitimacy. 50 Duke Law Journal 187 ff. (2000)

Weiss, Gerhard (Hrsg.), Multiagent Systems. A Modern Approach to Distributed Artificial Intelligence. Cambridge, 1999

Weisser, Ralf, Der neue Rundfunkstaatsvertrag. Neue Juristische Wochenschrift 2000, 3526 ff.

ders., Dienstleistungen zum Vertrieb digitaler Pay TV-Angebote. Zeitschrift für Urheber- und Medienrecht 1997, 877 ff.

Weitnauer, Hermann, Verdinglichte Schuldverhältnisse. In: Canaris/Diederichsen (Hrsg.), Festschrift für Karl Larenz zum 80. Geburtstag am 23. April 1983. München, 1983. S. 705 ff.

Wente, Jürgen K./Härle, Philipp, Rechtsfolgen einer außerordentlichen Vertragsbeendigung auf die Verfügungen in einer „Rechtekette" im Filmlizenzgeschäfts und ihre Konsequenzen für die Vertragsgestaltung – Zum Abstraktionsprinzip im Urheberrecht. GRUR 1997, 96 ff.

Werle, Raymund, Innovationspotenziale im Internet – Selbstregelung auf Strukturebene. In: Hoffmann-Riem (Hrsg.), Innovation und Telekommunikation. Rechtliche Steuerung von Innovationsprozessen in der Telekommunikation. Baden-Baden, 2000. S. 141 ff.

Westermann, Harry, Sachenrecht. 7. Auflage, Heidelberg, 1998

Wiebe, Andreas, Information als Naturkraft. Immaterialgüterrecht in der Informationsgesellschaft. GRUR 1994, 233 ff.

Wiechmann, Peter, Urheber- und gewährleistungsrechtliche Probleme der Kopiersperre bei digitalen Audio-Kassetten-Recordern. Zeitschrift für Urheber- und Medienrecht 1989, 111 ff.

Wieling, Hans Josef, Sachenrecht. Band I: Sachen, Besitz und Rechte an beweglichen Sachen. Berlin, 1990

Wildemann, Daniela, Vertragsabschluss im Netz nach US-amerikanischem Recht. Computer und Recht international 2000, 109 ff.

Winn, Jane Kaufman, Clash of the Titans: Regulating the Competition Between Established and Emerging Electronic Payment Systems. 14 Berkeley Technology Law Journal 675 ff. (1999)

Witte, Andreas, Anmerkung zu BGH, Urteil vom 6. 7. 2000, Az. I ZR 244/97 – OEM-Version. Computer und Recht 2000, 654 ff.

ders., Urheberrechtliche Gestaltung des Vertriebs von Standardsoftware. Computer und Recht 1999, 65 ff.

Wittgenstein, Philipp, Über die negativen Auswirkungen einer Verstärkung des Urheberrechts auf die Entwicklung des Internet. UFITA 2000, 39 ff.

Wohlmacher, Petra, Introduction to the Taxonomy of Multiple Cryptography. In: Dittmann/Nahrstedt/Wohlmacher (Hrsg.), Multimedia and Security. Workshop at ACM Multimedia '99. 30. 10. - 5. 11. 1999, Orlando, USA. GMD Report 85. Sankt Augustin 2000. Online erhältlich unter <http://www.gmd.de/publications/report/0085/Text.pdf>. S. 19 ff.

Wold, Erling/Blum, Thom/Keislar, Douglas/Wheaton, James, Classification, Sear, and Retrieval of Audio. 1999. <http://www.musclefish.com/crc/crcwin.html>

Wolf, Manfred/Horn, Norbert/Lindacher, Walter F. (Hrsg.) , AGB-Gesetz. Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen – Kommentar. 4. Auflage, München 1999

Wolfgang, Raymond B./Podilchuk, Christine I./Delp, Edward J., Perceptual Watermarks for Digital Images and Video. 87 Proceedings of the IEEE 1108 ff. (1999)

Wolfson, Joel Rothstein, Contract and Copyright Are Not at War: A Reply to „The Metamorphosis of Contract into Expand". 87 California Law Review 79 ff. (1999)

Wong, Chung Kei/Gouda, Mohamed/Lam, Simon S., Secure Group Communications Using Key Graphs. 8 IEEE/ACM Transactions on Networking 16 ff. (2000)

Woodridge, Michael, Intelligent Agents. In: Weiss (Hrsg.), Multiagent Systems. A Modern Approach to Distributed Artificial Intelligence. Cambridge, 1999. S. 27 ff.

Wünschmann, Christoph, Clearingstellen für Multimedia-Produkte und europäisches Wettbewerbsrecht. Zeitschrift für Urheber- und Medienrecht 2000, 572 ff.

Yee, Bennet/Tygar, Doug, Secure Coprocessors in Electronic Commerce Applications. In: Proceedings of the First USENIX Workshop on Electronic Commerce. 11.–12. 7. 1995, New York. Berkeley, 1995. S. 155 ff.

Yoshikoa, Makoto, MOWare and Superdistribution. 31 Fujitsu Scientific & Technical Jounal 76 ff. (1995)

Yoshiura, Hiroshi/Sasaki, Ryôchi/Takaragi, Kazuo, Secure Fingerprinting Using Public-Key Cryptography. In: Christianson (Hrsg.), Security Protocols. 6th International Workshop on Security Protocols. 15.–17. 4. 1998, Cambridge, UK. Berlin, 1999. S. 83 ff.

Zeng, Wenjun/Liu, Bede, A Statistical Watermark Detection Technique Without Using Original Images for Resolving Rightful Ownerships of Digital Images. 8 IEEE Transactions on Image Processing 1534 ff. (1999)

Zieschang, Thilo, Differentielle Fehleranalyse und Sicherheit von Chipkarten. In: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), Mit Sicherheit in die Informationsgesellschaft. 5. Deutscher IT-Sicherheitskongreß des BSI 1997 – Tagungsband. Ingelheim, 1997. S. 227 ff.

Zittrain, Jonathan, ICANN: Between the Public and the Private. Comments Before Congress. 14 Berkeley Technology Law Journal 1071 ff. (1999)

ders., What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication. 52 Stanford Law Review 1201 ff. (2000)

Zscherpe, Kerstin, Urheberrechtsschutz digitalisierter Werke im Internet. Multimedia und Recht 1998, 404 ff.

Zviran, Moshe/Haga, William J., Password Security: An Empirical Study. 15 (4) Journal of Management Information Systems 161 ff. (1999)

Zwißler, Sonja, Secure Electronic Transaction – SET. Datenschutz und Datensicherheit 1998, 711 ff.

Materialienverzeichnis

Die verwendeten Materialien werden im folgenden alphabetisch in der Weise aufgeführt, wie sie in der Arbeit zitiert werden.

4C Entity, LLC, 4C 12 Bit Watermark Specification. 12. 10. 1999. <http://www.4centity.com/4centity/data/tech/4cspec.pdf>

4C/Verance Watermark License Agreement, 4C Entity, LLC/Verance Corp.: Watermark Technology License Agreement. Revision 5. Ohne Datum (1999/2000 veröffentlicht). Erhältlich unter <http://www.4centity.com/4centity/licensing/verance>

Allamanche, Eric/Herre, Jürgen/Koller, Jürgen/Rump, Niels, Vorrichtung und Verfahren zum Erzeugen eines verschlüsselten Datenstroms und Vorrichtung und Verfahren zu Erzeugen eines entschlüsselten Audio- und/oder Videosignals. Deutsches Patent DE 19907964 C1 vom 10. 8. 2000

Ansell, Steven T./Cherenson, Andrew R., Territorial Determination of Remote Computer Location in a Wide Area Network for Conditional Delivery of Digitized Products. U.S. Patent 6151631 vom 21. 11. 2000. Erhältlich unter <http://www.uspto.gov/patft>

Antitrust Guidelines, U.S. Department of Justice/Federal Trade Commission: Antitrust Guidelines for the Licensing of Intellectual Property. 6. 4. 1995. 4 Trade Regulation Reporter (CCH) 13132

Aucsmith, David/Graunke, Gary, Tamper Resistant Methods and Apparatus. U.S. Patent 5892899 vom 6. 4. 1999. Erhältlich unter <http://www.uspto.gov/patft>

Bobrow, Jared B., Memorandum of Points and Authorities in Support of Ex Parte Application for the Issuance of a Temporary Restraining Order and Order to Show Cause in DVD CCA v. McLaughlin, Brunner, et al. 28. 12. 1999. Erhältlich unter <http://www.eff.org/pub/Intellectual_property/DVDCCA_case/19991228-tro-pi-memo.html>

Braudaway, Gordon W./Magerlein, Karen A./Mintzer, Frederick C., Color Correct Digital Watermarking of Images. U.S. Patent 5530759 vom 25. 6. 1996. Erhältlich unter <http://www.uspto.gov/patft>

Brown, David S., Dynamic Feedback Arrangement Scrambling Technique Keystream Generator. U.S. Patent No. 4860353 vom 22. 8. 1989. Erhältlich unter <http://www.uspto. gov/patft>

Bundesministerium der Justiz, Diskussionsentwurf eines Fünften Gesetzes zur Änderung des Urheberrechtsgesetzes. Dok.-Nr. 3600/13-5300/98. Berlin, 7. 7. 1998. Online erhältlich unter <http://www.bmj.bund.de/misc/1998/urh_98.htm>

Bundesregierung, Entwurf eines Gesetzes über die Anwendung von Normen für die Übertragung von Fernsehsignalen (Fernsehsignalübertragungs-Gesetz – FÜG). Bundestags-Drucksache 13/7337 vom 25. 3. 1997, S. 1 ff.

dies., Entwurf eines Gesetzes über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz). Bundestags-Drucksache IV/270 vom 23. 3. 1962, S. 1 ff.

dies., Entwurf eines Gesetzes zur Änderung von Vorschriften auf dem Gebiet des Urheberrechts. Bundestags-Drucksache 10/837 vom 22. 12. 1983, S. 7 ff.

dies., Entwurf eines Zweiten Gesetzes zur Änderung des Urheberrechtsgesetzes. Bundestags-Drucksache 12/4022 vom 18. 12. 1992, S. 1 ff.

Bundesrepublik Deutschland, Mitteilung der Bundesrepublik Deutschland an die Kommission der Europäischen Union vom 6. 10. 2000 betreff der Richtlinie 98/84/EG über den rechtlichen Schutz zugangskontrollierter Dienste und von Zugangskontrolldiensten; hier: Stand der Umsetzung. Erhältlich unter <http://www.sicherheit-im-internet.de/download/012.htm>

Computerprogramm-Richtlinie, Richtlinie des Rates vom 14. Mai 1991 über den Rechtsschutz von Computerprogrammen. ABl. EG Nr. L 122 vom 17. 5. 1991, S. 42 ff.

ContentGuard, Inc., XrML License Agreement. Ohne Datum. Erhältlich unter <http://www.xrml. org/xrml_license.stm>

dass., XrML: eXtensible rights Markup Language. Version 1.03; 23. 6. 2000. Erhältlich unter <http://www.xrml.org>

CSS License Agreement, DVD Copy Control Association: CSS License Agreement. Version 1.1. Ohne Datum (veröffentlicht im November 2000). Erhältlich unter <http://www.dvdcca.org/dvdcca/css>

CSS Procedural Specifications, DVD Copy Control Association: CSS Procedural Specifications. Version 1.1. Ohne Datum (veröffentlicht im November 2000). Erhältlich unter <http://www.dvdcca.org/dvdcca/css/application_proc.html>

Cybercrime-Übereinkommen (Entwurf), European Committee on Crime Problems: Draft Convention on Cyber-Crime. Dok. CDPC (2001) 17 vom 29. 6. 2001. Erhältlich unter <http://conventions.coe.int/treaty/en/projets/FinalCybercrime.htm>

Cybercrime-Übereinkommen (Entwurf), Draft Explanatory Memorandum, European Committee on Crime Problems: Draft Explanatory Memorandum to the Draft Convention on Cybercrime. Dok. CDPC (2001) 17 vom 29. 6. 2001. Erhältlich unter <http://conventions.coe.int/treaty/en/projets/FinalCyberRapex.htm>

Datenschutzrichtlinie, Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. ABl. EG Nr. L 281 vom 23. 11. 1995, S. 31 ff.

Davidson, Robert I./Myhrvold, Nathan, Method and System for Generating and Auditing a Signature for a Computer Program. U.S. Patent 5559884 vom 24. 9. 1996. Erhältlich unter <http://www.uspto.gov/patft>

DTCP License Agreement, Digital Transmission Licensing Administrator: Digital Transmission Protection License Agreement. Evaluation License Convertible to Product License. Ohne Datum. Erhältlich unter <http://www.dtcp.com/data/adopter_agreement.pdf>

E-Commerce-Richtlinie, Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. 6. 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABl. EG L Nr. 178 vom 17. 7. 2000, S. 1 ff.

Eddy, Chris, Declaration of Chris Eddy in Reply to Defendant Bunner's and McLaughlin's Opposition to DVD CCA's Application for a Preliminary Injunction. 18. 1. 2000. Erhältlich unter <http://www.eff.org/pub/Intellectual_property/DVDCCA_case/20000114-pi-eddy-dec/index.html>

Electronic Book Exchange Working Group, The Electronic Book Exchange System (EBX) Version 0.8. Draft, Juli 2000. Erhältlich unter <http://ebxwg.org/spec.htm>

Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft" des Deutschen Bundestages, Zweiter Zwischenbericht zum Thema Neue Medien und Urheberrecht. Bundestags-Drucksache 13/8110 vom 30. 6. 1997

Europäische Kommission, Anmeldung einer Lizenzvereinbarung. Sache Nr. IV/C-3/37.506 – Lizenzierung von DVD-Patenten (1999/C 242/04). ABl. EG Nr. C 242 vom 27. 8. 1999, S. 5 f.

dies., Die Entwicklung des Marktes für digitales Fernsehen in der Europäischen Union – Mitteilung. KOM (1999) 450 vom 9. 11. 1999

dies., Europas Weg in die Informationsgesellschaft – Ein Aktionsplan. Mitteilung der Kommission an den Rat und das Europäische Parlament sowie an den Wirtschafts- und Sozialausschuß und den Ausschuß der Regionen. KOM (94) 347 endg. vom 19. 7. 1994

dies., Geänderter Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Anwendung von Normen für die Ausstrahlung von Fernsehsignalen. KOM (94) 455 endg. vom 25. 10. 1994

dies., Geänderter Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft. KOM (1999) 250 endg. vom 21. 5. 1999. Erhältlich unter <http://europa.eu.int/comm/internal_market/en/intprop/intprop/news/copy2de.pdf>

dies., Gemeinsame Antwort von Herrn Monti im Namen der Kommission auf die Schriftlichen Anfragen E-1509/00 und E-1510/00. ABl. EG Nr. C 53E vom 20. 2. 2001, S. 158 f.

dies., Grünbuch der Kommission der Europäischen Gemeinschaften über den rechtlichen Schutz verschlüsselter Dienste im Binnenmarkt. KOM (96) 76 endg. vom 6. 3. 1996

dies., Grünbuch über Urheberrecht und die technologische Herausforderung – Urheberrechtsfragen, die sofortiges Handeln erfordern. Mitteilung der Kommission. KOM (88) 172 endg. vom 23. 8. 1988

dies., Initiativen zum Grünbuch über Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft. KOM (96) 568 endg. vom 20. 11. 1996

dies., Mitteilung der Kommission an den Rat, das Europäische Parlament und den Wirtschafts- und Sozialausschuß. Folgemaßnahmen zum Grünbuch über die Bekämpfung von Nachahmungen und Produkt- und Dienstleistungspiraterie im Binnenmarkt. KOM (2000) 789 vom 17. 11. 2000. Erhältlich unter <http://europa.eu.int/comm/internal_market/en/intprop/indprop/com789de.pdf>

dies., Stellungnahme der Kommission gemäß Artikel 251, Absatz 2, Buchstabe c) des EG-Vertrages, zu den Äbanderungen des Europäischen Parlaments des gemeinsamen Standpunkts des Rates betreffend den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft zur Änderung des Vorschlags der Kommission gemäß Artikel 250, Absatz 2 des EG-Vertrages. KOM (2001) 170 endg. vom 29. 3. 2001

dies., Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft. Grünbuch der Kommission. KOM (95) 382 endg. vom 19. 7. 1995

dies., Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt. KOM (1998) 586 endg. vom 18. 11. 1998

dies., Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft. KOM (97) 628 endg. vom 10. 12. 1997

dies., Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über den Zugangs zuelektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltungen. KOM (2000) 384 vom 12. 7. 2000. Erhältlich unter <http://europa.eu.int/comm/information_society/policy/framework/pdf/com2000384_de.pdf>. Abgedruckt in ABl. EG Nr. C 365 (E) vom 19. 12. 2000, S. 215 ff.

dies., Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über den rechtlichen Schutz der Dienste, die einer Zugangskontrolle unterliegen oder deren Gegenstand die Zugangskontrolle selbst ist. KOM (97) 356 endg. vom 22. 7. 1997

Europäisches Parlament, Änderungsanträge 5-197. Entwurf einer Empfehlung für die Zweite Lesung von Enrico Boselli betreffend den Gemeinsamen Standpunkt des Rates im Hinblick auf den Erlass der Richtlinie des Europäischen Parlaments und des Rates zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft. Dok. PE 298.368/5-197 vom 17. 1. 2001. Erhältlich unter <http://www.europarl.eu.int/meetdocs/committees/juri/20010124/429791de.doc> oder <http://www.europarl.eu.int/meetdocs/committees/juri/20010124/juri20010124.htm>

dass., Urheberrecht in der Informationsgesellschaft. Legislative Entschließung des Europäischen Parlaments zu dem Gemeinsamen Standpunkt des Rates im Hinblick auf den Erlass der Richtlinie des Europäischen Parlaments und des Rates zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (Verfahren der Mitentscheidung: zweite Lesung). Dok. Nr. A5-0043/2001. Vorläufige Ausgabe der in der Sitzung vom Mittwoch, 14. 1. 2001, angenommenen Texte. Dokument Nr. PE 300.203, S. 7-10. Erhältlich unter <http://www3.europarl.eu.int/omk/omnsapir.so/calendar?PP=PDF&TYPE=PV2&FILE=p0010214DE.pdf &LANGUE=DE>

dass., Urheberrecht in der Informationsgesellschaft. Vorschlag für eine Richtlinie des Europäischen Parlamants und des Rates zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft. ABl. EG Nr. C 150 vom 28. 5. 1999, S. 171 ff.

Europäisches Zugangskontroll-Übereinkommen, Europarat: European Convention on the Legal Protection of Services Based on, or Consisting of, Conditional Access; 24. 1. 2001. ETS Nr. 178. Erhältlich unter <http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=178>

Europäisches Zugangskontroll-Übereinkommen, Explanatory Report, Europarat: European Convention on the Legal Protection of Services Based on, or Consisting of, Conditional Access: Explanatory Report. 2001. Erhältlich unter <http://conventions.coe.int/treaty/en/Reports/Html/178.htm>

Europarat, Empfehlung Nr. R(91) 14 des Ministerkommitees an die Mitgliedstaaten über den rechtlichen Schutz verschlüsselter Fernsehdienste. 1991. Erhältlich unter <http:/www.coe.int>

ders., Empfehlung Nr. R(95) 1 des Ministerkommitees an die Mitgliedstaaten über Maßnahmen gegen die Bild- und Tonträgerpiraterie. 1995. Erhältlich unter <http://www.coe.int>

European Telecommunications Standard Institute (ETSI), Digital Video Broadcasting (DVB) – Framing Structure, Channel Coding and Modulation for Digital Terrestrial Television. ETSI EN 300 744 V.1.4.1. Januar 2001. Erhältlich unter <http://www.etsi.org>

dass., Digital Video Broadcasting (DVB) – Guidelines on implementation and usage of Service Information (SI). ETSI TR 101 211 V1.4.1. Juli 2000. Erhältlich unter <http://www.etsi.org>

dass., Digital Video Broadcasting (DVB) – Multimedia Home Platform (MHP) Specification 1.0. ETSI TS 101 812 V1.1.1. Juli 2000. Erhältlich unter <http://www.etsi.org>

dass., Digital Video Broadcasting (DVB) – Specification for Service Information (SI) in DVB Systems. ETSI EN 300 468 V1.4.1. November 2000. Erhältlich unter <http://www.etsi.org>

dass., DVB Scrambling Technology Licence and Non-Disclosure Agreement. Ohne Datum. Erhältlich unter <http://www.etsi.org/dvbandca/DVB/Licence. SCRAM.doc>

Federal Communications Commission, Annual Assessment of the Status of Competition in the Market for the Delivery of Video Programming. Seventh Annual Report. 8. 1. 2001. Erhältlich unter <http://www.fcc.gov/Bureaus/Cable/Reports/fcc01001.pdf>

dies., In Re Implementation of Section 304 of Telecommunications Act of 1996. Further Notice of Proposed Rule Making and Declaratoy Ruling. 18. 9. 2000. 15 FCC Rcd. 18,199 (F.C.C. September 18, 2000)

dies., In the Matter of Implementation of Section 304 of the Telecommunications Act of 1996. Report and Order. 24. 6. 1998. 13 FCC Rcd. 14,775 (F.C.C. June 24, 1998)

dies., In the Matter of Inquiry into the Need for A Universal Encryption Standard for Satellite Cable Programming. Report. 25. 4. 1990. 5 FCC Rcd 2,710 (F.C.C. April 25, 1990)

Fernsehsignalübertragungs-Richtlinie, Richtlinie 95/47/EG des Europäischen Parlaments und des Rates vom 24. 10. 1995 über die Anwendung von Normen für die Übertragung von Fernsehsignalen. ABl. EG Nr. L 281 vom 23. 11. 1995, S. 51 ff.

HDCP License, Digital Content Protection, LLC: HDCP License Agreement. 2001. Erhältlich unter <http://www.digital-cp.com/data/HDCPAA021401.pdf>

Hitachi, Ltd./Intel Corporation/Matsushita Electric Industrial Co., Ltd./Sony Corporation/Toshiba Corporation, 5C Digital Transmission Content Protection White Paper. Revision 1.0; 14. 7. 1998. Erhältlich unter <http://www.dtcp.com/data/wp_spec.pdf>

dies., Digital Transmission Content Protection Specification. Volume 1 (Informational Version). Revision 1.1; 25. 7. 2000. Erhältlich unter <http://www.dtcp.com/data/DTCP_spec11_informational.pdf>

Hoy, John J., Reply Declaration of John J. Hoy in DVD CCA v. McLaughlin, Brunner, et al. 18. 1. 2000. Erhältlich unter <http://www.eff.org/Legal/Cases/DVDCCA_case/20000114-pi-hoy-rep-dec/index.html>

IMPRIMATUR, The IMPRIMATUR Business Model. Version 2.1. Dokument IMP/I4039/B vom 6. 1. 1999. <http://www.imprimatur.net/IMP_FTP/BMv2.pdf>

Information Infrastructure Task Force. Working Group on Intellectual Property Rights, Intellectual Property and the National Information Infrastructure. The Report of the Working Group on Intellectual Property Rights. Washington, 1995. Online erhältlich unter <http://www.uspto.gov/web/offices/com/doc/ipnii>

Intel Corporation, High-bandwidth Digital Content Protection System. Revision 1.0; 17. 2. 2000. Erhältlich unter <http://www.digital-cp.com/data/HDCP10.pdf>

Intel Corporation/International Business Machines Corporation/Matsushita Electric Industrial Co., Ltd./Toshiba Corporation, Content Protection for Prerecorded Media Specification – DVD Book. Revision 0.93; 31. 1. 2001. Gedruckte Fassung erhältlich über <http://www.4centity.com/4centity/tech/cprm>

dies., Content Protection for Prerecorded Media Specification – Introduction and Common Cryptographic Elements. Revision 0.93; 31. 1. 2001. Gedruckte Fassung erhältlich über <http://www.4centity.com/4centity/tech/cprm>

dies., Content Protection for Recordable Media Specification – DVD Book. Revision 0.94; 18. 10. 2000. Gedruckte Fassung erhältlich über <http://www.4centity.com/4centity/tech/cprm>

dies., Content Protection for Recordable Media Specification – Introduction and Common Cryptographic Elements. Revision 0.94; 18. Oktober 2000. Gedruckte Fassung erhältlich über <http://www.4centity.com/4centity/tech/cprm>

dies., Content Protection for Recordable Media Specification – Portable ATA Storage Book. Revision 0.91; 13. 11. 2000. Gedruckte Fassung erhältlich über <http://www.4centity.com/4centity/tech/cprm>

dies., Content Protection for Recordable Media Specification – SD Memory Card Book. Revision 0.94; 28. 8. 2000. Gedruckte Fassung erhältlich über <http://www.4centity.com/4centity/tech/cprm>

dies., Content Protection System Architecture. A Comprehensive Framework for Content Protection. Revision 0.81; 17. 2. 2000. <http://www.4centity.com/4centity/data/tech/cpsa/cpsa081.pdf>

Interim CPRM/CPPM License Agreement, 4C Entity, LLC: 4C Interim CPRM/CPPM License Agreement. Revision 1_D. Ohne Datum (veröffentlicht 2000). Erhältlich unter <http://www.4centity.com/4centity/licensing/adopter>

International Electrotechnical Commission, Digital Audio Tape Cassette System (DAT) – Part 6: Serial Copy Management System. IEC 1119-6, Juni 1992. Erhältlich unter <http://www.iec.ch>

Internet Corporation for Assigned Names and Numbers, Registrar Accreditation Agreemeent. 4. 11. 1999. <http://ww.icann.org/nsi/icann-raa-04nov99.htm>

dies., Uniform Dispute Resolution Policy. 24. 10. 1999. <http://www.icann.org/udrp/udrp-policy-24oct99.htm>

Klein, Joel I., Business Review Letter to C. R. Ramos on DVD patent pool. 10. 6. 1999. 1999 WL 392163 (D.O.J.). Auch erhätlich unter <http://www.usdoj.gov/atr/public/busreview/2485.pdf>

ders., Business Review Letter to G. R. Beeney on DVD patent pool. 16. 12. 1998. 1998 WL 931772 (D.O.J.). Auch erhältlich unter <http://www.usdoj.gov/atr/public/busreview/2121.htm>

ders., Business Review Letter to G. R. Beeney on MPEG LA patent pool. 26. 6. 1997. 1997 WL 356954 (D.O.J.). Auch erhältlich unter <http://www.usdoj.gov/atr/public/busreview/1170.htm>

Kuhn, Markus Günther/Anderson, Ross John, Software Piracy Detector Sensing Electromagneitc Computer Emenations. UK Patent Application GB9722799.5 vom 29. 10. 1997, veröffentlicht am 5. 5. 1999 unter der Nummer GB2330924 (Patent noch nicht erteilt). Erhältlich unter <http://gb.espacenet.com>

Library of Congress, Copyright Office, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies. 65 Federal Register 64555-64574 (October 27, 2000). Online erhältlich unter <http://www.loc.gov/copyright/fedreg/65fr64555.pdf>

Motion Picture Expert Group , Information Technology – Multimedia Framework (MPEG-21). Dokument ISO/IEC JTC1/SC29/WG11 N 3500. 30. 9. 2000. <http://www.cselt.it/mpeg/public/mpeg-21_pdtr.zip>

Musikdownload24, Allgemeine Geschäftsbedingungen der BMG Entertainment Germany/Switzerland/Austria/Eastern Europe Holding GmbH. 1. August 2000. <http://www.musicdownload24.de/agb_01.html>, abgerufen am 22. 2. 2001

Open eBook Forum, Open eBook Publication Structure 1.0; 16. 9. 1999. Erhältlich unter <http://www.openebook.org/oebpsdownload.htm>

Open Platform Initiative for Multimedia Access, OPIMA Specification. Version 1.1; 27. 6. 2000. Erhältlich unter <http://www.cselt.it/opima>

Petrovic, Rade/Winograd, Joseph M./Jemili, Kanaan/Metois, Eric, Apparatus and Method for Encoding and Decoding Information in Analog Signals. U.S. Patent No. 5940135 vom 17. 8. 1999. Erhältlich unter <http://www.uspto.gov/patft>

POD Host Interface License Agreement, CableLabs, Inc.: Final POD Host Interface License Agreement. Brief von Richard R. Green an Margalie R. Salas, FCC, 15. 12. 2000. Erhältlich unter <https://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6512258522>

ProComp, Microsoft's Plan to Condition the Sale of Media Player on the Sale of Windows XP is Just the Latest Example of a Pattern of Continued Violations by Microsoft of both the 1995 Microsoft Consent Decree and the Sherman Act – White Paper. 26. 4. 2001. <http://www.procompetition.org/headlines/04_whitepaper.pdf>

Rat der Europäischen Union, Gemeinsamer Standpunkt (EG) Nr. 48/2000 vom Rat festgelegt am 28. September 2000 im Hinblick auf den Erlass der Richtlinie 2000/…/EG des Europäischen Parlamanets und des Rates vom … zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte. ABl. EG Nr. C 344 vom 1. 12. 2000, S. 1 ff.

Richtlinie zum Urheberrecht in der Informationsgesellschaft, 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. ABl. EG Nr. L 167 vom 22. 6. 2001, S. 10 ff.

Secure Digital Music Initiative, Amendment 1 to SDMI Portable Device Specification, Part I. Version 1.0. SDMI Dokument 99-09-23-02. 23. 9. 1999. <http://www.sdmi.org/download/port_device_spec_amend1.pdf>

dies., Call for Proposals for Phase II Screening Technology. Version 1.0. SDMI Dokument 000224-01; 24. 2. 2000. <http://www.sdmi.org/download/FRWG00022401-Ph2_CFPv1.0.PDF>

dies., SDMI Portable Device Specifiaction, Part 1. Version 1.0. SDMI Dokument pdwg99070802; 8. 7. 1999. <http://www.sdmi.org/download/port_device_spec_part1.pdf>

Signatur-Richtlinie, Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. 12. 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen. ABl. EG Nr. L 13 vom 19.1.2000, S. 12 ff.

Statutory Instrument 2000/1175, The Conditional Acess (Unauthorised Decoders) Regulations 2000. United Kingdom Statutory Instrument 2000 No. 1175. Online erhältlich unter <http://www.legislation.hmso.gov.uk/si/si2000/20001175.htm>

Trusted Computing Platform Alliance (TCPA), Main Specification. Version 1.0; 25. 1. 2001. Erhältlich über <http://www.trustedpc.org/home/Specification.htm>

dies., TCPA Design Philosophies and Concepts. Version 1.0; 25. 1. 2001. <http://www.trustedpc.org/home/pdf/Design Phil v1.pdf>

U.S. Congress, Office of Technology Assessment , Copyright & Home Copying. Technology Challenges the Law. OTA-CIT-422. Washington, 1989

dass., Intellectual Property Rights in an Age of Electronics and Information. OTA-CIT-302. Washington, 1986

U.S. House of Representatives, Conference Report on the Digital Millenium Copyright Act. House of Representatives Report No. 105-796, 105th Congress, 2nd Session (October 8, 1998) = 1998 U.S.C.C.A.N. 645. Online erhältlich unter <http:// thomas.loc. gov>

dass., Digital Millennium Copyright Act of 1998. House of Representatives Report No. 105-551, Part 2, 105th Congress, 2nd Session (July 22, 1998). Online erhältlich unter <http://thomas.loc.gov>

dass., WIPO Copyright Treaties Implementation and On-line Copyright Infringement Liability Limiation. House of Representatives Report No. 105-551, Part 1, 105th Congress, 2nd Session (May 22, 1998). Online erhältlich unter <http://thomas. loc.gov>

U.S. Senate, Audio Home Recording Act of 1992, Senate Report No. 102-294, 102nd Congress, 2nd Session (June 9, 1992). Erhältlich unter <http://thomas.loc.gov> und 1992 WL 133198

UCC 2B Entwurf, 1. 8. 1998, Uniform Commercial Code Article 2B Licenses. With Reporter's Notes. By the American Law Institute and the National Conference of Commissioners on Uniform State Laws. Draft, 1. 8. 1998. Online erhältlich unter <http://www.law.upenn.edu/bll/ulc/ucc2b/2b898.pdf>

UCITA, Uniform Computer Information Transactions Act (Last Revisions or Amendments Completed Year 2000). Drafted by the National Conference of Commissioners on Uniform State Laws and by it Approved and Recommended for Enactment in All the States at its Annual Conference Meeting in ist One-Hundred-and-Ninth-Year in St. Augustine, Florida, July 28-August 4, 2000. With Prefatory Note and Comments. 29. September 2000. Erhältlich unter <http://www.law.upenn.edu/bll/ulc/ucita/ucitaFinal00.pdf>

Universal Music Group/Intertrust Technologies Corporation, Bluematter End User License Agreement. <http://offers.bluematter.com/sniffer/terms.htm>. Abgerufen am 22. 2. 2001

U.S. Department of Commerce/National Telecommunications and Information Administration, Study Examining 17 U.S.C. Sections 109 and 117 Pursuant to Section 104 of the Digital Millennium Copyright Act. Report to Congress. März 2001. Erhältlich unter <http://www.ntia.doc.gov/ntiahome/occ/dmca2001/cover.htm>

U.S. Department of Justice, Antitrust Division, Notice Pursuant to the National Cooperative Research and Production Act of 1993; DVD Copy Control Association („DVD CCA"). 66 Federal Register 40727 ff. (August 3, 2001)

VO 240/96, Verordnung (EG) Nr. 240/96 der Kommission vom 31. Januar 1996 zur Anwendung von Artikel 85 Absatz 3 des Vertrages auf Gruppen von Technologietransfer-Vereinbarungen. ABl. EG Nr. L 31 vom 9. 2. 1996, S. 2 ff.

WCT Basic Proposal, Basic Proposal for the Substantive Provisions of the Treaty on Certain Questions Concerning the Protection of Literary and Artistic Works to be Considered by the Diplomatic Conference. WIPO-Dokument CRNR/DC/4 vom 30. 8. 1996. Erhältlich unter <http://www.wipo.int/eng/diplconf/pdf/4dc_e. pdf>

Willard, R. A., ICE (Identification Coding, Embedded). Presented at the 94th Audio Engineering Society Convention, 16.–19. März 1993, Berlin. Audio Engineering Society Preprint 3516 (D2-3). New York, 1993

WIPO Audiovisual Performances Treaty Basic Proposal, Basic Proposal for the Substantive Provisions of an Instrument on the Protection of Audiovisual Performances to be Considered by the Diplomatic Conference. WIPO-Dokument IAVP/DC/3 vom 1. 8. 2001. Erhältlich unter <http://www.wipo.int/eng/meetings/2000/iavp/pdf/iavp_dc3.pdf>

WIPO Database Treaty Basic Proposal, Basic Proposal for the Substantive Provisions of the Treaty on Intellectual Porperty in Respect of Databases to be Considered by the Diplomatic Conerence. WIPO-Dokument CRNR/DC/6 vom 30. 8. 1996. Erhältlich unter <http://www.wipo.int/eng/diplconf/pdf/6dc_e.pdf>

Wolosewicz, Jack, Apparatus and Method for Encoding and Decoding Information in Audio Signals. U.S. Patent No. 5774452 vom 30. 7. 1998. Erhältlich unter <http://www.uspto.gov/patft>

Wolosewicz, Jack/Jemili, Kanaan, Apparatus and Method for Encoding and Decoding Information in Analog Signals. U.S. Patent No. 5828325 vom 27. 10. 1998. Erhältlich unter <http://www.uspto.gov/patft>

Wroblewski, William J., Method and System for Preventing the Off Screen Copying of a Video or Film Presentation. U.S. Patent 6018374 vom 25. 1. 2000. Erhältlich unter <http://www.uspto.gov/patft>

Zugangskontrollrichtlinie, Richtlinie 98/84/EG des Europäischen Parlaments und des Rates vom 20. November 1998 über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten. ABl. EG Nr. L 320 vom 28. 11. 1998, S. 54 ff.

Einführung

Die Geschichte des Urheberrechts war schon immer ein Prozeß rechtlicher Reaktion auf die Herausforderungen der Technik.[1] Es ist daher nicht verwunderlich, daß das Internet und andere digitale Medien das Urheberrecht auf eine harte Probe stellen. Mit der Digitalisierung wird die Erstellung von Kopien, die nicht mehr vom Original zu unterscheiden sind, zum Kinderspiel. Seit Jahren kämpft die Software-Industrie gegen die Erstellung von Raubkopien. Nach und nach greift die Problematik auf andere Branchen über. Bis zum Frühjahr 2001 konnte man über die Musiktauschbörse Napster im Internet auf ein riesiges Musikarchiv zurückgreifen, ohne dabei durch urheberrechtliche Regelungen in irgendeiner Weise beschränkt zu sein. Dieses Angebot war so attraktiv, daß Napster innerhalb von weniger als zwei Jahren seit seiner Gründung über 70 Millionen Nutzer gewinnen konnte. Im Höhepunkt seiner Popularität – im Februar 2001 – wurden über Napster 2,79 Milliarden Mal Musikdateien kopiert. Damit hat das Napster-„Phänomen" eine Dimension erreicht, die zu deutlichen Umsatz- und Gewinneinbußen der Musikindustrie führen könnte. Auch die Filmindustrie macht sich Gedanken, wie sie die Gefahr von Raubkopien in den Griff bekommen könnte. Als im Mai 1999 eine neue Folge des Kassenschlagers „Star Wars" von *George Lucas* in die U.S.-amerikanischen Kinos kam, war der Film, dessen Produktionskosten auf 115 Millionen Dollar geschätzt wurden, innerhalb einer Woche im Internet verfügbar. Zwar war das Kopieren des Films beschwerlich: Die schlechte Qualität der Kopie, das große Datenvolumen (1,3 Gigabyte) sowie die Tatsache, daß der Film von ausländischen Rechnern mit schlechter Internet-Anbindung angeboten wurde, veranlaßte nur wirkliche Fans, diesen Weg zu beschreiten. Die Übertragungskapazitäten im Internet steigen jedoch schnell an, und durch bessere Kompressionsverfahren kann die Qualität der Filmkopien erhöht werden. Es ist daher nur eine Frage der Zeit, bis sich die Filmindustrie den Problemen stellen muß, denen sich die Musikindustrie heute ausgesetzt sieht.

Die gesamte Inhalteindustrie beginnt nach und nach, auf diese Bedrohung ihrer Einnahmequellen zu reagieren. Will sie gegen Raubkopierer rechtlich vorgehen, so stellen sich jedoch große Hürden. Da das Erstellen von Kopien einfach ist und fast keine Kosten verursacht, steigt die Anzahl

---

[1] *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, Einl. Rdnr. 1; ebenso für das U.S.-amerikanische Urheberrecht der U.S. Supreme Court in Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 430 f. (1984).

der potentiellen Täter rapide an. Gleichzeitig kann es in Netzwerken schwierig sein, die Täter überhaupt zu identifizieren und rechtliche Schritte gegen sie einzuleiten. Während die Gefahr von Urheberrechtsverletzungen durch den technischen Fortschritt rasant ansteigt, sind die Reaktionsmöglichkeiten des Rechts ernüchternd.[2]

Es ist daher nicht verwunderlich, daß die Inhalteindustrie zunehmend auf Schutzmöglichkeiten außerhalb des herkömmlichen Urheberrechts setzt. Dabei wird das sogenannte „Digital Rights Management" immer wichtiger. Eine allgemein anerkannte Definition des Begriffs existiert nicht. Man ist sich noch nicht einmal darüber einig, wie solche Systeme überhaupt bezeichnet werden sollten.[3] „Digital Rights Management"-Systeme – im folgenden als DRM-Systeme bezeichnet – sind elektronische Vertriebssysteme für digitale Inhalte. Sie ermöglichen die sichere Verbreitung digitaler Inhalte – unter anderem urheberrechtlich geschützte Musik-, Film- oder Sprachwerke – über das Internet oder andere digitale Medien –, beispielsweise CDs, mobile Abspielgeräte oder Mobiltelefone. DRM-Systeme ermöglichen den Rechteinhabern einen sicheren Vertrieb zu berechtigten Nutzern und geben ihnen die Kontrolle über den gesamten Vertriebsweg.[4] Daneben ermöglichen sie eine effektive und differen-

---

[2] *Lessig*, S. 125; *Bechtold*, GRUR 1998, 18, 19.

[3] Es wird auch der Begriff „Electronic Copyright Management System" (ECMS) verwendet, so vom Verfasser in GRUR 1998, 18 ff.; s. weiterhin *Gervais* in: Koskinen-Olsson/Gervais, S. 6, 9. Auch finden sich die Begriffe „Copyright Management System" (CMS) – s. *Cohen*, 97 Mich. L. Rev. 462, 471 (1998) –, „Automated Rights Management" (ARM) – s. *Bell*, 76 N. C. L. Rev. 557 (1998) –, „Electronic Rights Management System" (ERMS) – s. *Hill*, Proc. IEEE 87 (1999), 1228, 1229 – und „Intellectual Property Rights Management" (IPRM) – s. *Ramanujapuram/Ram*, Dr. Dobb's Journal, Dezember 1998, S. 20. In letzter Zeit scheint sich jedoch der Begriff „Digital Rights Management" durchzusetzen, der auch in dieser Arbeit verwendet wird.

[4] *Hartung/Ramme*, IEEE Communications Magazine 78, 79 (November 2000). Daneben finden sich noch andere Umschreibungen des Begriffs. *Bartolini/Cappellini/Piva/Fringuelli* in: Cammelli/Tjoa/Wagner (Hrsg.), S. 896, meinen: „[A DRM system] can be considered as an ensemble of services, connected through a network environment, cooperating together, to allow the protection of the [intellectual property rights] of multimedia data, on the basis of contracts agreed among the involved parties". Das XrML License Agreement von Contentguard – s. <http://www.xrml.org/xrml_license.stm> – definiert DRM wie folgt: „[DRM] means techniques, processes, procedures and algorithms related to establishing an environment that utilizes syntactically expressed declarative statements having an environment-wide meaning for the management of digital rights, including computer hardware and software, which enables or implements trusted licensing, secure rights and permissions specification, rights and permissions enforcement, establishment of a trusted computing environment, and trusted infrastructure, each for:

i. the secure preparation, transmission, prevention of misuse and/or consumption of protected digital works by authorized licensees, (such as watermarking and fingerprinting and software obfuscation;) and

ii. secure digital commerce transactions, including the automated and persistent enforcement of policies for consumption of digital goods, usage tracking, budget

zierte Rechteverwaltung und eröffnen so für digitale Inhalte neue Geschäftsmodelle. Im Vergleich zum herkömmlichen Urheberrecht versprechen sie, eine ungeahnt weitgehende Kontrolle über die Verbreitung und Nutzung digitaler Inhalte zu ermöglichen.

Zu diesem Zweck bedienen sich DRM-Systeme einer Fülle unterschiedlicher Schutzmechanismen. Eine zentrale Rolle spielen technische Schutzmaßnahmen. Verschlüsselungs- und Kopierkontrollverfahren, Metadaten, digitale Wasserzeichen, Verfahren zum Schutz von Authentizität und Integrität, manipulationssichere Hard- und Software und eine Vielzahl weiterer technischer Verfahren sollen dem Urheber ermöglichen, seine Werke auf sicherem Weg zum berechtigten Nutzer zu übertragen, und gleichzeitig verhindern, daß unberechtigte Dritte die Werke ebenfalls nutzen können. Dennoch wäre es zu kurz gegriffen, DRM-Systeme mit einem bloßen „Kopierschutz“ gleichzusetzen. Kopierschutzmaßnahmen können in DRM-Systemen eingesetzt werden, ein vollständiges DRM-System ist jedoch ein viel umfassenderes Vertriebskonzept für digitale Inhalte. So können die erwähnten technischen Schutzmaßnahmen mit Zahlungssystemen und weiteren technischen Komponenten kombiniert werden, wodurch sich ein umfassendes „E-Commerce“-System für digitale Inhalte ergibt. DRM-Systeme bauen nicht nur auf technischen Komponenten auf. Inhalteanbieter können sich durch Nutzungsverträge schützen, die jeder Nutzer abschließen muß, bevor er einen digitalen Inhalte in einem DRM-System nutzen kann. Die Entwickler technischer DRM-Komponenten verpflichten die Hersteller von Computern und Unterhaltungselektronikgeräten in Technologie-Lizenzverträgen, bestimmte Sicherheitsstandards und ähnliche Bedingungen einzuhalten. Diese Technologie-Lizenzverträge dienen ebenfalls mittelbar den Interessen der Inhalteanbieter. Auch der Gesetzgeber unterstützt die Entwicklung von DRM-Systemen. Schon im Jahr 1996 wurde in zwei völkerrechtlichen Verträgen der „World Intellectual Property Organization“ ein rechtlicher Schutz verankert, wonach die Umgehung technischer Schutzmaßnahmen verboten ist. Der Schutz in DRM-Systemen zeichnet sich also durch ein Konglomerat mehrerer unterschiedlicher Schutzmechanismen aus. Der wichtigste, aber bei weitem nicht einzige Schutzmechanismus ist der technische Schutz.

Die vorliegende Arbeit verwendet den Begriff „Digital Rights Management“ als ein Schlagwort für eine Vielzahl unterschiedlicher Systeme. DRM-Systeme finden sich im Online- wie im Offline-Bereich. In ihrer schwächsten Form verhindern oder erschweren DRM-Systeme, daß der Nutzer einen digitalen Inhalt kopieren kann. In ihrer stärksten Form erlauben DRM-Systeme die individuelle Abrechnung der Nutzung digitaler

management, fraud detection, account management, key management and similar functions, to occur over internal and external computer networks.“

Inhalte ähnlich den Telefongebühren; der einzelne Nutzungsvorgang eines Inhalts soll erfaßt werden. Die vorliegende Arbeit folgt bewußt dieser abstrakten Auffassung eines „Digital Rights Management", da sie allgemeine Entwicklungen aufzeigen will, die bei all diesen Systemen auftreten können. Oftmals wird sie implizit von der stärksten Form eines DRM-Systems ausgehen, da bei diesen Systemen die dargestellten Entwicklungen am deutlichsten erkennbar sind.

Ein solches umfangreiches DRM-System könnte wie folgt funktionieren:[5] Urheberrechtlich geschützte Werke werden verschlüsselt und mit zusätzlichen Informationen – wie z. B. einer kurzen Zusammenfassung, Lizenzbedingungen und Urheberangaben, digitaler Signatur und Wasserzeichen – in einem digitalen „Container" zusammengefaßt. Erhält ein Nutzer einen solchen „Container" über das Internet, so kann er zunächst das Werk selbst nicht lesen, da es verschlüsselt ist. Jedoch sind im Klartext Informationen über den Inhalt, Lizenzbedingungen und ähnliches erhältlich. Der Nutzer kann anschließend von einer zentralen Stelle („Clearing Center") gegen eine entsprechende Vergütung einen Schlüssel erwerben, mit dem er das verschlüsselte Werk aus dem „Container" entschlüsseln und dann verwenden kann. Dabei besteht ein differenziertes Abrechnungsmodell, nach dem ein Nutzer beispielsweise lediglich das Recht erwerben kann, das Werk auf dem Bildschirm zu betrachten, auszudrucken oder abzuspeichern. Auch kann das DRM-System die Nutzung des Werks genau kontrollieren. Es kann festlegen, daß der Nutzer das Werk nicht kopieren und an Dritte weitergeben kann. Es kann festlegen, daß er das Werk nur die nächsten 48 Stunden oder insgesamt nur 20 Mal nutzen kann. Das DRM-System kann für die Nutzungen einen Pauschalpreis berechnen oder für jede Nutzung einen geringen Betrag („pay per use"). Die Abrechnung kann über Kreditkarten, Bankeinzug oder vollständig elektronische Zahlungsmittel geschehen. Die Nutzer werden an die Nutzungsbedingungen durch den Abschluß von Nutzungsverträgen gebunden. Gleichzeitig kontrollieren technische Schutzmaßnahmen, daß die Nutzer das Werk auch tatsächlich nur im Rahmen der Nutzungsverträge nutzen können. In DRM-Systemen sind der differenzierten Ausgestaltung der Nutzungsmöglichkeiten fast keine Grenzen gesetzt. Dadurch werden neue Nutzungsarten und neue Geschäftsmodelle möglich.[6]

[5] Vgl. *Bechtold*, GRUR 1998, 18, 20 f.

[6] In diesem Zusammenhang mag auch die Beschreibung des InterTrust-Systems interessant sein. Das kalifornische Unternehmen InterTrust ist einer der wichtigsten Anbieter umfassender DRM-Systeme. S. *Shear*, S. 6 f.: „The technology system that InterTrust has developed protects content, in the instance of this discussion music, on a persistent basis throughout its commercial lifecycle. It does this by binding rules governing content use with governed content. This tamper resistant association persists regardless of the channel through or platform upon which the music is played, and the number of handlers of the content, the duration of time, or the physical location of the content. InterTrust technology creates a zone – independent of time, place, or device –

Die vorliegende Arbeit beschränkt sich jedoch nicht auf solch umfassende DRM-Systeme. Auch andere Systeme, die nur Teilmengen eines umfassenden DRM-Systems beinhalten, werden von der Untersuchung erfaßt. Darunter fallen beispielsweise DVDs, der digitale Nachfolger analoger Videokassetten, in denen sich bis zu zehn unterschiedliche technische Schutzmaßnahmen finden. DAT- und Minidisc-Geräte erlauben nur die Erstellung einer einzigen digitalen Kopie von Musikstücken. Besonders verbreitet sind DRM-Systeme im Pay-TV-Sektor. Eine Set-Top-Box auf einem Fernseher, die verschlüsselte Fernsehprogramme entschlüsseln und eventuell sogar die Nutzung einzelner Fernsehsendungen abrechnen kann („pay per use"), ist nichts anderes als Teil eines umfassenden DRM-Systems, mit dem der Pay-TV-Betreiber Filme auf sichere Weise an berechtigte, das heißt zahlende Kunden liefert.

Die Arbeit versteht damit unter dem Begriff des „Digital Rights Management" eine Vielzahl unterschiedlicher technischer und rechtlicher

where music is governed by technology and where rights-holders, including consumers, are free to express and protect their rights through the freedom to establish differing rules reflecting their individual interests. Within this technical protection zone, digital information such as music can be offered to consumers via a virtually limitless range of models: sale of downloads; subscriptions; pay-per-listen; superdistribution (consumer A delivering material to consumer B and so on); and file sharing. This freedom is also available for the implementation of a richly diverse range of policies that govern usage, and any consequences of usage, in relation to groups of any nature, such as special interest groups. To accommodate statutory limitations on copyright, special consumption rules can be created, either through law or through accepted practice of rights-holders, for particular consumers or classes of users: for schools and universities; for libraries and archival institutions; and for consumers with special needs such as the blind. Whatever the needs, whatever the relationship between different participants the digital information remains persistently protected while freely available according to agreed rules of use. If this protection is to remain effective throughout the lifecycle of the content then it follows that it must be possible to change the rules relating to use. Material can have a succession of different owners. It can change in value; it can be traded for different purposes; it can be used on multiple, different devices; and it can be loaned to other parties. Our system anticipates and accommodates all these possibilities. In our system, digital information and the rules governing its use by a particular user can exist and move independently of each other, coming together to give effect to the agreement between supplier, distributor, and consumer, and respecting whatever rules may be applied by government, or, for example, by financial institutions. An efficient system of protection must not only accommodate a wide variety of business offerings. It must also support the complex value chains through which many of the offerings are delivered. The architecture InterTrust has developed supports value chain relationships based on traditional commercial principles – we call this digital enabling of value chains ‚chain of handling and control'. This means that each actor in the value chain is able to create the rules it wishes to apply to the material in question within the scope of authority granted to the participant by the previous or governing actors in the value chain. A publisher could establish the commercial terms for a work within the authority granted by the author; the distributor could then set rules within the scope of authority granted by the publisher and so on through the value chain, all in accordance with law and accepted practice."

Phänomene, die alle miteinander zusammenhängen. Von anderen Autoren werden andere Bezeichnungen verwendet, oftmals werden die Einzelprobleme auch nicht in den größeren Zusammenhang von DRM-Systemen gestellt. Diesen Zusammenhang will die vorliegende Arbeit herausarbeiten.

Öfters wird eingewandt, DRM-Systeme würden in Zukunft keine Rolle spielen, eine Untersuchung ihrer Konsequenzen sei daher unnötig. Dabei werden technische und ökonomische Argumente vorgebracht. Aus technischer Sicht wird gegen DRM-Systeme eingewandt, daß es unmöglich sei, ein sicheres technisches Schutzsystem zu entwerfen. Es gehöre zur „Natur" digitaler Information – die nichts anderes als eine Reihe von Nullen und Einsen darstellt –, daß sie einfach und unendlich reproduzierbar sei. Auch ein noch so ausgeklügeltes technisches Schutzsystem könne dieses Faktum nicht ändern und einen absoluten Schutz bieten.[7] Dem ist entgegenzuhalten, daß diese Sichtweise zu stark auf die technischen Komponenten eines DRM-Systems beschränkt bleibt. Wie die vorliegende Arbeit zeigen wird, bauen DRM-Systeme auf einer Vielzahl unterschiedlicher Schutzmechanismen auf. Die Stärke des Schutzes von DRM-Systemen liegt gerade im Ineinandergreifen mehrerer Schutzmechanismen.[8] Außerdem zielen auch umfangreiche DRM-Systeme oftmals nicht auf einen hundertprozentigen Schutz digitaler Inhalte ab, da ein solches Schutzniveau gar nicht notwendig ist.[9]

Aus ökonomischer Sicht wird eingewandt, es sei äußerst zweifelhaft, ob sich DRM-Systeme überhaupt am Markt durchsetzen könnten. Zwar gebe es schon seit langer Zeit Versuche, technische Kopierschutzssysteme einzuführen. Diese Versuche seien aber regelmäßig gescheitert. Als Beispiel wird der Versuch der Softwareindustrie in den 80er Jahren genannt, mit Hilfe sogenannter „Dongles" – einer besonderen Art technischer Kopierschutzverfahren[10] – Computersoftware flächendeckend gegen das unberechtigte Kopieren zu schützen. Es ist jedoch sehr fraglich, ob der Mißerfolg von Dongles bei Computersoftware auf DRM-Systeme im heutigen Umfeld übertragbar ist.[11] Die kritischen Stimmen vernachlässigen auch, daß wir schon heute in vielen Bereichen von DRM-Systemen umgeben sind, die teilweise noch sehr rudimentär ausgestaltet sind, teil-

[7] In diese Richtung beispielsweise *Bruce Schneier* in einem Vortrag am „Institute for Mathematics and its Applications", Minneapolis, am 12. 2. 2001, Audio-Mitschnitt unter <http://www.ima.umn.edu/recordings/Public_Lecture/2000–2001/feb_12_01/schneier.ram>, Vortragsunterlagen unter <http://www.ima.umn.edu/talks/workshops/2–12–16.2001/schneier/DigitalRights.pdf>; s. a. *Kelsey/Schneier*, S. 2; *Gilmore*, c't 4/2001, S. 64, 67 f.

[8] S. dazu ausführlich unten Teil 3, A II.

[9] S. a. *Hardy*, 1996 U. Chi. Legal F. 217, 222 (1996): „100 percent assurance of anything – or zero risk – has never been a requirement of any business"; *Sander*, S. 4 ff.

[10] Zu den technischen Einzelheiten s. unten Teil 1, C IV 1 a.

[11] S. dazu unten Teil 3, B I 2 b cc 1.

weise aber auch ausdifferenzierte Vertriebsmodelle unterstützen. Bespielte Videokassetten, die zum Verkauf angeboten werden oder in Videotheken ausgeliehen werden können, werden durch Kopierschutzverfahren des U.S.-amerikanischen Unternehmens „Macrovision" geschützt. Diese Verfahren werden insgesamt bei über 2,5 Milliarden Videokassetten weltweit eingesetzt[12] und funktionieren bei 85% aller Konsumenten-Videorekorder.[13] 1998 existierten im europäischen Fernsehmarkt insgesamt 17 Pay-per-view-Dienste, die rund 2000 Kanäle anboten; viele dieser Anbieter senden digital und setzen technische Schutzmaßnahmen ein.[14] Zu dieser Zeit existierten in Deutschland, Frankreich, Großbritannien, Italien und Spanien zusammengenommen über 48 Millionen Abonnenten von Pay-TV-Sendern.[15] Das umfassend geschützte DVD-Format war so erfolgreich, daß innerhalb von nur drei Jahren seit seiner Einführung am Markt über 10 Millionen DVD-Spieler verkauft und über 30 Millionen Computer mit DVD-Laufwerken ausgestattet wurden. Kein anderes Unterhaltungselektronikgerät hat in solch kurzer Zeit jemals eine vergleichbare Marktdurchdringung erreicht.[16]

Trotz dieser Entwicklungen ist es unmöglich, eine sichere Vorhersage über die zukünftige Bedeutung von DRM-Systemen zu machen. Wenn der Verfasser die Bedeutung von DRM-Systemen als relativ hoch einschätzt, so liegt das auch an den immensen Forschungsanstrengungen in Unternehmen und Universitäten, die in den letzten Jahren im DRM-Bereich getätigt wurden. Weiterhin zeigt der Erlaß rechtlicher Umgehungsvorschriften in einer Vielzahl von Ländern, welche bedeutende Rolle die Gesetzgeber DRM-Systemen zusprechen.

A. Erkenntnisinteresse der Arbeit

Die vorliegende Arbeit will die Auswirkungen von DRM-Systemen auf das Urheberrecht untersuchen. Die zu untersuchende These lautet, daß Urheber und Leistungsschutzberechtigte im digitalen Umfeld zunehmend auf Schutzmechanismen außerhalb des Urheberrechts setzen, nämlich auf die technischen und vertraglichen Schutzmechanismen von DRM-Syste-

[12] S. die Aussagen von *Gerry Brill*, Macrovision Corp., in einer Diskussion am Franklin Pierce Law Center 1998, abgedruckt in 39 IDEA 291, 322 f. (1999).

[13] *Taylor*, DVD Demystified, S. 196.

[14] Insbesondere in Frankreich sind Pay-per-view-Dienste verbreitet, s. *European Communication Council* (Hrsg.), S. 54.

[15] *European Communication Council* (Hrsg.), S. 52.

[16] *Taylor*, DVD Demystified, S. 2, 548. Heute macht der Vertrieb von Filmen auf DVD etwa 35 % der weltweiten Einnahmen von Warner Brothers im Video-Heimsektor aus, s. Universal City Studios, Inc. v. Reimerdes, 111 F.Supp.2d 294, 311 Fn. 69 (S.D.N.Y. 2000).

men. Wenn DRM-Systeme ein mit dem Urheberrecht vergleichbares Schutzniveau bieten würden, könnten sie bis zu einem gewissen Maß das Urheberrecht in seiner bisherigen Funktion – Schutz der Urheber und Leistungsschutzberechtigten – ersetzen.

Eine umfassende Untersuchung zu den Auswirkungen von DRM-Systemen auf das Urheberrecht fehlt in Deutschland.[17] In den USA werden DRM-Systeme in der Rechtswissenschaft dagegen relativ stark diskutiert. Jedoch sind die Beiträge auf eine Unzahl einzelner Aufsätze verstreut. Eine umfassende Untersuchung zu DRM-Systemen existiert auch dort nicht.[18] Insgesamt existiert sowohl in Deutschland als auch in den USA äußerst wenig rechtswissenschaftliche und rechtsökonomische Literatur, die versucht, die Implikationen von DRM-Systemen mit all ihren Schutzmechanismen in einer vereinheitlichenden Analyse zu untersuchen. Die vorliegende Arbeit will diese Lücke füllen. Eine solche Untersuchung wird durch die Tatsache erschwert, daß DRM-Systeme im Schnittfeld zwischen Technik, Recht und Ökonomie angesiedelt sind. Eine Untersuchung von DRM-Systemen aus nur einer Perspektive – sei es die Perspektive des Technikers, des Juristen oder des Ökonomen – wird allenfalls Teilaspekte zu Tage fördern, ohne die tiefergreifenden Veränderungen, die durch DRM-Systeme hervorgerufen werden, adäquat zu erfassen. Selbst wenn man sich auf einen interdisziplinären Ansatz einläßt, bestehen jedoch hohe Hürden. Die technische Entwicklung von DRM-Systemen ist bei weitem nicht abgeschlossen. Umfassende Darstellungen der technischen Grundlagen von DRM-Systemen fehlen vollständig. In den meisten Fällen ist es daher erforderlich, auf die – für einen Juristen oft schwer verständliche – primäre Forschungsliteratur zurückzugreifen. Nicht anders sieht es bei den Ökonomen aus. Die Auswirkungen des Internet und anderer digitaler Medien auf ökonomische Standardmodelle sind noch in weiten Teilen unklar. Zwar bestehen umfangreiche Forschungsanstrengungen, um diese Wissenslücke zu schließen. Eine abschließende Darstellung, die gerade für ein interdisziplinäres Arbeiten wünschenswert erscheint, fehlt aber auch hier.[19] Wenn man diese Zustände bedenkt, erscheint es nicht verwunderlich, daß auch die Juristen noch in weiten Bereichen im Nebel stochern. Welche Auswirkungen DRM-Systeme auf das herkömmliche Urheberrecht haben und in welcher Weise

[17] Die Untersuchung von *Wand* beschäftigt sich ausschließlich mit dem rechtlichen Umgehungsschutz technischer Schutzmaßnahmen und erfaßt damit nur einen von mehreren Bereichen von DRM-Systemen im hier verstandenen Sinne.

[18] Die Darstellung des *National Research Council* gibt zwar einen informativen Überblick über die DRM-Problematik. Viele der in der vorliegenden Arbeit angesprochenen Fragen werden jedoch allenfalls gestreift.

[19] Das grundlegende Buch von *Shapiro/Varian* und das informative Werk des *European Communication Council* gehen zwar in diese Richtung, werfen aber – zu Recht – oftmals mehr Fragen auf, als daß sie Antworten bieten.

der Gesetzgeber beziehungsweise die Gerichte darauf reagieren sollten, ist teilweise umstritten und wird oft – insbesondere in Deutschland – noch gar nicht richtig problematisiert.

Die vorliegende Arbeit hat dreierlei zum Ziel. Als *erstes Ziel* will sie einen Überblick über den derzeitigen Stand der rechtlichen, technischen und ökonomischen Rahmenbedingungen von DRM-Systemen geben. In der derzeitigen juristischen Diskussion werden die technischen und ökonomischen Grundlagen von DRM-Systemen oftmals nur gestreift, auch wenn sie in der juristischen Argumentation an zentraler Stelle verwendet werden. Wenn man in juristischen Darstellungen liest, unter technischen Schutzmaßnahmen seien Hardware-Dongles zu verstehen, digitale Wasserzeichen seien die Lösung aller Probleme des Urheberschutzes im Internet und DRM-Systeme seien technisch ausgereift, so entspricht dies nicht dem heutigen Stand der technischen Entwicklung. Wenn in juristischen Darstellungen behauptet wird, durch DRM-Systeme würden unter dem Gesichtspunkt der ökonomischen Analyse urheberrechtliche Schrankenbestimmungen obsolet, so ist diese Aussage regelmäßig verkürzt und einseitig. Der Verfasser ist der Überzeugung, daß juristische Fragen von technischen Schutzmaßnahmen und DRM-Systemen nur dann adäquat behandelt werden können, wenn die technischen und – zu einem geringeren Maße – die ökonomischen Grundlagen dieser Phänomene verstanden werden.[20]

Als *zweites Ziel* will die Arbeit die Implikationen des „Digital Rights Management" auf das Urheberrecht untersuchen. Dabei verfolgt sie einen dezidiert interdisziplinären Ansatz im Schnittfeld von Recht, Technik und Ökonomie. Es ist das Ziel dieser Arbeit aufzuzeigen, daß die wirklichen Veränderungen, die durch DRM-Systeme auf das Urheberrecht zukommen könnten, nur bei einer Betrachtung aller drei Disziplinen adäquat erfaßt werden können. Die Arbeit läßt sich gleichzeitig als ein Plädoyer für mehr Interdisziplinarität im Internet-Recht verstehen. Wenn auch für eine juristische Untersuchung ungewöhnlich, scheut sich die Arbeit daher nicht, die technischen und ökonomischen Grundlagen von DRM-Systemen detailliert darzustellen.

Die Arbeit setzt sich zum *dritten Ziel*, die umfangreiche wissenschaftliche Diskussion zu DRM-Systemen, die sich in den letzten Jahren in den USA entwickelt hat, in Deutschland einzuführen. Wie in vielen Bereichen

[20] In diese Richtung geht auch *Hoeren*, wenn er in MMR 11/2000, S. XVIII, meint: „Sich in der Kunst der Steganographie auszukennen, ist für Internetrechtler ein Muß. [… Es ist] für Juristen wichtig […], über Grundkenntnisse im Bereich der digitalen Wasserzeichen zu verfügen. […] Denn wenn die Antwort auf die vielfältigen Probleme des Internet zumindest auch in den technischen Grundlagen des Internet zu suchen ist, muß sich ein Jurist auch Arkandisziplinen wie der Steganographie stellen." Zu digitalen Wasserzeichen und der Abgrenzung gegenüber der Steganographie s. unten Teil 1, C II 2 b bb 1.

des Internet-Rechts ist die Diskussion zu DRM-Systemen in den USA sehr viel weiter fortgeschritten als in Deutschland und Europa. Zwar existieren zu Einzelfragen der U.S.-amerikanischen Diskussion auch in Deutschland längere Abhandlungen. Eine umfassende Darstellung der U.S.-amerikanischen Diskussion zu DRM-Systemen in deutscher Sprache existiert jedoch nicht.

Die vorliegende Arbeit versucht nicht, alle auftretenden Einzelfragen im Bereich von DRM-Systemen zu analysieren, geschweige denn zu lösen. Sie will vielmehr die Entwicklung von DRM-Systemen in ihrer Gesamtheit darstellen und dabei allgemeine Entwicklungslinien herausarbeiten. Dieser Ansatz bringt es mit sich, daß die Arbeit oftmals mehr Fragen aufwirft, als sie beantworten kann. Wenn es nur schon gelingen würde, die richtigen Fragen zu stellen, wäre viel gewonnen.

B. Gang der Untersuchung

Im *ersten Teil* der Untersuchung wird ein ausführlicher Überblick über den derzeitigen technischen Stand von DRM-Systemen gegeben. Dabei werden die Funktionalität der unterschiedlichen technischen Komponenten und ihr derzeitiger Entwicklungsstand dargestellt sowie eine Bewertung zu der Frage abgegeben, welche Rolle sie in DRM-Systemen spielen beziehungsweise spielen werden. Im *zweiten Teil* werden die rechtlichen Grundlagen von DRM-Systemen dargestellt. Dabei wird auf die unterschiedlichen rechtlichen Schutzmechanismen eingegangen, die in DRM-Systemen relevant sind (Urheberrecht, Nutzungsverträge, Technologie-Lizenzverträge und rechtlicher Umgehungsschutz). Grundlage der Untersuchung ist die Rechtslage in der Europäischen Union, Deutschland und den USA. Im *dritten Teil* werden – aufbauend auf der deskriptiven Darstellung der ersten beiden Teile – die Auswirkungen von DRM-Systemen auf das herkömmliche Urheberrecht untersucht. In diesem Rahmen wird auch die rechtsökonomische Diskussion zu DRM-Systemen ausführlich dargestellt. Es wird der Frage nachgegangen, ob und inwieweit DRM-Systeme einen Ersatz für den Schutz durch das herkömmliche Urheberrecht bieten. Dabei zeigt sich die Notwendigkeit, den Schutz von DRM-Systemen zu beschränken.[21] Im *vierten Teil* wird untersucht, wie der Gesetzgeber auf diese Notwendigkeit theoretisch reagieren könnte und wie die Gesetzgeber in der Europäischen Union, Deutschland und den USA tatsächlich reagiert haben. Im *fünften Teil* wird in einem Ausblick dargestellt, daß die aufgeworfenen Probleme von DRM-Systemen

[21] Der dritte Teil stellt den analytischen Kern der Arbeit dar. Der ungeduldige Leser mag sich daher mit der Lektüre dieses Teils – und möglichst noch des vierten Teils – begnügen.

ein spezieller Anwendungsfall allgemeinerer Fragen eines entstehenden Informationsrechts sind, dessen Konturen heute noch in weiten Bereichen unklar sind.

C. Beschränkung der Untersuchung

Nachdem dargestellt wurde, mit was sich die vorliegende Untersuchung befaßt, erscheinen einige Worte angebracht, mit was sich die vorliegende Untersuchung *nicht* befaßt. DRM-Systeme werfen vielfältige rechtliche Probleme auf, von denen die vorliegende Untersuchung nur einen Teil behandelt.[22]

Erstens befaßt sich die Arbeit nicht mit Fragen des Urheberrechts außerhalb digitaler Medien. Auf analoge Speichermedien (Musikkassetten, Videokassetten, herkömmliche Bücher und ähnliches) geht die Arbeit nicht ein. Auch in Zukunft wird es öffentliche Aufführungen urheberrechtlich geschützter Werke geben, die von DRM-Systemen in keiner Weise berührt werden. Allerdings ist zu beachten, daß mehr und mehr urheberrechtliche Verwertungsformen in digitaler Form durchgeführt werden. Damit steigt auch der Anwendungsbereich von DRM-Systemen.

Zweitens beschäftigt sich die Arbeit schwerpunktmäßig mit den Auswirkungen von DRM-Systemen auf den Konsumentenmarkt. Daher geht die Arbeit nicht darauf ein, welche Auswirkungen DRM-Systeme auf das herkömmliche Geflecht von Urhebern, Leistungsschutzberechtigten, Produzenten, Verlagen, Agenten und Verwertungsgesellschaften haben könnten. Hier stellen sich vielfältige Probleme. So wäre die Bedeutung von Verwertungsgesellschaften zu untersuchen. Verwertungsgesellschaften waren entstanden, um ein besseres Vertragsgleichgewicht zwischen Rechteinhabern und Verwertern zu schaffen und um beiden Gruppen beim Rechteerwerb im täglichen Massengeschäft behilflich zu sein. Durch die Ubiquität urheberrechtlich geschützter Werke und die Internationalität der Sachverhalte war der einzelne Urheber außerstande, die Nutzung seiner Werke selbst zu kontrollieren. Auf der anderen Seite war es dem Verwerter praktisch nicht möglich, die notwendigen Rechte auf individuellem Weg zu beschaffen. Um die sehr hohen Transaktionskosten bei einer individuellen Rechtewahrnehmung zu vermeiden, entstanden Verwertungsgesellschaften.[23] Aufgrund des pauschalierenden Vergütungssystems der Verwertungsgesellschaften (s. nur § 7 WahrnG)[24] nimmt man jedoch eine Verzer-

[22] Einen Überblick über Rechtsprobleme von DRM-Systemen geben *Möschel/Bechtold*, MMR 1998, 571, 574 f., und *dies.* in: Pfitzmann/Roßnagel (Hrsg.).

[23] S. *Bechtold*, GRUR 1998, 18, 21 m.w.N., und *Pethig*, 144 JITE 462, 488 f. (1988).

[24] S. dazu *Schack*, Rdnr. 1216 ff.

rung der Vergütungsverteilung in Kauf: Die Ausschüttung an die Urheber entspricht nicht den tatsächlich getätigten Nutzungen. Daneben blieben Verwertungsgesellschaften second-best-Lösungen. Man schuf seinerseits kontrollbedürftige Monopolorganisationen.[25] Die daraus entstehenden Wohlfahrtsverluste ließen sich nur mit der Vermeidung hoher Transaktionskosten rechtfertigen. In bestimmten Bereichen könnten DRM-Systeme jedoch zu einer deutlichen Senkung von Transaktionskosten führen. Dadurch könnten pauschalierende Leerträger-, Geräte- und Betreiberabgaben, die in §§ 54 ff. UrhG geregelt sind und die von Verwertungsgesellschaften eingezogen werden (§ 54 h Abs. 1 UrhG), unnötig werden. In Zukunft könnte die einzelne Nutzung eines Werks kostengünstig registriert und zur Grundlage einer individuellen Abrechnung gemacht werden. Auch pauschale Lizenzen für das gesamte Repertoire einer Verwertungsgesellschaft, über die beispielsweise Sendeunternehmen im Rundfunkbereich verfügen, könnten überflüssig werden. Ein derartiges dezentrales Vergütungsmodell könnte sich gegenüber der traditionellen kollektiven Rechtewahrnehmung durch Verwertungsgesellschaften durch geringere Betriebskosten sowie deutlich geringere Transaktionskosten und Allokationsverzerrungen auszeichnen.[26] Unter ökonomischen Gesichtspunkten läßt sich dieser Trend von der Kollektiv- zur Individualverwertung mit dem englischen Begriff der „Disintermediation" kennzeichnen.[27] Der Produzent kann grundsätzlich mit dem Konsumenten direkt in Kontrakt treten. Andererseits läßt sich eine gegenläufige Entwicklung beobachten, die als „Reintermediation" bezeichnet wird. Im Internet entstehen zunehmend neue Arten von Intermediären – Informationsvermittler, Suchmaschinen, Portale und ähnliches. Eine vollständige „Disintermediation" ist keineswegs eine notwendige Folge des E-Commerce.[28] Für den Bereich der DRM-

[25] S. dazu *Tietzel/Weber* in: Ott/Schäfer (Hrsg.), S. 128, 138 f.; *Bechtold*, GRUR 1998, 18, 21; *Möschel/Bechtold*, MMR 1998, 571, 576; s. a. *Schack*, Rdnr. 1196a; *ders.*, JZ 1998, 753, 759; *Wand*, S. 59; *Dreier*, CR 2000, 45, 46 f.

[26] So schon ausführlich *Bechtold*, GRUR 1998, 18, 21 f.; *Möschel/Bechtold*, MMR 1998, 571, 576; vgl. weiterhin *Schack*, Rdnr. 1196a; *Schack*, JZ 1998, 753, 759; *Wand*, S. 59, 180; *Dreier*, CR 2000, 45, 46 f.; *Leinemann*, S. 166; *Garnett/James/Davies*, Rdnr. 28–46. *Tietzel/Weber* in: Ott/Schäfer (Hrsg.), S. 128, 143 ff., propagierten daher schon 1994 ein individuelles Vergütungssystem für Papierkopien durch die Einführung maschinenlesbarer Barcodes, wodurch Geräte- und Betreiberabgaben unnötig würden.

[27] Das Phänomen der „Disintermediation" läßt sich in vielen Bereichen des E-Commerce beobachten. In herkömmlichen Märkten können Intermediäre, beispielsweise Zwischenhändler, dazu beitragen, Transaktionskosten zwischen Anbietern und Nachfragern zu senken. Da im Internet Transaktionskosten sinken, könnten Intermediäre im digitalen Umfeld an Bedeutung verlieren; s. *Bailey*, S. 127.

[28] Zur „Disintermediation" und „Reintermediation" im E-Commerce-Bereich s. *European Communication Council* (Hrsg.), S. 18 f., 226 ff.; *Smith/Baily/Brynjolfsson* in: Brynjolfsson/Kahin (Hrsg.), S. 99, 121 ff.; *Bakos*, 41 (8) Comm. ACM, 35, 42 (August 1998); *Bailey*, S. 13 ff., 33 ff.; *Giaglis/Klein/O'Keefe*; *Chirsu/Kauffman*, 4 (4) International Journal of Electronic Commerce 7 ff. (Sommer 2000); *Patterson*.

Systeme und Verwertungsgesellschaften bedeutet dies, daß Urheber in DRM-Systemen zwar grundsätzlich eine Stellung zurückerhalten, die sie im Zeitalter der Massenvervielfältigung nahezu verloren hatten: die Möglichkeit der individuellen Rechtevergabe.[29] Jedoch erscheint es unrealistsch anzunehmen, daß in Zukunft jeder Urheber in einem DRM-System die Rechtevergabe und Nutzungskontrolle selbst in die Hand nehmen wird.[30] Zentrale Institutionen, die eine Mittlerfunktion zwischen dem Urheber und den Nutzern wahrnehmen, werden auch in DRM-Systemen nicht obsolet werden („Reintermediation"). Diese Mittlerfunktionen könnten von Verwertungsgesellschaften, aber auch von anderen Institutionen – Tonträgerunternehmen oder ganz neu geschaffenen Unternehmen[31] – wahrgenommen werden. Zumindest würde sich Bedeutung und Aufgabe der Verwertungsgesellschaften in einem solchen Umfeld deutlich wandeln.[32] Eine ausführliche Untersuchung zu den Auswirkungen von DRM-Systemen auf Verwertungsgesellschaften existiert nicht.[33] Dazu wären neben der Untersuchung der ökonomischen Grundlagen von Verwertungsgesellschaften[34] auch empirische Erhebungen notwendig. Die vorliegende Arbeit kann und will diese Untersuchung nicht leisten. An dieser Stelle soll nur auf die Problemdimension hingewiesen werden.

Mit dieser Beschränkung des Untersuchungsgegenstands hängt zusammen, daß die vorliegende Arbeit nicht darauf eingeht, welche Auswirkungen DRM-Systeme auf die Beziehungen der unterschiedlichen Rechteinhaber untereinander – Urheber, Inhaber von Leistungsschutzrechten, Verlage, Produzenten und so weiter – haben könnten.[35] Die Arbeit legt ihren Schwerpunkt auf die Auswirkungen des „Digital Rights Management" im Verhältnis zwischen den Rechteinhabern und den Nutzern,

---

[29] *Bechtold*, GRUR 1998, 17, 21 f.

[30] S. a. *Merges*, 84 Cal. L. Rev. 1293, 1382 (1996).

[31] In diese Richtung gehen die Ankündigungen der großen Tonträgerunternehmen im April 2001, ihre digitalen Musikangebote über gemeinsame Lizenzierungsstellen – „MusicNet" im Falle der Bertelsmann Music Group, EMI und Warner sowie „Pressplay" im Falle von Sony und Universal – zu vermarkten.

[32] S. a. *Dreier*, CR 2000, 45, 47.

[33] Einzig *Merges*, 84 Cal. L. Rev. 1293, 1380 ff. (1996), geht auf diese Frage ausführlicher ein. Er zeigt die Problemdimensionen auf und weist auf mehrere Probleme von DRM-Systemen in diesem Kontext hin. *Merges* steht der These einer „Disintermediation" in diesem Bereich skeptisch gegenüber, da Institutionen wie Verwertungsgesellschaften noch eine Fülle weiterer Funktionen hätten, die dabei nicht berücksichtigt würden, beispielsweise das Sammeln von Erfahrung hinsichtlich der Preisbildung und Nutzungsbedingungen bei urheberrechtlich geschützten Werken; auch sprächen deutliche Skalenvorteile für Verwertungsgesellschaften, s. *Merges*, 84 Cal. L. Rev. 1293, 1387 (1996).

[34] Eine rechtsökonomische Analyse U.S.-amerikanischer Verwertungsgesellschaften liefern *Besen/Kirby/Salop*, 78 Va. L. Rev. 383 (1992). In der deutschsprachigen Literatur ist u. a. der Beitrag von *Tietzel/Weber* in: Ott/Schäfer (Hrsg.), S. 128 ff., zu nennen.

[35] Auch hier können DRM-ähnliche Systeme Verwendung finden. Dabei geht es insbesondere um sog. „One-Stop-Shops", s. dazu unten Teil 1, D V.

nicht auf die Auswirkungen im Verhältnis der Rechteinhaber untereinander. Daher spricht die Arbeit oftmals pauschal von „den Rechteinhabern". Darunter können Urheber und Inhaber von Leistungsschutzrechten, aber auch Verwerter fallen, die entsprechende Nutzungsrechte erhalten haben (beispielsweise Verlage).[36] Die pauschale Bezeichnung als „Rechteinhaber" stellt natürlich eine Vereinfachung der tatsächlichen Rechtslage dar. Wie sich zeigen wird, ist für das vorliegende Erkenntnisinteresse eine Differenzierung nach unterschiedlichen Rechteinhabern jedoch nicht notwendig. Auch wird auf die rechtliche Qualifizierung der Vertragsbeziehungen zwischen den Rechteinhabern und den Anbietern eines technischen DRM-Systems sowie zwischen den DRM-Anbietern und den Nutzern nicht eingegangen.[37] Hin und wieder wird die Arbeit auch pauschal von den Auswirkungen von DRM-System auf „das Urheberrecht" sprechen. Darunter ist regelmäßig der gesamte Komplex ausschließlicher Verwertungsrechte zu verstehen, die in den Urheberrechtsgesetzen geregelt sind – also sowohl die Rechte der Urheber als auch die Rechte der Leistungsschutzberechtigten. Die vorliegende Untersuchung differenziert bei solchen Aussagen nicht zwischen Urhebern und Leistungsschutzberechtigten, da sie die Auswirkungen von DRM-Systemen auf den Schutz *aller* Rechteinhaber untersucht.

Als *dritte* Beschränkung des Untersuchungsgegenstands beschäftigt sich die vorliegende Arbeit nur am Rande mit eventuellen kartellrechtlichen Problemen von DRM-Systemen.[38] *Viertens* befaßt sich die Arbeit bei der Darstellung rechtlicher Regelungen nicht mit Fragen des anwendbaren Rechts. *Fünftens* geht die Arbeit nur vereinzelt auf die datenschutzrechtlichen Probleme von DRM-Systemen ein. Mit Hilfe von DRM-Systemen können grundsätzlich umfassende Nutzerprofile erstellt werden.[39]

---

[36] Andere wichtige „Rechteinhaber" in DRM-Systemen sind Tonträgerunternehmen und Filmstudios. Die Verwerter erhalten regelmäßig ein Nutzungsrecht von Urhebern oder Leistungsschutzberechtigten eingeräumt und sind damit ebenfalls – wenn auch nicht originäre – „Rechteinhaber".

[37] *Cichon*, S. 285 ff., untersucht an einem einfachen DRM-Modell die zugrundeliegenden Vertragsbeziehungen.

[38] S. dazu im Überblick *Möschel/Bechtold*, MMR 1998, 571, 575; *dies.* in: Pfitzmann/Roßnagel (Hrsg.), S. 8 ff.; zum Verhältnis von technischen Schutzmaßnahmen zu Art. 82 EGV ausführlich *Kirk*, I.P.Q. 1999, 37 ff.; zum Verhältnis von „One-Stop-Shops" und Clearingstellen zum europäischen Kartellrecht s. *Wünschmann*, ZUM 2000, 572 ff. Zur wettbewerbsrechtlichen Frage, ob ein „Reverse Engineering" digitaler Wasserzeichenverfahren zu Interoperabilitätszwecken zulässig ist, s. *Lai/Buonaiuti* in: Katzenbeisser/Petitcolas (Hrsg.), S. 191, 196 f.

[39] S. dazu ausführlich *Bygrave/Koelman* in: Hugenholtz (Hrsg.), S. 59 ff.; *Greenleaf*, „IP, Phone Home"; *International Working Group on Data Protection in Telecommunications*; *Sander*, S. 9 ff.; vgl. weiterhin *Weinberg*, 52 Stan. L. Rev. 1251 ff. (2000); *Cohen*, 13 Berkeley Tech. L. J. 1089, 1102 ff. (1998); *Froomkin*, 52 Stan. L. Rev. 1461, 1488 f. (2000); *Lai/Buonaiuti* in: Katzenbeisser/Petitcolas (Hrsg.), S. 191, 197 ff.; *Lessig*, S. 138 f.; *Gervais* in: Koskinen-Olsson/Gervais (Hrsg.), S. 6, 14 f.; *Ladeur*, MMR 2000, 715 ff.

Trotz des interdisziplinären Ansatzes geht die Arbeit *sechstens* nicht auf betriebswirtschaftliche Aspekte von DRM-Systemen ein. DRM-Systeme ermöglichen neue Geschäftsmodelle beim Vertrieb digitaler Inhalte.[40] So kann die Aggregation unterschiedlicher Inhalte zu Informationsbündeln eine wichtige Rolle spielen.[41] Auch könnten die Digitalisierung und DRM-Systeme traditionelle Wertschöpfungsketten verändern.[42]

Siebtens geht die Arbeit nur auf den urheberrechtlichen Anwendungsbereich von DRM-Systemen ein. Neben dem Schutz schöpferischer Leistungen können DRM-Systeme aus technischer Sicht noch in anderen Bereichen eingesetzt werden, unter anderem im Datenschutz, im Jugendschutz, zum Schutz medizinischer Daten oder von Daten im Geschäftssektor (Börsenkurse und ähnliches).[43] Wird in einer Klinik ein digitales Röntgenbild des Brustkorbs eines Patienten erstellt und zu einem niedergelassenen Arzt übertragen, so könnten DRM-Systeme diese Übertragung gegen unbefugte Zugriffe sichern. Gleichzeitig könnte der Patient und die Klinik von dem DRM-System Auskunft erhalten, ob und wann das Röntgenbild beim Arzt angekommen ist und wer zu welchem Zeitpunkt das Röntgenbild genutzt hat. Manche Ergebnisse der vorliegenden Untersuchung lassen sich auf solche Einsatzgebiete von DRM-Systemen übertragen. Diese Übertragung liegt jedoch nicht im Erkenntnisinteresse der Arbeit. *Schließlich* geht die Arbeit nur sporadisch auf einzelne DRM-Systeme ein, die heute am Markt verfügbar sind.[44] Dies wäre angesichts

---

[40] *Durfee/Franklin* in: Jajodia (Hrsg.), S. 63; *Sander*.

[41] S. dazu *Bakos//Brynjolfsson* in: Kahin/Varian (Hrsg.), S. 114 ff.; *Shapiro/Varian*, S. 53 ff.

[42] S. dazu *European Communication Council* (Hrsg.), S. 62 ff., 173 ff.; *Kulle*, S. 248 f.

[43] *Shear*, S. 2, meint: „Literally any digital information that is shared or stored will ultimetaly be implicated, however. This includes, for example, medical records, enterprise workflow, financial interactions, and the policy management of any stored or communicated information – policies ranging from privacy rights to enforcing government regulations to reliably automating commercial interests." Zur Verwendung technischer Schutzmaßnahmen im Patentrecht s. *Wand*, S. 9.

[44] Dagegen werden ausführlich die unterschiedlichen Standards dargestellt, die heute im DRM-Bereich existieren. Im Gegensatz zu den DRM-Systemen einzelner Anbieter sind bei DRM-Standards regelmäßig bessere Dokumentationen öffentlich verfügbar. Dennoch sollen an dieser Stelle einige wichtige Anbieter von DRM-Systemen genannt werden. Das wohl wichtigste Unternehmen in diesem Bereich mit dem umfassendsten DRM-Ansatz, das seit Anfang der 90er Jahre an DRM-Systemen arbeitet, ist InterTrust Technologies Corporation in Kalifornien, <http://www.intertrust.com>. Daneben etabliert sich in letzter Zeit Microsoft als Hauptkonkurrent, s. <http://www.microsoft.com/windows/windowsmedia/en/wm7/drm.asp>. Weiter zu erwähnen ist Contentguard, das zu Xerox gehört (s. <http://www.contentguard.com>), das „Electronic Media Management System" (EMMS) von IBM (s. <http://www-4.ibm.com/software/is/emms>) und das Liquid Audio DRM-System (s. <http://www.liquidaudio.com/services/distribution/drm/index.jsp>; Reciprocal, <http:// www.reciprocal.com>, bietet insbesondere Clearinghouse-Dienstleistungen für DRM-Systeme an. Das britische Unterneh-

der ungeheuren Vielzahl der beteiligten Akteure auch schwer möglich. Allein in den USA liegt die Zahl der Unternehmen, die Produkte für DRM-Systeme anbieten, bei weit über 100.[45] Die Arbeit will allgemeine Aussagen zu DRM-Systemen treffen, die von der Ausgestaltung eines bestimmten DRM-Systems weithin unabhängig sind.

D. Terminologisches

Bei einer interdisziplinären Untersuchung besteht regelmäßig keine Einigkeit über verwendete Begriffe. Dies zeigt sich auch bei DRM-Systemen. Was für den Urheberrechtler ein „Werk", eine „schöpferische Leistung" ist, sind für den Techniker bloße „Daten" und für den Ökonomen ein „Informationsgut". Was für den Urheberrrechtler der „Urheber" oder „Schöpfer" ist, ist für den Ökonomen der „Informationsproduzent". Um Mißverständnisse zu vermeiden, verwendet die vorliegende Arbeit eine weitgehend einheitliche Terminologie. Die Musikstücke, Videofilme, Texte und ähnliches, die in einem DRM-System geschützt werden, werden als „digitaler Inhalt" bezeichnet. Es wird auf die Verwendung des Begriffs „Werk" verzichtet. Der Schutz von DRM-Systemen greift unabhängig von den urheberrechtlichen Anforderungen an ein Werk.[46] In DRM-Systemen können auch Inhalte geschützt werden, die keinem Schutz durch das Urheberrecht oder ein verwandtes Schutzrecht unterliegen. Es geht um den Schutz von „Information" im weitesten Sinne.[47] Alles, was digitalisiert werden kann, ist Information und damit „digitaler Inhalt" im hier verstandenen Sinne.[48] Darunter fallen Bücher, Zeitschrif-

men Magex, <http:// www.magex.com>, bietet – aufbauend auf der DRM-Technologie von InterTrust – DRM-Dienstleistungen an. Das zu Bertelsmann gehörende Unternehme Digital World Services, <http://www.dwsco.com>, arbeitet an DRM-Lösungen, die unter anderem in Napster eingesetzt werden sollen. Manipulationssichere Hard- und Software für den DRM-Bereich werden auch von Wave Systems, http://www.wave.com>, entwickelt. Weitere Unternehmen im DRM-Umfeld sind das israelische Unternehmen Midbar Tech, <http://www.midbartech.com>, das britische Unternehmen Rightscom, <http://www.rightscom.com>, und das kanadische Unternehmen RightsMarket, <http://www.rightsmarket.com>.

[45] *Association of American Publishers*, Digital Rights Management for Ebooks, S. 6.

[46] Zu Anforderungen, insbesondere dem Begriff der „persönlichen geistigen Schöpfung" (s. § 2 Abs. 2 UrhG), s. *Schack*, Rdnr. 152 ff.

[47] Ähnlich die Definition von *Heide*, 15 Berkeley Tech. L. J. 993, 994 Fn. 1 (2000): „The term ‚information' product as used herein is used broadly to refer to any material capable of being digitized and distributed as part of a service over computer networks such as the Internet or any material incorporated in a physical carrier and distributed together with that carrier. The term is not intended to be a legal term of art and will include any copyrighted work as well as information and material not meeting the requisite originiality thresholds applicable to copyright protection."

[48] Ebenso *Shapiro/Varian*, S. 3.

ten, Filme, Musik, WWW-Seiten, Videospiele, aber auch Börsenkurse, Datenbanken und vieles mehr. Auch Computersoftware fällt unter den Begriff des „digitalen Inhalts"; Software kann in geschützter Form über ein DRM-System vertrieben werden.

Derjenige, welcher den digitalen Inhalt in einem DRM-System anbietet, wird als der „Inhalteanbieter" bezeichnet. Der Inhalteanbieter wird regelmäßig gleichzeitg ein Rechteinhaber sein.[49] Derjenige, der ein DRM-System unterhält und den Inhalteanbietern ermöglicht, ihre digitalen Inhalte über das DRM-System zu vertreiben, wird „DRM-Systembetreiber" genannt. Auch dies stellt eine grobe Vereinfachung dar. Regelmäßig werden die Aufgaben des „DRM-Systembetreibers" auf eine Vielzahl unterschiedlicher Akteure verteilt sein.[50] Diese Ausdifferenzierung in der Realität ändert jedoch nichts an den hier angestellten Untersuchungen. Ein DRM-System setzt sich aus unzähligen technischen Bestandteilen zusammen, die als „DRM-Systemkomponenten" bezeichnet werden. Derjenige, der einen digitalen Inhalt in einem DRM-System nutzt, also beispielsweise ein Musikstück anhört oder einen Videofilm ansieht, wird als Nutzer, teilweise auch als Konsument, bezeichnet. Er kann die digitalen Inhalte auf einem „DRM-kompatiblen Endgerät" benutzen. Endgeräte in diesem Sinne können Computer, Fernseher mit Set-Top-Boxen, digitale Videorekorder, mobile Abspielgeräte ähnlich einem MP3-Player, DVD-Spieler, „Personal Digital Assistants" (PDAs), ja sogar Mobiltelefone sein. Unter den Begriff des „Endgeräts" fallen aber nicht nur spezielle Hardwaregeräte. Manche DRM-Systeme funktionieren rein softwaregestützt; in diesem Fall muß der Nutzer eines DRM-Systems nur eine spezielle „DRM Client"-Software auf seinem Computer installieren. Auch diese DRM-Software fällt unter den Begriff des „Endgeräts". Damit digitale Inhalte in einem bestimmten DRM-System vertrieben werden können, müssen diese regelmäßig in einem speziellen Datenformat gespeichert werden. Damit ein Endgerät diese digitalen Inhalte nutzen kann, muß es das entsprechende Datenformat verstehen. Ist dies der Fall und kann das Endgerät auch mit den anderen Systemkomponenten eines DRM-Systems zusammenarbeiten, so handelt es sich um ein „DRM-kompatibles Endgerät". Derjenige, der versucht, den Schutz von DRM-Systemen zu umgehen und digitale Inhalte zu nutzen, ohne dafür das entsprechende Entgelt zahlen zu müssen, wird „Angreifer" genannt. Hin und wieder wird auch der Begriff des „Electronic Commerce" oder des „E-Commerce" verwen-

[49] Zum Begriff des „Rechteinhabers", worunter die Inhaber von Urheber- und Leistungsschutzrechten, aber auch Verwerter wie beispielsweise Verlage fallen können, s. oben bei Fn. 36.

[50] Eine abstrakte Darstellung der unterschiedlichen Akteure, die beim Betrieb eines DRM-Systems interagieren, findet sich bei *IMPRIMATUR*, IMPRIMATUR Business Model, ein grafischer Überblick ist bei *Möschel/Bechtold*, MMR 1998, 571, 574, abgedruckt.

det. Solche Modeworte sind mit Vorsicht zu genießen. Unter „E-Commerce“ kann man alles oder nichts verstehen. Ein Ansatz ist, darunter alle Transaktionen zu verstehen, die in irgendeiner Weise oder zu irgendeinem Zeitpunkt elektronische Mittel einsetzen. Nach einem anderen Ansatz fallen darunter nur Transaktionen, die *vollständig* elektronisch abgewickelt werden. Zwischen diesen beiden Extremen liegt eine Facette von Zwischenformen.[51]

[51] *O'Rourke*, 14 Berkeley Tech. L. J. 635, 638 (1999).

Teil 1: Technische Grundlagen des DRM

The [music] industry will take whatever steps it needs to protect itself and protect its revenue streams. It will not lose that revenue stream, no matter what. […] We will develop technology that transcends the individual user. We will firewall Napster at source – we will block it at your cable company, we will block it at your phone company, we will block it at your [Internet service provider]. We will firewall it at your PC. […] These strategies are being aggressively pursued because there is simply too much at stake.[52]

A. Allgemeines

Ein umfassender Überblick über die technischen Grundlagen von „Digital Rights Management"-Systemen existiert nicht, weder in deutscher noch in englischer Sprache. In der juristischen Literatur finden sich regelmäßig nur verstreute Hinweise auf bestimmte DRM-Systemkomponenten wie digitale Wasserzeichen oder Verschlüsselungsverfahren. Im technischen Bereich existiert zwar eine unüberschaubare Fülle an Literatur. Diese deckt aber in den meisten Fällen nur detaillierte Teilfragen von DRM-Systemen ab. Eine überblicksartige Darstellung fehlt auch in der technischen Literatur.[53] Dies liegt zumindest auch daran, daß sich viele der Systemkomponenten noch im Entwicklungsstadium befinden, eine abschließende Darstellung daher unmöglich ist. Die vorliegende Arbeit setzt sich zum Ziel, die Beziehung zwischen rechtlicher und technischer Regulierung bei DRM-Systemen zu untersuchen. Dafür ist es unerläßlich, einen ausführlichen Überblick über die technischen Grundlagen von DRM-Systemen zu geben, der in seinem Umfang über das in juristischen Darstellungen Übliche weit hinaus geht. Es wird versucht, in verständli-

---

[52] *Steve Heckler*, Senior Vice President von Sony Pictures Entertainment, Inc., USA, in einer Konferenzrede im August 2000; zitiert nach <http://www.uwiretoday.com/computing081700001.html> und <http://www.theregister.co.uk/content/6 12780.html>.

[53] Zwar existiert mit *Wayner*, Digital Copyright Protection, eine gute Einführung in technische Schutzmaßnahmen. Jedoch ist das Werk einerseits teilweise veraltet, andererseits deckt es nicht die gesamte Bandbreite der Komponenten ab, die in DRM-Systemen eingesetzt werden können. Dagegen deckt das neuere Werk von *Anderson* unter dem Gesichtspunkt des „Security Engineering" größere Bereich des technischen DRM ab, wenn auch nicht mit dem expliziten Ziel, eine Einführung in DRM-Technologien zu geben.

cher Weise einen Überblick über den derzeitigen Entwicklungsstand sowie zukünftige Entwicklungen im DRM-Bereich zu geben.

DRM-Systeme beruhen auf einer Vielzahl technischer Komponenten. Zwar läßt sich die Idee von DRM-Systemen mehrere Jahrzehnte zurückverfolgen (dazu unten B). Aber erst in den letzten Jahren, frühestens seit Beginn der 90er Jahre, wurden intensive Anstrengungen unternommen, um vollständig integrierte DRM-Systeme zu entwickeln und zu etablieren. Der wichtigste Grundpfeiler eines DRM-Systems ist die technische Kontrolle des Zugangs und der Nutzung eines digitalen Inhalts (dazu unten C I). Da DRM-Systeme eine möglichst weitgehende Automatisierung des Vertriebs digitaler Inhalte anstreben, sind Maßnahmen zur maschinenlesbaren Identifizierung der Inhalte, der Nutzungsbedingungen und der Nutzer notwendig (dazu unten C II). Schließlich muß die Sicherheit des DRM-Systems und seiner Komponenten gewährleistet sein (dazu unten C III und C IV). Mitunter enthalten DRM-Systeme auch Verfahren, die im Internet nach rechtswidrig erstellten Kopien geschützter digitaler Inhalte suchen (dazu unten C V). Neben den technischen Schutzmaßnahmen können DRM-Systeme mit Zahlungssystemen kombiniert (dazu unten C VI) und in umfassende ECommerce-Systeme integriert werden (dazu unten C VII).

Fragen der Integration unterschiedlicher Systemkomponenten und der Standardisierung spielen bei DRM-Systemen eine große Rolle. Mehrere Standardisierungsinitiativen haben dazu geführt, daß sich DRM-Systemkomponenten schon heute in einer Vielzahl von Unterhaltungselektronik-Geräten finden (dazu insgesamt unten D). Die technische Entwicklung von DRM-Systemen ist bei weitem noch nicht abgeschlossen. Viele Bereiche befinden sich noch im Entwicklungsstadium. Zwar ist eine genaue Vorhersage über die Bedeutung und konkrete Ausgestaltung künftiger DRM-Systeme unmöglich. Betrachtet man jedoch die künftigen Potentiale der technischen Entwicklung (dazu unten E), spricht vieles dafür, daß DRM-Systeme eine bedeutende Stellung in einem zukünftigen E-Commerce-Umfeld haben werden.

B. Historische Entwicklung

Die Idee eines elektronischen Systems zur Nutzung und Abrechnung urheberrechtlich geschützter Werk ist nicht neu.[54] Schon im Jahr 1945 skizzierte *Vannevar Bush* in einem einflußreichen Aufsatz ein elektronisches Gerät namens „Memex“, das dem Nutzer eine umfassende private Biblio-

[54] Die Arbeit verzichtet bewußt auf eine ausführliche Darstellung der historischen Entwicklung technischer Schutzmaßnahmen und greift nur einige wichtige Ereignisse exemplarisch heraus.

thek zur Verfügung stellen sollte.[55] 1960 begann der Australier *Theodor Holm Nelson* mit der Konzeptionierung eines umfassenden Hypertext-Systems mit dem Namen „Xanadu".[56] Das Ziel des noch heute bestehenden Projekts[57] ist, ein vernetztes, universelles und dezentrales Speichermedium für Daten aller Art, insbesondere Textdokumente, zu entwickeln. Es geht um die Vision einer digitalen Bibliotheksumgebung.[58] Xanadu enthält auch einen Mechanismus, der die Vergütung der Werknutzung ermöglicht.[59]

In den 80er Jahren wurden für unterschiedliche Bereiche technische Schutzmaßnahmen entwickelt. So versahen viele Software-Hersteller ihre Computersoftware mit sogenannten „Dongles" und ähnlichem, um Raubkopien zu verhindern.[60] Pay-TV-Systeme wurden mit Schutzmaßnahmen versehen, um sicherzustellen, daß nur zahlende Nutzer das Pay-TV-Programm sehen konnten.[61] Für andere Medien wurden ähnliche Systeme entwickelt.[62]

Seit den 80er Jahren wurde an umfangreichen DRM-Systemen im engeren Sinne gearbeitet. *Ryoichi Mori* entwickelte in Japan ab 1983 das

---

[55] *Bush*, 176 (1) The Atlantic Monthly 101 ff. (1945); s. a. *Endres/Fellner*, S. 75 f. Urheberrechtliche Fragen werden in dem Aufsatz nicht angesprochen. Da Memex das Anlegen von Querverweisen zwischen verschiedenen Dokumenten ermöglichte, wird *Bush* als der Vater des „Hypertext"-Konzepts angesehen, das im WWW seinen Siegeszug angetreten hat. Der Begriff „Hypertext" selbst wurde 1965 von *Theodor Holm Nelson* geprägt.

[56] <http://www.xanadu.com.au>.

[57] Es befindet sich seit mehreren Jahrzehnten in einer Art dauerhaften Entwicklungsstadiums.

[58] *Nelson*, S. 0/6, 1/25 ff.; s. a. *Endres/Fellner*, S. 76.

[59] Die Vergütung wird nach der konsumierten Datenmenge berechnet. Als Beispiel gibt *Nelson* den Preis von 0,001 Cent pro konsumiertem Byte an; s. *Nelson*, S. 2/43 f., 5/13 ff.; *ders.*, 32 Educom Review 32 (1993). Dabei erhält auch ein Urheber, dessen Werk in einem anderen Werk nur zitiert wird, eine anteilige Vergütung, *ders.*, S. 2/45. Weiterhin kann der Ersteller eines Hyperlinks vom Nutzer bei der Benutzung dieses Links eine Vergütung verlangen. Das ganze System wird von *Nelson* als „transcopyright" bezeichnet, s. *ders.*, 32 (1) Educom Review 32 (1993). S. zum ganzen auch *Samuelson/Glushko*, 6 Harv. J. Law & Tech. 237, 247 ff. (1993), insbesondere deren kritischen Anmerkungen zum Verhältnis von Xanadu zum Urheberrecht.

[60] Zu Dongles s. unten Teil 1, C IV 1 a. Daneben wurden Paßwörter verwendet oder Software-Routinen eingebaut, die das Datum oder eine Seriennummer des Computer überprüfen, s. *Grover* in: Grover (Hrsg.), S. 1, 7 ff. Auch wurden Disketten entwickelt, bei denen die darauf gespeicherten Programme nicht kopiert werden konnten, s. *Sather*, in: Grover (Hrsg.), S. 26 ff. Weiterhin wurden andere manipulationssichere Hardware, Verschlüsselungsverfahren und Identifizierungsverfahren eingesetzt. Zu sogenannten „birthmarks", digitalen Fingerabdrücken, Wasserzeichen u. ä. bei Computersoftware s. *Grover* in: Grover (Hrsg.), S. 122 ff. Weitere Literaturhinweise bei *Collberg/Thomborson*, S. 2.

[61] S. dazu unten Teil 1, D II 2.

[62] Beispiele solcher Systeme finden sich bei *U.S. Congress, Office of Technology Assessment*, Intellectual Property Rights, S. 116 ff.; *dass.*, Copyright & Home Copying, S. 56 ff.

„Superdistribution"-Konzept, das eine spezielle Form eines DRM-Systems darstellt.[63] In den frühen 90er Jahren fingen Bibliotheken an, sich für Urheberrechtsmanagement-Systeme zu interessieren.[64] In dieser Zeit wurden mehrere Übersichten über DRM-Technologien und deren Auswirkungen auf das Urheberrecht verfaßt.[65] Die Europäische Kommission unterstützte – insbesondere im Rahmen ihres ESPRIT-Programmes – mehrere Forschungsprojekte, in denen die technischen, betriebswirtschaftlichen und rechtlichen Rahmenbedingungen von DRM-Systemen untersucht wurden.[66] Daneben existierten Projekte, in denen Fragen des allgemeineren ECommerce untersucht wurden, die auch für den DRM-Bereich von Interesse sein können.[67]

---

[63] S. dazu unten Teil 1, E I.

[64] S. nur *Garrett/Lyons*, 44 (8) Journal of the American Society for Information Science 468 ff. (1993), und das „Stanford Digital Library Technologies Project", <http://www-diglib.stanford.edu>, das ein Teil der von der U.S.-Regierung finanzierten „Digital Libraries Initiative" ist, s. <http://www.dli2.nsf.gov>. Zu digitalen Bibliotheken allgemein s. umfassend *Endres/Fellner*; s. a. *Stefik*, Internet Dreams, S. 1 ff.

[65] S. *Northeast Consulting*; *Tuck*.

[66] Auf eine genaue Darstellung der Ausrichtung und Ergebnisse der einzelnen Projekte wird verzichtet. Das bekannteste Projekt war das IMPRIMATUR-Projekt, das von Ende 1995 bis Ende 1998 dauerte. Im Rahmen dieses Projekts wurden u. a. ein „IMPRIMATUR Business Model" entwickelt und technische Grundlagen von DRM-Systemen aufgearbeitet. Daneben erstellte das „Institute for Information Law" der Universität Amsterdam unter Prof. *Bernt Hugenholtz* eine Vielzahl hochinteressanter Dokumente, die die rechtlichen Rahmenbedingungen von DRM-Systemen untersuchten, s. *Hugenholtz* (Hrsg.), Copyright and Electronic Commerce. Nähere Informationen zum IMPRIMATUR-Projekt finden sich unter <http://www.imprimatur.net> sowie bei *Barlas* in: Brunnstein/Sint (Hrsg.), S. 264 ff.*; Augot/Boucqueau/Delaigle/Fontaine/Goray*, 87 Proc. IEEE 1251, 1264 f. (1999). Ein sehr breit angelegtes Vorgängerprojekt stellte das schon 1988 begonnene Projekt „Copyright In Transmitted Electronic Documents" (CITED) dar, s. dazu *Bing*, 4 International Journal of Law and Information Technology 234, 264 f. (1996); *Wand*, GRUR Int. 1996, 897, 900. Zum CITED-Folgeprojekt CopySMART s. *Minard* in: Rowland/Meadows (Hrsg.), S. 283 ff.; zur CITED-Demonstrationsplattform COPICAT s. *Bing*, 4 International Journal of Law and Information Technology 234, 265 (1996). Zum von Ende 1995 bis Ende 1998 finanzierten COPEARMS-Projekt s. *Watkins*, 30 Computer Networks and ISDN Systems 1589 (1998), und <http://www.bl.uk/information/ifla/copearms.html>. Zum OCTALIS-Projekt s. <http://www.igd.fhg.de/igd-a8/projects/octalis> und <http://www.cordis.lu/esprit/src/p119.htm>. Zum australischen Propagate-Projekt s. <http://www.propagate.net> und *Greenleaf*, 21 U. New South Wales L. J. 593, 620 f. (1998). Zu weiteren Projekten (u. a. OKAPI, TALISMAN) s. *Bing*, 4 International Journal of Law and Information Technology 234, 261 ff. (1996), und *Bechtold*, GRUR 1998, 18, 19 ff.

[67] So im Rahmen des „Secure Electronic Marketplace for Europe (SEMPER)"-Projekts, das von Herbst 1995 bis Anfang 1999 dauerte; s. dazu *Lacoste/Pfitzmann/Steiner/Waidner* (Hrsg.); <http://www.semper.org>. Spezielle Fragen des Urheberrechts wurden dabei nicht behandelt.

C. Mögliche technische Komponenten eines DRM-Systems

I. Zugangs- und Nutzungskontrolle

Ein wesentliches Ziel von DRM-Systemen ist, den Zugang und die Nutzung zu digitalen Inhalten zu kontrollieren und dadurch den Nutzer zu veranlassen, für den Zugang und die Nutzung zu zahlen. Für diese Kontrolle bieten sich mehrere Verfahren an. Am wichtigsten sind Verschlüssungsverfahren (dazu unten 1). Daneben können technische Systeme eingesetzt werden, die die Anzahl der Kopien kontrollieren, die ein Nutzer erstellen kann (dazu unten 2). Schließlich können Paßwörter eingesetzt werden (dazu unten 3).

1. Verschlüsselung

> *Encryption of content is the keystone of current copy protection efforts.*[68]

Mit Verschlüsselungstechniken können digitale Inhalte derart modifiziert werden, daß sie nur für Nutzer brauchbar sind, die über einen entsprechenden Schlüssel zum Entschlüsseln des digitalen Inhalts verfügen. Selbst wenn ein Nutzer den verschlüsselten Inhalt kopieren kann, ist dieser für ihn ohne einen entsprechenden Schlüssel nutzlos. Der Inhalteanbieter stellt in einem DRM-System den Schlüssel nur solchen Nutzern zur Verfügung, die zuvor ein entsprechendes Entgelt entrichtet haben.

a) Verschlüsselungsverfahren

Grundsätzlich kann zwischen sogenannten „symmetrischen" und „asymmetrischen" Verschlüsselungsverfahren unterschieden werden. Bei symmetrischen Verschlüsselungsverfahren wird für das Verschlüsseln wie für das Entschlüsseln der gleiche Schlüssel verwendet.[69] Verwendet ein DRM-System ein symmetrisches Verschlüsselungsverfahren, so verschlüsselt der Inhalteanbieter den digitalen Inhalt mit einem von ihm gewählten Schlüssel und überträgt den digitalen Inhalt sowie den Schlüssel an den Nutzer, der den Inhalt dann wieder mit Hilfe des Schlüssels entschlüsseln kann. Dabei muß der Anbieter sicherstellen, daß nur solche Nutzer Zugriff auf den Schlüssel haben, die zu einer Nutzung des digitalen Inhalts berechtigt sind. Zu diesen Zwecken kann der Dechiffrier-Schlüssel von der Soft- und Hardwareumgebung beim Nutzer derart ge-

---

[68] *Marks/Turnbull*, EIPR 2000, 198, 204.

[69] Zu symmetrischen Verschlüsselungsverfahren allgemein s. *Selke*, S. 42 ff.; *Bauer*, S. 177 f.; *National Research Council*, S. 284 ff.

speichert werden, daß Dritte und auch der Nutzer selbst den Schlüssel nicht auslesen können.[70]

In vielen technischen Schutzsystemen spielen symmetrische Verschlüsselungsverfahren eine zentrale Rolle.[71] Kopierschutzmaßnahmen in Pay-TV-Systemen bauen regelmäßig auf symmetrischen Verschlüsselungsverfahren auf. Der Schlüssel zum Dechiffrieren des Pay-TV-Programms wird dabei in der Set-Top-Box des Nutzers abgelegt. Symmetrische Verschlüsselungsverfahren haben jedoch einen Nachteil: Der Anbieter muß dem Nutzer den Schlüssel mitteilen, den er zum Chiffrieren der Inhalte verwendete, da der Schlüssel gleichzeitig zum Dechiffrieren der Inhalte verwendet wird. Gelingt es einem Angreifer, diese Mitteilung des Schlüssels abzuhören, so kann auch er die Inhalte entschlüsseln.[72]

Dieses Problem lösen asymmetrische Verschlüsselungsverfahren („public key"-Algorithmen). Dabei werden zur Ver- und Entschlüsselung jeweils verschiedene Schlüssel verwendet.[73] Einer der beiden Schlüssel ist nur dem Nutzer bekannt (privater Schlüssel), der andere Schlüssel ist öffentlich bekannt und beispielsweise in einer Datenbank abgelegt (öffentlicher Schlüssel). Verschlüsselt der Anbieter den Inhalt mit dem allgemein verfügbaren, öffentlichen Schlüssel eines bestimmten Nutzers, so kann dieser Nutzer den Inhalt mit seinem privaten Schlüssel entschlüsseln. Um zu gewährleisten, daß nur dieser Nutzer den Inhalt entschlüsseln kann, müssen asymmetrische Verschlüsselungsverfahren gewährleisten, daß ein mit dem öffentlichen Schlüssel verschlüsselter Inhalt *ausschließlich* mit dem dazugehörenden privaten Schlüssel, nicht aber mit dem – allgemein bekannten – öffentlichen Schlüssel dechiffriert werden kann. Auch darf es nicht möglich sein, vom allgemein bekannten öffentlichen Schlüssel auf den privaten Schlüssel zu schließen. 1976 wurde von *Whitfield Diffie* und *Martin Hellman* erstmals ein Verfahren vorgestellt, das diese Anforderungen erfüllt.[74] Dabei wird der öffentliche Schlüssel

---

[70] *National Research Council*, S. 286 f. Zu den notwendigen Hard- und Softwareanforderungen s. unten Teil 1, C IV.

[71] *National Research Council*, S. 156.

[72] Die Sicherheit symmetrischer Verschlüsselungsverfahren hängt daher von der sicheren Übertragung des symmetrischen Schlüssels ab. Wenn aber eine sichere Übertragung des Schlüssels möglich sein muß, so scheint auf den ersten Blick das ganze Verschlüsselungssystem keinen Sinn zu machen: Über diesen sicheren Kommunikationskanal könnten auch gleich die digitalen Inhalte übertragen werden. Dabei ist jedoch zu beachten, daß digitale Inhalte regelmäßig ein ungleich größeres Datenvolumen aufweisen als ein symmetrischer Schlüssel. Daher ist es viel einfacher, Schlüsselinformationen sicher zu übertragen als digitale Inhalte. S. *National Research Council*, S. 156 f.

[73] Zur Funktionsweise asymmetrischer Verschlüsselungsverfahren s. *Selke*, S. 63 ff.

[74] *Diffie/Hellman*, 22 IEEE Transactions on Information Theory 644 ff. (1976). Inzwischen ist bekannt, daß Kryptologen der Communications-Electronics Security Group (CESG) der britischen Regierung das asymmetrische Verschlüsselungskonzept schon sechs Jahre früher als *Diffie/Hellman* entwickelt hatten, ihre Ergebnisse jedoch nicht veröffentlichten, s. *Doraswamy/Harkins*, S. 23.

durch die Multiplikation zweier zufällig gewählter Primzahlen bestimmt.[75] Der private Schlüssel wird durch ein spezielles mathematisches Verfahren aus dem öffentlichen Schlüssel ermittelt.[76] Man geht davon aus, daß für einen Angreifer der schnellste Weg, eine asymmetrisch verschlüsselte Nachricht zu entschlüsseln, wenn er den privaten Schlüssel nicht kennt, eine Faktorisierung[77] des öffentlichen Schlüssels notwendig macht. Da der Rechenaufwand zur Faktorisierung des öffentlichen Schlüssels mit zunehmender Schlüssellänge exponentiell ansteigt,[78] ist es bei hinreichend langen öffentlichen Schlüsseln mit den heutigen Rechenkapazitäten faktisch unmöglich, diese Berechnung durchzuführen.[79]

Auch asymmetrische Verschlüsselungsverfahren haben ihre Nachteile. Einerseits setzen sie bestimmte Infrastruktureinrichtungen voraus: Es muß ein öffentlich zugängliches Verzeichnis der verwendeten öffentlichen Schlüssel existieren (sogenannte „Public Key Infrastructure", PKI).[80] Obwohl die zugrundeliegenden mathematischen Verfahren asymmetrischer Verschlüsselungsverfahren seit über zwei Jahrzehnten bekannt sind, wurde erst in den letzten Jahren mit dem Aufbau solcher Infrastrukturen begonnen.[81] Andererseits sind asymmetrische Verschlüsselungsverfahren viel rechenintensiver – und damit langsamer – als symmetrische Verfahren, da Berechnungen mit sehr großen Zahlen durchgeführt werden müssen. In Unterhaltungselektronik-Geräten, die über begrenzte Rechenkapazitäten verfügen, scheiden asymmetrische Verschlüsselungsverfahren aus diesem Grund oft aus. Viele heutige DRM-Systeme bauen auf symmetrischen Verschlüsselungsverfahren auf.

Eine andere Möglichkeit, die hohe Rechenintensität asymmetrischer Verschlüsselungsverfahren zu lindern, besteht in der Koppelung asymmetrischer Verfahren mit symmetrischen Verfahren. Dabei verschlüsselt der Anbieter einen Inhalt mit einem symmetrischen Verschlüsselungsverfahren. Den symmetrischen Schlüssel verschlüsselt er seinerseits mit einem asymmetrischen Verschlüsselungsverfahren. Der asymmetrisch verschlüs-

---

[75] Die folgende Darstellung orientiert sich an dem von *Rivest*, *Shamir* und *Adleman* 1977/1978 entwickelten RSA-Algorithmus, s. dazu und zu anderen asymmetrischen Verschlüsselungsalgorithmen *Selke*, S. 66 ff., 71 ff; *Schneier*, S. 461 ff.; *Bauer*, S. 178 ff.; *Wayner*, Digital Copyright Protection, S. 22 f.

[76] Dabei wird eine Modulo-Berechnung durchgeführt, also der ganzzahlige Teilungsrest bei einer Division bestimmt.

[77] Bei der Faktorisierung einer natürlichen Zahl werden die Primzahlen ermittelt, deren Multiplikation die bestimmte Zahl ergibt.

[78] Eine Erhöhung der Schlüssellänge um den Faktor 1,1 erhöht den Rechenaufwand um den Faktor 7, *Selke*, S. 75.

[79] *Bauer*, S. 183. Es existiert jedoch kein zahlentheoretischer Beweis, daß nicht ein anderer Angriff das Verschlüsselungsverfahren sehr viel schneller brechen könnte, s. *Selke*, S. 68.

[80] Zur Notwendigkeit von Zertifizierungsstellen s. a. unten Teil 1, C III 2 b.

[81] *National Research Council*, S. 289.

selte symmetrische Schlüssel wird dann mit dem symmetrisch verschlüsselten Inhalt an den Empfänger übertragen, der den Inhalt entschlüsseln kann, indem er die beschriebenen Schritte in umgekehrter Reihenfolge anwendet.[82] Da bei diesem Vorgehen, das weit verbreitet ist, nur der – relativ kurze – symmetrische Schlüssel asymmetrisch verschlüsselt wird, hält sich die erforderliche Rechenkapazität in Grenzen. Selbst diese „hybriden" Verschlüsselungsverfahren sind für den praktischen Einsatz in DRM-Systemen oftmals noch zu rechenintensiv.

b) Sonderprobleme

aa) Digitale Container

Der Schutz digitaler Inhalte durch Verschlüsselung endet, sobald der Inhalt in einem Endgerät entschlüsselt wird. Dann ist es möglich, den digitalen Inhalt in unverschlüsselter Form zu kopieren und weiterzugeben – ein möglicher Ansatzpunkt für Raubkopierer. Daher werden Verschlüsselungsverfahren nicht nur eingesetzt, um die Übertragung digitaler Inhalte vom Anbieter zum Nutzer zu sichern. Vielmehr werden sie auch noch eingesetzt, wenn sich die digitalen Inhalte beim Nutzer befinden. Dabei werden digitale Inhalte mit einem sogenannten „digitalen Container" versehen. Ein digitaler Container ist eine verschlüsselte Form eines digitalen Inhalts. Die Inhalte werden verschlüsselt in dem digitalen Container zum Nutzer übertragen und bleiben auch in dem Endgerät grundsätzlich verschlüsselt. Nur wenn der Nutzer berechtigerweise die Inhalte nutzen will, werden die Inhalte von einer speziellen Soft- oder Hardwarekomponente entschlüsselt.[83] Will der Nutzer die Inhalte an Dritte weitergeben, so ist dies nur in verschlüsselter Form möglich. Das Konzept der „digitalen Container" versucht, die digitalen Inhalte in möglichst vielen Stadien eines DRM-Systems in verschlüsseltem Zustand zu halten. Es wird in vielen heute angebotenen Systemen verwendet und stellt allgemein einen der wichtigsten Grundpfeiler von DRM-Systemen dar.[84]

bb) Veränderungen in der Nutzerschaft

Schlüssel zum Dechiffrieren digitaler Inhalte sind oft dauerhaft in Endgeräten gespeichert. Dies ist zum Beispiel bei Set-Top-Boxen im Pay-TV-Bereich der Fall. Auch in rein Software-basierten DRM-Systemen sind Dechiffrier-Schlüssel oftmals in der Software gespeichert. Es muß damit gerechnet werden, daß es Angreifern gelingt, die technischen Schutzmaß-

[82] S. dazu *Selke*, S. 77 ff.

[83] Bei Musikdateien wird oft auch nicht die gesamte Datei auf einmal entschlüsselt, sondern zeitabhängig nur immer der Abschnitt, auf den gerade zugegriffen wird. S. zum ganzen *National Research Council*, S. 161 f.

[84] S. dazu allgemein *Schneck*, 87 Proc. IEEE 1239, 1242 (1999). „Digitale Container" werden beispielsweise im System vom InterTrust, <http://www.intertrust.com>, sowie im Cryptolope-Konzept von IBM, <http://www.software.ibm.com/security/cryptolope>, eingesetzt.

nahmen in einem einzelnen Endgerät zu knacken und den Dechiffrier-Schlüssel zu extrahieren. Damit können sie Inhalte in dem DRM-System unberechtigt nutzen und eventuell weitere illegale Endgeräte herstellen. Ein langfristig sicheres DRM-System muß Mechanismen bereitstellen, um kompromittierte und illegale Endgeräte individuell zu deaktivieren und von der weiteren Nutzung des DRM-Systems auszuschließen (sogenannte „device revocation").[85] Das Verschlüsselungssystem eines DRM-Systems muß also mit einer dynamischen Änderung der Nutzerschaft zurechtkommen.

Dafür gibt es unterschiedliche Lösungsmöglichkeiten. Eine Lösungsmöglichkeit ist, daß der Anbieter den Inhalt für jeden Nutzer mit dessen individuellem Schlüssel verschlüsselt und an jeden einzelnen Nutzer überträgt.[86] Soll ein bestimmter Nutzer beziehungsweise dessen Endgerät von dem DRM-System ausgeschlossen werden, so stellt der Anbieter seine Übertragungen an diesen Nutzer ein.[87] Dieser Ansatz hat jedoch den Nachteil, daß der Anbieter bei einer Vielzahl von Nutzern für jeden Nutzer den Inhalt getrennt verschlüsseln muß. Die Verwaltung unzähliger Schlüssel, deren Anzahl in die Millionen gehen kann, ist komplex; auch kann dieses Vorgehen zu einer hohen Belastung der Rechner der Inhalteanbieter führen.[88]

Weiterhin gibt es zunehmend Übertragungen, bei denen Inhalte vom Anbieter zum Nutzer nicht jeweils individuell übertragen werden, sondern aus Kapazitätsgründen eine einheitliche Übertragung für eine Vielzahl von Nutzern stattfindet, wobei der Datenstrom erst möglichst nah am Empfänger vervielfältigt wird. Dabei ist eine individuelle Verschlüsselung der Inhalte für jeden Nutzer unmöglich, da die Inhalte nicht individuell an die Nutzer übertragen werden (siehe Abbildung 1, Teil b, S. 28). Diese sogenannten Punkt-zu-Multipunkt-Übertragungen („multicast", „broadcast") sind aus dem Fernseh- und Rundfunkbereich bekannt, werden aber auch für das Internet entwickelt.[89] Für breitbandige

[85] *Marks/Turnbull*, EIPR 2000, 198, 204. Zur Integration dieser Verfahren in DRM-Systeme durch Technologie-Lizenzverträge s. unten Teil 2, C II 2 e.

[86] Dieser Ansatz wurde beispielsweise im „Multimedia Protection Protocol" (MMP) verfolgt, das ab 1995 am Fraunhofer Institut für Integrierte Schaltungen entwickelt wurde und noch heute im Music-on-Demand-Projekt der Deutschen Telekom, <http://www.audio-on-demand.de/mod>, eingesetzt wird. S. dazu *Rump*.

[87] Ein vergleichbares Verfahren wird bei Bankkarten u. ä. eingesetzt, s. *Rankl/Effing*, S. 516.

[88] Dabei ist jedoch zu beachten, daß regelmäßig die digitalen Inhalte mit einem einheitlichen symmetrischen Schlüssel chiffriert werden. Erst dieser symmetrische Schlüssel wird dann seinerseits mit individuellen Nutzerschlüsseln chiffriert und an die Nutzer übertragen. Dadurch kann der Rechenaufwand in Grenzen gehalten werden. Weiterhin ist diese „point-to-point encryption" regelmäßig unter Sicherheitsaspekten zu bevorzugen, s. *Sander*, S. 8 f.

[89] „IP Multicast" ist ein Verfahren, in dem über das IP-Protokoll Punkt-zu-Multipunkt-Übertragungen ermöglicht werden, s. dazu *Federrath*, ZUM 2000, 804, 807;

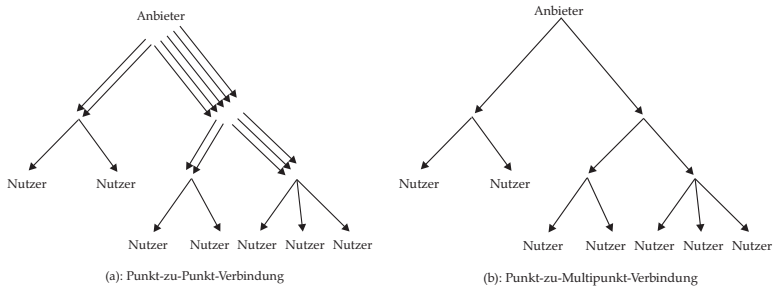


Abbildung 1: Übertragungsmethoden

Medienanwendungen, wie sie in DRM-Systemen oftmals angeboten werden (Video, Audio), werden Punkt-zu-Multipunkt-Verbindungen in Zukunft sehr wichtig sein.

Bei Punkt-zu-Multipunkt-Verbindungen und anderen Umgebungen, in denen eine individuelle Verschlüsselung digitaler Inhalte nicht möglich ist,[90] ist die Verschlüsselung digitaler Inhalte ein komplexes Unterfangen.[91] Dazu existieren Verfahren, bei denen die Verschlüsselung beim Anbieter mit einem einzigen Schlüssel, die Entschlüsselung bei den Nutzern jedoch mit einer Vielzahl unterschiedlicher Schlüssel möglich ist (sog. „point-to-multipoint encryption" oder „multiple-key encryption").[92]

Sahasrabuddhe/Mukherjee, 14 (1) IEEE Network 90 ff. (Januar/Februar 2000); *Loshin*, S. 33 ff. Im derzeitigen IP-Multicast-Modell existieren zwar weder Mechanismen, um die Anzahl der Nutzer des Systems zu ermitteln, noch bestehen Mechanismen, unberechtigte Sender oder Empfänger von der Nutzung des Systems auszuschließen. Jedoch existieren Erweiterungen, bei denen ein sicheres Schlüsselmanagement auch bei IP Multicast möglich ist, so im Rahmen des „Core Based Tree Multicast Protocol", s. *Ballardie*, RFC 1949; *Chu/Qiao/Nahrstedt* in: Wong/Delp (Hrsg.), S. 460, 461. Zu anderen Erweiterungen s. *Sahasrabuddhe/Mukherjee*, 14 (1) IEEE Network 90, 101 (Januar/Februar 2000); *Diot/Levine/Lyles/Kassem/Balensiefen*, 14 (1) IEEE Network 78, 84 (Januar/Februar 2000). Neben IP Multicast existieren auch andere Ansätze, um die Ineffizienz der herkömmlichen Punkt-zu-Punkt-Übertragungen im Internet zu beseitigen (z. B. Proxies oder das verteilte System von Akamai, <http://www.akamai.com>).

[90] Wenn ein Nutzer eine DRM-geschützte Musikdatei aus dem Internet bezieht, so liegt technisch betrachtet regelmäßig eine Punkt-zu-Punkt-Übertragung vor; obwohl hier eine individuelle Verschlüsselung möglich wäre, wird dies aus Performance-Gründen oft vermieden. Auch werden geschützte CDs regelmäßig mit einem einzigen Chiffrier-Schlüssel verschlüsselt; ansonsten müßte jedes einzelne Exemplar einer CD mit unterschiedlichem Inhalt gepreßt werden.

[91] Zu den Problemen im Überblick s. *Canetti/Pinkas*. S. a. *Doraswamy/Harkins*, S. 205 ff.

[92] S. dazu im Überblick *Wohlmacher* in: Dittmann/Nahrstedt/Wohlmacher (Hrsg.), S. 19 ff.; *Schneier*, S. 68 f., 527 f. Diese Verschlüsselungsverfahren müssen aber nicht notwendigerweise nur bei Punkt-zu-Multipunkt-Übertragungen eingesetzt werden. „Point-to-multipoint encryption"-Verfahren führen regelmäßig dazu, daß die verwendeten Schlüssel länger werden. Aus praktischen Gründen sind der Länge der eingesetzten Schlüssels und damit der „Point-to-multipoint encryption" Grenzen gesetzt.

Auch in einem solchen Umfeld müssen Verfahren existieren, um unberechtigte Nutzer von DRM-Systemen auszuschließen („device revocation"). Bei der sogenannten „broadcast encryption" werden die Nutzer in verschiedene Gruppen eingeteilt, die jeweils mit einem Schlüssel ausgestattet sind. Jeder Nutzer gehört mehreren Gruppen an und verfügt daher über mehrere Schlüssel. Der Anbieter kann einen bestimmten Nutzer von der Nutzung des digitalen Inhalts ausschließen, indem er den Inhalt nur mit den Schlüsseln solcher Gruppen verschlüsselt, denen der besagte Nutzer nicht angehört.[93] Dadurch wird dieser Nutzer vom DRM-System ausgeschlossen, ohne daß an seinem Endgerät etwas geändert werden muß.[94]

Bei einem anderen, mitunter „secure multicast" genannten Verfahren wird für die Kommunikation zwischen dem Inhalteanbieter und den Nutzern ein gemeinsamer Schlüssel verwendet.[95] Sollen Nutzer hinzugefügt oder entfernt werden, so übermittelt der Anbieter den berechtigten Nutzern einen neuen Schlüssel, mit dem der zukünftige Datenverkehr verschlüsselt wird.[96] Damit kein Dritter Kenntnis von dem neuen Schlüssel

[93] Im vorliegenden Zusammenhang ist unerheblich, ob dabei symmetrische oder asymmetrische Verschlüsselungsverfahren verwendet werden.

[94] *Canetti/Malkin/Nissim* in: Stern (Hrsg.), S. 456, 460. Tatsächlich sind „broadcast encryption"-Systeme komplexer. Dabei soll einerseits aus Effizienzgründen die Anzahl der im System verwendeten Schlüssel möglichst gering sein, andererseits soll die Anzahl der Nutzer, die sich zusammenschließen müssen, um einen allgemeinen Schlüssel („common key") zu berechnen, mit dem alle Inhalte entschlüsselt werden können, möglichst hoch sein (sog. „Kollusionsresistenz"). Die Schwierigkeit der „broadcast encryption" liegt in der intelligenten Festlegung der Gruppen. Zum Ganzen grundlegend *Fiat/Naor* in: Stinson (Hrsg.), S. 480 ff.; s. weiterhin *Gafni/Staddon/Yin* in: Wiener (Hrsg.) S. 372 ff.; *Abdalla/Shavitt/Wool* in: Franklin (Hrsg.), S. 140 ff.; *Canetti/Pinkas*, S. 14; *Federrath*, ZUM 2000, 804, 809. „Broadcast Encryption" wird unter anderem bei „Content Protection for Recordable Media" (CPRM) eingesetzt, s. dazu unten Fn. 573.

[95] Dafür können sowohl symmetrische als auch asymmetrische Verschlüsselungsverfahren verwendet werden. Diese Verfahren können nicht nur bei DRM-Systemen, sondern auch bei Telekonferenzen und anderen Netzwerk-basierten Anwendungen sowie in militärischen und nachrichtendienstlichen Bereichen Anwendung finden, s. *Wallner/Harder/Agee*, RFC 2627, S. 3.

[96] *Wallner/Harder/Agee*, RFC 2627, S. 2; *Canetti/Malkin/Nissim* in: Stern (Hrsg.), S. 456, 457. Im vorliegenden Zusammenhang können nur die Grundzüge der Verfahren angedeutet werden. Es gibt unzählige Varianten, bei denen beispielsweise keine zentrale Schlüsselvergabestelle existiert oder bei denen neue Schlüssel beim Nutzer lokal unter Verwendung eines Pseudo-Zufallszahlengenerators errechnet werden. Auch die Bezeichnungen für diese Verfahren differieren, teilweise wird von „group key management" gesprochen. Einen Überblick über den derzeitigen Forschungsstand geben *Wallner/Harder/Agee*, RFC 2627; *Canetti/Pinkas*, S. 8 ff., 13 ff.; *Balenson/McGrew/Sherman*, S. 3 ff.; *Chu/Qiao/Nahrstedt* in: Wong/Delp (Hrsg.), S. 460, 461 ff.; *Wong/Gouda/Lam*, 8 IEEE/ACM Transactions on Networking 16 ff. (2000); *Doraswamy/Harkins*, S. 206 ff.; *Mittra* in: ACM SIGCOMM 1997, S. 277, 287; s. ferner die „Secure Multicast Research Group" (SMuG) im Rahmen der „Internet Research Task Force" (IRTF), <http://www.ipmulticast.com/community/smug>.

erlangen kann, wird der Schlüssel entweder auf einem sicheren Übertragungsweg oder aber selbst wiederum verschlüsselt übertragen.[97] Im Gegensatz zur „broadcast encryption" muß bei diesem Verfahren bei Änderungen in der Nutzerschaft also ein neuer Schlüssel übertragen werden (sogenannntes „re-keying").[98]

Ein dritter Ansatz setzt nicht am einzelnen kompromittierten Endgerät, sondern an der *Kommunikation* zwischen den berechtigten Endgeräten und dem kompromittierten Endgerät an. Bei diesem Ansatz,[99] der beispielsweise im „Digital Transmission Content Protection"-System (DTCP)[100] realisiert ist, ist jedes Endgerät – zum Beispiel digitaler Videorekorder, digitaler Fernseher, Set-Top-Box, DVD-Spieler, MP3-Spieler, Computer – mit einer eindeutigen Identifizierungsnummer versehen. Gleichzeitig enthält jedes berechtigte Endgerät eine Liste aller kompromittierten Endgeräte. Wenn beispielsweise ein bestimmter DVD-Spieler kompromittiert wurde, so wird die Identifizierungsnummer dieses DVD-Spielers allen berechtigten Geräten mitgeteilt. Will der Angreifer ein DVD-Video auf dem kompromittierten DVD-Spieler anschauen, so wird der DVD-Spieler versuchen, die Videodaten an einen Computer- oder Fernsehbildschirm zu übertragen. Diese DRM-kompatiblen Geräte erkennen jedoch aus ihrer internen Liste, daß der DVD-Spieler kompromittiert wurde und verweigern dann die Zusammenarbeit.[101]

Bei allen Ansätzen, die den dynamischen Ausschluß unberechtigter Nutzer aus dem DRM-System ermöglichen, muß definiert werden, wann ein solcher Ausschluß initiiert werden soll. Aus der Sicht des Systembetreibers ist die Sicherheit des DRM-Systems nicht nur bei einem vollstän-

---

[97] Ein Beispiel eines solchen Verfahrens geben *Wallner/Harder/Agee*, RFC 2627, S. 10; *Harney/Muckenhirn*, RFC 2094.

[98] Je nach Verfahrensvariante kann die Übertragung neuer Schlüssel aber auf eine sehr geringe Anzahl von Nutzern beschränkt werden, so beispielsweise im „Hierarchical Tree Approach" von *Wallner/Harder/Agee*, RFC 2627, S. 14 f.; s. dazu *Doraswamy/Harkins*, S. 208 f.

[99] S. zum Folgenden *Hitachi/Intel/Matsushita/Sony/Toshiba*, 5C Digital Transmission Content Protection White Paper, S. 11 f.; *dies.*, Digital Transmission Content Protection Specification, S. 55 ff. *Datta*, S. 5 f.

[100] S. dazu unten Teil 1, D III 2 a.

[101] Dabei müssen die Listen der kompromittierten Endgeräte nicht vom Anbieter des DRM-Systems einzeln an jedes berechtigte Gerät geschickt werden; dies wäre bei offline-Systemen wie DVD oder CD auch schwer möglich. Vielmehr werden die Listen in die normale Übertragung digitaler Inhalte (Fernsehausstrahlung, Vertrieb von DVDs oder CDs, Internet-Download) sowie in neu hergestellte Endgeräte integriert. Nach und nach verbreiten sich die aktualisierten Listen von Gerät zu Gerät, bis nach einer gewissen Zeit alle berechtigten Endgeräte mit neuen Listen der kompromittierten Geräte ausgestattet sind. Dieses Verfahren baut daher stark auf der Kommunikation zwischen den verschiedenen Endgeräten auf. Weiterhin ist ein vollständiges und sicheres Authentisierungssystem notwendig, *Hitachi/Intel/Matsushita/Sony/Toshiba*, 5C Digital Transmission Content Protection White Paper, S. 12.

dig nachgewiesenen und erfolgreichen Angriff beeinträchtigt. Schon der bloße Verdacht einer Beeinträchtigung der Systemsicherheit kann ausreichen, um einzelne Nutzer und ihre Endgeräte vom DRM-System auszuschließen. Daher benötigen DRM-Systeme Risiko-Management-Infrastrukturen, durch die etwaige Angriffsversuche und Sicherheitsprobleme entsprechend bewertet und behoben werden können.[102]

Insgesamt besteht bei den dargestellten Ansätzen hinsichtlich der genauen Architektur des Schlüssel-Managements sowie hinsichtlich Effizienz-, Skalierungs- und Sicherheitsgesichtspunkten noch Forschunsgbedarf.[103] Diese Fragen sind bei großen Systemen mit Hunderttausenden oder mehr Nutzern äußerst komplex.

cc) Teilweise Verschlüsselung

Die Verschlüsselung digitaler Inhalte ist rechenintensiv und zeitaufwendig, wenn große Datenmengen anfallen. Dies ist insbesondere bei Audio- und Videodaten der Fall. Für diese Bereiche werden daher Verfahren entwickelt, bei denen nicht der gesamte Datenstrom, sondern nur Teile des Datenstroms verschlüsselt werden.[104] Dies hat zur Folge, daß ein unberechtigter Nutzer die digitalen Inhalte zwar nicht entschlüsseln kann, aber dennoch einen groben Eindruck der Inhalte erhält: Auch ein nichtautorisierter Decoder kann die digitalen Inhalte ausgeben, wenn auch mit einer deutlich verminderten Qualität.[105] Die Stärke der Verschlüsselung und damit die Qualitätsbeeinträchtigung kann dabei nahezu beliebig eingestellt werden.[106]

Ein anderes Verfahren baut nicht auf Charakteristika des Verschlüsselungs-, sondern auf Merkmalen des Kompressionsverfahrens auf. Videodaten benötigen regelmäßig zur Übertragung eine große Datenübertra-

---

[102] *Sander*, S. 7.

[103] S. zu diesen Fragen *Wallner/Harder/Agee*, RFC 2627; *Harney/Muckenhirn*, RFC 2094; *Diot/Levine/Lyles/Kassem/Balensiefen*, 14 (1) IEEE Network 78, 83 f. (Januar/Februar 2000); *Wong/Gouda/Lam*, 8 IEEE/ACM Transactions on Networking 16 ff. (2000); *Canetti/Pinkas*; *Mittra* in: ACM SIGCOMM 1997, S. 277 ff.; *Canetti/Malkin/Nissim* in: Stern (Hrsg.), S. 456 ff. Der Schwerpunkt der bisherigen Forschung lag auf der Etablierung einer Schlüssel-Management-Architektur und der anfänglichen Schlüsselverteilung. Fragen der späteren Änderung in der Nutzerschaft werden erst in letzter Zeit verstärkt untersucht.

[104] Zum Audiobereich s. *Allamanche/Herre/Buckenhof/Rump*, Patent DE 19907964 C1 vom 10. 8. 2000; *Fujii/Abe/Nishihara/Kushima*, 11 (1) NTT Review 116 (Januar 1999); *Roche/Dugelay/Molva* in: ICIP 1996, Band 3, S. 235.

[105] Auf die technischen Einzelheiten kann hier nicht eingegangen werden. Im Audio-Bereich werden solche Verfahren auch „audio scrambling algorithms" genannt. Ein solches Verfahren wurde für den Audio-Bereich am Fraunhofer-Institut für Integrierte Schaltungen entwickelt, s. *Allamanche/Herre/Buckenhof/Rump*, Patent DE 19907964 C1 vom 10. 8. 2000; s. dazu auch <http://www.iis.fhg.de/amm/techinf/ipmp/scrambling.html>.

[106] S. *Allamanche/Herre/Buckenhof/Rump*, Patent DE 19907964 C1 vom 10. 8. 2000, Spalten 4, 9.

gungskapazität, auch wenn sie davor komprimiert wurden. Da die Nutzer mit unterschiedlichen Geschwindigkeiten an Übertragungsnetze wie das Internet angebunden sind, hätte die einheitliche Übertragung digitaler Videodaten große Nachteile: Manche Nutzer könnten die Videodaten nicht empfangen, da sie nicht über die entsprechende Übertragungskapazität verfügen. Andere Nutzer könnten die Videodaten zwar empfangen, jedoch in einer schlechteren Qualität, als es ihre gute Übertragungskapazität eigentlich erlauben würde. Daher unterstützen viele der heutigen digitalen Video-Kompressionsverfahren die Kompression der Videodaten in mehreren „Schichten" („video layering").[107] Dabei werden die Videodaten zunächst in einer relativ schlechten Qualität komprimiert. Diese Schicht, die relativ wenig Übertragungskapazität benötigt, kann von nahezu jedem Nutzer verwendet werden. Zusätzlich existieren mehrere Kompressionsschichten, die die Videodaten in einer jeweils etwas besseren Qualität zur Verfügung stellen.[108] Dieses Verfahren ermöglicht eine elegante und effiziente Anpassung der Übertragungsqualität an die jeweilige Bandbreite, die einem Nutzer zur Videoübertragung zur Verfügung steht.[109] Aber auch für DRM-Zwecke sind diese Verfahren interessant, da die unterschiedlichen Komprimierungsschichten unterschiedlich verschlüsselt werden können.[110]

Beide dargestellten Verfahren, die die teilweise Verschlüsselung digitaler Inhalte erlauben und mitunter als „multiresolution encryption" bezeichnet werden, ermöglichen es, digitale Inhalte in unterschiedlichen Qualitätsstufen anzubieten und damit Nutzer mit unterschiedlicher individueller Zahlungsbereitschaft zu befriedigen.[111] Auch können die Verfahren für Werbezwecke genutzt werden. So können Videofilme, die mit diesen Verfahren verschlüsselt wurden, kostenlos verteilt werden. Der Nutzer kann den teilweise verschlüsselten Film in schlechter Qualität an-

---

[107] Allgemein werden solche Verfahren „multiresolution coding techniques" genannt.

[108] Dabei enthalten die einzelnen Schichten nicht die gesamten Videodaten; vielmehr werden in jeder Schicht nur die Unterschiede zur darunterliegenden Schicht kodiert. Bei der Dekomprimierung muß ein Nutzer daher die Daten mehrerer Kompressionsschichten gleichsam addieren, um seine gewünschte Qualitätsstufe zu erreichen.

[109] S. dazu allgemein *Li/Ammar/Paul*, IEEE Network März/April 1999, 46, 48, 52 m. w. N. Zur Anwendung dieses Verfahrens im MPEG-2-Video-Standard s. *Sayood*, S. 552 f. Diese Ansätze finden sich auch im europäischen DVB-Standard für terrestrische digitale Fernsehübertragungen wieder, s. *European Telecommunications Standard Institute*, ETSI EN 300 744.

[110] In Multicast-Umgebungen (s. dazu oben bei Fn. 89) können die einzelnen Qualitätsstufen beispielsweise verschiedenen Multicast-Gruppen mit unterschiedlichen Zugangsberechtigungen zugewiesen werden.

[111] *Fujii/Abe/Nishihara/Kushima*, 11 (1) NTT Review 116, 122 (Januar 1999). Dies wird teilweise „hierarchical access control" genannt, s. *Roche/Dugelay/Molva* in: ICIP 1996, Band 3, S. 235. Zu den ökonomischen Auswirkungen solcher Verfahren unter dem Gesichtspunkt der Preisdiskriminierung s. unten Teil 3, A III 3 b bb.

schauen, um zu prüfen, ob ihm der Film zusagt. Ist dies der Fall, so kann er einen Dechiffrier-Schlüssel erwerben und damit den Film in HiFi-Qualität entschlüsseln.[112]

dd) Portabilität und Beständigkeit von Nutzungsrechten

Ein DRM-System, das am Markt erfolgreich sein will, muß auf die Präferenzen der Nutzer Rücksicht nehmen.[113] Oftmals wollen Nutzer digitale Inhalte, die sie in einem DRM-System erworben haben, nicht nur auf einem einzelnen Endgerät, sondern an unterschiedlichen Orten auf unterschiedlichen Endgeräten nutzen können (im Wohnzimmer auf der Stereoanlage, im Büro auf dem Computer, unterwegs auf dem tragbaren Endgerät oder dem Laptop, im Autoradio oder über die Stereoanlage im Hotelzimmer; *Portabilität von Nutzungsrechten*). Auch muß ein DRM-System sicherstellen, daß ein Nutzer seine Zugangs- und Nutzungsrechte nicht verliert, wenn eines seiner Endgeräte Fehlfunktionen hat oder ausgetauscht werden muß (*Beständigkeit von Nutzungsrechten*). Idealerweise sollte ein DRM-System daher über eine Systemarchitektur verfügen, durch die die Portabilität und Beständigkeit von Nutzungsrechten gewährleistet ist. Das Ziel ist, die Nutzungsrechte nicht an bestimmte Endgeräte des Nutzers, sondern an die Person des Nutzers selbst zu binden („anytime, anywhere access to all ‚my' content").[114] Zu diesem Zweck können zentrale Datenbanken eingesetzt werden, in denen die Zugangs- und Nutzungsrechte des einzelnen Nutzers gespeichert sind und von dort auf die jeweiligen Endgeräte übertragen werden („rights locker architecture").

c) Zusammenfassung

Verschlüsselungsverfahren bieten vielfältige Möglichkeiten, um den Zugang zu digitalen Inhalten und deren Nutzung zu kontrollieren. Die Verfahren sind in vielen Bereichen technisch ausgereift, ihre Sicherheit ist beweisbar und ihr Sicherheitsniveau technisch kontrollierbar. Verschlüsselungsverfahren bilden damit einen Grundpfeiler für technische Schutzmaßnahmen in DRM-Systemen. In wichtigen Bereichen, insbesondere im Schlüssel-Management und der „device revocation", besteht jedoch noch Forschungs- und Implementierungsbedarf.

2. Kopierkontrollsysteme

Neben Verschlüsselungsverfahren bestehen in DRM-Systemen noch andere Ansätze der Zugangs- und Nutzungskontrolle. Viele DRM-Systeme wollen verhindern, daß ein Nutzer unbegrenzt Kopien der Inhalte anfer-

---

[112] *Allamanche/Herre/Buckenhof/Rump*, Patent DE 19907964 C1 vom 10. 8. 2000, Spalte 3 f.; *Fujii/Abe/Nishihara/Kushima*, 11 (1) NTT Review 116, 121 f. (Januar 1999).

[113] Zum folgenden s. *Sander*, S. 3.

[114] *Sander*, S. 3.

tigen kann. Daher existieren mehrere Verfahren, die das Erstellen mehrerer Kopien verhindern sollen. Zu diesem Zweck werden die digitalen Inhalte mit einer Zusatzinformation versehen, ob und wie oft sie kopiert werden dürfen.[115] Versucht ein Nutzer, mit einem DRM-kompatiblen Gerät die derart markierten Inhalte zu kopieren, so liest das Gerät zunächst diese Kopierkontrollinformationen aus und fertigt eine Kopie nur an, wenn dies nach den Kopierkontrollinformationen erlaubt ist. Solche Verfahren werden unter anderem beim „Digital Audio Tape" (DAT) sowie beim DVD-Standard eingesetzt.[116]

3. Paßwörter

Auch Paßwörter können zur Zugangs- und Nutzungskontrolle eingesetzt werden. Der Schutz von Informationen durch Paßwörter ist heutzutage allgegenwärtig. Paßwörter müssen entweder einmal oder bei jeder Nutzung der Information eingegeben werden. Von Bank-, eurocheque- und Kreditkarten sind oft vierstellige Geheimzahlen (sog. „personal identification numbers", PINs) bekannt.[117] Es handelt sich um einfache, aber auch relativ unsichere Möglichkeiten des technischen Schutzes.[118]

II. Identifizierung durch Metadaten

1. Allgemeines

Metadata is the lifeblood of e-commerce.[119]

DRM-Systeme wollen den Vertrieb digitaler Inhalte vollständig automatisieren. Zu diesem Zweck muß das DRM-System Informationen über die zu vertreibenden Inhalte haben: sogenannte „Metadaten". Die dauerhafte Identifizierung und Beschreibung digitaler Inhalte ist eine der Grundvoraussetzungen für die Verwaltung von Urheber- und Leistungsschutzrechten in DRM-Systemen. Bei Metadaten für DRM-Systeme handelt es sich um

1. Informationen über den *Inhalt* selbst: Informationen über den Titel, die Art des Inhalts, das Dateiformat und ähnliches (dazu unten 2 a aa);

---

[115] Solche Informationen werden auch als „Metadaten" bezeichnet, s. dazu unten Teil 1, C II.

[116] Zum bei DAT-Kassetten eingesetzten „Serial Copy Management System" s. unten Teil 1, D II 1, zum bei DVDs eingesetzten „Copy Generation Management System" (CGMS) s. unten Teil 1, D II 3 c. Die Informationen können entweder in speziell dafür vorgesehenen Datenbereichen (so bei DAT) oder mit Hilfe digitaler Wasserzeichen direkt in die Inhalte eingebettet werden (so bei Audio-DVDs).

[117] S. dazu *Rankl/Effing*, S. 452 ff.

[118] Zu dem Verhältnis zwischen Nutzerfreundlichkeit und Unsicherheit von Paßwörtern s. *Zviran/Haga*, 15 (4) Journal of Management Information Systems 161 ff. (1999). Zur Unsicherheit von PINs s. *Rankl/Effing*, S. 452 ff. Bei für ec-Karten verwendeten Algorithmus genügten bei 10,5% der Karten lange Zeit nur 72 Versuche, um die 4-stellige PIN zu erraten, s. *Rankl/Effing*, S. 454 m. w. N.

[119] *John Erickson*, zitiert nach *Rust/Bide*, S. 4.

2. Informationen über die *Rechteinhaber*: Dies können Urheber und Leistungsschutzberechtigte, aber auch Verwertungsgesellschaften und sonstige Verwerter sein (dazu unten 2 a aa);
3. Informationen über die *Nutzungsbedingungen*: Solchen Informationen kann entnommen werden, zu welchen Bedingungen ein Inhalt betrachtet, angehört, kopiert oder weitergegeben darf. Die Nutzungsbedingungen werden durch einen technischen Mechanismus mit dem Inhalt verbunden, um dessen Nutzung es geht (dazu unten 2 a bb);
4. Informationen über den *Nutzer*: In einem digitalen Inhalt können Informationen über den berechtigten Nutzer des Inhalts abgespeichert werden. Damit kann der Urheber beispielsweise zurückverfolgen, welcher Nutzer unberechtigte Raubkopien erstellt hat (dazu unten 3).

Metadaten sind Daten über Daten, also Information über Information.[120] Ziel von Metadaten ist es, Informationen in einer formalen und differenzierten Weise zu beschreiben, so daß sie automatisiert verarbeitet werden können.[121] Metadaten sind für viele Bereiche des E-Commerce und des Internet von elementarer Bedeutung.[122] Die Beschreibung der Eigenschaften von Werken in Katalogen und Datenbanken war schon immer ein zentrales Interesse von Bibliotheken. Daher ist nicht verwunderlich, daß gerade Bibliotheken und deren Verbände eine treibende Kraft bei der Entwicklung von Metadaten-Standards im digitalen Umfeld sind.[123]

---

[120] *Saarela*, S. 14. Der Begriff „Metadaten" kam in den 60er Jahren auf, und wird seit den 80er Jahren vermehrt verwendet, s. *Vellucci*, 33 Annual Review of Information Science and Technology 187, 190 f. (1998). In den letzten 20 Jahren ist die Anzahl wissenschaftlicher Veröffentlichungen zu Metadaten um den Faktor 37 gestiegen, s. *Ercegovac*, 50 Journal of the American Society for Information Science 1165 (1999). Die Definitionen des Begriffs sind mitunter reichlich abstrakt: „An item of metadata is a relationship that someone claims to exist between two entities", *Rust/Bide*, S. 11.

[121] *Saarela*, S. 15. Inzwischen existieren auch spezielle Software-Programme, die die Eingabe von Metadaten erleichtern, beispielsweise der „Reggie Metadata Editor", s. <http://metadata.net/dstc>.

[122] Außerhalb von DRM-Systemen sind Metadaten beispielsweise auch für Filtersysteme zum Jugendschutz, Suchmaschinen im Internet sowie alle sonstigen Bereiche wichtig, in denen es auf die Klassifizierung von Information und deren automatische Erkennung ankommt. So gibt es auch Metadaten, die Informationen über den *Inhalt* digitaler Daten enthalten, beispielsweise die Angabe, daß in einer Filmsequenz ein bestimmtes Motorrad von der linken auf die rechte Bildhälfte fährt. Solche Metadaten sind für audiovisuelle Datenbanken und Suchsysteme wichtig und werden beispielsweise im Rahmen des MPEG-7-Standards normiert. Zu MPEG-7 s. unten Teil 1, D IV, und *Nack/Lindsay*, IEEE Multimedia 65 ff. (Juli/September 1999). Andere Anwendungsbereiche für Metadaten finden sich bei *PricewaterhouseCoopers*, Metadata Watch Report #1.

[123] Zu Metadaten-Systemen im Bibliotheksbereich s. das von der Deutschen Forschungsgemeinschaft geförderte Metadaten-Projekt deutscher Bibliotheken, METALIB, <http://www.dbi-berlin.de/projekte/einzproj/meta/meta00.htm> sowie <http://lcweb.loc.gov/marc> und zur Übersicht <http://www2.sub.uni-goettingen.de/metaform/crosswalks.html>, <http://www2.sub.uni-goettingen.de/metaguide/index.html>; *Baca* (Hrsg.).

2. Identifizierung des Inhalts, der Rechteinhaber und der Nutzungsbedingungen

Durch Metadaten können Merkmale des digitalen Inhalts beschrieben sowie Rechteinhaber und Nutzungsbedingungen festgelegt werden. Um eine Interoperabilität unterschiedlicher Systeme zu gewährleisten, werden für alle drei Bereiche Metadaten-Standards entwickelt (dazu unten a). Die Metadaten eines digitalen Inhalts können dann mit dem digitalen Inhalt auf unterschiedliche Weise – zum Beispiel durch „digitale Wasserzeichen" – verbunden werden (dazu unten b).

a) Identifizierungsobjekte

aa) Identifizierung des Inhalts und der Rechteinhaber

(1) **Allgemeines.** In einem DRM-System müssen digitale Inhalte und deren Rechteinhaber weltweit eindeutig identifiziert werden können. Systeme zur Identifizierung von urheberrechtlich geschützten Werken und deren Rechteinhabern existieren schon seit langer Zeit. So verfügen Verwertungsgesellschaften über umfassende Verzeichnisse von Werken und deren Rechteinhabern (teils digital, teils in Papierform). Diese Verzeichnisse sind jedoch nicht nach einem einheitlichen Standard angelegt.[124] Die Bibliothekswissenschaft verfügt über umfangreiche Erfahrung in der Behandlung von Metadaten für Bücher.[125] Die Informatik kann auf lange Erfahrung mit Organisation und Management von Daten, etwa in Datenbanksystemen, zurückgreifen. Auch werden seit Beginn der 70er Jahre viele Konsumgüter – von Joghurtbechern über Getränkedosen bis zu Büchern und CDs – mit sogenannten „Barcodes" versehen, die eine automatische Identifizierung des Konsumguts ermöglichen.[126]

Regelmäßig sind diese Metadaten-Systeme hinsichtlich ihres Funktionsumfangs recht beschränkt. So geht es bei Metadaten für Bibliothekskataloge hauptsächlich um die Standardisierung der Beschreibung des Titels eines Buches sowie dessen Urheber, Verlag, Erscheinungsdatum und ähn-

---

[124] Zu Standardisierungsinitiativen der Verwertungsgesellschaften s. unten Teil 1, D V. Als Beispiel für ein solches Verzeichnis sei die „International Documentation of Audiovisual Works" der CISAC genannt, s. *Briem*, MR 1997, 260, 261.

[125] Zu Metadaten-Projekten im Bibliotheksumfeld s. umfassend *Vellucci*, 33 Annual Review of Information Science and Technology 187 ff. (1998); *Dempsey/Heery*, 54 Journal of Documentation 145 ff. (1998); *Ahronheim*, 24 Journal of Academic Librarianship 395, 397 ff. (1998). Zum EU-finanzierten Projekt BIBLINK s. *Day/Heery/Powell*, 55 Journal of Documentation 16 ff. (1999); *Gervais* in: Koskinen-Olsson/Gervais (Hrsg.), S. 6, 26. In den USA ist das MARC-Format („MAchine-Readable Cataloging") zu nennen, das u. a. von der Library of Congress entwickelt wurde, s. dazu *Gervais*, a. a. O., S. 6, 25; *Ercegovac*, 50 Journal of the American Society for Information Science 1165, 1166 (1999).

[126] Informationen zum System der „European Article Number" (EAN) und des „Universal Product Code" (UPC) finden sich unter <http://www.ean-ucc.org> und <http://www.uc-council.org>.

liches. Für ein vollständiges DRM-System sind aber umfangreichere Metadaten über digitale Inhalte erforderlich. Bei elektronischen Büchern („eBooks") kann dies unter anderem der Titel, Untertitel, Zugehörigkeit zu einer Reihe, Seitenanzahl, Auflage, Verleger, Publikationsdatum, Sprache, Schlagworte, Preis, Auszeichnungen, Hinweise auf WWW-Seiten, Zielmarkt und das verwendete Dateiformat umfassen. Auch müssen DRM-Systeme die einzelnen Rechteinhaber identifizieren können. Dies können Komponisten, Textdichter und Arrangeure, Verleger, ausführende Künstler, Tonträgerhersteller, Photographen, bildende Künstler, Schriftsteller, Journalisten, Übersetzer, Drehbuchautoren, Regisseure, Produzenten, Bühnenbildner, Schauspieler, Rundfunk- und Fernsehanstalten, Software-Programmierer, Unternehmen und viele andere sein.

Da an solchen Metadaten neben den Betreibern von DRM-Systemen auch Verlage, Bibliotheken, Archive, Verwertungsgesellschaften sowie die Tonträger- und Filmindustrie Interesse haben, wird seit einigen Jahren an einer übergreifenden Standardisierung von Metadaten gearbeitet.[127] Ein Ziel derzeitiger Initativen ist es, die bestehenden Identifizierungssysteme untereinander kompatibel zu machen oder in ein umfassendes System zu integrieren.[128] Auch wenn die Ausgangsinteressen beispielsweise von Bibliotheksverbänden einerseits und E-Commerce-Unternehmen andererseits sehr unterschiedlich sind,[129] besteht Übereinstimmung, daß das Ziel der ganzen Entwicklung ein einheitlicher Metadaten-Standard (oder zumindest verschiedene interoperable Standards) sein sollte.[130]

Inzwischen existiert eine unüberschaubare Vielzahl von Initiativen zur Standardisierung von Metadaten.[131] Es existieren sogar Projekte, die nur zum Ziel haben, einen Überblick über die verschiedenen Metadaten-Initiativen zu geben.[132] Die Beteiligung einer Unzahl von Akteuren aus den

---

[127] *Hill*, 87 Proc. IEEE 1228, 1235 (1999). Eine Standardisierungsinitiative im Buchverlagsbereich ist der „ONIX International"-Standard, s. <http://www.editeur.org/onix.html>.

[128] *Sollins/Masinter*, RFC 1737, S. 3; *Hill*, 87 Proc. IEEE 1228, 1233 (1999).

[129] Zu unterschiedlichen Anforderungen der Bibliothekswissenschaften und der Informatik s. *Burnett/Bor/Park*, 50 Journal of the American Society for Information Science 1209 ff. (1999).

[130] Vgl. *Bearman/Miller/Rust/Trant/Weibel*, 5 (1) D-Lib Magazine (Januar 1999), unter I.b. Dennoch ist es unrealistisch, daß in absehbarer Zukunft ein einziges allumfassendes Numerierungssystem existieren wird; ebenso *Green/Bide*.

[131] *Rust/Bide*, S. 6 f., zählen beispielhaft 14 Initiativen auf, *PricewaterhouseCoopers*, Standards Framework Report 1, S. 8, nennt gar 89 Initiativen. Einen Überblick gibt *PricewaterhouseCoopers*, Metadata Watch Report #1, <http://www.ifla.org/II/metadata.htm> und anschaulich <http://www.doi.org/doi_presentations/nov2000/metadata/sld014.htm>. Die Standardisierungsinitiativen unterscheiden sich oft in ihrer Ausrichtung. Viele Initiativen standardisieren nur die Syntax und Struktur der Metadaten, während sie deren Semantik einzelnen Metadatensystemen überlassen.

[132] Ein Beispiel für ein solches „Meta-Metadaten-Projekt" ist das von der Europäischen Union geförderte SCHEMAS-Projekt, <http://www.schemas-forum.org>.

unterschiedlichsten Bereichen macht die Etablierung von Metadaten-Standards extrem schwierig.[133] Da diese Standards zusätzlich eine langfristig stabile Lösung des Identifizierungsproblems bieten sollten,[134] handelt es sich um einen langwierigen Prozeß.[135]

Auch wenn sich die Charakteristika einzelner Metadatensysteme unterscheiden, lassen sich einige gemeinsame Anforderungen an Metadatensysteme feststellen.[136] Bei der Identifizierung digitaler Inhalte müssen Numerierungssysteme verwendet werden, die weltweit eindeutige Nummern vergeben.[137] Die Numerierungssysteme lassen sich danach unterscheiden, ob das System lediglich eine fortlaufende Numerierung verwendet (sogenannte „dumb identifiers"), oder ob schon aus der Identifizierungsnummer selbst Informationen über das Identifizierungsobjekt ausgelesen werden können (sogenannte „intelligent identifiers").[138] „Intelligente" Identifizierungssysteme haben mehrere Nachteile.[139] Daher läßt sich in den letzten zehn Jahren eine Tendenz von „intelligenten" Identifizierungssystemen hin zu bloßen Numerierungssystemen erkennen.[140] In einem solchen Numerierungssystem können weitergehende Informationen über

[133] Zu den Problemen im audiovisuellen Sektor s. *PricewaterhouseCoopers*, Metadata Watch Report #1, S. 17 ff. Dort stoßen europäische Ideen einer kollektiven Rechteverwertung mit dem traditionell stärker auf die Individualverwertung ausgerichteten amerikanischen Urheberrechtsverständnis aufeinander. So drängten amerikanische Filmproduzenten im Rahmen der Standardisierung einer Identifikationsnummer für audiovisuelle Werke („International Standard of Audiovisual Numbering", ISAN) darauf, die in der ISAN-Nummer enthaltenen Informationen so gering wie möglich zu halten. Sie waren nicht damit einverstanden, daß Basisdaten wie das Produktionsland oder -jahr eines Filmes aus der ISAN-Nummer ablesbar sind. Dem stand das Interesse von Verwertungsgesellschaften nach möglichst umfassenden Identifizierungssystemen gegenüber; s. dazu *Briem* MR 1997, 260.

[134] Die Metadatensysteme sollen Jahrzehnte oder länger eingesetzt werden können, s. *Paskin*, 87 Proc. IEEE, 1208, 1210, 1216 f. (1999). Teilweise wird vorgebracht, solche Systeme müßten die Informationsflut in mehreren hundert Jahren verkraften können, *Sollins/Masinter*, RFC 1737, S. 3.

[135] *Bearman/Miller/Rust/Trant/Weibel*, 5 (1) D-Lib Magazine (Januar 1999), unter VI.

[136] *Paskin*, 87 Proc. IEEE 1208, 1211 f. (1999).

[137] Dies gilt jedoch nicht in umgekehrter Richtung: Ein Inhalt kann durchaus über mehrere Nummern verfügen, s. 87 *Paskin*, Proc. IEEE 1208, 1209 (1999).

[138] So läßt sich direkt aus der ISBN-Nummer das Erscheinungsland eines Buches ermitteln. S. zur ganzen Kontroverse *Paskin*, 87 Proc. IEEE 1208, 1209 (1999); *Hill*, 87 Proc. IEEE 1228, 1232 (1999); *Green/Bide*; *Bing*, 4 International Journal of Law and Information Technology 234, 243 f. (1996); *de Kroon* in: Hugenholtz (Hrsg.), S. 229, 230 f.

[139] So ist oft im einzelnen umstritten, welche Daten in die „intelligente" Nummer integriert werden sollen. Regelmäßig sind solche Systeme an bestimmte Anwendungen gebunden. Es ist sehr schwierig, ein abstraktes und umfassendes „intelligentes" Identifizierungssystem zu entwerfen; s. dazu *Paskin*, 87 Proc. IEEE 1208, 1213 f. (1999).

[140] *Hill*, 87 Proc. IEEE 1228, 1232 (1999); *Paskin*, 87 Proc. IEEE 1208, 1214 (1999); *Green/Bidel*.

das Identifizierungsobjekt mit Hilfe der Nummer aus einer zentralen Datenbank abgerufen werden.[141]

Weiterhin ist fraglich, bis zu welchem Detail ein Inhalt mit Hilfe von Metadatensystemen identifiziert werden soll: Soll in einem Aufsatz nur der gesamte Aufsatz, jeder Abschnitt, jede Abbildung, jeder Satz, jedes Wort oder gar jeder Buchstabe adressierbar sein?[142] Auch muß beim Entwurf eines Numerierungssystems beachtet werden, wie viele Objekte insgesamt adressiert werden sollen; nur schon bei technisch-wissenschaftlicher Literatur wird von mindestens 100 Milliarden Beiträgen gesprochen, die adressierbar sein müssen.[143] Problematisch ist auch, wer den Aufbau und die Unterhaltung eines solchen Numerierungssystems finanziert.[144] Bei der Entwicklung der notwendigen Organisationsstrukturen sind unter anderem die Datensicherheit, Schutz von Datenintegrität und -authentizität, Performancegesichtspunkte und Skalierungsprobleme zu beachten.[145] Insgesamt ist die Entwicklung noch nicht abgeschlossen. Bisher hat sich noch kein System durchsetzen können, das als allgemeiner Standard akzeptiert wird.[146]

(2) **Einzelne Systeme.** Im folgenden wird ein Überblick über Metadatensysteme zur Identifizierung von Inhalten und Rechteinhabern gegeben, die schon existieren oder derzeit entwickelt werden.

(a) **Herkömmliche Identifizierungssysteme.** Seit den 60er Jahren besteht das „International Standard Book Number (ISBN)"-System für Bücher, Karten und ähnliche Medien. Eine ISBN-Nummer gibt über das Erscheinungsland, den Verlag und den Titel des Buches Auskunft.[147] Sie identifiziert nur eine bestimmte Ausgabe eines Werks; ist das Werk in einer anderen Ausgabe, Sprache oder Fassung erhältlich, so werden mehrere ISBN-Nummern vergeben.[148] Daneben wurde 1989 der „International Standard Recording Code" (ISRC) eingeführt. Er ermöglicht – ähnlich der ISBN – eine Identifizierung von Tonträgern. Die Einführung dieses Standards und dessen Integration in bestehende unternehmensinterne Numerierungssysteme verlief bei den Tonträgerunternehmen jedoch

---

[141] *Paskin*, 87 Proc. IEEE 1208, 1214 (1999).

[142] *Paskin*, 87 Proc. IEEE 1208, 1210 (1999); *Gill*, in: Baca (Hrsg.), S. 12; *Rust/Bide*, S. 10; *de Kroon* in: Hugenholtz (Hrsg.), S. 229, 231. Zu diesem Problem bei eBooks s. *Association of American Publishers*, Numbering Standards for Ebooks, S. 16 ff.

[143] *Paskin*, 87 Proc. IEEE 1208, 1212 (1999).

[144] *Paskin*, 87 Proc. IEEE 1208, 1213 (1999). Die Schaffung der ISBN war über einen Zeitraum von 20 Jahren mit Kosten von 8 Mio. $ verbunden, die von Verlagen und Bibliotheken getragen wurden, *Briem*, MR 1997, 260, 261.

[145] S. dazu ausführlich *Sollins*, RFC 2276.

[146] *Paskin*, 87 Proc. IEEE 1208, 1221 (1999).

[147] S. *Bing*, 4 International Journal of Law and Information Technology 234, 240 f. (1996) mit Beispiel; *de Kroon* in: Hugenholtz (Hrsg.), S. 229, 232.

[148] *Bing*, 4 International Journal of Law and Information Technology 234, 241 (1996).

schleppend und unvollständig.[149] Eine Übersicht über weitere gängige Identifizierungsstandards findet sich in Tabelle 1.[150] Auch wenn diese und andere herkömmlichen Numerierungssysteme nicht speziell für DRM-Systeme entwickelt wurden, können sie in DRM-Systeme integriert werden.[151]

Standard	Identifizierungsobjekt	Standardisierungsgremium
BICI (Book Item and Component Identifier)	Beiträge in Büchern	NISO
CAE/IPI (Compositeur, Auteur, Editeur Code/Interested Parties Identifier)[152]	Rechteinhaber	Verwertungsgesellschaften
ISAN (International Standard Audiovisual Number)[153]	Filme	ISO[154]
ISBN (International Standard Book Number)[155]	Bücher	ISO
ISMN (International Standard Music Number)[156]	Gedruckte Musiknoten	ISO
ISRC (International Standard Recording Code)[157]	Tonträger	ISO
ISSN (International Standard Serial Number)[158]	Periodika	ISO
ISRN (International Standard Report Number)[159]	Technische Berichte	ISO
ISTC (International Standard Textual Work Code)[160]	einzelne Textbeiträge	ISO

[149] Obwohl der ISRC schon vor mehr als 10 Jahren von der ISO standardisiert wurde, verwenden heute weniger als 50 % aller erhältlichen Tonträger dieses Identifizierungssystem, *Gervais* in: Koskinen-Olsson/Gervais (Hrsg.), S. 6, 21.

[150] S. a. *Kaestner*, Anhang 3; *de Kroon* in: Hugenholtz (Hrsg.), S. 229, 232 ff.

[151] So enthält beispielsweise der MPEG-2-Standard ein Datenfeld, in dem ISBN-, ISAN-, ISRC-, ISWC- und ähnliche Numerierungssysteme integriert werden können, s. dazu *Hill*, 87 Proc. IEEE 1228, 1235 (1999). Zu MPEG-2 s. unten Teil 1, D IV 2.

[152] S. dazu *Gervais* in: Koskinen-Olsson/Gervais (Hrsg.), S. 6, 22.

[153] ISO/TC 46/SC 9 Working Group 1, <http://www.nlc-bnc.ca/iso/tc46sc9/wg1.htm>; s. dazu *Gervais* in: Koskinen-Olsson/Gervais (Hrsg.), S. 6, 24; *Briem*, MR 1997, 260.

[154] Auf Initiative von CISAC, AGICOA und FIAPF.

[155] ISO 2108:1992.

[156] ISO 10957:1993.

[157] ISO 3901:1986; s. dazu *Bing*, 4 International Journal of Law and Information Technology 234, 255 ff. (1996).

[158] ISO 3297:1998; <http://www.issn.org>; s. dazu *Bing*, 4 International Journal of Law and Information Technology 234, 243 (1996); *de Kroon* in: Hugenholtz (Hrsg.), S. 229, 233.

[159] ISO 10444:1997.

Standard	Identifizierungs-objekt	Standardisierungs-gremium
ISWC (International Standard Work Code)[161]	Kompositionen	ISO[162]
PII (Publisher Item Identifier)[163]	Beiträge in Periodika und Büchern	Naturwiss. Gesellschaften und Verleger
SICI (Serial Item and Contribution Identifier)[164]	Periodika, Beiträge in Periodika	NISO/ANSI
UMID (Unique Material Identifier)[165]	Fernsehen, Film, einzelne Videosequenzen	SMPTE

Tabelle 1: Verbreitete Identifizierungsstandards

(b) Digital Object Identifier (DOI). Im Jahr 1998 wurde die „International DOI Foundation" mit dem Ziel gegründet, eine Infrastruktur für die Identifikation von Objekten in weltweiten Netzwerken zu schaffen. Kernstück der Initiative ist ein standardisiertes Identifizierungssystem, der „Digital Object Identifier" (DOI),[166] mit dessen Entwicklung ein Projekt der „Association of American Publishers" 1996 begonnen hatte.[167] Das DOI-System ist auf die Adressierung digitaler Inhalte im WWW zugeschnitten, kann jedoch auch für andere, nicht WWW-basierte Dokumente verwendet werden.[168] DOI könnte in Zukunft ein weithin akzeptierter Identifizierungsstandard werden.[169] Derzeit sind über drei Millionen Objekte beim DOI-System registriert, die hauptsächlich aus der Verlagsindustrie stammen.[170]

---

[160] ISO/TC 46/SC 9 Working Group 3, Project 21047, <http://www.nlc-bnc.ca/iso/tc46sc9/istc.htm>.

[161] ISO-Standard 15707 (Entwurf), s. <http://www.nlc-bnc.ca/iso/tc46sc9/iswc.htm>; *Bing*, 4 International Journal of Law and Information Technology 234, 257 ff. (1996).

[162] Auf Initiative von CISAC.

[163] S. dazu *Paskin*, 87 Proc. IEEE 1208, 1224 (1999); *Green/Bide*, S. 6 f.; <http://www.elsevier.nl/inca/homepage/about/pii>.

[164] ANSI/NISO Z39.56–1996, Version 2; s. *Paskin*, 87 Proc. IEEE 1208, 1224 (1999); <http://sunsite.berkeley.edu/SICI/>; *Green/Bide*, S. 5 f.

[165] Standard SMPTE 330M-2000; s. dazu *PricewaterhouseCoopers*, Metadata Watch Report #2, S. 8.

[166] <http://www.doi.org>.

[167] *Paskin*, S. 14; *ders.*, 87 Proc. IEEE 1208, 1224 (1999); s. a. ausführlich *de Kroon* in: Hugenholtz (Hrsg.), S. 229, 234 ff.

[168] Es ist umstritten, ob auch nicht-digitale Güter wie Bücher und Periodika DOI-Nummern erhalten sollten, s. *Gervais* in: Koskinen-Olsson/Gervais (Hrsg.), S. 6, 23.

[169] Ebenso *Hill*, 87 Proc. IEEE 1228, 1231 (1999).

[170] S. *Paskin*, S. 16. So verwenden u. a. der Heidelberger Springer-Verlag und die American Chemical Society das DOI-System. Auch soll DOI bei eBooks eingesetzt werden, s. dazu *Association of American Publishers*, Numbering Standards for Ebooks.

DOI enthält einerseits ein System zur Identifizierung urheberrechtlich geschützter Werke.[171] Es handelt sich um ein dauerhaftes Identifizierungssystem: Wird das Werk im Internet an einen neuen Speicherort verschoben, so ändert sich dessen DOI nicht.[172] Andererseits können mit DOI auch sonstige Informationen über das Werk und den Rechteinhaber ausgedrückt werden.[173] Insgesamt liegt der Schwerpunkt des DOI-Systems derzeit auf der Erstellung einer dauerhaften Numerierungsinfrastruktur und nicht auf der Definition darüber hinausgehender Metadaten.[174] Insbesondere verzichtet das DOI-Metadaten-System bewußt auf Metadaten für Nutzungsbedingungen, die oft Änderungen unterworfen sind und daher mit dem Hauptziel von DOI – der Schaffung dauerhafter Metadaten – schwer vereinbar sind.[175]

(c) **Dublin Core Metadata Initiative.** Die seit 1995 bestehende „Dublin Core Metadata Initiative"[176] definiert einen 15-teiligen Satz von Metadaten, mit dem elektronische Ressourcen beschrieben werden können (unter anderem Titel, Beschreibung, Schlagwort, Urheber, Verleger, Veröffentlichungsdatum, Sprache, Identifizierungsnummer).[177] Bei dem international angelegten Projekt, das sowohl den Bibliotheks- als auch den Online-Bereich ansprechen soll, geht es insbesondere um die Standardisierung von Metadaten in Textdokumenten. Jedoch wird Dublin Core auch für Audio- und Videodaten entwickelt.[178] Der Dublin Core soll auch für Urheber ohne Spezialkenntnisse bedienbar sein und ist daher

---

171 Die DOI-Syntax ist in ANSI/NISO Z39.84–2000, „Syntax for the Digital Object Identifier", standardisiert, abgedruckt bei *Paskin*, S. 51 ff. Es ist möglich, in das DOI-System bestehende Numerierungssysteme (ISBN u. ä.) zu integrieren.

172 Zu diesem Zweck kann in einer Datenbank (dem sog. „Handle System") zu einem (dauerhaften) DOI z. B. eine zugehörige (eventuell nicht dauerhafte) URL ermittelt werden: Der Nutzer sendet eine DOI-Nummer an das System und erhält als Antwort eine URL, unter der er den gesuchten Inhalt erhalten kann. Insoweit ähnelt das System dem DNS-Dienst bei Domain Namen. S. dazu *Paskin*, S. 29 ff.; *ders.*, 87 Proc. IEEE 1208, 1224 (1999). Zum Handle System s. <http://www.handle.net>.

173 So müssen bei der Registrierung eines Objekts beim DOI-System u. a. der Titel und der Ersteller des Inhalts angegeben werden , *s. Paskin*, S. 25 ff.

174 *Paskin*, S. 28. Die notwendigen Metadaten-Definitionen wurden daher nicht im Rahmen des DOI-Projekts standardisiert, vielmehr wird auf das INDECS-Projekts zurückgegriffen, s. *Paskin*, S. 26; zum INDECS-Projekt s. unten Teil 1, C II 2 a aa 2 e.

175 *Paskin*, S. 28.

176 <http://purl.org/DC>. Zur Geschichte s. *Weibel/Kunze/Lagoze/Wolf*, RFC 2413, S. 1 f.; *Ahronheim*, 24 Journal of Academic Librarianship 395, 396 f. (1998).

177 Eine vollständige Aufzählung findet sich bei *Weibel/Kunze/Lagoze/Wolf*, RFC 2413, S. 2.; vgl. ferner *Paskin*, 87 Proc. IEEE 1208, 1218 (1999); *Weibel*, in: Proceedings of the International Symposium on Research, Development and Practice in Digital Libraries 1997, S. 16, 17. Weitere Literaturhinweise zu Dublin Core gibt *Vellucci*, 33 Annual Review of Information Science and Technology 187, 208 ff. (1998).

178 *Hunter/Iannella* in: Nikolaou/Stephanidis (Hrsg.), S. 135, 138 ff.

möglichst einfach ausgestaltet.[179] Der Schwerpunkt von Dublin Core liegt auf Metadaten zur Informationsrecherche.[180] Eine Verbindung zu DRM-Systemen ist zwar vorgesehen; Dublin Core selbst enthält dafür aber keine Definitionen.[181]

Dublin Core hat in unterschiedlichsten Sektoren große Beachtung gefunden.[182] Es wird davon ausgegangen, daß dieses System in den nächsten Jahren eine zentrale Rolle spielen wird, auch weil es sich um eines der wenigen Systeme handelt, die heute schon einsatzbereit sind. Dennoch kann es nur als Ausgangspunkt einer langen Entwicklung hin zu einem umfassenden Metadaten-Standard angesehen werden.[183]

(d) Common Information System (CIS). Verwertungsgesellschaften haben ein großes Interesse, einheitliche Identifizierungssysteme für Werke zu entwickeln, um so die Rechteverwaltung und -verwertung im Verhältnis zu Verwertern (zum Beispiel Tonträgerherstellern oder Radiosendern) und im Verhältnis zu anderen Verwertungsgesellschaften zu vereinfachen.[184] Diesem Ziel dient das 1994 initiierte „Common Information System" (CIS), das von der „Confédération Internationale des Sociétés d'Auteurs et Compositeurs" (CISAC) und deren Mitgliedern[185] initiiert wurde. Mit CIS sollen die Datenbanken der verschiedenen Verwertungsgesellschaften und Verleger durch standardisierte Strukturen untereinander kompatibel gemacht werden. Unter dem Dach des CIS bestehen Datenbanken für die Identifizierung von Rechteinhabern und ihrer Werke.[186] Auch soll eine einheitliche Datenbank mit Informationen über Nutzungsbedingungen und ähnliches geschaffen werden.[187] Weiterhin soll im Rahmen des CIS eine Standardisierung von Numerierungssystemen erreicht werden. So wurden im Rahmen von CIS der „International

[179] *Weibel* in: Proceedings of the International Symposium on Research, Development and Practice in Digital Libraries 1997, S. 16, 17; *Lagoze*, 7 (1) D-Lib Magazine (January 2001).

[180] *Paskin*, 87 Proc. IEEE 1208, 1218 (1999).

[181] S. *Weibel/Kunze/Lagoze/Wolf*, RFC 2413, S. 6.

[182] *Bearman/Miller/Rust/Trant/Weibel*, 5 (1) D-Lib Magazine (Januar 1999), unter V, sprechen vom Dublin Core als dem „HTML of Web metadata". Zur Verwendung des Dublin Core bei eBooks s. *Open eBook Forum*, OEB Publication Structure 1.0, S. 12 ff.

[183] Teilweise kritisch *Paskin*, 87 Proc. IEEE 1208, 1219 (1999).

[184] *Hill*, 87 Proc. IEEE 1228, 1230 (1999); *Kaestner*, S. 40 f.

[185] Die CISAC ist ein internationaler Verbund von über 200 Verwertungsgesellschaften in fast 100 Ländern.

[186] So die „Interested Parties Information"-Datenbank und die „Works Information Database" (WID), s. *Kaestner*, S. 40 f. Im Jahr 2000 umfaßte die CAE-Datenbank 2,5 Millionen, die „Works Information Database" (WID) 1 Million, der Audio-visual Index (AVI) 1,3 Millionen Einträge; inzwischen wurden über 1 Million ISWC-Nummern vergeben.

[187] Sog. „Agreements and Schedule Information" (ASI) Datenbank, s. *Kaestner*, S. 41.

Standard Works Code" (ISWC) und die „International Standard Audiovisual Number" (ISAN) entwickelt, die als ISO-Standard verabschiedet werden sollen.[188] Die Verwertungsgesellschaften erhoffen sich davon Effizienzgewinne und die Möglichkeit einer automatisierten Rechtevergabe.[189] Schließlich will CIS auch – beispielsweise durch digitale Wasserzeichen – die Nutzung urheberrechtlich geschützter Werke im Netz kontrollieren können.[190]

(e) **INDECS-Projekt.** Das von der Europäischen Union geförderte Projekt „Interoperability of Data in ECommerce Systems" (INDECS) dauerte von 1998 bis 2000.[191] An diesem Projekt waren europäische, internationale und amerikanische Verwertungsgesellschaften, Verleger und Standardisierungsvereinigungen beteiligt. Dabei ging es nicht um die Entwicklung neuer Metadaten-Systeme; vielmehr sollte der Frage der Interoperabilität bestehender Systeme nachgegangen werden, um damit die Grundlage für ein allgemeines Metadatensystem zu legen.[192] Das INDECS-Projekt erfaßt auch Metadaten für Nutzungsbedingungen.[193]

(f) **Metadaten im WWW und sonstige Initiativen.** Im World Wide Web (WWW) müssen WWW-Seiten eindeutig identifizierbar sein. Dies wird durch die Adresse einer WWW-Seite, den sogenannten „Uniform Resource Locator" (URL), gewährleistet (zum Beispiel http://www.jura.uni-tuebingen.de). Aus mehreren Gründen wird an Reformen dieses Adressierungssystems gearbeitet.[194] Standardisierungsinitiativen existieren hier

---

[188] S. *Hill*, 87 Proc. IEEE 1228, 1230 (1999); *de Kroon* in: Hugenholtz (Hrsg.), S. 229, 233. Zu ISWC und ISAN s. a. oben Tabelle 1, S. 40 f.

[189] *Hill*, 87 Proc. IEEE 1228, 1230 (1999).

[190] Zu diesem Einsatzfeld digitaler Wasserzeichen s. unten Teil 1, C V 3.

[191] Zur Geschichte s. *Bearman/Miller/Rust/Trant/Weibel*, 5 (1) D-Lib Magazine (Januar 1999), unter I.b.

[192] Anschauliches Beispiel bei *Rust/Bide*, S. 12 ff.

[193] Jedoch werden die entsprechenden Metadaten-Sätze nicht vollständig von INDECS definiert, vielmehr wird auf rechtliche Definitionen verwiesen, s. *Rust/Bide*, S. 30. Damit schafft INDECS nur den Rahmen für den Einsatz solcher Metadaten.

[194] Wenn eine WWW-Seite im Internet an einen anderen Speicherort verschoben wird, so ändert sich auch deren URL. URLs ermöglichen keine dauerhafte Identifizierung digitaler Inhalte. Dies soll durch sog. „Uniform Resource Names" (URNs) ermöglicht werden, s. *Sollins/Masinter*, RFC 1737, S. 2 f.; *Berners-Lee/Fielding//Masinter*, RFC 2396, S. 4. Während ein URN gleichsam den Namen eines Objekts bezeichnet, bezeichnet die URL den physischen Speicherort des Dokuments. URNs stellen keinen eigenen Numerierungsstandard zur Verfügung; vielmehr bietet der URN-Standard eine standardisierte Syntax, mit der Numerierungsstandards ausgedrückt werden, *Daigle/van Gulik/Iannella/Faltstrom*, RFC 2611, S. 2. So können beispielsweise ISBN- oder ISSN-Nummern als URNs dargestellt werden, s. *Lynch/Preston/Daniel*, RFC 2288; *Hakala/Walravens*. Im praktischen WWW-Betrieb gibt der Nutzer eine URN ein. Daraufhin kontaktiert der Rechner des Nutzers eine zentrale Datenbank, von der er die zugehörige URL erhält. Der Rechner kontaktiert dann die URL und bezieht das dort erhältliche Dokument. Ein erster solcher „Resolver Discovery Service" wurde 1997 vorgeschlagen; eine überarbeitete Fassung findet sich bei *Mealling/Daniel*, RFC 2915.

seit Beginn der 90er Jahre.[195] Daneben lassen sich in WWW-Seiten schon seit langem mit Hilfe sogenannter „Meta-Tags" umfangreiche Metadaten integrieren.[196] Aus mehreren Gründen haben sich Meta-Tags zumindest im DRM-Bereich nicht durchsetzen können.[197] Im WWW-Umfeld existieren noch weitere Metadaten-Initiativen, die teilweise auf spezielle Bereiche zugeschnitten sind,[198] teilweise auch ein generelles Metadaten-System etablieren wollen.[199] Schließlich bestehen zahllose Initiativen, die Metadaten-Standards für zukünftige digitale Bibliotheken zu entwickeln.[200]

Weitere Literaturhinweise zu URNs finden sich unter <http://www.ifla.org/II/metadata.htm#urns>. Ein vergleichbares System sind die sogenannten „Persistent Uniform Resource Locators" (PURLs), s. <http://purl.org> und *de Kroon* in: Hugenholtz (Hrsg.), S. 229, 236. Der Begriff des „Uniform Resource Identifier" (URIs) stellt den Oberbegriff für diese unterschiedlichen Adressierungsschemata dar, *Berners-Lee*, RFC 1630, S. 3; zu „Uniform Resource Characteristics" (URCs), einem früher geplanten Metadaten-System, s. <http://www.ifla.org/II/metadata.htm#urcs>; s. zum ganzen *Paskin*, 87 Proc. IEEE 1208, 1220 f. (1999).

[195] Die URN-Syntax wurde im Mai 1997 standardisiert, *Moats*, RFC 2141, die allgemeinere URI-Syntax wurde im August 1998 standardisiert, *Berners-Lee/Fielding//Masinter*, RFC 2396. Die Standardisierung findet unter anderem im Rahmen einer Arbeitsgruppe der IETF statt, s. <http://www.ietf.org/html.charters/urn-charter. html>.

[196] Die im WWW erhältlichen Seiten sind in der „Hypertext Markup Language" (HTML) geschrieben. In HTML können mit Hilfe sogenannter „tags" neben Formatierungsanweisungen auch Metadaten ausgedrückt werden. So unterstützt der HTML-Standard Angaben wie <META name="Author" content="Stefan Bechtold">. Diese sog. „Meta-Tags" werden bei jedem Abruf einer WWW-Seite mitübertragen und vom Browser eventuell ausgewertet, werden dem Nutzer aber nicht angezeigt. Mit Hilfe von Meta-Tags können auch Dublin-Core-Metadaten ausgedrückt werden, s. *Kunze*, RFC 2731. Zur marken- und wettbewerbsrechtlichen Problematik von Meta-Tags s. unten bei Fn. 1242.

[197] So ist nicht standardisiert, welche Bedeutung die einzelnen Meta-Tags haben. Es ist unklar, ob der „Author" im obigen Beispiel der Ersteller der Web-Seite, der Urheber des darin enhaltenen Textes, dessen Verleger oder der Betreiber der Web-Seite ist. Auch lassen sich komplexere Aussagen nicht in Meta-Tags definieren, s. *Lassila*, IEEE Internet Computing Juli/August 1998, S. 30, 35. Meta-Tags spielen aber bei Suchmaschinen im Internet eine wichtige Rolle.

[198] Zur „Platform for Internet Content Selection" (PICS), die speziell auf Fragen des Jugendschutzes zugeschnitten ist, s. *Lassila*, IEEE Internet Computing Juli/August 1998, S. 30, 35, und <http://www.w3.org/PICS>.

[199] So zum Beispiel das 1997 von Netscape vorgeschlagene „Meta Content Framework", s. <http://www.w3.org/TR/NOTE-MCF-XML>. Zum 1997 von Microsoft beim W3C vorgeschlagenen „Channel Definition Format", das auf sogenannte push-Dienste zugeschnitten war, s. <http://www.w3.org/TR/NOTE-CDFsubmit.html>. Ein weiteres Identifizierungssystem, das unter anderem für digitale Inhalte im WWW (Text, Audio) gedacht ist, ist das „InterDeposit Digital Number"-System (IDDN), das von der französischen „Agence pour la Protection des Programmes" gegründet wurde, s. <http://www.iddn.org>. Weitere Systeme werden bei *Marchiori*, 30 Computer Networks and ISDN Systems 1 (1998), erwähnt.

[200] S. nur *Baldonado/Chang/Gravano/Paepcke*, 1 International Journal on Digital Libraries 108 ff. (1997).

Auch für eBooks werden standardisierte Metadaten-Systeme entwickelt,[201] ebenso für den Rundfunk- und Fernsehsektor.[202]

bb) Identifizierung der Nutzungsbedingungen

(**1**) **Allgemeines.** Neben Informationen zur Identität der Inhalte und ihrer Rechteinhaber müssen in einem DRM-System auch Informationen verfügbar sein, zu welchen Bedingungen die Inhalte genutzt werden dürfen. Seit einigen Jahren werden formalisierte Sprachen entwickelt, mit denen Nutzungsbedingungen (sogenannte „usage rules") in einer maschinenlesbaren Form ausgedrückt werden können (sogenannte „rights specification languages" oder „rights management languages"). Viele der heutigen DRM-Systeme verwenden solche Sprachen. Sie ermöglichen die standardisierte automatische Kommunikation zwischen verschiedenen Komponenten eines DRM-Systems hinsichtlich erlaubter Nutzungen und bilden gleichzeitig die Grundlage für Nutzungsverträge, die der DRM-Betreiber oder ein Inhalteanbieter mit dem Nutzer schließt.[203] Der Inhalteanbieter kommt mit den Einzelheiten der „rights management language" nicht in Berührung. Vielmehr legt er in einer anwenderfreundlichen Software-Anwendung die Nutzungsbedingungen fest, die dann von der Anwendung in eine maschinenlesbare, standardisierte Form gebracht werden.[204]

In welchem Umfang und in welcher Ausdifferenzierung Nutzungsbedingungen festgelegt werden können, hängt vom einzelnen DRM-System ab. In manchen Systemen sind dafür nur zwei Bits vorgesehen, die festlegen, ob eine Kopie des Inhalts erstellt werden darf oder nicht.[205] Nutzungsbedingungen, die in „rights management languages" ausgedrückt werden, können aber auch sehr umfangreich sein, wenn vielfältige Bedingungen für unterschiedliche Nutzungsarten festgelegt werden. Die grundsätzlichen Möglichkeiten solch umfangreicher „rights management languages" soll am Beispiel der bekanntesten und am Besten dokumentierten Sprache – nämlich XrML – dargestellt werden.[206]

---

[201] So z. B. *Association of American Publishers*, Metadata Standards for Ebooks.

[202] Zu MPEG-7, einem Metadatenstandard zur Beschreibung von Video- und Audio*inhalten*, s. unten Teil 1, D IV 2.

[203] Zu diesem rechtlichen Aspekt s. unten Teil 2, B I.

[204] *Contentguard*, XrML Version 1.03, S. 96.

[205] Das bei DAT-Geräten eingesetzte „Serial Copyright Management System" (SCMS) verwendet dieses Verfahren, s. dazu oben Teil 1, C I 2, und unten Teil 1, D II 1.

[206] Auf andere „rights management languages" wird in der Folge nur im Überblick eingegangen, da sich deren Funktionsumfang in der Regel nicht wesentlich unterscheidet. Zu der bei InterTrust eingesetzten „rights management language" s. *Gunter/Weeks/Wright*. Zu Identifizierungs- und Metadatensystemen im Bereich des digitalen Fernsehens s. *European Telecommunications Standard Institute*, ETSI EN 300 468 V1.4.1; *dass.*, ETSI TR 101 211 V1.4.1; s. dazu *Reimers*, Fernseh- und Kino-Technik 52 (1998), 82 f.

(2) eXtensible rights Markup Language (XrML). Die „eXtensible rights Markup Language" (XrML) von Contentguard, Inc., ist eine Fortentwicklung der „Digital Property Rights Language" (DPRL), die seit 1996 von *Mark Stefik* am „Palo Alto Research Center" des Unternehmens Xerox (Xerox PARC) entwickelt wurde.[207] Die Sprache ermöglicht die Definition von Nutzungsbedingungen digitaler Inhalte und stellt die Integrität und Authentizität der übertragenen Inhalte sicher. Rechteinhaber und Distributoren sollen die Möglichkeit erhalten, gemäß einem von ihnen gewählten Geschäftsmodell die Nutzungsmöglichkeiten, Nutzungsbedingungen und Zahlungsmodalitäten beim Vertrieb digitaler Inhalte in einer standardisierten maschinenlesbaren Sprache festzulegen.[208]

(a) Inhaltliche Beschränkung der Nutzung. Im einzelnen können folgende Nutzungsmöglichkeiten digitaler Inhalte mit XrML definiert werden:[209]

- Erstellen einer Kopie des digitalen Inhalts („copy"): Dabei kann festgelegt werden, wie oft von einem Original eine Kopie erstellt werden darf, und ob Kopien der Kopie (also Kopien der zweiten Generation) möglich sein sollen.
- Übertragen des Inhalts an einen Dritten („transfer"): Überträgt ein Nutzer den Inhalt an einen Dritten, so löscht das DRM-System den Inhalt beim ersten Nutzer dauerhaft, so daß nach dem Übertragungsvorgang nur noch der Dritte über den Inhalt verfügt.
- Ausleihen des Inhalts an einen Dritten („loan"): Leiht ein Nutzer den Inhalt an einen Dritten aus, so deaktiviert das DRM-System für die spezifizierbare Ausleihdauer den Zugriff des ersten Nutzers auf den Inhalt, während der Dritte Zugriff auf den Inhalt erhält. Nach Ablauf der Ausleihdauer wird der Zugriff des Dritten deaktiviert und der Zugriff des ursprünglichen Nutzers wieder hergestellt. So ist sichergestellt, daß immer nur ein Nutzer auf den Inhalt Zugriff hat.
- Anzeige oder Ausdrucken des Inhalts („play" oder „print").
- Exportieren des Inhalts („export"): Darunter ist die Abspeicherung des Inhalts in einer ungeschützten Form zu verstehen. Der exportierte digitale Inhalt verläßt also den DRM-Schutz.
- Bearbeiten eines Inhalts („edit"): Dabei kann auch festgelegt werden, welche Arten von Bearbeitungen dem Nutzer erlaubt sind. So kann dem Nutzer bei einer Audiodatei erlaubt sein, die Tonhöhe Musikstückes zu ändern, nicht aber, selbst Musik hinzuzufügen.[210]

---

[207] *Contentguard*, XrML Version 1.03, S. 5; s. a. *Stefik*, Internet Dreams, S. 228 ff.

[208] *Contentguard*, XrML Version 1.03, S. 5. Eine überblicksartige Beschreibung der Sprache (damals noch DPRL genannt) findet sich in *Gimbel*, 50 Stan. L. Rev. 1671, 1677 ff. (1998); s. a. *Stefik*, Internet Dreams, S. 228 ff.; *ders.*, 12 Berkeley Tech. L. J. 137, 139 ff. (1997).

[209] Eine vollständige Auflistung findet sich bei *Contentguard*, XrML Version 1.03, S. 30 ff.

[210] *Contentguard*, XrML Version 1.03, S. 38.

– Löschen des Inhalts („delete"): Die Möglichkeit des Löschens eines Inhalts kann beschränkt werden, um das unbeabsichtigte Löschen oder das unberechtigte Löschen durch Dritte zu verhindern.
– Sicherheitskopie des Inhalts („backup"): Dabei wird eine verschlüsselte lokale Kopie des Inhalts erstellt, auf die der Nutzer bei einem zufälligen unbeabsichtigten Löschen der Originalfassung zurückgreifen kann. Dieses Wiederherstellen („restore") kann wiederum an bestimmte Bedingungen geknüpft werden.[211]

(b) **Zeitliche, räumliche und persönliche Beschränkung der Nutzung.** In XrML können *zeitliche Beschränkungen* der Nutzungsmöglichkeiten eines Inhalts festgelegt werden.[212] Zum Beispiel kann die Nutzung der Test-Version eines Computerprogramms auf zwei Wochen und die Nutzung aktueller Finanzdaten auf wenige Stunden beschränkt werden. Auch kann die Nutzung auf insgesamt zehn Stunden beschränkt werden, wobei dem Nutzer offensteht, wann genau er den Inhalt benutzt.[213] In XrML kann auch eine *räumliche Beschränkung* der Nutzung geschützter Inhalte ausgedrückt werden. So kann die Nutzung auf ein bestimmtes Land, einen bestimmten Postleitzahlen-Bereich oder auf bestimmte IP-Adressen[214] beschränkt werden.[215] XrML bietet die Möglichkeit, die Nutzung digitaler Inhalte auf *bestimmte Personenkreise* zu beschränken. Damit kann sichergestellt werden, daß nur diejenigen Personen Zugriff auf die Inhalte haben, die dafür bezahlt haben. Auch kann festgelegt werden, wie viele Nutzer digitale Inhalte untereinander tauschen und gleichzeitig nutzen dürfen.[216]

(c) **Urheberrechtliche Schrankenbestimmungen.** Soll die Nutzung eines geschützten Inhalts wegen urheberrechtlicher Schrankenbestimmungen erlaubt werden, so kann in XrML bestimmten *Personen* (Studenten, Wissenschaftler etc.) die unentgeltliche Nutzung erlaubt werden. Es gibt keine Möglichkeit, die unentgeltliche Nutzung zu bestimmten *Zwecken* zu

---

[211] *Contentguard*, XrML Version 1.03, S. 42 f., führt als Beispiel eine Konfiguration an, nach der der Nutzer berechtigt ist, insgesamt drei Sicherheitskopien zu erstellen. Die erste Sicherheitskopie ist kostenlos, die zweite Wiederherstellung kostet 15 Dollar, und vor der dritten Wiederherstellung muß der Händler kontaktiert werden, bei dem der Nutzer den geschützten Inhalt erworben hat.

[212] S. dazu *Contentguard*, XrML Version 1.03, S. 46 f.

[213] Dafür sind manipulierungssichere Zeitmessungen notwendig, damit der Nutzer das System nicht überlisten kann. Ein vollständiges DRM-System verfügt mitunter über solche Komponenten. Zu manipulationssicherer Hard- und Software s. unten Teil 1, C IV. Auch kann ein Zeitvergleich mit einem zentralen Server stattfinden.

[214] Die IP-Adresse eines Rechners ist eine eindeutige Zahl (z. B. 134.2.34.92), die zur Adressierung des Rechners im Internet verwendet wird.

[215] *Contentguard*, XrML Version 1.03, S. 61.

[216] Dies ist insbesondere in P2P-Umgebungen wichtig, s. dazu unten Teil 1, E I. Dabei kann das System beispielsweise festlegen, daß ein Nutzer zwar berechtigt ist, den geschützten Song an einen Dritten weiterzugeben, daß der Dritte dann aber ohne Zahlung nur einen 20-sekündigen Ausschnitt hören darf.

erlauben. Dies wird damit begründet, daß XrML eine automatisierte Umgebung zur Nutzung geschützter Inhalte ermöglichen soll. Es übersteige die technischen Möglichkeiten heutiger Systeme festzustellen, zu welchem Zweck ein geschützter Inhalt genutzt werde.[217] Dennoch ist auffällig, daß XrML zwar umfassende Möglichkeiten enthält, Nutzungsbedingungen zu definieren, die Rechteinhaber schützen. Dagegen sind die Möglichkeiten, die Nutzungsbedingungen konform zu urheberrechtlichen Schrankenbestimmungen auszugestalten, recht beschränkt.[218] Auch unterliegt die Festlegungen von Nutzungsbedingungen in XrML grundsätzlich keinen zeitlichen Grenzen. Dies hat zur Folge, daß ein DRM-System digitale Inhalte auch technisch schützen kann, wenn der Schutz durch das Urheberrecht schon lange abgelaufen ist (s. § 64 UrhG).[219]

(**d**) **Sonstiges.** Alle dargestellten Möglichkeiten, die Nutzung des geschützten Inhalts zu definieren, können an die Bedingung geknüpft werden, dafür einen gewissen Betrag zu zahlen.[220] Dabei kann entweder eine Zahlung für jede einzelne Nutzung („per use fee") oder für einen bestimmten Nutzungszeitraum („metered fee") erfolgen. Auch können Mindest- und Höchstbeträge festgelegt werden, die immer zu zahlen sind. Schließlich können Rabatte, Gutscheine und ähnliches berücksichtigt werden.

Ein DRM-System muß kontrollieren, in welcher Umgebung die geschützten Inhalte verfügbar sind. Wenn ein DRM-System einen digitalen geschützten Inhalt von einem sicheren Server an ein ungeschütztes Endgerät überträgt, wird dem Nutzer eventuell die Möglichkeit zur Erstellung von Raubkopien gegeben. XrML bietet daher die Möglichkeit, die Sicherheit unterschiedlicher Hard- und Software-Umgebungen exakt zu beschreiben und zu vergleichen.[221] So kann beispielsweise festgelegt werden, daß das Ausdrucken nur auf speziellen Druckern möglich ist, die beim Ausdrucken automatisch ein digitales Wasserzeichen einfügen.[222] Oder es kann vorgesehen werden, daß ein Film nur auf Projektionsgeräten angezeigt werden kann, die für den Hausgebrauch vertrieben wer-

---

[217] Vgl. *Contentguard*, XrML Version 1.03, S. 71.

[218] Vgl. *Contentguard*, XrML Version 1.03, S. 71. Zum allgemeinen Konflikt zwischen DRM-Systemen und urheberrechtlichen Schrankenbestimmungen s. unten Teil 3, B II 3.

[219] S. *Contentguard*, XrML Version 1.03, S. 103. Dazu auch *ebda.*, S. 98, wo zu der Frage des Verhältnisses zwischen der zeitlichen Beschränkung des Urheberrechts auf 70 Jahre post mortem auctoris und dem potentiell zeitlich unbeschränkten Schutz von DRM-Systemen steht: „This issue goes beyond the scope of this document. […] The issue here is social and legal, not technological."

[220] *Contentguard*, XrML Version 1.03, S. 47 ff.

[221] *Contentguard*, XrML Version 1.03, S. 59 f.

[222] *Contentguard*, XrML Version 1.03, S. 62 ff. Zu digitalen Wasserzeichen s. unten Teil 1, C II 2 b bb.

den – für profesionelle Kino-Aufführungen wird der Inhalt dann in einer anderen Version mit anderen Nutzungsbedingungen vertrieben.[223]

(3) **Open Digital Rights Language (ODRL), Electronic Book eXchange (EBX).** Eine weitere Initiative, die einen offenen Standard einer „rights management language" etablieren will, wurde im Jahr 2000 unter dem Namen „Open Digital Rights Language" gestartet.[224] Abbildung 2 enthält ein fiktives Beispiel für Nutzungsbedingungen eines „eBooks",[225] die in ODRL ausgedrückt sind.[226]

```
 1  <?xml version="1.0"?>
 2  <rightsxmlns="http://odrl.net/0.8/"
 3      xmlns:xlink="http://www.w3.org/1999/xlink">
 4
 5    <asset ID="001">
 6      <uid idscheme="DOI">doi://10.9999/EB/rossi-0001</uid>
 7      <name> How to Wash Cats </name>
 8    </asset>
 9
10    <usage ID="002">
11      <asset xlink:href="#001"/>
12      <rightsholder xlink:href="#003"/>
13      <display>
14        <constraint>
15          <individual>
16            <uidscheme="X500">c=ZZ;o=People Directory; cn=Fritz Meier</uid>
17          </individual>
18          <accumulated> P10H </accumulated>
19          <interval> P4D </interval>
20        </constraint>
21      </display>
22      <print>
23        <remark> Can only Print 2 Copies </remark>
24        <constraint>
25          <count start="0" end="2"/>
26        </constraint>
27      </print>
28    </usage>
29
30  </rights>
```

Abbildung 2: Beispiel von Nutzungsbedingungen in ODRL

Danach darf eine bestimmte Person („Fritz Meier") das eBook während einer Periode von vier Tagen immer höchstens zehn Stunden lang benutzen bzw. lesen (Zeilen 13–21). Außerdem darf jede Person das eBook

[223] *Contentguard*, XrML Version 1.03, S. 34 f.
[224] *Iannella*; <http://www.odrl.net>.
[225] S. dazu unten Teil 1, D II 6.
[226] Es handelt sich um ein Beispiel, das den Beispielen in *Iannella*, S. 22 ff., nachgebildet wurde.

ausdrucken, allerdings nur insgesamt zwei Mal (Zeilen 22–27). Sonstige Nutzungen sind nicht erlaubt; insbesondere dürfen keine Dritten das eBook lesen, das eBook darf nicht kopiert werden, es darf nicht an Dritte weitergegeben werden, und es dürfen nicht Teile des eBooks zu Zitats- oder Bearbeitungszwecken entnommen werden.[227]

Im Rahmen der „Electronic Book eXchange Working Group" (EBX) wurde eine umfassende „rights management language"-Spezifikation für eBooks erarbeitet.[228] Sie enthält auch eine Spezifikation von Nutzungsbedingungen. Dabei kann unter anderem das Recht zum Weiterverkauf, Verschenken, Verleihen, Verändern (sogenannte „transfer rights") sowie zum Anzeigen, Drucken, Kopieren, Installieren, Löschen, Anmerken und Exportieren (sogenannte „usage rights") des eBooks gewährt werden.[229] Diese Rechte können auf bestimmte Personengruppen,[230] bestimmte Lesegeräte,[231] auf bestimmte Nutzungszeiten[232] oder auf bestimmte Teile des digitalen Textes beschränkt werden.[233]

cc) Resource Description Framework (RDF)

Das World Wide Web Consortium (W3C), ein wichtiges Standardisierungsgremium im WWW,[234] beschäftigt sich seit 1995 mit Metadaten, zuerst im Rahmen des „Platform for Internet Content Selection (PICS)"-Projekts, einem auf den Jugendschutzbereich zugeschnittenen Metadaten-System.[235] Da sich PICS nicht für ein allgemeines Metadaten-System eignete, entwickelte das W3C darauf aufbauend das „Resource Description Framework" (RDF).[236] RDF stellt eine Infrastruktur zur Codierung, zum

---

[227] Solche Nutzungsbedingungen sind keine theoretischen Spielereien. Tatsächliche Beispiele mit ähnlichen Einschränkungen werden unten Teil 3, B II 3 a, dargestellt.

[228] *Electronic Book Exchange Working Group*, The EBX System Specification Version 0.8. Im Februar 2001 kündigten EBX und das „Open eBook Forum" an, sich zusammenzuschließen; s. zu beiden Initiativen ausführlich unten Teil 1, D II 6.

[229] *Electronic Book Exchange Working Group*, S. 86 f.

[230] Diese können nach der Zugehörigkeit zu einem bestimmten Netzwerk oder zu einer Region, aber auch nach der Inhaberschaft bestimmter Lesegeräte oder IP-Adressen bestimmt werden, s. *Electronic Book Exchange Working Group*, S. 87.

[231] So kann die Ausgabe des digitalen Text auf einen normalen Bildschirm, einem normalen Drucker, einen manipulationssicheren Drucker („trusted printer") oder auf Disketten beschränkt werden, *Electronic Book Exchange Working Group*, S. 88.

[232] Dabei können Anfangs- und Endzeit der Nutzung, die gesamte Höchst-Nutzungsdauer, die Anzahl der möglichen Einzelnutzungen sowie die Zeitabstände, die zwischen den einzelnen Nutzungen liegen, festgelegt werden, *Electronic Book Exchange Working Group*, S. 89.

[233] *Electronic Book Exchange Working Group*, S. 87 f.

[234] Zu Aufgaben, Struktur und Verfahrensweise des W3C s. im Überblick *Mayer*, K&R 2000, 13, 18 f.

[235] S. dazu oben Fn. 198.

[236] *Lassila*, IEEE Internet Computing Juli/August 1998, S. 30, 36. Die Entwicklung von RDF baut noch auf vielen anderen Ideen auf, u. a. dem „Warwick Framework", dem „Dublin Core"-Projekt sowie Projekten von Microsoft und Netscape, s. dazu *Vellucci*, 33 Annual Review of Information Science and Technology 187, 210 f. (1998).

Austausch und zur Wiederverwendung von Metadaten zur Verfügung. RDF soll die Interoperabilität zwischen verschiedenen Anwendungen und Systemen herstellen, die Metadaten verwenden und untereinander austauschen.[237] Dazu standardisiert RDF Syntax und Struktur eines Metadaten-Systems, nicht aber die Bedeutung der verwendeten Metadaten-Felder.[238] Die Festlegung dieser Semantik wird den einzelnen Bereichen überlassen, die RDF verwenden (DRM-Systeme, Datenschutz, Bibliotheken). Als allgemein akzeptierter Standard hat sich RDF noch nicht durchsetzen können. Mitunter wird RDF eine zu komplexe und unübersichtliche Syntax vorgeworfen.[239] Insgesamt ist RDF ein ambitioniertes Projekt, das zu einem umfassenden Metadaten-System führen könnte. Die möglichen Anwendungsbereiche von RDF gehen weit über DRM-Systeme hinaus, was auch den sehr hohen Abstraktionsgrad der RDF-Spezifikationen erklärt.

dd) Zusammenfassung

Seit einigen Jahren existieren umfassende Versuche, Metadaten-Systeme zur Identifizierung digitaler Inhalte, ihrer Rechteinhaber und ihrer Nutzungsbedingungen zu entwickeln und zu standardisieren. Während im Bereich der Metadaten für Inhalte und Rechteinhaber zahlreiche Systeme existieren und auch die Standardisierungsbemühungen relativ weit fortgeschritten sind, befindet sich die Entwicklung von Metadaten-Sprachen für Nutzungsbedingungen erst am Anfang.

„Rights management languages" stellen praktisch die „lingua franca" eines DRM-Systems dar. Grundsätzlich kann mit Hilfe einer umfangreichen Definition der Nutzungsbedingungen die Nutzung eines digitalen Inhalts äußerst differenziert kontrolliert werden. Herkömmliche Geschäftsmodelle wie Buch-Clubs, zeitlich begrenzte Schnupperangebote, spezielle Preise für Geschäftskunden oder akademische Institutionen, selbst Vielflieger-Programme können damit in das digitale Umfeld übertragen werden. DRM-Systeme bieten damit die Möglichkeit einer stark ausgeprägten Nutzungsdifferenzierung in inhaltlicher, zeitlicher, räumlicher und persönlicher Hinsicht.

„Rights management languages" sind nur eine Komponente eines technischen Systems zum Schutz von Urheber- und Leistungsschutzrechten. Nutzungsbedingungen, die mit Hilfe solcher Sprachen definiert wurden,

---

RDF basiert – wie auch XrML, ODRL und EBX – auf XML. Zu den Unterschieden zwischen RDF und XML sowie dessen DTDs s. *Lassila*, a. a. O., S. 30, 34. S. weiterhin *Lassila/Swick*.

[237] *Lassila/Swick*, Abschnitt 2.2.3; *Lassila*, IEEE Internet Computing Juli/August 1998, S. 30, 34.

[238] S. zum ganzen *Lassila*, IEEE Internet Computing Juli/August 1998, S. 30, 34; *Brickley/Guha*.

[239] Auch wird kritisiert, daß der Adressierungsmechanismus von RDF zu grobrastrig ist; s. dazu *Saarela*, S. 22. Ein Lösungsansatz stellt die XPointer-Spezifikation dar, s. <http://www.w3.org/TR/xptr>.

können verändert, gefälscht und umgangen werden. Die Antwort auf diese Problematik liegt außerhalb von „rights management languages" und wird von anderen Komponenten eines DRM-Systems angegangen (wie zum Beispiel manipulationssicheren Hard- und Softwareumgebungen sowie Zertifizierungsinstanzen).[240]

Die Interoperabilität verschiedener Metadaten-Systeme ist ein schwieriges und teilweise ungelöstes Problem.[241] Teilweise wird von einer Standardisierung zum jetzigen Zeitpunkt abgeraten, da die Anforderungen an Metadaten-Systeme im derzeitig äußerst dynamischen Umfeld noch nicht klar seien.[242]

b) Identifizierungsverfahren

Von der bisher dargestellten Problematik der Definition von Metadaten ist die Frage zu trennen, wie die Metadaten mit dem digitalen Inhalt, auf den sie sich beziehen, verbunden werden sollen. Grundsätzlich können die Metadaten direkt mit dem digitalen Inhalt verbunden werden. Es ist aber auch möglich, die eigentlichen Metadaten in einer zentralen Datenbank zu speichern und den digitalen Inhalt nur mit einer Identifizierungsnummer zu versehen, die dann auf die Datenbank verweist.[243] In beiden Fällen müssen aber – mal mehr, mal weniger – Daten direkt mit dem digitalen Inhalt verbunden werden. Dafür existieren mehrere Ansätze, von denen im folgenden zwei dargestellt werden.

aa) Metadaten als Teil des Datenformats

Viele Datenformate enthalten spezielle Bereiche, die für Metadaten reserviert sind (oft im sogenannten „header"). So enthält der MPEG-2-Standard Möglichkeiten, Informationen über den Rechteinhaber am Beginn der Videodaten abzuspeichern.[244] Das bei DAT-Geräten verwendete SCMS speichert Kopierkontrollinformationen in zwei dafür reservierten Bits ab.[245] An diesen Verfahren ist jedoch problematisch, daß es grundsätzlich möglich ist, die Metadaten von den dazugehörigen digitalen Inhalten zu trennen.[246] Ein Angreifer könnte die Metadaten aus dem speziellen Datenbereich entfernen und die digitalen Inhalte ohne jegliche Metadaten an Dritte weiterverbreiten. Der Schutz durch das DRM-System, der auf Metadaten hinsichtlich des Inhalts, seiner Rechteinhaber

---

[240] S. dazu unten Teil 1, C III 2 b, und Teil 1, C IV.

[241] S. dazu *Cromwell-Kessler* in: Baca (Hrsg.); <http://www.ukoln.ac.uk/metadata/interoperability>.

[242] So hinsichtlich der Standardisierung von Metadaten für Nutzungsbedingungen *Association of American Publishers*, Metadata Standards for Ebook, S. 12.

[243] Zu der Unterscheidung zwischen „dumb" und „intelligent identifiers" s. oben bei Fn. 138 ff.

[244] S. dazu unten Fn. 623 und *Augot/Boucqueau/Delaigle/Fontaine/Goray*, 87 Proc. IEEE 1251, 1252 (1999).

[245] Zu SCMS s. unten Teil 1, D II 1.

[246] *Dittmann*, S. 43; *Nakamura/Ogawa/Takashima*, 11 NTT Review 124 (1999).

und der Nutzungsbedingungen basiert, wäre nicht mehr gewährleistet. Daher sollte es möglichst schwierig sein, die Metadaten von dem dazugehörenden digitalen Inhalt zu trennen.[247]

bb) Digitale Wasserzeichen

(1) **Allgemeines.** Dieses Ziel wird durch sogenannte „digitale Wasserzeichen" verfolgt. Damit können Informationen direkt in digitale Inhalte eingebettet werden.[248] Die eingebetteten Informationen verändern den Inhalt im allgemeinen nur in so geringem Maße, daß die Veränderungen für das menschliche Auge oder Gehör nicht wahrnehmbar sind. Durch digitale Wasserzeichen werden Metadaten derart mit dem digitalen Inhalt verwoben, daß ein einfaches Entfernen unmöglich ist, ohne den Inhalt selbst zu beschädigen.[249] Im folgenden sollen die technischen Grundlagen digitaler Wasserzeichen, der gegenwärtige Forschungsstand, ihre Anwendungsgebiete und ihre bestehenden Schwächen dargestellt werden.

Digitale Wasserzeichen stellen einen Teil eines größeren Forschungsgebiets dar, das mittlerweile unter dem Begriff „Information Hiding" firmiert und neben digitalen Wasserzeichen die sogenannte „Steganographie" umfaßt.[250] Im weitesten Sinne beschäftigt sich das „Information

[247] *Hill*, 87 Proc. IEEE 1228, 1232 f. (1999).

[248] Allgemeine Informationen zu digitalen Wasserzeichen geben *Katzenbeisser/Petitcolas* (Hrsg.); *Dittmann*; *Johnson/Duric/Jajodia*; *Langelaar/Setyawan/Lagendijk*, IEEE Signal Processing Magazine September 2000, 20 ff.; <http://www.watermarkingworld.org>; <http://www.cl.cam.ac.uk/~fapp2/watermarking>.

[249] *Dittmann*, S. 2.

[250] *Katzenbeisser/Petitcolas* (Hrsg.), S. XVII. Die Terminologie differiert jedoch erheblich. Teilweise werden auch Spread-Spectrum-Verfahren, anonyme Remailer und ähnliches zum Gebiet des „Information Hiding" gefaßt, s. *Petitcolas/Anderson/Kuhn*, 87 Proc. IEEE 1062 (1999). Die Begriffe „Steganographie" und „digitale Wasserzeichen" sind nicht deckungsgleich. Sie werden jedoch nicht immer trennscharf verwendet. Sowohl die Steganographie als auch digitale Wasserzeichen sind Verfahren, mit denen unbemerkt Informationen ausgetauscht werden können, indem die Informationen in eine andere, unauffällige Nachricht eingebettet wird, *Kutter/Hartung* in: Katzenbeisser/Petitcolas (Hrsg.), S. 97. Digitale Wasserzeichen wurden aber speziell zu dem Zweck entwickelt, Urheber- und Leistungsschutzrechte im digitalen Umfeld besser schützen zu können. Im Gegensatz zur Steganographie ist die Verheimlichung der Existenz einer geheimen Nachricht nicht das primäre Ziel digitaler Wasserzeichen, *Anderson/Petitcolas*, 16 IEEE Journal on Selected Areas in Communications 474, 475 f. (1998). Sie unterscheiden sich von steganographischen Verfahren dadurch, daß sie zusätzlich die Entfernung der Nachricht verhindern (sogenannte *Robustheit* und *Sicherheit*), *Petitcolas* in: Katzenbeisser/Petitcolas (Hrsg.), S. 1, 2; *Petitcolas/Anderson/Kuhn*, a. a. O., S. 1064; *Johnson/Duric/Jajodia*, S. 22. Dies hat die praktische Konsequenz, daß in digitalen Wasserzeichen in der Regel sehr viel weniger Informationen eingebettet werden können als mit Hilfe steganographischer Verfahren, *Kutter/Hartung*, a. a. O., S. 100. Grundsätzlich können digitale Wasserzeichen auch zu anderen Zwecken als dem Schutz von Urhebern eingesetzt werden. So existieren Wasserzeichenverfahren, die die Immaterialgüterrechte mehrerer Unternehmen schützen sollen, die bei der Entwicklung von bestimmten Computer-Chips (sog. „system chips") koopieren. Näher dazu *Torunoglu/Charbon*, 35 IEEE Journal of Solid-State Circuits 434 (2000).

Hiding" mit der unerkannten Kommunikation in unterschiedlichsten Ausprägungen.[251] Dieses interdisziplinäre Forschungsgebiet vereint Elemente aus den Bereichen der Elektrotechnik, der Signalverarbeitung, der Kommunikationstheorie und der Kryptologie. Es handelt sich um ein sehr junges und gleichzeitig äußerst dynamisches Forschungsgebiet. Die ersten wissenschaftlichen Aufsätze zu digitalen Wasserzeichen wurden Anfang der 90er Jahre veröffentlicht.[252] Seit Mitte der 90er Jahre nimmt die Publikationstätigkeit über digitale Wasserzeichen rasant zu.[253]

Alle Wasserzeichen-Verfahren bestehen aus einem Einbettungs- und einem Ausleseprozeß.[254] Das Wasserzeichen kann Daten jeglicher Art einbetten (Zahlen, Text, Bilder etc.). Dabei sollte ein Wasserzeichenverfahren grundsätzlich auch die Einbettung mehrerer Wasserzeichen in digitale Inhalte ermöglichen, um beispielsweise unterschiedliche Wasserzeichen für Informationen über den Urheber, ausübenden Künstler, Produzenten und Verleger oder auch den jeweiligen Nutzer[255] zu ermöglichen.[256] Die Metadaten können auch zunächst verschlüsselt und erst dann eingebettet werden. Dieses Vorgehen kann die Sicherheit des Systems insgesamt erhöhen, hat jedoch mit dem eigentlichen Wasserzeichenverfahren nichts zu tun. Vielmehr handelt es sich um eine Hintereinanderschaltung von Verschlüsselung und Wasserzeichenverfahren.[257]

(2) **Anforderungen an digitale Wasserzeichen.** Zwar unterscheiden sich viele Wasserzeichenverfahren im Detail, da sie für unterschiedliche Zwecke eingesetzt werden.[258] Dennoch lassen sich einige gemeinsame Anforderungen feststellen.

---

[251] Eine Einführung in dieses Gebiet bieten *Petitcolas/Anderson/Kuhn*, 87 Proc. IEEE 1062 ff. (1999) sowie ausführlich *Katzenbeisser/Petitcolas*; *Dittmann*; *Johnson/Duric/Jajodia*.

[252] Vgl. *Hartung/Kutter*, 87 Proc. IEEE 1079, 1080, 1085 f. (1999), m. w. N.

[253] Im Jahr 1998 wurden erstmals mehr als 100 wissenschaftliche Aufsätze über digitale Wasserzeichen publiziert, s. *Kutter/Hartung* in: Katzenbeisser/Petitcolas (Hrsg.), S. 97, 100. Eine kommentierte Bibliographie zum Forschungsgebiet „Information Hiding" von *Petitcolas* findet sich unter <http://www.cl.cam.uk/~fapp2/steganography/bibliography>.

[254] S. dazu *Dittmann*, S. 19 ff. Beim Auslesen des Wasserzeichens lassen sich die Verfahren in zwei Kategorien unterscheiden: Während die einen Verfahren nur feststellen können, ob ein bestimmtes Wasserzeichen in den digitalen Inhalt eingebettet ist („detectable watermark"), können die anderen Verfahren den Inhalt eines Wasserzeichens auslesen („readable watermark"); s. *Kutter/Hartung in: Katzenbeisser/Petitcolas* (Hrsg.), S. 108; *Bartolini/Bini/Cappeillini/Fringuelli/Meucci/Piva* in: Proceedings ICMCS 1999, Band 2, S. 199, 200.

[255] Zur Verwendung digitaler Wasserzeichen zur Nutzeridentifizierung s. unten Teil 1, C II 2 b.

[256] Solche Informationen lassen sich aber auch in einem gemeinsamen Wasserzeichen unterbringen.

[257] Vgl. *Furon/Duhamel* in: A. Pfitzmann (Hrsg.), S. 88, 90; *Aura* in: Anderson (Hrsg.), S. 265, 268.

[258] S. dazu *Dittmann*, S. 24 f., 32 f.

(a) **Fehlende Wahrnehmbarkeit.** Die Änderungen, die durch die Einbettung eines Wasserzeichens an dem digitalen Inhalt vorgenommen werden, müssen so gering sein, daß sie vom Menschen nicht wahrgenommen werden können (*fehlende Wahrnehmbarkeit*).[259] Dabei sind die menschlichen Hör- und Seheigenschaften zu berücksichtigen.[260] So reagiert das menschliche Auge bei Bildern auf Veränderungen in ruhigen Bildbereichen sehr viel sensibler als in unruhigen Bildbereichen.[261] Das Einbetten digitaler Wasserzeichen in Audiodaten ist grundsätzlich schwieriger als bei Bildern, da das menschliche Hörvermögen äußerst sensibel ist.[262] Auch erkennen professionelle Photographen Änderungen in einem Photo sehr viel besser als ein ungeschulter Laie.[263] Es muß daher beim Einsatz von Wasserzeichen immer auf die individuellen Einsatzbereiche geachtet werden. Je länger die einzubettenden Metadaten sind, desto schwieriger wird es, diese so einzubetten, daß der Inhalt nicht wahrnehmbar verändert wird. Das Einbetten einiger weniger Bits ist heute relativ einfach möglich.

(b) **Robustheit und Sicherheit.** Digitale Wasserzeichen müssen in DRM-Systemen robust und sicher sein. Da mit Hilfe digitaler Wasserzeichen digitale Inhalte mit Informationen über die Rechteinhaber und die Nutzungsbedingungen versehen werden sollen, sollte es für einen Angreifer idealiter unmöglich sein, diese Metadaten zu entfernen. Für den praktischen Einsatz in DRM-Systemen genügt es jedoch, daß es zumindest sehr schwer sein muß, die Metadaten zu entfernen, ohne gleichzeitig den digitalen Inhalt wahrnehmbar stark zu verändern *(Robustheit)*.[264] Insbesondere müssen

[259] *Kutter/Hartung* in: Katzenbeisser/Petitcolas (Hrsg.), S. 102; *Dittmann*, S. 26. Zwar existieren auch digitale Wasserzeichen, die sichtbar sind. So entwickelte IBM im Rahmen seines „Digital Libraries"-Projektes sichtbare Wasserzeichen für digitale Bilder, s. *Braudaway/Magerlein/Mintzer*, U.S. Patent No. 5530759 (1996); *Herrigel*, DuD 1998, 254, 255. Mit dieser sichtbaren Bildmarkierung soll unter anderem die gewerbliche Verwertung von Bildern verhindert werden, die im WWW veröffentlicht wurden, *Kutter/Hartung* in: Katzenbeisser/Petitcolas (Hrsg.), S. 100. Die Bibliothek des Vatikan greift seit 1995 auf die von IBM entwickelten sichtbaren digitalen Wasserzeichen zurück, *Gladney/Mintzer/Schiattarella*, 3 (7) D-Lib Magazine (Juli 1997). Aufgrund der vielfältigeren Einsatzmöglichkeiten liegt der Schwerpunkt der heutigen Forschung jedoch auf unsichtbaren Wasserzeichen, *Petitcolas/Anderson/Kuhn*, 87 Proc. IEEE 1062, 1064 (1999); *Herrigel*, DuD 1998, 254, 255.

[260] S. dazu *Wolfgang/Podilchuk/Delp*, 87 Proc. IEEE 1108 ff. (1999), und *Dugelay/Roche* in: Katzenbeisser/Petitcolas (Hrsg.), S. 121, 131 f.; *Dittmann*, S. 45 f.

[261] Um die fehlende Wahrnehmbarkeit zu erreichen, eignen sich daher unruhige Bildbereiche besser zur Einbettung digitaler Wasserzeichen, *Dugelay/Roche* in: Katzenbeisser/Petitcolas (Hrsg.), S. 121, 125. Ebenso können Wasserzeichen recht gut durch die Veränderung der Helligkeit einzelner Bildbereiche eingebettet werden, *Dittmann*, S. 45. Anderes gilt mitunter bei Videos, da sich hier Helligkeitsänderungen als Flackern bemerkbar machen können, s. *Dittmann*, S. 76.

[262] Vgl. *Johnson/Katzenbeisser* in: Katzenbeisser/Petitcolas (Hrsg.), S. 43, 61.

[263] *Kutter/Hartung* in: Katzenbeisser/Petitcolas (Hrsg.), S. 110.

[264] *Katzenbeisser* in: Katzenbeisser/Petitcolas (Hrsg.), S. 17, 32; vgl. *Dittmann*, S. 25. Die Begriffsdefinitionen differieren, s. *Petitcolas/Anderson/Kuhn*, 87 Proc. IEEE 1062, 1073 (1999).

eingebettete Metadaten auch nach Manipulationen der digitalen Inhalte, die notwendiger Bestandteil der Datenverarbeitung sind (zum Beispiel Kompression oder Formatkonvertierung), noch auslesbar sein.[265]

Ein Wasserzeichenalgorithmus ist *sicher*, wenn die eingebettete Information nicht zerstört, aufgespürt oder gefälscht werden kann, selbst wenn dem Angreifer das Einbettungs- und Ausleseverfahren bekannt ist. Auch wenn ihm die Existenz eines digitalen Wasserzeichens bekannt ist, sollte es für ihn möglichst schwer sein, das Wasserzeichen zu entfernen.[266] Eine Veränderung oder Entfernung des Wasserzeichens darf nur möglich sein, wenn damit gleichzeitig eine deutliche Qualitätsminderung des digitalen Inhalts verbunden ist.[267] Im Gegensatz zur Robustheit geht es bei der Sicherheit eines Wasserzeichenalgorithmus' um gezielte Angriffe auf das Wasserzeichen selbst.[268] Je größer die einzubettenden Metadaten sind, desto schwieriger wird es, diese robust und sicher einzubetten.

(3) Wasserzeichenverfahren

(a) Einbettungsverfahren. Digitale Wasserzeichen können auf unterschiedliche Arten in digitale Inhalte eingebettet werden. Ein Ansatz (sogenannte Bildraumverfahren, „spatial domain techniques") macht sich die Eigenschaft vieler digitaler Inhalte – unter anderem Bilder, Audio- und Videodaten – zu Nutzen, daß sie immer geringe Störungen enthalten, die bei der Aufnahme der Inhalte entstehen.[269] Dieses sogenannte „Rauschen" stört den Betrachter regelmäßig nicht. Digitale Wasserzeichen können in diese Rauschkomponenten eingebettet werden, ohne den Inhalt für einen Menschen wahrnehmbar zu verändern. Ein verbreitetes Einbettungsverfahren ist die Veränderung der sogenannten niederwertigsten Bits („least significant bits").[270] Dabei wird ein Charakteristikum des digitalen Inhalts – beispielsweise der Farbwert eines Bildpunktes oder die Lautstärke einer kurzen Musiksequenz – so geringfügig verändert, daß

[265] *Dittmann*, S. 25; *Matheson/Mitchell/Shamoon/Tarjan/Zane* in: Hirschfeld (Hrsg.), S. 226, 230.

[266] *Kutter/Hartung* in: Katzenbeisser/Petitcolas (Hrsg.), S. 100; *Dittmann*, S. 26.

[267] *Matheson/Mitchell/Shamoon/Tarjan/Zane* in: Hirschfeld (Hrsg.), Cryptography, S. 226, 230.

[268] *Dittmann*, S. 26; *Matheson/Mitchell/Shamoon/Tarjan/Zane* in: Hirschfeld (Hrsg.), S. 226, 230. Teilweise wird auch nicht zwischen Robustheit und Sicherheit unterschieden, sondern nur von der Robustheit eines Wasserzeichenverfahrens gesprochen.

[269] Technisch betrachtet entsteht dieses sogenannte „Rauschen" vor allem durch das thermische Rauschen von Halbleitern. S. allgemein *Katzenbeisser* in: Katzenbeisser/Petitcolas (Hrsg.), S. 28. Ein anschauliches Beispiel findet sich bei *Johnson/Duric/Jajodia*, S. 18.

[270] Digitale Daten werden in Computern im Binär-System verarbeitet. Dabei werden mehrere Bits zu einem Byte zusammengefaßt. Die binäre Zahl 01000110 entspricht z. B. der dezimalen Zahl 70. Bei einer Veränderung des niederwertigsten Bits wird die letzte Ziffer einer Binär-Zahl verändert (so wird z. B. 01000110 zu 01000111, dezimal betrachtet wird 70 zu 71).

dies für den menschlichen Betrachter nicht wahrnehmbar ist, von einem Computer aber ausgewertet werden kann.[271] Damit lassen sich nicht nur kurze Informationen einbetten. Es existieren Verfahren, mit denen sich ganze Bilder in einem anderen Bild verstecken lassen.[272]

Zumindest für digitale Wasserzeichen sind Bildraumverfahren aber relativ unsichere Verfahren.[273] Sie sind oft anfällig gegenüber verlustreichen Kompressionsverfahren[274] und anderen Signalverarbeitungsschritten. Es besteht ein Spannungsverhältnis zwischen der Robustheit eines Wasserzeichens, die für die Einbettung in den signifikanten Bereichen der digitalen Inhalte spricht,[275] und der notwendigen Unbemerkbarkeit des Wasserzeichens, die für die Einbettung in die am wenigsten signifikanten Bereiche der digitalen Inhalte spricht.[276]

Daher existieren Verfahren, bei denen das Wasserzeichen gerade in stark wahrnehmbare Bereiche eingebettet wird. Bei Bildern sind dies beispielsweise kontrastreiche Bereiche wie Kanten oder Linien. Das macht Wasserzeichen zwar resistenter gegen Kompressionsverfahren. Jedoch besteht nun die Gefahr, daß durch die Einbettung des Wasserzeichens wahrnehmbare Veränderungen am digitalen Inhalt entstehen (sogenannte „Artefakte").[277] Um solche Artefakte zu verhindern, versucht ein inwischen

---

[271] So sind im RGB-Farbmodell den einzelnen Punkten eines Bildes drei Werte zugeordnet, nämlich der Rot-, Grün- und Blau-Farbwert des Punktes. Wird bei einem dieser Farbwerte das niederwertigste Bit verändert, so bedeutet dies, daß der Rot-, Grün- bzw. Blau-Farbanteil des Bildpunktes geringfügig verändert wird. S. mit Beispiel *Johnson/Jajodia*, IEEE Computer Februar 1998, 26, 27 ff.; *Johnson/Duric/Jajodia*, S. 18 ff.

[272] Zum sog. „Image Downgrading" s. *Kurak/McHughes*, in: Proceedings of the Eighth IEEE Computer Security Applications Conference 1992, S. 153 ff.; *Johnson/Katzenbeisser* in: Katzenbeisser/Petitcolas (Hrsg.), S. 49; *Johnson/Duric/Jajodia*, S. 35, 37.

[273] *Johnson/Katzenbeisser* in: Katzenbeisser/Petitcolas (Hrsg.), S. 45; *Dittmann*, S. 49; *Johnson/Duric/Jajodia*, S. 21; *Breitbach/Imai* in: Franklin (Hrsg.), S. 125, 129; *Hartung/Kutter*, 87 Proc. IEEE 1079, 1092 (1999). Bildraumverfahren können dagegen für die Anforderungen steganographischer Kommunikation völlig ausreichen. Zur Steganographie s. oben Fn. 250.

[274] Solche Kompressionsverfahren, von denen nur MP3 im Musikbereich, JPEG im Bild- und MPEG im Videobereich genannt sein sollen, unterdrücken jene Informationen, die für das menschliche Auge oder Gehör nicht wahrnehmbar sind, um die zu übertragende Datenmenge zu reduzieren. Die unterdrückten Informationen sind aber oft gerade jene Rauschbereiche, in denen die dargestellten Verfahren das Wasserzeichen einbetten.

[275] Wird ein Wasserzeichen in wahrnehmbare, signifikante Bildbereiche eingebettet, so ist es weniger anfällig gegenüber verlustbehafteten Kompressionsverfahren u. ä.

[276] *Katzenbeisser* in: Katzenbeisser/Petitcolas (Hrsg.), S. 33; *Hartung/Kutter*, 87 Proc. IEEE 1079, 1082 (1999); *Anderson/Petitcolas*, 16 (4) IEEE Journal on Selected Areas in Communications 474, 476, 477 f. (1998); *Johnson/Jajodia*, IEEE Computer Februar 1998, 26, 28.

[277] Vgl. *Cox/Kilian/Leighton/Shamoon* in: Aucsmith (Hrsg.), S. 185, 187. Zu diesem Spannungsverhältnis zwischen Robustheit und Wahrnehmbarkeit eines Wasserzeichens s. auch unten Teil 1, C II 2 b bb 6.

weit verbreiteter Ansatz, das Wasserzeichen nicht an einer einzelnen Stelle des digitalen Inhalts einzubetten, sondern gleichsam über den gesamten Inhalt zu verteilen.[278] Dabei werden die digitalen Inhalte zunächst in eine andere Darstellungsform – den sogenannten Frequenzraum („frequency domain") – transformiert. Ein Bild wird bei der Darstellung im Frequenzraum nicht mehr als eine Ansammlung einzelner Bildpunkte dargestellt; vielmehr werden die Veränderungen beschrieben, die sich im Bild über größere Bereiche ergeben.[279] Es ist im vorliegenden Zusammenhang unmöglich, auf die komplexen Einzelheiten von Frequenzraum-Verfahren einzugehen.[280] Es ist aber ein Charakteristikum von Transformationen in den Frequenzraum, daß sie herausragende Charakteristika und Strukturen digitaler Inhalte gut abbilden. Wenn Wasserzeichen in diese heraus-

[278] Die Idee dazu stammt aus der militärischen Nachrichtenübermittlung und läßt sich bis in die 20er Jahre zurückverfolgen. Bei sog. „Bandspreizverfahren" („spread spectrum") wird ein (z. B. Funk-) Signal mit einer geringen Bandbreite in einem anderen Signal mit großer Bandbreite versteckt, indem das Erstere über das gesamte zweite breitbandige Signal verteilt oder „gespreizt" wird; dies gilt jedenfalls für „direct sequence spread spectrum"-Verfahren (im Gegensatz zu Verfahren, bei denen ein häufiger Wechsel der Sendefrequenz stattfindet). Zur Geschichte und den militärischen Einsatzmöglichkeiten von Bandspreizverfahren s. *Kahn*, 21 (9) IEEE Spectrum 70, 76 f. (1984); *Simon/Omura/Scholtz/Levitt*, S. 39ff. Außerhalb des militärischen Bereichs werden Bandspreizverfahren heute u. a. in der Satellitenkommunikation, beim Radar, beim Mobilfunk, bei drahtlosen LAN-Systemen sowie beim – auch in Fahrzeugnavigationssystemen verwendeten – „Global Positioning System" (GPS) eingesetzt. Grundsätzlich können die Gedanken von Bandspreizverfahren nicht nur bei Wasserzeichen verwendet werden, die im Frequenzraum operieren, sondern auch bei Wasserzeichen, die im Bildraum operieren: Die mehrmalige Einbettung eines Bildraum-Wasserzeichens führt faktisch auch dazu, daß das Wasserzeichen über den gesamten Inhalt „gespreizt" ist. S. zum ganzen *Johnson/Katzenbeisser* in: Katzenbeisser/Petitcolar (Hrsg.), S. 64; *Cox/Kilian/Leighton/Shamoon* in: Anderson (Hrsg.), S. 185 ff.; *Wayner*, Digital Copyright Protection, S. 148 ff.; *Peterson/Ziemer/Borth*; *Petitcolas/Anderson/Kuhn*, 87 Proc. IEEE 1062, 1067 (1999); *Hartung/Kutter*, 87 Proc. IEEE 1079, 1090 ff. (1999). Bandspreizverfahren sind auch unter juristischen Gesichtspunkten interessant. Sie erlauben, daß mehrere Personen gleichzeitig über den gleichen Frequenzbereich kommunizieren. Dadurch könnte die Notwendigkeit, die Frequenzbereiche jeweils bestimmten Personen zur Nutzung zuzuteilen (s. §§ 44 ff. TKG), entfallen. S. dazu ausführlich *Benkler*, 11 Harv. J. L. & Tech. 287 ff., 323 ff. (1998), und *Lessig*, S. 184 f.

[279] Für die Transformation vom Bildraum in den Frequenzraum steht eine Vielzahl mathematischer Funktionen zur Verfügung, u. a. die diskrete Kosinus-, Fourier-, Mellin-Fourier und die diskrete Wavelet-Transformation. Im Frequenzraum wird ein unruhiger Bildbereich mit anderen Koeffizienten beschrieben als ein ruhiger Bildbereich, *Taylor*, DVD Demystified, S. 94. Bekannteste Anwendungsbeispiele einer diskreten Kosinustransformation sind der Bild-Kompressionsstandard JPEG (s. dazu *Wayner*, Digital Copyright Protection, S. 51 ff.; *Johnson/Katzenbeisser* in: Katzenbeisser/Petitcolas (Hrsg.), S. 57 f.) und der Bewegtbild-Kompressionsstandard MPEG (s. dazu *Pohlmann*, S. 573 ff.). Eine Aufzählung von Wasserzeichenverfahren, die sich Frequenzraumverfahren bedienen, findet sich bei *Dittmann*, S. 46 ff.

[280] S. dazu *Wayner*, Digital Copyright Protection, S. 52 ff., 147 ff.; *Dugelay/Roche* in: Katzenbeisser/Petitcolas (Hrsg.), S. 123 ff.; *Dittmann*, S. 22, 44; *Johnson/Duric/Jajodia*, S. 27 ff.

ragenden Strukturen eingebettet werden, macht sie dies vergleichbar robust.[281] Viele Wasserzeichenverfahren, die im Frequenzraum operieren, können verlustreiche Kompressionsverfahren und Bildbearbeitung überstehen.[282] Selbst wenn Teile des Datenmaterials verändert werden, sind regelmäßig noch genügend Informationen in anderen Teilen des Datenmaterials vorhanden, um das Wasserzeichen zu rekonstruieren.[283] Dennoch sind die Veränderungen am Inhalt für den Betrachter nicht erkennbar.[284]

(**b**) **Einbettungsort.** In einem DRM-System muß es für einen Angreifer möglichst schwierig sein, digitale Wasserzeichen zu entfernen oder zu verändern. Um einen solchen Angriff zu verhindern, könnte der DRM-Betreiber versuchen, das Verfahren geheim zu halten, mit dem das digitale Wasserzeichen ausgelesen und überschrieben werden kann. Es ist jedoch eine der grundlegenden Maximen der Kryptographie, daß die Sicherheit eines Verschlüsselungsverfahrens nicht auf der Geheimhaltung des kryptographischen Algorithmus', sondern nur des verwendeten Schlüssels beruhen darf (sogenanntes „*Kerckhoff*"-Prinzip).[285] Auch bei digitalen Wasserzeichen muß davon ausgegangen werden, daß dem Angreifer das Einbettungs- und Ausleseverfahren bekannt ist.[286]

Die Sicherheit eines Wasserzeichenverfahrens muß auf anderem Weg gewährleistet werden. Dafür ist zu beachten, daß ein denkbarer Angriff auf ein Wasserzeichen darin besteht, die genaue Position des Wasserzeichens zu bestimmen, an der das Wasserzeichen in den digitalen Inhalt eingebettet wurde, dann das Wasserzeichen an dieser Stelle zu überschreiben und dadurch unbrauchbar zu machen.[287] Die Sicherheit eines Was-

---

[281] *Johnson/Katzenbeisser* in: Katzenbeisser/Petitcolas (Hrsg.), S. 56; *Cox/Kilian/Leighton/Shamoon* in: Anderson (Hrsg.), S. 185, 190 f.; *Johnson/Katzenbeisser* in: Katzenbeisser/Petitcolas (Hrsg.), S. 56, 66. Für Bilder ohne viele Grauwerte – wie insbesondere gedruckten Text – sind sie jedoch weniger geeignet, *s. Low/Maxemchuk*, 16 IEEE Journal on Selected Areas in Communications 561, 562 (1998).

[282] *Johnson/Katzenbeisser* in: Katzenbeisser/Petitcolas (Hrsg.), S. 56 f.; *Petitcolas/Anderson/Kuhn*, 87 Proc. IEEE 1062, 1067 f. (1999); *Cox/Kilian/Leighton/Shamoon* in: Anderson (Hrsg.), S. 185, 197 ff.

[283] *Johnson/Katzenbeisser* in: Katzenbeisser/Petitcolas (Hrsg.), S. 64.

[284] *Johnson/Katzenbeisser* in: Katzenbeisser/Petitcolas (Hrsg.), S. 56; *Cox/Kilian/Leighton/Shamoon* in: Anderson (Hrsg.), S. 185, 190.

[285] Grundsätzlich muß davon ausgegangen werden, daß dem Gegner der Algorithmus bekannt ist. Zum „*Kerckhoff*"-Prinzip s. *Bauer*, S. 207; *Petitcolas/Anderson/Kuhn*, 87 Proc. IEEE 1062, 1065 (1999); *Rankl/Effing*, S. 147 f.

[286] *Katzenbeisser* in: Katzenbeisser/Petitcolas (Hrsg.), S. 2S. 22; *Hartung/Kutter*, 87 Proc. IEEE 1079, 1080 (1999); *Langelaar/Setyawan/Lagendijk*, IEEE Signal Processing Magazine September 2000, 20, 22. Auch kann eine unabhängige Fachöffentlichkeit die Sicherheit eines Wasserzeichenverfahrens nur überprüfen, wenn das zugrundeliegende Verfahren bekannt ist, s. *Craver/Perrig/Petitcolas* in: Katzenbeisser/Petitcolas (Hrsg.), S. 149, 155; *Dittmann*, S. 19 f.

[287] Ohne diese Kenntnis muß der Angreifer regelmäßig größere Bereiche des Datenmaterials überschreiben, was insgesamt zu einer deutlichen Qualitätsminderung des

serzeichenverfahrens kann daher erhöht werden, wenn der genaue Einbettungsort des Wasserzeichens geheim gehalten wird. Zu diesem Zweck werden bei der Einbettung des Wasserzeichens regelmäßig ein oder mehrere Schlüssel verwendet, die die exakte Position bestimmen, an denen das Wasserzeichen eingebettet wird.[288] Bei diesem verbreiteten Ansatz ist es für einen Angreifer sehr schwer, das Wasserzeichen zu entdecken, auszulesen oder zu löschen, solange er nicht den geheimen Schlüssel kennt.[289]

Inhalts führen wird, *Matheson/Mitchell/Shamoon/Tarjan/Zane* in: Hirschfeld (Hrsg.), S. 226, 230.

[288] Damit dies an keiner statistisch auffälligen Stelle geschieht, werden zunächst aus diesem geheimen Schlüssel Zufallszahlen errechnet. Ansonsten könnte ein Angreifer durch den statistischen Vergleich mehrerer markierter Inhalte die Position der Wasserzeichen zu bestimmen versuchen, *Aura* in: Anderson (Hrsg.), S. 265, 269. Diese Zufallszahlen bestimmen die Stellen, an denen tatsächlich das Wasserzeichen eingefügt wird. Sie werden von einem sogenannten „Pseudozufallszahlengenerator" ermittelt. Dieser expandiert einen vergleichsweise kurzen Startwert (nämlich den geheimen Schlüssel) in eine längere Folge von Pseudozufallszahlen. Es handelt sich jedoch um keine echten Zufallszahlen, da sie mit Hilfe eines streng deterministischen Algorithmus berechnet wurden und damit bei Kenntnis des Algorithmus und seiner Eingangswerte auch vorhersagbar sind. Das Wasserzeichen wird nun an den Positionen eingebettet, welche durch die Pseudozufallszahlen festgelegt wurden. Dadurch läßt sich die Verteilung des Wasserzeichens über den digitalen Inhalt für einen Angreifer nicht von einem zufällig verteilten Rauschen unterscheiden. Will ein Berechtigter das Wasserzeichen auslesen, so muß er den geheimen Schlüssel kennen. Aus diesem berechnet er dann mit Hilfe des gleichen (deterministischen!) Pseudozufallsgenerators die Stellen, an denen das Wasserzeichen eingefügt wurde. Dann kann er es auslesen. Vgl. dazu *Dugelay/Roche* in: Katzenbeisser/Petitcolas (Hrsg.), S. 123; *Dittmann*, S. 22 f.; *Aura* in: Anderson (Hrsg.), S. 265, 271 f. Zu Pseudozufallsgeneratoren s. *Selke*, S. 167 f.; *Schneier*, S. 44 ff., 369 ff.

[289] Oftmals ist es in einem DRM-System jedoch notwendig, daß das Endgerät beim Nutzer das Wasserzeichen auslesen kann, um Informationen über den Rechteinhaber und die Nutzungsbedingungen zu erhalten. Wenn der geheime Schlüssel zu diesem Zweck ungeschützt im Endgerät gespeichert ist, könnte ein Angreifer den Schlüssel auslesen und damit Wasserzeichen verändern und überschreiben. Für dieses Problem existieren mehrere Lösungsmöglichkeiten. Eine Lösung ist, den geheimen Schlüssel beim Nutzer in manipulationssicherer Hard- oder Software zu speichern, s. dazu unten Teil 1, C IV; *Furon/Duhamel* in: Pfitzmann (Hrsg.), S. 89. Bei einer anderen Lösung wird der Ausleseprozeß des Wasserzeichens bei einer vertrauenswürdigen Instanz im Internet zentralisiert, *Petitcolas/Anderson/Kuhn*, 87 Proc. IEEE 1062, 1072 (1999). Die dritte Lösung liegt in der Entwicklung „asymmetrischer" Wasserzeichenverfahren. Dafür ist zu beachten, daß sich das angesprochene Problem auch beim Einsatz symmetrischer Verschlüsselungsverfahren bei der digitalen Signatur stellen würde: Würde der Absender ein Dokument mit einem Signaturverfahren unterschreiben, das auf einem symmetrischen Verschlüsselungsverfahren beruht, so würde auch der Empfänger den symmetrischen Schlüssel kennen und könnte dadurch die Signatur ändern und fälschen. Dieses Problem wird bei digitalen Signaturen gelöst, indem asymmetrische Verschlüsselungsverfahren eingesetzt werden, bei denen zum Ver- und Entschlüsseln unterschiedliche Schlüssel verwendet werden. Bei asymmetrischen Wasserzeichenverfahren wird beim Einbetten ein „privater" Schlüssel verwendet, der nur dem Einbettenden bekannt ist. Das Endgerät des Nutzers kann das Wasserzeichen mit einem allgemein bekannten „öffentlichen" Schlüssel auslesen. Mit diesem Schlüssel kann das Wasserzeichen aber nicht verändert, gelöscht oder überschrieben werden. Die Übertragung des aus der

Zwar existieren auch andere Angriffsmethoden, bei denen eine Kenntnis des genauen Einbettungsorts des Wasserzeichens nicht notwendig ist.[290] Dennoch wird die Sicherheit eines Wasserzeichenverfahrens durch die Verwendung geheimer Schlüssel merklich erhöht.

(4) **Mögliche Angriffspunkte bei digitalen Wasserzeichen.** Wie die bisherigen Ausführungen zeigen, sind digitale Wasserzeichen komplexe technische Verfahren, an die hohe Anforderungen gestellt werden, sollen sie in DRM-Systemen Verwendung finden. Heutige Wasserzeichenverfahren verfügen oftmals noch nicht über die notwendige Sicherheit gegenüber gezielten Angriffen. Wie ihre Sicherheit erhöht werden kann, ist Gegenstand der sogenannten „Stegoanalyse". Sie ist – wie die Kryptoanalyse im Bereich der Kryptographie – notwendiger Bestandteil bei der Entwicklung neuer und sicherer Verfahren.[291] Es sind unzählige Angriffe auf digitale Wasserzeichen denkbar. Bei Bildern oder Videos sind dies unter anderem das Schärfen des Bildes, Farb- und Kontrastveränderungen, das Hinzufügen von Rauschen, das Komprimieren, Rotieren, Skalieren, das Ab- und Ausschneiden von Datenbereichen, das Überspringen oder Hinzufügen von Datenbereichen (zum Beispiel von Zeilen und Spalten im Bild), das Verzerren oder Dehnen, das Aufteilen in mehrere Teilbilder,[292] das Kon-

Kryptographie stammenden Gedankens asymmetrischer Verfahren auf digitale Wasserzeichen erweist sich aus vielen Gründen als sehr schwierig, s. *Furon/Duhamel* in: A. Pfitzmann (Hrsg.), S. 90; *Dittmann*, S. 150; *Cox/Linnartz*, 16 IEEE Journal on Selected Areas in Communications 587 (1998). Insgesamt ist der Ansatz asymmetrischer Wasserzeichenverfahren noch recht neu; ein sicheres und einsetzbares Verfahren existiert heute nicht. Es ist ungeklärt, ob ein solches Verfahren überhaupt existieren kann. Das gesamte Problem wird mitunter als das „holy grail of watermarking" bezeichnet, s. *Craver/Perrig/Petitcolas* in: Katzenbeisser/Petitcolas (Hrsg.), S. 169 Fn. 2. Asymmetrische Wasserzeichenverfahren wurden u. a. vorgeschlagen von *Hartung/Girod* in: Proceedings ICIP 1997, Band 1, S. 528 ff.; *Furon/Duhamel* in: Pfitzmann (Hrsg.), S. 88 ff.; *Dittmann*, S. 150. Die Terminologie ist mintunter verwirrend. So wird einerseits zwischen „private key" (bzw. symmetrischen) und „public key" (bzw. asymmetrischen) Wasserzeichenverfahren unterschieden, wobei das Unterscheidungskriterium ist, ob zum Einbettungs- und Ausleseprozeß der gleiche Schlüssel verwendet wird oder nicht. Andererseits wird zwischen „private" (bzw. „nicht-blinden" oder „non-oblivious") und „public" (bzw. „blinden" oder „oblivious") Wasserzeichenverfahren unterschieden, wobei hier das Unterscheidungskriterium ist, ob zum Auslesen des eingebetteten Wasserzeichens der originale digitale Inhalt und das Original-Wasserzeichen zur Verfügung stehen müssen oder nicht. S. dazu *Kutter/Hartung* in: Katzenbeisser/Petitcolas (Hrsg.), S. 103, 105; *Petitcolas/Anderson/Kuhn*, 87 Proc. IEEE 1062, 1064 (1999).

[290] Schon die bloße verlustbehaftete Kompression kann Wasserzeichen entfernen, ohne daß der Angreifer irgendwelche Informationen über das Wasserzeichen haben muß; s. dazu auch sogleich im Text.

[291] *Johnson* in: Katzenbeisser/Petitcolas (Hrsg.), S. 80; s. a. *Craver/Perrig/Petitcolas* in: Katzenbeisser/Petitcolas (Hrsg.), S. 149 ff.; *Johnson/Duric/Jajodia*, S. 47 ff.

[292] Diese sog. „Mosaik-Attacke" nützt die Tatsache aus, daß in besonders kleinen Bildern keine Wasserzeichen eingebettet und/oder ausgelesen werden können. Bei der Mosaik-Attacke unterteilt der Angreifer das mit einem Wasserzeichen markierte Bild, das er unberechtigt auf seiner Webseite anbieten will, in mehrere Teilbilder. Wenn die

vertieren in andere Dateiformate, die Digital-Analog-Wandlung (zum Beispiel Ausdrucken eines Bildes mit nachfolgendem Einscannen, Abfilmen vom Fernsehbildschirm), das Drehen eines Bildes um wenige Grad, das Einfügen mehrerer Wasserzeichen,[293] das Vertauschen der Reihenfolge von Einzelbildern bei Videos sowie eine Kombination der aufgezählten Attacken.[294] Grundsätzlich sind Wasserzeichensysteme, die im Bildraum operieren, anfälliger gegenüber einer Kompression, während Wasserzeichensysteme, die im Frequenzraum operieren, anfälliger gegenüber geometrischen Veränderungen (Rotation, Skalierung, Verzerrung) und Tiefpaßfiltern sind.[295]

Mit StirMark[296] und unZign[297] existieren spezielle Programme, die die Sicherheit digitaler Wasserzeichen überprüfen, indem sie versuchen, das Wasserzeichen zu entfernen oder wenigstens unbrauchbar zu machen. Bei StirMark wird ein Bild, das mit einem Wasserzeichen markiert wurde, in geringem Umfang gedehnt, gekrümmt und gedreht.

Abbildung 3[298] (S. 64) zeigt die Anwendung von StirMark an einem mit einem Wasserzeichen versehenen Bild sowie – zur Veranschaulichung der Funktionsweise von StirMark – an einem Gitternetz. Die Qualität des Bildes wird durch StirMark nicht oder kaum wahrnehmbar verschlechtert. Nach Anwendung von StirMark kann das eingebette Wasserzeichen nicht mehr entdeckt oder ausgelesen werden.[299] Die mei-

Teilbilder auf der Webseite direkt nebeneinander dargestellt werden, ist für den Betrachter der Unterschied zwischen dem einheitlichen und dem zusammengesetzten Bild nicht wahrnehmbar. Durch eine solche Aufteilung sind jedoch die in das Gesamtbild eingebettete Wasserzeichen nicht mehr lesbar, wenn die einzelnen Teilbilder zu klein sind, als daß noch das Wasserzeichen aus dem Teilbild ausgelesen werden könnte. S. dazu *Craver/Perrig/Petitcolas* in: Katzenbeisser/Petitcolas (Hrsg.), S. 157 f.; *Dittmann*, S. 35 f.; *Petitcolas/Anderson/Kuhn*, 87 Proc. IEEE 1062, 1071 (1999).

[293] S. dazu *Craver/Perrig/Petitcolas* in: Katzenbeisser/Petitcolas (Hrsg.), S. 151 f.

[294] Vgl. dazu insgesamt *Craver/Perrig/Petitcolas* in: Katzenbeisser/Petitcolas (Hrsg.), S. 149 ff.; *Kutter/Hartung* in: Katzenbeisser/Petitcolas (Hrsg.), S. 107; *Hartung/Kutter*, 87 Proc. IEEE 1079, 1099 ff. (1999); *Petitcolas/Anderson/Kuhn* in: Aucsmith (Hrsg.), S. 218 ff.; *Dugelay/Roche* in: Katzenbeisser/Petitcolas (Hrsg.), S. 144; *Dittmann*, S. 25, 33 ff.; *Johnson/Duric/Jajodia*, S. 47 ff.; *Petitcolas/Anderson* in: Proceedings ICMCS 1999, Band 1, S. 574, 577. Bei anderen Datenmaterialien (Audio, Text, Video) existiert eine ähnliche Vielzahl möglicher Attacken; s. dazu bei Audiodaten *Craver/Perrig/Petitcolas* in: Katzenbeisser/Petitcolas (Hrsg.), S. 149; *Dittmann*, S. 89. Zu sonstigen nichttechnischen Angriffspunkten s. *Craver/Perrig/Petitcolas* in: Katzenbeisser/Petitcolas (Hrsg.), S. 166 ff.

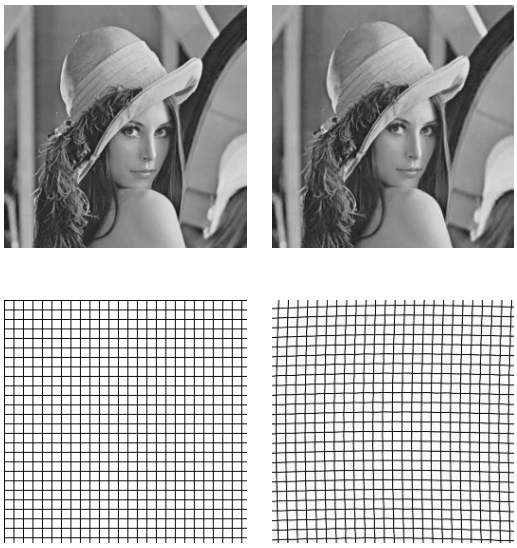
[295] *Dittmann*, S. 53; *Petitcolas/Anderson/Kuhn*, 87 Proc. IEEE 1062, 1069 (1999).

[296] Von *Petitcolas* und *Kuhn* entwickelt, erhältlich unter <http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark>.

[297] Erhältlich unter <http://www.cl.cam.ac.uk/~fapp2/watermarking/image_watermarking/unzign>; s. dazu *Hartung/Kutter*, 87 Proc. IEEE 1079, 1102 (1999).

[298] Das Bildmaterial stammt von der Web-Seite von *Fabien A. Petitcolas* unter <http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/samples2.html>.

[299] Das Wasserzeichen wird zwar nicht aus dem Bild entfernt. Durch die Manipulationen von StirMark geht jedoch die Synchronisation zwischen Einbettungs- und Aus-



(a): Original-Bild mit Wasserzeichen

(b): Bild nach StirMark-Angriff

Abbildung 3: StirMark-Angriff auf markiertes Bild

sten der heute verfügbaren Verfahren sind gegenüber StirMark nicht resistent.[300]

Daneben existieren Angriffe, die das Wasserzeichen selbst nicht verändern, aber dennoch seinen Wert als Identifizierungsmittel vernichten. Will sich ein Angreifer fälschlicherweise als Urheber eines digitalen Inhalts gerieren, so könnte er in den Inhalt, der schon vom wahren Urheber mit einem Wasserzeichen ausgestattet wurde, ein zweites Wasserzeichen einbetten, das den Angreifer als Urheber ausgibt. Kommt es zum Streit über die Urheberschaft, wird der wahre Urheber regelmäßig eine Fassung des digitalen Inhalts vorlegen können, in der gar kein Wasserzeichen eingebettet ist. Dadurch läßt sich der wahre Urheber vom Angreifer unterscheiden. Jedoch ist es unter gewissen Umständen möglich, daß der Angreifer vorspiegelt, in der tatsächlich wasserzeichenfreien Version, die der Urhe-

leseprozeß verloren. Dadurch wird es unmöglich, die genauen Punkte zu lokalisieren, an denen das Wasserzeichen eingebettet wurde (sog. „distortion attack"). Da StirMark bei der Berechnung der Manipulation Zufallsparameter verwendet, läßt sich die exakte Manipulation durch StirMark nicht vorherberechnen und daher sehr schwer im Entwurf eines Wasserzeichenverfahrens berücksichtigen, s. *Craver/Perrig/Petitcolas* in: Katzenbeisser/Petitcolas (Hrsg.), S. 156.

[300] Zur Funktionsweise von StirMark s. näher *Petitcolas/Anderson/Kuhn* in: Aucsmith (Hrsg.), S. 224 ff.; *Petitcolas/Anderson/Kuhn*, 87 Proc. IEEE 1062, 1069 (1999).

ber vorlegt, sei das Wasserzeichen des Angreifers enthalten.[301] Es ist dann unmöglich zu beweisen, welche Partei zuerst ihre Wasserzeichen in den digitalen Inhalt eingebettet hat.[302] Mit den gleichen Angriffsverfahren kann ein Angreifer auch vortäuschen, daß ein tatsächlich unmarkiertes Objekt von ihm mit einem Wasserzeichen markiert worden ist. Er kann also beispielweise die Urheberschaft an urheberrechtlich ungeschützten Inhalten vortäuschen.[303]

(5) **Anwendungsbeispiele.** Der bisherige Forschungsschwerpunkt liegt auf der Entwicklung digitaler Wasserzeichen für Bilder.[304] Derzeit können Wasserzeichenverfahren bei Bildern regelmäßig nur einige bis ein paar Dutzend Bits an Informationen aufnehmen.[305] Die meisten Systeme sind gegenüber komplexen Angriffen nicht resistent.[306] Aber auch für eine Vielzahl anderer Medien werden Wasserzeichenverfahren entwickelt. Heutige Wasserzeichenverfahren für Videodaten sind regelmäßig relativ robust gegen Kompressionen, haben aber Probleme bei geometrischen

[301] Dies ist durch die Subtraktion eines beliebigen Wasserzeichens von den Ausgangsdaten möglich; s. zu den Einzelheiten *Craver/Memon/Yeo/Yeung*, 16 IEEE Journal on Selected Areas in Communications 573, 576 ff. (1998); *Craver/Perrig/Petitcolas* in: Katzenbeisser/Petitcolas (Hrsg.), S. 160 ff.; *Dittmann*, S. 37; *Zeng/Liu*, 8 IEEE Transactions on Image Processing, 1534, 1535 f. (1999); *Hartung/Kutter*, 87 Proc. IEEE 1079, 1101 (1999).

[302] Für dieses Problem bestehen jedoch Lösungsansätze. So können Zeitstempel in das Wasserzeichen integriert werden, die die Priorität einer Wasserzeichen-Einbettung beweisen. Dabei kann der Rechteinhaber den digitalen Inhalt bei einer zentralen Instanz registrieren lassen, die ihm dann zu Beweiszwecken bestätigt, daß und zu welchem Zeitpunkt er die Registrierung vorgenommen hat, vgl. *Petitcolas/Anderson/Kuhn*, 87 Proc. IEEE 1062, 1071 (1999); *Dittmann*, S. 38 m. w. N.; *Zeng/Liu*, 8 IEEE Transactions on Image Processing 1534, 1536 (1999); *Hartung/Kutter*, 87 Proc. IEEE 1079, 1101 (1999). Beispielhaft für einen solchen Dienst sei das U.S.-amerikanische Unternehmen Surety.com, Inc., genannt, s. <http://www.surety.com>; Informationen zu weiteren Diensten bei <http://www.lockmydoc.com/drm/stamp.html>; zu den technischen Grundlagen s. *Adams/Cain/Pinkas/Zuccherato*. Die beste Lösung ist jedoch, durch ein spezielles Design des Wasserzeichenverfahrens zu verhindern, daß es zu einer solchen Situation überhaupt kommt. Dabei wird es (vereinfacht dargestellt) dem Angreifer durch den Einsatz von Einweg-Wasserzeichenverfahren gleichsam unmöglich gemacht, von den Ausgangsdaten ein Wasserzeichen zu subtrahieren; s. dazu *Craver/Memon/Yeo/Yeung*, 16 IEEE Journal on Selected Areas in Communications 573, 579 ff. (1998); *Craver/Perrig/Petitcolas* in: Katzenbeisser/Petitcolas (Hrsg.), S. 162 m. w. N.; *Hartung/Kutter*, 87 Proc. IEEE 1079, 1101 f. (1999).

[303] Dieser Angriff geschieht wiederum, in dem vom (unmarkierten) Datenobjekt ein vermeintliches, beliebiges Wasserzeichen subtrahiert wird. Dadurch kann der Angreifer vorspiegeln, in dem (unmarkierten) Datenobjekt sei sein Wasserzeichen enthalten. Hier gibt es bisher keine befriedigenden Lösungen; vgl. *Craver/Memon/Yeo/Yeung*, 16 IEEE Journal on Selected Areas in Communications, 573, 586 (1998).

[304] *Hartung/Kutter*, 87 Proc. IEEE 1079, 1084 (1999).

[305] *Dittmann*, S. 43, 52. Die genaue Zahl ist von der Bildgröße und den Verfahrensparametern abhängig.

[306] S. *Petitcolas/Anderson* in: Proceedings ICMCS 1999, Band 1, S. 574 ff.

Veränderungen.[307] Sie können meist nur einige Bits pro Einzelbild unterbringen.[308] Im Audiobereich existieren mehrere kommerzielle Wasserzeichenprodukte. Da die verwendeten Verfahren jedoch in der Regel nicht veröffentlicht werden, kann deren Sicherheit nicht beurteilt werden.[309] Weiterhin existieren Verfahren, mit denen Wasserzeichen in dreidimensionalen Modellen untergebracht werden können, die beispielsweise mit der „Virtual Reality Modeling Language" (VRML)[310] erstellt wurden.[311] Auch werden Wasserzeichenverfahren für gedruckte Musiknoten entwickelt.[312] Schließlich existieren Verfahren für gedruckten Text. Dabei kann der Abstand zwischen einzelnen Zeilen oder Wörtern geringfügig geändert werden, ohne daß dies dem Betrachter auffällt (sogenanntes „line-space" beziehungsweise „word-space encoding"). In diesen Abstandsveränderungen können Informationen abgespeichert werden (siehe Abbildung 4).

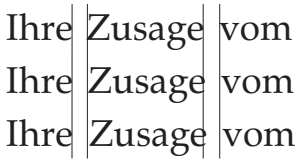


Abbildung 4: „word-space encoding"

Diese Verfahren sind im Idealfall gegenüber der Erstellung von Kopien, dem Ausdrucken mit nachfolgendem Einscannen, der Übertragung per Fax sowie Vergrößerungen und Verkleinerungen resistent. Gegen ein Abtippen des Textes helfen sie jedoch nicht.[313] Für Dokumente wie Zeit-

[307] *Dittmann*, S. 78.

[308] *Dittmann*, S. 78. Einen Überblick über den Stand der Technik geben *Dittmann*, S. 77 f.; *Hartung/Kutter*, 87 Proc. IEEE 1079, 1093 ff. (1999). Im Rahmen des von der Europäischen Union unterstützten „Tracing Authors' Rights by Labeling Image Services and Monitoring Access Network (TALISMAN)"-Projekts (ACTS-Projekt AC109, 1995–1998) wurden Wasserzeichenverfahren für Videos entwickelt, s. <http://www.cordis.lu/esprit/src/talisman.htm>.

[309] Vgl. *Dittmann*, S. 89 ff.

[310] S. dazu das „Web 3D Consortium" unter <http://www.vrml.org>.

[311] Einen Überblick über den Stand der Technik geben *Dittmann*, S. 102 ff.; *Hartung/Kutter*, 87 Proc. IEEE 1079, 1098 (1999). S. a. *Ohbuchi/Masuda/Aono*, 16 IEEE Journal on Selected Areas in Communications 551 ff. (1998).

[312] Die Entwicklung findet am Fraunhofer-Institut für Graphische Datenverarbeitung in Darmstadt im Rahmen des „Wedelmusic"-Projektes statt, s. <http://www.wedelmusic.org>.

[313] Dies kann auch mit Hilfe von Texterkennungssoftware (sog. OCR-Software) automatisiert werden. S. *Low/Maxemchuk*, 16 IEEE Journal on Selected Areas in Communications 561, 562 (1998); *Brassil/Low/Maxemchuk*, 87 Proc. IEEE 1181, 1190 (1999).

schriften- oder Zeitungsaufsätze, bei denen ein relativ geringes Schutzniveau ausreicht, sind solche Systeme jedoch durchaus interessant.[314]

Auch für Computerprogramme werden Wasserzeichenverfahren entwickelt.[315] Dabei treten spezielle Probleme auf, auf die hier nicht näher eingegangen werden kann.[316] Insgesamt handelt es sich bei digitalen Wasserzeichen für Computerprogramme um ein sehr junges Forschungsgebiet, auf dem bisher nur vereinzelt systematisch gearbeitet wurde.[317]

(6) Bewertung

Of course, no watermarking system can be made perfect.[318]

Trotz der geradezu stürmischen Forschungsanstrengungen in den letzten Jahren ist bei digitalen Wasserzeichen noch vieles offen. Die theoretischen Grundlagen sind noch nicht vollständig entwickelt, viele Fragen über den besten Implementierungsweg noch ungeklärt.[319] Bis heute wurde kein vollständig robustes und sicheres Wasserzeichen-Verfahren entwickelt. Auch ist zweifelhaft, ob ein solches Verfahren überhaupt existieren kann.[320] Von

---

[314] Vgl. *Brassil/Low/Maxemchuk*, 87 Proc. IEEE 1181, 1190 (1999).

[315] Jedoch ist die Anzahl der Veröffentlichungen zu diesem Thema viel geringer als zu Wasserzeichenverfahren für sonstige digitale Inhalte.

[316] Die herkömmlichen Wasserzeichenverfahren beruhen grundsätzlich auf der Einbettung von Daten in die Rauschkomponente digitaler Daten. Computerprogramme enthalten jedoch kein solches Rauschen, s. *Pieprzyk* in: Mambo/Zheng (Hrsg.), S. 178, 179. Dennoch werden für Computerprogramme Verfahren entwickelt, die digitalen Wasserzeichen für andere Medien vergleichbar sind. Einige Ansätze verändern die Anordnung von Teilen des Softwarecodes, ohne dabei die Funktionalität des Programms zu verändern. In der gezielten Änderung können Informationen gespeichert werden. Microsoft hat ein solches Verfahren patentiert, das vornehmlich für digitale Fingerabdrücke eingesetzt werden kann, s. *Davidson/Myhrvold*, U.S. Patent No. 5559884 (1996). IBM hat schon in den 80er Jahren ähnliche Schutzmechanismen in Gerichtsverfahren als Beweis für Urheberrechtsverletzungen vorgebracht (so zumindest der Bericht über ein Verfahren in Großbritannien bei *Collberg/Thomborson* in: Proceedings of POPL 1999, S. 311, 314). Weiterhin werden sog. dynamische Wasserzeichen entwickelt, die erst während der Programmausführung erzeugt werden und im Quellcode nur schwer zu entdecken sind. S. zum ganzen *Collberg/Thomborson* in: Proceedings of POPL 1999, S. 311 ff.; *Pieprzyk* in: Mambo/Zheng (Hrsg.), S. 178 ff. (mit Ausführungen zu Angriffsmöglichkeiten).

[317] Eine der ersten wissenschaftlichen Publikationen zu diesem Thema ist *Collberg/Thomborson* in: Proceedings of POPL 1999, S. 311 ff. Ein darauf aufbauendes Programm, das Wasserzeichen in Java-Programme einbettet, ist Sandmark, s. <http://www.cs.arizona.edu/sandmark>.

[318] *Cox/Kilian/Leighton/Shamoon* in: Aucsmith (Hrsg.), S. 185, 187. S. a. *Ergun/Kilian/Kumar* in: Stern (Hrsg.), S. 140, 141 („We know of no […] watermarking scheme that has survived a serious attack").

[319] Vgl. *Kutter/Hartung* in: Katzenbeisser/Petitcolas (Hrsg.), S. 118; *Hartung/Kutter*, 87 Proc. IEEE 1079, 1102 (1999); *Petitcolas/Anderson/Kuhn*, 87 Proc. IEEE 1062, 1072 (1999).

[320] *Petitcolas/Anderson/Kuhn*, 87 Proc. IEEE 1062, 1070 (1999). Im Bereich der Kryptographie kann die Existenz sicherer Verschlüsselungsverfahren dagegen mathe-

einem Schutz gegen Attacken durch Profis sind digitale Wasserzeichen heute noch recht weit entfernt.[321]

In der Praxis gilt die Faustregel, daß mit zunehmender Robustheit des Wasserzeichens dessen Wahrnehmbarkeit ansteigt.[322] Weiterhin sinkt regelmäßig mit zunehmender Menge einzubettender Informationen die Robustheit des Wasserzeichens ab.[323] Schließlich ist auch die Rechenintensität von Wasserzeichenverfahren zu beachten, die dem Einsatz komplexer Verfahren in der Praxis mitunter Grenzen setzt.[324] Regelmäßig muß ein Kompromiß zwischen diesen verschiedenen Anforderungen gefunden werden.[325] Fragen der Interoperabilität verschiedener Wasserzeichenverfahren sind noch weitgehend ungeklärt.[326] Da bei Wasserzeichenverfahren eine Vielzahl von Schlüsseln anfällt, sind Infrastrukturen zur Schlüsselverwaltung notwendig.[327] Ebenso sind eventuell Infrastrukturen für Zeitstempeldienste erforderlich.[328] Diesbezüglich steht die Entwicklung jedoch noch ganz in ihren Anfängen.

Es ist unklar, ob die dargestellten technischen Probleme mittelfristig gelöst werden können. So gibt es kritische Stimmen, die den Wert digitaler Wasserzeichen zum Schutz von Urheber- und Leistungsschutzrechten als gering einschätzen.[329] Die eingesetzten Verfahren müssten über einen möglichst langen Zeitraum einen wirksamen Schutz gewährleisten, auch wenn sich die Rechenkapazitäten, die den Angreifern zur Verfügung stehen, mit den Jahren deutlich erhöhen.[330] Allerdings ist zu beachten, daß die Anforderungen an Wasserzeichensysteme je nach Anwendungsgebiet stark differieren. Wasserzeichensysteme müssen nicht für alle denkbaren Einsatzgebiete alle dargestellten Eigenschaften aufweisen. Es gibt kein universell einsetzbares Wasserzeichenverfahren.[331] Insgesamt muß zumindest noch einiges an Forschungs- und Entwicklungsarbeit geleistet werden, bevor Wasserzeichenverfahren ernsthaft gegen intelligente An-

matisch bewiesen werden, s. *Anderson/Petitcolas*, 16 (4) IEEE Journal on Selected Areas in Communications 474, 477 (1998) m. w. N.

[321] *Kutter/Hartung* in: Katzenbeisser/Petitcolas (Hrsg.), S. 118; *Dittmann*, S. 165.

[322] *Kutter/Hartung* in: Katzenbeisser/Petitcolas (Hrsg.), S. 109.

[323] *Kutter/Hartung* in: Katzenbeisser/Petitcolas (Hrsg.), S. 109; *Johnson* in: Katzenbeisser/Petitcolas (Hrsg.), S. 88; *Dittmann*, S. 28; *Herrigel*, DuD 1998, 254, 256.

[324] *Dittmann*, S. 3.

[325] *Zeng/Liu*, 8 IEEE Transactions on Image Processing 1534 (1999); *Hartung/Kutter*, 87 Proc. IEEE 1079, 1103 (1999).

[326] *Mintzer/Braudaway/Bell*, 41 Comm. ACM 57 (Juli 1998).

[327] *Dittmann*, S. 152 f.; vgl. auch *Zeng/Liu*, 8 IEEE Transactions on Image Processing 1534, 1541 (1999).

[328] S. dazu oben Fn. 302.

[329] Kritisch z. B. *Craver/Perrig/Petitcolas* in: Katzenbeisser/Petitcolas (Hrsg.), S. 172.

[330] *Petitcolas/Anderson/Kuhn*, 87 Proc. IEEE 1062, 1072 (1999); *Breitbach/Imai* in: Franklin (Hrsg.), S. 125, 126.

[331] *Hartung/Kutter*, 87 Proc. IEEE 1079, 1098 (1999); *Petitcolas/Anderson/Kuhn*, 87 Proc. IEEE 1062, 1074 (1999).

griffe sicher sind.[332] Trotz all dieser Probleme stellen digitale Wasserzeichen einen wichtigen Baustein von DRM-Systemen dar. Sie versprechen eine sichere und dauerhafte Verbindung von Metadaten mit dem geschützten digitalen Inhalt.

3. Identifzierung der Nutzer

> *Sooner or later, any encryption system can be broken.*
> *We need watermarking technologies to tell us who did it.*[333]

Verschlüsselungssysteme bieten zumindest in der Form, in der sie im kommerziellen Bereich verwendet werden,[334] keinen absoluten Schutz. Um einen digitalen Inhalt nutzen zu können, muß dieser im Endgerät immer entschlüsselt werden. Gelingt es einem Angreifer, den Inhalt in dieser Form zu kopieren, so steht ihm eine ungeschützte Fassung des Inhalts zur Verfügung, die er an Dritte weiterverbreiten kann. Stößt ein Rechteinhaber später auf eine solche ungeschützte Raubkopie, so wäre es wünschenswert, wenn er zumindest feststellen könnte, wer die Raubkopie ursprünglich erstellt hat. Daher werden für DRM-Systeme unterschiedliche Verfahren entwickelt, mit denen die Nutzer des Systems eindeutig identifiziert werden können.

Die Identifizierung der Nutzer kann auch für andere Zwecke eingesetzt werden. Auf ihrer Grundlage können Angebote erstellt werden, die auf die individuellen Nutzungsgewohnheiten zugeschnitten sind. Weiterhin muß der Betreiber eines DRM-Systems bei einer nutzungsspezifischen Abrechnung Informationen darüber haben, welche Leistungen ein bestimmter Nutzer tatsächlich in Anspruch genommen hat. Im folgenden werden die unterschiedlichen Verfahren dargestellt, mit denen Nutzer in DRM-Systemen identifiziert werden. Die Verfahren setzen dabei an einer individuellen Identifizierung der Geräte (dazu unten a), der Inhalte (dazu unten b) oder der Schlüssel (dazu unten c), die er benutzt, an.

a) Identifizierung von Endgeräten und Speichermedien: Seriennummern

Zur Nutzeridentifizierung werden die Endgeräte der Nutzer regelmäßig mit eindeutigen Seriennummern versehen. Anfang 1999 kündigte Intel an, in den „Pentium III"-Prozessorchip eine eindeutige Seriennummer zu integrieren, die von Softwareprogrammen zu Identifizierungszwecken verwendet werden kann.[335] Computer, die an das Internet angeschlossen

---

[332] *Federrath*, ZUM 2000, 804, 808.

[333] Aussage eines Managers eines großen Tonträgerherstellers in Kalifornien, zitiert nach EETimes vom 3. 12. 1999, erhältlich unter <http://www.eetimes.com/story/eezine/OEG19990312S0009>.

[334] Im militärischen Sektor spielen Sicherheitsgesichtspunkte eine größere Rolle, so daß auch mehr Wert auf Sicherheit von Verschlüsselungssystemen gelegt wird. Dabei werden aber Einbußen bei der „Benutzerfreundlichkeit" solcher Systeme in Kauf genommen.

[335] S. dazu unten Fn. 709.

sind, können über ihre IP-Adresse[336] sowie ihre MAC-Adresse[337] identifiziert werden. Der Nutzer eines Computers kann mit Cookies identifiziert werden.[338] Computerprogramme funktionieren oftmals erst nach der Eingabe einer eindeutigen Seriennummer. Weiterhin existiert mit dem „Recorder Identification Code" (RID) seit 1995 aufgrund einer Vereinbarung zwischen der Unterhaltungselektronik- und der Tonträgerindustrie ein Numerierungssystem, mit dem jeder CD-Brenner mit einer eindeutigen Identifikation ausgestattet wird. Die Tonträgerindustrie wollte damit erreichen, daß bei raubkopierten Audio-CDs der CD-Brenner ermittelt werden kann, mit dem die Audio-CDs kopiert wurden.[339] Aufgrund einer ähnlichen Vereinbarung existiert seit 1994 mit dem „Source Identification Code" (SID) ein Numerierungssystem, mit dem Unternehmen, in denen CDs gepreßt werden, eindeutig identifiziert werden. Diese Identifikation ist auf jeder CD aufgedruckt, die von diesem Unternehmen hergestellt wird.[340]

b) Identifizierung digitaler Inhalte: digitale Fingerabdrücke

Auch existieren Verfahren, mit denen nicht die Endgeräte des Nutzers, sondern die Inhalte, die der Nutzer erhält, individuell für den Nutzer markiert werden. Gibt ein Nutzer derart markierte Inhalte an Dritte weiter, so kann er aufgrund der Markierung später ermittelt werden. Diese

---

[336] Zum Begriff der IP-Adresse s. oben Fn. 214. Insbesondere bei Anwendern, die sich über Telefonleitungen zeitweise bei Internet Service Providern in das Internet einwählen, wird die IP-Adresse jedoch über das „Dynamic Host Configuration Protocol" (DHCP) dynamisch zugewiesen; dann ist eine dauerhafte Identifizierung über die IP-Adresse nicht möglich. S. dazu auch *Weinberg*, 52 Stan. L. Rev. 1251, 1260 f. (2000).

[337] Ethernet-Karten verfügen über eine eindeutige Nummer („Media Access Control", MAC), die ebenfalls zu Identifizierungszwecken eingesetzt werden kann.

[338] Cookies sind weltweit eindeutige Einträge in einer Datei auf dem Nutzerrechner, die von einem WWW-Server generiert und beim nächsten Zugriff auf den WWW-Server wieder an ihn übermittelt werden. Cookies ermöglichen eine dauerhafte eindeutige und systematische Identifizierung. S. dazu *Köhntopp/Köhntopp*, CR 2000, 248, 252; *Dinant*, S. 5 f. Zu datenschutzrechtlichen Problemen s. *Ihde*, CR 2000, 413 ff.

[339] Das System ist Teil der CD-R- und CD-RW-Standardisierung, seine Verwendung für die Hersteller von CD-Brennern damit obligatorisch. Der RID Code ist Teil des Orange Books, dem Standard für CD-R und CD-RW. S. zum ganzen <http://www.licensing.philips.com/partner/data/sl01521.pdf> und allgemein <http://www.licensing.philips.com/cdsystems/cdcopyright.html>.

[340] Die Verwendung des SID ist grundsätzlich freiwillig. Jedoch existieren in manchen Ländern gesetzliche Vorschriften, die die Verwendung des Systems vorschreiben (so in Bulgarien und China, s. <http://www.licensing.philips.com/partner/sl01511.pdf>, S. 1. Derzeit wird der SID von etwa 80% der weltweit bekannten 484 CD-Preßwerke verwendet, die etwa 96% der identifizierbaren weltweiten CD-Herstellkapazität ausmachen, s. <http://www.ifpi.org/antipiracy/enforcement.htm>. S. allgemein <http://www.licensing.philips.com/cdsystems/cdcopyright.html>. Ein Verfahren, mit denen das CD-Preßwerk aufgrund von individuellen Ungenauigkeiten im Preßvorgang ermittelt werden kann, entwickelte das Unternehmen Intelligent Automation, <http://www.i-a-i.com>, s. dazu <http://www.wirednews.com/news/mp3/0,1285,39351,00.html>.

Markierungen werden digitale Fingerabdrücke („digital fingerprints")[341] genannt. Ein Ziel digitaler Fingerabdrücke ist, Beweise für rechtliche Schritte gegen den Nutzer zu liefern. Verfahren für digitale Fingerabdrücke werden für unterschiedliche digitale Datenformate, aber auch für gedruckten Text[342] entwickelt. Auch für Computersoftware bestehen Markierungsverfahren, die digitalen Fingerabdrücken vergleichbar sind.[343] Technisch betrachtet handelt es sich um digitale Wasserzeichen, die eine individuelle Kennzeichnung eines bestimmten Nutzers enthalten und in eine bestimmte Kopie des digitalen Inhalts eingefügt werden.[344] Hinsichtlich der technischen Grundlagen und der Anforderungen an Sicherheit und Robustheit digitaler Fingerabdrücke ist daher auf die Ausführungen zu digitalen Wasserzeichen zu verweisen.[345] Ein zusätzliches Problem, das bei normalen Wasserzeichen nicht auftritt, ist die sogenannte Kollusionsattacke („collusion attack"):[346] Schließen sich mehrere Nutzer zusammen, so können sie versuchen, ihre individuell markierten Fassungen des Inhalts zu vergleichen, die Unterschiede zwischen den Fassungen zu ermitteln, die individuell markierten Stellen zu ändern und damit eine Fassung des Inhalts zu berechnen, in der kein individueller Fingerabdruck mehr enthalten ist.[347] Jedoch existieren Verfahren, mit de-

[341] Teilweise differiert der Sprachgebrauch. *Johnson/Duric/Jajodia*, S. 83, verstehen unter „digitalen Fingerabdrücken" spezielle Formen normaler digitaler Wasserzeichen, die nicht der Nutzeridentifizierung dienen. Zu „audio fingerprints" s. unten Teil 1, C V 1.

[342] *Brassil/Low/Maxemchuk*, 87 Proc. IEEE 1181 ff. (1999); *Brassil/Low/Maxemchuk/O'Gorman*, 13 IEEE Journal on Selected Areas in Communications 1495 ff. (1995)

[343] Regelmäßig wurden digitale Wasserzeichenverfahren für Computersoftware zur Identifizierung der Nutzer, nicht der Urheber entwickelt. Weiterhin können Techniken wie die Code Obfuscation (s. dazu unten Teil 1, C IV 2 b) für digitale Fingerabdrücke bei Computersoftware eingesetzt werden. Dabei stellt sich dann auch nicht das Problem der Kollusionsattacke (s. dazu sogleich im Text), da die Unterschiede zwischen verschiedenen durch Code Obfuscation markierten Versionen der Software zu groß sind, um durch einen Vergleich die Markierung zu entfernen, s. *Collberg/Thomborson* in: Proceedings of POPL 1999, S. 311, 322; *Collberg/Thomborson/Low*, S. 31.

[344] *Dittmann*, S. 39.

[345] S. oben Teil 1, C II 2 b bb.

[346] Dies ist nicht das einzige zusätzliche Problem. So kann der Inhalteanbieter bei normalen digitalen Fingerabdrücken nie nachweisen, ob der identifizierte Nutzer den digitalen Inhalt tatsächlich illegal weiterverbreitet hat oder ob nicht vielmehr ein Mitarbeiter des DRM-Anbieters oder des Inhalteanbieters den digitalen Fingerabdruck einfügte, um einen Nutzer zu diffamieren bzw. den Verdacht von sich abzulenken. Zur Lösung dieses Problems werden sog. „asymmetrische digitale Fingerabdrücke" entwickelt, bei denen bewiesen werden kann, daß der vollständige Fingerabdruck nur vom Nutzer selbst stammen kann, da nur dieser den gesamten Fingerabdruck kannte. S. dazu *Lee* in: Katzenbeisser/Petitcolas (Hrsg.), S. 175, 184; *Pfitzmann/Waidner*, DuD 1998, 258 ff.; *Pfitzmann/Schunter* in: Maurer (Hrsg.), S. 84 ff.; *Yoshiura/Sasaki/Takaragi* in: Christianson (Hrsg.), S. 83 ff.

[347] *Lee* in: Katzenbeisser/Petitcolas (Hrsg.), S. 180; *Boneh/Shaw* in: Coppersmith (Hrsg.), S. 452 ff.; *Dittmann*, S. 39, 116 f.; *Pfitzmann/Waidner*, DuD 1998, 258, 259.

nen die digitalen Fingerabdrücke auch bei einer Kollusion mehrerer Nutzer nicht vollständig entfernt werden können.[348] Diesbezüglich besteht noch Forschungsbedarf.[349]

Ein Novum des digitalen Zeitalters war der Wegfall von Qualitätsverlusten: Original und digitale Kopie sind nicht mehr voneinander zu unterscheiden. Mit Hilfe digitaler Fingerabdrücke wird die Unterscheidung von Original und einer Kopie grundsätzlich wieder möglich.[350]

c) Identifizierung des Dechiffrier-Schlüssels

Ein Angreifer beeinträchtigt die Sicherheit eines DRM-Systems auch, wenn es ihm gelingt, einen Dechiffrier-Schlüssel auszulesen, und er diesen Schlüssel an Dritte weitergibt. Die Dritten beziehen die Inhalte in verschlüsselter Form von anderer Seite (beispielsweise direkt vom Anbieter) und entschlüsseln sie mit dem Dechiffrier-Schlüssel, den sie vom Angreifer erhalten haben. Solche Angriffe sind bei Pay-TV-Systemen oder verschlüsselten CD-ROMs beobachtet worden. Eine Markierung des Inhalts selbst mit Hilfe digitaler Fingerabdrücke würde hier nicht helfen: Der Angreifer hat nicht den digitalen Inhalt, sondern nur den Dechiffrier-Schlüssel weitergegeben. Daher wird an Verfahren gearbeitet, die den Dechiffrier-Schlüssel selbst mit einer eindeutigen Markierung versehen.

aa) Individuelle Verschlüsselung

Eine einfache Lösung ist, für jeden Nutzer die Inhalte individuell zu verschlüsseln. Gibt ein Nutzer seinen Dechiffrier-Schlüssel an einen Dritten weiter, so kann der Nutzer anhand seines Dechiffrier-Schlüssels identifiziert werden.[351] Auch kann eine Identifizierungsnummer der Endgeräte

---

[348] Diese Verfahren beruhen regelmäßig darauf, daß die Nutzer nicht wissen, in welcher Reihenfolge die Markierungs-Bits angeordnet werden müssen, um den korrekten digitalen Fingerabdruck zu erhalten. Beschreibungen der technischen Grundlagen finden sich bei *Lee* in: Katzenbeisser/Petitcolas (Hrsg.), S. 182 ff. Kollusionsresistenz kann auch erreicht werden, wenn sich die digitalen Fingerabdrücke unterschiedlicher Nutzer nicht vollständig unterscheiden. Das Ziel ist, aus diesen Übereinstimmungen der Fingerabdrücke zumindest einen der beteiligten Nutzer zu identifizieren, s. *Matheson/Mitchell/Shamoon/Tarjan/Zane* in: Hirschfeld (Hrsg.), S. 227, 236. Vgl. weiterhin *Dittmann*, S. 117 ff., 167 ff.; *Pfitzmann/Waidner*, DuD 1998, 258, 261 ff.; *Boneh/Shaw* in: Coppersmith (Hrsg.), S. 452 ff.; *Ergun/Kilian/Kumar* in: Stern (Hrsg.), S. 140 ff.

[349] S. *Dittmann*, S. 115, 132 f. So können viele der kollusionssicheren Fingerabdruck-Verfahren Nutzer lediglich mit einer gewissen statistischen Fehlerrate identifizieren, die aber beliebig verringert werden kann, s. *Fiat/Tassa* in: Wiener (Hrsg.), S. 354, 356. Die derzeitigen Verfahren sind regelmäßig entweder nur gegen die Kollusion einer relativ geringen Zahl von Nutzern resistent oder aber für den praktischen Einsatz zu rechenintensiv, *Pfitzmann/Waidner*, DuD 1998, 258, 259, 263.

[350] Vgl. *Herrigel*, DuD 1998, 254, 257; *Gass*, ZUM 1999, 815, 818.

[351] Zu diesem Zweck existieren auch Verfahren, bei dem im Dechiffrier-Schlüssel des Nutzers persönliche Informationen (Kreditkarten-Nummer, Bankverbindung, Telefonnummer etc.) enthalten sind. Dadurch sollen Nutzer von der Weitergabe des Dechiffrier-Schlüssels abgeschreckt werden. Zu diesem Verfahren s. *Dwork/Lotspiech/Naor* in: Proceedings of STOC 1996, S. 489 ff.; *Pfitzmann* in: Anderson (Hrsg.), S. 49, 52.

Teil des Dechiffrier-Schlüssels werden. Dieses Verfahren zielt darauf ab, daß der digitale Inhalt nur auf dem berechtigten Endgerät entschlüsselt werden kann.[352]

bb) Traitor Tracing

Bei Punkt-zu-Multipunkt-Übertragungen[353] hilft eine individuelle Verschlüsselung nicht weiter, da die digitalen Inhalte in einheitlich verschlüsselter Form an eine Vielzahl von Nutzern übertragen werden. Es sind andere Verfahren erforderlich, mit denen auch bei Punkt-zu-Multipunkt-Übertragungen eine Identifizierung von Nutzern möglich ist, die den Dechiffrier-Schlüssel zur Verfügung zu stellen. Dabei wird auf Verfahren aufgebaut, die die Verschlüsselung mit einem einheitlichen Schlüssel, aber die Entschlüsselung mit unterschiedlichen Schlüsseln erlauben.[354] Zur Nutzeridentifizierung wird nicht der digitale Inhalt selbst, sondern der Dechiffrier-Schlüssel sowie die Entschlüsselungsfunktion mit einem digitalen Fingerabdruck versehen.[355] Diese sogenannten „traitor tracing"-Verfahren[356] sind damit das Äquivalent von digitalen Fingerabdrücken im Bereich von Punkt-zu-Multipunkt-Übertragungen, bei denen eine vom jeweiligen Nutzer abhängige Kennzeichnung des Medieninhalts selbst nicht möglich ist.[357] Gibt ein Nutzer seinen Dechiffrier-Schlüssel an Dritte weiter und wird dieser Schlüssel beispielsweise in einem Piraten-Pay-TV-Decoder gefunden, so kann der Nutzer identifiziert werden.[358] In

Einen ähnlichen Ansatz schlagen *Brassil/Low/Maxemchuk*, 87 Proc. IEEE 1181, 1182 (1999), für gedruckten Text vor. Zu einem anderen System, das auf dem für jeden Nutzer individualisierten Wechsel zwischen zwei parallel übertragenen verschlüsselten Versionen eines übertragenen Videofilms aufbaut, s. *Chu/Qiao/Nahrstedt* in: Wong/Delp (Hrsg.), S. 460, 468 ff.

352 S. dazu *National Research Council*, S. 161. Dieses Verfahren wird beispielsweise im Rahmen des CPRM-Standards eingesetzt, s. unten Teil 1, D II 4.

353 S. oben Teil 1, C I 1 b bb.

354 Zu dieser „point-to-multipoint encryption" s. oben bei Fn. 92.

355 S. *Pfitzmann* in: Anderson (Hrsg.), S. 49, 53; *Boneh/Franklin* in: Wiener (Hrsg.), S. 338.

356 Wörtlich übersetzt „Aufspüren des Verräters".

357 *Pfitzmann/Waidner*, DuD 1998, 258, 259. Durch sog. asymmetrisches „traitor tracing" soll sichergestellt werden, daß diese Beweise auch nicht durch Fälschung vom Anbieter des DRM-Systems erstellt werden können, s. dazu *Pfitzmann* in: Anderson (Hrsg.), S. 49 ff. Zum gleichen Problem bei digitalen Fingerabdrücken s. oben Fn. 346. Dennoch bestehen wichtige Unterschiede zwischen dem „traitor tracing" und digitalen Fingerabdrücken. Die Sicherheit des „traitor tracing" und der oft damit kombinierten „broadcast encryption" kann mathematisch bewiesen werden. Die mathematischen Grundlagen digitaler Fingerabdrücke und digitaler Wasserzeichen sind dagegen unklarer; bisher ist nicht bewiesen, ob ein sicheres Verfahren digitaler Fingerabdrücke überhaupt existieren kann.

358 Es ist im vorliegenden Rahmen nicht möglich, die technischen Grundlagen des „traitor tracing" zu erläutern. „Traitor tracing"-Verfahren sind im einzelnen recht kompliziert. So ist es nicht notwendig, die in einem Piraterie-Decoder verwendeten Schlüssel auszulesen, um den Nutzer zu identifizieren. Vielmehr können die „traitor tracing"-Verfahren den Piraterie-Decoder gleichsam als „black box" aufgreifen und dennoch

Verbindung mit anderen Verfahren (insbesondere der „broadcast encryption")[359] stellen „traitor tracing"-Verfahren bei Punkt-zu-Multipunkt-Übertragungen eine wirksame Möglichkeit dar, Nutzer eines DRM-Systems zu identifizieren, die unberechtigten Dritten Zugang zum System verschaffen („traitor tracing"), und sie dann von der weiteren Nutzung des Systems auszuschließen (durch „broadcast encryption").[360] Die Forschung ist noch lange nicht abgeschlossen, insbesondere was die Effizienz der „traitor tracing"-Verfahren angeht.[361] So existiert auch hier das schon von digitalen Fingerabdrücken bekannte[362] Problem der Kollusionsattacke.[363]

Rückschlüsse auf die im Decoder verwendeten Schlüssel ziehen, s. *Naor/Pinkas* in: Krawczyk (Hrsg.), S. 502, 504, 508. Auch werden den Nutzern regelmäßig nicht Schlüssel zugewiesen, mit denen sie direkt die verschlüsselten Inhalte entschlüsseln können. Vielmehr können sie mit ihren Schlüsseln und bestimmten vom Anbieter mitgeteilten Daten einen Schlüssel berechnen, mit dem dann die verschlüsselten Inhalte entschlüsselt werden können, s. *Naor/Pinkas* in: Krawczyk (Hrsg.), S. 502, 505. Grundlegend zum „traitor tracing" *Chor/Fiat/Naor* in: Desmedt (Hrsg.), S. 257 ff.; anschaulich *Pfitzmann* in: Anderson (Hrsg.), S. 49, 53 f. Vgl. ferner *Boneh/Franklin* in: Wiener (Hrsg.), S. 338 ff. Einen Überblick geben *Pfitzmann/Waidner*, DuD 1998, 258, 259; *Federrath*, ZUM 2000, 804, 809.

[359] S. dazu oben bei Fn. 93 f.

[360] S. zu dieser Kombination *Gafni/Staddon/Yin* in: Wiener (Hrsg.), S. 372 ff.; *Naor/Pinkas* in: Krawczyk (Hrsg.), S. 502, 506.

[361] So können viele „traitor tracing"-Verfahren Nutzer lediglich mit einer gewissen statistischen Fehlerrate identifizieren, die jedoch beliebig verringert werden kann, s. *Fiat/Tassa* in: Wiener (Hrsg.), S. 354, 356. *Naor/Pinkas* Krawczyk (Hrsg.), S. 502 ff., schlagen ein System vor, bei dem nur solche Schlüssel in Piraterie-Decodern zurückverfolgt werden können, die mit einer bestimmten, beliebig auszuwählenden Wahrscheinlichkeit die digitalen Inhalte entschlüsseln können. Diese Einschränkung führt zu deutlichen Effizienzgewinnen und kann für den praktischen Einsatz hinnehmbar sein. Wenn beispielsweise durch Marktanalysen festgestellt wird, daß Nutzer einen Piraterie-Pay-TV-Decoder nicht akzeptieren, wenn dieser nur 80% der Bilder des TV-Programmes entschlüsselt, muß ein „traitor tracing"-Verfahren auch nur auf solche Piraterie-Decoder zugeschnitten sein, bei denen die Dechiffrier-Rate höher liegt. S. weiterhin *Boneh/Franklin* in: Wiener (Hrsg.), S. 338, 352.

[362] S. oben bei Fn. 346 ff.

[363] Zum gleichen Problem bei der „broadcast encryption" s. oben Fn. 94. Schließt sich eine größere Anzahl böswilliger Nutzer zusammen, so ist es möglich, aus allen ihren Schlüsseln einen neuen Schlüssel zu berechnen, mit dem sich die Inhalte immer noch dechiffrieren lassen, die aber keinen Rückschluß mehr auf einen oder mehrere der böswilligen Nutzer zulassen, s. *Federrath*, ZUM 2000, 804, 809. Zwar läßt sich bei den „traitor tracing"-Verfahren die Zahl der böswilligen Nutzer, die sich zusammenschließen müssen (sog. Kollusionsresistenz), beliebig festsetzen, *Chor/Fiat/Naor* in: Desmedt (Hrsg.), S. 257, 262; *Naor/Pinkas* in: Krawczyk (Hrsg.), S. 502, 506. Je höher diese Zahl gewählt wird und je sicherer damit das System ist, desto rechenintensiver werden aber die Verfahren. Damit muß auch hier eine Abwägung zwischen Sicherheit und Effizienz getroffen werden. In der Praxis mag diese Zahl in der Größenordnung von 20 böswilligen Nutzern liegen, *Boneh/Franklin* in: Wiener (Hrsg.), S. 338, 339.

III. Schutz der Authentizität und Integrität

DRM-Systeme wollen ein umfassendes Sicherheitskonzept für den Vertrieb digitaler Inhalte bieten. Dabei muß sichergestellt sein, daß die in einem DRM-System übertragenen Inhalte nicht von einem Angreifer verändert werden können (Schutz der Integrität).[364] Auch muß sichergestellt sein, daß die Inhalte tatsächlich von derjenigen Instanz stammen, die sich als Absender der Inhalte ausgibt (Schutz der Authentizität). Um das gewünschte Sicherheitsniveau zu erreichen, müssen in einem DRM-System Integrität und Authentizität der digitalen Inhalte, der Metadaten, der Nutzer und der eingesetzten DRM-Systemkomponenten gewährleistet sein (dazu unten 1). Dafür existieren unterschiedliche Verfahren, die unter 2 dargestellt werden.

1. Schutzobjekte

a) Authentizität und Integrität digitaler Inhalte

In einem DRM-System muß sichergestellt sein, daß der übertragene Inhalt auch tatsächlich von demjenigen stammt, der als Inhalteanbieter angegeben ist. Ansonsten könnte ein Dritter einem Inhalteanbieter einen Inhalt „unterschieben" (Problem der Authentizität). Weiterhin muß sichergestellt sein, daß digitale Inhalte auf dem Übertragungsweg (sei es online per Internet oder offline per CD-ROM oder ähnlichen Medien) nicht verändert wurden (Integrität). Eine Veränderung der Inhalte kann unter anderem gegen urheberpersönlichkeitsrechtliche Interessen des Urhebers verstoßen.[365]

Hinsichtlich der Integritätsprüfung digitaler Inhalte sind zwei Verfahrensansätze zu unterscheiden. Beim ersten Verfahrensansatz kann jede kleinste Änderung am digitalen Inhalt entdeckt werden (sogenannte „*complete verification*").[366] Oft ist es jedoch nicht wünschenswert, daß

---

[364] Eine detaillierte Untergliederung des Begriffs „Integrität" nehmen *Federrath/Pfitzmann*, DuD 2000, 704, 706, vor.

[365] Die Integrität digitaler Inhalte muß auch gewährt bleiben, damit nicht die Aussage der Inhalte verfälscht wird. Dies ist gerade in digitalen Medien problemlos möglich. Eine bekannte Fotografie vom 14. 5. 1998 zeigt Bill Clinton, Helmut Kohl und Bernhard Vogel bei einem Besuch im thüringischen Eisenach vor einer großen Menschenmenge. Auf dem Originalbild der Agentur Reuters findet sich in der Menschenmenge ein Plakat mit der Aufschrift „Ihr habt auch in schlechten Zeiten dicke Backen". In einer später von der Thüringer Landesregierung veröffentlichten Broschüre wurde das Foto publiziert, jedoch das Plakat digital wegretuschiert; vgl. *Dittmann*, S. 135 f. Ein anderes Beispiel im Umfeld der Lewinsky-Affäre des U.S.-Präsidenten Bill Clinton findet sich unter <http://www.ctr.columbia.edu/~cylin/auth/auth.html>.

[366] Dafür existieren Verfahren, bei denen von einem digitalen Bild Prüfsummen erzeugt werden, die dann mit einem digitalen Signaturverfahren signiert werden. Wird das Bild später verändert, so stimmen die neu errechneten Prüfsummen nicht mehr mit den signierten Prüfsummen überein. Jede kleinste Änderung des Bildes führt zu einer Veränderung der Prüfsumme. S. zum ganzen *Friedman*, 39 IEEE Transactions on Con-

jede kleinste Änderung des Inhalts bei einer Integritätsprüfung entdeckt wird. So werden digitale Inhalte in einem DRM-System systembedingt bestimmten Datenveränderungen wie Kompression, Formatkonvertierung, Skalierung oder auch kleinen Übertragungsfehlern ausgesetzt, die nicht als inhaltliche Veränderung des Inhalts aufgefaßt werden können und daher auch nicht dessen Integrität beeinträchtigen.[367] Ein neuerer, inhaltsabhängiger Verfahrensansatz versucht daher, nur im Fall einer inhaltlichen Veränderung eine Beeinträchtigung der Integrität des Inhalts zu melden (sogenannte „*content verification*").[368] Gerade im kontinentaleuropäischen Raum, wo dem Urheberpersönlichkeitsrecht eine wichtige

sumer Electronics 905 ff. (1993), der ein solches Verfahren für den Einsatz in digitalen Fotokameras darstellt.

[367] *Dittmann*, S. 135.

[368] Dafür existieren digitale Signaturverfahren, bei denen aus einem Bild charakteristische Bildmerkmale extrahiert („feature extraction") und digital signiert werden. Diese Bildmerkmale sind auch nach einer Kompression noch vorhanden. Nach einer Extraktion charakteristischer Bildmerkmale werden diese digital signiert, s. *Augot/Boucqueau/Delaigle/Fontaine/Goray*, 87 Proc. IEEE 1251, 1254 (1999). Diese Verfahren können somit absichtliche Manipulationen erkennen, fassen Veränderungen durch Kompression und Formatkonvertierung jedoch nicht als Angriff auf die Integrität des digitalen Inhalts auf. Ein solches Verfahren wird von *Lin/Chang* in: Dittmann/Wohlmacher/Horster/Steinmetz (Hrsg.), S. 49 ff., vorgestellt. *Schneider/Chang*, Proceedings of ICIP 1996, Band 3, S. 227 ff.; *Augot/Boucqueau/Delaigle/Fontaine/Goray*, 87 Proc. IEEE 1251, 1254 (1999). Auch existieren sog. „Hash"-Funktionen mit vergleichbaren Eigenschaften. Bei diesen – auch „robust hash" oder „visual hash" genannten – Verfahren ändert sich die Prüfsumme eines Inhalts nicht bei jeder Veränderung eines Bits des Inhalts, sondern nur bei Veränderungen charakteristischer Merkmale. Ein solches Verfahren wird von *Fridrich/Goljan* in: Proceedings of ITCC 2000, S. 178 ff., vorgestellt. Allgemein zu „Hash"-Funktionen s. sogleich im Text. Schließlich wird an Wasserzeichenverfahren geforscht, die gegenüber absichtlichen Manipulationen empfindlich, gegenüber üblichen Datenveränderungen (Kompression, Formatkonvertierung u. ä.) jedoch robust sind. Der Entwurf solcher Verfahren erweist sich jedoch als schwierig. S. zum ganzen *Dittmann*, S. 139; *Fridrich*, in: Proceedings of ISPACS 1998, S. 173 ff.; *Marvel/Hartwig/Boncelet* in: Wong/Delp (Hrsg.), S. 131 ff. Eine gut funktionierende Lösung wurde noch nicht gefunden, die Forschung steht hier erst in ihren Anfängen, s. *Dittmann/Steinebach*, DuD 2000, 593 m. w. N. So wird beispielsweise versucht, die Existenz charakteristischer Bildmerkmale wie Konturen oder Linien eines Bildes in einem Wasserzeichen im Bild abzuspeichern. Wird das charakteristische Bildmerkmal entfernt, so stimmt die Beschreibung des Bildes im Wasserzeichen mit dem Bild selbst nicht mehr überein. S. dazu *Dittmann/Steinebach*, DuD 2000, 593, 594. Andere Ansätze finden sich bei *Fridrich* in: Proceedings of ICIP 1998, Band 2, S. 404 ff. Grundsätzlich können für die dargestellten Zwecke sowohl digitale Signaturen als auch digitale Wasserzeichen eingesetzt werden. Einerseits sind digitale Wasserzeichen besser geeignet als digitale Signaturen; so ist regelmäßig ein digitales Wasserzeichen schwerer zu entfernen als eine digitale Signatur. S. dazu insgesamt *Lin/Delp* in: Dittmann/Nahrstedt/Wohlmacher (Hrsg.), S. 47, 48; *Dittmann*, S. 2, 135. Andererseits sind digitale Wasserzeichen zur Integritätsprüfung sind zwar generell die elegantere Lösung als digitale Signaturen, jedoch oft entweder zu fragil, um auch nach einer Datenkompression noch vorhanden zu sein, oder zu robust, um durch eine verändernde Manipulation gelöscht zu werden; *Lin/Chang* in: Dittmann/Wohlmacher/Horster/Steinmetz (Hrsg.), S. 49, 50.

Stellung zukommt, können diese Verfahren interessant sein, ermöglichen sie doch, eine inhaltsverändernde Manipulation von einer bloßen technisch bedingten Konvertierung zu unterscheiden.[369]

b) Authentizität und Integrität von Metadaten

DRM-Systeme benötigen Metadaten unter anderem, um Inhalte zu identifizieren und die Nutzung digitaler Inhalte zu kontrollieren und Zahlungsvorgänge zu initiieren.[370] Die Sicherheit eines DRM-Systems hängt entscheidend von der Zuverlässigkeit der Metadaten ab. Daher muß sichergestellt sein, daß ein Angreifer die Metadaten – die beispielsweise die Beschränkung enthalten, daß der Inhalt nur zwei Mal kopiert werden darf – nicht verändern kann (Integrität). Auch muß sichergestellt sein, daß ein Angreifer die Metadaten nicht komplett austauscht und sich dann als vermeintlicher Rechteinhaber ausgibt (Authentizität).[371]

c) Authentizität und Integrität von Nutzern und Systemkomponenten

Schließlich muß sichergestellt sein, daß ein Nutzer, an den ein digitaler Inhalt übertragen wird, auch tatsächlich derjenige berechtigte Nutzer ist, als der er sich ausgibt. Ansonsten könnte ein Angreifer in einem DRM-System vortäuschen, ein berechtigter Nutzer zu sein (Authentizität). Weiterhin muß sichergestellt sein, daß die Komponenten eines DRM-Systems – also Hard- und Software beim DRM-Anbieter, bei Netzbetreibern und bei den Nutzern – DRM-kompatibel sind. Es muß verhindert werden, daß ein Angreifer ein Piratengerät in das DRM-System einschmuggelt und das Gerät als eine berechtigte DRM-Komponente ausgibt (Authentizität). Auch muß gewährleistet sein, daß Hard- und Software in DRM-Systemen nicht von einem Angreifer manipuliert wurden (Integrität).[372] Ansonsten wäre die Sicherheit des DRM-Systems beeinträchtigt.

---

[369] *Augot/Boucqueau/Delaigle/Fontaine/Goray*, 87 Proc. IEEE 1251, 1254 (1999).

[370] Zu Metadaten s. oben Teil 1, C II.

[371] *Hill*, 87 Proc. IEEE 1228, 1233 (1999). Daher werden alle Metadaten, die in einem XrML-Dokument (s. dazu oben Teil 1, C II 2 a bb 2) definiert werden, mit einer digitalen Signatur versehen, um die Integrität und Authentizität der Nutzungsbedingungen zu garantieren, vgl. *Contentguard*, XrML Version 1.03, S. 16 ff., 23 f., 26. Wenn Metadaten in XML ausgedrückt werden, können sie auch die Sicherheitsmechanismen nutzen, die allgemein für XML-Daten entwickelt werden, s. dazu unten Fn. 512. Auch wenn Metadaten unverschlüsselt und unsigniert übertragen werden, kann ihre Integrität gewährleistet werden: Teile der Metadaten können Bestandteil des Dechiffrierschlüssels sein, der zum Entschlüsseln des geschützten digitalen Inhalts notwendig ist. Wenn die Metadaten geändert werden, so ändert sich dadurch auch der Dechiffrierschlüssel, was die Entschlüsselung der Inhalte unmöglich macht, s. *Intel/IBM/Matsushita/Toshiba*, Content Protection System Architecture, S. 7. Neben diesen technischen Schutzmöglichkeiten für Metadaten existiert auch ein umfangreicher rechtlicher Schutz von Metadaten, s. dazu unten Teil 2, D I 3.

[372] Vgl. *Rubin* in: Proceedings of the Symposium on Network and Distributed System Security 1995, S. 47 ff.

2. Schutzverfahren

Um die Authentizität und Integrität der digitalen Inhalte, der Metadaten, der Nutzer und der DRM-Systemkomponenten gewährleisten zu können, werden in DRM-Systemen unterschiedliche Verfahren eingesetzt.

a) Integrität durch Hash-Funktionen

Die Integrität von digitalen Inhalten und Metadaten kann durch die Berechnung sogenannter „Prüfsummen" gewährleistet werden. Dabei wird mit sogenannten „Hash"-Funktionen aus dem digitalen Inhalt ein kurzer Wert errechnet, in den sämtliche Bits des Inhalts in genau festgelegter Weise einfließen. Eine kleine Änderung in den Bits des Inhalts führt dabei zu einer signifikanten Änderung der Prüfsumme, die vom DRM-System zusätzlich zu dem eigentlichen Inhalt übermittelt wird.[373] Der Empfänger berechnet seinerseits aus dem digitalen Inhalt, den er erhalten hat, eine Prüfsumme. Stimmt diese Prüfsumme mit der an ihn übertragenen Prüfsumme überein, so ist der Inhalt mit hoher Wahrscheinlichkeit korrekt übertragen worden. Ist dies nicht der Fall, liegt garantiert ein Fehler vor.[374]

b) Integrität und Authentizität durch digitale Signaturen

Mit Hilfe asymmetrischer Verschlüsselungsverfahren können „digitale Signaturen" erzeugt werden, die bei entsprechend hoher Schlüssellänge im Rahmen der heutigen Rechnergeschwindigkeiten nicht geknackt werden können. Digitale Signaturen sind ein Grundpfeiler des sicheren E-Commerce und unterliegen in Deutschland und anderen Ländern umfangreichen gesetzlichen Regelungen. Zur Authentisierung und Integritätsprüfung wird bei digitalen Signaturen aus dem zu übertragenden Inhalt mit Hilfe einer Hash-Funktion eine eindeutige Kurzfassung erzeugt, diese mittels eines – nur dem Absender bekannten – privaten Schlüssels verschlüsselt und an den Originaltext angehängt. Jedermann kann die Integrität des Inhalts überprüfen, indem er nach Übertragung des signierten Inhalts mit Hilfe des – allgemein bekannten – öffentlichen Schlüssels die übertragene Kurzfassung dechiffriert, selbst eine Kurzfas-

---

[373] Es existieren auch „Hash"-Funktionen, bei denen sich die Prüfsumme nur bei inhaltlichen Änderungen, nicht aber bei üblichen Signalverarbeitungsschritten ändert. Zu diesen „visual" oder „robust hash"-Funktionen s. o. Fn. 368.

[374] *Selke*, S. 91. Im vorliegenden Rahmen kann auf die technischen Einzelheiten nicht eingegangen werden. Es existiert eine Vielzahl unterschiedlicher Verfahren. Gemeinsames Merkmal ist, daß alle Verfahren Prüfsummen für beliebig lange Daten auf einfache und schnelle Weise berechnen können. Aus einer Prüfsumme darf der Inhalt nicht konstruiert werden können, die genau diese Prüfsumme liefert. Zu diesem Zweck werden sog. „Einweg"-Hash-Funktionen verwendet, die aus Inhalten mit variabler Länge einen Wert mit fester Länge berechnen, aus dem der Inhalt nicht zurückberechnet werden kann, *Rankl/Effing*, S. 178. S. ausführlich *Schneier*, S. 429 ff. Zu den „Message Authenticiation Codes" (MACs), einer speziellen Prüfsummenform, die auf Verschlüsselungsverfahren aufbaut, s. *Selke*, S. 106 ff.; *Schneier*, S. 455 ff.

sung aus dem Original-Inhalt erstellt und beide Kurzfassungen vergleicht. Unterscheiden sie sich, so wurde der Inhalt nach der Signierung verändert (Integrität).[375] Es kann auch sichergestellt werden, daß der Inhalt tatsächlich von dem angegebenen Absender abgeschickt wurde. Zu diesem Zweck werden bei asymmetrischen Verschlüsselungsverfahren sogenannte Zertifizierungsinstanzen dazwischengeschaltet. Dabei kontaktiert der Empfänger eines signierten Inhalts eine Zertifizierungsinstanz, die ihm mitteilen kann, ob der verwendete öffentliche Schlüssel tatsächlich zu dem angeblichen Absender gehört (Authentizität).[376] Mit Verfahren zur digitalen Signierung können einerseits die Integrität und Authentizität von digitalen Inhalten und Metadaten sichergestellt werden; andererseits gewährleisten digital signierte Zertifikate, daß in einem DRM-System die Authentizität der angeschlossenen Systemkomponenten gewährleistet ist.

c) Integrität digitaler Inhalte durch fragile Wasserzeichen

Um zu überprüfen, ob digitale Inhalte während der Übertragung verändert wurden,[377] können digitale Wasserzeichen eingesetzt werden. Digitale Wasserzeichen zur Integritätsprüfung unterscheiden sich von digitalen Wasserzeichen zu Identifizierungszwecken: Wasserzeichen zu Identifizierungszwecken[378] sind idealerweise gegen möglichst viele Manipulationen resistent.[379] Für die Integritätsprüfung werden dagegen sogenannte „fragile" Wasserzeichen[380] eingesetzt, die schon bei kleinen Veränderungen des Datenmaterials zerstört werden.[381] Digitale Wasserzeichen zum Integritätsschutz wurden bisher hauptsächlich für den Bildbereich entwickelt. Eine Ausweitung auf andere Medien ist aber zu erwarten.[382]

Digitale Wasserzeichen können auch zur Selbstkorrektur des digitalen Inhalts nach einer Manipulation eingesetzt werden. So können mit Hilfe digitaler Wasserzeichen in ein digitales Bild Informationen über das Bild selbst eingebettet werden. Nach einer Manipulation des Bildes wird das

---

375 S. dazu *Selke*, S. 108 ff.

376 Die Einzelheiten sind natürlich komplexer. S. *Selke*, S. 138 ff.; *Schneier*, S. 185 ff.

377 Solche Veränderungen können auch durch verlustbehaftete Komprimierungsverfahren entstehen.

378 S. dazu oben Teil 1, C II 2 b bb.

379 Vgl. dazu oben Teil 1, C II 2 b bb 2 b.

380 Mitunter auch „tamper-proofing watermarks" genannt, so von *Augot/Boucqueau/Delaigle/Fontaine/Goray*, 87 Proc. IEEE 1251, 1255 (1999).

381 Bei fragilen Wasserzeichen werden die Informationen regelmäßig mit geringer Stärke eingebettet. Kann im Ausleseprozeß das Wasserzeichen gefunden werden, ist mit großer Wahrscheinlichkeit keine Manipulation des Datenmaterials erfolgt, s. *Dittmann*, S. 136; *Dittmann/Steinebach*, DuD 2000, 593; *Lin/Delp* in: Dittmann/Nahrstedt/Wohlmacher (Hrsg.), S. 47 ff. Daneben bestehen auch noch andere Ansätze, s. dazu im Überblick *Fridrich* in: Dittmann/Nahrstedt/Wohlmacher (Hrsg.), S. 41 ff. Zu „kontext-sensitiven" fragilen Wasserzeichen s. oben Fn. 368.

382 Vgl. *Dittmann*, S. 135, 147.

Wasserzeichen, das diese Manipulation überstanden hat, ausgelesen. Idealerweise könnte mit Hilfe der im Wasserzeichen enthaltenen Informationen der Originalzustand des Bildes wiederhergestellt werden.[383]

d) Authentizität von Systemkomponenten durch Challenge-Response-Verfahren

Bevor ein DRM-System digitale Inhalte an ein Endgerät überträgt, muß das DRM-System feststellen, ob das Endgerät DRM-kompatibel ist und nicht von einem Angreifer kompromittiert wurde. Zu diesem Zweck ist zwischen den verschiedenen Systemkomponenten eines DRM-Systems eine gegenseitige Authentisierung notwendig. Zu diesem Zweck wird oftmals auf sogenannte „Challenge-Response"-Verfahren zurückgegriffen. Dabei stellt die eine Systemkomponente der anderen eine zufällig erzeugte Frage („challenge"). Die andere Systemkomponente berechnet mit einem – beiden Systemkomponenten bekannten – Algorithmus eine Antwort und sendet diese an die ursprüngliche Systemkomponente zurück („response"). Der Algorithmus ist vorzugsweise ein Verschlüsselungsverfahren mit einem geheimen Schlüssel, der das gemeinsame Geheimnis der Systemkomponenten darstellt.[384]

IV. Manipulationssichere Systeme

Die in einem DRM-System anfallenden Daten (unter anderem digitale Inhalte und Metadaten) werden von Geräten verarbeitet, die sich in der Einflußsphäre der Nutzer befinden (Computer, DVD-Spieler, MP3-Geräte, Monitore, Lautsprecher und ähnliches). Versucht ein Nutzer, diese Geräte oder die von den Geräten verarbeiteten Daten zu manipulieren, so kann dadurch die Sicherheit des DRM-Systems insgesamt beeinträchtigt werden. Beispielsweise kann ein Angreifer ein Endgerät derart manipulieren, daß er Dechiffrier-Schlüssel auslesen kann, die in dem Endgerät gespeichert sind. Die Schlüssel können später von Dritten zur unberechtigten Nutzung geschützter Inhalte genutzt werden. DRM-Systeme müssen also gegen Manipulationen durch die Nutzer resistent sein. Sowohl die eingesetzte Hardware als auch die DRM-Softwareprogramme müssen manipulationssicher („tamper proof") ausgestaltet sein.[385]

---

[383] Tatsächlich können die derzeitigen Verfahren nur eine Annäherung an den Originalzustand erreichen. S. dazu insgesamt *Lin/Chang* in: Wong/Delp (Hrsg.), S. 104 ff., und deren SARI-Projekt („Self-Authentication-and-Recovery Images"), s. <http://www.ctr.columbia.edu/sari>, sowie *Fridrich* in: Dittmann/Nahrstedt/Wohlmacher, S. 41 ff. m. w. N. Zum verwandten Problem des „Image Downgrading" s. oben Fn. 272.

[384] S. dazu ausführlich, auch zu asymmetrischen Authentisierungs-Verfahren, *Rankl/Effing*, S. 189 ff. Beispielsweise baut das „Content Scramble System" bei DVDs auf einem „Challenge-Response"-Verfahren auf, s. dazu unten Teil 1, D II 3 b.

[385] Einer der ersten und bekanntesten Vertreter des Ansatzes, manipulationssichere Hardware in DRM-Systemen einzusetzen, ist *Mark Stefik*, Forscher am Xerox Palo Alto Research Center (PARC). Er nennt solche Systeme „trusted systems", s. *Stefik*,

1. Manipulationssichere Hardware

Im folgenden sollen anhand zweier Beispiele – Dongles und Smartcards – allgemeine Charakteristika und Probleme manipulationssicherer Hardware dargestellt werden, die in DRM-Systemen eingesetzt werden kann. Solche Hardware kann beispielsweise in Computer, Set-Top-Boxen, eBook-Lesegeräte, DVD-Spieler, mithin in alle denkbaren Endgeräte integriert werden.

a) Dongles

Bei Computersoftware wurden insbesondere in den 80er Jahren sogenannte „Dongles“[386] eingesetzt. Dabei handelt es sich um Hardware-Bauteile, die an eine Schnittstelle eines Computers angeschlossen werden. In diesem Dongle sind Schlüssel gespeichert, die notwendig sind, um ein bestimmtes Softwareprogramm benutzen zu können.[387] Zwar ist es auch ohne den Dongle möglich, eine Kopie des Programms zu erstellen; ohne Original-Dongle ist dieses jedoch nicht nutzbar und daher wertlos.[388] Insgesamt bieten Dongles ein recht hohes Maß an Sicherheit.[389] Aufgrund der recht umständlichen Handhabung und ihrer teilweisen Fehleranfälligkeit haben sich Dongles nur bei teuren Spezialprogrammen, nicht aber im Massenmarkt durchsetzen können.[390]

Internet Dreams, S. 226 ff.; *ders.*, The Internet Edge, S. 56 ff.; *ders.*, 12 Berkeley Tech. L. J. 137, 139 ff. (1997).

[386] Zur unklaren Etymologie des Wortes s. *Schneck*, 87 Proc. IEEE 1239, 1241 (1999).

[387] *Wayner*, Digital Copyright Protection, S. 81; *Schneck*, 87 Proc. IEEE 1239, 1241 (1999); *Kaestner*, S. 4. Umfassend insbesondere *Phipps* in: Grover (Hrsg.), S. 66 ff. Neben solchen „passiven“ Dongles werden auch „aktive“ Dongles eingesetzt, die selbst bestimmte Rechenoperationen ausführen können, *Schneck*, 87 Proc. IEEE 1239, 1241 (1999). Oft werden dabei asymmetrische Verschlüsselungssysteme verwendet. Das Softwareprogramm verschlüsselt einen geheimen Wert mit einem öffentlichen Schlüssel und überträgt diesen an den Dongle. Der Dongle entschlüsselt die Daten mit seinem privaten Schlüssel und überträgt das Ergebnis zurück an die Software. Bei einem funktionsfähigen Dongle muß dieses Ergebnis mit dem ursprünglichen geheimen Wert übereinstimmen, s. *Wayner*, a. a. O., S. 83 f. Bei aufwendigeren Dongles werden ganze Teile des Programmcodes verschlüsselt, s. *Zieschang* in: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), S. 227, 233. Es gibt Hersteller, die sich auf die Herstellung solcher Dongles spezialisiert haben, z. B. PACE Anti-Piracy, <http://www.paceap.com>, Eutron, <http://www.eutron.it>, Marx Software Security, <http://www.marx.com>, und Aladdin Knowledge Systems, <http://www.aks.com/hasp>.

[388] *Raubenheimer*, NJW-CoR 1996, 174.

[389] Jedoch muß beispielsweise verhindert werden, daß ein Angreifer die Kommunikation zwischen dem Dongle und dem Softwareprogramm abhören kann und dadurch eine Simulation des Dongles erstellen kann, *Wayner*, Digital Copyright Protection S. 86.

[390] S. dazu *Phipps* in: Grover (Hrsg.), S. 65 f.

b) Smartcards

Für DRM-Systeme weitaus wichtiger sind sogenannte „Smartcards". Smartcards enthalten eine integrierte Schaltung, die über Elemente zur Datenübertragung, -speicherung und verarbeitung verfügt.[391] Auf diesen Chips können dauerhaft Daten gespeichert werden, die auch ohne Stromzufuhr erhalten bleiben.[392] Der wichtigste Vorteil von Smartcards ist, daß die in ihnen gespeicherten Daten gegen unerwünschten Zugriff und gegen Manipulation geschützt werden können.[393] Dadurch können geheime Daten in die Karte geladen werden, die nur noch intern vom Rechenwerk des Chips auf der Smartcard, nicht aber von außen ausgelesen werden können.[394] Smartcards finden heute in Pay-TV-Systemen, Telefonkarten, Mobiltelefonen, Zugangskontrollsystemen, Krankenversicherungskarten und sonstigen Mitgliedskarten Anwendung.[395] In DRM-Systemen können die einzelnen Nutzer mit Smartcards ausgestattet werden, in denen in einer manipulationssicheren Umgebung Dechiffrier-Schlüssel abgespeichert sind.[396] Viele der heutigen Pay-TV-Systeme beruhen auf diesem Prinzip.[397]

Um das Auslesen geheimer Daten aus der Smartcard und sonstige Angriffe auf deren Funktionsweise zu verhindern, existiert eine Fülle technischer Schutzmaßnahmen, von denen hier nur einige erwähnt werden sollen.[398] Einerseits existieren *passive Schutzmaßnahmen*. Viele Angriffe auf Smartcards beruhen auf physikalischen Manipulationen der Smartcard. Um dies zu verhindern, werden bei sicheren Smartcards beispielsweise interne Datenleitungen so geführt, daß sie nicht von außen kontaktierbar sind.[399] Weiterhin werden Chips in Smartcards mit Epoxidharz bedeckt,

---

391 *Rankl/Effing*, S. 47. Smartcards „sind kleine Computer in Scheckkartenformat und ohne Mensch-Maschine-Schnittstelle", *Rankl/Effing*, S. 126.

392 In sog. EEPROMs und Flash-EEPROMs, s. *Rankl/Effing*, S. 97 ff.

393 *Rankl/Effing*, S. 47. Regelmäßig ist aber die Speicherkapazität der Smartcards begrenzt und ihre Rechengeschwindigkeit nicht sehr hoch, s. *Wayner*, Digital Copyright Protection, S. 81.

394 *Rankl/Effing*, S. 47.

395 In den USA setzte die Verbreitung von Smartcards nur verzögert ein. Dies liegt auch daran, daß die grundlegenden Erfindungen für die Chipkartentechnik aus Deutschland und Frankreich stammen, *Rankl/Effing*, S. 32.

396 Auch können im Rahmen des Verschlüsselungssystems auf der Smtartcards eigenständig Rechenoperationen durchgeführt werden. Dabei findet oft das (symmetrische) Triple-DES-Vefahren Anwendung. Das asymmetrische RSA-Verfahren wird wegen seiner Rechen- und Speicherintensität seltener verwendet, asymmetrische Verfahren auf der Grundlage elliptischer Kurven sind wiederum besser geeignet, *Rankl/Effing*, S. 158, 162, 168.

397 *Wayner*, Digital Copyright Protection, S. 81.

398 Eine Auflistung möglicher Schutzmaßnahmen findet sich bei *Münch* in: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), S. 215, 222 ff.; *Ermer*, CR 2000, 126, 129 ff.

399 *Ermer*, CR 2000, 126, 130.

um Angreifern den Zugriff auf den Chip selbst unmöglich zu machen.[400] Mitunter wird auch auf sogenannte „Dummy"-Strukturen gesetzt. Das sind Elemente auf dem Halbleiter, die keine eigentliche Funktion haben, sondern nur einen Angreifer verwirren sollen. Daneben existieren *aktive Schutzmaßnahmen*. Dabei ergreift die Smartcard, die im Grunde ein Kleinstcomputer ist, Gegenmaßnahmen, sobald sie einen Angriff entdeckt. So kann beispielsweise auf die Chipoberfläche einer Smartcard eine sogenannte „Passivierungsschicht" aufgetragen werden. Für Angriffe ist es oft notwendig, die Passivierungsschicht zu entfernen. In den Chip kann jedoch ein Sensor integriert werden, der prüft, ob die Passivierungsschicht noch vorhanden ist. Ist sie nicht mehr vorhanden oder beschädigt,[401] so schaltet sich der gesamte Chip ab, was bestimmte Angriffe zuverlässig verhindert.[402] Auch muß die auf einer Smartcard enthaltene Software gegen Angriffe sicher sein. Zu diesem Zweck werden oft Datenbereiche mit Hilfe von Prüfsummen auf etwaige Manipulationen überprüft und abgeschottete Speicherbereiche erstellt, die einer Anwendung keinen unerlaubten Zugriff auf Speicherbereiche anderer Anwendungen ermöglichen.[403] Schließlich muß verhindert werden, daß auf dem Betriebssystem, das auf der Smartcard läuft, beliebige Programme ausgeführt werden können; ansonsten wäre das Einschleusen von Viren oder trojanischen Pferden möglich. Zur Lösung dieses Problems bieten sich Authentisierungs- und Signierungsverfahren an.[404]

Trotz dieser und anderer Schutzmaßnahmen sind Angriffe auf Smartcards immer wieder erfolgreich. In Deutschland tauchten beispielsweise 1998 manipulierte Telefonkarten auf, die beliebig oft kostenlos wiederaufladbar waren. Die möglichen Angriffsszenarien unterscheiden sich erheblich hinsichtlich ihrer technischen Komplexität. Um dem Leser ein Gefühl dafür zu vermitteln, mit welchen Angriffen der Betreiber eines

---

[400] Jedoch kann diese Epoxidharz-Schicht von Angreifern mit Salpetersäure entfernt werden, s. *Anderson/Kuhn* in: Proceedings of the 2nd USENIX Workshop on Electronic Commerce, S. 1, 3 f.

[401] Die Entfernung der Passivierungsschicht ist mit Hilfe sog. Lasercutter mit einer Genauigkeit von Teilen eines Mikrometers möglich, s. *Rankl/Effing*, S. 493. Auch können Mikroprobennadeln mit einer Ultraschall-Vibration die Entfernung ermöglichen, s. *Anderson/Kuhn* in: Proceedings of the 2nd USENIX Workshop on Electronic Commerce, S. 1, 4.

[402] *Rankl/Effing*, S. 488 f. Bei anderen erkannten Angriffen kann eine Smartcard so programmiert werden, daß sie den Zugriff auf die Karte sperrt oder die gespeicherten Schlüssel löscht, sobald sie einen Angriff erkennt. Dabei besteht jedoch die Schwierigkeit, abstrakt zu formulieren, wann ein Angriff vorliegt und wann nicht. S. dazu *Rankl/Effing*, S. 481. Auch können die entsprechenden Schutzmechanismen ihrerseits wieder umgangen werden; s. dazu *Zieschang* in: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), S. 227, 237.

[403] S. dazu mit Beispiel *Rankl/Effing*, S. 508 ff.

[404] Aus diesen und anderen Gründen spielen Viren und trojanische Pferde bei Smartcards derzeit keine Rolle; s. dazu *Rankl/Effing*, S. 516 f.

DRM-Systems rechnen muß, sollen im folgenden einige fortschrittliche Angriffe auf Smartcards dargestellt werden.[405]

Während des Betriebs einer Smartcard kann es vorkommen, daß verwendete Schlüssel oder andere geheime Daten vorübergehend im flüchtigen Speicher[406] der Smartcard gespeichert werden. Ein Angreifer kann auf unterschiedliche Arten versuchen, diese Daten aus dem Arbeitsspeicher auszulesen. So können unter Umständen mit Hilfe von Elektronenmikroskopen die Schaltungszustände der entsprechenden Transistoren ausgelesen werden. Als Schutz bieten sich stromführende, metallhaltige oder lichtundurchchlässige Schutzschichten über den gefährdeten Bereichen des Chips an.[407] RAM-Speicherbausteine verlieren regelmäßig ihren Dateninhalt, wenn man ihre Stromversorgung abschaltet. Dies erschwert Angriffe auf Smartcards, da die Stromabschaltung auch von der Smartcard selbst initiiert werden kann. Jedoch bleibt der Speicherinhalt nach der Stromabschaltung meistens noch einige Sekunden erhalten.[408] Auch bleibt er dauerhaft erhalten, wenn man den Speicherbaustein auf unter –60° C abkühlt.[409]

1995 wurde gezeigt, daß bestimmte Verschlüsselungssysteme erhebliche Laufzeitunterschiede aufweisen, je nachdem, welcher Schlüssel verwendet wird und welche Daten verschlüsselt werden sollen. Daraus kann ein Angreifer Rückschlüsse auf den geheimen Schlüssel ziehen, auch wenn dieser sicher in einer Smartcard abgespeichert ist (sog. „timing attack“).[410] Hier existieren aber Lösungsmöglichkeiten.[411] Ein weiterer schwerwiegender Angriff ist die sogenannte Leistungsanalyse („power analysis“), die 1998 vorgestellt wurde.[412] Dabei wird mit hoher zeitlicher Auflösung der Stromverbrauch einer Smartcard gemessen. Unter bestimmten Voraussetzungen kann aus den Änderungen im Stromverbrauch auf die internen Abläufe und verarbeiteten Daten des Prozessors

[405] Zwar sind viele der beschriebenen Angriffe inzwischen beim Entwurf neuerer Smartcards schon berücksichtigt und stellen daher oft kein ernstzunehmendes Sicherheitsrisiko mehr dar. Dennoch sollen sie im vorliegenden Zusammenhang erwähnt werden, um die Bandbreite möglicher Angriffe und die außerordentliche Komplexität, die zu ihrer Vermeidung erforderlich ist, aufzuzeigen. Einen Überblick geben *Rank/Effing*, S. 469 ff.; *Anderson/Kuhn* in: Proceedings of the 2nd USENIX Workshop on Electronic Commerce, S. 1 ff.

[406] „Random Access Memory“, RAM.

[407] *Rankl/Effing*, S. 485 ff.; *Anderson/Kuhn* in: Proceedings of the 2nd USENIX Workshop on Electronic Commerce, S. 1, 3.

[408] Zur diesbezüglichen Schwäche der Verschlüsselungsmechanismen eines VISA-Geldautomaten s. *Anderson/Kuhn* in: Christianson/Crispo/Lomas/Roe (Hrsg.), S. 125, 132 ff.

[409] S. dazu *Rankl/Effing*, S. 486; *Anderson/Kuhn* in: Proceedings of the 2nd USENIX Workshop on Electronic Commerce, S. 1, 8.

[410] *Kocher* in: Koblitz (Hrsg.), S. 104 ff. S. dazu im Überblick *Rankl/Effing*, S. 505 f.

[411] S. dazu *Rankl/Effing*, S. 505 f.

[412] Grundlegend *Kocher/Jaffe/Jun* in: Wiener (Hrsg.), S. 388 ff. Vgl. auch <http://www.cryptography.com/dpa>.

geschlossen werden.[413] Dafür ist lediglich eine Ausrüstung im vierstelligen Dollar-Bereich notwendig.[414] Gegen diesen Angriff existieren Lösungsansätze auf Hardware-[415] wie auf Softwareebene.[416]

Weiterhin können durch die Bestrahlung mit fokussierten Ionenstrahlen gezielt bitweise Manipulationen an gespeicherten Daten vorgenommen werden. Auf diese Weise kann unter bestimmten Umständen der in einem Speicherbaustein gespeicherte symmetrische Schlüssel ausgelesen werden.[417] Zwar kostet eine Apparatur zur Erzeugung und exakten Steuerung von fokussierten Ionenstrahlen mehrere Millionen Mark, sie kann aber auch tageweise an Forschungsinstituten gemietet oder von Universitätsmitgliedern mitunter kostenlos genutzt werden.[418] Bei Pay-TV-Decodern wurden solche Angriffe schon erfolgreich durchgeführt.[419] Als Schutz messen aufwendig geschützte Smartcards die Ionenstrahlung in der Umgebung und löschen bei erhöhten Werten sensible Speicherbereiche.[420] Schließlich können die Speicherzustände auf Smartcards durch eine gezielte Veränderung der Betriebstemperatur,[421] die Unterbrechung der Stromversorgung zu bestimmten Zeitpunkten[422] und die Veränderung der Taktfrequenz[423] manipuliert werden.

---

413 Teilweise wird auch zusätzlich die elektromagnetische Strahlung des Chips ausgewertet. Solche physikalischen Analysen können auch mit der mehrmaligen Eingabe veränderter Werte (wie einer PIN) kombiniert werden, um die Reaktion der Smartcard auf die unterschiedlichen Werte zu ermitteln. S. zum ganzen im Überblick *Rankl/Effing*, S. 494 ff., 504.

414 <http://www.cryptography.com/dpa/qa>.

415 Z. B. Spannungsregler, die einen gleichmäßigen Stromverbrauch sicherstellen; künstliche Stromrauschquellen; entsprechend modifiziertes halbleitertechnisches Prozessordesign, damit dieser einen kostanten Stromverbrauch aufweist.

416 U. a. die ausschließliche Benutzung von Maschinenbefehlen mit sehr ähnlichem Stromverbrauch oder die zufällige Auswahl unter mehreren möglichen Abläufen für gleiche Berechnungen. S. zum ganzen im Überblick *Rankl/Effing*, S. 496 f.

417 S. dazu *Rankl/Effing*, S. 497 f.; *Anderson/Kuhn* in: Proceedings of the 2nd USENIX Workshop on Electronic Commerce, S. 1, 5 f.

418 *Rankl/Effing*, S. 475; *Anderson/Kuhn* in: Proceedings of the 2nd USENIX Workshop on Electronic Commerce, S. 1, 5.

419 *Anderson/Kuhn* in: Proceedings of the 2nd USENIX Workshop on Electronic Commerce, S. 1, 5.

420 So ein bei IBM entwickelter Prozessor, *Smith/Weingart*, 31 Computer Networks 831, 839 (1999).

421 *Anderson/Kuhn* in: Proceedings of the 2nd USENIX Workshop on Electronic Commerce, S. 1, 2. Zur Möglichkeit einer Temperaturüberwachung s. *Rankl/Effing*, S. 490; *Smith/Weingart*, 31 Computer Networks 831, 839 (1999).

422 So konnte bei Smartcards in frühen Pay-TV-Systemen durch eine Unterbrechung der Stromzufuhr erreicht werden, daß der Pay-TV-Decoder den Empfang der Pay-TV-Kanäle nicht sperren konnte, s. *Anderson/Kuhn* in: Proceedings of the 2nd USENIX Workshop on Electronic Commerce, S. 1, 2. Zu Lösungsmöglichkeiten s. *Rankl/Effing*, S. 502 ff.; *Smith/Weingart*, 31 Computer Networks 831, 839 (1999).

423 *Anderson/Kuhn* in: Proceedings of the 2nd USENIX Workshop on Electronic Commerce, S. 1, 2; 31 *Smith/Weingart*, Computer Networks 831, 839 (1999).

Insgesamt sind für viele der dargestellten Angriffsszenarien ein großer technischer Aufwand und detailliertes technisches Wissen erforderlich, was regelmäßig nur einer kleinen Anzahl von Spezialisten zur Verfügung steht. Dennoch muß der Anbieter eines DRM-Systems davon ausgehen, daß ein potentieller Angreifer sich das notwendige Wissen und die notwendige Ausrüstung zumindest besorgen kann.[424] Daneben beruhen viele möglichen Angriffe auf Smartcards gar nicht auf physikalischen Eigenheiten der Smartcard oder unsicheren mathematischen Algorithmen; vielmehr spielen oft menschliche Fehler eine Rolle. Insbesondere kann die Sicherheit einer Smartcard durch Programmier- und Designfehler in der Hard- oder Software beeinträchtigt werden.[425]

c) Sonstige Hardware

Die ausführliche Darstellung von Schutzmaßnahmen bei Smartcards zeigen exemplarisch die Schwierigkeiten, ein umfassendes Sicherheitskonzept auf Hardwareebene einzuführen. In sonstigen Hardwarekomponenten können vergleichbare Schutzkonzepte eingesetzt werden. So sind insbesondere manipulationssichere Coprozessoren für DRM-Systeme gut geeignet.[426] Technisch betrachtet unterscheiden sich Smartcards und sichere Coprozessoren regelmäßig nur durch den höheren Komplexitätsgrad von Coprozessoren.[427] Letztlich können die dargestellten Konzepte in allen Arten von DRM-Endgeräten eingesetzt werden.

---

[424] *Rankl/Effing*, S. 475.

[425] Beispiele bei Smartcards geben *Zieschang* in: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), S. 227, 235; *Schindler* in: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), S. 241 ff.

[426] S. dazu grundlegend *Yee/Tygar* in: Proceedings of the 1st USENIX Workshop on Electronic Commerce, S. 155 ff. Vgl. weiterhin *Smith/Palmer/Weingart* in: Hirschfeld (Hrsg.), S. 73 ff.; *Smith/Weingart*, 31 Computer Networks 831 ff. (1999). Entsprechende Prozessoren werden für den Massenmarkt u. a. von IBM entwickelt, s. <http://www.research.ibm.com/secure_systems/scop.htm>.

[427] *Smith/Palmer/Weingart* in: Hirschfeld (Hrsg.), S. 73, 79. Zwischen Smartcards und sicheren Coprozessoren lassen sich hinsichtlich der Komplexität und Sicherheit noch weitere Zwischenstufen ausmachen, so beispielsweise sichere Prozessoren in PCMCIA-Steckkarten (auch „personal tokens" genannt) und spezielle Prozessoren zur Beschleunigung von Verschlüsselungsabläufen (auch „crypto accelerators"). Der sichere Coprozessor wird in ein normales PC-System integriert und steht für spezielle Berechnungen des DRM-Systems zur Verfügung. Dabei kommuniziert er mit anderen PC-Komponenten erst nach erfolgreicher gegenseitiger Authentizitäts- und Integritätsprüfung, *Yee/Tygar* in: Proceedings of the 1st USENIX Workshop on Electronic Commerce, S. 155, 166; *Smith/Weingart*, Computer Networks 31 (1999) 831, 836.

2. Manipulationssichere Software

a) Allgemeines

> *What is required are techniques that will render software execution virtually unobservable or unmodifiable on […] fundamentally unsecure platforms.*[428]

Auch die Softwarekomponenten eines DRM-Systems, die unter anderem für das Abspielen digitaler Inhalte, für die Nutzungskontrolle und die Abrechnung zuständig sind, müssen gegenüber Manipulationen resistent sein. Ein Angreifer kann versuchen, durch Beobachten des Softwareprogrammes und der von ihm belegten Speicherbereiche Informationen über dessen Funktionsweise zu erlangen. Mit diesen Informationen können technische Schutzmaßnahmen in DRM-Systemen umgangen werden. Um solche Angriffe zu verhindern, wurde es traditionell für notwendig erachtet, auf manipulationssichere Hardware zurückzugreifen.[429] Angriffe auf Software, die in einer manipulationssicheren Hardwareumgebung ausgeführt wird, sind regelmäßig unmöglich, solange der Hardwareschutz nicht geknackt wurde. Heutige Konsumenten-PCs verfügen jedoch über keinerlei manipulationssichere Hardwarekomponenten. Aus vielerlei Gründen ist es äußerst schwierig, auf dem Massenmarkt manipulationssichere PCs einzuführen. Daher wird versucht, einen gewissen Manipulationsschutz auf Softwareebene zu erreichen, so daß DRM-Systeme auch auf herkömmlichen PCs ein befriedigendes Schutzniveau bieten können.

Dafür kann ein Computerprogramm vor der Ausführung mit Hilfe von Hash-Funktionen[430] überprüfen, ob es von Angreifern verändert wurde.[431] Auch existieren Ansätze, bei denen ein Programm die Ergebnisse seiner eigenen Berechnungen auf ihre Richtigkeit überprüft und eventuell korrigiert (sogenanntes „result checking").[432] Schließlich werden Verschlüsselungsverfahren eingesetzt. Dabei wird beispielsweise der ausführbare Objektcode eines Computerprogramms in mehrere Teile unterteilt, die jeweils verschlüsselt werden.[433] Wird das Programm aufgerufen, so wird immer nur ein Teil entschlüsselt und ausgeführt. Bevor ein zweiter Teil ausgeführt wird, wird der erste Teil wieder verschlüsselt. Dadurch erhält ein Angreifer nie Zugriff auf das gesamte Programm. Dies macht sicherheitsrelevante Informationen wie Dechiffrier-Schlüssel, die über das

---

[428] *Aucsmith/Graunke*, U.S. Patent No. 5892899 (1999), Spalte 1.

[429] S. dazu *Gilmont/Legat/Quisquater* in: Wong/Delp (Hrsg.), S. 472 ff.

[430] S. dazu oben Teil 1, C III 2 a.

[431] *Collberg/Thomborson*, S. 11.

[432] S. dazu nur *Wasserman/Blum*, 44 Journal of the ACM 826 ff. (1997).

[433] Im folgenden wird ein Verfahren stark vereinfacht dargestellt, das von *Aucsmith* und *Graunke* entwickelt und von Intel patentiert wurde; s. *Aucsmith* in: Anderson (Hrsg.), S. 317 ff.; *Aucsmith/Graunke*, U.S. Patent No. 5892899 (1999); <http://developer.intel.com/software/security>. S. zum ganzen auch *Collberg/Thomborson*, S. 12.

gesamte Programm verteilt abgespeichert sind, robuster gegen Angriffe.[434] Auch kann die Ausführung des zweiten Teils eines Programms von der Ausführung des ersten Teils abhängig gemacht werden: Wenn bei der Ausführung des ersten Programmteils Manipulationen vorgenommen werden, ist die Ausführung des zweiten Programmteils nicht mehr möglich.[435] Weiterhin wird an Verfahren gearbeitet, bei denen die Programmfunktionen unmittelbar in verschlüsseltem Zustand ausgeführt werden. Eine unverschlüsselte Fassung, die zum Opfer eines Angriffs werden könnte, liegt dann gar nie vor.[436] Schließlich können auch eine genaue und fälschungssichere Dokumentierung aller Schritte, die das Softwareprogramm ausführt, speziell ausgestaltete Verschlüsselungsverfahren[437] sowie die Einschaltung vertrauenswürdiger dritter Instanzen („trusted third parties")[438] weiterhelfen. Da bei Computersoftware oft menschliche Programmierfehler Ausgangspunkt erfolgreicher Angriffe sind, ist dies ein weiterer Ansatzpunkt zur Erhöhung der Systemsicherheit.[439]

b) Code Obfuscation

Eine andere Möglichkeit, Software manipulationssicher auszugestalten, ist die sogenannte „Code Obfuscation". Softwareprogramme sind auf dem Computer des Nutzers regelmäßig nur als Maschinencode gespeichert. Dieser Code kann unmittelbar vom Computer ausgeführt werden, ist aber für Menschen nicht ohne weiteres verständlich. Will ein Angreifer verstehen, wie das Programm funktioniert und welche Schritte es ausführt, so muß er es analysieren und in eine höhere Programmiersprache zurückführen, die für einen Menschen besser verständlich ist. Dieser gesamte Analyse-Prozeß, der die ursprüngliche Entwicklung des Computerprogramms in umgekehrter Reihenfolge nachvollzieht, wird „Reverse Engineering" genannt.[440] Mit Hilfe des „Reverse Engineering" kann die Funktionsweise eines Computerprogramms untersucht werden. Das ist in

[434] *Aucsmith* in: Anderson (Hrsg.), S. 317, 320.

[435] *Aucsmith* in: Anderson (Hrsg.), S. 317, 328.

[436] Dies ist eine stark vereinfachte Darstellung eines Verfahrens aus dem Bereich der Sicherheit mobiler Software-Agenten, das derzeit nur auf ganz spezielle Funktionen anwendbar ist. Das Ziel dieses Verfahrens ist es, auf einem unsicheren Computer ein Softwareprogramm auszuführen, ohne daß der Computer „versteht", was gerade auf ihm ausgeführt wird. S. zum ganzen *Sander/Tschudin* in: Proceedings of the IEEE Symposium on Security and Privacy 1998, S. 215 ff.; *Tschudin* in: Klusch (Hrsg.), S. 431, 442 f.; *Papaioannou* in: Klusch/Kerschberg (Hrsg.), S. 247, 251 ff. Zur Sicherheit mobiler-Software-Agenten s. unten Teil 1, E III.

[437] S. zu beidem *Papaioannou* in: Klusch/Kerschberg (Hrsg.), S. 247, 251 m. w. N.

[438] S. dazu *Corradi/Cremonini/Montanari/Stefanelli*, 24 Information Systems 519, 522 (1999). S. a. *Rankl/Effing*, S. 515.

[439] *Smith/Palmer/Weingart* in: Hirschfeld (Hrsg.), S. 73, 75.

[440] Die Begriffe Disassemblierung und Dekompilierung sind damit nicht deckungsgleich. Sie betreffen nur einen kleineren Ausschnitt des Reverse-Engineering-Prozesses. S. zum ganzen *Marly*, Softwareüberlassungsverträge, Rdnr. 1042 ff.; *ders.*, Urheberrechtsschutz für Computersoftware in der Europäischen Union, S. 273 ff.

einem DRM-System aus zwei Gründen unerwünscht: Einerseits will der DRM-Betreiber verhindern, daß ein Angreifer durch das „Reverse Engineering" Kenntnisse über DRM-Softwarekomponenten erhält und damit die Sicherheit des Gesamtsystems beeinträchtigen kann. Andererseits können über ein DRM-System auch Computerprogramme als digitale Inhalte an die Nutzer vertrieben werden.[441] Mit Hilfe des „Reverse Engineering" können Angreifer Konkurrenzprodukte mit der gleichen Funktionalität erstellen beziehungsweise Teile des Computerprogramms in andere Computerprogramme integrieren.[442] Der Softwarehersteller, dessen Programm über ein DRM-System vertrieben wird, will diese unerwünschte Konkurrenz oftmals verhindern.[443]

Seit einigen Jahren werden technische Verfahren entwickelt, die das „Reverse Engineering" zumindest erschweren sollen.[444] Bei der sogenannten „Code Obfuscation"[445] wird der Quellcode eines Computerprogramms derart transformiert, daß das Programm nach der Transformation zwar funktionell identisch ist, ein „Reverse Engineering" aber deutlich erschwert wird.[446] Während herkömmliche manipulationssichere Software nach einem Angriff nicht mehr ordnungsgemäß funktioniert oder gar nicht mehr ausführbar ist, ist es das Ziel der „Code Obfuscation", ein funktional gleichwertiges Äquivalent zu schaffen, bei dem die Erforschung der Funktionsweise unmöglich gemacht wird. Zu diesem Zweck können Datenstrukturen oder die Namen von Variablen verändert, Programmklassen modifiziert oder neu geschaffen, neue Abstraktionsebenen geschaffen oder bestehende entfernt, redundanter neuer Quellcode eingefügt oder die Reihenfolge von Rechenoperationen zufällig verändert werden.[447] Es handelt sich noch um einen sehr jungen Forschungsbereich.

---

[441] Zum weiten Begriff des digitalen Inhalts s. oben Einführung, bei Fn. 46 ff.

[442] *Collberg/Thomborson/Low*, S. 1. Zwar ist bei herkömmlichen Programmiersprachen das „Reverse Engineering" in der Regel sehr aufwendig und daher nicht weit verbreitet, *Collberg/Thomborson/Low*, S. 1. Im Gegensatz dazu ist bei der plattformunabhängigen Programmiersprache Java, die in den letzten Jahren populär geworden ist, das Reverse Engineering sehr einfach, da viele Informationen, die im Quellcode eines Java-Programms enthalten sind, auch im endgültigen sog. Bytecode enthalten sind. Damit steigt die Gefahr, die für Urheber von Computerprogrammen vom Reverse Engineering ausgehen, deutlich an, *Collberg/Thomborson*, S. 5; *Collberg/Thomborson/Low*, S. 1, auch zu den technischen Grundlagen.

[443] Um das „Reverse Engineering" zu unterbinden, versuchen Softwarehersteller seit langem, es durch entsprechende Lizenzverträge und gesetzliche Verbote (vgl. § 69 e UrhG) zu verhindern.

[444] Neben dem im folgenden vorgestellten Verfahren existieren noch andere Ansätze, so beispielsweise der auf einer Verschlüsselung von Funktionen aufbauende Ansatz von *Sander/Tschudin* in: Aucsmith (Hrsg.), S. 111 ff.

[445] Englisch für Verwirrung, Vernebelung.

[446] S. dazu *Collberg/Thomborson*, S. 5 ff.

[447] Ausführlich dazu *Collberg/Thomborson/Low*, S. 4 ff.; *Mambo/Murayama/Okamoto* in: Proceedings of the New Security Paradigms Workshop 1997, S. 23, 25 ff. Die „Code Obfuscation" kann keinen absoluten Schutz gegen das „Reverse Engineering"

3. Zusammenfassung

No provably tamper-proof system exists.[448]

Der Entwickler eines DRM-Systems muß damit rechnen, daß professionelle Angreifer erhebliche finanzielle Mittel aufwenden werden, um den technischen Schutz des Systems zu umgehen. Es ist praktisch unmöglich, ein ganzes System so zu bauen, daß perfekte Sicherheit herrscht.[449] Zwar existieren in extrem sicherheitsrelevanten Bereichen manipulationssichere Hardwarelösungen, die ein sehr hohes Maß an Sicherheit bieten.[450] Diese sind jedoch für den normalen E-Commerce nicht geeignet. Manipulationssichere Hardwareumgebungen sind oft teuer und mitunter schwierig zu handhaben. Für den Urheberschutz konnten sie daher zumindest bisher noch keine größere Bedeutung erlangen.[451] Ein weiteres Problem manipulationssicherer Hardware ist, daß im Vergleich zu herkömmlichen Computerumgebungen viele Rahmenbedingungen – Interaktion zwischen manipulationssicherer Hardware und anderen unsicheren Hard- und Softwarekomponenten, Auslieferung, Installation und Initialisierung der manipulationssicheren Hardware, Aktualisieren von Hard- oder Software – sehr viel komplizierter sind.[452]

Die Entwicklung manipulationssicherer Software befindet sich erst an ihrem Anfang.[453] Die Sicherheit von Verfahren zur „Code Obfuscation" sind heute weder theoretisch noch praktisch beweisbar. Wissenschaftliche Veröffentlichungen zu dem Thema sind rar, auch wenn die Verfahren in der Praxis relativ häufig eingesetzt werden. Dies liegt daran, daß die eingesetzten Methoden weder sicher genug sind noch über ein entsprechendes theoretisches Fundament verfügen, um in einer breiteren Öffentlichkeit dargestellt werden zu können. Der gesamte Bereich der manipulationssicheren Software ist heute noch keine exakte Wissenschaft und wird von Kennern der Materie eher als „schwarze Magie" bezeichnet. Bei entsprechendem Aufwand können diese Verfahren heute alle geknackt

---

bieten. Auch werden die Programme durch Obfuscation-Techniken oft etwas langsamer, *Collberg/Thomborson*, S. 3. Entsprechende Hilfsmittel existieren für unterschiedliche Programmiersprachen, für Java z. B. SourceGard von 4thPass, <http://www.4thpass.com/sourceguard>, für C <http://archiv.leo.org/pub/comp/usenet/comp.sources.misc/opqcp/>. Einen Überblick über weitere Hilfsmittel geben <http://www.cs.arizona.edu/~collberg/Research/Obfuscation/Resources.html> und <http://www.meurrens.org/ip-Links/java/codeEngineering/obfusc.html#secObfuscators>.

[448] *Smith/Weingart*, 31 Computer Networks 831, 838 (1999)

[449] *Rankl/Effing*, S. 469; *Anderson/Kuhn* in: Christianson/Crispo/Lomas/Roe (Hrsg.), S. 125; s. a. *Baylin/McCormac/Maddox*, S. 218.

[450] Z. B. bei der Sicherung vor dem unberechtigtem Zünden atomarer Waffen, s. dazu *Anderson/Kuhn* in: Proceedings of the 2nd USENIX Workshop on Electronic Commerce S. 1, 6 f.

[451] S. a. *Federrath*, ZUM 2000, 804, 805. Eine Ausnahme bildet der Pay-TV-Bereich.

[452] S. dazu im Überblick *Smith/Palmer/Weingart* in: Hirschfeld (Hrsg.), S. 73, 80 ff.; *Smith/Weingart*, 31 Computer Networks 831, 839 ff., 846 ff. (1999).

[453] *Collberg/Thomborson*, S. 13.

werden. Derzeit geht es allenfalls darum, den Aufwand, der für eine Umgehung der manipulationssicheren Software getrieben werden muß, nach und nach zu erhöhen. Manipulationssichere Hard- und Software bieten daher keinen umfassenden Schutz, sondern können nur ein Baustein unter vielen für ein umfassendes DRM-System sein.[454]

V. Suchsysteme (copy detection)

Das vornehmliche Ziel von DRM-Systemen ist, die Erstellung unberechtigter Kopien digitaler Inhalte zu verhindern („pre-infringement control"). Jedoch können auch Komponenten eingesetzt werden, die der Ermittlung schon erstellter unberechtigter Kopien dienen („post-infringement control").[455] Zu diesem Zweck können Suchsysteme eingesetzt werden, die im Internet nach unberechtigten Kopien digitaler Inhalte suchen. Solche Suchsysteme können noch zu anderen Zwecken eingesetzt werden, die im folgenden ebenfalls kurz dargestellt werden.

1. Suche zur Feststellung rechtswidriger Kopien

Suchsysteme können im Internet nach digitalen Inhalten suchen, die dort ohne Berechtigung angeboten oder genutzt werden. Dafür existieren Suchmaschinen, die das Internet systematisch auf Texte, Audio- und Videodateien durchsuchen. Bei einem anderen Ansatz bettet der Inhalteanbieter in seine Inhalte digitale Wasserzeichen ein, die Metadaten hinsichtlich des Inhalts und der Rechteinhaber enthalten. Sind diese Wasserzeichen ausreichend robust, so kann ein Raubkopierer diese nicht entfernen. Mit Hilfe einer Suchmaschine können dann Inhalte im Internet aufgespürt und auf solche Wasserzeichen untersucht werden.[456] Findet die Suchmaschine einen Inhalt mit eingebettetem Wasserzeichen, so wird überprüft, ob der Anbieter oder Nutzer des digitalen Inhalts über die erfoderlichen Nutzungsrechte verfügt. Ist dies nicht der Fall, können rechtliche Schritte gegen den Anbieter und/oder den Nutzer unternommen werden. Solche Verfahren werden schon heute von der Film- und Musikindustrie sowie von Verwertungsgesellschaften eingesetzt.[457]

---

[454] *Anderson/Kuhn* in: Proceedings of the 2nd USENIX Workshop on Electronic Commerce, S. 1, 10.

[455] Auch digitale Fingerabdrücke und das „traitor tracing" sind im Bereich der „post-infringement control" anzusiedeln, wenn sie zum Ziel haben, Raubkopierer zu identifizieren. S. dazu oben Teil 1, C II 3 b, und C II 3 c bb.

[456] Ein solches System bietet DigiMarc für den Bildbereich unter dem Namen „MarcSpider" an, s. <http://www.digimarc. com/imaging/prspider.htm>. S. zur Robustheit allgemein oben Teil 1, C II 2 b bb 2 b. Solche Verfahren können durch die sog. „Mosaik-Attacke" umgangen werden, s. dazu oben Fn. 292.

[457] So z. B. der „MusicBot" der amerikanischen Verwertungsgesellschaft BMI, s. <http://www.bmi.com/iama/webcaster/technology/musicbot.asp>. Ein Unternehmen, das solche Dienstleistungen anbietet, ist die britische „Copyright Control Services", <http://www.copyrightcontrol.com>. Ein Softwareprodukt, das solche Suchvor-

Bauen Suchverfahren auf eingebetteten digitalen Wasserzeichen auf, so sind sie mit den allgemeinen Problemen von Wasserzeichenverfahren belastet: Regelmäßig sind digitale Wasserzeichen heute nicht ausreichend sicher und robust. Angreifer können die Wasserzeichen entfernen und die Suche nach markierten Inhalten damit unmöglich machen. Daher werden in letzter Zeit insbesondere für den Musikbereich[458] Verfahren entwickelt, die eine Suche nach rechtswidrigen Kopien erlauben, ohne daß an den Musikdateien selbst Veränderungen vorgenommen werden müssen.[459] Bei diesen Verfahren, die mitunter „audio fingerprinting" genannt werden, extrahiert ein Softwareprogramm aus einer Musikaufnahme charakteristische akustische Merkmale und speichert sie in einer Datenbank ab. Der Fingerabdruck repräsentiert akustische Merkmale, die auch für den menschlichen Hörer wahrnehmbar sind. Damit sind diese Verfahren eng verwandt mit den oben erwähnten Verfahren zur „content verification".[460] Auch wenn ein Nutzer die Musikdatei verändert, komprimiert, in ein anderes Datenformat konvertiert, neu aufnimmt oder andere Manipulationen an ihr vornimmt, ändert sich der „audio fingerprint" der Musikaufnahme nicht. Eine Suchmaschine kann das Internet nach Musikdateien durchsuchen und durch den „audio fingerprint" feststellen, um welches Musikstück es sich dabei handelt. Mit dieser Information kann herausgefunden werden, wer die Rechteinhaber dieses Musikstücks sind und ob es sich bei der gefundenen Datei um eine rechtmäßig Kopie handelt.[461] Im Vergleich zu Suchsystemen, die auf digitalen Wasserzeichen aufbauen, sind „audio fingerprint"-Verfahren vielversprechend: Der Nutzer erhält digitale Inhalte, die für das Suchsystem in keiner Weise verändert werden mußten. Damit ist es einem Angreifer unmöglich, et-

gänge automatisiert, ist „BaySpider" des kalifornischen Unternehmens BayTSP, <http://www.baytsp.com/products/main/bayspider.htm>. Ein Verfahren für den Textbereich ist der im Rahmen des Stanford Digital Library Projektes entwickelte „Stanford Copy Analysis Mechanism" (SCAM), s. *Garcia-Molina/Ketchpel/Shivakumar*, Safeguarding and Charging for Information on the Internet, in: Proceedings of ICDE 1998, S. 182, 187 ff., und <http://www-db.stanford.edu/~shiva/SCAM/scamInfo.html>. S. zum ganzen auch *Bechtold*, ZUM 1997, 427, 445.

458 Die Verfahren können grundsätzlich aber auch bei anderen digitalen Inhalte eingesetzt werden.

459 Wissenschaftliche Veröffentlichungen zu diesem Thema sind äußerst rar; s. jedoch *Wold/Blum/Keislar/Wheaton* m. w. N. Einige sehr kleine Unternehmen entwickeln solche Verfahren, u. a. Relatable, <http://www.relatable.com>, Cantametrix, <http:// www.cantametrix.com> Freetantrum von eTantrum, <http://freetantum.org>, Tuneprint, <http://www.tuneprint.com>, Musclefish, <http://www.musclefish.com>, und Audible Magic, <http://www.audiblemagic.com>.

460 S. oben Teil 1, C III 1 a. Insbesondere können Verfahren eines „visual" oder „robust hash" zu dem hier beschriebenen Zweck eingesetzt werden; s. dazu oben Fn. 368.

461 Daneben können „audio fingerprint"- und „visual hash"-Verfahren auch zu anderen Zwecken eingesetzt werden, u. a. für Suchsysteme zur Nutzungsregistrierung (s. unten Fn. 467) oder zur Verwaltung von Musikstücken auf Nutzerrechnern.

waige Markierungen zu entfernen und das Suchsystem zu kompromittieren. Weiterhin können solche Verfahren bezüglich digitaler Inhalte eingesetzt werden, die schon bisher im Internet verfügbar waren, ohne in irgendeiner Weise technisch geschützt zu sein (beispielsweise Musik-MP3-Dateien). Aus diesen Gründen hat Napster solche Verfahren in sein Filtersystem integriert, um so den Zugriff auf unberechtigte Kopien von Musikstücken über Napster weiter zu erschweren.

Mitunter werden auch weitergehende Ansätze vorgeschlagen. So könnten die beschriebenen Suchverfahren auch in Netzwerkkomponenten (Router etc.) integriert werden. Diese würden den gesamten Datenverkehr im Internet auf urheberrechtlich verletzende Materialien durchsuchen und eventuell die entsprechenden Rechteinhaber kontaktieren.[462] Solche Ansätze scheitern jedoch regelmäßig an der zu hohen Belastung der Netzwerkkomponenten und den damit verbundenen Performance-Einbußen.[463]

---

[462] S. *Matsui/Takashima*, 11 NTT Review 134, 135 (1999) m. w. N. Von diesem Ansatz sind Systeme zu unterscheiden, bei denen aufgrund sog. Negativlisten der Zugriff auf urheberrechtsverletzende Webseiten verweigert wird. Ein solches Filtersystem wird seit 1999 von der deutschen Landesgruppe der International Federation of the Phonographic Industry (IFPI) unter dem Namen „Rights Protection System" (RPS) propagiert, s. dazu *Bortloff*, GRUR Int. 2000, 665, 669 f.; *Lippert*, CR 2001, 478 ff.; <http://www.ifpi.de/recht/re-22.htm>; Fitug Fact Sheet, <ftp://ftp.fitug.de/pub/eu/RPS02.PDF>; <http://www.fitug.de/news/pes/012000-l.html>. Danach erstellt die IFPI eine Liste ausländischer Webseiten (URLs), die nicht lizenzierte Musikdateien anbieten. Diese Liste wird in die Cachingfunktion von Servern der deutschen Internet Service Provider integriert. Ruft der Nutzer die URL einer Musikdatei auf, so prüft der Cache, ob die URL auf der Negativliste steht. Ist dies der Fall, so wird der Zugang zu dieser Adresse und damit der Musikdatei von Deutschland aus verweigert, s. *Bortloff*, GRUR Int. 2000, 665, 669. Das von der IFPI auch als „virtuelle Grenzbeschlagnahme" bezeichnete RPS fungiert damit als Filtersystem. S. dazu auch unten Fn. 2267.

[463] Noch weitergehend ist der Vorschlag von *Kuhn/Anderson* in: Aucsmith (Hrsg.), S. 124, 136 f.; *Petitcolas/Anderson/Kuhn*, 87 Proceedings of the IEEE 1062, 1068 (1999): Herkömmliche Röhrenbildschirme geben während ihres Betriebes ständig elektromagnetische Strahlung ab. Schon seit den 60er Jahren ist bekannt, daß mit entsprechender Ausrüstung das auf dem Bildschirm angezeigte Bild noch in größerer Entfernung rekonstruiert werden kann. Die Autoren schlagen für Computersoftware vor, mit Hilfe steganographischer Verfahren in die Bildschirmausgabe eines Computerprogramms einen digitalen Fingerabdruck mit einer individuellen Seriennummer einzubetten, der vom Nutzer nicht bemerkt wird. Bei entsprechender Konfiguration und Umweltbedingungen kann dieses Signal noch in einer Entfernung von einigen Dutzend Metern bis hin zu wenigen Kilometern empfangen werden. Wenn sich die Rechteinhaber mit der entsprechenden Ausrüstung in einem unauffälligen Kleinwagen in Wohngebiete begeben, könnten sie durch die Auswertung der elektromagnetischen Strahlung von Bildschirmen in der Umgebung überprüfen, ob ein Nutzer Software mit einer illegal kopierten oder ganz ohne Seriennummer benutzt. Für dieses sehr weitgehende Verfahren haben *Kuhn* und *Anderson* in Großbritannien die Erteilung eines Patents beantragt, s. *Kuhn/Anderson*, UK Patent Application GB9722799.5 vom 29. 10. 1997 (Patent noch nicht erteilt).

2. Suche zur Feststellung von Integritätsverletzungen

Suchmaschinen können im WWW auch gezielt nach Inhalten suchen, die von Nutzern verändert wurden.[464] Dafür spürt die Suchmaschine Inhalte auf, die mit einem robusten Wasserzeichen versehen wurden, das Informationen über einen bestimmten Rechteinhaber enthält. Dann sucht sie in diesen Inhalten nach einem eingebetteten zweiten, jedoch fragilen Wasserzeichen.[465] Ist dieses zweite Wasserzeichen vorhanden, wurde der Inhalt nicht verändert. Fehlt es, so ist die Integrität des Inhalts nicht gewährleistet.[466]

3. Suche zur Nutzungsregistrierung

Schließlich können Suchsysteme eingesetzt werden, um Nutzungsvorgänge zu registrieren. So könnten zum Beispiel bei Musikübertragungen im Internet durch Internet-Radio-Stationen die übertragenen Musikdatenströme ein digitales Wasserzeichen enthalten, das Informationen über Inhalt und Rechteinhaber enthält. Dieses Wasserzeichen könnte von Rechteinhabern oder Verwertungsgesellschaften ausgewertet werden und als Grundlage für ein individuelles Vergütungssystem zwischen Rechteinhabern und Internet-Radio-Station dienen (sogenanntes „broadcast monitoring").[467]

VI. Zahlungssysteme

DRM-Systeme erlauben die Nutzung digitaler Inhalte regelmäßig nur gegen die Zahlung eines bestimmten Geldbetrages. Dabei kann die einzelne Nutzung abgerechnet werden („pay per use"), oder es kann ein genereller Zugang, beispielsweise nach Zahlung einer monatlichen Pauschale, gewährt werden („pay per subscription").[468] Dafür bieten sich unterschied-

[464] Zur Notwendigkeit, die Integrität digitaler Inhalte in DRM-Systemen zu schützen, s. oben Teil 1, C III 1 a.

[465] Zum fragilen Wasserzeichen s. oben Teil 1, C III 2 c.

[466] Vgl. *Dittmann*, S. 145.

[467] *Langelaar/Setyawan/Lagendijk*, IEEE Signal Processing Magazine September 2000, 20 f. Ein solches System wurde 1994 bei EMI unter dem Namen „Identification Coding, Embedded" (ICE) entwickelt, s. dazu *Mintzer/Braudaway/Bell*, 41 Comm. ACM 57, 62 (July 1998), *Bing*, 4 International Journal of Law and Information Technology 234, 246 f. (1996) und *Willard*. Daneben können auch die oben dargestellten „audio fingerprint"- und „visual hash"-Verfahren zur Nutzungsregistrierung eingesetzt werden, s. oben Fn. 461.

[468] Welches dieser Modelle eingesetzt wird, hängt nicht zuletzt vom jeweiligen Geschäftsmodell und der Marktsituation ab. So kann es für ein Unternehmen im Vergleich zu einem „pay per use"-Modell, der auf der Micropayment-Abrechnung der individuellen Nutzung eines bestimmten Inhalts beruht, gewinnbringender sein, die Inhalte zu bündeln und diese dann im Abonnement zu verkaufen; s. dazu *Fishburn/Odlyzko/Siders* in: Kahin/Varian (Hrsg.), S. 167 ff.; *Fishburn/Odlyzko*, 13 Economic Theory 447 ff. (1999). Auch bevorzugen Nutzer mitunter den „pay per subscription"-Ansatz, selbst wenn eine individuelle Abrechnung für sie billiger käme. Dabei überschätzen sie

liche Zahlungssysteme an, die von monatlichen Rechnungen über Bankeinzug und Kreditkarten bis hin zu rein elektronischen Zahlungsmitteln reichen.[469] Daneben existieren Möglichkeiten indirekter Erlösformen wie die Finanzierung über eingeblendete Werbung, über den Verkauf von Nutzungsprofilen durch den DRM-Betreiber an dritte Unternehmen,[470] über die Vermittlung von Transaktionen[471] und ähnliches. Darauf soll im folgenden nicht näher eingegangen werden.[472]

Da die jeweils eingesetzten Zahlungssysteme vom technischen Schutz eines DRM-Systems weitgehend unabhängig operieren, soll nur ein kurzer Überblick über mögliche elektronische Zahlungssysteme gegeben werden.[473] So existieren Verfahren, mit denen Kreditkartendaten in sicherer Weise über das Internet übertragen werden können. Diesem Zweck dient insbesondere das „Secure Electronic Transaction"-System (SET), das 1997 von Visa und Mastercard veröffentlicht wurde. SET ist ein softwarebasiertes System zur gesicherten elektronischen Bezahlung auf Kreditkartenbasis im Internet und privaten Netzen.[474] Weiterhin existieren Zahlungssysteme, die auf spezieller Konsumentenhardware aufbauen. In Deutschland gehören zu dieser Kategorie die in ec-Karten integrierte Geldkarte sowie die Zahlungsfunktionen in Telefonkarten.[475] Auch

unbewußt die Häufigkeit, mit der sie den Dienst nutzen werden, oder sie wollen sich nicht bei jeder Nutzung erneut die Kostenfrage stellen; s. *Fishburn/Odlyzko*, 13 Economic Theory 447, 448 (1999) m. w. N. Beim Angebot von Musik in DRM-Systemen läßt sich deutlich eine Entwicklung von „pay per use"-Modellen hin zu Abonnement-Modellen erkennen.

469 *Bechtold*, GRUR 1998, 18, 20.

470 Dabei sammelt die DRM-Software beim Nutzer Daten über dessen Nutzungsgewohnheiten. Dieses Nutzerprofil wird an den DRM-Anbieter übertragen und von diesem an dritte Unternehmen verkauft oder selbst zur Erstellung personalisierter Werbung verwendet.

471 So kann eine DRM-Software einem Nutzer beim Abspielen eines Musikstücks das Cover einer CD anzeigen, auf dem dieses Musikstück enthalten ist. Klickt der Nutzer mit der Maus auf dieses Cover, so wird er automatisch zu einem bestimmten Händler im Internet weitergeleitet, bei dem er die CD erwerben kann. Für die Vermittlung dieses Kunden zahlt der Händler an den DRM-Systembetreiber einen geringen Betrag.

472 S. dazu im Überblick *European Communication Council*, S. 26 ff., 167 ff. Diese indirekten Erlösformen können auch mit herkömmlichen Zahlungssystemen kombiniert werden.

473 S. dazu auch *Edgar*; *Sutter*. Zum Einsatz elektronischer Zahlungsmittel in digitalen Bibliotheken und DRM-Systemen s. *Endres/Fellner*, S. 335 ff.

474 S. dazu *Zwißler*, DuD 1998, 711; *Wayner*, Digital Cash, S. 159 ff.; *O'Mahoney/Peirce/Tewari*, S. 101 ff.; *Bundesamt für Sicherheit in der Infomationstechnik*, S. 32 ff.; *Pichler*, S. 69 ff.; *Edgar*, S. 6 f.

475 S. dazu *Gentz*, DuD 1999, 18; *Neumann*, S. 18 f. Im internationalen Bereich ist insbesondere das inzwischen zu MasterCard gehörende Mondex-System, <http://www.mondex.com>, zu erwähnen; s. dazu *Wayner*, Digital Cash, S. 210 ff.; *O'Mahoney/Peirce/Tewari*, S. 183 ff.

existieren rein softwarebasierte Ansätze für „digitales Geld".[476] Dabei entspricht eine „digitale Banknote" im wesentlichen einer digital signierten und eindeutigen Seriennummer.[477] Solche Systeme eignen sich als Online-Zahlungssystem im Internet und kommen in ihrer Funktionalität und ihren Eigenschaften dem realen Geld sehr nahe.[478] Auch existieren sogenannte „Micropayment"-Systeme. Diese erlauben die Abrechnung von Pfennigbeträgen oder sogar von Pfennigbruchteilen.[479] Schließlich können zur Zahlung in DRM-Systemen digitale Geschenkgutscheine, Werbe- und Treueprämien sowie Vielfliegermeilen und ähnliches verwendet werden.[480]

---

[476] Solche Systeme werden u. a. angeboten von eCash Technologies, Inc. – <http://www.ecashtech.com>, <http://www.ecash.de> (früher DigiCash) –, das von der Deutschen Bank 24 erprobt wurde. Zu rechtlichen Problemen von digitalem Geld s. *Pichler*; *Neumann*; s. a. *Winn*, 14 Berkeley Tech. L. J. 675 ff. (1999). Zu den technischen Grundlagen und den Sicherheitsanforderungen s. umfassend *Wayner*, Digital Cash; *O'Mahoney/Peirce/Tewari*; *Stolpmann*; *Bundesamt für Sicherheit in der Informationstechnik*; im Überblick *Edgar*, S. 8 ff.

[477] *Hagemann/Schaup/Schneider*, DuD 1999, 5, 7.

[478] *Hagemann/Schaup/Schneider*, DuD 1999, 5, 7. Im folgenden sei die Funktionsweise von digitalem Geld am Beispiel des Verfahrens erklärt, das bei eCash eingesetzt wird und maßgeblich von *David Chaum* entwickwelt wurde. Bei eCash generiert der Kunde mit einer speziellen Software eine digitale Münze mit einer von ihm bestimmten Werthöhe, die mit einer eindeutigen Seriennummer versehen ist. Diese digitale Münze schickt der Kunde an seine Bank, die ihn mit ihrer digitalen Signatur versieht und das Ergebnis dem Kunden zurücksendet. Der Kunde kann nun mit der Münze bezahlen, indem er einem Händler (oder auch einer anderen Privatperson) die Seriennummer und die Signatur der Bank mitteilt. Mit diesen Informationen kann der Händler das digitale Geld bei der Bank einlösen. Tatsächlich ist das bei eCash eingesetzte Verfahren sehr viel komplexer. Insbesondere wird durch sog. „blinde Signaturen" die Anonymität des Zahlungsvorganges sichergestellt, s. dazu unten Fn. 717. Auch muß verhindert werden, daß ein Händler das digitale Geld doppelt bei der Bank einlösen kann oder daß ein Kunde einen digitalen Geldschein auf seinem Computer vervielfältigt. S. dazu im Überblick *Selke*, S. 151 f; *Bundesamt für Sicherheit in der Infomationstechnik*, S. 37 ff.; *Pichler*, S. 4 ff.; s. im einzelnen *O'Mahoney/Peirce/Tewari*, S. 146 ff.; *Wayner*, Digital Cash, S. 189 ff.; *Knorr/Schläger*, DuD 1997, 396, 399 f. Daneben existiert eine Vielzahl anderer digitaler Geldsysteme, deren technischer Aufbau sich teilweise erheblich von dem hier dargestellten unterscheidet. Zu dem auch in Deutschland bekannten, rein kontenbasierten CyberCash, das jedoch Ende 2000 sein digitales Geldprojekt einstellte, s. *Hagemann/Schaup/Schneider*, DuD 1999, 5, 8; *Wayner*, Digital Cash, S. 141 ff.; *Bundesamt für Sicherheit in der Infomationstechnik*, S. 40 ff.; *Pichler*, S. 51 ff.

[479] Z.B. das Millicent-System von Compaq, <http://www.millicent.com>, s. dazu *Bundesamt für Sicherheit in der Infomationstechnik*, S. 46 ff.; *Wayner*, Digital Cash, S. 217 ff.; *O'Mahoney/Peirce/Tewari*, S. 191 ff.; *Pichler*, S. 80 ff; *Edgar*, S. 12 f.; weiterhin das IBM Micro Payments System, <http://www-4.ibm.com/software/webservers/commerce/payment/mpay/index.htm>. Zu den Micropayment-Aktivitäten des W3C s. <http://www.w3.org/ECommerce/Micropayments>.

[480] Dafür werden Systeme entwickelt, in denen die digitale Ausgabe, Verwahrung und Einlösung solcher Prämien standardisiert wird. In einem solchen System kann der Kunde eine digitale Werbeprämie oder einen Geschenkgutschein nicht nur bei dem Unternehmen einlösen, das diese Prämie ausgegeben hat. Vielmehr stellt das System

Insgesamt existiert eine Vielzahl neuer Zahlungssysteme, die auch ausreichende Sicherheitsvorkehrungen bieten. Dennoch ist es in den letzter Zeit um alternative Zahlungssysteme im Internet ruhiger geworden. Der weitaus größte Teil aller Zahlungen im Internet erfolgt heutzutage mittels Kreditkarte.[481]

VII. Integrierte E-Commerce-Systeme

Ein DRM-System muß über Mechanismen verfügen, mit denen ein Nutzer computergestützt den gewünschten digitalen Inhalt identifizieren und einen entsprechenden Anbieter suchen kann. Interessiert sich der Nutzer für den digitalen Inhalt, sollte er über die Vertragsbedingungen informiert werden und eventuell notwendige Vertragsverhandlungen führen können. Schließlich muß das DRM-System auch die Vertragsabwicklung unterstützen. All diese Stadien in einem DRM-System sollten idealiter computergestützt ablaufen können. Die herkömmlichen Stadien der Vertragsanbahnung, -aushandlung und abwicklung müssen in elektronischen Prozessen abgebildet werden. Ein DRM-System benötigt ein umfassendes E-Commerce-System. Für solche Systeme existieren mehrere Standards.

1. Electronic Data Interchange (EDI)

„Electronic Data Interchange" (EDI) ist ein Standard, der bis in die 70er Jahre zurückreicht und den elektronischen Datenaustausch strukturierter geschäftlicher Informationen ermöglicht (zum Beispiel elektronischer Austausch von Bestellungs-, Lieferbestätigungs- und Rechnungsdokumenten). Er wird in vielen Industriesektoren (insbesondere im Bankenwe-

sicher, daß die Prämie als Zahlungsmittel von möglichst vielen Unternehmen anerkannt wird. Im Rahmen der „Trade Working Group" der IETF wird ein solches System unter dem Namen „generic rights trading" entwickelt, das in XML realisiert wird. Die Prämien werden dort als „electronic rights" bezeichnet. S. dazu *Fujimara*; *Matsuyama/Fujimara* in: Proceedings of the 1st ACM Conference on Electronic Commerce, S. 110 ff. Um den Mißbrauch digitaler Prämien zu verhindern (gefälschte oder doppelt eingelöste Prämien, Vervielfältigung einer Prämie, Veränderung des Prämieninhalts), sind technische Schutzmaßnahmen erforderlich, die in mancher Hinsicht den technischen Schutzmaßnahmen in DRM-Systemen ähneln. So wird u. a. auf Verschlüsselung, digitale Signaturen und manipulationssichere Hardware wie Smartcards gesetzt. S. dazu *Fujimara*, S. 4 ff., 10; *Terada/Kuno/Hanadate/Fujimara* in: Domingo-Ferrer/Chan/Watson (Hrsg.), S. 51 ff.

[481] Regelmäßig werden die Kreditkartendaten dabei mit Hilfe des von Netscape entwickelten „Secure Sockets Layer (SSL)"-Protokolls übertragen, s. dazu *Wayner*, Digital Cash, S. 111 ff.; *O'Mahoney/Peirce/Tewari*, S. 71 ff. Eine darauf aufbauende Standardisierung stellt das „Transport Layer Security"-Protokoll TLS dar, s. dazu *Dierks/Allen*, RFC 2246 und die TLS Working Group der IETF, <http://www.ietf.org/html.charters/tls-charter.html>. Selbst das von Kreditkartenunternehmen entwickelte SET konnte sich bisher nicht durchsetzen. Oftmals werden Kreditkartendaten auch völlig ungeschützt übertragen.

sen, aber auch im Automobilbereich und im Transportwesen) verwendet.[482] Die hohen Kosten und die Komplexität des EDI-Systems führten jedoch – neben anderen Faktoren – dazu, daß sich EDI bis heute nur für den Datenverkehr zwischen großen Unternehmen sowie im Behördensektor hat durchsetzen können.[483] Zwar wird vielfach daran gearbeitet, EDI mit XML und dem ECommerce im allgemeinen kompatibel zu machen.[484] Insgesamt ist EDI jedoch stark auf den „business-to-business"-Bereich zugeschnitten.[485]

2. XML-basierte Systeme

Die „eXtensible Markup Language" (XML) ist eine vom W3-Konsortium (W3C)[486] spezifizierte Meta-Beschreibungssprache für strukturierte Daten.[487] Mittelfristig wird erwartet, daß XML die im WWW verwendete „Hypertext Markup Language" (HTML), die selbst einen XML-Dialekt darstellt, ersetzen wird. Insbesondere soll XML auch die Grundlage für zahlreiche E-Commerce-Anwendungen werden.

Speziell für den DRM-Bereich ist das „Internet Open Trading Protocol" (IOTP) von Interesse, das auf XML aufbaut. Die erste Version von IOTP wurde im April 2000 veröffentlicht.[488] Inzwischen existieren mehrere Pilotprojekte, die IOTP verwenden.[489] IOTP stellt einen interoperablen Rahmen für den elektronischen Handel über das Internet zur Verfügung.[490] Es definiert Inhalt, Format und Abfolge von Nachrichten, die zwischen den Parteien eines elektronischen Handels im Internet anfal-

[482] Tatsächlich ist EDI nur ein Sammelbegriff für unterschiedliche Systeme und Standards. Am weitesten verbreitet ist der UN/EDIFACT-Standard („Electronic Data Interchange for Administration, Commerce and Transport"). S. zum ganzen *Kilian* in: Kilian/Heussen (Hrsg.), Kap. 23; *Cruellas/Kesterson/Medina/Rubia*, 38 Jurimetrics J. 497 (1998); zu EDI aus ökonomischer und juristischer Sicht s. *Kilian/Picot/Neuburger/Niggl/Scholtes/Seiler*. Informationen sind bei der Deutschen EC/EDI-Gesellschaft e. V., <http://www.dedig.de>, erhältlich.

[483] *Cruellas/Kesterson/Medina/Rubia*, 38 Jurimetrics J. 497, 501 (1998).

[484] S. die ebXML-Initative von UN/CEFACT und OASIS, <http://www.ebxml.org>; s. weiterhin <http://www.xmledi-group.org>; *Glushko/Tenenbaum/Meltzer*, 42 (3) Comm. ACM 106, 107 (März 1999).

[485] Da sich die vorliegende Arbeit schwerpunktmäßig mit DRM-Systemen im „business-to-consumer"-Bereich beschäftigt, wird auf EDI nicht weiter eingegangen.

[486] Zum W3C s. oben Teil 1, C II 2 a cc.

[487] S. dazu im kurzen Überblick *Fox*, DuD 2000, 609. Nähere Informationen sind beim W3C unter <http://www.w3.org/XML> erhältlich.

[488] *Burdett*, RFC 2801.

[489] Ein groß angelegtes E-Commerce-Projekt, das auf IOTP aufbaut, ist das japanische „Standard Smart Card Integrated Settlement System" – SMILE. S. dazu und zu anderen Projekten *Burdett/Eastlake/Goncalves*, S. 16 f.

[490] S. allgemein *Burdett/Eastlake/Goncalves*; *Burdett*, RFC 2801, und <http://www.ietf.org/html.charters/trade-charter.html>. Zu künftigen Erweiterungen s. *Burdett/Eastlake/Goncalves*, S. 267 ff.

len.[491] Dabei geht es unter anderem um die Identifizierung und Suche von Produkten und Vertragspartnern, um das Austauschen von Vertragsangebot und -annahme, Authentisierung der Parteien,[492] Zahlungsabwicklung und Zustellung des verkauften Guts[493] sowie weitere Fragen der Vertragsabwicklung (beispielsweise eventuelle Rückabwicklungsansprüche). IOTP sieht auch Mechanismen vor, um technischen Problemen (beispielsweise Übertragungsfehlern) und sonstigen unerwarteten Ereignissen (fehlende Deckung der Kreditkarte des Kunden, fehlende Verfügbarkeit des bestellten Artikels, Widerruf der Bestellung) zu begegnen.[494] An IOTP-Transaktionen sind neben den Herstellern, Händlern, Vermittlern und Kunden die Betreiber von Zahlungs- und digitalen Vertriebssystemen sowie Supportunternehmen beteiligt.[495] Im Rahmen von IOTP können unterschiedliche Zahlungssysteme wie Kreditkarten, die Geldkarte oder digitales Geld eingesetzt werden.[496] IOTP standardisiert keine speziellen technischen Schutzmaßnahmen für den Vertrieb digitaler Inhalte. Vielmehr geht es um die Standardisierung und Interoperabilität jener Komponenten, die in einem vollständigen DRM-System außer technischen Schutzmaßnahmen noch benötigt werden.

Im Rahmen des von der Europäischen Union geförderten Projekts „Generic Architecture for Information Availability" (GAIA)[497] wird ein System entwickelt, das eine Vermittlerfunktion zwischen Anbietern und Kunden beim elektronischen Handel anbietet, indem es dem Kunden eine einheitliche Methode zur effizienten Produktsuche, Herstelleridentifizierung, Produktbestellung und -lieferung bietet. Dabei geht es um den Vertrieb digitaler Inhalte.[498] Daneben soll die sogenannte „Electronic Commerce Modeling Language" (ECML), die seit Juni 1999 von einem Industriekonsortium entwickelt wird, die vereinfachte und standardisierte Übertragung von Kundeninformationen (Adresse, Zahlungsweise etc.) an die Händler mit Hilfe sogenannter „digital wallets" ermöglichen.[499]

---

[491] *Burdett/Eastlake/Goncalves*, S. 2.

[492] Zur Gewährleistung von Sicherheit, Authentizität und Integrität können im Rahmen von IOTP digitale Signaturen eingesetzt werden, s. *Burdett*, RFC 2801, S. 74 ff.; *Davidson/Kawatsura*, RFC 2802.; *Burdett/Eastlake/Goncalves*, S. 41 ff.

[493] Zwar kann IOTP auch beim Vertrieb körperlicher Güter eingesetzt werden. Im vorliegenden Zusammenhang wird jedoch nur auf den Vertrieb digitaler Daten abgestellt. S. dazu *Burdett*, RFC 2801, S. 8, 16 f.

[494] S. dazu *Burdett/Eastlake/Goncalves*, S. 61 ff.

[495] *Burdett*, RFC 2801, S. 17; *Burdett/Eastlake/Goncalves*, S. 2.

[496] Die Interoperabilität zu bestehenden Zahlungssystemen wird durch ein „Payment API" sichergestellt, s. dazu *Hans/Beykirch/Hiroya/Kawatsura*; *Burdett/Eastlake/Goncalves*, S. 245 ff.

[497] <http://www.syspace.co.uk/GAIA>.

[498] *Blinov/Bessonov/Clissman*, RFC 2552, S. 2.

[499] <http://www.ecml.org>; *Burdett/Eastlake/Goncalves*, S. 259 ff.

Insgesamt bestehen vielfältige Anstrengungen, um einheitliche Standards zur sicheren und effizienten Geschäftsabwicklung im Internet zu schaffen. Diese E-Commerce-Systeme können auch von DRM-Systemen eingesetzt werden.

VIII. Schutz im analogen Bereich

DRM-Systeme zielen darauf ab, digitale Inhalte umfassend technisch zu schützen. Dem Angreifer soll es möglichst schwer gemacht werden, den Inhalt in analoger Form zu erhalten, da dann viele der beschriebenen Schutzmaßnahmen nicht mehr greifen. Trotz aller Schutzmaßnahmen wird es einem Angreifer jedoch mitunter gelingen, eine analoge Fassung des DRM-geschützten Inhalts zu erstellen. Daher existieren Verfahren, die den technischen Schutz auch nach einem Übergang vom digitalen in den analogen Bereich gewährleisten sollen. Auf eine Darstellung der technischen Grundlagen analoger Kopierschutzverfahren wird hier verzichtet. Es sei nur daran erinnert, daß robuste digitale Wasserzeichen auch Digital-Analog-Wandlungen überstehen sollten.[500] Theoretisch greift der Schutz digitaler Wasserzeichen damit auch im analogen Bereich.[501] Weiterhin bestehen im analogen Bereich Äquivalente zu Verschlüsselungsverfahren.[502] Solche Verfahren sind insbesondere bei Videokassetten und Pay-TV seit den 80er Jahren verbreitet.[503]

---

[500] S. dazu oben Teil 1, C II 2 b bb 4.

[501] Zu Schwachstellen heutiger Wasserzeichenverfahren s. oben Teil 1, C II 2 b bb 6.

[502] Solche Verfahren werden oft nicht „encryption", sondern „scrambling" genannt.

[503] Einer der wichtigsten Hersteller solcher Kopierschutzverfahren ist das amerikanische Unternehmen Macrovision, <http://www.macrovision.com>. Während ein Verfahren von Macrovision zu einem verrauschten, unruhigen Bild führt („automatic gain control"-Verfahren), versieht ein anderes Verfahren („ColorStripe") das Bild mit horizontalen Streifen, s. *Taylor*, DVD Demystified, S. 196; *Bloom/Cox/Kalker/Linnartz/Miller/Traw*, 87 Proc. IEEE 1267, 1268 (1999); s. dazu auch unten Fn. 537. In den USA müssen diese Kopierschutzverfahren seit 2000 in analoge Videorekorder und -kameras eingebaut werden, s. unten Teil 2, D II 1 b. Einen Überblick über relevante Patente in diesem Bereich gibt *Wayner*, Digital Copyright Protection, S. 207 ff.; s. a. *Anderson*, S. 424 ff. Ein anderes interessantes Verfahren für den analogen Bereich wurde im Jahr 2000 von Macrovision patentiert. Immer öfter werden Kinofilme in den ersten Spieltagen in den Kinos mit Videokameras abgefilmt. Um dies zu verhindern, wird bei dem patentierten Verfahren über das normale Leinwandbild ein Infrarot-Bild projiziert, das für den Zuschauer nicht sichtbar ist. Da die meisten Videokameras bestimmte Bereiche des Infrarotspektrums mit aufnehmen, wird die Videoaufnahme dadurch unbrauchbar gemacht. Auch kann ein fokussiertes Infrarotbild auf die Leinwand projiziert werden, in dem beispielsweise Informationen über das einzelne Kino enthalten sind. Damit kann der Ursprungsort der illegalen Kopie ermittelt werden. Das Verfahren kann auch bei Videokassetten und der Anzeige auf normalen Fernsehbildschirmen eingesetzt werden. S. zum ganzen *Wroblewski*, U.S. Patent No. 6018374 (2000).

D. Standards im DRM-Bereich

I. Allgemeines

Like a cryptographic system, any DRM system is as strong as its weakest component.[504]

Wie die bisherige Untersuchung zeigt, existiert im technischen Sinne kein „einheitliches" DRM-System. DRM-Systeme setzen sich aus unzähligen technischen Komponenten zusammen. Um ein durchgängig hohes Sicherheitsniveau und eine effiziente Vertriebsplattform für digitale Inhalte zu bieten, ist es besonders wichtig, daß die einzelnen Komponenten eines DRM-Systems reibungslos miteinander funktionieren und ineinandergreifen. Fragen der Systemintegration und der Standardisierung genießen bei DRM-Systemen hohe Priorität.

Schon seit längerem wird versucht, industrieweite Standards für DRM-Systeme zu etablieren. Dies ist ein höchst komplexes Unterfangen. Das Unterfangen ist technisch komplex, da DRM-Systeme den Schutz digitaler Inhalte in den unterschiedlichsten Medien – CDs, DVDs, Rundfunk/Fernsehen – durchgängig gewährleisten müssen. Das Unterfangen ist organisatorisch komplex, da in die Standardisierungsarbeiten viele unterschiedliche Parteien mit oft gegenläufigen Interessen einbezogen werden müssen; neben den Rechteinhabern – insbesondere der Musik- und Filmindustrie – zählen dazu die Unterhaltungselektronik-, Computer-, Fernsehtechnik- und die Telekommunikationsindustrie.[505]

Viele der allgemeinen Grundsätze von DRM-Systemen – beispielsweise die zentrale Stellung der Verschlüsselung oder die technische Integration von Nutzungsbedingungen – sind das Ergebnis eines jahrelangen Verhandlungsprozesses der genannten Verhandlungspartner. Aus diesen Verhandlungen resultiert auch der Versuch der letzten Jahre, Rahmenbedingungen für eine umfassende DRM-Infrastruktur zu standardisieren, die *alle* Arten der Nutzung digitaler Inhalte und *alle* Konsumentengeräte umfaßt.[506] Vom Ersteller der Inhalte bis zum Nutzer muß eine durchgehende Kette DRM-kompatibler Komponenten existieren, die in ihrer Kombination gewährleisten, daß der technische Schutz digitaler Inhalte jederzeit gewährleistet ist. Keines der Geräte darf die digitalen Inhalte unverschlüsselt an unberechtigte Dritte weitergeben.[507] Damit dies funktioniert, sind Standards erforderlich, die das Ineinangreifen von DRM-Komponenten regeln.

---

[504] *Hartung/Ramme*, IEEE Communications Magazine 78, 79 (November 2000).
[505] *Marks/Turnbull*, EIPR 2000, 198, 203.
[506] *Marks/Turnbull*, EIPR 2000, 198, 204.
[507] *Marks/Turnbull*, EIPR 2000, 198, 204.

Die erste Möglichkeit, diese Ideen umzusetzen, bot sich bei der Einführung der „Digital Versatile Disc“ (DVD).[508] Da sich die Film- und die Unterhaltungselektronikindustrie mit der Computerindustrie nicht auf ein einheitliches Vorgehen hinsichtlich technischer Schutzmaßnahmen im DVD-Standard einigen konnten, wurde im Mai 1996 die „Copy Protection Technical Working Group“ (CPTWG)[509] gegründet, die sich in der Regel monatlich in Burbank, Kalifornien, trifft.[510] In diesem recht locker und offen organisierten Gremium entwickelten Vertreter der drei Branchen viele der in DVDs eingesetzten Schutzsysteme. Noch heute ist die CPTWG eines der wichtigsten Arbeitsgremien[511] im DRM-Bereich. Aber auch andere Gremien arbeiten an Standards für DRM-Systemen.[512] Im folgenden sollen die Ergebnisse solcher Standardisierungsinitiativen dargestellt werden. Darauf wird im weiteren Verlauf der Untersuchung noch öfters zurückzugreifen sein.

Standardisierungsinitiativen haben dazu geführt, daß DRM-Komponenten schon heute in einer Vielzahl von Unterhaltungselektronikgeräten enthalten sind; an neuen Geräten mit DRM-Komponenten wird gearbeitet (dazu insgesamt unten II). In einem DRM-System ist es jedoch nicht ausreichend, wenn nur die einzelnen Endgeräte mit DRM-Komponenten ausgestattet sind. Vielmehr muß auch die *Kommunikation zwischen* den

---

[508] S. dazu unten Teil 1, D II 3.

[509] <http://www.cptwg.org>.

[510] Zu den Einzelheiten s. ausführlich *Marks/Turnbull*, EIPR 2000, 198, 204 f., 208. S. weiterhin *Bloom/Cox/Kalker/Linnartz/Miller/ Traw*, 87 Proc. IEEE 1267, 1268 (1999). Die Musikindustrie ist bei der CPTWG traditionell schwächer vertreten und gründete statt dessen ihre eigene Initiative namens SDMI. S. dazu unten Teil 1, D II 5.

[511] Die CPTWG ist kein Gremium, in dem Standards verabschiedet werden. Vielmehr handelt es sich um eine offenere Diskussionsplattform, die bei Bedarf aber auch fester gefügte Arbeitsgruppen bildet, s. *Marks/Turnbull*, EIPR 2000, 198, 208.

[512] Neben den im folgenden erwähnten Standardisierungsgremien sei noch auf das W3C (s. dazu allgemein oben Teil 1, C II 2 a cc) hingewiesen. Einerseits unterhält es mehrere Standardisierungsinitiativen im Bereich des allgemeinen ECommerce: 1999 startete das W3C zusammen mit der IETF eine Initiative zur Entwicklung digitaler Signaturen, mit denen digitale Inhalte, insbesondere XML-Daten, signiert werden können. Die Signatur dient der Integritäts- und Authentizitätsprüfung vom XML-Daten, s. *Reagle*, RFC 2807; *Eastlake/Reagle/Solo*, sowie die Homepage der XML-Signature Working Group, <http://www.w3.org/Signature>. Im Jahr 2000 begann eine (spätere W3C-)Arbeitsgruppe, sich mit der Verschlüsselung von XML-Daten zu befassen, XML Encryption Working Group, <http://www.w3.org/Encryption>. Zu den Aktivitäten des W3C im Bereich des E-Commerce im Überblick s. *Michel*. Andererseits erwägt das W3C auch spezielle Initiativen für DRM-Systeme. Im Januar 2001 veranstaltete das W3C zu dieser Frage einen Workshop, s. <http://www.w3.org/2000/12/drm-ws/Overview.html>. Zu den Standardisierungsgremien im Internet-Bereich – Internet Society, Internet Architecture Board (IAB), Internet Engineering Task Force (IETF), Internet Engineering Steering Group (IESG), Internet Research Task Force (IRTF), Internet Research Steering Group (IRSG), Internet Assigned Numbers Authoriy (IANA), Internet Corporation for Assigned Names and Numbers (ICANN) und das World Wide Web Consortium (W3C) – äußerst informativ *Mayer*, K&R 2000, 13 ff.

Geräten vor Angriffen geschützt werden. Hierfür existieren spezielle Standards (dazu unten III). Um die Sicherheit eines DRM-Systems insgesamt gewährleisten zu können, sind weiterhin Standards erforderlich, die das Ineinandergreifen der unterschiedlichen DRM-Komponenten auf abstrakter Ebene regeln. Es geht um die Standardisierung übergreifender Schutzarchitekturen (dazu unten IV). Abschließend wird auf Standardisierungsinitiativen von Verwertungsgesellschaften im DRM-Bereich eingegangen (dazu unten V).

II. Schutz bei Endgeräten

1. Digital Audio Tape (DAT)

Im Juni 1989 unterzeichneten Vertreter der Tonträgerindustrie (insbesondere die IFPI und die RIAA) und mehrerer Unterhaltungselektronikhersteller (unter anderen Grundig, Mitsubishi, Philips und Sony) nach langen Verhandlungen in Athen eine Vereinbarung, in dem sich die Parteien für das digitale Kassettenformat „Digital Audio Tape“ (DAT) auf ein Kopierschutzsystem namens „Serial Copy Management System“ (SCMS) einigten (sogenanntes „Athens Agreement“).[513] DAT-Geräte, die für den privaten Konsumentenbereich ausgelegt sind, verfügen seither mit SCMS über ein System, das verhindert, daß von einer digitalen Kopie eines Inhalts eine weitere Kopie (digitale Kopie der zweiten Generation) erstellt werden kann.[514] Wenn ein Musikstück von einer CD das erste Mal auf eine DAT-Kassette kopiert wird, wird das Musikstück in zwei bestimmten Bits mit der Markierung versehen, daß es sich um eine digitale Kopie handelt. Versucht ein Nutzer, diese Kopie mit einem DAT-Gerät digital zu kopieren, liest das DAT-Gerät diese Bits zunächst aus und verhindert dann die Erstellung einer weiteren Kopie.[515] DAT konnte sich im Konsu-

[513] Zur Entstehungsgeschichte s. *U.S. Congress, Office of Technology Assessment*, Copyright & Home Copying, S. 28; *Marks/Turnbull*, EIPR 2000, 198, 203; *N. B. Nimmer/D. Nimmer*, § 8B.01[C], S. 8B-8 f.; *Garnett* in: World Intellectual Property Organization (Hrsg.), S. 101, 108; *McKuin*, 16 Hastings Comm/Ent L.J. 311, 322 (1994). Zur rechtlichen Komponente des „Athens Agreement“ s. unten Teil 2, D II 1 b. Heute wird es als Fehler angesehen, daß an den damaligen Verhandlungen nicht auch die Computerindustrie beteiligt war. Sonst wären vielleicht schon in diesem frühen Stadium Kopierschutzmechanismen in handelsübliche PCs eingebaut worden, s. *Marks/Turnbull*, EIPR 2000, 198, 203. Zu einem anderen, ebenfalls in den 80er Jahren entwickelten und „Copy Code“ genannten System, welches das Kopieren von CDs auf DAT-Kassetten verhindern sollte, indem auf CDs der Frequenzbereich zwischen 3700 und 3900 Hertz nicht aufgezeichnet wurde, DAT-Geräte dieses Frequenzloch erkannten und daraufhin das Kopieren der CD verweigerten, s. *Wiechmann*, ZUM 1989, 111, 113.

[514] Zur Koppelung von SCMS mit CSS durch Know-how-Lizenzverträge s. unten Teil 2, C II 2 b.

[515] Die technischen Einzelheiten ergeben sich u. a. aus *International Electrotechnical Commission*, IEC 1119–6, und sind auch in *U.S. Senate*, S. Rep. No. 102–294, S. 17 ff.,

mentenbereich nicht durchsetzen. In professionellen DAT-Geräten können die entsprechenden SCMS-Bits regelmäßig frei gesetzt und der Kopierschutz umgangen werden.[516]

2. Pay-TV

Die technischen Schutzmaßnahmen im Pay-TV Bereich werden regelmäßig unter dem Begriff „Conditional Access" zusammengefaßt.[517] Die in Europa verwendeten Schutzmaßnahmen werden im Rahmen des 1993 gegründeten „Digital Video Broadcasting Project" (DVB)[518] entwickelt und vom „European Telecommunications Standards Institute" als Standard verabschiedet.[519] Sie finden inzwischen auch über Europa hinaus verbreitet Anwendung.[520] Dabei wird das TV-Programm in verschlüsselter Form[521] über Kabel, terrestrische Funk- oder Satellitennetze zum Nutzer übertragen. Beim Nutzer ist eine Set-Top-Box installiert, die das Pro-

näher beschrieben. S. allgemeiner *N. B. Nimmer/D. Nimmer*, § 8B.03[B], S. 8B-46 ff.; *Marks/Turnbull*, EIPR 2000, 198, 212; *Kaestner* S. 15; *U.S. Congress, Office of Technology Assessment*, Copyright & Home Copying, S. 28 f.; *McKuin*, 16 Hastings Comm/Ent L.J. 311, 325 f. (1994).

[516] S. *Kaestner*, S. 15.

[517] S. zum ganzen *Cutts*, 9 Electronics & Communication Engineering Journal 21 (1997).

[518] <http://www.dvb.org>.

[519] S. *Europäische Kommission*, KOM (1999) 450 v. 9. 11. 1999, S. 22 und Art. 2 lit. c der Fernsehsignalübertragungs-Richtlinie; *Luetteke*, 183 ABU Technical Review 3 (Juli/August 1999); *Ladeur*, CR 1999, 395, 403. Zur Lage in den USA vgl. auch den Standard „Conditional Access System for Terrestrial Broadcast" des Advanced Television Systems Committee vom 17. 7. 1999. Daneben sind noch die „European Broadcast Union" (EBU) und das „Comité Européen de Normalisation Electrotechnique" (CENELEC) an der Normierung beteiligt. Früher waren in Europa die analogen Systeme EuroCrypt und VideoCrypt, in den USA ist das Videocipher-System weit verbreitet. Einen Überblick über heute in Europa eingesetzte Pay-TV-Verschlüsselungssysteme gibt <http://www.set-top-box.de/codiert/cas.htm>.

[520] In den USA wurden im analogen Fernsehen schon in den 50er Jahren Versuche mit technischen Schutzmaßnahmen gemacht, *Macq/Quisquater*, 83 Proc. IEEE 944 (1995). Heute befaßt sich in den USA die Subgroup 8 der Technology Group 3 des „Advanced Television Systems Committee" (ATSC), <http://www.atsc.org>, mit Fragen der Kopierschutzes in Pay-TV-Systemen. Einen Überblick über DVB-Normen gibt *Reimers*, Fernseh- und Kinotechnik 52 (1998), 82 ff. Da sich die vorliegende Arbeit mit DRM-Systemen für digitale Inhalte beschäftigt, bleiben im folgenden technische Schutzmaßnahmen für analoge Pay-TV-Systeme unbeachtet, s. dazu *Schwenk* in: Seiler (Hrsg.), S. 163, 165 f.; *Ciciora/Farmer/Large*, S. 724 ff.; *Baylin/McCormac/Maddox*, S. 193 ff. Zur Umstellung auf digitale Fernsehtechnik s. *Europäische Kommission*, KOM (1999) 450 v. 9. 11. 1999, S. 21.

[521] Die Terminologie unterscheidet sich bei Pay-TV-Systemen. So wird ein kryptographischer Schlüssel in diesem Zusammenhang „control word" und die Verschlüsselung nicht „encryption", sondern „scrambling" genannt. Bei analogen Pay-TV-Systemen wird nicht von „Verschlüsselung" der Inhalte, sondern von „Verschleierung" (so *Federrath*, ZUM 2000, 809) oder von „Verwürfelung" (so *Reimers*, Fernseh- und Kino-Technik 52 (1998), 82, 83) gesprochen.

gramm entschlüsselt und an den Fernseher weiterreicht.[522] Neben der Verschlüsselung sind noch weitere der oben dargestellten Techniken wie Schlüssel-Management, Smartcards und Metadaten Teil eines „Conditional Access"-Systems.[523] Regelmäßig sind auch Verfahren enthalten, durch die kompromittierte Set-Top-Boxen von der weiteren Nutzung ausgeschlossen werden können („device revocation").[524] Trotz all dieser technischen Schutzmaßnahmen ist die Piraterie bei Pay-TV-Systemen weit verbreitet.[525] Dies liegt zumindest teilweise auch daran, daß manche der heutigen Pay-TV-Systeme mit veralteten und unzureichenden technischen Schutzmaßnahmen versehen sind.

Im Rahmen des DVB-Projekts wird seit Ende 1997 die sogenannte „Multimedia Home Platform" entwickelt.[526] Dieser Standard will der zunehmenden Medienkonvergenz Rechnung tragen und unter anderem eine einheitliche Set-Top-Box für digitales Fernsehen, interaktive Dienste und Internet-Zugang ermöglichen. Es geht um die Schaffung einer anbieter-neutralen Plattform, die auf der von Sun Microsystems entwickelten

[522] Um das Risiko zu verringern, daß Angreifer den in einer Set-Top-Box verwendeten Dechiffrier-Schlüssel ermitteln und einen Piraten-Decoder bauen, verwenden Pay-TV-Systeme regelmäßig zwei verschiedene Schlüssel. Die Videodaten werden mit sog. „session keys" verschlüsselt. Dabei ändert sich der verwendete „session key" alle paar Sekunden. Den berechtigten Nutzern werden neben den Videodaten in sogenannten „entitlement control messages" (ECM) auch die jeweils aktuellen „session keys" übermittelt, wobei die Übertragung dieser „session keys" wiederum mit sog. „management keys" verschlüsselt wird, *Macq/Quisquater*, 83 Proc. IEEE 944, 950 (1995). Weiterhin überträgt der Pay-TV-Betreiber an die Set-Top-Boxen sog. „entitlement management messages" (EMM), mit denen der Betreiber festlegt, welche Nutzer zur Verwendung der ECMs und damit zum Entschlüsseln der Videodaten berechtigt sind. Dies kann wiederum mit Hilfe von Verschlüsselungsverfahren geschehen, *Schwenk* in: Seiler (Hrsg.), S. 163, 169 f.; *Macq/Quisquater*, a. a. O., S. 950 f. Während der DVB/ETSI-Standard eine (geheimgehaltene) Standardisierung der Verschlüsselung der Videodaten enthält („Common Scrambling Algorithm"), konnte man sich auf keinen einheitlichen Standard zur Verschlüsselung der ECMs einigen. Vielmehr enthält der DVB/ETSI-Standard ein „common interface", das die Interoperabilität zwischen den „Conditional Access"-Verfahren verschiedener Anbieter und den Endgeräten verschiedener Hersteller sicherstellt; s. dazu und den zugrundeliegenden Verfahren SimulCrypt und MultiCrypt *Reimers*, Fernseh- und Kino-Technik 52 (1998), 82, 83 f.; *Cutts*, 9 Electronics & Communication Engineering Journal 21, 22 f. (1997); zum obligatorischen Einsatz des „Common Scrambling Algorithm" durch europäisches Recht s. unten Teil 2, D II 1 a. Mit dem DVB „common interface" ist im U.S.-amerikanischen Bereich der „Point of Deployment" der OpenCable-Initative vergleichbar, <http://www.opencable.com>; zu der dabei verwendeten Patent-Lizenz s. unten Teil 2, C II 1.

[523] Zum Überblick s. *de Bruin* in: de Bruin/Smits, S. 203 ff. Vgl. weiterhin *Cutts*, 9 Electronics & Communication Engineering Journal 21 ff. (1997); *Macq/Quisquater*, 83 Proc. IEEE 944 ff. (1995). Zu Metadaten im DVB-Bereich s. *European Telecommunications Standard Institute*, ETSI EN 300 468 V1.4.1; *dass.*, ETSI TR 101 211 V1.4.1.

[524] S. dazu *Kravitz/Goldschlag* in: Franklin (Hrsg.), S. 158, 165 f.

[525] Vgl. die Usenet-Newsgroup alt.satellite.tv.crypt sowie umfassend, wenn auch veraltet *Baylin/McCormac/Maddox*.

[526] <http://www.mhp.org>.

Programmiersprache Java basiert.[527] Eine erste Normierung wurde Mitte 2000 veröffentlicht.[528] Dabei wird unter anderem die Authentizitäts- und Integritätsprüfung von Softwareprogrammen genormt, die auf einer Set-Top-Box des Nutzer laufen.[529] Eine Normierung im Bereich technischer Schutzmaßnahmen ist derzeit noch nicht enthalten, aber für die Zukunft geplant.[530]

3. Digital Versatile Disc (DVD)

a) Allgemeines

Die Digital Versatile Disc (DVD) wird derzeit hauptsächlich als Speichermedium für Videofilme und Videospiele[531] eingesetzt, soll aber auch Audio-CDs (DVD-Audio) und CD-ROMs (DVD-ROM) ersetzen.[532] DVDs haben die Größe einer CD, jedoch eine um bis zum Faktor 25 erhöhte Speicherkapazität.[533]

Einer der umstrittensten Bereiche des DVD-Standardisierungsprozesses, der mehrere Jahre dauerte und an dem die Unterhaltungselektronik-, Computer-, Film- und die Musikindustrie beteiligt war, war die konkrete Ausgestaltung der technischen Schutzmaßnahmen in DVDs und DVD-Geräten. Die Filmindustrie Hollywoods hatte angekündigt, ihre Filme nur dann auf einem digitalen Speichermedium wie der DVD zu veröffentlichen, wenn ein sicherer Kopierschutz zur Verfügung stehe.[534] Im Rahmen der CPTWG wurden dann Vorschläge für Kopierschutzmaßnahmen in DVDs entwickelt.[535]

---

[527] S. dazu *Vogt*, Fernseh- und Kino-Technik 53 (1999), 21; *Luetteke*, 183 ABU Technical Review 3 ff. (Juli/August 1999).

[528] *European Telecommunications Standard Institute*, ETSI TS 101 812 Version 1.1.1.

[529] S. dazu *European Telecommunications Standard Institute*, ETSI TS 101 812 Version 1.1.1, S. 106 ff.

[530] Dabei soll die „Multimedia Home Platform" aber unabhängig von einem speziellen DRM-System sein. Es soll vielmehr sichergestellt werden, daß unterschiedliche DRM-Systeme auf die „Multimedia Home Platform" zugreifen können, s. *Vogt*, Fernseh- und Kino-Technik 53 (1999), 21, 22.

[531] Beispielsweise ist die Sony PlayStation 2 mit einem DVD-Laufwerk ausgestattet.

[532] Zu der mitunter verwirrenden Vielfalt an DVD-Formaten (u. a. DVD-Video, DVD-Audio, DVD-VR, DVD-AR, DVD-ROM, DVD-R, DVD-RW und DVD-RAM) s. *Taylor*, DVD Demystified, S. 144 ff. Zum bisherigen Erfolg der DVD s. oben bei Fn. 16.

[533] *Taylor*, DVD Demystified, S. 3. Das Standardwerk von *Taylor* gibt einen erschöpfenden Überblick über die DVD-Technologie.

[534] Zu den jahrelangen Verhandlungen s. *Taylor*, DVD Demystified, S. 45 ff.; *Marks/Turnbull*, EIPR 2000, 198, 205 f.

[535] Insbesondere einigten sich die Film-, Computer- und Unterhaltungselektronikindustrie in der CPTWG auf die Verwendung von CSS für Video-DVDs, *Marks/Turnbull*, EIPR 2000, 198, 206. Die CPTWG schlägt ihre Vorschläge der Working Group 9 des DVD Forum vor, die ihrerseits dem gesamten DVD Forum Vorschläge macht; s. dazu *Taylor*, DVD Demystified, S. 191 f.

Insgesamt existieren bei DVD heute bis zu zehn technische Schutzmaßnahmen, die teilweise schon in allen DVD-Geräten enthalten sind und sich teilweise noch im Entwicklungsstadium befinden.[536] Neben dem bekanntesten Verfahren, dem „Content Scramble System" (CSS), enthalten alle heutigen DVD-Geräte Schutzmaßnahmen, die das Erstellen analoger Kopien von Videofilmen verhindern sollen (sogenanntes „analog protection system").[537] Im folgenden werden die wichtigsten derzeitigen Schutzmaßnahmen dargestellt.[538]

b) Content Scramble System (CSS)

Das „Content Scramble System" (CSS)[539] ist ein Verschlüsselungs- und Authentisierungs-System, welches das direkte Kopieren entschlüsselter

[536] *Taylor*, DVD Demystified, S. 192. Die Zählweise differiert teilweise.

[537] Zu diesem Zweck werden zwei Verfahren von Macrovision eingesetzt, s. dazu oben Fn. 503. Sie verhindern jedoch nicht das Aufnehmen der RGB-Signale, einem im PC-Bereich verbreiteten Standard, s. *Cox/Linnartz*, 16 IEEE Journal on Selected Areas in Communications 587, 588 (1998); zu der daraus resultierenden Schutzlücke bei DVDs s. unten Fn. 920.

[538] Neben den im direkt folgenden angeführten Verfahren wird CPPM (s. dazu unten Teil 1, D II 4) bei DVD-Audio eingesetzt (s. *Taylor*, DVD Demystified, S. 193) und CPRM (s. dazu unten Teil 1, D II 4) von allen DVD-Aufnahmegeräten, die nach 1999 verkauft wurden, unterstützt; s. *Taylor*, DVD Demystified, S. 200. Schließlich sollen auch DTCP und HDCP (s. dazu unten Teil 1, D III 2) in DVD-Systemen Anwendung finden; s. dazu *Taylor*, DVD Demystified, S. 199 f. Eine Variante des DVD-Formats wurde ab Mitte 1998 unter dem Namen „Divx" in den USA vermarktet. Dabei konnte der Nutzer eine Divx-DVD für $ 4,50 kaufen und diese in einem speziellen DVD-Gerät 48 Stunden lang anschauen. Nach Ablauf der 48 Stunden wurde die weitere Nutzung der Divx-DVD durch das Gerät unterbunden. Dann konnte der Nutzer die Divx-DVD für $ 3,25 für weitere 48 Stunden nutzen. Für diese Schutzmaßnahme setzte Divx u. a. eine Triple-DES-Verschlüsselung, digitale Wasserzeichen sowie eine Online-Verbindung zu einem Divx-Zentralcomputer ein. Die Idee des Konzepts war, eine Alternative zu Videotheken zu bieten: Der Nutzer kauft eine Divx-DVD für einen billigen Preis, anstatt in die Videothek zu gehen. Nach Ablauf der „Leihfrist" wirft er die Divx-DVD in den Papierkorb. Obwohl die anfänglichen Verkaufszahlen recht vielversprechend waren, konnte sich Divx – nicht nur wegen schlechter Presseberichte, sondern auch, weil sich die Kunden mit dem Kopierschutzkonzept nicht anfreunden konnten – nicht durchsetzen. Im Juni 1999 kündigte der Hersteller an, daß Divx nicht weiter angeboten wird. S. zum ganzen *Taylor*, DVD Demystified, S. 63 ff.; *Schneck*, 87 Proc. IEEE 1239, 1242 (1999); Wand, S. 15 f. Von „Divx" ist das Kompressionsverfahren „Divx ;)" (und dessen Fortentwicklungen Divx Deux und OpenDivx) zu unterscheiden. Dieses auf MPEG-4 basierende Verfahren, das ursprünglich aus einem „Reverse Engineering" des Microsoft Media Players hervorgegangen war, ist ein sehr effizientes Verfahren zur Kompression von Videodaten. Bei entsprechender Weiterentwicklung könnte „Divx ;-)" im Videobereich eine ähnliche Bedeutung zukommen wie MP3 im Audiobereich. Zu „Divx ;-)" s. <http://www.projectmayo.com> und Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 313 ff. (S.D.N.Y. August 17, 2000).

[539] Mitunter wird auch vom „Content Scrambl*ing* System" gesprochen. Der offizielle Name, der auch von der „DVD Copy Control Association" (<http://www.dvdcca.org>) verwendet wird, lautet jedoch „Content Scramble System".

Videodaten von einer DVD verhindern soll.[540] Es wurde 1996 im Rahmen der CPTWG für DVDs hauptsächlich von Matsushita[541] und Toshiba entwickelt.[542] Durch CSS werden Teile der Videodaten auf einer DVD verschlüsselt abgespeichert. Sie können nur mit Hilfe eines sogenannten „title keys" entschlüsselt werden, der seinerseits in verschlüsselter Form auf jeder DVD enthalten ist. Durch ein ausgeklügeltes Authentisierungs- und Kommunikationsverfahren zwischen dem DVD-Spieler und der Decoder-Hard- oder Software wird sichergestellt, daß nur berechtigte Decoder die Videodaten entschlüsseln können.[543]

In Fachkreisen war schon lange bekannt, daß CSS kein besonders sicheres Schutzsystem ist.[544] Ab Oktober 1999 tauchte denn auch im Inter-

[540] *Taylor*, DVD Demystified, S. 192. CSS ist kein „Kopierschutz" im eigentlichen Sinne. Mit entsprechender Ausrüstung kann eine DVD bitweise digital kopiert werden; dies wird auch durch CSS nicht verhindert. Ein bloßes Kopierprogramm genügt dafür aber nicht, s. *Bloom/Cox/Kalker/Linnartz/Miller/Traw*, 87 Proc. IEEE 1267, 1269 (1999).

[541] Matsushita Electric Industrial Co. Ltd. bietet Produkte unter den Namen Panasonic, Quasar und National an.

[542] Zur Entstehungsgeschichte s. *Marks/Turnbull*, EIPR 2000, 198, 205 f.; Universal City Studios, Inc. v. Reimerdes, 111 F.Supp.2d 294, 309 f. (S.D.N.Y. 2000).

[543] Genau genommen ist CSS ein kryptographisches Verfahren zum Verteilen und Management von kryptographischen Schlüsseln, *Taylor*, DVD Demystified, S. 484. Grob funktioniert das Verfahren wie folgt: Einerseits ist jeder DVD-Spieler mit einer kleinen Anzahl an sog. „player keys" ausgestattet, die den DVD-Spieler als autorisiertes CSS-Abspielgerät identifizieren. Diese „player keys" werden von der Organisation, die CSS lizenziert (DVD Copy Control Association), an Gerätehersteller vergeben; derzeit existieren über 400 solcher Schlüssel. Andererseits ist auf jeder Video-DVD ein „disk key" enthalten, der die DVD identifiziert. Der „disk key" ist jedoch auf der DVD nicht im Klartext und nicht nur ein Mal enthalten, sondern insgesamt über 400 Mal jeweils mit den einzelnen „player keys" verschlüsselt abgespeichert. Will ein DVD-Spieler eine DVD abspielen, so versucht er – nach einer Authentisierungsphase, die auf einem „Challenge-Response"-Verfahren beruht (s. dazu oben Teil 1, C III 2 d) –, mit seinem eigenen „player key" den auf der DVD gespeicherten „disk key" zu entschlüsseln. Wenn es sich um einen gültigen „player key" handelt, wird der DVD-Spieler bei einem der über 400 auf der DVD verschlüsselt abgespeicherten „disc keys" Erfolg haben. Mit Hilfe des entschlüsselten „disc keys" kann dann ein sog. „title key" entschlüsselt werden, der ebenfalls auf der DVD abgespeichert ist. Mit diesem entschlüsselten „title key" kann dann der DVD-Spieler die Videodaten tatsächlich entschlüsseln. Dabei sind insgesamt nur ca. 15 % der Videodaten verschlüsselt, um den Rechenaufwand in Grenzen zu halten. Zu den Einzelheiten s. *Taylor*, DVD Demystified, S. 481 ff.; <http://eon. law.harvard.edu/openlaw/DVD/dvd-discuss-faq-html>. Einen Überblick geben auch *Marks/Turnbull*, EIPR 2000, 198, 212 f. Zu der lizenzrechtlichen Seite von CSS s. unten Teil 2, C II.

[544] CSS baut auf Schlüsseln mit einer Länge von 40 Bit auf, von denen nur 25 Bit bei den einzelnen Schlüsseln jeweils unterschiedlich sind. Mit Hilfe sog. „brute force"-Angriffe, bei denen alle theoretisch denkbaren Schlüsselkombinationen ausprobiert werden, sind Verfahren mit solch kurzer Schlüssellänge relativ problemlos zu knacken. S. *Taylor*, DVD Demystified, S. 487; *Maes/Kalker/Linnartz/Talstra/Depovere/Haitsma*, 17 (5) IEEE Signal Processing Magazine 47, 48 (September 2000). Allerdings wurde geltend gemacht, daß die Beschränkung auf 40 Bit lange Schlüssel bei CSS mit Exportbeschränkungen für Verschlüsselungsverfahren zusammenhing, s. *Cox/Linnartz*, 16 IEEE Jounal on Selected Areas in Communications 587, 588 (1998); *Hoy*, S. 10.

net ein Windows-Programm namens DeCSS auf.[545] Das Programm, das von einer deutsch-norwegischen Hackergruppe geschrieben worden war,[546] ermöglicht die Entschlüsselung CSS-geschützter DVDs.[547] In der Folgezeit wurden im Internet – teilweise anonym – auch die Einzelheiten des bisher geheimen CSS-Verfahrens veröffentlicht.[548]

c) Copy Generation Management System (CGMS)

Das „Copy Generation Management System" (CGMS) bettet in digitale oder analoge Videosignale Informationen darüber ein, ob von den Videodaten Kopien erstellt werden dürfen oder nicht.[549] Es handelt sich um ein System, das dem bei DAT-Geräten eingesetzten SCMS[550] ähnelt. Wie SCMS verhindert auch CGMS nicht die Erstellung mehrerer Kopien von einem Original. Vielmehr kann es nur die Kopie der zweiten Generation verhindern. Auch CGMS wird in DVDs eingesetzt.[551]

d) Digitale Wasserzeichen

Audio-DVDs enthalten ein vom U.S.-amerikanischen Unternehmen Verance entwickeltes digitales Wasserzeichen.[552] Damit werden die Kopierkontroll-Informationen des CGMS direkt in die Audio-Daten einge-

---

[545] S. *Hoy*, S. 2 ff.; <http://eon.law.harvard.edu/openlaw/DVD/research/chronology.html>. *Taylor*, DVD Demystified, S. 79, meint: „Anyone familiar with CSS was surprised that it had taken so long for the system to be cracked." Dies ist nicht der erste Angriff auf CSS. Schon im November 1997 wurden Lücken im Kopierschutzsystem der DVD festgestellt. Mit dem damaligen Programm „softDVDcrack" wurde jedoch nicht CSS selbst geknackt, sondern vielmehr ein Fehler in einem Software-Decoder ausgenutzt. Dieser Fehler wurde vom Hersteller des Software-Decoders schnell behoben. S. dazu *Taylor*, DVD Demystified, S. 68.

[546] Die Gruppe, deren Mitglieder größtenteils anonym blieb, nannte sich „Masters of Reverse Engineering" (MoRE). Das einzige namentlich bekannte Mitglied ist der damals 16-jährige Norweger *Jon Johansen*, der auch – aufbauend auf dem Code anderer Mitglieder der Gruppe – das eigentliche Windows-Programm DeCSS geschrieben hatte.

[547] Dabei nutzten die Hacker eine Schwäche in einem DVD-Software-Decoder des Unternehmens Xing aus. Dort war der „player key" nicht in verschlüsselter Form abgespeichert und konnte somit von Angreifern ausgelesen werden, s. *Hoy*, S. 2. S. zum ganzen auch Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 308 ff. (S.D.N.Y. August 17, 2000).

[548] S. dazu das Open DVD Forum an der Harvard Law School, <http://eon.law.harvard.edu/openlaw/DVD> und die „CSS Gallery" von *David Touretzky* unter <http://www.cs.cmu.edu/~dst/DeCSS/Gallery>.

[549] *Taylor*, DVD Demystified, S. 197; *Bloom/Cox/Kalker/Linnartz/Miller/Traw*, 87 Proc. IEEE 1267, 1268 (1999); *Cox/Linnartz*, 16 IEEE Journal on Selected Areas in Communications 587, 588 f. (1998).

[550] S. dazu oben Teil 1, D II 1.

[551] Zur Koppelung von CGMS mit CSS durch Know-how-Lizenzverträge s. unten Teil 2, C II 2 b.

[552] Verance entwickelte auch das in der SDMI Phase I verwendete Wasserzeichen, s. dazu unten Teil 1, D II 5. Zu den Bedingungen, unter denen das Wasserzeichenverfahren lizenziert wird, s. unten Teil 2, C II. Zur Frage, ob dieses Wasserzeichen zu Qualitätseinbußen führt, s. *Taylor*, DVD Demystified, S. 84 f.

bettet.[553] Dadurch sollen diese Informationen insbesondere die Digital-Analog-Wandlung mit anschließender Redigitalisierung überstehen.[554] Ein DRM-kompatibles Endgerät liest vor der Ausgabe des digitalen Inhalts das digitale Wasserzeichen aus. Wenn das Wasserzeichen die Information „no copy" enthält, wird die Ausgabe des digitalen Inhalts verhindert.[555] Für DVD-Video werden ähnliche Verfahren erwogen, die Standardisierungsentwicklung ist hier aber noch nicht abgeschlossen.[556]

e) Regional Code Playback Control

Filmstudios haben ein starkes Interesse daran, eine Kontrolle über die geographische Verbreitung der DVDs zu haben.[557] Daher ist im DVD-Vi-

[553] *Taylor*, DVD Demystified, S. 198 f.; *Marks/Turnbull*, EIPR 2000, 198, 210. Zu den Besonderheiten dieses Wasserzeichens gegenüber sonstigen Wasserzeichen (insbesondere geringe Anforderungen an die Kapazität des Wasserzeichens, dagegen hohe Anforderungen an geringe Rechenintensität und Kosten) s. *Cox/Linnartz*, 16 IEEE Journal on Selected Areas in Communications 587, 589 (1998).

[554] *Bloom/Cox/Kalker/Linnartz/Miller/Traw*, 87 Proc. IEEE 1267, 1269 (1999). Zu möglichen Sicherheitsschwächen solcher Wasserzeichen s. *Dittmann*, S. 33, 38 f.

[555] *Marks/Turnbull*, EIPR 2000, 198, 204.

[556] *Bloom/Cox/Kalker/Linnartz/Miller/Traw*, 87 Proc. IEEE 1267, 1274 (1999); *Maes/Kalker/Linnartz/Talstra/Depovere/Haitsma*, 17 (5) IEEE Signal Processing Magazine 47 ff. (September 2000). Dabei werden unterschiedliche Alternativen erwogen. Einerseits wird erwogen, die CGMS-Informationen mit Hilfe von Wasserzeichen direkt in die Videodaten einzubetten; wenn keine weiteren Kopien erstellt werden dürfen,wird ein zweites Wasserzeichen in die Videodaten eingebettet, das ein entsprechendes CGMS-Bit setzt. Einer der Hauptnachteile dieses Ansatzes ist, daß das Nutzergerät über die Möglichkeit verfügen muß, dieses zweite Wasserzeichen einzubetten. Dadurch kann ein Angreifer eventuell die Sicherheit des Systems beeinträchtigen. Andererseits wird erwogen, die CGMS-Information nicht in ein Wasserzeichen, sondern in einen getrennten Zähler (sog. „ticket") zu integrieren; dabei wird kryptographisch sichergestellt, daß das Endgerät die in dem Zähler ausgedrückte Anzahl der noch erlaubten Kopien zwar immer verringern, nie aber erhöhen kann. Dieser Ansatz hat zwar den Vorteil, sicherer zu sein, jedoch den Nachteil, daß die Metadaten nicht direkt in die Videodaten eingebettet sind und daher immer zusätzlich zu den Inhalten übertragen werden müssen. S. zum ganzen *Bloom/Cox/Kalker/Linnartz/Miller/ Traw*, 87 Proc. IEEE 1267, 1274 f. (1999); *Maes/Kalker/Linnartz/Talstra/Depovere/Haitsma*, 17 (5) IEEE Signal Processing Magazine 47, 55 f. (September 2000); *Linnartz* in: Quisquater/Deswarte/Meadows/Gollmann (Hrsg.), S. 257 ff.; *Anderson*, S. 433 f.

[557] Die Filmindustrie führt dafür viele Gründe an. *Ein Grund* ist, daß Filme in unterschiedlichen Regionen der Welt zu unterschiedlichen Zeiten auf DVD veröffentlicht werden sollen. Wenn ein Film im Sommer eines Jahres in Deutschland anläuft, ist der Film in den USA vielleicht schon auf DVD erschienen, da er dort im vorangegangen Herbst in den Kinos lief. Wenn die DVD nun auch in Deutschland verfügbar wäre, würde dies zu geringeren Kinoeinnahmen in Deutschland führen und damit die Wertschöpfungskette gefährden, auf der die Filmindustrie aufbaut: Der Film wird nur einmal produziert, aber oft sechs Mal verkauft (aufeinander folgende Veröffentlichung von Filmen im Kino, in Flugzeugen und Hotels, in Videotheken, zum käuflichen Erwerb auf Video/DVD, im Pay-TV, zuletzt im Free-TV; s. zu dieser sog. „Windowing"-Strategie *European Communication Council* (Hrsg.), S. 66, 71 f.; *Detering*, S. 84 ff.). *Ein weiterer Grund* ist, daß Filmstudios bestimmte Filme zu bestimmten Jahreszeiten veröffentlichen wollen: Ein „Sommerhit" muß auf der Nordhalbkugel im Juli, auf der

deo-Standard ein sogenanntes „Regional Code Playback Control“ integriert, welches das Abspielen bestimmter DVDs in bestimmten geographischen Regionen verhindert.[558] Auch dieses System wurde im Rahmen der CPTWG entwickelt.[559]

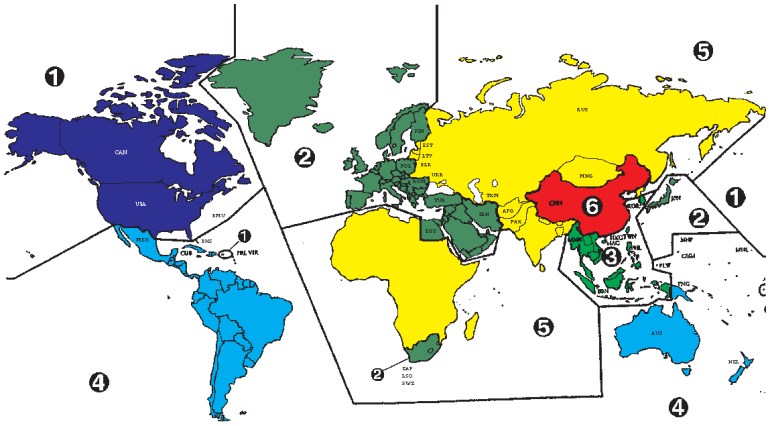


Abbildung 5: Regional-Codes bei DVD-Video[560]

Südhalbkugel jedoch im folgenden Januar veröffentlicht werden. Dazu kommt, daß es aus logistischen und finanziellen Gründen sehr schwierig ist, einen Film auf der ganzen Welt gleichzeitig in die Kinos zu bringen. *Ein weiterer Grund* ist, daß Filmstudios die Verbreitungsrechte an Filmen für einzelne Länder bestimmten Distributoren oftmals exklusiv einräumen. Das „Regional Code Playback Control“-System gewährleistet, daß die DVDs eines Distributors auch nur in seinem exklusiven Lizenzgebiet genutzt werden können. Dadurch unterstützt das „Regional Code Playback Control“-System die Interessen der Filmstudios an einer räumlich aufgeteilten Einräumung des Verbreitungsrechts. *Ein weiterer Grund* ist, daß die Raubkopie-Problematik bei DVDs auf bestimmte Regionen beschränkt werden soll. Durch das „Regional Code Playback Control“ wird beispielsweise verhindert, daß Raubkopien von DVDs, die in China illegalerweise im großen Stil hergestellt wurden, nach USA importiert und auf dem U.S.-Schwarzmarkt vertrieben werden. *Schließlich* können Regionen-Codes verwendet werden, um Filme in den einzelnen Regionen in leicht veränderten Fassungen zu veröffentlichen und damit lokalen Gesetzen (z. B. Jugendschutz-Vorschriften) oder Marktbesonderheiten gerecht zu werden. S. zum ganzen *Marks/Turnbull*, EIPR 2000, 198, 213; *Europäische Kommission*, ABl. EG Nr. C 53E vom 20. 2. 2001, S. 158.

[558] Für ein vergleichbares System für den online-Vertrieb digitaler Inhalte erhielt Liquid Audio im November 2000 ein Patent, s. *Ansell/Cherenson*, U.S. Patent No. 6151631 (2000) und <http://www.liquidaudio.com/support/pc/liqplayer/genplayer_suppt/terr_restrict.html>. Auch die von Sony entwickelte Spielekonsole „Playstation“ verfügt über ein vergleichbares System, das verhindern kann, daß in Japan oder USA erworbene Playstation-Speichermedien auf einer in Europa erworbenen Playstation ausgeführt werden können, s. dazu Sony Computer Entertainment America, Inc. v. Gamemasters, Inc. 87 F. Supp. 2d 976, 981 (N.D.Cal. 1999).

[559] *Marks/Turnbull*, EIPR 2000, 198, 213.

[560] Karte erhältlich unter <http://www.unik.no/~robert/hifi/dvd/world.html>.

Für das Regionen-Management wurde der Weltmarkt in insgesamt sechs Regionen aufgeteilt.[561] Das System baut auf einem Zusammenspiel von DVD-Spielern und DVDs auf:[562] Einerseits werden alle DVD-Spieler mit dem „Regional-Code" jener Region versehen, in welcher sie verkauft werden sollen. Andererseits werden alle DVD-Video-Titel, die mit CSS geschützt sind,[563] mit dem Regional-Code jener Region versehen, in welcher sie verkauft werden sollen. Wenn eine DVD auf einem DVD-Spieler abgespielt werden soll, so prüft der DVD-Spieler zunächst, ob die DVD über den gleichen Regional-Code wie der DVD-Spieler verfügt. Ist dies nicht der Fall, so spielt der DVD-Spieler die DVD nicht ab. Beim „Regional Code Playback Control"-System handelt es sich also nicht um ein Verschlüsselungssystem; vielmehr werden nur bestimmte Bits auf der DVD und im DVD-Spieler gesetzt, um sie einer Region zuzuordnen.[564]

Durch dieses System können beispielsweise DVDs, die in den USA erworben wurden, nicht auf deutschen DVD-Spielern abgespielt werden. Allerdings sind im Internet eine Vielzahl von Informationen erhältlich, wie man die Beschränkung in DVD-Spielern, nur DVDs bestimmter Regionen abzuspielen, aushebeln kann.[565] Auch werden mitunter DVD-Spieler angeboten, welche die „Regional Code Playback Control"-Bits gar nicht auslesen.[566] Während die Hersteller von DVD-Spielern und DVD-Computerlaufwerken lizenzrechtlich verpflichtet sind, das „Regional Code Playback Control"-System in ihre Geräte einzubauen,[567] ist die Verwendung in DVDs selbst optional, jedoch auch dort weit verbreitet.

---

[561] Eine weitere „Region" (Nr. 8) umfaßt spezielle Aufführungsorte wie Flugzeuge, Kreuzfahrtschiffe und Hotels, s. dazu § 2.1 (b) (v) CSS License Agreement. Insgesamt könnten bis zu 16 Regionen festgelegt werden, s. *Taylor*, DVD Demystified, S. 187. Bemerkenswert an der Aufteilung ist einerseits, daß Japan, Westeuropa, Südafrika und der mittlere Osten eine gemeinsame Region bilden (Nr. 2). Andererseits ist China eine eigene Region (Nr. 6), wohl hauptsächlich wegen der verbreiteten Raubkopie-Problematik in China.

[562] S. zum ganzen *Taylor*, DVD Demystified, S. 187 ff.

[563] Bei anderen DVD-Arten wie ungeschützten DVD-Video-Titeln, DVD-Audio oder DVD-ROM wird die „Regional Code Playback Control" nicht eingesetzt, s. *Taylor*, DVD Demystified, S. 187.

[564] *Taylor*, DVD Demystified, S. 187, 491 f.

[565] Inzwischen existieren jedoch auch DVDs, die ihrerseits zunächst den auf dem DVD-Spieler eingestellten Regionen-Code überprüfen und die Zusammenarbeit mit dem DVD-Spieler verweigern, wenn er nicht mit dem Regionen-Code der DVD übereinstimmt. Dieses Verfahren wurde Ende 2000 unter dem Namen „Region Code Enhancement" bekannt, s. dazu *Taylor*, DVD Demystified, S. 189; *Taylor*, DVD Frequently Asked Questions, Frage 1.10.

[566] *Taylor,* DVD Demystified, S.189. Filmstudios und das DVD-Forum versuchen mitunter, dagegen markenrechtlich vorzugehen.

[567] Zur Koppelung der „Regional Code Playback Control" mit CSS durch einen Know-how-Lizenzvertrag s. unten Teil 2, C II 2 b. Aus Sicherheitsgründen müssen die DVD-Spieler seit dem 1. 1. 2000 die „Regional Code Playback Control" auf Hardware-Ebene unterstützen (sog. „Region Playback Control Phase II"), s. unten Fn. 930.

4. Content Protection for Recordable and Prerecorded Media (CPRM/CPPM)

Die „Content Protection for Recordable Media (CPRM)"-Spezifikation,[568] die von vier Computer- und Unterhaltungselektronikherstellern entwickelt wird,[569] ermöglicht die sichere Speicherung digitaler Audio- und Video-Inhalte auf physikalischen auswechselbaren Speichermedien wie der beschreibbaren DVD und ähnlichem.[570] Alle Inhalte werden kryptographisch mit dem Medium fest verbunden, auf dem sie abgespeichert werden. Dadurch wird verhindert, daß der verschlüsselte Inhalt auf ein anderes Medium kopiert wird und dort entschlüsselt werden kann.[571] Beispielsweise kann B von A eine CPRM-geschützte DVD ausleihen und auf seinem eigenen DVD-Spieler anschauen. Er kann die DVD aber nicht

[568] <http://www.4centity.com/4centity/tech/cprm>. CPRM ist Teil der übergreifenden CPSA s. dazu Teil 1, D IV 1. Nähere Informationen bei *Intel/IBM/Matsushita/Toshiba*, CPRM Specification – Introduction and Common Cryptographic Elements.

[569] Intel, IBM, Matsushita, Toshiba, die mitunter auch „4C" (für „4 companies") genannt werden; s. a. <http://www.4centity>. com. Zur lizenzrechtlichen Seite von CPRM/CPPM s. unten Teil 2, C II.

[570] Dies können auch SD Memory Cards, CompactFlash-Karten und das IBM Microdrive sein. Zum Einsatz von CPRM bei beschreibbaren DVDs s. *Intel/IBM/Matsushita/Toshiba*, CPRM Specification – DVD Book. Zum Einsatz bei SD Memory Cards hinsichtlich Audiodaten s. *Intel/IBM/Matsushita/Toshiba*, CPRM Specification – SD Memory Card Book. CPRM ist jedoch nicht auf diese Speichermedien beschränkt. Im Dezember 2000 gingen Meldungen durch die Presse, wonach CPRM in die ATA-Spezifikation, einem weit verbreiteten Standard für normale Festplatten, übernommen werden soll und dadurch Kopierschutzmechanismen zukünftig auch bei normalen Festplatten greifen würden, was beispielsweise das Erstellen von Sicherungskopien beeinträchtigen könnte, s. <http://www.theregister.co.uk/content/2/15620.html>; <http://news.cnet.com/news/0–1005–200–4292282.html> sowie den Beitrag von *John Gilmore* vom 18. 1. 2001 in der Mailingliste
yptography@c2.net, erhältlich unter <http://cryptome.org/jg-wwwcp.htm>. Diese Berichte entsprachen zumindest teilweise nicht den tatsächlichen Plänen des ATA-Standardisierungsgremiums T13. Aufgrund der öffentlichen Kritik wurde der Vorschlag für die ATA-Spezifikation nochmals deutlich auf mobile Speichermedien beschränkt, wozu allerdings auch mobile Festplatten wie das IBM Microdrive gehören können, s. *Lotspiech*, S. 1; *Intel/IBM/Matsushita/Toshiba*, CPRM Specification – Portable ATA Storage Book, S. 1–1. S. dazu auch <http://www.4centity.com/4centity/data/tech/cprmfactsheet.pdf>; *Bögeholz*, c't 2/2001, S. 24 f.

[571] Zu diesem Zweck wird beim Verschlüsselungsvorgang eine individuelle Seriennummer („media identifier") desjenigen Speichermediums mitverwendet, auf dem der Inhalt gespeichert wird. Der „media identifier" wird beim Fertigungsprozeß des Speichermediums in einem Bereich des Speichermediums gespeichert, der später von Schreibgeräten physikalisch nicht überschrieben werden kann. Die Entschlüsselung von einem anderen Medium aus, auf das der verschlüsselte Inhalt kopiert wurde, schlägt fehl, da das neue Medium über einen anderen „media identifier" verfügt und ein Kopieren des „media identifiers" nicht möglich ist. S. dazu *Intel/IBM/Matsushita/Toshiba*, CPRM Specification – Introduction and Common Cryptographic Elements, S. 1–1 f.; *Intel/IBM/Matsushita/Toshiba*, CPRM Specification – DVD Book, S. 3–1 ff.; *Taylor*, DVD Demystified, S. 194 f., 489.

auf einen DVD-Rohling kopieren und diese Kopie anschauen. Durch CPRM sollen Raubkopien verhindert werden.[572] Zu diesem Zweck enthält CPRM Verschlüsselungsmechanismen, ein System zum Schlüsselmanagement sowie die Möglichkeit, kompromittierte Geräte von der weiteren Nutzung CPRM-geschützter Inhalte auszuschließen („device revocation").[573] CPRM wird von allen DVD-Schreibgeräten unterstützt, die nach 1999 vertrieben wurden.[574]

Ein eng verwandtes Verfahren ist „Content Protection for Prerecorded Media" (CPPM), das für Speichermedien gedacht ist, die vom Nutzer nicht beschrieben werden können. Es wird insbesondere bei DVD-Audio eingesetzt.[575] Durch eine Koppelung des Verschlüsselungsverfahrens an das individuelle Speichermedium sollen Raubkopien CPPM-geschützter Medien unmöglich gemacht werden.[576] CPPM enthält neben Kopierschutzinformationen wie CPRM Verschlüsselungsmechanismen, ein System zum Schlüsselmanagement sowie die Möglichkeit, kompromittierte Speichermedien von der weiteren Nutzung CPPM-geschützter Inhalte auszuschließen.

---

[572] *Taylor*, DVD Demystified, S. 194.

[573] S. zum ganzen *Intel/IBM/Matsushita/Toshiba*, CPRM Specification – Introduction and Common Cryptographic Elements; *Taylor*, DVD Demystified, S. 194 f. Für die Ausschließung kompromittierter Medien bedient sich CPRM eines „broadcast encryption"-Verfahrens, hinsichtlich des Authentisierungsverfahren greift CPRM auf CSS zurück, *Taylor*, DVD Demystified, S. 489; *Intel/IBM/Matsushita/Toshiba*, CPRM Specification – DVD Book, S. 6–1 ff.

[574] *Taylor*, DVD Demystified, S. 194. S. dazu auch *Intel/IBM/Matsushita/Toshiba*, CPRM Specification – DVD Book.

[575] Ursprünglich sollte bei Audio-DVDs ein verbessertes CSS-System eingesetzt werden (sog. CSS2). Nachdem CSS geknackt worden war, wurde 1999 stattdessen CPPM ausgewählt, das insgesamt robuster als CSS ist, s. *Taylor*, DVD Demystified, S. 193; *Marks/Turnbull*, EIPR 2000, 198, 209. Zu den technischen Einzelheiten s. *Intel/IBM/Matsushita/Toshiba*, CPPM Specification – DVD Book.

[576] Zur Entschlüsselung berechnet das Endgerät aus einem im Endgerät gespeicherten „device key" und einem auf dem Speichermedium abgespeicherten „media key block" einen geheimen „media key". Aus diesem „media key" kann mit Hilfe einer eindeutigen Seriennummer, mit der jedes Speichermedium ausgestattet ist (sog. „album identifier"), ein „content key" errechnet werden. Mit diesem „content key" kann dann der verschlüsselte Inhalt dechiffriert werden. Der „album identifier" wird bei DVDs beim Fertigungsprozeß in einem Bereich der DVD gespeichert, der von DVD-Schreibgeräten später physikalisch nicht beschrieben werden kann (sog. „lead-in area"). Ein Kopieren des Inhalts auf eine beschreibbare DVD ist zwecklos, da der „album identifier" nicht mitkopiert wird, so daß eine Entschlüsselung unmöglich ist. S. zu den Einzelheiten *Intel/IBM/Matsushita/Toshiba*, CPPM Specification – Introduction and Common Cryptographic Elements, S. 1–1 f.; *Intel/IBM/Matsushita/Toshiba*, CPPM Specification – DVD Book, S. 2–2 f.; *Taylor*, DVD Demystified, S. 193 f., 488. Hinsichtlich des Authentisierungsverfahren greift CPRM auf CSS zurück, *s. Intel/IBM/Matsushita/Toshiba*, CPPM Specification – DVD Book, S. 2–8 f.

5. Secure Digital Music Initiative (SDMI)

1998 nahm die Verbreitung von Musik über das Internet im sogenannten MP3-Format[577] deutlich zu. Da das MP3-Format selbst über keinerlei Kopierschutzmechanismen verfügt,[578] wurde teilweise schon der Tod der Musikindustrie heraufbeschworen. Die Tonträgerindustrie und ihre Interessenvertretungen[579] versuchten auf unterschiedlichen Wegen, diese Gefahr zu bannen. So verklagten sie einerseits – erfolglos – einen Hersteller eines MP3-Abspielgerätes.[580] Andererseits gründeten sie Anfang 1999 die „Secure Digital Music Initiative" (SDMI), der inzwischen etwa 150 Unternehmen aus der Musik-, Computer- und Unterhaltungselektronik-Branche angehören.[581]

Ziel von SDMI ist es, eine Spezifikation zu erstellen, die das sichere Abspielen, Kopieren und Aufnehmen digitaler Audiodaten auf tragbaren Geräten, Computern usw. unter Kontrolle eines DRM-Systems ermöglicht. Dabei legt SDMI nicht nur eine Schnittstelle zu proprietären DRM-Systemen fest, sondern standardisiert auch selbst die Anforderungen an die DRM-Systeme.[582] Derzeit geht es hauptsächlich um die Integrierung

---

[577] MP3 ist ein Dateiformat, das durch einen guten Kompressionsmechanismus die effiziente Übertragung von Musikdateien ermöglicht. MP3 steht als Abkürzung für „MPEG-1 Audio Layer III". Das MP3-Format hat in den letzten Jahren einen wahren Siegeszug angetreten. Beispielsweise sind fast alle über Napster und ähnliche P2P-Systeme gehandelten Musikdateien im MP3-Format abgespeichert.

[578] Zwar sind im MP3-Datenformat zwei Bits für Kopierkontrollinformationen reserviert; dort könnten die Metadaten des von DAT-Geräten her bekannten SCMS untergebracht werden. Diese Bits werden jedoch faktisch nicht verwendet. Auch existiert bei MP3-Abspielhardware oder -software kein Mechanismus, um diese Metadaten umzusetzen und das unberechtigte Kopieren digitaler Inhalte zu verhindern. Allerdings entwickelte das Fraunhofer-Institut für Integrierte Schaltungen, das MP3 entwickelt hatte, daneben eines der ersten DRM-Systeme namens MMP, s. dazu unten Fn. 623.

[579] In den USA die „Recording Industriy Association of America" (RIAA), <http://www.riaa.com>, in Europa die „International Federation of Phonographic Industries" (IFPI), <http://www.ifpi.org>.

[580] Die RIAA verklagte Diamond Multimedia Systems, weil deren „Rio Player" nicht das von DAT-Geräten her bekannte Kopierschutzsystem SCMS verwende. Dazu sei Diamond nach dem Audio Home Recording Act (17 U.S.C. §§ 1001 ff.) verpflichtet. Die Klage wurde als unbegründet abgewiesen, Recording Industry Association of Amercia v. Diamond Multimedia Systems, 180 F. 3d 1072 (9th Cir. 1999), deutsche Übersetzung in GRUR Int. 1999, 974 ff.

[581] <http://www.sdmi.org>. SDMI wurde bis Januar 2001 von *Leonardo Chiariglione* geleitet, der auch Gründer anderer wichtiger Initiativen im DRM-Bereich ist (MPEG, OPIMA, FIPA). Zur Entstehungsgeschichte von SDMI s. *Marks/Turnbull*, EIPR 2000, 198, 210 f.

[582] Die Realisierung dieser Anforderungen bleibt dann jedoch einzelnen Unternehmen überlassen, s. *Hartung/Ramme*, IEEE Communications Magazine 78, 81 (November 2000). Ein „SDMI-kompatibles" Gerät kann daher nicht notwendigerweise alle „SDMI-kompatiblen" digitalen Inhalte abspielen. Die einzige wirkliche Standardisierung einer Technologie betraf bisher das für die SDMI-Phase I verwendete Wasserzeichen von Verance, s. dazu unten Fn. 584.

technischer Schutzmaßnahmen in tragbare MP3-Player.[583] Digitale Audiodaten sollen mit einer robusten Markierung versehen werden. Diese Markierung enthält die Information, ob von den Audiodaten Kopien erstellt werden dürfen oder nicht. Ist dies nicht der Fall, spielt ein SDMI-kompatibles Abspielgerät die Audiodaten nicht ab. Trotz langwieriger Verhandlungen ist von SDMI bis heute noch kein endgültiger Standard verabschiedet worden.[584]

---

[583] *Secure Digital Music Initiative*, SDMI Portable Device Specification Part 1, S. 14 ff. Während die SDMI-Spezifikationen anfänglich umfangreiche Vorschriften über Metadaten enthielten (auch bezüglich der Beschreibung von Nutzungsbedingungen), wurde wegen der Komplexität solcher Fragen dieser Bereich in späteren Versionen nur noch eingeschränkt behandelt, s. *PricewaterhouseCoopers*, Metadata Watch Report #1, S. 14 f.

[584] Erste Standardisierungen im Juli 1999 betrafen Fragen der Markteinführung. SDMI hatte sich für ein zweiphasiges Verfahren entschieden, um die Markteinführung SDMI-kompatibler Geräte zu beschleunigen. Dadurch sollte erreicht werden, daß SDMI-kompatible Geräte schon auf den Markt gebracht werden können (Phase I), bevor der vollständige SDMI-Standard (Phase II) verabschiedet wurde. Diese Geräte sollten dann zu einem späteren Zeitpunkt durch ein Upgrade mit dem vollständigen SDMI-Standard kompatibel gemacht werden. Im Juli 1999 wurde die Phase-I-Spezifikation (SDMI Portable Device Specification Part I) veröffentlicht. Danach müssen Geräte beim Abspielen von Inhalten nach einem Wasserzeichen suchen, das dem Gerät mitteilt, ob inzwischen der SDMI-Phase-II-Standard verabschiedet wurde. Phase-II-Inhalte sind auf einem Phase-I-Gerät nur nach einem (freiwilligen) Upgrade des Geräts abspielbar. S. dazu *Secure Digital Music Initiative*, SDMI Portable Device Specification Part 1, S. 21. Weiterhin wurde in einem Zusatzdokument vom September 1999 festgelegt, daß Phase-I-kompatible Geräte nach einem sog. „Copy Control Information" (CCI) Bit suchen müssen, das dem Gerät anzeigt, ob der digitale Inhalt kopiert werden darf oder nicht. Wenn das Bit anzeigt, daß der Inhalt nicht mehr kopiert werden darf, so muß das Gerät den Inhalt zurückweisen. S. dazu *Secure Digital Music Initiative*, Amendment 1 to SDMI Portable Device Specification, Part I, S. 1 f. Nach einer offenen Ausschreibung wurde im September 1999 entschieden, daß dieses „CCI Bit" – primitive Metadaten über Nutzungsbedingungen – mit Hilfe eines von Verance (<http:// www.verance.com>, früher ARIS Technologies) entwickelten Wasserzeichenverfahrens direkt in die digitalen Inhalte eingebettet werden muß. Das Bit (sog. „trigger"), das dem Gerät mitteilt, daß inzwischen die SDMI Phase II existiert, kann ebenfalls mit diesem Wasserzeichenverfahren eingebettet werden; das schreibt SDMI jedoch nicht zwingend vor. S. zum ganzen *Secure Digital Music Initiative*, Amendment 1 to SDMI Portable Device Specification, Part I, S. 1 f.; *Marks/Turnbull*, EIPR 2000, 198, 211. Zum Wasserzeichen-Verfahren von Verance, das von der 4C Entity lizensiert wird, s. *4C Entity*, 4C 12 Bit Watermark Specification; zu den Bedingungen, unter denen dieses Wasserzeichenverfahren lizenziert werden kann, s. unten Teil 2, C II. Im Februar 2000 veröffentlichte SDMI dann einen Aufruf, dem Konsortium Technologien vorzuschlagen, die die robuste Markierung zu Kopierschutzzwecken in der Phase II ermöglicht, *Secure Digital Music Initiative*, Call for Proposals for Phase II Screening Technology. Im September 2000 rief SDMI einen öffentlichen Wettbewerb über $ 10.000 aus; das Preisgeld sollte erhalten, wer eines von sechs von SDMI in Erwägung gezogenen Markierungstechnologien knackte. Zu diesem Zweck wurden Klangbeispiele im Internet veröffentlicht, die mit den entsprechenden Systemen markiert waren. Die Aufgabe bestand darin, diese Markierungen zu entfernen, ohne die Klangqualität hörbar zu verschlechtern. Bei den sechs von SDMI zur Verfügung gestellten Klangbeispielen waren vier mit Wasserzeichenverfahren markiert. Der

6. eBooks

Auch in Lesegeräten für sogenannte „eBooks" – also digitale Texte – sind DRM-Komponenten integriert.[585] Mehrere Standardisierungsinitiativen nehmen sich DRM-Fragen bei eBooks an.[586] Die Entwicklung von Standards zur Interoperabilität von DRM-Systemen wird für den Erfolg von eBooks als entscheidend angesehen.[587]

Im Rahmen des „Open eBook Forum" (OEB)[588] wurde 1999 ein Dokument verabschiedet, welches das in eBooks verwendete Datenformat standardisieren soll.[589] Das Format baut auf XML auf. Hinsichtlich der in eBooks verwendeten Metadaten für die Identifizierung von Inhalt und Rechteinhaber greift es auf den Dublin Core[590] zurück.[591] Eine Standardisierung von Metadaten für Nutzungsbedingungen fehlt,[592] ebenso die Integrierung sonstiger technischer Schutzmaßnahmen. Dagegen wurde im Rahmen der „Electronic Book eXchange Working Group" (EBX)[593] eine umfassende DRM-Spezifikation für eBooks erarbeitet.[594] Der Nutzer

---

Wettbewerb war in Technikerkreisen hoch umstritten. So hatte die Electronic Frontier Foundation (EFF) aus San Francisco zum Boykott des Wettbewerbs aufgerufen, da man nicht noch die Tonträgerindustrie bei der Entwicklung eines sicheren Kopierschutzsystems unterstützen solle. Während SDMI selbst am Ende des Wettbewerbs bekannt gab, daß nur zwei Systeme geknackt worden waren, sagten mehrere Forschergruppen aus, sie hätten mehr oder teilweise sogar alle Systeme erfolgreich geknackt. Die zwei bekanntesten Forschergruppen stammten einerseits von der Princeton und Rice University sowie dem Xerox PARC (s. dazu <http://www. cs.princeton.edu/sip/sdmi>), andererseits aus Frankreich (s. dazu <http://www.julienstern.org/sdmi>). Zu den längeren Zielen von SDMI s. *Marks/Turnbull*, EIPR 2000, 198, 211. Zu SDMI aus rechtlicher Sicht umfassend *Levy*, 5 Va. J. L. & Tech. 12 ff. (2000).

585 Die verwendeten Begriffe differieren erheblich. Im folgenden wird als „eBook" ein digitaler Text bezeichnet, der auf einem eBook-Lesegerät („ebook reading device") betrachtet werden kann. Dieses Lesegerät kann entweder ein spezielles Softwareprogramm (beispielsweise die eBook Reader von Microsoft und Adobe) oder ein spezielles Hardwaregerät (beispielsweise das Rocket eBook) sein. Die Idee, spezielle handliche Hardwaregeräte zum Betrachten digitaler Texte zu entwickeln, ist nicht neu. Schon ab Ende der 60er Jahre wurde am Palo Alto Research Center von Xerox (Xerox PARC) an solchen Geräten gearbeitet; bekannt ist insbesondere das „Dynabook" von *Alan Kay*. Grundlegend *Kay/Goldberg*, 10 (3) IEEE Computer 31 (1977). Zur Geschichte s. weiterhin *Cawkell*, 51 (2) Aslib Proceedings 54, 55 (Februar 1999) m. w. N., zu den Entwicklungen am Xerox PARC s. *Hiltzik*, S. 94, 163 ff.

586 S. dazu *Mooney*, 7 (1) D-Lib Magazine (January 2001).

587 *Association of American Publishers*, Digital Rights Management for Ebooks, S. 6, 26 ff.

588 <http://www.openebook.org>.

589 *Open eBook Forum*, OEB Publication Structure 1.0.

590 S. dazu oben Teil 1, C II 2 a aa 2 c.

591 *Open eBook Forum*, S. 12 ff.

592 S. *Open eBook Forum*, S. 18.

593 <http://ebxwg.org>. EBX und OEB kündigten im Februar 2001 an, sich zusammenzuschließen.

594 *Electronic Book Exchange Working Group*, The EBX System Specification Version 0.8.

kann vom Verleger einen digitalen Text in verschlüsselter Form erwerben. Nach einer entsprechenden Zahlung erhält er einen dazugehörenden Dechiffrier-Schlüssel, mit dem er den Text entschlüsseln kann.[595] Der Nutzer kann den digitalen Text auch an Dritte weitergeben. Jedoch stellt das eBook-Lesegerät sicher, daß der digitale Text dann bei ihm selbst gelöscht wird.[596] Die Nutzungsbedingungen werden in sogenannten „EBX vouchers" auf XML-Basis codiert.[597] Der Standard enthält eine eigenständige Definition hinsichtlich der Metadaten für Nutzungsbedingungen,[598] greift aber hinsichtlich der Metadaten für die Identifizierung von Inhalt und Rechteinhaber auf den Dublin Core zurück.[599] Daneben umfaßt der Standard auch eine Schlüsselverwaltung[600] sowie Authentisierungsmechanismen.[601] Neben dieser Standardisierungsinitiative hat die „Association of American Publishers" im Rahmen ihrer „Open eBook Publishing Standards Initiative"[602] detallierte Anforderungen an Metadaten für Nutzungsbedingungen entwickelt.[603]

III. Schutz bei Datenübertragungen

Um die Sicherheit des gesamten DRM-Systems gewährleisten zu können, reicht es nicht aus, wenn die einzelnen Geräte eines DRM-Systems sicher ausgestaltet sind. Vielmehr muß auch die Kommunikation zwischen den Geräten gegenüber Angriffen abgesichert sein. Werden digitale Inhalte, Metadaten und ähnliches zwischen zwei DRM-kompatiblen Geräten übertragen, so muß neben einer Verschlüsselung der Daten auch ihre

---

595 Genauer funktioniert das Verfahren wie folgt: Der Verleger eines digitalen Textes verschlüsselt das eBook mit einem symmetrischen Verschlüsselungsverfahren. Jedes eBook-Lesegerät ist mit einem individuellen asymmetrischen Schlüsselpaar ausgestattet. Will ein Nutzer einen digitalen Text erwerben, so lädt er einerseits den verschlüsselten digitalen Text aus dem DRM-System herunter. Andererseits verschlüsselt der Verleger oder Betreiber des DRM-Systems den symmetrischen Schlüssel, mit dem der digitale Text verschlüsselt wurde, seinerseits mit dem individuellen öffentlichen Schlüssel des Nutzers. Mit Hilfe seines nur ihm bekannten privaten Schlüssels kann der Nutzer diese Nachricht entschlüsseln und erhält damit den symmetrischen Schlüssel zum Entschlüsseln des digitalen Textes. S. näher *Electronic Book Exchange Working Group*, S. 13 f.

596 *Electronic Book Exchange Working Group*, S. 18 f., 64 ff.

597 *Electronic Book Exchange Working Group*, S. 14, 85 ff.

598 *Electronic Book Exchange Working Group*, S. 85 ff. S. dazu oben Teil 1, C II 2 a bb 3.

599 *Electronic Book Exchange Working Group*, S. 82 ff.

600 *Electronic Book Exchange Working Group*, S. 38 ff.

601 *Electronic Book Exchange Working Group*, S. 95 ff.

602 <http://www.publishers.org/home/ebookstudy.htm> und *Association of American Publishers*, Metadata Standards for Ebooks; *dies*. Numbering Standards for Ebooks; *dies*., Digital Rights Management for Ebooks. Zu DOI für eBooks (DOI-EB) s. <http://www.doi.org/ebooks.html>.

603 *Association of American Publishers*, Digital Rights Management for Ebooks, S. 34 ff.

Authentizität und Integrität gewährleistet sein. Zu diesem Zweck existieren mehrere Standards, die entweder die sichere Kommunikation im allgemeinen Internet (dazu unten 1) oder die Kommunikation zwischen verschiedenen Endgeräten eines DRM-Systems betreffen (dazu unten 2).

1. Übertragungen im Internet: IPSec

Ein DRM-System kann viele Daten – Inhalte, Metadaten, Systemkontrolldaten und ähnliches – über das Internet übertragen. Seit einigen Jahren existiert mit der sogenannten „IPSec"-Protokollfamilie eine Ergänzung zur TCP/IP-Protokollsuite. IPSec führt Sicherheitsmaßnahmen auf der IP-Ebene[604] ein und steht damit allen Anwendungen im Internet zur Verfügung.[605] IPSec stellt ein standardisiertes, anwendungsunabhängiges, robustes und erweiterbares Sicherheitskonzept zur Verfügung. Es ermöglicht Verschlüsselung sowie Authentizitäts- und Integritätsprüfung des gesamten Datenverkehrs auf IP-Ebene.[606] Von dieser Sicherheitsarchitektur können alle über das Netzwerk laufenden Anwendungen, also auch ein DRM-System, Gebrauch machen.[607] Dies kann die Sicherheit eines DRM-Systems erhöhen.

---

[604] Die Kommunikation wird im Internet durch die TCP/IP-Protokollfamilie ermöglicht, die auf einem Schichtenmodell aufbaut, s. dazu *Doraswamy/Harkins*, S. 55; *Loshin*, S. 17 ff. Eine Softwareanwendung kommuniziert mit der Anwendungsschicht („application layer"), die die Daten dann über die Transport- („transport layer") und die Netzwerkschicht („network layer") bis hinunter zur Datenübertragungsschicht („data link layer") weiterreicht. Die Datenübertragungsschicht ist dann für die eigentliche Übertragung der IP-Pakete („network layer") über ein physikalisches Netzwerk verantwortlich. Werden Sicherheitsfunktionen in einer recht tiefen Netzwerkschicht realisiert, so können alle Anwendungen auf diese Funktionalität der Netzwerkprotokolle zurückgreifen. Damit werden Sicherheitsfunktionen unabhängig von bestimmten Anwendungen und Betriebssystemen.

[605] Zu IPSec allgemein s. *Doraswamy/Harkins*; *Stallings*, 3 (1) Internet Protocol Journal 11 (März 2000); *Doraswamy/Harkins* sowie die Homepage der IPSec Working Group der IETF, <http://www.ietf.org/html.charters/ipsec-charter.html>. Dort findet sich auch eine Auflistung der beinahe 20 RFCs, in denen IPSec standardisiert ist, von denen die wichtigsten in ihrer heutigen Fassung aus dem Jahre 1998 stammen. Das grundlegende RFC ist *Kent/Atkinson*, RFC 2401. Schon seit längerem bestehen Protokolle, die eine verschlüsselte Kommunikation mit Authentizitäts- und Integritätsprüfung auf der Transportschichtebene ermöglichen, insbesondere das von Netscape entwickelte „Secure Sockets Layer"-Protokoll SSL, s. oben Fn. 481.

[606] Es kann hier nicht auf die Einzelheiten der recht komplexen IPSec-Spezifikation eingegangen werden. Grundsätzlich besteht IPSec aus drei Teilen: einem Protokoll, das u. a. die Authentizitäts- und Integritätsprüfung von IP-Paketen ermöglicht („Authentication Header", AH), einem Protokoll, das zusätzlich noch die Verschlüsselung der IP-Pakete ermöglicht („Encapsulation Security Payload", ESP), und einem Protokoll zur Schlüsselverwaltung („Internet Key Exchange", IKE). S. zum ganzen *Stallings*, 3 (1) Internet Protocol Journal 11 (März 2000); *Doraswamy/Harkins*.

[607] *Stallings*, 3 (1) Internet Protocol Journal 11, 12 (März 2000). Neben E-Commerce-Anwendungen wie DRM-Systemen kann IPSec u. a. in sog. „Virtual Private Networks" (VPNs) eingesetzt werden. Teilweise werden DRM-Systeme auch als spezielle VPNs angesehen.

2. Übertragungen zwischen Endgeräten

Beim Nutzer eines DRM-Systems werden digitale Inhalte oft zwischen verschiedenen Endgeräten oder auch innerhalb eines Endgeräts zwischen verschiedenen Komponenten übertragen. So werden Inhalte vom Computer zum tragbaren MP3-Spieler übertragen, um dort als Musik ausgegeben werden zu können, oder sie werden zum angeschlossenen Bildschirm oder zur Festplatte übertragen, um dort angezeigt beziehungsweise abgespeichert werden zu können. In einem vollständigen DRM-System müssen auch diese Übertragungswege mit technischen Schutzmaßnahmen versehen sein. Ansonsten könnte ein Angreifer die digitalen Inhalte auf dem Übertragungsweg unverschlüsselt abhören. Außerdem muß die Integrität und Authentizität der Geräte sichergestellt sein, zwischen denen die Inhalte übertragen werden. Ansonsten könnte ein Angreifer ein manipuliertes Gerät in das DRM-System „einschmuggeln".

a) Digital Transmission Content Protection (DTCP)

Diesem Problem nahm sich die „Digital Transmission Discussion Group" (DTDG) im Rahmen der CPTWG an. Nach vielen Vorschlägen setzte sich ein System der Unternehmen Hitachi, Intel, Matsushita, Sony und Toshiba durch, das den offiziellen Titel „Digital Transmission Content Protection" (DTCP) trägt.[608] DTCP will Audio- und Videodaten bei der Übertragung von einem Endgerät zum anderen Endgerät (PC zu digitalem Fernseher, DVD-Spieler zu PC, DVD-Spieler zu digitalem Fernseher, digitaler Videorecorder zu PC, digitaler Videorecoder zu digitalem Fernseher etc.) schützen.[609] Dadurch kann ein PC zum Beispiel sicherstellen, daß er die geschützten digitalen Inhalte nur zu einem Abspielgerät überträgt, das selbst DRM-kompatibel ist und Angreifern keinen Zugriff auf

---

[608] <http://www.dtcp.com>. Wegen der beteiligten fünf Unternehmen wird das System manchmal auch „5C" (für „5 companies") genannt. S. zur Entstehungsgeschichte näher *Marks/Turnbull*, EIPR 2000, 198, 208; *Bloom/Cox/Kalker/Linnartz/Miller/Traw*, 87 Proc. IEEE 1267, 1270 f. (1999); *Datta*. Ausführliche Informationen zu DTCP enthalten *Hitachi/Intel/Matsushita/Sony/Toshiba*, DTCP Specification, und *dies.*, 5C DTCP White Paper. Zum Überblick s. *Taylor*, DVD Demystified, S. 199. DTCP wurde für ein spezielles Übertragungssystem namens „Firewire" entwickelt, das die einfache Verbindungsmöglichkeit unterschiedlichster Gerätetypen wie Festplatten, Scanner oder Videokamers über einen gemeinsamen seriellen Datenbus ermöglicht und gerade für die Verbindung von Computer und Audio-/Videoequipment gut geeignet ist. Firewire ist nur der gebräuchliche Name, der von Apple geprägt wurde. Tatsächlich handelt es sich bei Firewire um eine Implementierung des IEEE-1394-Standards. S. dazu *Dembowski*, c't 2/1997, S. 284 ff. Informationen zu IEEE 1394 finden sich bei der „1394 Trade Association" unter <http://www.1394ta.org>. Es wird jedoch davon ausgegangen, daß DTCP auch in anderen Datenbus-Systemen (wie z. B. USB) Einsatz finden kann, s. *Hitachi/Intel/Matsushita/Sony/Toshiba*, DTCP Specification, S. 15, 77 ff.; *Taylor*, DVD Demystified, S. 199.

[609] Zur Koppelung von DTCP mit CSS durch eine Know-how-Lizenz s. unten Teil 2, C II 2 b.

die ungeschützten Inhalte gibt.[610] Die digitalen Inhalte werden nach einer gegenseitigen Authentisierung verschlüsselt übertragen, der entsprechende Schlüssel wird in kurzen Intervallen (zwischen 30 Sekunden und 2 Minuten) gewechselt.[611] Das System kann auch manipulationssicher Metadaten über Nutzungsbedingungen übertragen.[612] Schließlich ist es möglich, kompromittierte Geräte von der weiteren Nutzung geschützter Inhalte auszuschließen („device revocation").[613]

b) High-bandwidth Digital Content Protection System (HDCP)

Das von Intel entwickelte „High-bandwidth Digital Content Protection System" (HDCP)[614] ermöglicht die sichere Kommunikation zwischen einem Computer bzw. dessen Grafiksystem und einem digital angesteuerten Bildschirm.[615] Dies wird durch drei Komponenten erreicht, die auch schon von anderen beschriebenen Systemen bekannt sind (gegenseitige Authentisierung der beteiligten Geräte, verschlüsselte Datenübertragung und Möglichkeit des Ausschlusses kompromittierter Geräte).[616] Durch HDCP kann ein DRM-System gewährleisten, daß die Übertragung der digitalen Inhalte bis zum letztmöglichen Punkt – dem Bildschirm, an dem der Inhalt ausgegeben wird – technisch geschützt ist.

---

610 Bei DTCP „Device Authentication and Key Exchange" (AKE) genannt, s. *Hitachi/Intel/Matsushita/Sony/Toshiba*, DTCP Specification, S. 15; *dies.*, 5C DTCP White Paper, S. 1 f.

611 Zum Schlüsselwechsel s. *Hitachi/Intel/Matsushita/Sony/Toshiba*, DTCP Specification, S. 45. Grundsätzlich bedient sich DTCP asymmetrischer Verschlüsselungsverfahren, s. *ebda.*, S. 29 ff.

612 Bei DTCP „Copy control information" (CCI) genannt. Diese Metadaten können Informationen enthalten, daß die Inhalte überhaupt nicht, nur einmal, ab jetzt nicht mehr oder aber unbegrenzt kopiert werden dürfen, s. *Hitachi/Intel/Matsushita/Sony/Toshiba*, DTCP Specification, S. 15, 47; *Marks/Turnbull*, EIPR 2000, 198, 209. Die manipulationssichere Übertragung wird erreicht, indem bei einer Veränderung der Metadaten die Entschlüsselung der digitalen Inhalte fehlschlägt, s. *Hitachi/Intel/Matsushita/Sony/Toshiba*, DTCP Specification, S. 46 f.; *dies.*, 5C DTCP White Paper, S. 2 f.

613 Bei DTCP „system renewability" genannt, s. dazu oben Teil 1, C I 1 b bb.

614 *Intel*, High-bandwidth Digital Content Protection System; <http://www.digital-cp.com>.

615 Das Verfahren ist auf die „Digital Visual Interface (DVI)"-Spezifikation zugeschnitten, einem Standard aus dem Jahr 1999 zum Anschluß digital angesteuerter Displays an Computern, der den traditionellen VGA-Standard ersetzen soll. S. dazu die Homepage der „Digital Display Working Group" (DDWG) unter <http://www.ddwg.org> und *Taylor*, DVD Demystified, S. 199 f. Zur Koppelung von HDCP mit CSS und DVI durch die CSS-Know-how-Lizenz s. unten Teil 2, C II 2 b.

616 S. dazu ausführlich *Intel*, High-bandwidth Digital Content Protection System, S. 4 ff. Zum Überblick s. *Taylor*, DVD Demystified, S. 200, 490. Die gegenseitige Authentisierung wird aus Sicherheitsgründen etwa alle zwei Sekunden wiederholt.

IV. Übergreifende Schutzarchitekturen

Wie gezeigt wurde, bestehen DRM-Systeme nicht nur aus einer Vielzahl unterschiedlicher technischer Schutzmaßnahmen. Es existiert auch eine Vielzahl unterschiedlicher Standards, die jeweils Teilbereiche des „Digital Rights Management" abdecken. Ein DRM-System kann eine sichere Vertriebsplattform für digitale Inhalte nur gewährleisten, wenn all diese Komponenten und Standards ineinandergreifen und ein einheitlich hohes Schutzniveau gewährleisten. Daher existieren Standards, die auf abstrakter Ebene Fragen einer übergreifenden DRM-Schutzarchitektur regeln.

1. Content Protection System Architecture (CPSA)

Die von Intel, IBM, Matsushita und Toshiba entwickelte „Content Protection System Architecture" (CPSA)[617] versucht, einen allgemeinen Rahmen für den PC- und Unterhaltungselektronikbereich zu schaffen, in dem die bestehenden und zukünftige technische Schutzmaßnahmen für Audio- und Video-Inhalte ineinandergreifen. Es soll ein einheitliches Schutzniveau für PCs, DVD-Spieler und DVD-Aufnahmegeräte, Set-Top-Boxen, digitales Fernsehen, MP3-Geräte usw. geschaffen werden.[618]

2. Motion Picture Expert Group (MPEG)

Die „Motion Picture Expert Group" (MPEG) ist eine Arbeitsgruppe der „International Organisation for Standardisation" (ISO).[619] Seit 1988 hat MPEG zahlreiche technische Standards in Audio- und Video-Bereich entwickelt und verabschiedet, von denen der hauptsächlich am Erlanger Fraunhofer Institut für Integrierte Schaltungen[620] entwickelte Kompressionsmechanismus MP3[621] für Audiodateien der Bekannteste ist.[622] Mehrere MPEG-Standards enthalten Standardisierungen zu DRM-Fragen, insbesondere MPEG-4, MPEG-7 und MPEG-21.[623]

---

[617] *Intel/IBM/Matsushita/Toshiba*, Content Protection System Architecture. CPSA arbeitet eng mit SDMI und CPTWG zusammen.

[618] *Intel/IBM/Matsushita/Toshiba*, Content Protection System Architecture, S. 5. Zu diesem Zweck werden bestimmte Anforderungen an DRM-Systeme aufgestellt, beispielsweise die Sicherstellung der Integrität von Metadaten und die Verschlüsselung digitaler Inhalte. Als Beispiele für CPSA-konsistente Systeme werden u. a. CPRM, CSS, DTCP und HDCP genannt. S. *ebda.*, S. 7 ff.

[619] Der offizielle Titel der „Motion Picture Expert Group" lautet ISO/IEC JTC1/SC29/WG11 („Coding of Moving Pictures and Audio"). Ihre Homepage findet sich unter <http://www.cselt.it/mpeg>.

[620] <http://www.iis.fhg.de>.

[621] Auch dies ist nur eine populäre Abkürzung. Der Standard heißt tatsächlich MPEG-1 Audio Layer III.

[622] Auch mit anderen Standards ist MPEG höchst erfolgreich; so findet MPEG-2 u. a. beim digitalen Fernsehen und DVDs Anwendung. Zur Arbeit von MPEG und deren Standards s. *Chiariglione*.

[623] Auch MPEG-2 enthält gewisse DRM-Komponenten, insbesondere die Möglichkeit der Identifizierung von digitalen Inhalten sowie eine Anbindung an „conditional

Im 1993 begonnenen und 1998 in erster Fassung verabschiedeten MPEG-4-Standard, der insbesondere Fragen des Datenformats, der objektbasierten Datenrepräsentation sowie der Datenkompression für Multimedia-Applikationen betrifft,[624] wurden im Rahmen des sogenannten „Intellectual Property Management & Protection" (IPMP) technische DRM-Fragen für Audio und Video behandelt.[625] IPMP selbst standardisiert jedoch kein DRM-System, sondern nur Schnittstellen zwischen MPEG-4 und proprietären DRM-Systemen.[626] Dabei können auch mehrere proprietäre DRM-Systeme gleichzeitig unterstützt werden.[627] Die Arbeit am MPEG-7-Standard wurde 1996 begonnen, ist aber noch nicht abgeschlossen. Er beschäftigt sich schwerpunktmäßig mit dem Problem der Suche nach Video- und Audio-*Inhalten* und definiert zu diesem Zweck Verfahren zur inhaltlichen Beschreibung von Multimedia-Da-

access"-Systeme im Pay-TV-Bereich. So ist in MPEG-2 ein Datenfeld vorgesehen, in dem ISBN-, ISAN-, ISRC-, ISWC- und ähnliche Numerierungssysteme integriert werden können, s. dazu *Hill*, 87 Proc. IEEE 1228, 1235 (1999) und oben Fn. 151. S. weiterhin *Koenen*, S. 1. Die MPEG-1 Audio Layer III-Standardisierung (MP3) enthält keine DRM-Komponenten. Mitunter wird daher dem Fraunhofer Inistitut für Integrierte Schaltungen vorgeworfen, daß die heutigen Probleme der Musikindustrie mit raubkopierten MP3s vermieden worden wären, wenn sich die Entwickler nicht nur um Fragen der Kompression, sondern auch um Fragen des Urheberschutzes gekümmert hätten. Der Vorwurf ist in dieser Schärfe unberechtigt. Am Fraunhofer Institut für Integrierte Schaltungen wurde schon ab 1995 eines des ersten Systeme zum technischen Urheberschutz entwickelt („Multimedia Protection Protocol", MMP). Es wird im Music-on-Demand-Projekt der Deutschen Telekom – <http://www.audio-on-demand.de/mod> – eingesetzt. S. dazu *Rump*. Zu DRM-Fragen bei MPEG im Überblick s. *Koenen*.

624 Zu MPEG-4 im Überblick s. *Pereira*, 15 Signal Processing: Image Communication 271 ff. (2000).

625 S. dazu allgemein *Hill*, 87 Proc. IEEE 1228, 1235 ff. (1999); *Koenen*, S. 1 ff. IPMP kann daneben auch zur Vergütung von Patenten, die in MPEG-4-Software-Decodern beim Decodieren von MPEG-4-Inhalten berührt werden, verwendet werden. S. zu diesem Anwendungsbereich von DRM-Systemen, der außerhalb dieser auf das Urheberrecht konzentrierten Untersuchung steht, *Lacy/Rump/Kudumakis*, S. 5 ff.; *Koenen*, IEEE Spectrum 26, 29 (Februar 1999). Zur Anfang 2001 verabschiedeten MPEG-4 IPMP Extension s. *Koenen*, S. 3.

626 Einerseits enthält IPMP ein Numerierungssystem („Intellectual Property Identifiation Data Set", IPI), das etablierte Systeme wie ISBN, ISWC und DOI integriert, *Hill*, 87 Proc. IEEE 1228, 1236 (1999); *Herpel/Eleftheriadis*, 15 Signal Processing: Image Communciations 299, 305 f. (2000). Dabei können auch Datenfelder individuell definiert werden und die digitalen Inhalte in jeder gewünschten Granularität identifiziert werden, *Lacy/Rump/Kudumakis*, S. 4; *Koenen*, S. 2. Die IPI Data Sets enthalten aber keine Metadaten hinsichtlich der Nutzungsbedingungen. Andererseits können in sogenannten „IPMP Descriptors" und „IPMP Streams" Informationen über Zugangsberechtigungen sowie verwendete Schlüssel gespeichert und übertragen werden. Auf die Einzelheiten kann hier nicht eingegangen werden, s. allgemein *Herpel/Eleftheriadis*, 15 Signal Processing: Image Communciations 299, 306 (2000); *Lacy/Rump/Kudumakis*, S. 3 f. Ein Beispiel für die Interaktion zwischen IPMP und einem proprietären DRM-System gibt *Hartung/Ramme*, IEEE Communications Magazine 78, 80 (November 2000).

627 S. *Hartung/Ramme*, IEEE Communications Magazine 78, 79 (November 2000).

ten.[628] Auch für MPEG-7 wird an einer IPMP-ähnlichen Lösung für den DRM-Bereich gearbeitet; jedoch befinden sich die Arbeiten dazu noch in einer frühen Phase.[629] Im Mai 2000 begannen die Arbeiten an MPEG-21 („Multimedia Framework"), das Rahmenbedingungen für eine künftig konvergierende Multimediaumgebung setzen will. Dabei wird auch über die eindeutige Identifizierung und Beschreibung von Multimedia-Daten, über Metadaten für Rechteinhaber und Nutzungsbedingungen sowie sonstige DRM-Komponenten nachgedacht.[630] MPEG-21 will, auf den Entwicklungen von MPEG-7 aufbauend, einen einheitlichen Rahmen für DRM-Systeme schaffen.[631] Auch hier befindet sich die Arbeit jedoch noch in den Anfängen, mit ersten Ergebnissen ist nicht vor Ende 2001 zu rechnen.

3. Open Platform for Multimedia Access (OPIMA)

Die 1998 gegründete „Open Platform Initiative for Multimedia Access" (OPIMA),[632] eine Initiative im „Industrial Technical Agreement"-Programm der „International Electrotechnical Commission" (IEC),[633] hat eine standardisierte Multimedia-Plattform spezifiziert, die trotz unterschiedlicher proprietärer DRM-Systeme einen einheitlichen Zugriff auf multimediale Inhalte gewährleistet.[634] Unterschiedliche Anwendungen wie Pay-TV, Video-on-Demand, Audio-on-demand, Computerspiele, Internet-Dienste, Software-Distribution, Home Shopping und ähnliches sollen in einem einheitlichen Gerät genutzt werden können. Die OPIMA-Spezifikation ist für alle Medienarten (Audio, Video, Text etc.) und Hardwareumgebungen (Computer, Set-Top-Boxen, Music-Player etc.) konzipiert.[635] Ein gewisser Schwerpunkt von OPIMA liegt jedoch auf dem

---

[628] So ist es mit heutigen Suchmaschinen im Internet beinahe unmöglich, nach Bild- oder Video*inhalten*, also beispielsweise der Schlußszene aus dem Film *Casablanca*, zu suchen. Dies liegt an fehlenden Standards zur Beschreibung von Bildinhalten. Diesem Problem widmet sich MPEG-7. Während es bei MPEG-1, MPEG-2 und MPEG-4 schwerpunktmäßig um die Repräsentation digitaler Audio- und Video-Daten selbst ging, dreht es sich bei MPEG-7 um die Repräsentation von inhaltlichen Informationen über diese Audio- und Video-Daten. Dies ist nicht identisch mit Metadaten in dem in dieser Arbeit verstandenen Sinne. Das hauptsächliche Ziel von MPEG-7 ist, die Suche nach audiovisuellen Daten genauso einfach zu machen wie die Suche nach Text. S. zu MPEG-7 allgemein *Nack/Lindsay*, IEEE Multimedia 65 ff. (Juli/September 1999).

[629] S. dazu *Pereira*, MPEG-7 Requirements; *Koenen*, S. 3 f.

[630] *Motion Picture Expert Group*, Information Technology – Multimedia Framework (MPEG-21), S. V, 15 ff.

[631] *Motion Picture Expert Group*, Information Technology – Multimedia Framework (MPEG-21), S. 21.

[632] <http://www.cselt.it/opima>. Eine Mitgliederliste (u. a. IBM, InterTrust, Philips, Mitsubishi und Toshiba) findet sich unter <http://www.cselt.it/opima/members.html>.

[633] <http://www.iec.ch>.

[634] *Open Platform Initiative for Multimedia Access*, S. 5.

[635] *Open Platform Initiative for Multimedia Access*, S. 6.

Pay-TV-Umfeld, wo OPIMA die Set-Top-Box standardisiert.[636] OPIMA will nicht ein bestimmtes DRM-System standardisieren. Vielmehr geht es um die Standardisierung einer einheitlichen Schnittstelle, mit der proprietäre technische Schutzsysteme unterschiedlicher Anbieter kommunizieren können. Der Kunde soll in die Lage versetzt werden, ein einziges Endgerät zu benutzen, über das er digitale Inhalte der unterschiedlichsten Anbieter nutzen kann. Mit welchen proprietären technischen Schutzmaßnahmen die einzelnen digitalen Inhalte versehen sind, soll dem Kunden verborgen bleiben.

4. Trusted Computing Platform Alliance (TCPA)

Die „Trusted Computing Platform Alliance" (TCPA) stellt eine Initiative namhafter Hard- und Softwarehersteller dar.[637] Dabei geht es um die Standardisierung einer umfassenden manipulationssicheren Hardware- und Betriebssystemsumgebung für den PC-Bereich. Dafür werden unter anderem Verschlüsselungsverfahren sowie Integritäts- und Authentizitätsprüfungen eingesetzt.[638]

V. Initiativen von Verwertungsgesellschaften

Bei Multimediaprodukten sind die einzelnen Texte, Bilder, Musikstücke und Filme, die zum Multimediaprodukt zusammengesetzt werden, regelmäßig urheberrechtlich geschützt. Daher muß der Hersteller des Multimediaprodukts von vielen Rechteinhabern eine entsprechende Genehmigung einholen. Sind die Rechteinhaber in unterschiedlichen Verwertungsgesellschaften organisiert, wird die Lage unübersichtlich.[639] Immerhin gibt es allein in Deutschland fast ein Dutzend Verwertungsgesellschaften.[640]

Angesichts dieser Lage errichten Verwertungsgesellschaften inzwischen zunehmend sogenannte „One-Stop-Shops", die eine zentrale Informationsvermittlung für den Erwerb der notwendigen Nutzungsrechte bieten.[641] In Deutschland gründeten im November 1996 neun Verwer-

---

[636] *Open Platform Initiative for Multimedia Access*, S. 2 f.

[637] Der TCPA gehören 145 Mitglieder an; sie wurde 1999 von Compaq, Hewlett-Packard, IBM, Intel und Microsoft gegründet. S. <http://www.trustedpc.org>.

[638] Zu weiteren Einzelheiten s. *Trusted Computing Platform Alliance*, TCPA Design Philosophies and Concepts; *dies.*, Main Specification.

[639] Vgl. *Möschel/Bechtold*, MMR 1998, 571; *Schippan*, EIPR 2000, 24. Beispiele aus dem U.S.-amerikanischen Bereich gibt *Merges*, 84 Cal. L. Rev. 1293, 1374 Fn. 281 (1996).

[640] Eine – unvollständige – Übersicht gibt <http://www.gema.de/publik/faq/verwertungsgesellschaften.html>, eine vollständige Auflistung findet sich bei *Schack*, Rdnr. 1159.

[641] Für solche Systeme wird auch der Begriff „Multimedia Rights Clearance Systems" (MMRCS) verwendet.

tungsgesellschaften[642] die „Clearingstelle Multimedia der Verwertungsgesellschaften für Urheber- und Leistungsschutzrechte GmbH" (CMMV).[643] CMMV tritt als Informationsvermittlungsstelle auf, die über das Internet erreichbar ist. Nach einer entsprechenden Anfrage des Nutzers ermittelt CMMV die zuständige Verwertungsgesellschaft und die Lizenzbedingungen. Mit Hilfe dieser Information tritt der Nutzer zwecks Rechteeinholung entweder selbst mit den einzelnen Verwertungsgesellschaften in Kontakt, oder er zahlt die erforderliche Vergütung an die CMMV als Inkassostelle.[644] In anderen europäischen Ländern bestehen ähnliche Projekte.[645] Auch auf europäischer Ebene existieren mehrere Projekte, die sich der „One Stop Shop"-Problematik annehmen.[646] So sollen im Rahmen des „Very Extensive Rights Data Information (VERDI)"-Projekts[647] die nationalen Clearingstellen aus sieben Mitgliedstaaten[648] zu einem gemeinsamen Rechteinformations- und Lizenzierungsdienst zusammengefügt werden. Dadurch soll Multimediaproduzenten ein großes internationales und kategorienübergreifendes Repertoire zur Verfügung stehen. Sie sollen in kürzester Zeit länder-, kultur- und sprachübergreifend die Nutzungsrechte an Werken verschiedenster Kategorien einholen können.[649]

In einem ersten Schritt agieren One-Stop-Shops regelmäßig als reine Informationsvermittlungsstellen. Es wird jedoch auch darüber nachgedacht, daß sie selbst Nutzungsrechte vergeben.[650] One-Stop-Shops sind

---

642 Gema, VG Wort, VG Bild-Kunst, GVL, VGF, VFF, GWFF, GÜFA und AGICOA.

643 <http://www.cmmv.de>.

644 S. zum ganzen *Kreile/Becker*, GRUR Int. 1996, 691 f.; *Melichar* in: Lehmann (Hrsg.), Internet- und Multimediarecht, S. 213 f.; *Möschel/Bechtold*, MMR 1998, 571 f.; *Schippan*, EIPR 2000, 24, 25.

645 1995 gründeten fünf französische Verwertungsgesellschaften SESAM, <http://www.sesam.org>. Weitere Projekte bestehen in Finnland, Irland, Italien, den Niederlanden, Norwegen, Portugal, Spanien und der Schweiz. S. *Schippan*, EIPR 2000, 24, 25; *Möschel/Bechtold*, MMR 1998, 571. Ähnliche Ansätze existieren auch in Südkorea und Malaysia, *Koskinen-Olsson* in: Koskinen-Olsson/Gervais (Hrsg.), S. 29, 34. Das amerikanische „Copyright Clearance Center" (CCC) (<http://www.copyright.com>) bietet ein System an, bei dem man über das WWW das Vervielfältigungsrecht an über 1,75 Millionen Text-Dokumenten erwerben kann. Der Rechteinhaber kann die Preise und Nutzungsbedingungen ebenfalls über das WWW festsetzen. Ein ähnliches System für Photographien wird in den USA unter dem Namen „Media Image Resource Alliance" (MIRA) angeboten, <http://www.mira.com>. Eine Übersicht über solche Systeme findet sich unter <http://www.verdi-project.com/analysis/mmrcs.html>.

646 Unter dem „INFO 2000"-Programm der Europäischen Kommission werden allein zehn Pilotprojekte unterstützt, s. *Schippan*, ZUM 1999, 135 ff; *ders.*, EIPR 2000, 24 ff., dort auch zur Entstehungsgeschichte und der MMRCS-Studie 1997. Eines dieser Projekte ist das INDECS-Projekt, s. dazu oben Teil 1, C II 2 a aa 2 e.

647 <http://www.verdi-project.com>.

648 Deutschland, Finnland, Frankreich, Irland, Italien, Niederlande und Spanien.

649 *Schippan*, ZUM 1999, 135, 141; *ders.*, EIPR 2000, 24, 27.

650 *Schippan*, ZUM 1999, 135, 142; *ders.*, EIPR 2000, 24, 28; *Möschel/Bechtold*, MMR 1998, 571.

nicht mit DRM-Systemen gleichzusetzen. Während es bei One-Stop-Shops vornehmlich um die vereinfachte und gebündelte Lizenzierung unterschiedlicher Werke geht, wollen DRM-Systeme ein digitales Vertriebssystem für digitale Inhalte bieten. Dennoch können sich beide Bereiche überlappen. So wird im Rahmen des VERDI-Projekts erwogen, ob im Rahmen des One-Stop-Shops auch digitale Inhalte übertragen werden sollen. Wenn One-Stop-Shops dazu noch selbst als Lizenzvergabestelle tätig würden, würde die Grenze zwischen Anbietern von One-Stop-Shops und von DRM-Systemen stärker verwischt.[651]

Insgesamt läßt sich feststellen, daß Verwertungsgesellschaften sich zunehmend mit Fragen der Lizenzierung im digitalen Umfeld beschäftigen. Derzeit geht es hauptsächlich um Fragen der vereinfachten Lizenzierung bei Multimediaprodukten. Auch wenn DRM-Systeme für Verwertungsgesellschaften in Zukunft eine wichtige Rolle spielen könnten, kommen derzeit die treibenden Impulse bei der Entwicklung von DRM-Systemen nicht von Verwertungsgesellschaften, sondern von der Tonträger- und Filmindustrie, Computer- und Unterhaltungselektronikherstellern sowie von spezialisierten DRM-Unternehmen.

E. Ausblick

Die Entwicklung von DRM-Systemen ist bei weitem noch nicht abgeschlossen. Immer wieder tauchen neue Konzepte auf, die in DRM-Systemen eingesetzt werden können. Im folgenden sollen einige der wichtigsten Konzepte dargestellt werden, mit denen ein zukünftiges DRM-System ausgestattet sein könnte. Schon heute werden sie in manchen DRM-Systemen eingesetzt.

I. Superdistribution / Peer-to-Peer Networking (P2P)

Das besondere Charakteristikum eines DRM-Systems, das „Superdistribution" unterstützt, besteht darin, daß die digitalen Inhalte nicht nur vom Anbieter direkt verbreitet werden können (siehe Abbildung 6, Teil a), sondern daß jeder Nutzer die digitalen Inhalte in geschützter Form an einen oder mehrere Dritte weitergeben kann. Wenn der Dritte die entsprechende DRM-Client-Software installiert hat, kann er den Inhalt ebenfalls entschlüsseln und nutzen. Das DRM-System berechnet dem Dritten dafür die festgelegte Nutzungsgebühr. Superdistribution ermöglicht somit die

[651] S. dazu *Schippan*, ZUM 1999, 135, 142; *ders.*, EIPR 2000, 24, 28. Die britische „Authors Licensing and Collecting Society" (ALCS) bietet mit ihrem System ByLine ein System für den journalistischen Bereich an, bei dem die einzelnen Zeitungs- und Zeitschriftenartikel unter anderem mit digitalen Wasserzeichen geschützt werden, s. <http://www.universalbyline.com/scoop.html>.

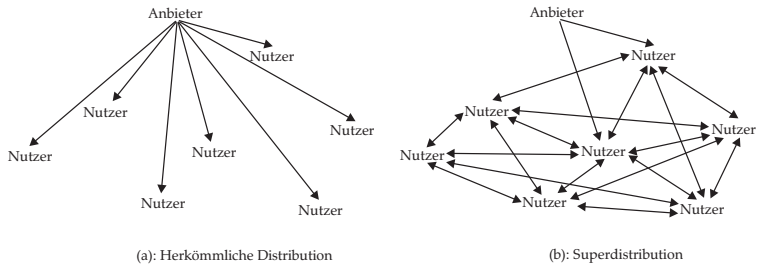


Abbildung 6: Superdistribution

dezentrale Distribution digitaler Inhalte unter gleichzeitiger Wahrung der Interessen der Rechteinhaber, da die digitalen Inhalte nur in technisch geschützt Form weiterverbreitet werden (siehe Abbildung 6, Teil b).[652] Die Nutzer müssen Inhalte nicht mehr direkt vom Anbieter beziehen, sondern können sie – technisch geschützt – untereinander tauschen.

Das Konzept der Superdistribution wurde Anfang der 80er Jahre in Japan von *Ryoichi Mori* entwickelt und ab Ende der 80er Jahre von der „Japan Electronic Industry Development Association" ausgebaut.[653] Die Entwickler verstehen unter Superdistribution ein vollständiges DRM-System.[654] Wichtiges Charakteristikum der Superdistribution in dem von *Mori* verstandenen Sinne ist, daß der Nutzer keine Gebühr für den *Erwerb* des digitalen Inhalts, sondern erst für dessen *Nutzung* entrichten muß. Dadurch koppelt die Superdistribution die Vergütung von der Distribution der digitalen Inhalte ab.[655] Digitale Inhalte sollen wie Elektrizität, Wasser oder Gas nach ihrer Nutzung abgerechnet werden.[656]

---

[652] *Mori/Kawahara*, 38 Transactions of the Information Processing Society of Japan 1465 (1997); *Mori/Kawahara*, E 73 Transactions of the IEICE 1133 (1990). Ein solches System, das auch auf manipulationssicherer Hardware aufbaut, wird ausführlich dargestellt von *Cox*, S. 170 ff.

[653] *Mori/Kawahara*, 38 Transactions of the Information Processing Society of Japan 1465, 1467 (1997); *Mori/Kawahara*, E 73 Transactions of the IEICE 1133 (1990). Zu ähnlichen Konzepten aus dieser Zeit s. *Cox*, S. 155.

[654] S. dazu *Mori/Kawahara*, 38 Transactions of the Information Processing Society of Japan 1465 (1997).

[655] *Mori/Kawahara*, 38 Transactions of the Information Processing Society of Japan 1465 (1997); *Mori/Kawahara*, E 73 Transactions of the IEICE 1133 (1990) („Superdistribution software is much like public domain software for which physical measures are used to ensure that the software producer is fairly compensated […]"); *Cox*, S. 157 („The revenue stream originates when the software is used, not when it is acquired").

[656] *Yoshioka*, 31 Fujitsu Scientific & Technical Journal 76, 81 (1995).

Gegenüber diesem umfassenden Verständnis des Begriffs „Superdistribution" wird heutzutage mit diesem Begriff nur die Möglichkeit des Datentauschs unter den Nutzern verbunden.[657] Dieser Aspekt ist in letzter Zeit auch unter dem Stichwort „File Sharing" oder „Peer-to-Peer Networking" (P2P)[658] bekannt geworden.[659] Der Erfolg von Napster – einem P2P-System, das den Tausch von MP3-Dateien unter Nutzern erlaubt und innerhalb von weniger als zwei Jahren über 70 Millionen Nutzer gewann – zeigt die hohe Akzeptanz dieses Distributionswegs bei den Nutzern.[660] Aber auch von Anbieterseite wird er geschätzt, da er mit vergleichsweise geringen Investitionen in Bandbreite und Übertragungskapazitäten verbunden ist.[661] P2P-Systeme, die über keine technischen Schutzmaßnahmen verfügen, stellen für die Musik- und Filmbranche, letztlich für die gesamte Inhalteindustrie, eine Bedrohung dar.[662] Daher werden in letzter Zeit verstärkt Systeme entwickelt, die entsprechend dem dargestellten „Superdistribution"-Konzept DRM-Schutzmaßnahmen in

[657] So beispielsweise in *Association of American Publishers*, Digital Rights Management for Ebooks, S. 40. Ein wieder etwas anderes Verständnis des Begriffs findet sich in *National Research Council*, S. 302 f. Dort wird darauf abgestellt, daß der Erwerber digitaler Inhalte diese neu kombinieren kann und dieses Paket an Dritte weiterverbreiten kann.

[658] Der Begriff des P2P-Networking ist weiter, als die hier erwähnten Systeme vermuten lassen. Unter P2P fallen beispielsweise auch verteilte Rechensysteme wie das „Seti@home"-Projekt, <http://setiathome.ssl.berkeley.edu>.

[659] Das bekannteste P2P-System – Napster, <http://www.napster.com> – verfügt über ein zentrales Inhaltsverzeichnis, über das der Tauschkontakt zwischen zwei Nutzern hergestellt wird. Daneben existieren unzählige weitere P2P-Systeme, die teilweise vollständig dezentralisiert sind (Gnutella, <http://gnutella.wego.com> und <http://www.gnutella.co.uk>, oder Jungle Monkey, <http://www.junglemonkey.net>) und teilweise zusätzlich noch eine vollständige anonyme Kommunikation ermöglichen (beispielsweise Freenet, <http://freenet.sourceforge.net>, oder Publius, <http://www.cs.nyu.edu/~waldman/publius>). Im folgenden kann auf die unterschiedlichen Systemarchitekturen und deren technische und rechtliche Auswirkungen nicht eingegangen werden, s. dazu *Oram*; *Möller*; *Federrath*, ZUM 2000, 804, 806. Zu weiteren P2P-Projekten (u. a. Aimster, Filetopia, iMesh, Jungle Monkey, Spinfrenzy sowie diverse Napster- und Gnutella-Clones) s. Wired 8.10 (Oktober 2000), S. 234 ff. Zu P2P umfassend *Oram* (Hrsg.), Peer-to-Peer.

[660] Dabei ist natürlich zu beachten, daß Napster deswegen so beliebt ist, weil über das System Millionen von Musikstücken kostenlos zu beziehen sind. Jedoch war es auch schon vor dem Entstehen von Napster möglich, im Internet kostenlos MP3-Dateien zu erhalten. Erst die Kombination der P2P-Technologie mit einer ansprechenden Benutzeroberfläche haben Napster zu seinem heutigen Erfolg verholfen.

[661] S. zu den Vorteilen auch *Lessig*, Expert Report, S. 17 ff.

[662] Zu den Rechtsstreitigkeiten um Napster in den USA s. A&M Records, Inc. v. Napster, Inc., 54 U.S.P.Q.2D (BNA) 1746; 2000 WL 573136 (N.D.Cal. May 5, 2000) – auf deutsch veröffentlicht in GRUR Int. 2000, 1066 – und A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896 (N.D.Cal. August 10, 2000). S. dazu auch *Berschadsky*, 18 J. Marshall J. Computer & Info. L. 755 (2000); *Kochinke/Geiger*, K&R 2000, 594, 596 f.; *Bechtold*, MMR 9/2000, S. XXI.

einem P2P-Umfeld anwendbar machen.[663] Dabei spielen „digitale Container" eine wichtige Rolle.[664] Solche DRM-Systeme verbinden die Vorteile von P2P-Systemen (geringe Distributionskosten, hohe Nutzerakzeptanz) mit der Sicherheit technischer Schutzmaßnahmen.[665]

II. DRM im „Mobile Commerce"

Mit neuen Mobilfunk-Technologien wie dem „General Packet Radio Service" (GPRS) und den „Universal Mobile Telecommunications Services" (UMTS) erhalten Nutzer einen schnellen drahtlosen Zugang zum Internet. Mobile Endgeräte wie Mobiltelefone und „Personal Digital Assistants" (PDAs) könnten dann ebenfalls die durch ein DRM-System geschützten digitalen Inhalte beziehen. Schon heute wird an einer Einbeziehung mobiler Endgeräte in DRM-Systeme gearbeitet.[666]

Für DRM-Systeme wirft der sogenannte „Mobile Commerce" (M-Commerce) einerseits neue Probleme auf. Wenn mobile Endgeräte mit Verschlüsselungs- und Kompressionsverfahren zurecht kommen müssen, steigen die Anforderungen an die Rechenleistung und Komplexität der Geräte. Mobile Endgeräte müssen jedoch kompakt sein und dürfen nicht zu viel Strom verbrauchen. Dies beschränkt die mögliche Komplexität der Geräte.[667] Andererseits erweisen sich mobile Endgeräte für DRM-Systeme in mancherlei Hinsicht sogar als besser geeignet als herkömmliche Computer, die an das Internet angeschlossen sind. So ist bei mobilen

---

[663] Dabei ist es eine zweitrangige Frage, ob der Nutzer für jede einzelne Nutzung zahlen muß („pay per use") oder ob er über eine Monatsgebühr einen pauschalen Zugang zum System erhält („pay per subscription"), wie dies bei Napster geplant ist. Auch im zweiten Fall müssen die digitalen Inhalte durch technische Schutzmaßnahmen gesichert werden, um zu verhindern, daß unberechtigte Dritte die Inhalte ohne Zahlung nutzen können.

[664] S. dazu oben Teil 1, C I 1 b aa.

[665] Heute unterstützen u. a. die DRM-Systeme von IBM (Electronic Media Management System) und InterTrust die Distribution in P2P-Netzwerken. Auch existieren aus dem P2P-Bereich Bestrebungen, diese Systeme um technische Schutzmaßnahmen zu erweitern. So integriert das Unternehmen Flycode (<http://www.flycode.com>, früher AppleSoup) DRM-Lösungen in ein P2P-Netzwerk; das Unternehmen CXC arbeitet an einem Verschlüsselungssystem für Gnutella, s. <http://www.cxc.com/where2.html>. Im Februar 2001 stellte Intel mit der „Peer-to-Peer Trusted Library" Möglichkeiten vor, in P2P-Anwendungen Authentifizierungs-, Verschlüsselungs- und digitale Signaturverfahren zu integrieren, s. <http://sourceforge.net/projects/ptptl>. Zum etwas anders gearteten Ansatz von „Mojo Nation", <http://www.mojonation.net>, das auf einem Micropayment-System beruht, s. <http://www.mojonation.net/docs/technical_overview.shtml> und <http://www.telepolis.de/deutsch/inhalt/te/8466/1.html>.

[666] So wird beispielsweise im Rahmen von SDMI über eine Einbeziehung mobiler Endgeräte in die DRM-Spezifikationen nachgedacht, s. *Hartung/Ramme*, IEEE Communications Magazine 78, 81 (November 2000). Auch InterTrust (<http://www.intertrust.com>) arbeitet an einer Integration mobiler Endgeräte in sein DRM-System.

[667] Vgl. *Hartung/Ramme*, IEEE Communications Magazine 78, 84 (November 2000).

Endgeräten regelmäßig eine verläßliche Identifizierung des Nutzers möglich, da die Geräte standardmäßig mit einer eindeutigen Seriennummer ausgestattet sind.[668] Solche persönlichen Identifizierungen können beispielsweise für digitale Fingerabdrücke benutzt werden.[669] Im Gegensatz dazu ist im Internet eine verläßliche Identifizierung des einzelnen Nutzers oft schwierig.[670] Weiterhin sind DRM-Systeme in geschlossenen Umgebungen wie proprietären Mobilfunknetzen tendenziell sicherer als in offenen Netzen wie dem Internet.[671]

III. Software-Agenten

Software-Agenten, die im Auftrag ihres Besitzers bestimmte Aufgaben ausführen, könnten in DRM-Systemen zentrale Funktionen übernehmen. Unter dem Begriff „Software-Agent“[672] werden viele unterschiedliche Technologien zusammengefaßt. Eine einheitliche Definition existiert nicht. Software-Agenten unterscheiden sich regelmäßig dadurch von normalen Computerprogrammen, daß sie auf einen bestimmten Nutzer personalisiert sind und gleichsam autonom handeln.[673] Es handelt sich um ein interdisziplinäres Forschungsgebiet, das seit einigen Jahren zuneh-

[668] So sind bei Mobiltelefonen des in Europa verbreiteten GSM-Standards die einzelnen Nutzer über eine eindeutige Seriennummer ihrer im Telefon enthaltenen SIM-Karte („International Mobile Subscriber Identifier“, IMSI) bzw. über die Seriennummer des Telefons selbst („International Mobile Equipment Identifier“, IMEI) identifizierbar. Dies führt natürlich zu erhöhten datenschutzrechtlichen Bedenken. S. dazu insgesamt *Hartung/Ramme*, IEEE Communications Magazine 78 ff. (November 2000); *Durand*.

[669] S. dazu *Hartung/Ramme*, IEEE Communications Magazine 78, 83 f. (November 2000).

[670] Die Einführung eindeutiger und auswertbarer Seriennummern für Prozessoren oder auch Zusatzgeräte (DVD-Spieler, MP3-Player) mit eindeutigen Identifizierungsnummern könnte das Problem beseitigen.

[671] So ist es schwieriger, handelsübliche PCs, auf denen DRM-Komponenten ausgeführt werden, vor Angriffen zu schützen, als Mobiltelefone. S. dazu *Hartung/Ramme*, IEEE Communications Magazine 78, 84 (November 2000).

[672] In der technischen Literatur sind die Begriffe „intelligenter Agent“ oder „mobiler Agent“ verbreiteter. Die vorliegende Arbeit verwendet den Begriff „Software-Agent“, um für den juristischen Leserkreis klarzustellen, daß es sich dabei um spezielle Softwareprogramm handelt.

[673] *Guttman/Moukas/Maes* in: Klusch (Hrsg.), S. 131; *Lieberman* in: Klusch (Hrsg.), S. 279, 280; *Brenner/Zarnekow/Wittig*, S. 29 f. Zu weiteren Charakteristika (wie Kommunikation, Kooperation, Mobilität, Lernfähigkeit, Proaktivität und Reaktivität) s. *Brenner/Zarnekow/Wittig*, S. 39 ff.; *Information and Privacy Commissioner/Registratiekamer*, S. 4, 9. Zu anderen Definitionsansätzen s. *Woodridge* in: Weiss (Hrsg.), S. 27, 28 ff. Auch kann zwischen Informations-, Kooperations- und Transaktionsagenten unterschieden werden, s. *Brenner/Zarnekow/Wittig*, S. 23 f. § 102 (a) (27) UCITA (s. dazu unten Teil 2, B II 3 a bb) definiert einen „electronic agent“ als „computer program, or electronic or other automated means, used independently to initiate an action, or to respond to electronic messages or performances, on the person's behalf without review or action by an individual at the time of the action or response to the message or performance.“

mend an Beachtung gewinnt und in dem Fragen der Künstlichen Intelligenz,[674] der Netzwerk- und Kommunikationstheorie, der Entscheidungstheorie, der Psychologie sowie der Mikroökonomie einschließlich der Spieltheorie aufeinandertreffen.[675] Im folgenden kann kein umfassender Überblick über diesen Bereich gegeben werden.[676] Vielmehr sollen einige Entwicklungen im Bereich der Software-Agenten dargestellt werden, die von besonderer Bedeutung für DRM-Systeme sind.

Eine einfache Form von Software-Agenten sind Preisvergleich-Dienste. Heutzutage existiert im Internet eine Vielzahl von Diensten, die dem Nutzer in kurzer Zeit für ein gesuchtes Produkt einen Preisvergleich unterschiedlicher Anbieter ermöglichen.[677] Das Einsatzgebiet von Software-Agenten ist jedoch viel weiter. Software-Agenten können in den unterschiedlichsten Phasen des E-Commerce Anwendung finden. Bei der Produktauswahl und suche können Software-Agenten den Nutzer unterstützen, indem der Agent dem Nutzer Produktempfehlungen gibt, die speziell auf den einzelnen Nutzer zugeschnitten sind.[678] Nach der Auswahl des gewünschten Produkts können Software-Agenten automatisiert Preisvergleiche erstellen. Weiterhin existieren Systeme, die Verhandlungen über die Vertragsbedingungen automatisieren.[679]

---

[674] Sog. verteilte Künstliche Intelligenz (distributed artificial intelligence), s. *Guttman/Moukas/Maes* in: Klusch (Hrsg.), S. 131, 142 ff.; *Brenner/Zarnekow/Wittig*, S. 42 ff.

[675] S. *Brenner/Zarnekow/Wittig*, S. 40. Zum Verhältnis zwischen Software-Agenten und Spieltheorie s. *Rosenschein/Zlotkin*. Eine umfassende, von *Helin* zusammengestellte Bibliographie zu Software-Agenten findet sich unter <http://www.cs.helsinki. fi/~hhelin/agents/biblio.html>.

[676] S. dazu *Klusch* (Hrsg.); *Weiss* (Hrsg.); *Brenner/Zarnekow/Wittig*.

[677] Solche Preisvergleich-Systeme sind z. B. DealTime, <http://www.dealtime.de> und <http://www.dealtime.com>, BottomDollar, <http://www.bottomdollar.com>, und EvenBetter, <http://www.evenbetter.de>. Das erste dieser Preisvergleich-Systeme wurde von Andersen Consulting unter dem Namen „Bargain Finder" entwickelt, s. *Bechtold*, GRUR 1998, 18, 21, Fn. 41. S. zum ganzen *Guttman/Moukas/Maes* in: Klusch (Hrsg.), S. 131, 136 ff.; *Brenner/Zarnekow/Wittig*, S. 310 ff.

[678] S. dazu *Guttman/Moukas/Maes* in: Klusch (Hrsg.), S. 131, 134 ff. So finden heutzutage bei großen E-Commerce-Anbietern Systeme Anwendung, die einem Kunden bei der Suche nach einem bestimmten Produkt Empfehlungen für ähnliche Produkte geben. Diese Empfehlungen basieren auf den Kaufgewohnheiten anderer Kunden des Anbieters. Diese Systeme werden mitunter „collaborative information filtering" genannt, s. Klusch (Hrsg.), S. 127 f. Das bekannteste System ist „Firefly", das ursprünglich am MIT entwickelt wurde und seit einigen Jahren beim Internet-Buchhändler Amazon eingesetzt wird. S. dazu *Lieberman*, in: Klusch (Hrsg.), S. 279, 287 f.; *Guttman/Moukas/Maes* in: Klusch (Hrsg.), S. 131, 135 f.; *Brenner/Zarnekow/Wittig*, S. 287 ff.

[679] Ein solches System, das die Verhandlungen hinsichtlich des Preises automatisiert, ist das bis 1999 am MIT Media Lab entwickelte „Kasbah"-System, s. dazu *Chavez/Maes* in: Crabtree (Hrsg.), S. 75 ff.; *Guttman/Moukas/Maes*, in: Klusch (Hrsg.), S. 131, 141; *Brenner/Zarnekow/Wittig*, S. 328 ff. Solche Preisverhandlungen können auch im Rahmen eines automatisierten Auktionssystems stattfinden, s. *Noriega/Sierra* in: Klusch (Hrsg.), S. 153 ff. und deren „Fishmarket"-Projekt.

Diese verschiedenen Komponenten können auch in einem umfassenden Software-Agenten-System zusammengefaßt werden, das alle Stadien – von der Produktidentifizierung über die Anbieteridentifizierung bis zu den Vertragsverhandlungen und der Vertragsabwicklung – vollständig automatisiert.[680] Dabei treten mehrere Software-Agenten miteinander in Interaktion (sogenannte „Multi-Agenten-Systeme").[681] Ein E-Commerce-System, das auf einem Multi-Agenten-System agiert, wird als „agent-mediated electronic commerce" bezeichnet. In solchen agentenbasierten Marktplätzen werden die Marktteilnehmer durch ihre einzelnen Agenten vertreten, die im Auftrag ihrer Besitzer Aufgaben erfüllen.[682] Sie werden schon heute für den DRM-Bereich entwickelt.[683] In einem solchen Szenario kann der Nutzer einem Software-Agenten seine persönlichen Präferenzen hinsichtlich eines zu erwerbenden Musikstücks nennen, beispielsweise die Musikrichtung, den Künstler, das Aufnahmedatum, die Aufnahmequalität, die individuelle Zahlungsbereitschaft, die Verhandlungsstrategie des Software-Agenten und ähnliches. Der Software-Agent sucht dann entsprechende Angebote aus dem Internet zusammen und präsentiert diese dem Nutzer entweder in übersichtlicher Form oder veranlaßt gleich die Übertragung eines bestimmten Musikstücks, übernimmt also alle Phasen der Vertragsanbahnung, schließung und -abwicklung.[684]

Ein auf Software-Agenten basierender „Electronic Commerce" ist kein genaues Abbild eines herkömmlichen Marktsystems. Aufgrund der Automatisierung des Marktgeschehens können Marktprozesse anders gestaltet werden. Die schon erwähnten Preisvergleich-Dienste ermöglichen dem Kunden eine ungekannt effiziente Möglichkeit, zwischen verschiedenen Produktanbietern zu vergleichen. Suchagenten senken Transaktions-

---

[680] Ein solches System ist das bis 2000 ebenfalls am MIT Media Lab entwickelte „Tête-à-Tête"-Projekt, das beispielsweise auch die Vertragsverhandlungen über Garantielänge, Versandkosten, Zahlungs- und Rücknahmebedingungen und ähnliches automatisiert, s. dazu *Guttman/Moukas/Maes* in: Klusch (Hrsg.), S. 131, 141 f. und *Lieberman* in: Klusch (Hrsg.), S. 279, 289 f. Zu Fortentwicklungen im Rahmen des MARI-Projektes s. *Tewari/Maes* in: Proceedings of the 2nd ACM Conference on Electronic Commerce 2000, S. 86 ff.; *dies.* in: Finin/Grosof (Hrsg.), S. 70 ff., und <http://www.media.mit.edu/~gtewari/MARI>. Zu anderen Projekten s. die Homepage der „Software Agents Group" am MIT Media Lab unter <http://agents.www.media.mit.edu/groups/agents>.

[681] *Brenner/Zarnekow/Wittig*, S. 35.

[682] *Brenner/Zarnekow/Wittig*, S. 310. Zur Behandlung dieser sogenannten „Computererklärungen" im deutschen Recht s. unten Teil 2, B II 2 b. Der U.S.-amerikanische UCITA sieht den Vertragsschluß zwischen elektronischen Agenten oder zwischen einer natürlichen Person und einem elektronischenen Agenten als wirksam an. S. dazu unten Teil 2, B II 3 b.

[683] Erste Ansätze finden sich u. a. bei *Gallego/Delgado/García* in: Horlait (Hrsg.), S. 205 ff.

[684] S. dazu Klusch (Hrsg.), S. 128 ff.; *Kephart/Hanson/Greenwald*, 32 Computer Networks 731, 732 (2000).

kosten. Die vollständige Automatisierung kann zu neuen Arten der Preisfestlegung und Vertragsaushandlung führen.[685] Auch kann die Vertragsdurchsetzung verändert werden. So existieren Verfahren, die mit Hilfe eines komplexen Zusammenspiels von Verschlüsselungs- und Authentisierungsverfahren sowie speziellen Austauschstrategien sicherstellen, daß bei einem digitalen Güteraustausch entweder beide Parteien das jeweils gewünschte Gut (digitaler Inhalt gegen Entgelt) erhalten oder daß keiner der beiden Parteien auch nur Teile der Güter erhält (sogenannte „fair exchange"-Protokolle). Dadurch kann vermieden werden, daß der Nutzer von einem DRM-System digitale Inhalte beziehen kann, ohne dafür gleichzeitig bezahlen zu müssen.[686]

Neben den dargestellten Software-Agenten wird noch eine besondere Form von Software-Agenten entwickelt, die sich im Internet frei von Rechner zu Rechner bewegen und jeweils auf dem Rechner, auf den sie sich kopiert haben, ausgeführt werden. Diese sogenannten „mobilen" Software-Agenten können im Auftrag ihrer Besitzer auf fremden Rechnern Aufgaben erfüllen; sie können dort beispielsweise mit anderen mobilen Software-Agenten in Interaktion treten und Verträge aushandeln beziehungsweise abschließen.[687] Mobile Software-Agenten stellen im Vergleich zur Ausführung herkömmlicher Computerprogramme auf einem lokalen Rechner drei zusätzliche Probleme: Erstens muß gewährleistet sein, daß der mobile Software-Agent Ressourcen des fremden Rechners – beispielsweise Dateien oder den Arbeitsspeicher des Rechners – verwenden kann. Zweitens muß gewährleistet sein, daß der mobile Agent auf dem fremden Rechner keine unberechtigten Aktionen ausführt und diese dadurch schädigt (Schutz der Plattform vor dem mobilen Agenten).[688] Drittens muß gewährleistet sein, daß der mobile Software-Agent nicht von dem fremden Rechner unberechtigterweise manipuliert werden kann (Schutz des mobilen Agenten vor der Plattform). Bei der letzten

[685] Neben den schon heute im Internet verbreiteten Auktionen existieren auch andere Ansätze, s. *Kephart/Hanson/Greenwald*, 32 Computer Networks 731 ff. (2000).

[686] Die Einzelheiten sind recht komplex und bauen auf einem gestaffelten Austausch der Güter oder auf einer Einschaltung einer vertrauenswürdigen dritten Instanz auf. Auch müssen „fair exchange"-Protokolle nicht notwendigerweise von Software-Agenten ausgeführt werden. S. dazu insgesamt *Asokan/Schunter/Waidner*; *Lacoste/Pfitzmann/Steiner/Waidner* (Hrsg.), S. 155 ff. Ein verwandtes System, das mit Hilfe einer vertrauenswürdigen dritten Instanz den digitalen Güteraustausch absichert, ist Netbill, s. <http://www.netbill.com>.

[687] Zur Verwendung mobiler Software-Agenten zur Suche von Musikdateien im Internet s. *Kravtsova/Meyer* in: Horlait (Hrsg.), S. 195 ff.

[688] Hier schneidet sich das Problemfeld mobiler Software-Agenten mit Computerviren.

Anforderung handelt es sich heute noch um ein offenes, aber äußerst bedeutsames[689] Forschungsproblem.[690]

Software-Agenten könnten tiefgreifende Auswirkungen auf DRM-Systeme im Speziellen und auf den E-Commerce im allgemeinen haben.[691] Die Entwicklung eines auf Software-Agenten basierenden E-Commerce befindet sich erst in den Anfängen.[692] Zwar lassen sich schon heute im Internet Auswirkungen einfacher Agenten-Systeme beobachten.[693] Es wird jedoch noch recht lange dauern, bis die zugrundeliegenden Technologien so ausgereift und die erforderlichen Standards geschaffen sind, daß der durch Software-Agenten vollständig automatisierte Handel mit all seinen technischen und ökonomischen Auswirkungen weite Verbreitung findet.[694] Auch hier stellen sich umfangreiche und komplexe Fragen der

[689] Um mobile Software-Agenten im E-Commerce-Bereich einsetzen zu können, muß gewährleistet sein, daß sie auf fremden Rechnern in einer sicheren Umgebung ausgeführt werden. Ein Beispiel mag dies erläutern. Verhandeln zwei natürliche Personen auf einem Basar über den Abschluß eines Geschäfts, so verfolgen beide unterschiedliche Strategien. Beispielsweise will der Verkäufer einen möglichst hohen, der Käufer einen möglichst niedrigen Kaufpreis erzielen. Das Aushandeln der Vertragsbedingungen baut darauf auf, daß beide Vertragspartner die Strategie des jeweils anderen Vertragspartners nicht kennen. So weiß der Käufer nicht, welches der niedrigste Preis ist, zu dem der Verkäufer noch bereit ist, die Ware zu verkaufen. Dieses Bild läßt sich auf mobile Software-Agenten übertragen: Verhandeln zwei mobile Software-Agenten über einen Vertragsschluß, so findet ein fairer Verhandlungsprozeß nur statt, wenn Software-Agent B nicht im einzelnen über die Verhandlungsstrategie des Software-Agenten A informiert ist. Weiß Software-Agent B beispielsweise, daß der Software-Agent A einen digitalen Inhalt bis zu einem bestimmten Höchstpreis erwerben wird, so wird Software-Agent B seine Verhandlungsstrategie entsprechend anpassen. Werden beide Software-Agenten gemeinsam auf einem Rechner ausgeführt, so muß daher verhindert werden, daß der Software-Agent B auf die Speicherbereiche des Software-Agenten A Zugriff nehmen kann. Ebenfalls muß verhindert werden, daß der Rechner selbst die Speicherbereiche der beiden mobilen Software-Agenten manipulieren und dadurch die Rahmenbedingungen der Vertragsverhandlungen verändern kann (Schutz des mobilen Agenten vor der Plattform).

[690] *Messerschmitt/Szyperski*, S. 16 Fn. 58. Um die sichere Ausführung mobilen Software-Codes auf fremden Rechnern zu gewährleisten, kann auf manipulationssichere Software gesetzt werden, s. dazu oben Teil 1, C IV 2, insb. die in Fn. 436 gegebenen Literaturhinweise. Vgl. a. *Papaioannou* in: Klusch/Kerschberg (Hrsg.), S. 247, 251 ff. m. w. N. Eine umfassende Bibliographie zu Sicherheitsfragen mobiler Agentensysteme findet sich unter <http://www.informatik.uni-stuttgart.de/ipvr/vs/projekte/mole/security.html>.

[691] S. nur *Kephart/Hanson/Greenwald*, 32 Computer Networks 731 ff. (2000).

[692] *Guttman/Moukas/Maes* in: Klusch (Hrsg.), S. 131, 147. Es existieren noch Probleme, deren Komplexität auch von Experten oft unterschätzt werden, *Nwana/Ndumu*, 14 (2) The Knowledge Engineering Review 1 ff. (1999).

[693] So können Bieter beim Auktionshaus eBay einen Software-Agenten damit beauftragen, für den Bieter das sukzessive Erhöhen des Gebots zu übernehmen. Zu Preisvergleichsystemen s. oben bei Fn. 674.

[694] *Guttman/Moukas/Maes* in: Klusch (Hrsg.), S. 131, 152; *Brenner/Zarnekow/Wittig*, S. 350; *Papaioannou* in: Klusch/Kerschberg (Hrsg.), S. 247 ff.

Interoperabilität und der Standardisierung.[695] Bei mobilen Software-Agenten stellen sich dazu noch große Sicherheitsprobleme. Es ist unklar, ob sie befriedigend gelöst werden können. Über den Einsatz in akademischen Testprojekten sind mobile Software-Agenten noch nicht hinaus gekommen.

IV. Technischer Schutz von Vertragsketten

In einem DRM-System können technische Schutzmaßnahmen direkte Auswirkungen auf rechtliche Rahmenbedingungen haben. In einem einfachen Geschäftsmodell verbreitet ein Inhalteanbieter, der digitale Inhalte selbst erstellt oder entsprechende Nutzungsrechte von Urhebern und Leistungsschutzberechtigten erworben hat, digitale Inhalte über ein DRM-System direkt an den Nutzer.[696] In DRM-Systemen werden jedoch mehr und mehr Zwischenhändler enstehen. Sie kaufen digitale Inhalte bei mehreren Rechteinhabern ein, aggregieren sie zu einem einheitlichen Produkt, fügen Zusatzdienste (Zusatzinformationen, Kundenservice etc.) hinzu (sogenanntes „content packaging" oder „content aggregation") und verkaufen dieses Gesamtpaket zu einem höheren Preis an die Nutzer weiter.[697] Beim Erwerb der digitalen Inhalte schließt der Zwischenhändler mit den einzelnen Rechteinhabern Nutzungsverträge ab. Beim Verkauf der Inhalte durch den Zwischenhändler an den einzelnen Nutzer werden dann wiederum Nutzungsverträge abgeschlossen. Somit besteht eine indirekte vertragliche Beziehung vom Rechteinhaber über den Zwischenhändler bis zum Nutzer in Form einer Vertragskette.[698]

Nach allgemeinen rechtlichen Grundsätzen kann der Zwischenhändler dem Nutzer vertraglich niemals mehr Nutzungsrechte einräumen oder übertragen, als ihm selbst vertraglich eingeräumt oder übertragen wur-

---

[695] S. dazu *Guttman/Moukas/Maes* in: Klusch (Hrsg.), S. 131, 147 ff. Zu Standards und Formaten für die Kommunikation zwischen mehreren Software-Agenten (z. B. die „Knowledge Query and Manipulation Language" KQML und das „Knowledge Interchange Format") s. *Brenner/Zarnekow/Wittig*, S. 96 ff.; *Huhns/Stephens* in: Weiss (Hrsg.), S. 79, 88 ff; *Kone/Shimazu/Nakajima*, 2 Knowledge and Information Systems 259 ff. (2000). Ein Standardisierungsgremium in diesem Bereich ist die „Foundation of Intelligent Physical Agents" (FIPA), <http://www.fipa.org>.

[696] Diese Möglichkeit einer direkten Geschäftsbeziehung zwischen Produzenten und Kunden, ohne daß Händler oder Vermittler dazwischengeschaltet sind, wird mitunter auch „disintermediation" genannt. S. dazu oben Einführung, bei Fn. 27.

[697] Schon in heutigen Feldversuchen von DRM-Systemen durch Tonträgerunternehmen tritt gegenüber dem Kunden oftmals nicht das Tonträgerunternehmen selbst in Erscheinung, sondern neuartige Zwischenhändler. Diese Entwicklung wird auch als „reintermediation" bezeichnet. S. zum ganzen *Durfee/Franklin*, Distribution Chain Security, in: Jajodia (Hrsg.), S. 63. Zur Wertschöpfungskette allgemein s. *European Communication Council* (Hrsg.), S. 173 ff.; zur Aggregation allgemein s. *Bakos/Brynjolfsson* in: Kahin/Varian (Hrsg.), S. 114 ff.

[698] Zur rechtlichen Seite solcher Nutzungsverträge s. unten Teil 2, B.

den („nemo plus iuris transferre potest quam ipse habet"). Ein gutgläubiger Erwerb ist bei Immaterialgüterrechten regelmäßig ausgeschlossen.[699] Will der Nutzer sichergehen, daß er als Nutzungsberechtigter zweiten Grades tatsächlich über die fraglichen Nutzungsrechte verfügt, so müßte er sich alle höherstufigen Nutzungsverträge vorlegen lassen. Dann könnte er prüfen, ob die ihm eingeräumten Nutzungsrechte vom originären Rechteinhaber auch tatsächlich weiterlizenziert wurden.

Dieses Interesse des Nutzers an einer insgesamt wirksamen Vertragskette wird mitunter auch „*distribution chain integrity*" genannt.[700] Jedoch hat der Zwischenhändler ein Interesse, die Bedingungen des Nutzungsvertrages, den er mit dem ursprünglichen Rechteinhaber abgeschlossen hat, gegenüber dem Nutzer geheimzuhalten.[701] Dieses Interesse an einer inhaltlichen Geheimhaltung der Vertragskette wird mitunter auch „*distribution chain privacy*" genannt.[702] Zwischen beiden Interessenlagen (Interesse des Nutzers an inhaltlicher Offenlegung, Interesse des Zwischenhändlers an inhaltlicher Geheimhaltung der Vertragskette) besteht ein Spannungsverhältnis. Es wird an technischen Systemen gearbeitet, die dieses Spannungsverhältnis aufzulösen versuchen (sogenannte „distribution chain security").[703] Dabei wird eine vertrauenswürdige dritte Instanz eingeschaltet, die einen automatisierten Vergleich aller Nutzungsverträge einer Vertragskette durchführt („contract certifier"). Diese Instanz kann dem Nutzer dann versichern, daß der Zwischenhändler tatsächlich über die Nutzungsrechte verfügt, die er an den Nutzer vertraglich weiterreichen will. Gleichzeitig wird dem Nutzer jedoch nicht der Inhalt des Vertrags zwischen dem Rechteinhaber und dem Zwischenhändler offenbart.[704] Der Vergleich beider Nutzungsverträge kann vollständig auto-

[699] S. dazu auch unten bei Fn. 1401.

[700] So bei *Durfee/Franklin* in: Jajodia (Hrsg.), S. 63 ff., auf deren Beitrag dieser Abschnitt beruht.

[701] Einerseits möchte der Zwischenhändler eventuell dem Nutzer gegenüber verbergen, woher er die Inhalte bezogen hat, um zu verhindern, daß sich der Nutzer die Inhalte unter Umgehung des Zwischenhändlers direkt beim ursprünglichen Rechteinhaber besorgt. Andererseits können in diesem Nutzungsvertrag auch Informationen über den vom Zwischenhändler zu entrichtenden Kaufpreis enthalten sein. Der Zwischenhändler will verhindern, daß der Nutzer nach Kenntnis dieses Vertrags selbst bessere Vertragsbedingungen verlangt.

[702] *Durfee/Franklin* in: Jajodia (Hrsg.), S. 63 ff.

[703] So in dem im November 2000 vorgestellten Beitrag von *Durfee/Franklin* in: Jajodia (Hrsg.), S. 63 ff.

[704] Der ursprüngliche Inhalteanbieter teilt den Inhalt seines Nutzungsvertrags mit dem Zwischenhändler der vertrauenswürdigen dritten Instanz mit. Wenn der Zwischenhändler den aggregierten digitalen Inhalt an einen Nutzer verkaufen will, teilt der Nutzer den Inhalt seines Nutzungsvertrags mit dem Zwischenhändler ebenfalls dieser dritten Instanz mit. Die dritte Instanz vergleicht beide Nutzungsverträge und überprüft, ob der Zwischenhändler dem Nutzer irgendwelche Nutzungsrechte einräumen will, über die er selbst gar nicht verfügt. Wenn dies nicht der Fall ist, teilt die Instanz dem Nutzer dieses positive Ergebnis mit. Wird ein solches Verfahren in ein DRM-System

matisiert werden.[705] Im Idealfall merkt der Nutzer von der gesamten Sicherheitsprüfung nichts; vielmehr wird nur intern die Sicherheit des DRM-Systems erhöht.[706]

V. Spannungsverhältnis zwischen Identifizierung und Anonymität

DRM-Systeme ermöglichen oft eine eindeutige Nutzeridentifizierung.[707] Dies kann wünschenswert sein, um besondere Angebote zu erstellen, die auf die Nutzungsgewohnheiten des individuellen Nutzers zugeschnitten sind. Bei einer nutzungsspezifischen Abrechnung („pay per use") muß der Betreiber eines DRM-Systems Informationen darüber haben, welche Leistungen ein bestimmter Nutzer tatsächlich in Anspruch genommen hat. Auch können so Nutzer nachträglich identifiziert werden, die unberechtigterweise Raubkopien erstellt haben.

Verfahren der Nutzeridentifizierung ermöglichen es aber auch, umfassende Nutzerprofile zu erstellen, aus denen sich beispielsweise ergibt, welcher Nutzer welchen Musikstil zu welchen Zeiten in welcher Umgebung bevorzugt.[708] Dies wirft datenschutzrechtliche Probleme auf.[709]

---

integriert, kann der Nutzer sicher sein, daß der Zwischenhändler zur Einräumung der entsprechenden Nutzungsrechte auch tatsächlich berechtigt ist.

[705] In einem DRM-System liegen die Nutzungsverträge idealiter vollständig in streng formalisierter und digitaler Form vor, da sie mit Hilfe von Metadaten-Systemen wie XrML abgefaßt wurden. In einem Prototyp benötigte ein solches System auf einem Intel Pentium III 450 MHz unter Linux für die einzelnen Verfahrensschritte zwischen wenigen Millisekunden und 2 Sekunden, s. *Durfee/Franklin* in: Jajodia (Hrsg.), S. 63, 68 f.

[706] Das System ist im einzelnen sehr viel komplexer. So ist beispielsweise wünschenswert, daß der „contract certifier" selbst keine Kenntnis von den Inhalten der Verträge erhält. Daher werden die Nutzungsverträge an den „contract certifier" immer nur in einer speziell verschlüsselten Form übertragen, die der „contract certifier" selbst nicht entschlüsseln kann. Das scheinbare Paradoxon, die inhaltliche Übereinstimmung zweier Nutzungsverträge zertifizieren zu müssen, ohne deren Inhalt zu kennen, läßt sich mathematisch mit Hilfe mehrerer sogenannter „Zero-Knowledge"-Beweise elegant lösen. Zu „Zero-Knowledge"-Beweisen s. *Selke*, S. 148 ff.; *Schneier*, S. 101 ff., zur Anwendung im vorliegenden Fall s. *Durfee/Franklin*, in: Jajodia (Hrsg.), S. 63, 65 f. Weiterhin verwendet der „contract certifier" zur Zertifizierung digitale Signaturen. Das von *Durfee/Franklin* vorgestellte System will teilweise auch die Interessen des ursprünglichen Inhalteanbieters schützen, beispielsweise das Interesse an ordnungsgemäßer Zahlung sowie das Interesse, daß die digitalen Inhalte auch beim Nutzer beispielsweise nur in einer manipulationssicheren Hardwareumgebung gespielt werden können. Auf diesen Aspekt des Beitrags wird hier nicht eingegangen. Neben diesem hier vorgestellten Ansatz existieren noch andere Lösungen. So kann ein DRM-System beispielsweise durch eine Kombination von Verschlüsselungs- und Signierungsverfahren sicherstellen, daß der Zwischenhändler Metadaten gar nicht oder nur eingeschränkt verändern darf.

[707] Zu Möglichkeiten der Nutzeridentifizierung in DRM-Systemen s. oben Teil 1, C II 3.

[708] S. dazu *Brassil/Low/Maxemchuk*, 87 Proc. IEEE 1181, 1192 f. (1999).

[709] Dabei handelt es sich um keine Zukunftsmusik. 1999 wurde bekannt, daß eine – weit verbreitete Software – zum Abspielen von Musikdateien Informationen über die Hörgewohnheiten der einzelnen Nutzer über das Internet zum Softwarehersteller über-

Zwar kann im vorliegenden Zusammenhang auf die damit zusammenhängenden rechtlichen Fragen nicht eingegangen werden. Es soll aber überblicksartig gezeigt werden, daß bei einer entsprechenden technischen Ausgestaltung datenschutzrechtliche Probleme von DRM-Systemen entweder beseitigt oder doch zumindest deutlich abgeschwächt werden können.[710]

Zu diesem Zweck werden sogenannte „Privacy-Enhancing Technologies" (PETs) entwickelt. Sie zielen darauf ab, Datenschutz auf technischem Wege zu erreichen.[711] Solche Verfahren können auch in DRM-Systemen eingesetzt werden.[712] So kann der Nutzer in DRM-Systemen unter

trug. Dazu verwendete die „RealJukebox" von RealNetworks eine eindeutige Identifizierungsnummer für jeden Nutzer und übertrug u. a. die Namen der CDs, die der Kunde abspielte. S. dazu *Weinberg*, 52 Stan. L. Rev. 1251, 1261 f. (2000); *Litman*, 52 Stan. L. Rev. 1283, 1306 f. (2000); *Köhntopp/Köhntopp*, CR 2000, 248, 257. Ebenfalls 1999 wurde bekannt, daß Microsoft-Office-Dokumente (Word, Excel etc.) unter gewissen Umständen mit einer eindeutigen Identifizierung des Rechners versehen wurden, auf dem diese Dokumente erstellt wurden: falls der Rechner für den Internet-Zugang mit einer Ethernet-Karte ausgestattet war, wurde in die Office-Dokumente die (eindeutige) Identifizierungsnummer der Ethernet-Karte, die sog. MAC-Adresse, integriert; s. dazu *Weinberg*, a. a. O., S. 1262; *Dinant*, S. 3; <http://www.microsoft.com/presspass/features/1999/03–08custletter2.asp>. Bis 1999 übertrug ein Registrierungsprogramm für Microsoft Windows 98 eine eindeutige Kennung des Nutzerrechners zusammen mit anderen Nutzerdaten an Microsoft. Wiederum wurde dabei die MAC-Adresse übertragen, s. dazu *Weinberg*, a. a. O., S. 1262; <http://www.microsoft.com/presspass/features/1999/03–08custletter2.asp>; *Köhntopp/Köhntopp*, CR 2000, 248, 257. Anfang 1999 kündigte Intel an, in den neuen „Pentium-III"-Prozessorchip eine eindeutige Seriennummer zu integrieren, die von Softwareprogrammen zu Identifizierungszwecken gebraucht werden konnte, s. dazu *Weinberg*, a. a. O., S. 1263 ff.; *Froomkin*, 52 Stan. L. Rev. 1461, 1490 f. (2000); *Cornelius*, DuD 1999, 529 ff.; *Köhntopp/Köhntopp* a. a. O., S. 257; *Dinant*, S. 2. Zwar haben sich diese Problemfälle in der Zwischenzeit dadurch entschärft, daß die Hersteller die entsprechenden Identifizierungsmechanismen auf öffentlichen Druck hin entweder ganz abgeschafft oder derart konfiguriert haben, daß der einzelne Nutzer sie abstellen kann. Beim Intel Pentium III kann der Nutzer das Auslesen der Seriennummer (genauer: des individualisierenden Teils der Seriennummer) durch Software inzwischen verhindern, s. *Cornelius*, DuD 1999, 529, 530. Die grundsätzliche Problematik einer Nutzeridentifizierung bleibt jedoch bestehen. Die datenschutzrechtlichen Bedenken führten auch dazu, daß Metadaten zur Nutzeridentifizierung regelmäßig vom rechtlichen Schutz der Veränderung oder Entfernung von Metadaten ausgenommen sind, s. dazu unten Teil 2, D I 3 c.

710 S. a. *Sander*, S. 9 ff. Zu PETs im Bereich von PKIs und Smartcards s. *Brands*.

711 *Burkert* in: Agre/Rotenberg (Hrsg.), S. 125, s. dort auch zu den Grenzen von PET. Zu PET umfassend *Hes/Borking*, einer überarbeiteten Fassung einer Studie, die 1995 gemeinsam vom kanadischen Information and Privacy Commissioner in Ontario und der niederländischen Registratiekamer in zwei Bänden veröffentlicht wurde. Eine Übersicht über heute einsetzbare PETs gibt <http://www.epic.org/privacy/tools.html>.

712 Ebenso *Weinberg*, 52 Stan. L. Rev. 1251, 1279 f. (2000), der für die Verwendung von Pseudonymen in DRM-Systemen plädiert; s. weiterhin *Vora/Reynolds/Dickinson/Erickson/Banks*. Ein Verfahren für conditional access-Systeme im Pay-TV-Bereich entwickeln *Lee/Chang/Lin/Hwang*, 46 IEEE Transactions on Consumer Electronics 20 ff. (2000). Zur anonymen Authentisierung in dynamischen Gruppen s. *Schechter/Parnell/*

einem Pseudonym auftreten. Bei der Pseudonymisierung werden personenbezogenen Daten einem Pseudonym statt einer natürlichen Person zugeordnet; ohne Kenntnis der Zuordnungsfunktion können keine Rückschlüsse auf die natürliche Person gemacht werden.[713] Eine der Möglichkeiten, einen Nutzer in einem DRM-System eindeutig zu identifizieren, sind digitale Fingerabdrücke.[714] Es werden Verfahren entwickelt, bei denen der Kunde beim Erwerb des digitalen Inhalts seine Identität nicht preisgeben muß, aber der Anbieter später dennoch einen Kunden identifizieren kann, falls dieser den Inhalt unberechtigt an Dritte weitergegeben hat (sogenannte anonyme digitale Fingerabdrücke). Dafür werden unter anderem Registrierungsstellen zwischengeschaltet, bei denen sich die Nutzer registrieren. Nur die Registrierungsstellen kennen die Identität des Nutzers.[715] Ähnliche Verfahren lassen sich auch für das „traitor tracing" einsetzen.[716]

Hartemink in: Franklin (Hrsg.), S. 184 ff. m. w. N. Zur Arbeit der NymIP-Initiative, die Anonymitäts- und Pseudonymitäts-Dienste auf IP-Ebene einführen will, s. <http://nymip.sourceforge.net>. Ein kommerzielles System, das das vollständig anonyme Surfen im Internet ermöglicht, bei dem auch der Systembetreiber keine Informationen über das Nutzerverhalten speichern kann, ist „Freedom" von Zero-Knowledge Systems, s. <http://www.freedom.net>. Ein ähnliches Verfahren wird von einer Projektgruppe um Prof. *Andreas Pfitzmann* an der TU Dresden entwickelt, s. <http://anon.inf.tu-dresden.de> und <http://www.inf.tu-dresden.de/~hf2/anon>. Ein umfassendes System, in dem trotz Angebotsindividualisierung den datenschutzrechtlichen Bedenken Rechnung getragen werden soll, schlagen *Arlein/Jai/Jakobsson/Monrose/Reiter* in: Proceedings of the 2nd ACM Conference on Electronic Commerce 2000, S. 176 ff., vor.

[713] Pseudonyme können entweder vom Betroffenen selbst oder von einem vertrauswürdigen Dritten (s. § 7 Abs. 1 SigG) vergeben werden. S. dazu *Roßnagel/Scholz*, MMR 2000, 721, 725; *Pfitzmann/Waidner/Pfitzmann*, DuD 1990, 305 f. Auch besteht die Möglichkeit, eine dritte Instanz als Treuhänder in die Vertragsabwicklung selbst einzubeziehen, s. *ebda.*, S. 306 f. Dabei können diese Pseudonyme auch je nach unterschiedlichen Diensten oder Anbietern gewechselt werden. S. dazu allgemein *Hes/Borking*, S. 33 f.; *Chaum*, 28 Comm. ACM 1030 ff. (1985); *Federrath/Pfitzmann* in: Bartsch/Lutterbeck (Hrsg.), S. 319, 323 ff.; *Vora/Reynolds/Dickinson/Erickson/Banks*, S. 5. Von der Pseudonymität ist die Anonymität zu unterscheiden, bei zwar Daten über eine Person vorhanden sind, diese jedoch dieser Person von niemand anderem zugeordnet werden können; s. dazu *Roßnagel/Scholz*, a. a. O., S. 723 f. Zu Kategorisierungsmöglichkeiten von Pseudonymen s. *Pfitzmann/Waidner/Pfitzmann*, DuD 1990, 243, 247 f.; *Pfitzmann*, DuD 1999, 405, 406; *Federrath/Pfitzmann*, a. a. O., S. 323 ff.

[714] S. dazu oben Teil 1, C II 3 b.

[715] Die bisher bekannten Verfahren sind aber noch sehr ineffizient, *Pfitzmann/Waidner* in: Fumy (Hrsg.), S. 88, 90. Im vorliegenden Zusammenhang können die technischen Grundlagen dieser Verfahren nicht dargestellt werden. Sie bedienen sich unter anderem auch blinder digitaler Signaturen und sogenannter „Zero Knowledge"-Beweise. Zu anonymen Fingerabdrücken s. *Pfitzmann/Waidner* in: Fumy (Hrsg.), S. 88 ff.; *Pfitzmann/Sadeghi* in: Okamoto (Hrsg.), S. 404 ff.; *Camenisch* in: Okamoto (Hrsg.), S. 415 ff.; *Lee* in: Katzenbeisser/Petitcolas (Hrsg.), S. 175, 187 f.

[716] *Pfitzmann/Waidner* in: Fumy (Hrsg.), S. 88, 90. Zum „Traitor Tracing" allgemein s. oben Teil 1, C II 3 c bb.

Eine weitere Möglichkeit der Nutzeridentifizierung in DRM-Systemen liegt in der Verwendung digitaler Zahlungssysteme. Digitale Geldmünzen sind mit eindeutigen Seriennummern ausgestattet, um das Kopieren und Fälschen dieser Geldmünzen zu verhindern. Bezahlt der Kunde in einem DRM-System mit einer Geldmünze, könnte die Seriennummer der Geldmünze von der Bank und dem Betreiber des DRM-Systems dazu gebraucht werden, die Kauf- und Nutzungsgewohnheiten einzelner Kunden zu erfassen. Jedoch kann mit Hilfe sogenannter „blinder digitaler Signaturen" ein vollständig anonymes digitales Zahlungsmittel geschaffen werden.[717]

[717] Bei der Ausgabe digitaler Geldmünzen durch eine Bank versieht die Bank jede Münze mit einer digitalen Signatur. Mit Hilfe „blinder" digitaler Signaturen, einem von *David Chaum* 1982 entwickelten Verfahren, kann erreicht werden, daß die Bank beim Signaturvorgang nicht weiß, welche Geldmünze mit welcher Seriennummer sie gerade signiert. Blinde digitale Signaturen sind eine spezielle Form der digitalen Signatur. Bei einer blinden digitalen Signatur weiß der Unterschreibende selbst nicht, was er eigentlich unterschreibt. Bei digitalem Geld bedeutet dies, daß die Bank eine digitale Münze signiert und damit als Zahlungsmittel akzeptiert, ohne deren Seriennummer zu kennen, *Petersen*, DuD 1997, 403, 407. Der Einsatz blinder digitaler Signaturen bei digitalem Geld läßt sich am besten an folgendem Vergleich beschreiben: Der Kunde gibt einen digitalen „Münzrohling", der mit einer eindeutigen Seriennummer versehen ist, in einem verschlossenen Umschlag an die Bank. Die Bank kann die Seriennummer nicht lesen. Jedoch kann sie den Umschlag digital signieren; diese Signatur drückt sich dann wie bei einer Blaupause vom Umschlag auch auf den Geldmünzenvordruck durch. Nachdem die Bank den verschlossenen Umschlag an den Kunden zurückgegeben hat, öffnet dieser den Umschlag und kann eine gültige, von der Bank digital signierte Geldmünze entnehmen. Mit dieser Geldmünze kann der Kunde dann bei einem Händler bezahlen, der die Geldmünze bei der Bank wieder einreichen kann. S. dazu *Hes/Borking*, S. 32 f.; *O'Mahoney/Peirce/Tewari*, S. 48 ff.; *Selke*, S. 151 f.; *Neumann*, S. 30 f.; *Stolpmann*, S. 56 f. Auf weitere Fragen (beispielsweise das Problem, daß bei Doppeleinreichungen digitaler Münzen der Verursacher festgestellt werden muß) kann hier nicht eingegangen werden, s. dazu u. a. *Wayner*, Digital Cash, S. 57 ff.; *O'Mahoney/Peirce/Tewari*, S. 149 f. Zu den technischen Einzelheiten s. *Knorr/Schläger,* DuD 1997, 396, 399 f.; *Chaum*, Scientific American August 1992, 76, 77 f.; *Hagemann/Schaup/Schneider*, DuD 1999, 5, 7; *Bundesamt für Sicherheit in der Informationstechnik*, S. 39 f.; *Wayner*, Digital Cash, S. 33 f.; *O'Mahoney/Peirce/Tewari*, S. 48 ff. Einen Überblick über die Anonymität sonstiger digitaler Zahlungssysteme gibt *Wayner*, Digital Cash, S. 84 ff. Bei Cybercash bleibt der Käufer gegenüber einem Treuhänder nicht anonym, gegenüber dem Händler agiert er faktisch zumindest unter einem Pseudonym, s. *Knorr/Schläger*, DuD 1997, 396, 400; *Hagemann/Schaup/Schneider*, DuD 1999, 5, 8. Beim SET-Standard ist der Händler über das gekaufte Produkt und den Preis informiert, weiß aber nicht den Namen des Käufers; die Kreditkartengesellschaft kennt die Identität des Käufers und den bezahlten Betrag, erhält aber keine Informationen über das gekaufte Produkt, s. *Knorr/Schläger*, DuD 1997, 396, 401; *Zwißler*, DuD 1998, 711, 712 ; *Hagemann/Schaup/Schneider*, DuD 1999, 5, 8; *Wayner*, a. a. O., S. S. 86. Bei der Geldkarte wird über Schattenkonten jede einzelne Zahlungstransaktion erfaßt, s. *Knorr/Schläger*, DuD 1997, 396, 401; *Gentz*, DuD 1999, 18, 20. Zu anonymen digitalen Zahlungssystemen unter Verwendung von Pseudonymen s. *Pfitzmann/Waidner/Pfitzmann*, DuD 1990, 305, 308 ff. Zu weiteren Verfahren im Bereich anonymen elektronischen Geldes s. *Petersen*, a. a. O., S. 403 ff.; *Brassil/Low/Maxemchuk*, 87 Proc. IEEE 1181, 1192 f. (1999).

Software-Agenten, die einzelne Nutzer in einem DRM-System gleichsam elektronisch vertreten, verfügen unter Umständen über detallierte Nutzerinformationen. Dann besteht die Gefahr, daß personenbezogene Daten von den Software-Agenten an unberechtigte Dritte (beispielsweise den DRM-Systembetreiber oder andere Software-Agenten) weitergegeben werden. Aber auch in Agentensysteme können PETs integriert werden.[718]

Schließlich existieren Systeme, mit denen Datenschutzbedingungen in standardisierter maschinenlesbarer Form ausgedrückt werden können. Die „Platform for Privacy Preferences Project" (P3P) des W3C will einen Industriestandard für maschinenlesbare Datenschutzerklärungen schaffen. Dabei drücken Anbieter im WWW ihre Datenschutzbedingungen in einem standardisierten Format auf der Grundlage von XML aus, das automatisiert heruntergeladen und von der Nutzer-Software (WWW-Browser und ähnliches) ausgelesen wird. Diese Nutzersoftware kann dem Nutzer Informationen über die Datenschutzerklärungen des Anbieters anzeigen und auf der Grundlage von Nutzerpräferenzen entsprechend reagieren.[719] Bei einer entsprechenden Konfiguration der Nutzer-Software kann dies vollautomatisch geschehen. Durch P3P können Nutzer leicht und sicher entscheiden, ob und unter welchen Umständen sie ihre persönlichen Daten preisgeben wollen. P3P stellt damit letztlich eine „rights management language" für den Datenschutzbereich dar.[720] Es ist ein wichtiges Projekt aus dem Datenschutzbereich, das sowohl in technischen als auch juristischen Kreisen große Aufmerksamkeit erhalten hat.[721]

---

[718] S. dazu ausführlich *Information and Privacy Commissioner/Registratiekamer*, insb. S. 29 ff. Im Rahmen des von der Europäischen Kommission und dem niederländischen Wirtschaftsministerium geförderten Projektes PISA („Privacy Incorporate Software Agent"), das Anfang 2001 begonnen wurde und auf drei Jahre angelegt ist, sollen Software-Agentensysteme entwickelt werden, die den Datenschutz beachten, s. dazu <http://www.tno.nl/instit/fel/pisa>.

[719] *Cranor*, DuD 2000, 479; *Cavoukian/Gurski/Mulligan/Schwartz*, DuD 2000, 475; *Dinant*, S. 8 f.; *Lohse/Janetzko*, CR 2001, 55, 57 f.; Nähere Informationen finden sich unter <http://www.w3.org/P3P>.

[720] Zum Begriff der „rights management language" s. oben Teil 1, C II 2 a bb 1.

[721] Darüber ist jedoch nicht zu vergessen, daß P3P keinen Durchsetzungsmechanismus enthält, der sicherstellt, daß das Unternehmen die von ihm angeführten Datenschutzbedingungen auch tatsächlich erfüllt, *Cranor*, DuD 2000, 479; *Cavoukian/Gurski/Mulligan/Schwartz*, DuD 2000, 475, 478. Dies trifft zumindest für die derzeitige Fassung von P3P 1.0 zu.

F. Bewertung

„Digital Rights Management"-Systeme wollen eine sichere Plattform für den Vertrieb digitaler Inhalte im Online- und Offline-Bereich bieten. Sie bestehen aus einer Vielzahl unterschiedlicher technischer Komponenten, von denen Verschlüsselungsverfahren und Metadaten die wichtigsten sind. In diesem Teil der Untersuchung wurden die einzelnen Komponenten vorgestellt, die in einem DRM-System eingesetzt werden können. Das bedeutet nicht, daß jedes DRM-System über alle diese Komponenten verfügt. Regelmäßig wird es nur eine relativ kleine Teilmenge der dargestellten Komponenten einsetzen. Die umfassende Darstellung denkbarer DRM-Komponenten soll aufzeigen, über welches Potential DRM-Systeme verfügen.

DRM-Systeme ermöglichen einen umfassenden technischen Schutz digitaler Inhalte und eröffnen neue Arten des Vertriebs und der Vermarktung. Im Idealfall operiert das DRM-System vom Nutzer völlig unbemerkt im Hintergrund.[722] Die technische Entwicklung von DRM-Systemen ist noch lange nicht abgeschlossen. Einzelne Komponenten sind vergleichsweise ausgereift, andere Komponenten befinden sich erst im frühen Entwicklungsstadium. Für ein funktionierendes DRM-System ist das Ineinandergreifen zahlloser technischer Komponenten erforderlich. Fragen der Systemintegration und der Standardisierung spielen daher eine herausragende Rolle. Eines der großen ungelösten Probleme ist die Interoperabilität unterschiedlicher DRM-Systeme. Die Anzahl der heute existierenden Standardisierungsinitiativen im DRM-Bereich ist nahezu unüberschaubar.[723] Initiativen, die in diesem Bereich offene Standards setzen wollen, werden oft durch bestehende Patente an wichtigen DRM-Komponenten behindert.[724] Auch kooperieren Unternehmen mitunter

[722] *National Research Council*, S. 154. Will der Nutzer ein Musikstück über seinen DRM-Player anhören, so drückt er auf dessen Start-Taste. Alles weitere – Einholen der Erlaubnis zum Abspielen, Dechiffrieren des Musikstückes, Veranlassung eines entsprechenden Zahlungsvorganges etc. – übernimmt automatisch das DRM-System, ohne daß der Nutzer davon etwas merkt. Zumindest in herkömmlichen PC-Umgebungen ist es regelmäßig sehr schwierig, ein „unsichtbares" und benutzerfreundliches DRM-System zu entwickeln, ohne gleichzeitig Abstriche an der Sicherheit des Systems zu machen, *National Research Council*, S. 294.

[723] Eine Übersicht über Standards, die für den DRM-Bereich interessant sein können, findet sich unter <http://158.169.50.95:10080/oii/en/oiistand.html>. Teilweise wird gefordert, daß die WIPO in Genf hierbei eine zentrale Rolle übernehmen sollte, so *Gervais* in: Koskinen-Olsson/Gervais (Hrsg.), S. 6, 18 f.; *Koskinen-Olsson* in: Koskinen-Olsson/Gervais (Hrsg.), S. 29, 35. S. weiterhin *Erickson*, 7 (4) D-Lib Magazine (April 2001).

[724] *Mooney*, 7 (1) D-Lib Magazine (January 2001).

nicht mit den Standardisierungsinitiativen, weil sie sich entweder bei einem Alleingang kompetitive Vorteile erhoffen,[725] oder weil sie keine Möglichkeit sehen, wie bei einer offenen Standardisierung die Sicherheit ihres DRM-Systems gewahrt bleiben kann.

Der Versuch, das herkömmliche urheberrechtliche Verwertungssystem digital abzubilden, ist ein äußerst schwieriges Unterfangen. Nutzungsbedingungen sind regelmäßig komplexe rechtliche Dokumente; an einem digitalen Inhalt kann eine Vielzahl unterschiedlicher Personen Urheber-, Leistungsschutz- oder Nutzungsrechte besitzen. Die Abbildung all dieser rechtlichen Beziehungen in elektronischen Systemen ist schwierig. Auch müssen DRM-Systeme mittelfristig mit dem Verhältnis zwischen bestehenden Werken und Neuschöpfungen umgehen können. Neuschöpfungen bauen oftmals auf schon bestehenden Werken auf, indem sie aus diesen zitieren oder sie be- bzw. umarbeiten. Ein DRM-System sollte diese Weiterverwertung geschützter Werke ermöglichen und eventuell in sein Vergütungssystem einbinden. Gerade in diesen Bereichen besteht bei DRM-Systemen noch erheblicher Forschungsbedarf.[726]

Kein technisches Schutzsystem ist perfekt.[727] Softwareprogramme, die die Umgehung von technischen Schutzmaßnahmen ermöglichen, verbreiten sich im Internet mindestens genauso schnell wie die Inhalte, zu deren Schutz die technischen Schutzmaßnahmen dienen sollen.[728] Es muß immer eine Abwägung zwischen der erreichbaren Sicherheit eines DRM-Systems und den dabei anfallenden Kosten getroffen werden.[729] Ein hundertprozentiger Schutz gegen jegliche Raubkopien ist oftmals gar nicht erforderlich.[730] Das Ziel ausgreifter DRM-Systeme ist es daher regelmäßig nicht, professionelle Angreifer mit großen Ressourcen an der Erstellung von Raubkopien zu hindern. DRM-Systeme sind auf den Massenmarkt zugeschnitten und wollen dem normalen Nutzer die Erstellung von Raubkopien unmöglich machen.[731]

---

[725] *Mooney*, 7 (1) D-Lib Magazine (January 2001).

[726] Die Frage, wie DRM-Systeme mit mehreren Rechteinhabern sowie dem Verhältnis von Neuschöpfungen zu DRM-geschützten Werken umgehen sollten, behandeln *Kumazawa/Kamada/Yamada/Hoshino/Kambayashi/Mohania* in: Proceedings of the ACM 2000 Digital Libraries Conference, S. 254 f. m. w. N.

[727] Ebenso *Sander*, S. 4 ff.; *National Research Council*, S. 153.

[728] *Breitbach/Imai* in: Franklin (Hrsg.), S. 125 f.

[729] *National Research Council*, S. 153.

[730] Ebenso *Hardy*, 1996 U. Chi. Legal F. 217, 222 (1996): „100 percent assurance of anything – or zero risk – has never been a requirement of any business."

[731] Teilweise wird sogar die Aufgabe von technischen Schutzsystemen nur im „keeping honest people honest" gesehen (so *Marks/Turnbull*, EIPR 2000, 198, 208 und *Bloom/Cox/Kalker/Linnartz/Miller/Traw*, 87 Proc. IEEE 1267, 1268 (1999), jeweils zur CPTWG). S. a. *Cox/Linnartz*, 16 IEEE Journal on Selected Areas in Communications 587 (1998).

Viele der aufgezeigten Probleme scheinen mittelfristig lösbar zu sein. Aus technischer Sicht ermöglichen DRM-Systeme eine ungekannt weitgehende Kontrolle über den Zugang zu digitalen Inhalten und über deren Nutzung. Schon heute werden DRM-Komponenten in vielen Unterhaltungselektronik- und Computerprodukten eingesetzt. Bei entsprechenden rechtlichen und ökonomischen Rahmenbedingungen könnten DRM-Systeme zum Grundpfeiler eines künftigen E-Commerce für digitale Inhalte werden.

Teil 2: Rechtliche Grundlagen des DRM

Inhalteanbieter können sich in DRM-Systemen nicht nur durch technische Schutzmaßnahmen schützen. Ihnen stehen auch mehrere rechtliche Schutzmechanismen zur Verfügung, die im folgenden Teil der Arbeit dargestellt werden sollen. Dabei geht die Untersuchung auf die relevanten Regelungen des Völkerrechts, des Europarechts sowie des deutschen und des U.S.-amerikanischen Rechts ein.

Inhalteanbieter werden in DRM-Systemen – wie allgemein im digitalen Umfeld – durch das herkömmliche Urheberrecht geschützt (dazu unten A). Zusätzlich versuchen Inhalteanbieter zunehmend, ihre Schutzinteressen durch eine vertragliche Bindung der Nutzer zu sichern (dazu unten B). Viele technische DRM-Komponenten unterliegen dem Patentschutz oder werden als Geschäftsgeheimnis gehütet. Will ein Hardware- oder Softwarehersteller solche DRM-Komponenten in seine Endgeräte einbauen, muß er mit dem Entwickler der DRM-Komponenten einen Patent- oder Know-how-Lizenzvertrag abschließen. Diese Lizenzverträge enthalten umfangreiche Bestimmungen zur konkreten Ausgestaltung eines DRM-Systems und schützen mittelbar die Interessen der Inhalteanbieter (dazu unten C). Schließlich werden DRM-Komponenten seit einigen Jahren auf internationaler wie nationaler Ebene rechtlich reguliert. Insbesondere wird ein rechtlicher Schutz gegen die Umgehung technischer Schutzmaßnahmen etabliert (dazu unten D).

Viele der dargestellten rechtlichen Schutzmechanismen gewähren keinen grenzenlosen Schutz, sondern werden ihrerseits gesetzlich beschränkt. Urheberrechtliche Verwertungsrechte finden ihre Grenzen in den Schrankenbestimmungen der §§ 45 ff. UrhG. Nutzungsverträge können gegen unabdingbare Vorschriften des Urheberrechts sowie gegen Vorschriften des Kartellrechts und des AGB-Rechts verstoßen. Auch der rechtliche Schutz gegen die Umgehung technischer Schutzmaßnahmen ist oft mit Beschränkungen versehen. Der folgende Teil der Arbeit geht auf diese Beschränkungen rechtlicher Schutzmechanismen nicht ein. Die Arbeit wird sich zu einem späteren Zeitpunkt der Frage widmen, ob und inwieweit rechtliche Schutzmechanismen in DRM-Systemen gesetzlich beschränkt werden müssen.[732]

---

[732] S. dazu unten Teil 3, B II 3, und Teil 4.

A. Schutz durch das Urheberrecht

Wie jeder Urheber oder Leistungsschutzberechtigte wird der Inhalteanbieter, der seine digitalen Inhalte in DRM-Systemen anbietet, durch das Urheberrecht geschützt. Das Urheberrecht schützt in seinem Kern bestimmte kulturelle Geistesschöpfungen, indem es ein Werk seinem Urheber zuordnet und diesem bestimmte Rechte zugesteht. Es hat, gesamtgesellschaftlich betrachtet, den Zweck, zum geistigen, kulturellen und kulturwirtschaftlichen Fortschritt beizutragen. Individuell betrachtet sichert es dem Urheber den Lohn für seine Arbeit der Werkschöpfung.[733]

Das Urheberrecht ist ein traditionell international ausgerichtetes Rechtsgebiet. Die wichtigste urheberrechtliche völkerrechtliche Konvention, die „Revidierte Berner Übereinkunft" (RBÜ), stammt ursprünglich aus dem Jahr 1886. Daneben existiert das Welturheberrechtsabkommen (WUA), das durch den Beitritt der USA zur RBÜ im Jahr 1989 weitgehend bedeutungslos geworden ist, sowie seit 1994 im Rahmen des WTO-Abkommens die Regeln des „Trade Related Aspects of Intellectual Property Rights (TRIPS)"-Abkommens. Auf dem Gebiet der Leistungsschutzrechte ist das Rom-Abkommen aus dem Jahre 1961 zu erwähnen.[734] Im Rahmen der „World Intellectual Property Organization" (WIPO),[735] die unter anderem die RBÜ verwaltet, wurde seit 1991 an einem Protokoll zur RBÜ und an einem möglichen neuen Vertrag zum Schutz von ausübenden Künstler und Tonträgerherstellern gearbeitet. Nach langen Vorarbeiten[736] wurden Ende Dezember 1996 auf einer diplomatischen Konferenz der „WIPO Copyright Treaty" (WCT) und der „WIPO Performances and Phonograms Treaty" (WPPT) verabschiedet.[737] Beide Verträge wollen eine Antwort auf die Herausforderungen geben, denen sich das Urheberrecht durch die Digitalisierung und das Internet ausgesetzt sieht. Da sich der WPPT nur auf den Schutz im Audio-, nicht aber im audiovisuellen Bereich bezieht,[738] fand im Dezember 2000 bei der WIPO eine erneute diplomatische Konferenz

---

733 S. dazu *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, Einl. Rdnr. 11 ff.

734 Zur Übersicht über weitere völkerrechtliche Konventionen s. *Haedicke*, Jura 1996, 64 ff.

735 <http://www.wipo.int>.

736 Zur Entstehungsgeschichte s. *v. Lewinski*, GRUR Int. 1997, 667 ff.; *v. Lewinski/Gaster*, ZUM 1997, 607 ff.; *Wand*, S. 24 ff.

737 S. dazu unten Teil 2, D I 2 a aa 1. Ein weiterer Vertragsentwurf zum rechtlichen Schutz von Datenbanken wurde auf der Konferenz aus zeitlichen und inhaltlichen Gründen nicht einmal zum Verhandlungsgegenstand gemacht, s. *v. Lewinski*, GRUR Int. 1997, 667, 680.

738 Die Ausklammerung audiovisueller Darbietungen ergibt sich für Tonträgerhersteller aus der Definition des Tonträgers in Art. 2 lit. b WPPT; für ausübende Künstler ergibt sich die Ausklammerung daraus, daß ihnen Verwertungsrechte (Vervielfälti-

statt, bei der ein Protokoll zum WPPT verabschiedet werden sollte, das auch ausübenden Künstlern im Film- und Fernsehbereich Verwertungs- und Persönlichkeitsrechte auf dieser völkerrechtlichen Ebene zugestehen sollte.[739] Aufgrund von Meinungsverschiedenheiten zwischen den USA und den Mitgliedstaaten der Europäischen Union über das Verhältnis zwischen ausübenden Künstlern und Produzenten sowie über das anwendbare Recht bei urhebervertragsrechtlichen Vereinbarungen kam jedoch keine Einigung zustande.[740]

Die Institutionen der *Europäischen Gemeinschaft* beschäftigten sich lange Zeit kaum mit dem Urheberrecht und Leistungsschutzrechten. Seit mehr als zehn Jahren finden sich aber Bestrebungen zur Harmonisierung des Urheberrechts auf europäischer Ebene.[741] Nach einem Grünbuch der Kommission über das „Urheberrecht und die technologische Herausforderung" (1988)[742] veröffentlichte die Kommission 1991 ein „Arbeitsprogramm auf dem Gebiet des Urheberrechts und der verwandten Schutzrechte",[743] das die Grundlage für die folgenden fünf urheberrechtlichen Harmonisierungsrichtlinien der sogenannten „ersten Generation" darstellte. Es handelt sich um[744]

- die Richtlinie zum Schutz von Computerprogrammen vom 14. 5. 1991 (Computerprogrammrichtlinie),[745]
- die Richtlinie zum Vermiet- und Verleihrecht sowie zu bestimmten dem Urheberrecht verwandten Schutzrechten im Bereich des geistigen Eigentums vom 19. 11. 1992 (Vermiet- und Verleihrichtlinie),[746]
- die Richtlinie zur Koordinierung bestimmter urheber- und leistungsschutzrechtlicher Vorschriften betreffend Satellitenrundfunk und Kabelweiterverbreitung vom 27. 9. 1993 (Satellitenrichtlinie),[747]

---

gungs-, Verbreitungs- und Vermietrecht sowie das Recht auf Zugänglichmachung) immer nur für „auf Tonträger festgelegte Darbietungen" gewährt werden, s. Art. 7–10 WPPT. Der Schutz audiovisueller Darbietungen wurde im WPPT bewußt ausgeklammert, da keine akzeptable Kompromißlösung gefunden werden konnte, s. v. *Lewinski*, GRUR Int. 1997, 667, 680 f.

739 S. dazu WIPO Audiovisual Performances Treaty Basic Proposal, WIPO-Dok. IAVP/DC/3 vom 1. 8. 2000.

740 *V. Lewinski*, GRUR Int. 2001, 529 ff.

741 S. dazu *Reinbothe*, ZEuP 2000, 5 ff.; *Schack*, ZEuP 2000, 799 ff.; *Haller*, S. 53 ff.; ausführlich *Schippan,* auch zu hier nicht erwähnten Aktivitäten auf europäischer Ebene.

742 Grünbuch über Urheberrecht und die technologische Herausforderung – Urheberrechtsfragen, die sofortiges Handeln erfordern. Mitteilung der Kommission, KOM (88) 172 endg. vom 23. 8. 1988. S. dazu GRUR Int. 1988, 719 f.; *Schippan*, S. 54 ff.

743 Arbeitsprogramm der Kommission auf dem Gebiet des Urheberrechts und der verwandten Schutzrechte, Mitteilung der Kommission, KOM (90) 584 endg. vom 17. 1. 1991. S. dazu GRUR Int. 1991, 756; *Schippan*, S. 57 f.

744 S. dazu *Schippan*, S. 59 ff.

745 Richtlinie 91/250/EWG, ABl. EG Nr. L 122 vom 17. 5. 1991, S. 42.

746 Richtlinie 92/100/EWG, ABl. EG Nr. L 346 vom 27. 11. 1992, S. 61.

747 Richtlinie 93/83/EWG, ABl. EG Nr. L 248 vom 6. 10. 1993, S. 15.

– die Richtlinie zur Harmonisierung der Schutzdauer des Urheberrechts und bestimmter verwandter Schutzrechte vom 29. 10. 1993 (Schutzdauerrichtlinie)[748] und
– die Richtlinie über den rechtlichen Schutz von Datenbanken vom 11. 3. 1996 (Datenbankrichtlinie).[749]

Neben der Harmonisierung grundlegender urheberrechtlicher Vorschriften wurde erkannt, daß das Urheberrecht auf europäischer Ebene auf die Anforderungen der Informationsgesellschaft reagieren müsse.[750] Im Juli 1995 legte die Kommission ihr Grünbuch „Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft" vor.[751] Die Schlußfolgerungen des anschließenden Konsultationsprozeß präsentierte die Kommission 1996 in ihrer Mitteilung „Initiativen zum Grünbuch über Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft".[752] Im Rahmen der sogenannten „zweiten Generation" urheberrechtlicher Richtlinien auf Gemeinschaftsebene legte die Kommission im Dezember 1997 ihren Vorschlag für eine Richtlinie zur Harmonisierung des Urheberrechts und der Leistungsschutzrechte in der Informationsgesellschaft vor. Diese Richtlinie wurde im April 2001 vom Rat der Europäischen Union verabschiedet.[753]

Das *U.S.-amerikanische* Urheberrecht ist im „Copyright Act" aus dem Jahre 1976 geregelt und im 17. Kapitel des United States Code (17 U.S.C.) kodifiziert.[754] Auch wenn sich das U.S.-amerikanische „Copyright Law" in seiner Grundausrichtung deutlich vom kontinentaleuropäischen Urheberrecht unterscheidet, ähneln sich recht viele Regelungen des „Copyright Act" und europäischer Urheberrechtsgesetze. Dies liegt an der vergleichsweise hohen Harmonisierung des Urheberrechts durch völkerrechtliche Verträge.

In *Deutschland* ist das Urheberrecht im UrhG aus dem Jahr 1965 (mit inzwischen zahlreichen Änderungen) geregelt. Neben Vorschriften zum Schutz der Urheber finden sich – daran angelehnt – Vorschriften über sogenannte Leistungsschutzrechte (§§ 70 ff. UrhG).[755] Dort werden Leistungen, die nicht persönliche geistige Schöpfungen im Sinne des § 2 II UrhG darstellen und damit dem Urheberrechtsschutz nicht zugänglich

[748] Richtlinie 93/98/EWG, ABl. EG Nr. L 290 vom 24. 11. 1993, S. 9.
[749] Richtlinie 96/9/EG, ABl. EG Nr. L 77 vom 27. 3. 1996, S. 20.
[750] S. dazu *Reinbothe*, ZEuP 2000, 5, 13 ff.
[751] *Europäische Kommission*, KOM (95) 382 endg. vom 19. 7. 1995.
[752] *Europäische Kommission*, KOM (96) 568 endg. vom 20. 11. 1996.
[753] Zur Richtlinie s. ausführlich unten Teil 2, D I 2 a bb 2.
[754] Zum U.S.-amerikanischen Urheberrecht im Internet s. umfassend *Rieder*; *R. T. Nimmer*, Kapitel 4; *Klett*. Einen allgemeinen Überblick über das U.S.-amerikanische Urheberrecht geben *Götting/Fikentscher* in: Assmann/Bungert (Hrsg.), Kap. 7, Rdnr. 196 ff.
[755] Zum Reformbedarf s. *Schricker* (Hrsg.), Urheberrecht auf dem Weg zur Informationsgesellschaft, S. 219 ff.

sind, aus persönlichkeitsrechtlichen Erwägungen oder mit dem Ziel des Schutzes organisatorisch-wirtschaftlicher Leistungen auf kulturellem Gebiet geschützt.[756] Für die Tätigkeiten der urheberrechtlichen Verwertungsgesellschaften (GEMA, VG Wort, VG Bild-Kunst etc.) sind die Regelungen des Urheberrechtswahrnehmungsgesetzes (WahrnG) von Bedeutung.

Auch in Deutschland wird über Reformen nachgedacht, die das Urheberrecht an das Internet und die Digitalisierung anpassen sollen. Diesem Zweck dient der Diskussionsentwurf eines Fünften Urheberrechts-Änderungsgesetzes, den das Bundesjustizministerium im Juli 1998 vorstellte.[757] Dadurch sollten insbesondere die beiden WIPO-Verträge aus dem Jahr 1996 umgesetzt werden. Gleichzeitig war eine zumindest teilweise Umsetzung der europäischen Richtlinie zum Urheberrecht in der Informationsgesellschaft angestrebt.[758] Da sich die Verabschiedung der Richtlinie unerwartet lange hinauszögerte, wurde seit 1998 keine aktualisierte Fassung des Diskussionsentwurfs vorgelegt. Nachdem die Richtlinie im Mai 2001 verabschiedet wurde, wird die diesbezügliche Reformdiskussion in Deutschland wieder aufleben.[759]

Das deutsche Urheberrecht weist dem Urheber eine Vielzahl von Ausschließlichkeitsrechten, sogenannte „Verwertungsrechte", zu. Auch wenn sich im Detail Auslegungsprobleme ergeben, decken die Verwertungsrechte im digitalen Umfeld doch eine Vielzahl von Nutzungshandlungen ab. Bei einer Übertragung digitaler Inhalte über das Internet kann das Vervielfältigungsrecht des Urhebers gemäß § 16 UrhG betroffen sein.[760] Bei der Nutzung digitaler Inhalte auf einem Computer ensteht regelmäßig eine Kopie des Inhalts in dessen Arbeitsspeicher (RAM). Es ist umstritten, ob diese Kopie nach geltendem Urheberrecht unter das ausschließliche Vervielfältigungsrecht gemäß §§ 16, 69c Nr. 1 UrhG fallen; von der herrschenden Meinung wird dies bejaht.[761] Der Meinungsstreit könnte sich

---

[756] Schutz der ausübenden Künstler, Tonträgerhersteller, Sendeunternehmen, wissenschaftlichen Ausgaben, Lichtbilder, Filmhersteller, Veranstalter etc.; s. dazu *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, Einl. Rdnr. 28.

[757] S. dazu unten Teil 2, D I 2 b cc 1.

[758] *Bundesministerium der Justiz*, Diskussionsentwurf eines 5. UrhG-ÄndG, S. 3.

[759] Daneben verfolgt das Bundesjustizministerium derzeit eine umfassende Reform des Urhebervertragsrechts.

[760] S. dazu nur *Bechtold*, Multimedia und das Urheberrecht, S. 6 ff.; *Loewenheim* in: Schricker (Hrsg.), UrhG-Kommentar, § 16 Rdnr. 16 ff.; *Koehler*, S. 36 ff.; *Klett*, S. 73 ff., 116 ff.; *Schippan*, S. 85, 92 ff.; *Ahrens*, ZUM 2000, 1029, 1031 f.

[761] *Marly*, Softwareüberlassungsverträge, Rdnr. 135 ff.; *Nordemann* in: Fromm/Nordemann (Hrsg.), § 16 Rdnr. 2; *Loewenheim* in: Schricker (Hrsg.), UrhG-Kommentar, § 69c Rdnr. 9; *Schack*, Rdnr. 379; *Bechtold*, ZUM 1997, 427, 430; *Lehmann* in: Beier/Götting/Lehmann/Moufang (Hrsg.), S. 543, 566. Eine Mindermeinung verneint dies, u. a. *Hoeren*, Rdnr. 109; *Hoeren/Schuhmacher*, CR 2000, 137, 142 ff.; offengelassen in BGH 112, 264, 267 – Betriebssystem. Zu den Problemen der herrschenden Meinung s. *Bechtold*, GRUR 1998, 18, 26; *Litman*, 13 Cardozo Arts & Ent. L. J. 29 ff.

durch die Umsetzung der europäischen Richtlinie zum Urheberrecht in der Informationsgesellschaft in deutsches Recht auflösen: Nach Art. 5 Abs. 1 der Richtlinie müssen die Mitgliedstaaten bestimmte vorübergehende Vervielfältigungshandlungen, die technisch bedingt sind und keine eigenständige wirtschaftliche Bedeutung haben, vom Vervielfältigungsrecht ausnehmen. Darunter können auch Kopien im Arbeitsspeicher von Computern fallen.[762]

Wird ein digitaler Inhalt im Internet zum Abruf angeboten und abgerufen, ist in der deutschen Urheberrechtsliteratur umstritten, ob diese Vorgänge unter das Senderecht im Sinne des § 20 UrhG,[763] unter ein verbreitungsähnliches Recht analog § 17 UrhG[764] oder – nach der h. M.[765] – unter ein unbenanntes Recht der öffentlichen Wiedergabe im Sinne des § 15 Abs. 2 UrhG (entweder in direkter oder in analoger Anwendung) fallen.[766] Um diesen Meinungsstreit auf internationaler wie nationaler Ebene zu beenden, wurde 1996 in den beiden WIPO-Verträgen ein sogenanntes „right of communication to the public" verankert, das viele der Übertragungen über das Internet zweifelsfrei erfassen soll.[767] Es wird auf

(1994). Zur Rechtslage im U.S.-amerikanischen Urheberrecht s. MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511, 518 (9th Cir. 1993); *R. T. Nimmer*, § 4.07; *Ginsburg*, S. 7 f.; *Klett*, S. 132 ff.; *Rieder*, S. 60 ff. Zur Lage nach dem WCT und der europäischen Computerrichtlinie s. *Bechtold*, Multimedia und das Urheberrecht, S. 8 f.

762 *Hoeren*, MMR 2000, 515, 516; *Koelman*, EIPR 2000, 272, 275.

763 *Nordemann/Goddar/Tönhardt/Czychowski*, CR 1996, 645, 649; *Spindler*, ZUM 1996, 533, 543. S. a. *Schippan*, S. 87 ff. m. w. N.; *Klett*, S. 85 ff.

764 *Schwarz*, GRUR 1996, 836, 842; *Katzenberger*, AfP 1997, 434, 437; *Zscherpe*, MMR 1998, 404, 407; *Marly*, Urheberrechtsschutz für Computersoftware, S. 251 f.; s. a. *Koehler*, S. 25 f.; *Bechtold*, Multimedia und das Urheberrecht, S. 15; *Schippan*, S. 85 ff., *Klett*, S. 75 ff., jeweils m. w. N.

765 *V. Ungern-Sternberg* in: Schricker (Hrsg.), UrhG-Kommentar, § 15 Rdnr. 24; *Kroitzsch* in: Möhring/Nicolini (Hrsg.), § 15 Rdnr. 28; *Schricker* (Hrsg.), Urheberrecht auf dem Weg zur Informationsgesellschaft, S. 133; *Koehler*, S. 27 ff.; *Schippan*, S. 89 f.; *Wandtke/Schäfer*, GRUR 2000, 187, 190; *Ahrens*, ZUM 2000, 1029, 1030; *Bechtold*, Multimedia und das Urheberrecht, S. 16 ff. m. w. N.

766 Zu diesem Meinungsstreit existiert inzwischen eine unübersehbare Fülle an Literatur. Auch ist umstritten, ob schon das bloße Bereithalten zum Abruf einem Verwertungsrecht unterfällt; *v. Ungern-Sternberg* in: Schricker (Hrsg.), UrhG-Kommentar, § 15 Rdnr. 28, plädiert für ein unbenanntes Verwertungsrecht in entsprechender Anwendung des § 15 Abs. 2 UrhG. Lehnt man dies – wie z. B. *Koehler*, S. 36 – ab, so wäre mittelfristig eine Gesetzesänderung erforderlich, da sowohl Art. 8 WCT und Art. 10 WPPT als auch Art. 3 der europäischen Richtlinie zum Urheberrecht in der Informationsgesellschaft schon das bloße Zugänglichmachen als ein dem Urheber zustehendes Verwertungsrecht ansehen, s. *v. Ungern-Sternberg*, a. a. O., § 15 Rdnr. 27; *v. Lewinski*, GRUR Int. 1998, 637, 639.

767 Art. 6 WCT lautet: „[…] haben die Urheber von Werken der Literatur und Kunst das ausschließliche Recht, die öffentliche drahtlose oder drahtgebundene Wiedergabe ihrer Werke zu erlauben, *einschließlich der Zugänglichmachung ihrer Werke in der Weise, daß sie Mitgliedern der Öffentlichkeit an Orten und zu Zeiten ihrer Wahl zugänglich sind*" (Hervorhebung durch den Verfasser). Entsprechende Regelungen finden sich in Art. 10 und 14 WPPT für ausübende Künstler und Tonträgerhersteller.

europäischer Ebene durch die Richtlinie zum Urheberrecht in der Informationsgesellschaft umgesetzt,[768] die wiederum der Umsetzung in deutsches Recht harrt. Schon heute ist in Deutschland aber unbestritten, daß das Anbieten und Übertragen digitaler Inhalte im Internet – und damit auch in Online-DRM-Systemen – grundsätzlich unter eines der Verwertungsrechte des Urhebers fällt. § 15 UrhG formuliert ein allgemeines Verwertungsrecht, durch das dem Urheber alle Verwertungsarten seines Werkes, auch die neu entstehenden, vorbehalten werden.[769] Es geht nur um die Frage, *welches* Verwertungsrecht einschlägig ist. Neben den Regelungen zu urheberrechtlichen Verwertungsrechten greifen im digitalen Umfeld auch die urheberpersönlichkeitsrechtlichen Vorschriften der §§ 12-14 UrhG.[770]

Es zeigt sich, daß das Urheberrecht zumindest aus theoretischer Sicht auch im digitalen Umfeld einen weitreichenden Schutz bei Online- und Offline-Verwertungen bietet. Zudem ist seit vielen Jahren die Tendenz zu beobachten, den Schutz des Urheberrechts und verwandter Schutzrechte immer weiter zu stärken und auszudehnen.[771] Naturgemäß stellen sich bei näherer Betrachtung eine Fülle von Einzelproblemen. So treten schwierige Probleme des Urheberrechts im Internet bei der Reichweite urheberrechtlicher Schrankenbestimmungen[772] und bei der Haftungsproblematik im Schnittfeld zwischen dem UrhG und dem Teledienstegesetz auf.[773] Es ist nicht das Ziel dieser Arbeit, solche allgemeinen Fragen des

[768] Art. 3 Abs. 2 der Richtlinie zum Urheberrecht in der Informationsgesellschaft.

[769] S. *Bechtold*, ZUM 1997, 427, 431.

[770] S. dazu *Klett*, S. 92 ff.; *Schricker* (Hrsg.), Urheberrecht auf dem Weg zur Informationsgesellschaft, S. 89 ff.

[771] Einerseits besteht die Tendenz, immer neue urheberrechtsähnliche Ausschließlichkeitsrechte zu schaffen. In Europa ist in diesem Zusammenhang die Datenbankrichtlinie zu nennen. Zu Tendenzen in den USA s. *Lemley*, 75 Tex. L. Rev. 873, 898 ff. (1997); zur Anwendung der amerikanischen „trespass doctrine" als Ersatz für ein immaterialgüterrechtliches Ausschließlichkeitsrecht s. eBay v. Bidder's Edge, 100 F.Supp.2d 1058 (C.D. Cal. 2000); *Burk*, 4 J. Small & Emerg. Bus. L. 27 (2000); *O'Rourke*, 53 Vand. L. Rev. 1965, 1986 ff., 1993 ff. (2000). Andererseits wurde die urheberrechtliche Schutzfrist im Laufe der letzten 300 Jahre immer weiter verlängert. Das erste moderne Urhebergesetz, die britische „Statute of Anne" von 1710, sah eine Schutzfrist von 14 Jahren ab Veröffentlichung des Werks vor. Das preußische UrhG von 1837 kannte bereits eine Schutzfrist von 30 Jahren post mortem auctoris. Im Rahmen der berühmten Parsifal-Debatte wurde im deutschen Reichstag eine abermalige Verlängerung der Schutzfrist erwogen; erst 1934 kam es dann aber zu einer Verlängerung auf 50 Jahre und 1965 auf 70 Jahre post mortem auctoris; s. zum ganzen *Schack*, Rdnr. 468. In den USA beträgt die Schutzdauer seit dem „Sonny Bono Copyright Term Extension Act" von 1998 (Pub. L. No. 105–298, 112 Stat. 2827) ebenfalls 70 Jahre post mortem auctoris, s. 17 U.S.C. § 302 (a); s. dazu *Garon*, 17 Cardozo Arts & Ent. L. J. 493, 522 ff. (1999); Eldred v. Reno, 2001 WL 127725 (D.C. Cir. Feb 16, 2001). S. zum ganzen auch *Laddie*, EIPR 1996, 253 ff.

[772] S. dazu *Schricker* (Hrsg.), Urheberrecht auf dem Weg zur Informationsgesellschaft, S. 153 ff.; *Bechtold*, Multimedia und das Urheberrecht, S. 11 ff., 18 ff.

[773] S. dazu *Freytag*; *Spindler*, CR 2001, 324 ff.; rechtsvergleichend *Klett*, S. 162 ff.

Urheberrechts im Internet zu untersuchen. Einerseits wurden sie in den letzten Jahren schon in vielen Aufsätzen und einigen umfangreichen Abhandlungen analysiert.[774] Andererseits sind solche Fragen allgemeine urheberrechtliche Probleme des Internet und der Digitalisierung, nicht aber spezifische urheberrechtliche Probleme von DRM-Systemen.

An dieser Stelle mag die Feststellung genügen, daß Inhalteanbieter[775] in DRM-Systemen auf das gesamte Repertoire der urheberrechtlichen Verwertungsrechte, der Urheberpersönlichkeitsrechte und der Leistungsschutzrechte zurückgreifen können, um ihre Schutzinteressen im digitalen Umfeld zu wahren. Aus praktischer Sicht liegen die größten Probleme des Urheberrechts im Internet nicht darin, daß das Urheberrecht unter theoretischen Gesichtspunkten keinen ausreichenden Schutz bieten würde. Vielmehr mangelt es im Internet an effektiven Durchsetzungs- und Verfolgungsmechanismen. DRM-Systeme versprechen, diese Probleme zu lösen oder doch zu lindern. Die Lösung von DRM-Systemen liegt jedoch nicht in einer Stärkung des urheberrechtlichen Schutzes, sondern in weiteren – technischen und rechtlichen – Schutzmechanismen, von denen die rechtlichen im folgenden dargestellt werden.

B. Schutz durch Nutzungsverträge

I. Bedeutung von Nutzungsverträgen in DRM-Systemen

Inhalteanbieter können ihre Interessen in DRM-Systemen durch Nutzungsverträge schützen. Bevor der Nutzer in einem DRM-System digitale Inhalte nutzen kann, schließt er zunächst einen oder mehrere Verträge ab. Dafür muß er eventuell eine spezielle DRM-kompatible Hardware- oder Softwarekomponente erwerben. Auch muß er den digitalen Inhalt aus dem DRM-System beziehen.[776] Diesen tatsächlichen Vorgängen liegt jeweils ein Vertragsschluß zugrunde. Wer der Vertragspartner des Nutzers ist, hängt vom fraglichen Vorgang und der Ausgestaltung des DRM-Systems ab. Mögliche Vertragspartner sind der Inhalteanbieter, Rechteinhaber, der DRM-Systembetreiber[777] oder Zwischenhändler.

In einem DRM-System können Inhalteanbieter und DRM-Systembetreiber die Nutzung digitaler Inhalte nur unter der Bedingung gestatten, daß die Nutzer davor bestimmte vertragliche Verpflichtungen eingehen.

---

[774] S. nur *Schricker* (Hrsg.), Urheberrecht auf dem Weg zur Informationsgesellschaft; *Bechtold*, Multimedia und das Urheberrecht.

[775] Zur Verwendung dieses Begriffs in der Arbeit s. oben Einführung, D.

[776] Bei einem Online-DRM-System ist darunter beispielsweise das Herunterladen eines Musikstücks von einem Server im Internet, bei Offline-DRM-Systemen beispielsweise der Erwerb einer geschützten DVD zuverstehen.

[777] Zur Verwendung dieser Begriffe s. oben Einführung, D.

So findet sich in einem Vertrag, den der Nutzer vor der Installation eines bestimmten DRM-Systems abschließen muß, die Bestimmung, daß dem Nutzer ein „einfaches, nicht übertragbares Recht" eingeräumt wird, „den angebotenen Musiktitel *einmal* abzuspielen (pay-per-play)".[778] Es wird ihm verboten, „die Musiktitel in irgendeiner Weise zu ändern oder geänderte Versionen zu benutzen, die Musiktitel für Dritte zu kopieren, zugänglich zu machen bzw. weiterzuleiten, nachzuahmen, zu verkaufen, weiterzuverkaufen oder für kommerzielle Zwecke welcher Art auch immer zu nutzen. Eine Weiterübertragung der Rechte an Dritte ist ausdrücklich ausgeschlossen."[779] Weiterhin wird er verpflichtet, digitale Musikstücke nur auf tragbare Abspielgeräte zu kopieren, die dem SDMI-Standdard[780] entsprechen. Digitale Inhalte dürfen nicht auf CDs, DVDs oder einen anderen Computer kopiert werden. Bilder und Texte dürfen nicht ausgedruckt werden.[781]

---

[778] So nach § 4 S. 3 der AGB i.d.F. vom 1. August 2000 des Musikdownload24-Angebots (<http://www.musicdownload24.de>) der BMG Entertainment (Bertelsmann), das hinsichtlich der technischen DRM-Komponenten auf die Technologie von InterTrust zurückgreift, erhältlich unter <http://www.musicdownload24.de/agb_01.html>, abgerufen am 22. 2. 2001. § 4 S. 3 der AGB lautet vollständig: „Im Rahmen des Angebots überträgt BMG Kunden das einfache, nicht übertragbare Recht, die angebotenen Musiktitel zum ausschließlichen persönlichen Gebrauch entweder (i) auf die eigene Festplatte herunterzuladen und die Musiktitel beliebig oft wiederzugeben (Download) oder (ii) herunterzuladen zum einmaligen Abspielen (‚Pay-Per-Play').".

[779] § 4 S. 4 f. der AGB, s. Fn. 778.

[780] S. dazu oben Teil 1, D II 5.

[781] Diese Beispiele sind dem „End User License Agreement" des Universal Music Group-Projekts „Bluematter" (<http://www.bluematter.com>) entnommen, das auf Technologie von InterTrust zurückgreift. Das „End User License Agreement" ist erhältlich unter <http://offers.bluematter.com/sniffer/terms.htm>, abgerufen am 22. 2. 2001. Die „Schedule A – Business Rules" lauten auszugsweise:

„1. You may only download Content to a portable device that is (i) compatible with the InterTrust Technologies Corp. digital rights management system, (ii) compliant with the requirements of the Secure Digital Music Initiative (SDMI), and (iii) compliant with UMG's content security requirements.
2. You may not copy or ‚burn' Content onto CDs, DVDs, flash memory, or other storage devices (other than the hard drive of the computer upon which you installed the Software). In the future, UMG may permit you to make these types of copies of UMG Content to certain SDMI-compliant storage media.
3. You may not transfer your rights to use any particular copy of Content to another. For example, you may not transfer your rights to another at death, in divorce, or in bankruptcy. This is not an exclusive listing; it is only a set of examples. Notwithstanding this Business Rule, you may email a Content Reference to another consumer to enable that consumer to purchase his or her own rights in Content.
4. You may not transfer or copy Content (with the rights you have purchased) to another computer, even if both computers are owned by you. You will be able to copy locked Content to another computer, whether that computer is owned by you or not, but the rights you have purchased to use that Content will not travel with the copy. In the future, UMG may permit you to make these types of transfer of UMG Content along with the rights you have purchased.

Daneben finden sich in Verträgen, die der Nutzer vor der Installation DRM-kompatibler Soft- oder Hardware abschließen muß, Klauseln, die die Sicherheit des DRM-Systems selbst betreffen. So wird der Nutzer verpflichtet, die Softwarekomponenten eines DRM-Systems nicht an Dritte weiterzugeben, sie zu bearbeiten, zu verändern und keine Schritte des „Reverse Engineering“[782] zu unternehmen.[783] Er wird verpflichtet, die technischen Schutzmechanismen der DRM-Software nicht zu umgehen, zu verändern oder dies auch nur zu versuchen.[784] Schließlich wird der Nutzer verpflichtet, eine Aktualisierung und Veränderung von DRM-Softwarekomponenten zuzulassen, wenn dies aus Sicherheits- oder Interoperabilitätsgründen notwendig ist.[785] Auch wird der Nutzer in sol-

5. You may not print the photographic images, lyrics, and other non-music elements that are distributed with Content.
6. When you purchase the right to unlimited use of Content, the use rights associated with that Content terminate upon your death.
7. There is currently no free UMG Content. All rights must be purchased. The only exception to this rule is that 30 second audio clips may sometimes be made available by UMG without charge […]“.

[782] S. zu diesem Begriff oben Teil 1, C IV 2 b.

[783] So im Rahmen des „End User License Agreements“ des Universal Music Group-Projekts Bluematter, s. oben Fn. 781. § 3 des End User License Agreements lautet in Ausschnitten:

„3. Restrictions.

(a) […] You may make one back-up copy of the Software for archival purposes, so long as such copy contains the copyright and proprietary notices furnished with the original copy;

(b) […] you will not under this License Agreement: (i) rent, lease, loan, sell, copy (except as permitted above), or distribute the Software in whole or in part; (ii) use the Software or any portion thereof to create any tool or software product that can be used to create software applications of any nature whatsoever; […] (iv) modify, alter, decompile, disassemble, reverse engineer or emulate the functionality of (for purposes inconsistent with this License Agreement), reverse compile or otherwise reduce to human readable form, or create derivative works of the Software without the prior written consent of Licensors; […]“.

[784] § 3 (d) des „End User License Agreements“ des Universal Music Group-Projekts Bluematter lautet: „You further acknowledge and agree that you may not, and shall not, tamper with the Software or undertake any activity intended to bypass, modify, defeat or otherwise circumvent (or having the intended effect of facilitating, modifying, or assisting the bypassing, defeating or circumventing of) proper and/or secure operation of the Software and/or any mechanisms operatively linked to such software to detect and/or make more difficult attempts to bypass, modify, defeat, or otherwise circumvent the proper and/or secure operation of the Software“. Eine entsprechende Klausel findet sich im „End User License Agreement“ des RealPlayers Version 8 von RealNetworks: „You may not take any action to circumvent or defeat the security or content usage rules provided or enforced by either the DRM or the Software“, zitiert nach *Thornburg*, 34 U.C. Davis L. Rev. 151, 175 f. (2000).

[785] § 2 des „End User License Agreements“ des Universal Music Group-Projekts Bluematter lautet: „You agree to abide by the rules and policies established from time to time by your deployment manager and/or InterTrust. Such rules and policies will be applied generally in a nondiscriminatory manner to users of the InterTrust Software,

chen DRM-Installationsverträgen darauf hingewiesen, daß die Software-Komponenten des DRM-Systems ihre Funktion automatisch einstellen, wenn der Nutzer gegen die Nutzungsbedingungen verstößt.[786]

Ähnliche Bestimmungen finden sich in Nutzungsverträgen, die der Nutzer abschließen muß, bevor er in einem DRM-System Zugang zu einem digitalen Inhalt erhält. Wie oben dargestellt wurde,[787] enthalten DRM-Systeme umfangreiche „rights management languages". Damit können nahezu beliebig ausdifferenzierte Nutzungsbedingungen festgelegt werden. Diese werden einerseits als Metadaten in maschinenlesbarer Form codiert und somit Teil des technischen DRM-Systems. Andererseits finden sich die Nutzungsbedingungen regelmäßig in den langen Nutzungsverträgen wieder, die der Nutzer on- oder offline abschließen muß, bevor er den digitalen Inhalt nutzen darf. Bestimmungen, nach denen der Nutzer ein eBook innerhalb von vier Tagen höchsten zehn Stunden lang benutzen, insgesamt zwei Mal ausdrucken und nicht an Dritte weitergeben darf, können nicht nur in den Metadaten eines DRM-Systems, sondern auch in dem Nutzungsvertrag enthalten sein, den der Nutzer abschließen muß, bevor er Zugriff auf das eBook erhält. Legt der Inhalteanbieter keine individuellen Nutzungsbedingungen fest, wird auf standardisierte Nutzungsbedingungen des DRM-Systems zurückgegriffen, zu deren Einhaltung sich der Nutzer vertraglich verpflichtete, als er das DRM-System bei sich installierte.[788]

---

and may include, for example, required updates, modifications, and/or reinstallations of the InterTrust Software to address security and/or interoperability issues". Vor der Installation des Liquid Audio Players 5, der ein DRM-System enthält, muß der Nutzer beispielsweise einem „End User License Agreement" zustimmen, das ähnliche Verpflichtungen enthält. Auch das „End User License Agreement" des RealPlayers Version 8 von RealNetworks enthält eine entsprechende Klausel, s. *Thornburg*, 34 U.C. Davis L. Rev. 151, 176 (2000).

[786] So enthält das „End User License Agreement", dem der Nutzer vor der Installation des Liquid Audio Player 5 zustimmen muß, folgende Klausel: „2. Disabling Software. The Software contains code which may be used to disable such Software. This disabling code may be used to ensure that the Software is not used in violation of this agreement, including without limitation to infringe intellectual property rights in the software or any content. Customer agrees and acknowledges that upon any termination or expiration of this agreement, and provided that the parties have not agreed in writing to renew this agreement, the software may, at Liquid Audio's Discretion, cease to function in some or all respects, and customer may lose access to data made with, or stored using, the software. […] Customer agrees and acknowledges that the disabling of the software is a key feature of the license rights and responsibilities conveyed under this agreement". Das „End User Licer License Agreement" wird beim Aufruf des Installationsprogramms des Liquid Audio Players 5 angezeigt. Die abgedruckte Fassung ist dem Liquid Audio Player 5.3.0.12 entnommen, der am 22. 2. 2001 von <http://www. liquidaudio.com/downloads/index2.html> heruntergeladen wurde.

[787] S. Teil 1, C II 2 a bb.

[788] Dieses Verfahren wird beispielsweise bei Bluematter eingesetzt, s. dazu oben Fn. 781. § 5 von dessen „End User License Agreement" lautet ausschnittsweise:

Insgesamt zeigt sich, daß Inhalteanbieter ihre Interessen in DRM-Systemen oftmals durch eine vertragliche Bindung der einzelnen Nutzer wahren wollen.[789] In diesen Verträgen, die die Arbeit als „Nutzungsverträge" bezeichnet, werden oftmals Nutzungsrechte im urheberrechtlichen Sinn (§§ 31 ff. UrhG) eingeräumt. Sie enthalten aber auch Klauseln, die mit urheberrechtlichen Nutzungsrechten nichts zu tun haben. Das Charakteristische solcher Nutzungsverträge ist daher nicht die Einräumung urheberrechtlicher Nutzungsrechte, sondern die Existenz einer vertraglichen Beziehung zwischen dem Urheber und dem Nutzer. Digitale Inhalte werden in DRM-Systemen an eine große Anzahl von Nutzern vertrieben.

„Authorized Use of UMG content.
The Software may enable you to listen to, view, and/or read (as the case may be) music, images, video, text, and other material that may be obtained by you in digital form. This material, collectively ‚Content', may be owned by UMG or by third parties. However, in all circumstances, you understand and acknowledge that your rights with respect to Content you obtain for use in connection with the Software will be limited by copyright law and by the Business Rules with which authorized copies of the Content are electronically packaged. ‚Business Rules' are the rules assigned by a Content owner to its Content that limit your access to and use of Content. […]
You may obtain from a Content owner certain rights to use the owner's Content. For example, the Content owner may grant you the right to listen to an audio track he or she owns in exchange for some payment by you or no payment by you; the Content owner may grant you the right to listen to an audio track for a specific number of playbacks or for as many playbacks as you wish; or the Content owner may permit you to listen to a portion of an audio track at no cost but require you to purchase additional rights to listen to the entire audio track. These examples are not exclusive but are intended to give you an idea of the types of Business Rules that may apply to certain Content. Business Rules will be provided with Content offers. In the absence of contrary Business Rules provided with a Content offer, the Business Rules listed on Schedule A (which appears below and is an integral part of this License Agreement) shall apply. […]
Content, when it is made available to you, is only for your personal use. Even when you obtain the right to use certain Content indefinitely and for as many playbacks as you wish, your use is pursuant to the Business Rules assigned by the Content owner. […] Except where Business Rules expressly provide otherwise, all terms of this License Agreement that pertain to Software, including without limitation the prohibitions against reverse engineering and unauthorized copying, pertain with equal force to Content.
The Software enables Content owners to control your access to their Content in accordance with the Business Rules. UMG, as a Content owner, reserves the right to use the Software at any time to enforce the Business Rules with or without notice to you […]".

[789] Dies gilt auch, wenn der Nutzer gar keinen Vertrag mit dem Inhalteanbieter selbst, sondern nur mit dem DRM-System-Betreiber geschlossen hat. Wenn dem Nutzer in einem DRM-Installationsvertrag bestimmte Bedingungen auferlegt werden, zu denen er die digitalen Inhalte nutzen darf, so dienen diese Bedingungen letztlich nicht den Interessen des DRM-Systembetreibers. Der DRM-Systembetreiber integriert solche Bedingungen in den Vertrag mit dem Nutzer vielmehr, um den Inhalteanbietern versichern zu können, eine sichere Vertriebsplattform für ihre digitalen Inhalte anzubieten. Mittelbar dienen solche Klauseln dem Schutz der Inhaltenabieter.

DRM-Systeme können über hunderttausende oder gar Millionen von Nutzern verfügen. Das Besondere solcher Nutzungsverträge ist, daß in einem *Massenmarkt* eine vertragliche Beziehung zwischen dem Inhalteanbieter und jedem einzelnen Nutzer besteht.

Darin unterscheiden sich digitale Inhalte in DRM-Systemen deutlich von herkömmlichen Medien. Beim Kauf eines normalen Buchs schließt der Käufer einen Kauftvertrag mit einem Buchhändler über das körperliche Werkexemplar ab. Mit dem Urheber steht er in keiner vertraglichen Beziehung. Dies ist auch unnötig, da die Zulässigkeit der denkbaren Handlungen, die der Käufer an dem Buch vornimmt – Lesen des Buchs, Übernehmen von Ideen oder Zitieren des Buchs, Verkaufen oder Verleihen des Buchs etc. –, im Urheberrechtsgesetz geregelt sind.[790] Zwar schützt das Urheberrecht auch den Inhalteanbieter in DRM-Systemen.[791] Wenn aber der Inhalteanbieter eine vertragliche Beziehung zum Nutzer aufbaut, kann er diesen vertraglichen Schutzmechanismus aber sehr viel besser beeinflussen als das notwendigerweise pauschalierende Urheberrecht: So kann er kann dem Nutzer nur ganz beschränkte Nutzungsrechte einräumen.

Das Phänomen, daß Rechteinhaber mit dem inflexiblen Urheberrecht unzufrieden sind und dieses Problem durch vertragliche Beziehungen zum Kunden lösen wollen, ist kein Novum von DRM-Systemen. Es läßt sich auch bei herkömmlichen Medien beobachten. In den 30er Jahren sah das U.S.-amerikanische Urheberrecht noch kein ausschließliches Verwertungsrecht der öffentlichen Wiedergabe für Tonaufnahmen vor. Um eine öffentliche Wiedergabe auf vertraglichem Wege zu verhindern, druckte die „RCA Manufacturing Company“ auf die von ihr hergestellten Schallplatten einen Hinweis, nach dem die gekaufte Schallplatte nur für nichtkommerzielle Zwecke benutzt werden dürfe.[792] Würde ein solcher Aufdruck zu einem wirksamen Vertragsschluß zwischen dem Schallplat-

[790] S. a. *Netanel*, 106 Yale L. J. 283, 305 (1996).

[791] S. oben Teil 2, A.

[792] Der Hinweis lautete: „Only For Non-Commercial Use on Phonographs in Homes. Mfr. & Original Purchaser Have Agreed This Record Shall Not Be Resold Or Used For Any Other Purpose. See Detailed Notice on Envelope“, zitiert nach RCA Co. v. Whiteman, 114 F.2d 86, 87 (2d Cir. 1940). Die Klausel wurde vom Gericht jedoch für unwirksam gehalten. S. a. *D. Nimmer/Brown/Frischling*, 87 Cal. L. Rev. 17, 44 (1999); *Litman*, 13 Berkeley Tech. L. J. 931, 939 (1998). Schon im Jahre 1908 hatte sich der U.S. Supreme Court mit der Frage zu beschäftigen, ob eine Klausel auf der Innenseite eines Buchdeckels wirksam sei, nach der ein Händler das Buch nicht zu einem Preis von weniger als $ 1.00 weiterverkaufen dürfe und er ansonsten eine Urheberrechtsverletzung begehe. Der Supreme Court verneinte dies, s. Bobbs-Merrill Co. v. Straus, 210 U.S. 339, 28 S. Ct. 722 (1908); s. dazu auch *Nimmer/Brown/Frischling*, 87 Cal. L. Rev. 17, 45 (1999); *Lunney*, 1 Tulane J. Tech. & Intell. Abs. 11 (1999). Aus diesem Caselaw entwickelte sich nach und nach die U.S.-amerikanische „first sale doctrine“, das Äquivalent zum Erschöpfungsgrundsatz.

tenunternehmen und dem Käufer führen, könnte das Schallplattenunternehmen seine Schutzinteressen durch diesen vertraglichen Schutzmechanismus wahren. In Deutschland gab es ähnliche Ansätze. Vor der Umsetzung der europäischen Vermiet- und Verleihrichtlinie[793] durch das 3. UrhGÄndG 1995 war das Vermiet- und Verleihrecht nur als Teil des allgemeinen Verbreitungsrechts gemäß § 17 a. F. UrhG erfaßt. Daher versuchten die Hersteller von Videokassetten und Tonträger beim Vertrieb dieser Produkte, durch Aufdrucke auf die Werkstücke den Erwerbern die gewerbsmäßig Vermietung zu untersagen.[794] Das wichtigste Beispiel, in denen Rechteinhaber im Massenmarkt eine vertragliche Beziehung zum Nutzer aufbauen wollen, sind sogenannte „Schutzhüllenverträge" bei Computersoftware.[795]

II. Wirksamkeit der Nutzungsverträge

1. Allgemeines

Mit Hilfe von DRM-Nutzungsverträgen versucht der Rechteinhaber, in einem Massenmarkt eine vertragliche Beziehung zu jedem einzelnen Nutzer seines Inhalts aufzubauen und die Nutzer in den Nutzungsverträgen rechtlichen Beschränkungen zu unterwerfen. Es stellt sich die Frage, ob solche Nutzungsverträge überhaupt rechtlich wirksam sind.

Die vorliegende Arbeit untersucht abstrakt die Implikationen von DRM-Systemen. Es ist nicht ihr Ziel, die rechtliche Wirksamkeit von Nutzungsverträgen in einem bestimmten DRM-System zu untersuchen. Sie will nur untersuchen, ob *Einwände grundsätzlicher Art* existieren, wonach Nutzungsverträge der dargestellten Art in DRM-Systemen rechtlich nicht wirksam sein *können*. Solche Einwände sind aus dreierlei Richtung denkbar. Erstens könnten Nutzungsverträge in DRM-Systemen mit sogenannten „Schutzhüllenverträgen" bei Computersoftware vergleichbar sein, deren Wirksamkeit äußerst umstritten ist. Zweitens werden Nutzungsverträge in DRM-Systemen oftmals über das Internet abgeschlossen werden. Dann stellt sich die Frage, ob solche online abgeschlossenen Verträge wirksam sind. Drittens wird in solchen Nutzungsverträgen oftmals das Recht, einen digitalen Inhalt zu nutzen, in inhaltlicher, zeitlicher und persönlicher Hinsicht stark beschränkt. Es stellt sich die Frage, ob unter urheberrechtlichen Gesichtspunkten die Einräumung solch eng beschränkter Nutzungsrechte überhaupt möglich ist. Im folgen-

[793] Zur Richtlinie s. oben bei Fn. 746.

[794] S. zum ganzen *Loewenheim* in: Schricker (Hrsg.), UrhG-Kommentar, 1. Aufl., § 17 Rdnr. 13 f.; *Hubmann*, Film und Recht 1984, 495 ff.; BGH GRUR 1986, 736 – Schallplattenvermietung. Auf die Frage der Wirksamkeit solcher Aufdrucke wird im folgenden nicht eingegangen.

[795] S. dazu sogleich im Text.

den soll diesen drei Fragen nachgegangen werden. Dabei wird auf die deutsche und die U.S.-amerikanische Rechtslage eingegangen.

2. Wirksamkeit nach deutschem Recht

a) Schutzhüllenverträge bei Computersoftware

Erwirbt ein Käufer heutzutage ein Softwareprogramm bei einem Händler, so findet sich auf der Verpackung des physikalischen Datenträgers (CD-ROM) der Hinweis, daß der Kunde mit dem Öffnen der Verpackung die Bedingungen des beiliegenden Vertrages anerkenne. Der Vertrag – auch „Schutzhüllenvertrag“[796] genannt – ist auf einem ausführlichen Beipackzettel oder auf einem Umschlag abgedruckt, in dem der Datenträger steckt. In dem Vertrag sind unter anderem Klauseln enthalten, die die Berechtigung zur Nutzug des Softwareprogramms regeln.[797] So finden sich Klauseln, daß der Käufer das Programm nur auf einem einzigen Computer benutzen darf (sogenannte CPU-Klausel), daß er die Software nicht oder nur unter bestimmten Bedingungen weitergeben darf,[798] daß er die Software nicht auf verschiedenen Computern oder nicht in einem Netzwerk benutzen darf (sogenannte Netzwerkklauseln) oder daß er das Programm nur in Verbindung mit einem neuen Computer erwerben darf (sogenannte OEM-Klauseln).[799] Auch sind vertragliche Verbote des „Reverse Engineering“[800] weit verbreitet.[801]

Wie bei DRM-Systemen begnügt sich der Softwarehersteller nicht mit dem Schutz durch das Urheberrecht. Er will den Nutzer vertraglich binden und dabei Schutzinteressen wahren, die durch das Urheberrecht nicht in gleicher Weise geschützt werden. Die Wirksamkeit von Schutzhüllenverträgen bei Computersoftware ist äußerst umstritten. Falls sich diese Bedenken auf Nutzungsverträge bei DRM-Systemen übertragen ließen, wäre es für den Inhalteanbietern in DRM-Systemen schwierig, seine Interessen auf vertraglichem Weg zu schützen. Daher soll im folgenden untersucht werden, aus welchen Gründen die Wirksamkeit von Schutz-

---

[796] Der Vertragstyp hat über das U.S.-amerikanische Recht Eingang in das moderne deutsche Vertragsrecht gefunden, *Diedrich*, MMR 1998, 513.

[797] Daneben finden sich u. a. Gewährleistungs- und Haftungsbegrenzungen in Schutzhüllenverträgen. Zu Schutzhüllenverträgen allgemein s. *Schuhmacher*, CR 2000, 641; *Marly*, Softwareüberlassungsverträge, Rdnr. 366; *Hoeren*, Rdnr. 386 f.; *Pres*, S. 179 ff.; *Kochinke/Günther*, CR 1997, 129 f.

[798] Zu entsprechenden Klauseln im amerikanischen Bereich s. *Lemley*, 87 Cal. L. Rev. 111, 131 (1999).

[799] Zu den Klauseln im Überblick *Polley*, CR 1999, 345 f.; *Schuhmacher*, CR 2000, 641, 645; umfassend *Marly*, Softwareüberlassungsverträge, Rdnr. 882 ff.

[800] Zum Begriff s. oben Teil 1, C IV 2 b.

[801] Zur Rechtslage in Deutschland *Marly*, Softwareüberlassungsverträge, Rdnr. 1039 ff. Zur Lage in den USA s. *Lemley*, 87 Cal. L. Rev. 111, 129 f. (1999), auch zu weiteren üblichen Nutzungsverbeinbarungen. Beispiele tatsächlich verwendeter amerikanischer Nutzungsvereinbarungen gibt *Gomulkiewicz*, 13 Berkeley Tech. L. J. 891, 909 ff. (1999). S. weiterhin *Minassian*, 45 UCLA L. Rev. 569, 572 ff. (1997).

hüllenverträgen zweifelhaft ist und ob diese Zweifel auch auf Nutzungsverträge in DRM-Systemen zutreffen.

Dabei sind die Besonderheiten von Schutzhüllenverträgen zu beachten. Nach Vorstellung der Softwarehersteller wird der Schutzhüllenvertrag zwischen dem Käufer der Software *und dem Softwarehersteller* geschlossen. Dies soll selbst dann gelten, wenn der Käufer die Software nicht direkt beim Softwarehersteller, sondern – was die Regel ist – von einem Händler erwirbt. Nach Vorstellung der Softwarehersteller schließt der Käufer zwei Verträge ab, die beide die Überlassung desselben Computerprogramms zum Gegenstand haben: einerseits den sogenannten „Softwareüberlassungsvertrag“[802] mit dem Händler, andererseits den Schutzhüllenvertrag mit dem Hersteller.[803] Erst der Schutzhüllenvertrag regelt die Einzelheiten der erlaubten Programmnutzung.[804] Die Bedingungen des

[802] Die rechtliche Qualifizierung des Softwareüberlassungsvertrags ist seit langem heillos umstritten. Aus urheberrechtlicher Sicht sind die Einzelheiten dieses Streits weniger bedeutend, da der Softwareüberlassungsvertrag ein Verpflichtungsgeschäft ist und die einzelnen Ansichten oftmals nur zu unterschiedlichen Konsequenzen im Leistungsstörungsrecht führen, *Lehmann* in: Beier/Götting/Lehmann/Moufang (Hrsg.), S. 543, 561. Grundsätzlich ist zwischen Individual- und Standardsoftware sowie nach der Überlassungszeit (Überlassung auf Dauer oder auf Zeit) zu unterscheiden. Insbesondere bei Standardsoftware besteht hinsichtlich nahezu keiner Frage Einigkeit. Die auf Dauer angelegte Überlassung von Standardsoftware wird als Kaufvertrag, als kaufähnlicher Vertrag, als Werklieferungsvertrag, als mietähnlicher Vertrag, als Vertrag zwischen Kauf und Rechtspacht, als Lizenzvertrag, als Know-how-Lizenzvertrag oder als Vertrag sui generis eingeordnet, s. dazu umfassend *Marly*, Softwareüberlassungsverträge, Rdnr. 62 ff., 165 ff.; *Hoeren*; *Hoeren/Schuhmacher*, CR 2000, 137 f.; *Ulmer*, CR 2000, 493. Mit dieser Kategorisierungsfrage eng verbunden ist der Meinungsstreit, ob ein Computerprogramm eine Sache i. S. d. § 90 BGB ist, s. dazu *Marly*, a. a. O., Rdnr. 90 ff.; *Bydlinski*, AcP 198 (1998), 287, 305 ff.; *Hoeren*, Rdnr. 71 ff. Ein paralleles Problem ergibt sich bei der schuldrechtlichen Einordnung von Verträgen, bei dem die Software über das Internet heruntergeladen wird, s. *Cichon*, S. 232 ff.; *Bydlinski*, a. a. O., S. 313 f.; *Hoeren*, Rdnr. 346 ff. Zur schuldrechtlichen Einordnung beim Online-Erwerb sonstiger digitaler Inhalte s. *Cichon*, S. 281 ff. Hinsichtlich des Meinungsstreits bringt es *Bydlinski*, a. a. O., S. 288, auf den Punkt: „Keiner weiß etwas Genaues; aber alle können damit leben.“ Die Diskussion wird dadurch erschwert, daß oft nicht genügend zwischen dem Vertragsverhältnis Hersteller-Händler und Händler-Kunde differenziert wird. Unter dem Begriff „Softwareüberlassungsvertrag“ wird regelmäßig der Vertrag zwischen dem Händler und dem Kunden verstanden. In diesem Vertrag können grundsätzlich auch Nutzungsbedingungen festgelegt werden. Zumindest bei Computersoftware versuchen die Hersteller jedoch regelmäßig, eigenständig solche Nutzungsbedingungen in einem „Schutzhüllenvertrag“ festzulegen. Der Schutzhüllenvertrag ist vom Softwareüberlassungsvertrag zu unterscheiden (s. dazu *Hoeren*, Rdnr. 398 ff.; *Marly*, a. a. O., Rdnr. 377 f.; *Schuhmacher*, CR 2000, 641, der ihn zu Unterscheidungszwecken „Lizenzvertrag“ nennt). Vorliegegend geht es um diesen Schutzhüllenvertrag.

[803] *Schuhmacher*, CR 2000, 641.

[804] *Schuhmacher*, CR 2000, 641. Es ist unklar, in welchem Verhältnis diese beiden Verträge stehen. Zwar wäre es grundsätzlich denkbar, beide Vorgänge als Teil eines einheitlichen Vertrags anzusehen. So könnten die im Schutzhüllenvertrag enthaltenen Nutzungsbedingungen als Allgemeine Geschäftsbedingungen Teil des Softwareüberlassungsvertrags zwischen Händler und Kunde sein. Danach würde der Händler die Soft-

Schutzhüllenvertrags sind regelmäßig auf der Außenseite der Verpackung aufgedruckt. Nach Vorstellung der Softwarehersteller wird der Schutzhüllenvertrag nicht schon mit dem Erwerb der Software durch den Käufer geschlossen, sondern erst mit dem Öffnen der Verpackung; eine entsprechende Klausel findet sich in den Schutzhüllenverträgen.[805] Entsprechende Probleme stellen sich, wenn die Schutzhüllenverträge online geschlossen werden. In Deutschland wird dann mitunter von „Enter"-Verträgen gesprochen.[806] Dabei werden dem Käufer beim erstmaligen Starten eines erworbenen Computerprogramms die Bedingungen des „Schutzhüllenvertrags" angezeigt. Nach Vorstellung der Softwarehersteller akzeptiert der Käufer durch das Betätigen der „Enter"-Taste die Vertragsbedingungen, so daß eine direkte vertragliche Beziehung zum Softwarehersteller hergestellt wurde.

Es ist äußerst fraglich, ob in dem bloßen Aufreißen einer Verpackung eine wirksame Vertragsannahme durch den Kunden gesehen werden

ware dem Kunden zu den Bedingungen des Herstellers überlassen. Diese Konstruktion wird jedoch regelmäßig abgelehnt, da sie weder im Interesse des Herstellers, der eine direkte vertragliche Beziehung zum Nutzer wünscht, noch im Interesse des Händlers ist, der seine Geschäfte nach einheitlichen Bedingungen und nicht nach den unterschiedlichen Bedingungen der einzelnen Hersteller abwickeln möchte, *Schuhmacher*, a. a. O., S. 642; *Marly*, Softwareüberlassungsverträge, Rdnr. 376; ebenso für Urheberrechtshinweise auf Videokassetten *Hubmann*, Film und Recht 1984, 495, 497. Schließlich würde eine Einbeziehung oft gemäß § 2 AGBG an einem unzureichenden Hinweis auf die Geltung der AGB scheitern, s. dazu *Schuhmacher*, a. a. O., S. 642; *Pres*, S. 180 ff. Eine andere Konstruktionsmöglichkeit wäre, daß der Händler hinsichtlich des Nutzungsvertrags in Vertretung des Herstellers handelte. Dies ist jedoch nach Konstruktion der Schutzhüllenverträge nicht beabsichtigt und kommt auch in der Praxis kaum vor, *Schuhmacher*, a. a. O., S. 642; ebenso für Urheberrechtshinweise auf Videokassetten *Hubmann*, Film und Recht 1984, 495, 497. *Marly*, a. a. O., Rdnr. 375, sieht in einer solchen Konstruktion auch einen Verstoß gegen §§ 3 und 9 Abs. 2 Nr. 2 AGBG. Aus diesen Gründen sind die Bedingungen des Schutzhüllenvertrags regelmäßig nicht schon Teil des Softwareüberlassungsvertrags zwischen Händler und Kunden. Aus der Aufsplittung in zwei Verträge entstehen jedoch zusätzliche Probleme. So erscheint fraglich, inwieweit der Schutzhüllenvertrag mit dem Softwarehersteller den Inhalt des Softwareüberlassungsvertrags mit dem Händler verändern kann. Es wird vertreten, der Käufer habe beim Erwerb der Computersoftware vom Händler schon das Recht erworben, die zur Ausführung des Programms erforderlichen urheberrechtlich relevanten Handlungen vorzunehmen, § 69 d UrhG. Die gesonderte Einräumung eines (eventuell stärker beschränkten) Nutzungsrechts seitens des Herstellers verstoße gegen §§ 3, 9 AGBG, s. *Schuhmacher*, CR 2000, 641, 644; *Hoeren*, Rdnr. 425 ff., 433 ff.; s. a. *Marly*, Softwareüberlassungsverträge, Rdnr. 891.

[805] Manchmal ist der Schutzhüllenvertrag nicht einmal auf die Außenseite der Verpackung gedruckt, sondern nur in der Verpackung beigelegt. Dann hat der Käufer vor Erwerb der Software keine Möglichkeit, die Vertragsbedingungen überhaupt zur Kenntnis zu nehmen.

[806] So von *Schuhmacher*, CR 2000, 641, und *Marly*, Softwareüberlassungsverträge, Rdnr. 367; *Hoeren*, Rdnr. 390 f.

kann. Daher wird die Wirksamkeit von Schutzhüllenverträgen mehrheitlich verneint.[807] Gleiches gilt für die erwähnten „Enter"-Verträge.[808]

Es zeigt sich, daß die verworrene Problematik der Wirksamkeit von Schutzhüllenverträgen auf zwei besonderen Konstellationen beruht: Einerseits soll durch Schutzhüllenverträge eine vertragliche Beziehung des Käufers zum Softwarehersteller geschaffen werden, auch wenn der Käufer die Software gar nicht von diesem erworben hat. Andererseits soll im bloßen Aufreißen einer Verpackung durch den Käufer eine wirksame Vertragsannahme erblickt werden. Bestehen diese beiden Konstellationen nicht, spricht auch nichts gegen die Wirksamkeit derart modifizierter Schutzhüllenverträge. Aus diesem Grund sind solche Verträge wirksam, wenn der Käufer die Software direkt beim Softwarehersteller erwirbt. In diesem Fall handelt es sich um normale allgemeine Geschäftsbedingungen.[809] Andererseits sind solche Verträge wirksam, wenn der Kunde nach dem Aufreißen der Verpackung auf eine andere, unzweifelhafte Weise die Annahme des Schutzhüllenvertrags erklärt.[810]

---

[807] In den aufgedruckten Vertragsbedingungen liegt ein wirksames Vertragsangebot durch den Softwarehersteller. Es bestehen erhebliche Zweifel an einer wirksamen Annahmeerklärung durch den Anwender. Zwar könnte diese Annahmeerklärung grundsätzlich konkludent erfolgen, wenn der Kunde die Verpackung öffnet und die darin enthaltene Software nutzt. Daß der Hersteller nichts von der Annahme erfährt, wäre wegen § 151 BGB ebenfalls unschädlich, *Schuhmacher*, CR 2000, 641, 642; *Marly*, Softwareüberlassungsverträge, Rdnr. 378. Problematisch ist jedoch, ob der tatsächlichen Handlung der Verpackungsöffnung wirklich die Bedeutung einer Willenserklärung beigemessen werden kann. Die herrschende Meinung lehnt dies ab. Der Softwarehersteller könne nicht einseitig festlegen, daß dem Realakt in Form des Aufreißens der Verpackung eine bestimmte rechtliche Bedeutung zukomme; vielmehr seien nach § 157 BGB die Verkehrssitte und der Grundsatz von Treu und Glauben heranzuziehen, s. nur *Marly*, a. a. O., Rdnr. 380, m. w. N. Der Kunde habe beim Öffnen der Schutzhülle kein Erklärungsbewußtsein, und für ein fahrlässiges Verhalten des Kunden, bei dem er sich einen fahrlässig gesetzten Erklärungsinhalt trotz fehlenden Erklärungsbewußtseins als eigene Willenserklärung zurechnen lassen muß, sei nichts ersichtlich. Der Hersteller sei nicht schutzwürdig; sein Diktat könne nicht zur Entstehung einer Verkehrssitte führen, *Marly*, a. a. O., Rdnr. 381. Damit sind Schutzhüllenverträge nach herrschender Meinung unwirksam. S. zum ganzen *Schuhmacher*, a. a. O., S. 642 f.; *Marly*, a. a. O., Rdnr. 365 ff.; *Hoeren*, Rdnr. 415 ff.; *Pres*, S. 183 f. A.A. OLG Stuttgart, CR 1989, 685, 687, wo Schutzhüllenverträge ohne Begründung für wirksam gehalten werden; ebenso a. A. *Moritz* in: Kilian/Heussen (Hrsg.), Kap. 42, Rdnr. 176; *Schneider*, CR 1996, 657, 662.

[808] Auch hier ist fraglich, ob eine wirksame Annahmeerklärung durch den Käufer vorliegt; verneinend *Schuhmacher*, CR 2000, 641, 643; *Hoeren*, Rdnr. 410 ff.; s.a. *Marly*, Softwareüberlassungsverträge, Rdnr. 383.

[809] *Schuhmacher*, CR 2000, 641, 644; *Marly*, Softwareüberlassungsverträge, Rdnr. 370. Dann greifen freilich die Bestimmungen des AGB-Gesetzes ein.

[810] Dies ist beispielsweise bei Registrierkarten-Systemen oder der Online-Registrierung der Fall. Dabei wird der Käufer regelmäßig deutlich darauf hingewiesen, daß er mit der Registrierung die Bedingungen des Nutzungsvertrags anerkenne. Dabei kann der Käufer von dem Inhalt des Nutzungsvertrags auch problemlos Kenntnis nehmen. In solchen Konstellationen wird eine wirksame Annahmeerklärung bejaht, s. *Schuhma-*

Es zeigt sich, daß die Bedenken gegen die Wirksamkeit von Schutzhüllenverträgen auf spezifischen Einzelheiten des heutigen Vertriebsmodells der Softwarehersteller beruhen. Diese Bedenken sprechen nicht grundsätzlich gegen eine wirksame vertragliche Beziehung zwischen Rechteinhabern und Nutzern im Massenmarkt. Wenn der Inhalteanbieter und der DRM-Systembetreiber den Bedenken zu Schutzhüllenverträgen Rechnung tragen und ihr Vertriebsmodell entsprechend anders ausgestalten, ist unter diesem Gesichtspunkt nichts gegen die Wirksamkeit von Nutzungsverträgen in DRM-Systemen zu sagen. Zu diesem Zweck könnte der Inhalteanbieter beispielsweise den Nutzungsvertrag direkt mit dem Nutzer abschließen. Auch kann die für Computersoftware typische Aufsplittung in zwei unterschiedliche Verträge – Softwareüberlassungsvertrag und Schutzhüllenvertrag – in DRM-Systemen vermieden werden. Zwar können Nutzungsverträge in DRM-Systemen immer noch gegen Vorschriften des AGB-Gesetzes oder des Urheberrechts verstoßen. Zumindest unter dem Gesichtspunkt der Schutzhüllenverträge erscheinen wirksame Nutzungsverträge in DRM-Systemen jedoch grundsätzlich möglich.[811]

b) Wirksamer Vertragsschluß im Internet

Nutzungsverträge werden in vielen DRM-Systemen online abgeschlossen. Es stellt sich die Frage, ob gegen die Wirksamkeit solcher Nutzungsverträge Bedenken bestehen. Es handelt sich dabei um die allgemeinere Problematik, ob über das Internet wirksame Verträge abgeschlossen werden können. Bei solchen Verträgen stellen sich vielfältige Probleme im Hinblick auf den Zugang von Willenserklärungen, das anwendbare Recht, die Einbeziehung Allgemeiner Geschäftsbedingungen, die rechtliche Wirksamkeit von digitalen Signaturen, die Einhaltung von Formvorschriften sowie die Anwendbarkeit von Verbraucherschutzvorschriften. Auf diese Probleme wird hier nicht näher eingegangen.[812] Es ist nämlich

cher, CR 2000, 641, 643 f.; *Hoeren*, Rdnr. 432; *Marly*, Softwareüberlassungsverträge, Rdnr. 389.

[811] *Perritt,* 1996 U. Chi. Legal F. 261, 292 Fn. 121 (1996), bezeichnet DRM-Systeme wegen der im Vergleich zu herkömmlichen Schutzhüllenverträgen („shrinkwrap licenses") höheren Rechtssicherheit daher als „the ultimate shrinkwrap".

[812] S. dazu im Überblick *Mehrings* in: Hoeren/Sieber (Hrsg.), Teil 13.1; *Marly*, Softwareüberlassungsverträge, Rdnr. 231 ff. S. weiterhin *Kaiser/Voigt*, K&R 1999, 445 ff.; *Lauktien/Varadinek*, ZUM 2000, 466 ff.; *Thot*, S. 52 ff.; *Rehbinder/Schmaus*, UFITA 2000, 313 ff. Zu den Auswirkungen der sog. E-Commerce-Richtlinie s. *Spindler*, MMR-Beilage 7/2000, 4 ff. Zur digitalen Signatur im Überblick s. *Mertes/Zeuner* in: Hoeren/Sieber (Hrsg.), Teil 13.3. Zur Novelle des Signaturgesetzes infolge der Signatur-Richtlinie s. *Tettenborn*, CR 2000, 683 ff. Zum Verbraucherschutz im Internet im Überblick s. *Waldenberger* in: Hoeren/Sieber (Hrsg.), Teil 13.4. Zu den Auswirkungen des Fernabsatzgesetzes, auch zu einem eventuellen Widerrufsrecht bei der Online-Lieferung von Audio-, Video- und Softwaredateien nach § 3 Abs. 1 Nr. 2 lit. b oder § 3 Abs. 2 Nr. 1 3. Variante FernAbsG, s. *Piepenbrock/Schmitz*, K&R 2000, 378, 384 f.

trotz all dieser Probleme unstreitig, daß über das Internet wirksam Verträge abgeschlossen werden können.[813] Damit steht der Wirksamkeit online abgeschlossener Nutzungsverträge in DRM-Systemen auch unter diesem Gesichtspunkt nichts *Grundsätzliches* im Wege.

Ein zusätzliches Problem könnte darin erblickt werden, daß in Zukunft Software-Agenten wichtige Aufgaben in DRM-Systemen übernehmen könnten. So könnten sie ihrem Besitzer Teile der Vertragsanbahnung, des Vertragsabschlusses und der Vertragsdurchführung autonom abnehmen.[814] Wird in einem DRM-System ein Nutzungsvertrag gleichsam autonom durch einen Software-Agenten abgeschlossen, scheint fraglich, ob ein solcher „Vertrag" auch für den Nutzer verbindlich ist, auf dessen Veranlassung der Software-Agent gehandelt hat. In der deutschen Literatur wird die Problematik oft unter dem Stichwort der „Computererklärung" behandelt. Darunter sind Willenserklärungen zu verstehen, die nicht nur elektronisch übermittelt, sondern zusätzlich von einem Computerprogramm zwar auf Veranlassung eines Menschen, aber ohne *konkretes* menschlisches Zutun automatisiert erzeugt werden.[815] Erklärungen von Software-Agenten können als solche „Computererklärungen" aufgefaßt werden. Teilweise wird vertreten, Computererklärungen seien keine Willenserklärungen, da im Zeitpunkt ihrer Erstellung kein konkreter menschlicher Beteiligungsakt erfolge, der die Grundlage für die Zurechnung zum dahinterstehenden Menschen sei.[816] Die ganz herrschende Meinung sieht Computererklärungen jedoch als wirksame Willenserklärungen an. Der Einsatz des Computers beruhe auf dem Willen seines Betreibers, der sich die vom Computer erstellten Erklärungen als „eigene" Willenserklärungen zurechnen lassen wolle.[817] Die Begründungen diffe-

[813] *Kaiser/Voigt*, K&R 1999, 445, 452 („Es ist möglich, den formfreien Rechtsverkehr vollständig auf das Internet zu verlagern"). S. dazu auch Art. 9 der E-Commerce-Richtlinie, ABl. EG Nr. L 178 vom 17. 7. 2000, S. 1.

[814] Zu den technischen Grundlagen s. oben Teil 1, E III.

[815] Von der Computererklärung sind sog. „elektronische Willenserklärungen" zu unterscheiden, bei denen eine normale menschliche Willenserklärung auf elektronischem Wege übermittelt wird. Füllt ein Nutzer am Computer eine Bestellmaske durch Eingabe seines Namens, seiner Anschrift und des gewünschten Produkts aus, und werden diese Daten an den Empfänger online übermittelt („elektronische Willenserklärung"), so finden die bekannten Regeln der Rechtsgeschäftslehre unmittelbar Anwendung; *Mehrings* in: Hoeren/Sieber (Hrsg.), Teil 13.1, Rdnr. 31; *Heun*, CR 1994, 595. Die Terminologie differiert teilweise; so werden „Computererklärungen" auch als „automatisierte", „vollelektronische" oder „elektronische" Willenserkläungen bezeichnet, s. *Mehrings*, a. a. O., Rdnr. 23.

[816] *Clemens*, NJW 1985, 1998, 2001. Für einen speziellen Fall im Bereich des bargeldlosen Zahlungsverkehrs ebenfalls ablehnend *Möschel*, AcP 186 (1986), 187, 195 f.

[817] *Mehrings* in: Hoeren/Sieber (Hrsg.), Teil 13.1, Rdnr. 40 ff.; *Kuhn*, S. 81; *Medicus*, Rdnr. 256; *Heinrichs* in: Palandt, Einf. v. § 116 Rdnr. 1; *Heun*, CR 1994, 595, 596.

rieren im einzelnen.[818] Damit könnten selbst Software-Agenten in DRM-Systemen wirksame Nutzungsverträge abschließen.[819] Der Vision eines „agent-mediated electronic commerce“[820] steht aus rechtlicher Sicht nichts *Grundsätzliches* entgegen.[821]

c) Einräumung beschränkter Nutzungsrechte

Inhalteanbieter können mit „rights management languages“[822] die Bedingungen, zu denen ein Nutzer einen digitalen Inhalt nutzen kann, auf technischem Wege in nahezu beliebiger Weise und äußerst differenziert kontrollieren. Die Nutzungsbedingungen finden sich zusätzlich oftmals in den Nutzungsverträgen wieder. Beziehen sich die Bedingungen auf Bereiche, die einem urheberrechtlichen Verwertungsrecht unterliegen, so räumt der Inhalteanbieter dem Nutzer in dem Vertrag ein urheberrechtliches Nutzungsrecht im Sinne des § 31 UrhG ein. Wird das Nutzungsrecht in inhaltlicher, zeitlicher, persönlicher oder räumlicher Hinsicht beschränkt, stellt sich die Frage, ob eine solche Beschränkung unter urheberrechtlichen Gesichtspunkten wirksam ist.

Nach der in Deutschland herrschenden monistischen Auffassung ist das Urheberrecht ein einheitliches Recht, dessen persönlichkeits- und verwertungsrechtliche Bestandteile untrennbar miteinander verbunden sind, so daß das Urheberrecht als Ganzes unübertragbar ist, § 29 S. 2 UrhG.[823] Der Urheber[824] kann über seine Verwertungsrechte nur durch Abspaltung

---

[818] Teilweise wird eine Computererklärung schon aufgrund der allgemeinen Rechtsgeschäftslehre als Willenserklärung angesehen; da das Computerprogramm von einem Menschen stamme und der Programmbetrieb auf dem Willen des Betreibers beruhe, gingen die „Erklärungen“ des Programms zumindest mittelbar auf einen menschlichen Willen zurück, s. *Medicus*, Rdnr. 256. Teilweise wird eine Parallele zum Verkauf durch Warenautomaten, teilweise zur Blanketterklärung gezogen, teilweise werden §§ 164 ff. BGB analog angewandt. S. dazu und zu weiteren Fragen von Computererklärungen *Mehrings* in: Hoeren/Sieber (Hrsg.), Teil 13.1, Rdnr. 39 ff.; *Kuhn*, S. 54 ff.; *Heun*, CR 1994, 595.

[819] Ein wirksamer Vertragsschluß liegt auch vor, wenn beide Vertragspartner Computererklärungen verwenden, s. *Mehrings* in: Hoeren/Sieber (Hrsg.), Teil 13.1, Rdnr. 27 f.

[820] S. dazu oben Teil 1, E III.

[821] Die europäische E-Commerce-Richtlinie enthält keine speziellen Regelungen zu Software-Agenten. Zwar war im ersten Kommisions-Vorschlag der für die Richtlinie zu Art. 9 der Hinweis enthalten, daß u. a. die „Verwendung bestimmter elektronischer Systeme wie z. B. ‚intelligenter‘ Softwaremodule“ nicht behindert werden darf, s. den ersten Vorschlag zur E-Commerce-Richtlinie, *Europäische Kommission*, KOM (1998) 586 endg., S. 28; in der englischen Fassung wird korrekter von „intelligent software *agents*“ gesprochen. Spätere Richtlinienentwürfe enthielten diese Formulierung aber nicht mehr; kritisch dazu *Lerouge*, 18 J. Marshall J. Computer & Info. L. 403, 418 (1999); s. weiterhin *Poggi*, 41 Va. J. Int'l L. 224, 265 (2000).

[822] Zu dem Begriff s. oben Teil 1, C II 2 a bb 1.

[823] S. *Schack*, Rdnr. 306 ff.

[824] Auch wenn im folgenden die Rechtsstellung des Urhebers behandelt wird, sind zusätzlich die Rechte von Leistungsschutzberechtigten zu beachten. So können bei-

einzelner Nutzungsrechte verfügen, § 31 Abs. 1 S. 1 UrhG.[825] Der Urheber kann dem Nutzer ausschließliche oder einfache Nutzungsrechte einräumen, § 31 Abs. 1 S. 2 UrhG. Nach § 32 UrhG ist es möglich, die eingeräumten Nutzungsrechte räumlich, zeitlich oder inhaltlich zu beschränken. Der Zuschnitt des Nutzungsrechts ist aber nur in gewissen Grenzen möglich. Obwohl im Immaterialgüterrecht kein numerus clausus wie im Sachenrecht existiert,[826] ist doch auf den Verkehrsschutz Rücksicht zu nehmen. Danach sind Nutzungsrechte nur insofern abspaltbar, als es sich nach der Verkehrsauffasung um übliche, technisch und wirtschaftlich eigenständige und damit klar abgrenzbare konkrete Nutzungsformen handelt.[827] Diese Grundsätze können die Möglichkeiten von Inhalteanbietern in DRM-Systemen begrenzen, in Nutzungsverträgen urheberrechtliche Nutzungsrechte auf einzelne Nutzungen zuzuschneiden.[828]

Weiterhin ist zu beachten, daß die dargestellten Grundsätze nur für die Einräumung von Nutzungsrechten auf der Ebene des Verfügungsgeschäfts gelten. Davon ist die Ebene des Verpflichtungsgeschäfts zu trennen. Auch im Urheberrecht gilt das allgemeine zivilrechtliche Trennungsprinzip, nach dem gedanklich zwischen Verpflichtung und Verfügung zu trennen ist.[829] Selbst wenn dem Nutzer auf der Ebene des Verfügungsgeschäfts ein weites Nutzungsrecht[830] eingeräumt wird, kann die Ausübung

---

spielsweise Tonträger- und Filmhersteller in entsprechender Anwendung der §§ 31–33 UrhG ebenfalls Nutzungsrechte einräumen, s. *von Gamm*, § 85 Rdnr. 3; § 94 Rdnr. 4; *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, vor §§ 28 ff. Rdnr. 36; nach anderer Ansicht finden die §§ 31 ff. UrhG dagegen keine Anwendung, s. *Hertin* in: Fromm/Nordemann (Hrsg.), §§ 85/86 Rdnr. 15.

[825] Zur konstitutiven Wirkung der Einräumung von Nutzungsrechten (sog. „gebundene Rechtsübertragung") s. *Schack*, Rdnr. 530.

[826] *Schack*, Rdnr. 541.

[827] BGH CR 2000, 651, 652; *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, §§ 31/32 Rdnr. 8; *Schack*, Rdnr. 541 ff.; *Schricker*, Verlagsrecht, § 28 Rdnr. 23.

[828] S. dazu unten Teil 4, B II.

[829] Dies ergibt sich schon aus § 40 Abs. 1 S. 1 und Abs. 3 UrhG; s. *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, vor §§ 28 ff. Rdnr. 58; *Lehmann* in: Beier/Götting/Lehmann/Moufang (Hrsg.), S. 543, 545 f.; *Wente/Härle*, GRUR 1997, 96. Umstritten ist hingegen, ob im Urheberrecht auch das Abstraktionsprinzip gilt, nach dem das Verfügungsgeschäft in seiner Gültigkeit grundsätzlich vom Bestand und der Gültigkeit des zugrundeliegenden Verpflichtungsgeschäfts unabhängig ist. Dies wird von der wohl herrschenden Meinung unter analoger Anwendung des § 9 Abs. 1 VerlG verneint, so von *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, vor §§ 28 ff. Rdnr. 62; *Schricker*, Verlagsrecht, § 9 Rdnr. 3; *Hertin* in: Fromm/Nordemann (Hrsg.), vor § 31 Rdnr. 10; *Wente/Härle*, GRUR 1997, 96, 97 ff. Bei der Übertragung bereits abgespaltener Nutzungsrechte soll jedoch das Abstraktionsprinzip wieder gelten, *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, vor §§ 28 ff. Rdnr. 62. S. zum ganzen auch *Schack*, Rdnr. 525 ff.

[830] Bei einfachen Nutzungsrechten, um die es im DRM-Umfeld meist geht, ist umstritten, ob sie quasi-dinglicher oder nur obligatorischer Natur sind. Nach herrschender Meinung haben auch einfache Nutzungsrechte gegenständlichen, quasi-dinglichen

des Nutzungsrechts auf schuldrechtlicher Ebene beliebig eingeschränkt werden.[831] Dabei können auch solche Einschränkungen und Modalitäten der Nutzung vereinbart werden, die auf der Ebene des Verpflichtungsgeschäfts nicht möglich wären.[832] Beispielsweise finden sich im Verlagsbereich schuldrechtliche Abreden über die Ausstattung der Werkexemplare, die Modalitäten des Vertriebs und den Ladenpreis – schuldrechtliche Vereinbarungen, die den Umfang des eingeräumten Nutzungsrechts auf der Ebene des Verfügungsgeschäfts nicht schmälern.[833]

Insgesamt zeigt sich, daß aus urheberrechtlicher Sicht keine *grundsätzlichen* Einwände gegen die Einräumung eng umrissener Nutzungsrechte in DRM-Nutzungsverträgen bestehen.

3. Wirksamkeit nach U.S.-amerikanischem Recht

a) Shrinkwrap Licenses

Auch im U.S.-amerikanischen Softwarerecht ist die Wirksamkeit von Schutzhüllenverträgen bei Computersoftware, den sogenannten „shrinkwrap licenses",[834] seit langem umstritten. Die tatsächliche Ausgestaltung von „shrinkwrap licenses" in den USA entspricht der tatsächlichen Ausgestaltung von Schutzhüllenverträgen in Deutschland. Es stellt sich wie

Charakter. Dies wird unter anderem mit § 33 UrhG begründet, s. *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, vor §§ 28 ff. Rdnr. 49; *Schack*, Rdnr. 540; *Rehbinder*, Rdnr. 306; *Schricker*, Verlagsrecht, § 28 Rdnr. 23; a. A. (schuldrechtlicher Charakter) *Hertin* in: Fromm/Nordemann (Hrsg.), §§ 31/32 Rdnr. 2; *Spautz* in: Möhring/Nicolini (Hrsg.), § 31 Rdnr. 39. Insgesamt hat der Streit keine große Bedeutung, da man sich darüber einig ist, daß einfache Nutzungsrechte keine Abwehrrechte gegenüber Dritten gewähren, *Spautz* in: Möhring/Nicolini (Hrsg.), § 31 Rdnr. 39; *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, vor §§ 28 ff. Rdnr. 49; *Schricker*, Verlagsrecht, § 28 Rdnr. 23. Zur Frage, ob der BGH in CR 2000, 651 – OEM-Version – einfache Nutzungsrechte faktisch als bloße obligatorische Rechte ansieht, s. *Chrocziel*, CR 2000, 738, 739.

[831] *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, vor §§ 28 ff. Rdnr. 57; §§ 31/32 Rdnr. 8; *Schack*, Rdnr. 544; *Bydlinski*, AcP 198 (1998), 287, 297; *Lehmann* in: Beier/Götting/Lehmann/Moufang (Hrsg.), S. 543, 560; BGH CR 2000, 651, 652, 653 – OEM-Version.

[832] *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, vor §§ 28 ff. Rdnr. 57 („Das Schuldrecht kann als Instrument zur Feinabstimmung der Interessen der Vertragspartner dienen"); s. a. BGH GRUR 1986, 736, 737 – Schallplattenvermietung; BGH CR 2000, 651, 653 – OEM-Version; *Hubmann*, Film und Recht 1984, 495 ff. Wenn man der Ansicht folgt, daß einfache Nutzungsrechte immer nur schuldrechtlichen Charakter haben, so stellt sich das Problem der Aufspaltbarkeit im Rahmen des § 32 UrhG gar nicht. Der schuldrechtliche Charakter des einfachen Nutzungsrechts würde beliebige Gestaltungsformen zulassen, *Hertin* in: Fromm/Nordemann (Hrsg.), §§ 31/32 Rdnr. 2; *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, vor §§ 28 ff. Rdnr. 49; unklar insoweit *Spautz* in: Möhring/Nicolini (Hrsg.), § 32 Rdnr. 1.

[833] BGH CR 2000, 651, 653 – OEM-Version; *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, vor §§ 28 ff. Rdnr. 57.

[834] Zur Entstehung des Begriffs s. *Contreras/Slade*, CRi 2000, 104, 105.

im deutschen Recht[835] die Frage, ob „shrinkwrap licenses" wirksame Verträge sind und ob, falls dies nicht der Fall sein sollte, die Gründe für ihre Unwirksamkeit auf Nutzungsverträge in DRM-Systemen übertragbar sind.

Herkömmlicherweise wurde von U.S.-amerikanischen Gerichten bei Schutzhüllenverträgen kein wirksamer Vertragsschluß angenommen.[836] In den letzten Jahren sind jedoch durch eine wegweisende Gerichtsentscheidung und ein umfassendes Gesetzgebungsprojekt deutliche Tendenzen erkennbar, daß schon herkömmliche „shrinkwrap licenses" zu einem gültigen Vertrag führen sollen. Damit bestünden unter diesen Gesichtspunkten gegen die Wirksamkeit von Nutzungsverträgen in DRM-Systemen nach U.S.-amerikanischem Recht noch weniger Bedenken als nach deutschem Recht. Sowohl die Gerichtsentscheidung als auch das Gesetzgebungsprojekt haben die Diskussion um DRM-Systeme in den USA maßgeblich beeinflußt. Auf sie wird im Verlauf der Untersuchung noch in mehreren Zusammenhängen zurückzukommen sein. Daher sollen beide Ereignisse im folgenden etwas ausführlicher dargestellt werden.

aa) ProCD, Inc. v. Zeidenberg

1997 entschied der 7th Circuit des U.S. Court of Appeals unter Judge *Easterbrook* in zweiter Instanz, daß bei Schutzhüllenverträgen ein wirksamer Vertragsschluß vorliege.[837] Die ProCD-Entscheidung war insofern revolutionär, als ein U.S.-Gericht zum ersten Mal eine „shrinkwrap licen-

[835] S. dazu oben Teil 2, B II 2 a.

[836] So beispielsweise in Step-Saver Data Systems, Inc. v. Wyse Technology, 939 F.2d 91, 104 ff. (3rd Cir. 1991); Arizona Retail Sys., Inc. v. Software Link, Inc., 831 F. Supp. 759, 762 ff. (D. Ariz. 1993); s. a. Novell, Inc. v. Network Trade Center, Inc., 25 F.Supp.2d 1218 (D.Utah 1997), *vacated in part by* Novell, Inc. v. Network Trade Center, Inc., 187 F.R.D. 657 (D.Utah 1999); Morgan Laboratories, Inc. v. Micro Data Base Systems, Inc., 41 U.S.P.Q.2d 1850 (N.D. Cal. 1997). S. zum ganzen *Madison*, 67 Fordham L. Rev. 1025, 1026 (1998) m. w. N.; *Bott*, 67 U. Cin. L. Rev. 237, 240 ff. (1998); *Monroe*, 1 Marq. Intell. Prop. L. Rev. 143 (1997); *Minassian*, 45 UCLA L. Rev. 569, 574 ff. (1997); *Lemley*, 68 S. Cal. L. Rev. 1239 (1995); *R. T. Nimmer,* § 11.12[2], S. 11–33 ff.; *Kochinke/Günther*, CR 1997, 129, 133 f. Die Entscheidung Vault Corp. v. Quaid Software Ltd., 847 F.2d 255 (5th Cir. 1988) verneint ebenfalls die Wirksamkeit einer „shrinkwrap license", jedoch aus einem anderen Grund: Der dortige Vertrag unterlag dem damaligen „Software License Enforcement Act" des Bundesstaates Louisiana, dessen einschlägige Vorschriften nach Ansicht des Gerichts jedoch gegen das bundesrechtliche Urheberrecht verstießen und damit unwirksam waren („federal preemption"), s. dort S. 269 f.; zur „preemption" allgemein s. unten Teil 4, B III 1 a.

[837] ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1450–1453 (7th Cir. 1996). In erster Instanz war dies noch mit einer ausführlichen Begründung verneint worden, ProCD, Inc. v. Zeidenberg, 908 F.Supp. 640, 650–656 (W.D.Wis. 1996). S. auch *Kochinke/Günther*, CR 1997, 129, 130 ff.; *Lejeune*, CR 2000, 265, 267; *Wang*, 15 J. Marshall J. Computer & Info. L. 439, 442 ff. (1997); *Contreras/Slade*, CRi 2000, 104, 106. Auf die Einzelheiten der Begründung wird im vorliegenden Rahmen nicht eingegangen.

se“ für wirksam erklärte.[838] Inzwischen sind andere Gerichte diesem Trend gefolgt.[839] In der Literatur wurden die Ausführungen zur vertraglichen Wirksamkeit von „shrinkwrap licenses“ mehrheitlich begrüßt.[840] Teilweise findet sich die pauschale Aussage, seit der ProCD-Entscheidung würden „shrinkwrap licenses“ wirksame Verträge darstellen.[841] In der Folge haben U.S.-amerikanische Gerichte auch „Enter“-Verträge[842] – in den USA „click-wrap licenses“ genannt – als wirksam anerkannt.[843]

bb) Uniform Computer Information Transactions Act (UCITA)

(1) **Allgemeines.** Der 1999 verabschiedete „Uniform Computer Information Transactions Act“ (UCITA) enthält neben vielen anderen Vorschriften, die für das Software- und Internetrecht relevant sind, auch Vorschriften zu „shrinkwrap licenses“. Das Modellgesetz[844] hat eine bewegte

---

[838] Neben der Frage der Wirksamkeit von „shrinkwrap licenses“ behandelt die ProCD-Entscheidung noch eine Reihe weiterer Fragen, die für DRM-Systeme von zentralem Interesse sind, u. a. Fragen der Preisdiskriminierung und des Verhältnisses zwischen „copyright law“ und „contract law“. Auf diese Fragen wird im weiteren Verlauf der Untersuchung noch eingegangen.

[839] So haben neben einer weiteren Entscheidung des 7th Circuits, Hill v. Gateway 2000, Inc., 105 F.3d 1147 (7th Cir. 1997), der Supreme Court des Staates Washington, M.A. Mortenson Co., Inc. v. Timberline Software Corp., 998 P.2d 305, 313 (2000), und die Appellate Division des Supreme Courts des Bundesstaates New York, Brower v. Gateway 2000, Inc., 676 N.Y.S.2d 569, 572 (N.Y.App.Div. 1998), die Wirksamkeit von „shrinkwrap licenses“ anerkannt. Bei diesen drei Entscheidungen bestand jedoch die Besonderheit, daß dem Käufer jeweils ein befristetes Rückgaberecht zustand, s. Hill v. Gateway 2000, Inc., 105 F.3d 1147, 1149 (7th Cir. 1997); M.A. Mortenson Co., Inc. v. Timberline Software Corp., 998 P.2d 305, 308 (2000); Brower v. Gateway 2000, Inc., 676 N.Y.S.2d 569, 572 (N.Y.App.Div. 1998). S. dazu auch *Lejeune*, CR 2000, 265, 268; zu weiteren Entscheidungen s. *R. T. Nimmer,* § 11.12[1], S. S11–31 ff., § 11.12.[2][b], S. S11–44ff.

[840] *Covotta/Sergeef*, 13 Berkeley Tech.L.J. 35, 41 (1998); *Grusd*, 10 Harvard J. L. & Tech. 353, 361 ff. (1997); *Baker*, 92 Nw. U. L. Rev. 379 (1997); *O'Rourke*, 12 Berkeley Tech. L. J. 53, 57 ff. (1997); *Garon*, 17 Cardozo Arts & Ent. L. J. 491, 549 f. (1999). Ablehnend *Mercer*, 30 Creighton L. Rev. 1287, 1345 (1997). Weitere Literaturhinweise finden sich bei *Lemley*, 87 Cal. L. Rev. 111, 120 Fn. 20 (1999); *Mercer*, a. a. O., S. 1345.

[841] Siehe *Mahajan*, 67 Fordham L. Rev. 3297, 3312 (1999); kritischer *Bott*, 67 U. Cin. L. Rev. 237, 244 (1998).

[842] Zum Begriff s. oben bei Fn. 806.

[843] Beispielsweise in Caspi v. Microsoft Network, 732 A.2d 528 (N.J.Super.A.D. 1999). Das bloße Anzeigen von Nutzungsbedingungen auf einer Web-Seite, ohne daß der Nutzer explizit seine Zustimmung erklärt, reicht nicht aus, Ticketmaster Corp v. Tickets.com, Inc., 2000 WL 525390, S. 3 (C.D.Cal., March 27, 2000) (auch erhältlich über *Bechtold*, The Link Controversy Page). S. dazu insgesamt *Contreras/Slade*, CRi 2000, 104, 106 f.; *R. T. Nimmer,* § 11.12[2], S. S11–38 ff.

[844] Anders als das Urheberrecht fällt das Vertragsrecht in den USA in die Kompetenz der einzelnen Bundesstaaten. Mangels einer umfassenden Bundesgesetzgebungskompetenz im Zivil- und Handelsrecht erfolgt die Rechtsvereinheitlichung in den USA vielfach durch „Uniform Laws“. Das bekannteste dieser Modellgesetze ist der „Uniform Commercial Code“ (UCC), dessen Änderungen von der „National Conference of Commis-

Entstehungsgeschichte hinter sich.[845] 1986 empfahl ein Ausschuß der „American Bar Association", ein einheitliches Gesetz für Software-Verträge zu schaffen.[846] Seit 1991 wurde überlegt, im Rahmen der Revision des Art. 2 UCC – des für Waren geltenden Handelsrechts – ein spezielles Vertragsrecht für immaterielle Güter im Informationszeitalter zu schaffen.[847] 1995 wurde entschieden, beide Projekte zu trennen und das hier interessierende Projekt als neuen Artikel 2B UCC zu entwerfen.[848] Schon bald zeigte sich, daß das „UCC 2B"-Projekt wegen seines Umfangs und seiner Wichtigkeit[849] zu dem seit Jahrzehnten umstrittensten Projekt im Rahmen der Revision des gesamten UCC werden sollte.[850]

Insbesondere die Vorschriften zu „shrinkwrap licenses" und zum Verhältnis zwischen Art. 2B UCC und dem Urheberrecht waren heftiger Kritik ausgesetzt.[851] Da das „American Law Institute" (ALI) den Entwurf nicht länger mittragen wollte,[852] entschied die verbleibende „National Conference of Commissioners for Uniform Laws" (NCCUSL) im Jahr 1999, das Projekt als eigenständiges Modellgesetz unter dem Titel „Uniform Computer Information Transactions Act" (UCITA) weiterzuverfolgen. Am 30. 7. 1999 wurde der UCITA von den Commissioners der einzelnen Bundesstaaten mit großer Mehrheit verabschiedet.[853] Bis zum

sioners for Uniform Laws" (NCCUSL, <http://www.nccusl.org>) und dem „American Law Institute" (ALI, <http://www.ali.org>) – einer Vereinigung von Professoren, Richtern und Anwälten, die insbesondere die „Restatements of Law" veröffentlicht – verabschiedet werden müssen. Modellgesetze werden von den Commissioners der einzelnen Bundesstaaten per Abstimmung angenommen und dann den Bundesstaaten zur Transformation in das jeweilige Landesrecht übergeben. Dabei können die Bundesstaaten grundsätzlich auch vom Modellgesetz abweichen. Zum allgemeinen Verfahren der UCC-Revisionen s. *Culhane*, 26 Creighton L. Rev. 29 (1992).

[845] Zur Entstehungsgeschichte des UCITA s. a. *Lejeune*, CR 2000, 201 f.; *ders.*, K&R 1999, 210 f.

[846] *Warlick*, 45 J. Copyright Soc'y U.S.A. 158, 161 (1997).

[847] *Nimmer/Cohn/Kirsch*, 19 Rutgers Computer & Tech. L.J. 281 (1993).

[848] *Warlick*, 45 J. Copyright Soc'y U.S.A. 158, 161 (1997); *Lejeune*, CR 2000, 201.

[849] *Towle*, 36 Hous. L. Rev. 121, 122 (1999), meint gar, der UCITA sei „the most important and intellectually impressive legislative proposal in current memory."

[850] *Lejeune*, CR 2000, 201 f. Eine Aufzählung kritischer Stimmen aus unterschiedlichen Bereichen findet sich bei *Shah*, 15 Berkeley Tech. L. J. 85, 87 (2000). Bis zum Februar 2001 wurden in U.S.-amerikanischen Law Reviews und Law Journals über 400 juristische Aufsätze zum UCITA veröffentlicht (Ergebnis einer Westlaw-Recherche des Verfassers im Februar 2001).

[851] So insbesondere im Rahmen der im April 1998 an der UC Berkeley Law School veranstalteten Konferenz zum Verhältnis zwischen Art. 2B UCC und dem „intellectual property", deren Beiträge in 13 (3) Berkeley Technology Law Journal (1998) und 87 (1) California Law Review (1999) abgedruckt sind. Weitere Aufsätze finden sich in 16 (2) John Marshall Journal of Computer and Information Law (1997).

[852] Dies ist Voraussetzung für eine Integration in den UCC, s. oben Fn. 844.

[853] S. *Lejeune*, CR 2000, 201, 202. Im Sommer 2000 hat die NCCUSL mehreren Änderungen des UCITA zugestimmt. Die aktuelle Fassung stammt vom 29. 9. 2000 und ist unter <http://www.law.upenn.edu/bll/ulc/ucita/ucitaFinal00.pdf> abrufbar. So-

August 2001 wurde das Modellgesetz in zwei Bundesstaaten in einzelstaatliches Recht umgesetzt.[854] Auch in seiner endgültigen Fassung ist das Modellgesetz noch äußerst umstritten.[855] Es wird mit einer zumindest schleppenden Umsetzung in den Bundesstaaten gerechnet.[856]

Vor Erlaß des UCITA wurden Verträge über Immaterialgüter und Informationen im weiteren Sinne oftmals unter die Regelungen des Art. 2 UCC subsumiert. Die Anwendung dieses auf materielle Güter zugeschnittenen Gesetzes konnte in vielen Fällen jedoch keine adäquate Lösung bieten.[857] Die umfangreichen Regelungen des UCITA – ein mit seinen offiziellen Anmerkungen immerhin über 340 Seiten langes Werk – wollen diesen Mißstand beseitigen. UCITA regelt eine Fülle von Fragen des Vertragsschlusses, der Vertragsauslegung, der Gewährleistung, der Übertragung vertraglicher Ansprüche, der Vertragserfüllung, der Leistungsstörung, des Verhältnisses zum Urheberrecht sowie von Rechtswahl- und Gerichtsstandsklauseln.[858] Es ist der weltweit erste Versuch, das Recht der Transaktion von Information umfassend zu kodifizieren.[859] Ein vergleichbar umfassendes und ambitioniertes Gesetzgebungsvorhaben existiert weder in Europa noch Japan.[860]

Das Modellgesetz findet auf „computer information transactions" Anwendung, § 103 (a) UCITA.[861] Nach der sehr weiten Definition in § 102

---

weit nichts Besonderes vermerkt ist, bezieht sich die vorliegende Arbeit immer auf diese Fassung vom 29. 9. 2000. Eine umfassende Sammlung von Informationen zum UCITA, einschließlich der verschiedenen Fassungen, findet sich auf der von *Carol A. Kunze* verwalteten Webseite <http://www.ucitaonline.com>. Informationen zum Enstehungsprozeß finden sich unter <http://www.2bguide.com>, ebenfalls von *Kunze*.

[854] In Maryland trat der UCITA mit Wirkung zum 1. 10. 2000, in Virginia mit Wirkung zum 1. 7. 2001 in Kraft; aktuelle Informationen finden sich unter <http://www.ucitaonline.com/whathap.html>. Zur Umsetzung in Virginia s. *Spooner*, 7 Rich.J.L. & Tech. 27 (Winter 2001).

[855] S. beispielsweise *Rudin*, 7 Rich. J.L. & Tech. 13 (Symposium 2000); *Heller*, 7 Rich. J.L. & Tech. 14 (Symposium 2000); *Shah*, 15 Berkeley Tech. L. J. 85, 104 ff. (2000).

[856] *Contreras/Slade*, CRi 2000, 104, 107.

[857] S. dazu *Lejeune*, CR 2000, 201, 202.

[858] Es ist im vorliegenden Rahmen unmöglich, einen vollständigen Überblick über die Regelungen des UCITA zu geben; s. dazu *Lejeune*, CR 2000, 201 ff.; *ders.*, CR 2000, 265 ff.; *Diedrich*, MMR 1998, 513, 514 ff.; *Dively/Ring*; *Shah*, 15 Berkeley Tech. L. J. 85 ff. (2000).

[859] *Samuelson*, 87 Cal. L. Rev. 1, 2 (1999), meint, UCITA solle für die Informationsgesellschaft das erreichen, was der UCC für die Industriegesellschaft erreicht habe.

[860] *O'Rourke*, 14 Berkeley Tech. L. J. 635, 645 (1999); *Kochinke/Günther*, CR 1997, 129, 137; *Lejeune*, K&R 1999, 210. Zur Lage in Japan s. *Matsumoto*, 13 Berkeley Tech. L. J. 1283 (1998).

[861] Der Anwendungsbereich des Gesetzes schwankte in seiner Entstehungsgeschichte stark. Während anfangs nur der Software-Bereich geregelt werden sollte (s. *Warlick*, 45 J. Copyright Soc'y U.S.A. 158 (1997)), wurde der Anwendungsbereich mit der Zeit auf die Lizenzierung von Information aller Art ausgeweitet. Dies rief den Protest insbesondere der Film-, Fernseh-, Tonträger- und Verlagsbranche hervor, die die Vision eines

(a) (11) UCITA sind darunter Verträge und deren Durchführung zu verstehen, bei denen es um die Schaffung, Änderung, Übertragung oder Lizenzierung von Information aller Art geht. Die Informationen müssen entweder in elektronischer Form vorliegen („computer information", s. § 102 (a) (10) UCITA), oder es muß sich um Rechte an Information handeln, die dem Patent-, Urheber-, Geschäftsgeheimnis- oder Markenschutz unterliegen („informational rights", s. § 102 (a) (37) UCITA). In den Anwendungsbereich des UCITA fallen beispielsweise Verträge, die den Zugang zu Information gewähren („access contracts", s. § 102 (a) (1) UCITA), Verträge zum Vertrieb digitaler Inhalte, Softwareentwicklungsverträge, Supportverträge, Verträge zur Entwicklung von Multimediawerken usw.[862] Damit kann eine Vielzahl der Verträge, durch die in DRM-Systemen Nutzungsrechte an digitalen Inhalten eingeräumt werden sollen, dem UCITA unterfallen.[863]

(2) **Vorschriften zu Mass-Market Licenses.** Der UCITA enthält spezielle Vorschriften zur Wirksamkeit von „shrinkwrap licenses" und „click-wrap licenses".[864] Beide fallen unter den Begriff der „mass-market license",

---

einheitliches Lizenzierungsrecht angesichts der Unterschiedlichkeit der Branchen für utopisch hielt (so ein gemeinsames Schreiben führender amerikanischer Industrieverbände dieser Branchen vom 10. 9. 1998, erhältlich unter <http://www.2bguide.com/docs/v9–98.pdf>; s. a. *O'Rourke*, 14 Berkeley Tech. L. J. 635, 648 (1999); *Lejeune*, CR 2000, 201, 203). Diese Kritik führte zu einer starken Beschränkung des Anwendungsbereichs. Daneben hängt das Schwanken des Anwendungsbereichs mit der technischen Entwicklung zusammen, die bestimmte Vorstellungen obsolet werden ließen, welche der Reform in den frühen 90er Jahren zugrunde lagen, s. *Dodd*, 36 Hous. L. Rev. 195, 203 Fn. 15 (1999); *Gomulkiewicz*, 12 Berkeley Tech. L. J. 891, 894 (1998). S. dazu auch *R. T. Nimmer*, 36 Hous. L. Rev. 1, 3 (1999). Auch heute wird teilweise kritisiert, daß man dem UCITA immer noch anmerke, daß er ursprünglich Software-Lizenzverträge regeln wollte und sein Anwendungsbereich später erweitert wurde, *Rudin*, 7 Rich. J.L. & Tech. 13, Abs. 4 (Symposium 2000); s. a. *Diedrich*, MMR 1998, 513, 518.

[862] Nicht erfaßt werden die traditionellen, nicht digitalen Bereiche, s. *Lejeune*, CR 2000, 201, 203.

[863] Zwar besteht eine Ausnahmebestimmung, nach der Verträge über (u. a.) Schaffung, Erwerb, Nutzung, Bearbeitung, Zugangsgewährung, Übertragung und Lizenzierung von Rechten im Film- und Fernsehsektor sowie hinsichtlich Tonaufnahmen vom UCITA nicht erfaßt werden, § 103 (d) (3) UCITA; kritisch dazu *Dodd*, 36 Hous. L. Rev. 195, 203 Fn. 15 (1999). Die herkömmlichen Rechtsbeziehungen zwischen Produzenten, Schauspielern, Regisseuren, Drehbuchautoren u. ä. sollten durch den UCITA nicht berührt werden. Die Ausnahme gilt im Film- und Fernsehsektor jedoch nicht, wenn es sich um Transaktionen im Massengeschäft handelt, § 103 (d) (3) (A) (i) UCITA. Auch fallen Multimediawerke, bei denen audiovisuelle Komponenten nur einen Teil des Gesamtwerks darstellen, gar nicht unter die Ausnahme, s. den „Official Comment" No. 5 (c) zu § 103 UCITA, *UCITA*, S. 56. Weiterhin ist zu beachten, daß die Parteien eines Vertrags, der von sich aus nicht unter den Anwendungsbereich des UCITA fällt, vereinbaren können, daß die Regelungen des UCITA gelten sollen, § 104 UCITA („opt-in").

[864] Zum Begriff der „click-wrap license" s. oben bei Fn. 843.

s. § 102 (a) (44) UCITA. „Mass-market licenses" sind standardisierte Vertragsbedingungen für Verträge mit Verbrauchern sowie für bestimmte Verträge mit gewerblichen Kunden, § 102 (a) (45) UCITA.[865] Nach den Regelungen des UCITA sind solche Verträge in weitem Umfang wirksam. So wird ausdrücklich geregelt, daß die Vertragsbedingungen bei „mass-market licenses" dem Vertragspartner nicht schon beim ursprünglichen Vertragsschluß zur Verfügung gestellt werden müssen. Vielmehr genügt es, wenn sie ihm zu dem Zeitpunkt zugänglich gemacht werden, zu dem dieser die Informationen zum ersten Mal nutzt. Für die wirksame Einbeziehung solcher Vertragsbedingungen reicht eine konkludente Zustimmung des Vertragspartners aus, die schon in der bloßen Nutzung der Information liegen kann, § 209 (a) UCITA.[866] Falls der Vertragspartner mit den Vertragsbedingungen nicht einverstanden ist, steht ihm nach § 209 (b) UCITA lediglich ein Rückgaberecht zu.

Durch diese – sehr umstrittenen[867] – Regelungen wird die Wirksamkeit einer Vielzahl von Schutzhüllenverträgen gesetzlich festgeschrieben.[868] Auch „click-wrap licenses" sind nach dem UCITA in sehr weitem Umfang wirksam.[869]

cc) Zwischenergebnis

In den letzten Jahren läßt sich in der U.S.-amerikanischen Rechtsprechung und Gesetzgebung die deutliche Tendenz erkennen, daß herkömmliche „shrinkwrap licenses" in weitem Umfang als wirksame Verträge angesehen werden . Die oben dargestellten Bedenken gegen die Wirksamkeit solcher Verträge[870] spielen im U.S.-amerikanischen Recht eine immer geringere Rolle. Schon aus diesem Grund sind im U.S.-amerikanischen

[865] Näher dazu der „Official Comment" Nr. 39 zu § 102, UCITA, S. 34 f.

[866] S. § 112 (a) (2) UCITA und der „Official Comment" Nr. 3 b zu § 112 , *UCITA*, S. 86. *Dodd*, 36 Hous. L. Rev. 195, 209 (1999), bringt es auf den Punkt: UCITA „frees assent from time". Außerhalb von „Mass-market licenses" können unter gewissen Voraussetzungen (auch standardisierte) Vertragsbedingungen selbst nach Beginn der ersten Nutzung ohne zeitliche Begrenzung eingeführt werden (sog. „layered contracting"); für die wirksame Annahme genügt auch hier konkludentes Verhalten, s. § 208 (1), (2) UCITA; s. dazu *Lejeune*, CR 2000, 265, 268. Die Beschränkungen des § 209 UCITA bei „Mass-market licenses" gegenüber dem allgemeineren § 208 UCITA sind nicht vertraglich abdingbar, § 113 (a) (3) (E) UCITA.

[867] S. dazu *Lejeune*, CR 2000, 265, 267 f.; *Rudin*, 7 Rich. J.L. & Tech. 13, Abs. 6 f. (Symposium 2000).

[868] Dies begrüßt *Lejeune*, CR 2000, 265, 272, mit dem Hinweis, daß sich das auf Schutzhüllenverträgen aufbauende Vertriebsmodell inzwischen weltweit durchgesetzt habe und auch die Juristen die Realitäten des Wirtschaftslebens zur Kenntnis nehmen müßten. Einen Überblick über die ganze Entwicklung gibt *Wang*, 15 J. Marshall J. Computer & Info. L. 439 (1997).

[869] S. dazu *Contreras/Slade*, CRi 2000, 104, 107 f.

[870] S. oben Teil 2, B II 2 a.

Recht die Einwände gegen „shrinkwrap licenses“ nicht auf die Ausgestaltung von Nutzungsverträgen in DRM-Systemen übertragbar.[871]

b) Wirksamer Vertragsschluß im Internet

Nutzungsverträge, die in DRM-Systemen über das Internet abgeschlossen werden, müssen bei Anwendbarkeit des U.S.-amerikanischen Rechts nach diesem Recht wirksam sein.[872] Auch nach U.S.-amerikanischem Recht können Verträge wirksam über das Internet abgeschlossen werden.[873] Der UCITA enthält umfangreiche Vorschriften zum Vertragsangebot, zur Annahme und sonstigen Fragen der Wirksamkeit von Verträgen, die online abgeschlossen wurden.[874] So wird die Einbeziehung allgemeiner Geschäftsbedingungen bei Internet-Transaktionen geregelt, § 211 UCITA.[875] Auch der Einsatz von Software-Agenten ist möglich:[876] Verwendet eine Person einen Software-Agenten zum Vertragsschluß oder zur durchführung, so ist sie an die Handlungen des Software-Agenten rechtlich gebunden, auch wenn die einzelnen Handlungen des Agenten von ihr nicht überwacht wurden, § 107 (d) UCITA.[877] Ein Vertrag kann wirksam zwischen zwei Software-Agenten ohne irgendwelche menschlichen Eingriffe geschlossen werden, §§ 202 (a), 206 UCITA.

Auch nach U.S.-amerikanischem Rechts steht der Wirksamkeit online abgeschlossener Nutzungsverträge in DRM-Systemen und der Vision ei-

---

[871] Ebenso *Bell*, 76 N. C. L. Rev. 557, 605 f. (1998). *R. T. Nimmer,* § 11.12[2][a], S. S11–40 schreibt.: „The enforceability in general of on-screen licenses is not seriously in doubt“. S. weiterhin *Lemley*, 35 Jurimetrics J. 311, 318 f. (1995); *Towle*, 36 Hous. L. Rev. 121, 171 Fn. 128 (1999); *Contreras/Slade*, CRi 2000, 104, 105, 108; *Lejeune*, CR 2000, 265, 267. Zu allgemeinen Gründen, daß beide Konstellationen nicht vollständig vergleichbar sind, s. oben bei Fn. 809 ff.

[872] S. dazu allgemein oben Teil 2, B II 2 b.

[873] Einen Überblick über die relevanten Regelungen (Electronic Signatures in Global and National Commerce Act, Uniform Electronic Transactions Act, Uniform Computer Information Transactions Act) gibt *R. T. Nimmer*, CRi 2000, 97 ff.; vgl. weiterhin *Thot*, S. 7 ff., 32 ff., 37 ff.; *Wildemann*, CRi 2000, 109 ff. Umfassend *R. T. Nimmer,* § 12.09 ff., S. 12–34 ff. mit Supplement.

[874] S. dazu im Überblick *Wildemann*, CRi 2000, 109 ff.; *Lejeune*, CR 2000, 265 ff.

[875] S. dazu *Lejeune*, CR 2000, 265, 266.

[876] Der Begriff des „electronic agents“, der vom UCITA verwendet wird, umfaßt nicht nur Software-Agenten, s. die Definition in § 102 (a) (27) UCITA und der „Official Comments“ Nr. 27 zu § 102, *UCITA*, S. 30. Kritisch zu diesen Regelungen *Lerouge*, 18 J. Marshall J. Computer & Info. L. 403, 418 ff. (1999); s. weiterhin *Lejeune*, CR 2000, 265 f.; *Middlebrook/Muller*, 56 Bus. Law. 341, 352 ff. (2000). Zu Regelungen über Software-Agenten in anderen U.S.-amerikanischen Gesetzen s. *Poggi*, 41 Va. J. Int'l L. 224, 264 (2000); *Middlebrook/Muller*, a. a. O., S. 348 ff.; *Sommer*, 15 Berkeley Tech. L. J. 1145, 1177 ff. (2000). Zu rechtlichen Problemen von Software-Agenten allgemein s. *Lerouge*, a. a. O., S. 403 ff.; *Radin*, 75 Ind. L. J. 1125 (2000); *Allen/Widdison*, 9 Harv. J. L. & Tech. 25 (1996). Zu Software-Agenten in technischer Hinsicht s. oben Teil 1, E III.

[877] S. weiterhin § 213 UCITA.

nes „agent-mediated electronic commerce“ damit nichts Grundsätzliches entgegen.

c) Einräumung beschränkter Nutzungsrechte

Für einen wirksamen vertraglichen Schutz in DRM-Systemen müßte es nach U.S.-amerikanischem Recht möglich sein, die Einräumung von Nutzungsrechten vertraglich in inhaltlicher, persönlicher oder räumlicher Sicht zu beschränken.[878] Nach 17 U.S.C. § 201 (d) (2) ist die Einräumung ausschließlicher Lizenzen an urheberrechtlichen Verwertungsrechten möglich.[879] Daneben ist die Erteilung einfacher Lizenzen möglich.[880] Die Verwertungsrechte können grundsätzlich beliebig aufgespalten und in ihren Bestandteilen getrennt übertragen werden, s. 17 U.S.C. § 201 (d) (2). Dadurch sind Beschränkungen der Lizenz in inhaltlicher, zeitlicher oder räumlicher Art möglich.[881] Auch aus Sicht des U.S.-amerikanischen Urheberrechts bestehen damit keine grundsätzlichen Einwände gegen die Einräumung eng umrissener Nutzungsrechte in DRM-Nutzungsverträgen.[882]

III. Zusammenfassung

Inhalteanbieter versuchen in DRM-Systemen, ihre Interessen durch eine vertragliche Bindung der einzelnen Nutzer zu schützen. Solche Nutzungsverträge können in weitem Umfang wirksam sein. Die Bedenken, die gegen Schutzhüllenverträge vorgebracht werden, sind auf Nutzungsverträge in DRM-Systemen nicht ohne weiteres übertragbar. Im U.S.-amerikanischen Recht ist zusätzlich zu beachten, daß in letzter Zeit schon Schutzhüllenverträge als wirksam angesehen werden. Auch der Vertragsschluß über das Internet und der Einsatz von Software-Agenten steht der Wirksamkeit von Nutzungsverträgen in DRM-Systemen nicht entgegen. Gleiches gilt grundsätzlich bezüglich der Einräumung eng umrissener Nutzungsrechte.

In den USA läßt sich die Tendenz erkennen, daß immaterielle Güter (Software, digitale Inhalte) zunehmend nicht mehr wie körperliche Gegenstände an einen Käufer veräußert werden, sondern daß die Nutzer nur noch durch einen Lizenzvertrag zur Nutzung der immateriellen Güter

---

[878] S. dazu allgemein oben Teil 2, B II 2 c.

[879] Die ausschließliche Lizenz wird als eine Unterart der Übertragung des Urheberrechts angesehen (s. 17 U.S.C. § 101 (Transfer of copyright ownership)), der Inhaber einer ausschließlichen Lizenz dem Urheberrechtsinhaber gleichgestellt; s. dazu *Goldstein*, Copyright, § 4.4.1.1, S. 4:50–2 f.; *Bodewig* in: Beier/Götting/Lehmann/Moufang (Hrsg.), S. 833, 848.

[880] S. *Goldstein*, Copyright, § 4.4.1.1, S. 4:50–2 f.

[881] S. *Nimmer/Brown/Frischling*, 87 Cal. L. Rev. 17, 52 (1999); *Bodewig* in: Beier/Götting/Lehmann/Moufang (Hrsg.), S. 833, 851.

[882] Beschränkungen der Vertragsfreiheit können sich jedoch aus der sogenannten „preemption doctrine“ ergeben. Darauf wird weiter unten eingegangen, s. Teil 4, B III 1.

berechtigt werden.[883] Besonders forciert wird diese Tendenz in den USA mit der Einführung des UCITA; während früher Gerichte versuchten, auf Softwareüberlassungsverträge und ähnliches das für normale Güter geltende Recht, den Art. 2 UCC, analog anzuwenden, behandelt der UCITA Verträge über digitale Inhalte explizit als „Lizenzverträge".[884]

C. Schutz durch Technologie-Lizenzverträge

I. Allgemeines

Viele technische Komponenten von DRM-Systemen sind durch Patente geschützt. Daneben hüten DRM-Entwickler zahlreiche Komponenten als Geschäftsgeheimnis. So werden bei Verschlüsselungssystemen die verwendeten Schlüssel nicht veröffentlicht, sondern als Geschäftsgeheimnis geheim gehalten, da ansonsten das Verschlüsselungssystem nicht mehr sicher wäre.[885]

---

[883] S. zu dieser Tendenz *Nimmer/Brown/Frischling*, 87 Cal. L. Rev. 17, 34 ff. (1999); ausführlich *Rice*, 22 U. Dayton L. Rev. 622 ff. (1997). Zwar haben U.S.-amerikanische Gerichte vor allem aufgrund von Rechtsfolgeüberlegungen den Softwarekauf grundsätzlich als Warenkaufverträge („sale of goods") nach Art. 2–105, 106 UCC und nicht als bloße Lizenzierung eingeordnet, s. *Warlick*, 45 J. Copyright Soc'y U.S.A. 158, 160 (1997) m. w. N.; *Lejeune*, K&R 1999, 210, 211 m. w. N.; guter Überblick bei *Lemley*, 87 Cal. L. Rev. 111, 118 Fn. 15 (1999). Aber die U.S.-amerikanische Praxis hat längst das Zeitalter der Warenkaufverträge hinter sich gelassen und lizenziert die Benutzung der Software, *Diedrich*, MMR 1998, 513. Weiterhin behandelt der UCITA Verträge über digitale Inhalte explizit als „Lizenzverträge", s. § 102 (a) (41) UCITA. Im amerikanischen Recht forcierten Softwareunternehmen den Trend zur Lizenzierung, da bei einer Einordnung als Kaufvertrag der Erschöpfungsgrundsatz nach 17 U.S.C. § 109 (a) eingreift, was bei einer Einordnung als Lizenzvertrag nicht der Fall ist: Nach 17 U.S.C. § 109 (a) kommt nur der „*owner* of a particular copy" in den Genuß der „first-sale doctrine". S. zum ganzen *Rudin*, 7 Rich. J.L. & Tech. 13, Abs. 18 (Symposium 2000); *Nimmer/Brown/Frischling*, 87 Cal. L. Rev. 17, 34 ff. (1999); *Reichman/Franklin*, 147 U. Penn. L. Rev. 875, 904 (1999); *Lemley*, a. a. O., S. 119; *Rice*, 22 U. Dayton L. Rev. 622, 625, 643 ff. (1997); *R. T. Nimmer,* § 11.04 f. Ein Beispiel für eine Entscheidung, bei dem die Abgrenzung zwischen „sale" und „licensing" relevant wird, ist Novell, Inc. v. Network Trade Center, Inc., 25 F. Supp. 2d 1218 (D. Utah 1997) m. Anm. *Mahajan*, 67 Fordham L. Rev. 3297, 3322 (1999).

[884] § 102 (a) (41) UCITA definiert „license" als „contract that authorizes access to, or use, distribution, performance, modification, or reproduction of, information or informational rights, but expressly limits the access or uses authorized or expressly grants fewer than all rights in the information, whether or not the transfereee has title to a licensed copy. […]". Nach § 102 (b) (11) UCITA i. V. m. § 2–106 (1) UCC ist ein „sale" „the passing of title from the seller to the buyer for a price", s. a. den „Official Comment" Nr. 37 zu § 102 UCITA, *UCITA*, S. 33.

[885] Zwar sind Dechiffrier-Schlüssel bei DRM-Systemen oft in Endgeräten oder auf Speichermedien enthalten. Auch in diesem Fall können sie aber als Geschäftsgeheimnis gehütet werden: Die Schlüssel werden ihrerseits kryptographisch oder durch manipulationssichere Systemumgebungen geschützt und sind für einen Angreifer idealiter nicht

Wollen die Hersteller von Unterhaltungselektronik, Computern und Speichermedien DRM-Komponenten in ihre Endgeräte einbauen oder wollen Inhalteanbieter ihre digitalen Inhalte mit DRM-Komponenten schützen, müssen sie von dem Hersteller der DRM-Komponenten eine Patent- oder Know-how-Lizenz[886] erwerben.[887] Durch den Abschluß ei-

auslesbar, auch wenn dieser im Besitz eines Endgeräts ist. Gelingt es einem Angreifer dennoch, den geheimen Schlüssel auszulesen und verbreitet er diesen über das Internet, so beseitigt dies noch nicht den Geheimnisschutz, sofern der Know-How-Inhaber unverzüglich gegen die Verbreitung vorgeht. Ansonsten könnte der Dritte Ansprüche des Know-How-Inhabers (z. B. §§ 17 f. UWG) dadurch vereiteln, daß der das geheime Know-How möglichst schnell über das Internet zu verbreiten; s. dazu DVD Copy Control Ass'n, Inc. v. McLaughlin, 2000 WL 48512, S. 3 (Cal. Super. Jan. 21, 2000), auch erhältlich unter <http://www.eff.org/pub/Intellectual_property/DVDCCA_case/20000120-pi-order.html>.

[886] Zum Begriff des Geschäftsgeheimnisses und des „Know-hows" s. *Altin-Sieber*, S. 57 ff.; allgemein zur Know-how-Lizenz im deutschen Recht s. *Martinek*, Moderne Vertragstypen Band II, S. 203 ff.; *Altin-Sieber*, S. 114 ff.; zum Schutz des Geschäftsgeheimnisses im U.S.-amerikanischen Recht s. im Überblick *Elsing/Van Alstine*, Rdnr. 790 ff.

[887] Mitunter bündeln mehrere Unternehmen, die DRM-Komponenten entwickelt haben, ihre Technologien auch zur gemeinschaftlichen Lizenzierung. Dafür wird oftmals eine separate Lizenzierungsorganisation errichtet, so die „DVD Copy Control Association, Inc." (<http://www.dvdcca.org/dvdcca>) für CSS, der „Digital Transmission Licensing Administrator" (<http://www.dtcp.com>) für DTCP, die „4C Entity, LLC" (<http://www.4centity.com>) für CPRM, CPPM und das SDMI-Phase-I-Wasserzeichen und „Digital Content Protection, LLC" (<http://www.digital-cp.com>) für HDCP. Hinter den ersten drei genannten Organisationen verbirgt sich „License Management International, LLC" (<http://www.lmicp.com>). Von dieser gemeinsamen Lizenzierung von DRM-Komponenten sind Patentpools zu unterscheiden, die bestimmte Speicher- oder Kompressionstechnologien betreffen. So berührt der DVD-Standard etwa 4000 Patente, von denen Matsushita ca. 25%, Pioneer und Sony jeweils etwa 20%, Philips, Hitachi und Toshiba jeweils 10% und Thomson etwa 5% halten, s. *Taylor*, DVD Demystified, S. 51. Um die Lizenzierung der DVD-Technologie zu erleichtern, gründeten Hitachi, Matsushita, Mitsubishi, Time Warner, Toshiba und JVC 1999 einen Patentpool zur gemeinsamen Erteilung von Schlüsselpatent-Lizenzen im DVD-Bereich. Dieser Patentpool wurde im Mai 1999 bei der EG-Kommission angemeldet und von dieser in einem „comfort letter" im Oktober 2000 i. S. d. Art. 81 Abs. 3 EGV positiv beurteilt, s. *Europäische Kommission*, ABl. EG Nr. C 242 vom 27. 8. 1999, S. 5 f., und die Pressemitteilung IP/00/1135 der Kommission vom 9. 10. 2000, erhältlich über die RAPID-Datenbank, <http://europa.eu.int/rapid/start>. In den USA beurteilte das Department of Justice im Dezember 1998 im Rahmen der sog. „business review procedure" (28 C.F.R. § 50.6, s. dazu *Elsing/Van Alstine*, Rdnr. 911) einen Patentpool mit DVD-bezogenen Schlüsselpatenten von Philips, Sony und Pioneer positiv, s. *Klein*, Business Review Letter to G. R. Beeney on DVD patent pool, 1998 WL 931772 (D.O.J.), ebenso im Juni 1999 einen zweiten Patentpool mit DVD-bezogenen Schlüsselpatenten von Hitachi, Matsushita, Mitsubishi, Time Warner, Toshiba und JVC, s. *Klein*, Business Review Letter to C. R. Ramos on DVD patent pool, 1999 WL 392163 (D.O.J.). Einen ähnlichen Patentpool im Bereich von MPEG-2 hatte das Department of Justice schon 1997 positiv beurteilt, s. *Klein*, Business Review Letter to G. R. Beeney on MPEG LA patent pool, 1997 WL 356954 (D.O.J.). Die erwähnten DVD-Patentpools lizenzieren jedoch nur die dem DVD-Standard zugrundeliegenden Patente, nicht aber Patente im

nes solchen Technologie-Lizenzvertrags erhält der Lizenznehmer einerseits das Recht, die entsprechende Technologie in seinen Produkten zu verwenden. Andererseits werden ihm eventuelle Geschäftsgeheimnisse offengelegt, beispielsweise die Dechiffrier-Schlüssel mitgeteilt, die der Hersteller in einen DVD-Spieler integrieren muß, damit dieser verschlüsselte Inhalte abspielen kann.[888]

Darüber hinaus finden sich in DRM-Technologie-Lizenzverträgen vielfältige Klauseln, die mittelbar dem Schutz der Inhalteanbieter dienen. Dabei ist zu beachten, daß Inhalteanbieter – hier insbesondere Filmstudios und Tonträgerunternehmen – ihre Inhalte in digitaler Form nur für den Massenmarkt veröffentlichen wollen, wenn die Inhalte durch ein DRM-System mit hohem Sicherheitsniveau geschützt sind. Dadurch wollen Inhalteanbieter Raubkopien verhindern. Inhalteanbieter haben ein starkes Interesse daran, daß DRM-Systeme sicher ausgestaltet sind. In Verhandlungen mit den Entwicklern von DRM-Technologien haben Inhalteanbieter immer wieder klar gemacht, daß sie ihre Inhalte nur in einem DRM-System mit akzeptablem Sicherheitsniveau veröffentlichen werden.[889] Die Entwickler von DRM-Technologien haben ihrerseits ein starkes Interesse daran, daß die Hersteller von Unterhaltungselektronik, Computern und ähnlichem die DRM-Komponenten auf sichere Weise in ihre Endgeräte integrieren. Ansonsten würden die Inhalteanbieter ihre digitalen Inhalte nicht in Formaten veröffentlichen, die von solchen – unsicheren – Endgeräten gelesen werden könnten. Mangels verfügbarer Inhalte könnten sich diese Endgeräte am Markt nicht durchsetzen. Damit könnte sich aber auch die eingesetzte DRM-Technologie des Entwicklers nicht durchsetzen.

Aus diesem Grund verpflichten die Entwickler von DRM-Technologien in Technologie-Lizenzverträgen die Lizenznehmer regelmäßig, daß in den von den Lizenznehmern hergestellten Endgeräten bestimmte Schutzniveaus und Sicherheitsstandards eingehalten werden müssen. Der Entwickler einer DRM-Technologie lizenziert die Technologie an die Hersteller von Unterhaltungselektronikgeräten, Computern und Speichermedien nur, wenn diese auch bestimmte Klauseln über den Schutz digitaler Inhalte beachten. Solche Klauseln dienen mittelbar dem Interesse der Inhalteanbieter.[890]

DRM-Bereich. Technische Schutzmaßnahmen sind nicht Bestandteil des DVD-Standards im engeren Sinne, s. unten Fn. 897.

[888] Dies ist u. a. bei den CSS-, CPRM/CPPM-, HDCP- und DTCP-Lizenzen der Fall, die den Lizenznehmer berechtigten, die notwendigen Chiffrier- und Dechiffrier-Schlüssel zu erhalten.

[889] Vereinbarungen zwischen unterschiedlichen Unternehmen oder Branchen zum Schutz von Urheberrechten sind schon länger bekannt. Zum „Recorder Identification Code“ und dem „Source Identification Code“ s. oben bei Fn. 339 f.

[890] Ebenso *Federal Communications Commission*, 15 FCC Rcd. 18,199 (September 18, 2000), Abs. 27.

Diese Zusammenhänge und die außerordentliche Breite der Regelungen in solchen DRM-Technologielizenzen wurden in der wissenschaftlichen Diskussion bisher fast überhaupt nicht beachtet.[891] Jedoch hat sich die U.S.-amerikanische Federal Communications Commission inzwischen mit den Bedingungen eines solchen Lizenzvertrags im Pay-TV-Bereich beschäftigt.[892] Eine Untersuchung wird dadurch erschwert, daß viele der verwendeten Lizenzverträge nicht öffentlich bekannt sind.[893] Im folgenden sollen typische Klauseln vorgestellt werden, die in einer Vielzahl von DRM-Technologie-Lizenzverträgen wiederkehren. Dabei wird auf jene Technologie-Lizenzverträge zurückgegriffen, die – teilweise online, teilweise offline – öffentlich zugänglich sind (dazu unten II). Dabei stellt sich die Frage, ob solche Klauseln unter kartellrechtlichen Aspekten wirksam sind (dazu unten III).

II. Einzelne Vertragsklauseln

1. Ausgewertete Technologie-Lizenzverträge

Für die folgende Untersuchung wurden mehrere Lizenzverträge von DRM-Komponenten und Systemen ausgewertet, die heute am Markt verfügbar sind.

Video-DVDs verfügen über mehrere Schutzmaßnahmen, von denen das „Content Scramble System" (CSS) das Bekannteste ist.[894] Die technischen Einzelheiten von CSS sind als Geschäftsgeheimnis geschützt.[895] Um CSS

[891] Die einzigen rechtswissenschaftlichen Ausführungen stammen von *Marks/Turnbull*, EIPR 2000, 198, 206 f., die – naturgemäß recht unkritisch, da durch Unternehmensjuristen von Time Warner und Matsushita verfaßt – solche Lizenzen im DVD-Bereich darstellen.

[892] Zu dem „POD Host Interface License Agreement" s. unten Teil 2, C II 1. Die *Federal Communications Commission*, 15 FCC Rcd. 18,199 (September 18, 2000) schreibt in Absatz 15: „Through the use of contractual licensing requiring consumer electronic manufacturers to install certain copy protection technology in their equipment in exchange for access to desirable digital content, copyright holders will be able to control, through the insertion of coded instructions in the digital stream, whether such equipment will allow consumers to make one copy, unlimited copies, or prohibit copying altogether of digital content received from an MVPD [multichannel video programming distributor, z. B. ein Kabelnetzbetreiber]. It is the first generation of this licensing and technology and its relation to the Commission's navigation device rules that we address here." In ihrem „declaratory ruling" hat sich die FCC jedoch nur zu einer speziellen Auslegungsfrage ihres eigenen früheren „navigation devices order" geäußert und keine allgemeine Aussage zur Zulässigkeit solcher Lizenzvertragsklauseln gemacht, s. *Federal Communications Commission*, 15 FCC Rcd. 18,199 (September 18, 2000), Abs. 25 ff.

[893] Dazu kritisch *Gilmore*, c't 4/2001, S. 64 f.

[894] Zu den technischen Grundlagen von CSS und den anderen Schutzmaßnahmen s. oben Teil 1, D II 3.

[895] DVD Copy Control Ass'n, Inc. v. McLaughlin, 2000 WL 48512, S. 1 (Cal. Super. Jan. 21, 2000), auch erhältlich unter <http://www.eff.org/pub/Intellectual_property/DVDCCA_case/20000120-pi-order.html>; s. weiterhin *Bobrow*, S. 6, 12 f.

verwenden zu können, müssen die Hersteller von DVD-Geräten, DVDs und ähnlichem eine CSS-Lizenz erwerben. Diese wird – außer einer Verwaltungsgebühr von $ 15.000 pro Jahr ohne weitere Kosten – von der zu diesem Zweck gegründeten „DVD Copy Control Association, Inc." (DVD CCA) in Kalifornien vergeben.[896] Zwar sind die Hersteller von DVD-Geräten und DVDs nicht verpflichtet, CSS einzusetzen.[897] Da die Filmstudios ihre Filme nur zur Veröffentlichung auf DVDs freigeben, wenn diese mit CSS geschützt sind,[898] besteht für die Hersteller von DVD-Geräten ein faktischer Zwang, CSS zu benutzen.

Das Schutzsystem HDCP[899] ist bei digital angesteuerten Bildschirmen einsetzbar. Diese Bildschirme arbeiten nach der „Digital Visual Interface (DVI)"-Spezifikation. Zwar fordert weder die DVI-Spezifikation noch die dazugehörige Lizenz, daß die Hersteller digital angesteuerter Bildschirme das Schutzsystem HDCP einsetzen.[900] Wie bei DVD-Video und anderen Systemen kann jedoch für die Hersteller ein faktischer Zwang entstehen, HDCP zu benutzen, wenn die Inhalteanbieter ihre Inhalte nur in einer HDCP-kompatiblen Verschlüsselung verbreiten.

---

[896] Die Einzelheiten der CSS-Lizenz wurden ursprünglich von Matsushita entwickelt, nachdem sich die Film-, Computer- und Unterhaltungselektronikindustrie in der CPTWG über deren grundsätzliches Aussehen geeinigt hatte, s. *Marks/Turnbull*, EIPR 2000, 198, 206. Während die Technologie ursprünglich von Matsushita Electric Industrial Co. und Toshiba, den Entwicklern von CSS, direkt lizenziert wurde, übertrugen beide Unternehmen Ende 1999 diese Lizenzierungsfunktion der Ende 1998 gegründeten DVD CCA, s. *Bobrow*, S. 8; Universal City Studios, Inc. v. Reimerdes, 111 F.Supp.2d 294, 310 Fn. 60 (S.D.N.Y. 2000). Heute sind über 200 Unternehmen Mitglied der DVD CCA, eine Auflistung der Mitglieder findet sich in *U.S. Department of Justice, Antitrust Division*, 66 Fed. Rev. 40727 ff. (August 3, 2001). Für die Herstellung von DVD-Produkten ist neben einer CSS-Lizenz noch eine Vielzahl anderer Patent- und Know-how-Lizenzen erforderlich, u. a. eine Lizenz für die Benutzung des DVD-Formats und -Logos (lizenziert durch die in Tokyo ansässige „DVD Format/Logo Licensing Corporation, LLC", <http://www.dvdfllc.co.jp>), eine Lizenz der Dolby Laboratories zur Benutzung des Dolby-Digital-(AC-3)-Systems sowie Lizenzen von mehreren Patentpools, die Schlüsselpatente im DVD-Bereich lizenzieren (s. dazu oben Fn. 887); s. dazu im Überblick <http://www.licensing.philips.com/ dvdsystems/dvdlicensing.html>; *Taylor*, DVD Demystified, S. 204 ff. Diese anderen Lizenzverträge enthalten regelmäßig keine Bestimmungen über DRM-Komponenten.

[897] Tatsächlich existieren für den DVD-Standard alternative technische Schutzmaßnahmen. Die bekannteste ist „Divx", s. dazu oben Fn. 538; s. a. *Marks/Turnbull*, EIPR 2000, 198, 205; *Taylor*, DVD Demystified, S. 193. In der frühen Entwicklungszeit des DVD-Formats war geplant, die technischen Schutzmaßnahmen als Teil der allgemeinen DVD-Spezifikation auszugestalten. Im Lauf der Zeit entschied man sich jedoch, beide Vorhaben zu trennen, s. *Taylor*, a. a. O., S. 191 f.

[898] Die Verwendung von CSS war die wichtigste Bedingung der Filmindustrie, ein digitales Speichermedium wie DVD zu unterstützen. Im Rahmen der CPTWG einigte man sich dann auf CSS; s. zum ganzen oben Teil 1, D II 3 a.

[899] S. dazu oben Teil 1, D III 2 b.

[900] In umgekehrter Richtung bestimmt die HDCP-Lizenz, daß HDCP nur im Rahmen von DVI-Bildschirmen eingesetzt werden darf, § 2 Exhibit C, HDCP License Agreement.

Auch in den SDMI-Spezifikationen[901] finden sich Bestimmungen, wie die spezifizierten Schutzmaßnahmen einzusetzen sind. Jedoch handelt es sich bei der SDMI-Spezifikation um kein verbindliches Dokument: Die Gerätehersteller sind nicht vertraglich verpflichtet, alle Einzelheiten der SDMI-Spezifikation umzusetzen.[902] Mit dieser Beschränkung auf eine rechtlich unverbindliche Spezifikation sollte einerseits kartellrechtlichen Bedenken begegnet werden.[903] Andererseits war es nie das Ziel von SDMI, ein einheitliches DRM-System zu standardisieren.[904] Die bisher einzige Ausnahme ist, daß alle SDMI-kompatiblen Geräte ein bestimmtes, proprietäres Wasserzeichenverfahren („ARIS-SDMI-1") enthalten müssen, das von dem Unternehmen Verance entwickelt wurde.[905] In leicht abgewandelter Form wird dieses Wasserzeichenverfahren auch in Audio-DVDs verwendet („ARIS/SOLANA-4C").[906] Diese Verfahren sind unter anderem durch Patente und Geschäftsgeheimnisse geschützt.[907] Will ein Unternehmen SDMI- bzw. Audio-DVD-kompatible Abspielgeräte herstellen, so muß es einen Technologie-Lizenzvertrag – im folgenden: „4C/Verance Watermark License Agreement" – mit einer von Verance beauftragten Lizenzierungsstelle abschließen.[908]

---

[901] Zu SDMI allgemein s. oben Teil 1, D II 5.

[902] „The end result of the process […] will be a specification, not an agreement. Each music company […] will make its own decision as to the degree of security it finds acceptable in light of marketplace coniditions and each technology company will decide whether and the extent to which it incorporates the SDMI specifications in its designs", *Secure Digital Music Initiative*, SDMI Portable Device Specification Part 1, S. 5. Jedoch führt die *Secure Digital Music Initiative* ebda. aus: „Technology companies can reasonably conclude that an SDMI-Compliant product will meet the security needs of records companies and that consumers purchasing such devices will have broad, legitimate access to music."

[903] „SDMI is not intended to be […] an agreement that limits competition. […] antitrust laws permit, indeed under appropriate circumstances encourage, the creation of neutral standards that benefit the affected industry and consumers. The SDMI specification is such a standard", *Secure Digital Music Initiative*, SDMI Portable Device Specification Part 1, S. 5.

[904] SDMI legt bestimmte Anforderungen an DRM-Systeme fest, überläßt die Realisierung dieser Anforderungen jedoch den einzelnen Unternehmen.

[905] Zu diesem SDMI-Phase-I-Wasserzeichen von Verance s. oben Fn. 584. Zwar wäre es auch denkbar, mehrere Wasserzeichensysteme nebeneinander einzusetzen. Da die Einbettung mehrerer Wasserzeichen aber zu einer deutlichen Qualitätsverminderung und zu erhöhten Rechenkapazitätsanforderungen führen kann, hatten sowohl die Musik- als auch die Unterhaltungselektronik- und Computerindustrie ein Interesse daran, sich auf ein einziges Wasserzeichenverfahren für die SDMI-Phase I zu einigen. S. dazu *Marks/Turnbull*, EIPR 2000, 198, 211.

[906] S. dazu oben Teil 1, D II 3 d.

[907] S. u. a. *Wolosewicz*, U.S. Patent No. 5774452 (1998); *Wolosewicz/Jemili*, U.S. Patent No. 5828325 (1998); *Petrovic/Winograd/Jemili/Metois*, U.S Patent No. 5940135 (1999).

[908] S. dazu auch *Marks/Turnbull*, EIPR 2000, 198, 211.

In den USA wird im Rahmen der „OpenCable"-Initiative an einem offenen Standard für Pay-TV-Systeme gearbeitet.[909] Die OpenCable-Initiative wird von einer Vielzahl von Kabelnetzbetreibern, Computerunternehmen und der Filmindustrie unterstützt und von der FCC unterstützend begleitet. Es wird mit einer breiten Umsetzung dieses Standards im digitalen Kabel- und Satellitenfernsehbereich gerechnet. Der Standard baut unter anderem auf einem patentierten Verschlüsselungsverfahren auf (sog. „DFAST").[910] Zur Nutzung dieses Verfahrens müssen die Hersteller von Entschlüsselungskomponenten in Set-Top-Boxen, Videorekordern, PCs und ähnlichem eine Patentlizenz erwerben. Ansonsten könnten ihre Endgeräte die mit dem OpenCable-System geschützten Inhalte nicht entschlüsseln. In dem entsprechenden Patent-Lizenzvertrag, dem sogenannten „POD Host Interface License Agreement" finden sich Bestimmungen zur Sicherheit digitaler Inhalte, die für die vorliegende Analyse von Interesse sind.[911]

---

[909] Es ist hier nicht möglich, auf die Entstehungsgeschichte und den Zweck dieser breit angelegten Initiative einzugehen. Zur kurzen Einordnung: Nach 47 U.S.C. § 549 (= § 629 Communications Act) ist die FCC verpflichtet sicherzustellen, daß im Kabel- und Satellitenfernsehbereich der Kunde seine Set-Top-Box nicht notwendigerweise vom Betreiber des Kabel- bzw. Satellitennetzes erwerben muß, sondern daß er sie auch bei Drittanbietern kaufen kann. Dadurch soll Wettbewerb auf dem Markt der Set-Top-Boxen erreicht werden. Technisch kann dies durch sog. „MultiCrypt"-Verfahren erreicht werden. Dabei stellt der Netzbetreiber eine offene Schnittstelle zur Verfügung, über die verschiedene proprietäre Schutzsysteme mit der Set-Top-Box kommunizieren können; s. dazu oben Fn. 522. Im Rahmen der OpenCable-Initiative wurde ein solches „MultiCrypt"-System entwickelt. Die Entwicklung wurde von der FCC eng begleitet, die sich von der OpenCable-Initiative eine Öffnung des Wettbewerbs auf dem Set-Top-Boxen-Markt erhofft. S. dazu *Federal Commuications Commission*, 13 FCC Rcd. 14,775 (June 24, 1998); *dies.*, 15 FCC Rcd. 18,199 (September 18, 2000), Abs. 6 ff.; *dies.*, Annual Assessment, S. 82 ff.; s. a. im Überblick *Rosenthal*, RTkom 2000, 182, 187. In Deutschland findet sich eine Regelung mit der gleichen Zielrichtung in § 53 RfStV. Die OpenCable-Initiative steht im Zusammenhang mit der Digitalisierung des terrestrischen Fernsehens (sogenannter „analoger Switch-Off"), s. dazu *Grünwald*, MMR 2001, 89 ff.; vgl. weiterhin *Monopolkommission*, XIII. Hauptgutachten, Tz. 613 ff., 622, 626 ff.

[910] „Dynamic Feedback Arrangement Scrambling Technique", s. *Brown*, U.S. Patent No. 4860353 (1989).

[911] Die einzelnen Bestimmungen des „POD Host Interface License Agreement" waren monatelang Gegenstand eines erbitterten Streits zwischen der Filmindustrie und Verbraucherschutzverbänden, die die FCC drängten, auf den Lizenzvertrag regulierend einzuwirken; s. dazu *Federal Communications Commission*, 15 FCC Rcd. 18,199 (September 18, 2000), unter III.B. In ihrer Entscheidung vom September 2000 hat sich die FCC hinsichtlich der einzelnen Bestimmungen sehr zurückgehalten. Sie hat sich allerdings offengehalten, in Zukunft die einzelnen Lizenzbestimmungen auf ihre Vereinbarkeit mit urheberrechtlichen Grundsätzen zu überprüfen, *ebda.*, Abs. 29. Im Dezember 2000 wurde die endgültige Fassung des Lizenzvertrags an die FCC geschickt, s. *POD Host Interface License Agreement*. Die folgenden Ausführungen beziehen sich auf die Endfassung des Lizenzvertrages vom Dezember 2000. Frühere Versionen dieses Dokuments wurden „DFAST License Agreement" genannt. S. zum ganzen auch *Federal Communciations Commission*, Annual Assessment, S. 82 ff.

Schließlich wurden die jeweiligen Technologie-Lizenzverträge der CPRM/CPPM-Technologie[912] sowie von DTCP[913] ausgewertet.

2. Typische Technologie-Lizenzvertragsklauseln

a) Allgemeines

Obwohl die einzelnen DRM-Technologien unterschiedlichen Zwecken dienen und von unterschiedlichen Unternehmen entwickelt wurden, sind ihre Technologie-Lizenzverträge oft in weiten Teilen sehr ähnlich.[914] Dies läßt sich durch die intensive Kooperation der Unternehmen, unter anderem in der CPTWG,[915] erklären. Die Lizenzgeber solcher DRM-Technologie-Lizenzverträge sind regelmäßig Unternehmen, die eine technische DRM-Komponente entwickelt haben, oder sonstige Institutionen, die vom entwickelnden Unternehmen mit der Lizenzierung beauftragt wurden. Lizenznehmer sind einerseits die Hersteller von Unterhaltungselektronik-Geräten (von MP3-Abspielgeräten über Stereoanlagen, DVD-Spielern bis zu digitalen Fotokameras), Computern und Speichermedien (DVDs, CDs, Festplatten) sowie DRM-spezifischer Komponenten (Ver- und Entschlüsselungssyssteme auf Hard- oder Softwarebasis), andererseits die Inhalteanbieter selbst (Filmstudios, Tonträgerunternehmen etc.).[916]

DRM-Technologie-Lizenzverträge sind regelmäßig umfangreiche Dokumente, die neben den hier interessierenden Fragestellungen noch eine Fülle anderer lizenzrechtlicher Probleme betreffen.[917] Im folgenden wer-

---

[912] Zu den technischen Grundlagen s. oben Teil 1, D II 4.

[913] Zu den technischen Grundlagen s. oben Teil 1, D III 2 a.

[914] So finden sich in den CPRM/CPPM-Lizenzbestimmungen über weite Strecken ähnliche Klauseln wie in der CSS-Lizenz, s. beispielsweise § 2 ff. Exhibit B-3 Interim CPRM/CPPM License Agreement. Dies liegt auch daran, daß sich hinter beiden Lizenzgebern (DVD CCA und 4C Entity) die „License Management International, LLC", <http://www.lmicp.com>, verbirgt.

[915] Zur „Copy Protection Technical Working Group" s. oben bei Fn. 509.

[916] S. zu den möglichen Lizenznehmern auch *Taylor*, DVD Demystified, S. 485 f. Zwar müssen auch die Inhalteanbieter von den Entwicklern technischer DRM-Komponenten Technologie-Lizenzen erwerben, um ihre Inhalte in dem betreffenden DRM-System vertreiben zu können. Regelmäßig wurden die Bedingungen der Technologie-Lizenzverträge aber in enger Kooperation zwischen den Technologie-Entwicklern und den Inhalteanbietern entwickelt, z. B. durch Kooperation im Rahmen der CPTWG. Technologie-Lizenzverträge dienen mittelbar dem Interesse der Inhalteanbieter, s. dazu oben bei Fn. 890.

[917] Es sei nur am Rande darauf hingewiesen, daß solche Lizenzverträge mitunter Klauseln enthalten, die die Privatsphäre der Nutzer schützen sollen. Dadurch soll die Akzeptanz DRM-kompatibler Endgeräte beim Nutzer erhöht werden. So wird der Hersteller digital angesteuerter Bildschirme, der HDCP einsetzen will, in der HDCP-Lizenz verpflichtet, die HDCP-Komponenten (insbesondere individuelle Dechiffrier-Schlüssel) nicht zur invididuellen Identifikation des Nutzers und der Erstellung von Nutzerprofilen zu verwenden. § 6.1 HDCP License Agreement lautet: „Adopter shall not use any portion of the HDCP Specification, any implementation thereof or the

den schwerpunktmäßig Bestimmungen der CSS-Lizenz dargestellt.[918] Soweit andere Technologielizenzen entsprechende, abweichende oder weiterreichende Klauseln enthalten, wird im Text darauf hingewiesen.

b) Koppelung mit anderen DRM-Komponenten

Der CSS-Lizenzvertrag enthält umfangreiche Bestimmungen zu der Frage, wie die mit CSS geschützten Videodaten weiter geschützt werden müssen, wenn sie die CSS-Umgebung verlassen. Es geht um die Koppelung des CSS-Schutzes mit anderen DRM-Komponenten.

Gibt ein DVD-Spieler[919] die entschlüsselten Videodaten als *analoges* Signal an einen Fernseher weiter, so muß der DVD-Spieler die Videodaten mit zwei analogen Kopierschutzverfahren des Unternehmens Macrovision versehen, § 6.2.1.1 (1) CSS Procedural Specifications. Diese Verfah-

---

Device Keys or KSVs for the purpose of identifying and individual or creating, or facilitating the creation of, any means of collecting or aggregating information about an individual or any device or product in which HDCP, or any portion thereof, is implemented. Adopter may not use the Device Keys or KSVs for any purpose other than to support the authentication of a Licensed Product with another Licensed Product and to manage Revocation."

[918] Einen Überblick über die diesbezüglichen Bestimmungen der CSS-Lizenz geben *Marks/Turnbull*, EIPR 2000, 198, 206 f., und *Taylor*, DVD Demystified, S. 204. Alle folgenden Ausführungen beziehen sich auf die CSS-Lizenz Version 1.1. Die CSS-Lizenz besteht aus einem „CSS License Agreement", den „Procedural Specifications" und den „Technical Specifications". Daneben bestehen noch Lizenzteile, die sich nach der Art des jeweiligen Lizenznehmers richten („Assembler", „Reseller", „Content Provider", „Authoring Studio", „DVD Disc Replicator", „DVD Disc Formatter Manufacturer", „DVD Player Manufacturer", „DVD-ROM Drive Manufacturer", „DVD Decoder Manufacturer", „Descramble Module Manufacturer", „Authentication Chip Manufacturer", „Verification Product Manufacturer" und „Integrated Product Manufacturer"). Das „CSS License Agreement" enthält allgemeine Bestimmungen der Lizenzeinräumung (u. a. Recht zur Vergabe von Unterlizenzen, Kosten, Weitergabe geheimer Informationen an Mitarbeiter der Unternehmens, Vertragsbeendigung, Schadensersatz etc.). Die „Technical Specifications" befassen sich mit speziellen Fragen für die Hersteller von DVD-Spielern, CSS-Entschlüsselungsmodulen, Authentisierungsmodulen etc. Die im vorliegenden Zusammenhang wichtigsten Bestimmungen sind in den „Procedural Specifications" enthalten. Auf die Darstellung der Einzelheiten der über 40-seitigen CSS Procedural Specifications wird verzichtet. Die entsprechenden Dokumente sind bei <http://www.dvdcca.org/dvdcca> erhältlich.

[919] Die CSS Procedural Specifications verstehen unter einem „DVD player" (im folgenden: DVD-Spieler) ein eigenständiges DVD-Abspielgerät, das über interne Entschlüsselungsverfahren verfügt und beispielsweise direkt an einen Fernseher angeschlossen werden kann, § 1.26 CSS Procedural Specifications. Dagegen wird unter einem „DVD drive" (im folgenden: DVD-Computerlaufwerk) ein DVD-Abspielgerät verstanden, das – ähnlich einem CD-ROM-Laufwerk – in einen Computer eingebaut wird und bei dem die Entschlüsselung der Videodaten entweder durch eine speziellen Hardware oder durch ein Softwareprogramm erfolgt, das mit dem DVD-Computerlaufwerk im engeren Sinne nichts mehr zu tun hat, s. § 1.25 CSS Procedural Specifications. Schließlich gibt es noch das „integrated product", bei dem ein DVD-Spieler oder eine andere CSS-Komponente Teil eines größeren, einheitlich integrierten Produkts ist (z. B. die Sony Playstation II), s. § 1.29 und § 6.2.8 CSS Procedural Specifications.

ren führen bei einem Kopieren der Videodaten auf eine herkömmliche analoge Videokassette zu einem verrauschten und unruhigen beziehungsweise zu einem mit horizontalen Streifen versehenen Bild.[920] Weiterhin muß der DVD-Spieler die Videodaten mit CGMS-Metadaten versehen, § 6.2.1.1 (1) CSS Procedural Specifications.[921] Ähnliche Klauseln finden sich in dem DTCP-, dem CPRM/CPPM- sowie dem „POD Host Interface"-Lizenzvertrag.[922]

Gibt ein DVD-Spieler die entschlüsselten Videodaten als *digitales* Signal weiter, so müssen die Übertragungswege mit DTCP[923] beziehungsweise HDCP[924] geschützt sein, § 6.2.1.2 CSS Procedural Specifications.[925] Diese Schutzarchitektur wird in den DTCP- und HDCP-Lizenzen weitergeführt. Nach der HDCP-Lizenz dürfen Geräte HDCP-geschützte Videodaten an andere Geräte in digitaler Form nur weiterreichen, wenn

---

[920] Zu den technischen Grundlagen dieser Verfahren s. oben Fn. 503. Der Macrovision-Kopierschutz ist jedoch nicht lückenlos. Insbesondere sind die Übertragungen von DVD-Computerlaufwerken an Computermonitore, die – was heute der Regelfall ist – über sog. RGB-Signale angesteuert werden, durch nicht geschützt, da die analogen Kopierschutzsysteme von Macrovision bei RGB-Signalen nicht greifen, s. dazu oben Fn. 537. Diese Schutzlücke wurde auch in der CSS-Lizenz wegen der weiten Verbreitung von RGB-Computermonitoren in Kauf genommen, *Marks/Turnbull*, EIPR 2000, 198, 207. Einen Ausweg bietet nur HDCP, das bei digital angesteuerten (DVI-)Bildschirmen anwendbar ist.

[921] Zu den technischen Grundlagen von CGMS s. oben Teil 1, D II 3 b. Bei CSS-geschützten Videoinhalten dürfen digitale Audiodaten nur weitergegeben werden, wenn sie mit SCMS-Informationen versehen sind, § 6.2.1.3. CSS Procedural Specifications. Zu den technischen Grundlagen von SCMS s. oben Teil 1, D II 1.

[922] Dagegen dürfen Videodaten, die mit HDCP verschlüsselt wurden, in entschlüsseltem Zustand in analoger Form überhaupt nicht an dritte Geräte weitergegeben werden, §§ 3.3, 3.4 Exhibit C, HDCP License. Videodaten, die mit DTCP geschützt sind, müssen bei einer analogen Übertragung mit den Macrosivision-Schutzverfahren und CGMS-Metadaten ausgestattet werden, § 4.3.1, 4.3.2 Exhibit B, Part 1, DTCP License Agreement. Auch hier greift eine Ausnahme für RGB-Computermonitore, bei denen die Schutzmaßnahmen von Macrovision nicht greifen, § 4.2.3 Exhibit B, Part 1, DTCP License Agreement. Die Lizenznehmer von CPRM/CPPM verpflichten sich, die Macrovision-Schutzverfahren sowie – auf Verlangen der Inhalteanbieter – digitale Wasserzeichen einzusetzen, § 3.4 Exhibit B-1 Interim CPRM/CPPM License Agreement. Nach dem „POD Host Interface License Agreement" dürfen geschützte Videoinhalte in analoger Form an andere Geräte (Fernseher etc.) nur ausgegeben werden, wenn sie mit den Macrovision-Schutzverfahren versehen werden, § 2.2.1 Exhibit C, POD Host Interface License Agreement. Eine Ausnahme gilt wiederum für die Übertragung an RGB-Computermonitore, § 2.2.2 Exhibit C, POD Host Interface License Agreement.

[923] Zu den technischen Grundlagen von DTCP s. oben Teil 1, D III 2 a.

[924] Zu den technischen Grundlagen von HDCP s. oben Teil 1, D III 2 b.

[925] Ähnliche Bestimmungen finden sich für Audio-DVD-Spieler in § 4.2.1 (i) und § 4.2 Exhibit B-1 Interim CPRM/CPPM License Agreement. Nach dem „POD Host Interface"-Lizenzvertrag dürfen Inhalte nur ausgegeben werden, wenn sie durch DTCP geschützt werden, § 2.4.1 Exhibit C, POD Host Interface License Agreement; s. a. *Federal Communications Commission*, 15 FCC Rcd. 18,199 (September 18, 2000), Absatz 17.

die Daten in diesen Geräten weiterhin durch HDCP geschützt werden, §§ 3.4, 5.3 Exhibit C, HDCP License.[926]

Nach dem CSS-Lizenzvertrag dürfen entschlüsselte komprimierte Videodaten nicht über einen Datenbus[927] geschickt werden, der von einem Angreifer abgehört werden kann, § 6.2.4.2 (2) CSS Procedural Specifications.[928] Der CSS-Lizenzvertrag sieht weiter vor, daß DVD-Spieler mit dem „Regional Code Playback Control"-System[929] ausgestattet sein müssen und nur DVDs einer bestimmten Region abspielen dürfen, § 6.2.1.4 CSS Procedural Specifications.[930] Nach dem CSS-Lizenzvertrag dürfen DVD-Spieler keine Videodaten von beschreibbaren DVDs entschlüsseln, da die Videodaten in einem solchen Fall wahrscheinlich auf die beschreibbare DVD kopiert wurden, § 6.2.1.5 CSS Procedural Specifications.[931] DVD-Computerlaufwerke[932] müssen über Authentisierungskomponenten[933] verfügen, die eine sichere Übertragung der verschlüsselten Videodaten zur authentifizierten Entschlüsselungssoftware oder -hardware ermöglichen, § 6.2.2.1 CSS Procedural Specifications.

Zusätzlich sieht der DTCP-Lizenzvertrag vor, daß geschützte Inhalte, die mit der Kopierkontrollinformation „Copy One Generation" versehen sind,[934] nur auf ein Gerät kopiert werden dürfen, das den Inhalt seiner-

[926] Das Gleiche gilt für DTCP, § 4.4 Exhibit B, Part 1, DTCP License Agreement.

[927] Ein Datenbus ist ein Übertragungsleitungssystem innerhalb eines PCs (z. B. zwischen Arbeitsspeicher und Prozessor), an den teilweise auch externe Geräte angeschlossen werden können.

[928] Solche unsicheren Datenbusse sind z. B. PCI, PCMCIA oder Cardbus. Ein sicherer Datenbus ist Firewire, wenn auf ihm DTCP betrieben wird, s. dazu oben Fn. 608. S. auch *Marks/Turnbull*, EIPR 2000, 198, 206 f. Entsprechende Bestimmungen finden sich in den HDCP-, DTCP- und „POD Host Interface"-Lizenzverträgen, s. § 2 Exhibit D, HDCP License; § 2.2 Exhibit C, DTCP License Agreement; § 2 Exhibit B, POD Host Interface License Agreement. Beim POD Host Interface-Lizenzvertrag gilt dies jedoch nicht für digitale komprimierte Audiodaten, § 2 Exhibit B, POD Host Interface License Agreement; sie dürfen zu einem externen Dolby-Digital-Decoder über eine (digitale und ungeschützte) SP/DIF-Schnittstelle ausgegeben werden.

[929] Zu den technischen Grundlagen der „Regional Code Playback Control" s. oben Teil 1, D II 3 e.

[930] Aus Sicherheitsgründen ist es seit dem 1. 1. 2000 erforderlich, daß DVD-Computerlaufwerke die „Regional Playback Control" auf Hardwareebene unterstützen (sogenannte „Regional Playback Control Phase II"). Es ist nicht mehr ausreichend, daß die Region des DVD-Laufwerks durch eine Softwarekomponente festgesetzt wird, § 6.2.2.2 (2) CSS Procedural Specifications; s. a. *Taylor,* DVD Demystified*, S. 4*91. Dies gilt nur für DVD-Computerlaufwerke, nicht für DVD-Spieler, s. <http://www.dvdcca.org/dvdcca/rpc.html>.

[931] S. dazu auch *Marks/Turnbull*, EIPR 2000, 198, 207. Eine entsprechende Bestimmung findet sich für Audio-DVD-Spieler, die CPPM verwenden, in § 4.1.3 Exhibit B-1 Interim CPRM/CPPM License Agreement.

[932] Zur Unterscheidung zwischen DVD-Spielern und DVD-Computerlaufwerken s. oben Fn. 919.

[933] Zu den technischen Grundlagen bei CSS s. oben Fn. 543.

[934] Eine solche Kopierkontrollinformation entspricht im Ergebnis dem SCMS-System.

seits verschlüsselt und dabei kryptographisch mit dem individuellen Speichermedium fest verbindet. Dadurch wird sichergestellt, daß der kopierte Inhalt nicht auf ein drittes Speichermedium kopiert und von dort genutzt werden kann, § 3.2 Exhibit B, Part 1, DTCP License Agreement.[935] Um das schnelle Raubkopieren in großem Stil zu verhindern, enthält die CPPM/CPRM-Lizenz Bestimmungen, die die Übertragungsgeschwindigkeit bei Audiodaten begrenzen.[936]

Es zeigt sich, daß DRM-Technologie-Lizenzverträge umfangreiche Bestimmungen enthalten, durch die sichergestellt werden soll, daß die lizenzierten DRM-Komponenten mit anderen DRM-Komponenten gekoppelt werden, so daß insgesamt in Endgeräten ein durchgängig hohes Schutzniveau gewährleistet ist.

c) Standard-Nutzungsbedingungen

Grundsätzlich können die Inhalteanbieter in DRM-Systemen selbst festlegen, mit welchen Nutzungsbedingungen sie ihre Inhalte versehen werden sollen. Mehrere Technologie-Lizenzverträge enthalten Bestimmungen, die die Hersteller von Endgeräten verpflichten, daß ihre Geräte die von den Inhalteanbietern in Metadaten festgelegten Nutzungsbedingungen befolgen müssen.[937]

Legt der Inhalteanbieter keine individuellen Nutzungsbedingungen fest, so sehen mehrere Technologie-Lizenzverträge allgemeine Nutzungsbedingungen vor, die in diesem Fall eingreifen („default settings"). Nach dem CPRM/CPPM-Lizenzvertrag dürfen digitale Inhalte auf ein anderes Gerät jeweils nur einmal kopiert werden, § 3.3.6 Exhibit B-1 Interim

[935] Eine solche kryptographische Bindung an ein individuelles Speichermedium ist beispielsweise mit CPRM möglich, s. oben Teil 1, D II 4. Zur Nutzeridentifizierung durch individuelle Verschlüsselung allgemein s. oben Teil 1, C II 3 c aa. Weiterhin enthält der DTCP-Lizenzvertrag nähere Bestimmungen zur Interoperabilität von DTCP und CSS sowie Conditional-Access-Systemen aus dem Pay-TV-Bereich, s. Exhibit B, Part 2 und 3, DTCP License Agreement.

[936] So muß nach § 4.2.1 (ii), (iii) Exhibit B-1 Interim CPRM/CPPM License Agreement bei der Übertragung digitaler Audiodaten über SP/DIF oder USB Audio sowie analoger Audiodaten die Qualität der Audiodaten hörbar verschlechtert werden, wenn die Daten in mehr als 1.5-facher Geschwindigkeit übertragen werden. Eine ähnliche Klausel findet sich im „POD Host Interface"-Lizenzvertrag. Werden in einem Pay-TV-System, das auf dem POD Host Interface aubaut, Videodaten in hoher Auflösung übertragen („High Definition Television," HDTV), so dürfen sie nur an andere Geräte weitergegeben werden, wenn dabei die Auflösung vermindert wird, § 2.3 Exhibit C, POD Host Interface License Agreement.

[937] S. § 3.1.1 Exhibit B-2 Interim CPRM/CPPM License Agreement; § 3 Exhibit B, Part 1, DTCP License Agreement; § 3 Exhibit C, POD Host Interface License Agreement. Wenn also ein Inhalt mit dem Metadatum „Copy Never" versehen ist, ist der Hersteller eines Endgeräts, das CPRM oder CPPM unterstützt, lizenzvertraglich verpflichtet, daß das Erstellen einer Kopie dieses Inhalts mit seinem Endgerät unmöglich ist.

CPRM/CPPM License Agreement.[938] Nach der – allerdings unverbindlichen[939] – SDMI-Spezifikation dürfen die Nutzer SDMI-kompatibler Geräte grundsätzlich bis zu vier Kopien digitaler Inhalte anfertigen, wovon bis zu drei Kopien auf tragbare Geräte oder Medien übertragen werden dürfen.[940] Von dieser Grundsatzregel kann der Inhalte-Anbieter jedoch abweichen.[941]

Im Gegensatz zu diesen Klauseln wird in Technologie-Lizenzverträgen mitunter auch zwingend festgelegt, daß es dem Nutzer ermöglicht werden *muß*, eine bestimmte Anzahl von Kopien zu erstellen. Nach den Lizenbestimmungen für das bei SDMI und Audio-DVDs eingesetzte Wasserzeichen dürfen Audio-DVDs und CDs nur Kopierkontrollinformationen enthalten, nach denen zumindest das einmalige Kopieren der Inhalte in CD-Qualität erlaubt ist. Der Lizenzvertrag untersagt es grundsätzlich, Audio-DVDs oder CDs herzustellen, die überhaupt nicht kopiert werden können, § 5.4.1 4C/Verance Watermark License Agreement.[942] Die Musikindustrie will ein völliges Kopierverbot verhindern, da dies von den Kunden nicht akzeptiert werde.[943]

d) Sicherheit der Implementierung

Die Entwickler von DRM-Technologien wollen sicherstellen, daß die Hersteller von Endgeräten ihre Technologien auf sichere Weise implementieren. Daher werden die Hersteller von Endgeräten in Technologie-Lizenzverträgen dazu verpflichtet, daß ihre Software- und Hardwarekomponenten durch entsprechende Maßnahmen (Verschlüsselung, Integritätsprüfung, manipulationssichere Systeme etc.) vor Angriffen geschützt werden müssen.[944] Werden CSS-Videodaten durch eine Softwarekomponente entschlüsselt, so muß sichergestellt sein, daß die Entschlüsselungskomponente durch allgemein verfügbare Hilfsmittel (beispielsweise sogenannte „Debugger") keinesfalls und mit professioneller Ausrüstung (beispielsweise In-Circuit-Emulatoren oder Logikanalysato-

[938] Dies ist nicht identisch mit den Einstellungen des SCMS-Systems. Bei SCMS kann ein Original auf ein anderes Aufnahmegerät unbegrenzt oft kopiert werden, solange dieses Original vorliegt. Bei den Standardeinstellungen von CPPM kann das Original auf ein anderes Aufnahmegerät nur einmal kopiert werden; soll es nochmal kopiert werden, ist dies nur auf ein anderes Aufnahmegerät möglich. Zu SCMS und dem Verbot der „Kopie der zweiten Generation" s. oben Teil 1, D II 1).

[939] S. dazu oben bei Fn. 902 ff.

[940] *Secure Digital Music Initiative*, SDMI Portable Device Specification Part 1, S. 18.

[941] *Secure Digital Music Initiative*, SDMI Portable Device Specification Part 1, S. 14, 18.

[942] Diese Beschränkung gilt nur bei Audio-DVDs und CDs, nicht bei online übertragenen Inhalten, § 5.4.2 4C/Verance Watermark License Agreement.

[943] S. dazu *Marks/Turnbull*, EIPR 2000, 198, 211.

[944] So § 3 Exhibit C Interim CPRM/CPPM License Agreement; § 1.2 Exhibit G, 4C/Verance Watermark License Agreement; § 3 Exhibit D, HDCP License; § 3 Exhibit C, DTCP License Agreement; § 3 Exhibit B, POD Host Interface License Agreement.

ren) nur mit Schwierigkeiten kompromittiert werden kann, § 6.2.4.2 CSS Procedural Specifications.[945] Ähnliche Vorschriften finden sich für den Fall, daß die Entschlüsselung durch eine Hardwarekomponente ausgeführt wird, § 6.2.5 und § 6.2.6 CSS Procedural Specifications.[946]

e) Verfahren bei Kompromittierung der Schutzmaßnahme

Neben Lizenzvertragsklauseln, die einen erfolgreichen Angriff auf DRM-Komponenten verhindern sollen, existieren auch Klauseln, die in Fällen eingreifen, in denen ein solcher Angriff dennoch gelingt. So finden sich im CSS-Lizenzvertrag Klauseln, nach denen der Hersteller eines Endgeräts, in das CSS-Komponenten integriert sind, bei einer Kompromittierung seiner CSS-Implementierung verpflichtet ist, die Implementierungsschwachstelle innerhalb genau festgelegter Zeiträume in den neu vertriebenen Produkten zu beseitigen. Diese Verpflichtung gilt nicht nur, wenn die CSS-Implementierung kompromittiert wird. Sie gilt auch, wenn eine der anderen technischen Schutzmaßnahmen kompromittiert wird, zu deren zusätzlicher Implementierung der Gerätehersteller durch die CSS-Lizenz verpflichtet wurde,[947] § 6.2.4.3, § 6.2.5.5 und § 6.2.6 CSS Procedural Specifications, § 4.2.2 CSS License Agreement.[948] Ändern die Entwickler des CSS-Verfahrens dessen Schutzarchitektur, weil beispielsweise Schwachstellen bekannt geworden sind, so sind die Lizenznehmer verpflichtet, diese Änderungen zu übernehmen, § 6.2.13 CSS Procedural Specifications.

Nach den Bestimmungen der CPRM/CPPM-Lizenz sind der Lizenzgeber sowie Filmstudios und Tonträgerunternehmen berechtigt, bestimmte Endgeräte des Lizenznehmers von der weiteren Nutzung des DRM-Systems auszuschließen („device revocation"),[949] wenn die Dechiffrier-

[945] Zu diesem Zweck sollen geheime Dechiffrier-Schlüssel und Algorithmen durch Verschlüsselungsverfahren und „Code Obfuscation" geschützt werden, § 6.2.4.2 (1) CSS Procedural Specifications. Schließlich müssen Integritätsprüfungen durchgeführt werden, um unautorisierte Modifikationen zu entdecken, § 6.2.4.2 (3) CSS Procedural Specifications. Zu manipulationssicherer Software und „Code Obfuscation" s. oben Teil 1, C IV 2, zu Integritätsprüfungen von Systemkomponenten s. oben Teil 1, C III 1 c.

[946] Die anderen Technologie-Lizenzverträge enthalten entsprechende Klauseln, s. § 4 Exhibit C Interim CPRM/CPPM License Agreement; § 1.3 Exhibit G, 4C/Verance Watermark License Agreement; § 3.5 Exhibit D, HDCP License; § 3.5 Exhibit C, DTCP License Agreement; § 3 (e) Exhibit B, POD Host Interface License Agreement. Nach dem HDCP-Lizenzvertrag dürfen im digitalen Bildschirm keine dauerhaften Kopien der entschlüsselten Inhalte verfügbar sein, § 3.2 Exhibit C, HDCP License.

[947] Hier wirkt die lizenzvertragliche Koppelung unterschiedlicher DRM-Komponenten fort, s. dazu oben Teil 2, C II 2 b.

[948] Ähnliche Bestimmungen finden sich in § 1.4 Exhibit G, 4C/Verance Watermark License Agreement; § 3.6 Exhibit D, HDCP License; § 3.6 Exhibit C, DTCP License Agreement; § 3 (f) Exhibit B, POD Host Interface License Agreement.

[949] Zu den technischen Grundlagen s. oben Teil 1, C I 1 b bb.

Schlüssel dieser bestimmten Endgeräte kopiert, ausgelesen oder veröffentlicht wurden, § 9.2 Interim CPRM/CPPM License Agreement.[950]

f) Keine Herstellung von Umgehungstechnologie

Die Entwickler von DRM-Technologien wollen verhindern, daß sie solchen Herstellern von Endgeräten eine Lizenz zur Benutzung ihrer DRM-Technologie einräumen, welche die dadurch erworbenen Informationen mißbrauchen und Vorrichtungen herstellen, mit denen die DRM-Technologie umgangen werden werden kann. Daher enthält der CSS-Lizenzvertrag eine Klausel, wonach der Lizenznehmer nicht berechtigt ist, Hardware oder Software herzustellen, mit der der CSS-Schutz umgangen werden kann. Die Klausel ist nicht auf CSS beschränkt. Sie verbietet die Herstellung von Umgehungsvorrichtungen für alle in DVDs eingesetzten DRM-Komponenten (Macrovision, CGMS, DTCP, HDCP, SCMS, Regional Code Playback Control etc.),[951] § 6.2.12 CSS Procedural Specifications.[952]

g) Rechtsfolgen bei Verletzung der Lizenzbestimmungen

DRM-Technologie-Lizenzverträge müssen auch die Frage regeln, welche Rechtsfolgen ein Verstoß des Lizenznehmers gegen Bedingungen des Lizenzvertrags hat. Verstößt der Lizenznehmer gegen eine der Bestimmungen des CSS-Lizenzvertrags, so ist der Lizenzgeber berechtigt, die Lizenzeinräumung zu unterbrechen oder zu beenden, § 6.1 (b) CSS License Agreement. Einige Lizenzbestimmungen können nicht nur vom Lizenzgeber – der DVD Copy Control Association – sondern auch von Filmstudios durchgesetzt werden, § 9.5 CSS License Agreement (sogennante „third party beneficiary rights").[953] Daneben finden sich regelmäßig umfangreiche Bestimmungen zur Höhe des Schadensersatzes und dergleichen.

---

[950] Zum Schutz der Interessen der Lizenznehmers kann sich ein Streitschlichtungsverfahren anschließen, § 9.3 ff. CPRM/CPPM License Agreement. Ähnliche Bestimmungen finden sich in § 4 sowie § 3, Procedural Appendix, DTCP License Agreement.

[951] Auch hier wirkt die lizenzvertragliche Koppelung unterschiedlicher DRM-Komponenten fort, s. dazu oben Teil 2, C II 2 b.

[952] Ähnliche Klauseln finden sich im „POD Host Interface"-Lizenzvertrag. Danach dürfen Endgeräte eingebettete Wasserzeichen des Schutzsystems nicht entfernen oder verändern, § 2.6 Exhibit C, POD Host Interface License Agreement. Ermöglicht der Hersteller eines DTCP-Geräts die Übertragung DTCP-geschützter Videodaten ins Internet, so verstößt er gegen die DTCP-Lizenz, § 4.4.1 Exhibit B, Part 1, DTCP License Agreement.

[953] S. dazu *Marks/Turnbull*, EIPR 2000, 198, 207 f. Auch der HDCP- und der DTCP-Lizenzvertrag räumt Inhalteanbietern entsprechende Rechte ein. Gleiches gilt nach § 9.2 4C/Verance Watermark License Agreement für Filmstudios, Tonträgerunternehmen etc.

III. Kartellrechtliche Wirksamkeit

Wie gezeigt wurde, finden sich in DRM-Technologie-Lizenzverträgen umfangreiche Bestimmungen, durch die ein hohes Schutzniveau in DRM-Systemen gewährleistet werden soll. Damit dienen solche Klauseln mittelbar dem Interesse der Inhalteanbieter, die ihre Inhalte im betreffenden DRM-System veröffentlichen wollen. Ein Schutz durch Technologie-Lizenzverträge würde jedoch ausscheiden, wenn Lizenzvertragsklauseln der dargestellten Art rechtlich unwirksam wären. Gesetzliche Vorschriften, die inhaltliche Anforderungen an DRM-Technologie-Lizenzverträge stellen, sind rar. In den USA[954] und Europa[955] existieren spezielle Vorschriften allenfalls im Bereich der Pay-TV-Regulierung. Die einzige bisherige Äußerung in der Literatur zu der allgemeinen Problematik bejaht unkritisch die Wirksamkeit solcher Technologie-Lizenzverträge.[956]

---

[954] So ergibt ein Gegenschluß aus 47 C.F.R. § 76.1204 (c), daß ein Kabelnetzbetreiber in den USA durch Lizenzverträge die Herstellung von Endgeräten unterbinden kann, die sein Schutzsystem unterlaufen. Die Vorschrift bestimmt: „No multichannel video programming distributor (z. B. Kabelnetzbetreiber) shall by *contract*, agreement, patent, intellectual property right or otherwise preclude the addition of features or functions to the equipment […] that are not designed, intended or function to defeat the conditional access controls of such devices or to provide unauthorized access to service." Zum Erlaß der Vorschrift durch die FCC im Rahmen der sogenannten „navigation devices order" s. *Federal Communications Commission*, 13 FCC Rcd. 14,775 (June 24, 1998).

[955] Art. 4 lit. b 2. Spiegelstrich der europäischen Fernsehsignalübertragungs-Richtlinie regelt Patent- und Know-how-Lizenzklauseln bei DRM-Komponenten im digitalen Pay-TV-Bereich (zur Fernsehsignalübertragungs-Richtlinie s. a. unten Teil 2, D II 1 a). Die im Vergleich zur EG-Richtlinie leichter verständliche Formulierung des § 9 Abs. 3 Fernsehsignalübertragungs-Gesetz (FÜG), der den Art. 4 lit. b 2. Spiegelstrich der EG-Richtlinie sinngemäß in deutsches Recht umsetzt, lautet:
„Der Rechtsinhaber darf die Vergabe [von Patent- und Know-how-Lizenzen an Zugangsberechtigungssystemen und produkten] nicht an Bedingungen knüpfen, mit denen der Einbau
1. […]
2. von anderen Elementen, die einem *anderen* Zugangssystem eigen sind,
in ein Gerät untersagt, verhindert oder erschwert werden soll. Der Lizenznehmer muß angemessene Bedingungen des Rechteinhabers, mit denen die Sicherheit der Transaktionen der Anbieter von Zugangsberechtigtungssystemen sichergestellt wird, hinnehmen." Derzeit wird an einer Reform der europäischen Regelung gearbeitet, s. Anhang I Teil I lit. c des Vorschlags der Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung, KOM (2000) 384 vom 12. 7. 2000, S. 23. Der Vorschlag wurde am 1. 3. 2001 in erster Lesung im Europäischen Parlament behandelt. S. weiterhin § 13 der von allen Landesmedienanstalten übereinstimmend beschlossenen Satzung über die Zugangsfreiheit zu digitalen Diensten gemäß § 53 Abs. 7 Rundfunkstaatsvertrag vom 26. 6. 2000, erhältlich unter <http://www.artikel5.de/gesetze/digizu.html>; s. dazu auch *Holznagel*, MMR 2000, 480, 483 ff.

[956] Es handelt sich um eine Äußerung zweier U.S.-amerikanischer Autoren. *Marks/Turnbull*, EIPR 2000, 198, 206, meinen: „The CSS system developed by MEI

Dies könnte aber unter kartellrechtlichen Gesichtspunkten zweifelhaft sein. Dies gilt insbesondere für die Verpflichtung des Lizenznehmers in DRM-Technologie-Lizenzverträgen, neben der eigentlich lizenzierten Technologie noch andere DRM-Komponenten in das Endgerät zu integrieren.[957] Solche lizenzvertraglichen Koppelungsbindungen können kartellrechtlich problematisch sein. Oftmals bestehen jedoch zwischen den unterschiedlichen DRM-Komponenten komplementäre Abhängigkeitsverhältnisse: Eine einzelne Schutzkomponente wie CSS, die nur einen bestimmten Abschnitt in der Verbreitung digitaler Inhalte vom Anbieter zum Nutzer schützt, ist wertlos, wenn nicht die anderen Abschnitte mit äquivalenten Schutzkomponenten ausgestattet sind.[958] Durch die lizenzvertragliche Koppelung unterschiedlicher DRM-Komponenten soll in einem umfassenden DRM-System ein einheitliches und durchgängiges Schutzniveau geschaffen werden. Ohne dieses Schutzniveau würden die Inhalteanbieter ihre Inhalte nicht in dem betreffenden DRM-System anbieten. Fehlen die Inhalte, entsteht für das betreffende DRM-System und die einzelnen DRM-Komponenten auch keine Nachfrage. Ohne Klauseln in DRM-Technologie-Lizenzverträgen, durch die mehrere DRM-Komponenten zu einer umfassenden Schutzarchitektur kombiniert werden, würden Unternehmen die DRM-Komponenten gar nicht entwickeln, ein Wettbewerb zwischen den Entwicklern unterschiedlicher DRM-Komponenten würde erst gar nicht entstehen. Damit sind solche Lizenzklauseln oftmals schon gar nicht wettbewerbsbeschränkend im Sinne des Art. 81 EGV.[959] Ähnliches gilt für andere Klauseln in DRM-Technologie-Lizenzverträgen. Selbst wenn eine Wettbewerbsbeschränkung vorliegt, kann die Gruppenfreistellungsverordnung für Technologietransfer-Vereinbarungen aus dem Jahr 1996 greifen,[960] die bestimmte Vereinbarungen im Schnittfeld von Kartellrecht und Immaterialgüterrecht wegen ihrer inno-

[Matsushita Electric Industrial] and Toshiba is proprietary; these companies engineered the technology and hold certain intellectual property rights with respect to it. Therefore, any party that wants to use the CSS technology – either to encrypt content or decrypt content – must obtain a license. […] *Because a license is necessary to use the CSS technology, this license can impose obligations as to how the technology is used and how content should be treated once it is decrypted.* To ensure that content owners, consumer electronics manufacturers and computer manufacturers would actually use the CSS technology, it was crucial that a consensus be reached by all three industries as to the obligations imposed by the license" (Hervorhebung vom Verfasser).

[957] S. dazu oben Teil 2, C II 2 b.

[958] Zu der daraus erwachsenden Notwendigkeit der Systemintegration und der Standardisierung s. oben Teil 1, D I.

[959] Ebenso *Möschel/Bechtold* in: Pfitzmann/Roßnagel (Hrsg.), S. 9.

[960] Verordnung (EG) Nr. 240/96 der Kommission vom 31. Januar 1996 zur Anwendung von Artikel 85 Absatz 3 des Vertrages auf Gruppen von Technologietransfer-Vereinbarungen. ABl. EG Nr. L 31 vom 9. 2. 1996, S. 2 ff. Zum Zweck der VO 240/96 s. *Ullrich* in: Immenga/Mestmäcker (Hrsg.), EG-Wettbewerbsrecht, Band I, S. 1276, Rdnr. 11. Einen Überblick über die VO 240/96 gibt *Ebel*, WuW 1996, 779 ff.

vations- und wettbewerbsförderlichen Wirkung vom Verbot des Art. 81 EGV ausnimmt.[961] Ein ähnliches Bild ergibt sich im deutschen und im U.S.-amerikanischen Kartellrecht.[962]

Es ist im vorliegenden Rahmen unmöglich, eine breitere kartellrechtliche Analyse der einzelnen Technologie-Lizenzverträge zu leisten.[963] Hinter den angerissenen Fragen steht letztlich die Problematik der kartellrechtlichen Beurteilung von Standards und Normen.[964] Es zeigt sich aber, daß Klauseln in DRM-Technologie-Lizenzverträgen, durch die eine umfassende und sichere DRM-Schutzarchitektur gewährleistet werden soll,

[961] Die VO 240/96 bezieht sich u. a. auf Patentlizenz- und Know-how-Vereinbarungen zwischen zwei Unternehmen, Art. 1 Abs. 1 VO 240/96. Sie findet keine Anwendung auf Vereinbarungen zwischen Mitgliedern eines Patent- oder Know-how-Pools, s. Art. 5 Abs. 1 Nr. 1 VO 240/96. Die dargestellten DRM-Komponenten unterliegen entweder dem Patentschutz, oder es handelt sich um technische Kenntnisse, die geheim und wesentlich sind, also um Know-How im Sinne des Art. 10 Nr. 1 VO 240/96; s. zu diesen Voraussetzungen *Ullrich* in: Immenga/Mestmäcker (Hrsg.), EG-Wettbewerbsrecht, Band I, S. 1292 ff., Rdnr. 25 ff. Auch die VO 240/96 stellt klar, daß viele Koppelungs- und Ausschließlichkeitsbindungen in Technologie-Lizenzverträgen schon gar nicht wettbewerbsbeschränkend sind und nur „aufgrund besonderer wirtschaftlicher oder rechtlicher Umstände" unter Art. 81 Abs. 1 EGV fallen, s. Art. 2 Abs. 2 und Erwägungsgrund 18 der VO 240/96. Nach Art. 2 Abs. 1 Nr. 5 VO 240/96 können Klauseln in DRM-Technologie-Lizenzverträgen freigestellt sein, die notwendig sind, um bezüglich der lizenzierten Technologie ein bestimmtes Qualitätsniveau einzuhalten oder eine technisch einwandfreie Nutzung zu gewährleisten. Die Aufzählung in Art. 2 VO 240/96 ist nicht abschließend, Erwägungsgrund 18, VO 240/96.

[962] Im deutschen Kartellrecht können bei Patentlizenzen § 17, bei Know-How-Lizenzen § 17 i. V. m. § 18 Nr. 1 GWB eingreifen; s. dazu *Emmerich*, in: Immenga/Mestmäcker (Hrsg.), GWB-Kommentar, §§ 17, 18; *Martinek*, Moderne Vertragstypen, Band II, S. 268 ff. Im U.S.-amerikanischen Kartellrecht können die „Antitrust Guidelines for the Licensing of Intellectual Property" vom 6. 4. 1995 einschlägig sein, s. 4 Trade Reg. Rep. (CCH) 13132. Dies ist eine Verwaltungsvorschrift des U.S. Department of Justice und der Federal Trade Commission. Auch wenn im einzelnen dogmatische Unterschiede zwischen den Guidelines und der VO 240/96 bestehen, kommen sie in vielen Fällen zum gleichen Ergebnis; s. dazu *Meyer*, GRUR Int. 1997, 498, 506 f.; *Mummenthey*, CR 1998, 113 ff.; *Carlson*, 16 Yale J. on Reg. 359, 377 (1999). Nach § 5.3 Antitrust-Guidelines kann beispielsweise die Koppelung mehrer Lizenzen („package licensing") als eine Form des „tying arrangements" zulässig sein, wenn dies effizienz- und wettbewerbsfördernd wirkt; s. dazu *R. T. Nimmer,* § 11.13, S. 11–41 ff.

[963] Dies ist schon deshalb schwierig, da viele der Lizenzverträge nicht öffentlich zugänglich sind. Eine breitere Analyse müßte das Ineinandergreifen der unterschiedlichen Technologien und ihrer Lizenzbedingungen untersuchen. Zur Herstellung von DVD-Geräten und -Medien müssen beispielsweise bis zu acht Patent- und Know-How-Lizenzverträge mit unterschiedlichen Vertragspartnern (teilweise einzelne Unternehmen, teilweise Patentpools) geschlossen werden, s. dazu auch oben Fn. 896. Von diesen Lizenzbestimmungen sind nur einige wenige öffentlich zugänglich.

[964] Zum Verhältnis des Kartellrechts zur Standardisierung im Internet und anderen High-Tech-Bereichen s. *Lemley*, 28 Conn. L. Rev. 1041 ff. (1996); *Monopolkommission*, IX. Hauptgutachten, Tz. 811 ff.; *Schallop*, 28 AIPLA Q. J. 195 ff. (2000); *Carlson*, 16 Yale J. on Reg. 359, 394 f. (1999). Zur Bedeutung von Standards in Netzwerkmärkten s. *Shy*; *Lemley/McGowan*, 86 Cal. L. Rev. 479, 515 ff. (1998). S. weiterhin *C. Shapiro* in: Dreyfuss/Zimmerman/First (Hrsg.), S. 84 ff.

auch unter kartellrechtlichen Gesichtspunkten in weitem Umfang zulässig sein können.

IV. Zusammenfassung

Die Entwickler von DRM-Technologien versuchen, durch umfangreiche Technologie-Lizenzverträge die Sicherheit ihrer DRM-Komponenten und eines darauf aufbauenden DRM-Systems im Massenmarkt zu gewährleisten und damit eine sichere Vertriebsplattform für digitale Inhalte zu bieten. Entsprechende Lizenzvertragsklauseln dienen zumindest mittelbar dem Interesse der Inhalteanbieter, die nur bei einem entsprechendem Schutzniveau bereit sind, ihre Inhalte in einem bestimmten DRM-System zu verbreiten. Einem solchen Schutz durch Technologie-Lizenzverträge stehen auch unter kartellrechtlichen Gesichtspunkten keine grundsätzlichen Bedenken entgegen.

D. Schutz technischer DRM-Komponenten

In den letzten Jahren haben auch die Gesetzgeber auf nationaler wie internationaler Ebene erkannt, daß technische Schutzmechanismen zum Schutz von Urhebern und Leistungsschutzberechtigten immer wichtiger werden. Daher finden sich zunehmend gesetzliche Regelungen, durch die technische DRM-Komponenten spezifisch reguliert werden. Am bedeutendsten sind dabei Vorschriften, die die Umgehung technischer Schutzmaßnahmen verbieten (unten I). Daneben finden sich Vorschriften, die in bestimmten Fällen die Verwendung von DRM-Komponenten gesetzlich vorschreiben (unten II).

I. Schutz durch Umgehungsvorschriften

1. Allgemeines

Die meisten heutigen technischen Schutzmaßnahmen im DRM-Bereich können bei entsprechendem Aufwand umgangen werden.[965] Bieten technische Schutzmaßnahmen keinen hunderprozentigen Schutz, so kann durch zwei Ansätze versucht werden, diese Schwäche zu beseitigen. Einerseits kann versucht werden, die technischen Schutzkomponenten zu verbessern und das technische Schutzniveau zu erhöhen. Mitunter ist dies jedoch nicht möglich: Technische Verfahren können inhärenten Schwächen unterliegen, sie sind eventuell noch nicht ausgereift, oder eine sichere Implementierung ist schlicht zu kostspielig.[966] Selbst wenn die Sicher-

[965] S. dazu oben Teil 1, F.

[966] In DRM-Systemen muß eine Abwägung zwischen der erreichbaren Systemsicherheit und den dabei anfallenden Kosten gettroffen werden, s. dazu oben Teil 1, F.

heit technischen Schutzmaßnahmen in einem DRM-System erhöht werden kann, ist zu beachten, daß die Methoden und Fähigkeiten derjenigen, die technische Schutzkomponenten kompromittieren wollen, ebenfalls immer besser und ausgefeilter werden.[967] Deswegen kann andererseits versucht werden, einen ergänzenden rechtlichen Schutz zu schaffen. In diesem Zusammenhang ist es die Aufgabe des Rechts, einen Schutz gegen die Umgehung technischer Schutzmaßnahmen bereitzustellen.[968]

Seit einigen Jahren wird auf internationaler, europäischer und nationaler Ebene versucht, einen solchen rechtlichen Umgehungsschutz zu etablieren. Zwar existierten schon früher vereinzelt auf nationaler Ebene bereichsspezifische Regelungen, die die Umgehung technischer Schutzmaßnahmen betrafen.[969] Erst in den letzten Jahren wird aber versucht, eine umfassende Regelung zu konzipieren und diese auch international zu verankern. Die Einführung solcher umfassender Umgehungsregelungen erfolgt auf vehementen Druck der Musik- und Filmindustrie, die sich nicht allein auf technische Schutzmaßnahmen verlassen will.[970]

Im folgenden soll ein Überblick über die Vorschriften zum rechtlichen Schutz technischer Schutzmaßnahmen gegeben werden. Dabei wird auf Regelungen des Völker- und Europarechts sowie auf die deutsche und U.S.-amerikanische Rechtslage eingegangen. Auch wenn in Einzelheiten erhebliche Unterschiede bestehen, folgen alle Regelungen bestimmten strukturellen Grundmustern: Auf der einen Seite wird die Umgehung technischer Schutzmaßnahmen verboten (dazu unten 2). Dadurch kann eine Vielzahl technischer DRM-Komponenten geschützt werden, unter anderem Verschlüsselungsverfahren zur Zugangs- und Nutzungskontrolle, Kopierkontrollsysteme und Paßwörter,[971] Systeme zum Schutz von Authentizität und Integrität[972] sowie manipulationssichere Hard- und Software.[973] Auf der anderen Seite finden sich innerhalb des rechtlichen Schutzes technischer Schutzmaßnahmen spezielle Vorschriften zum Schutz von Metadaten (dazu unten 3). So wird die Entfernung oder Veränderung richtiger Metadaten, mitunter auch das Bereitstellen falscher Metadaten verboten. Bei diesen rechtlichen Vorschriften geht es haupt-

---

967 Vgl. *Smith/Weingart*, 31 Computer Networks 831, 838 (1999).

968 *Möschel/Bechtold*, MMR 1998, 571, 576.

969 Secs. 296 ff. des britischen „Copyright, Designs and Patents Act of 1988"; Vorschriften des U.S.-amerikanischen „Audio Home Recording Acts" 1992, insb. 17 U.S.C. § 1002 (c). Auf diese und andere Vorschriften wird im folgenden noch eingegangen werden.

970 Dies zeigt sich an den von immensem Lobbyismus begleiteten Gesetzgebungsvorhaben in der EU, den USA und bei der WIPO; s. a. *Marks/Turnbull*, EIPR 2000, 198, 204.

971 Zu den technischen Grundlagen s. oben Teil 1, C I.

972 Zu den technischen Grundlagen s. oben Teil 1, C III.

973 Zu den technischen Grundlagen s. oben Teil 1, C IV.

sächlich um Metadaten, die den digitalen Inhalt, dessen Rechteinhaber und die Nutzungsbedingungen identifizieren.[974]

Technische Schutzmaßnahmen bergen die Gefahr, daß urheberrechtliche Schrankenbestimmungen unterlaufen werden. Um einen Ausgleich zwischen dem technischen Schutz des Inhalteanbieters und urheberrechtlichen Schrankenbestimmungen zu schaffen, beschränkt der Gesetzgeber den rechtlichen Umgehungsschutz oftmals. Entsprechend der Ausrichtung des vorliegenden Teils der Untersuchung[975] werden die folgenden Ausführungen diesen Aspekt ausklammern. Darauf wird an einer späteren Stelle zurückzukommen sein.[976]

2. Verbot der Umgehung technischer Schutzmaßnahmen

Die gesetzlichen Verbote, technische Schutzmaßnahmen zu umgehen, betreffen nicht nur die tatsächliche Umgehung technischer Schutzmaßnahmen (dazu unten a). Heute werden oftmals Vorrichtungen, Technologien und Dienstleistungen angeboten, mit denen technische Schutzmaßnahmen umgangen werden können.[977] Aus Sicht der Inhalteanbieter liegt die eigentliche Gefahr der Umgehung technischer Schutzmaßnahmen nicht in der Umgehung durch einzelne Privatpersonen, sondern in der – kommerziellen – Verbreitung dieser Vorrichtungen.[978] Um die Effektivität des Rechtsschutzes zu erhöhen, werden daher auch die Herstellung und der Vertrieb von Vorrichtungen, Technologien und Dienstleistungen verboten, mit denen technische Schutzmaßnahmen später tatsächlich umgangen werden können. Mit solchen sogenannten „vorbereitenden Handlungen“ beschäftigt sich der Abschnitt b.

a) Verbot der tatsächlichen Umgehung

aa) Völkerrechtlicher Rechtsrahmen

Auf völkerrechtlicher Ebene finden sich Vorschriften, die die tatsächliche Umgehung technischer Schutzmaßnahmen verbieten, insbesondere in zwei völkerrechtlichen Verträgen aus dem Jahr 1996 (dazu unten 1). Daneben finden sich in anderen völkerrechtlichen Verträgen verstreut Regelungen, die ebenfalls einen solchen Rechtsschutz gewähren können (dazu unten 2).

(1) **WIPO-Verträge.** Ende Dezember 1996 wurden auf einer diplomatischen Konferenz der World Intellectual Property Organization (WIPO)

---

974 Zu den technischen Grundlagen s. oben Teil 1, C II.

975 S. dazu oben bei Fn. 732.

976 S. dazu unten Teil 3, B II 3, und Teil 4.

977 Dieses Phänomen ist im Pay-TV-Bereich seit langer Zeit bekannt, wo relativ problemlos „Piraten-Decoder“ erworben werden können. Ein anderes Beispiel ist die Verbreitung von DeCSS, einem Computerprogramm, welches das in Video-DVDs enthaltene Schutzsystem CSS umgeht, s. dazu oben Teil 1, D II 3 b.

978 Anm. 1 zu Art. 6 in *Europäische Kommission*, KOM (97) 628 endg., S. 37; *Wand*, S. 2.

zwei völkerrechtliche Verträge verabschiedet – der „WIPO Copyright Treaty“ (WCT) und der „WIPO Performances and Phonograms Treaty“ (WPPT).[979] Während der WCT Fragen des Urheberschutzes behandelt, geht es beim WPPT um den Schutz von ausübenden Künstlern und von Tonträgerherstellern. Der WCT wurde von 51 Staaten unterzeichnet (WPPT: 50 Staaten) und inzwischen von 24 Staaten (WPPT: 22 Staaten) ratifiziert.[980] Damit sind beide Verträge noch nicht in Kraft, Art. 20 WCT, 29 WPPT.[981]

In Art. 11 WCT und Art. 18 WPPT finden sich Vorschriften bezüglich der tatsächlichen Umgehung technischer Schutzmaßnahmen. Die endgültige Fassung beschränkt sich auf eine sehr allgemein gehaltene Vorschrift, die den Vertragsstaaten große Spielräume bei der Umsetzung lässt.[982] Nach Art. 11 WCT[983] haben die Staaten einen „angemessenen Rechtsschutz und wirksame Rechtsbehelfe gegen die Umgehung wirksamer technologischer Maßnahmen“ vorzusehen, „die von Urhebern in Zusammenhang mit der Ausübung ihrer Rechte“ nach dem WCT oder der RBÜ „getroffen werden und die Handlungen in bezug auf ihre Werke einschränken, die nicht von den betroffenen Urhebern gestattet oder gesetzlich erlaubt sind.“

Diese Vorschrift schützt einen weiten Bereich technischer Schutzmaßnahmen. Als einzige Einschränkung sieht die Vorschrift vor, daß die geschützte technische Maßnahme „wirksam“ sein muß. Eine genauere Definition, was eine „wirksame“ Schutzmaßnahme auszeichnet, fehlt. Es sollen wohl Maßnahmen ausgeschlossen werden, die technisch völlig unzureichend sind und leicht umgangen werden können.[984] Um eine Parallelität zwischen dem Schutz technischer Maßnahmen und dem Urheberrecht herzustellen, werden technische Maßnahmen nur geschützt, wenn

[979] Die Verträge sind in englischer Sprache unter <http://www.wipo.int/treaties> abrufbar und in IIC 1997, 208 ff., abgedruckt.

[980] Diese Informationen mit dem Stand vom 30. 6. 2001 stammen von <http://www.wipo.int/treaties/docs/english/u-page31.doc>.

[981] Dafür müssen die Verträge jeweils von 30 Staaten ratifiziert worden sein. Spätestens mit der Umsetzung der europäischen Richtlinie zum Urheberrecht in der Informationsgesellschaft in den Mitgliedstaaten der Europäischen Union werden beide Verträge in Kraft treten.

[982] Der ursprüngliche Entwurf der beiden Vorschriften enthielt eine detaillierte Regelung der Problematik, s. Art. 13 WCT Basic Proposal. Während der diplomatischen Konferenz war die Definition der Umgehungsvorrichtungen, der Umgehungshandlungen, die subjektiven Anforderungen beim Täter sowie Art und Voraussetzungen der rechtlichen Sanktionen umstritten; *v. Lewinski* in: Hoeren/Sieber (Hrsg.), Teil 7.9, Rdnr. 34; *dies*., GRUR Int. 1997, 667, 676; *Vinje*, EIPR 1997, 230, 234 f.; *v. Lewinski/Gaster*, ZUM 1997, 607, 619; *Haller*, S. 37 ff.; ausführlich *Wand*, S. 26 ff.

[983] Im folgenden wird Art. 11 WCT dargestellt. Art. 18 WPPT unterscheidet sich davon nur hinsichtlich des anderen Begünstigten des Rechtsschutzes (statt Urheber ausübende Künstler und Tonträgerhersteller).

[984] Ebenso *Koelman/Helberger* in: Hugenholtz (Hrsg.), S. 165, 172; *Wand*, S. 41f.

Urheber diese im Zusammenhang mit der Ausübung ihrer Rechte nach dem WCT oder der RBÜ anwenden.[985] Danach sind beispielsweise technische Maßnahmen zum Schutz von Datensammlungen und bestimmten Datenbanken von diesem völkerrechtlichen Schutz nicht erfaßt, da sie weder nach der RBÜ noch nach dem WCT geschützt sind.[986] Art. 11 WCT verbietet – als erste urheberrechtliche Vorschrift überhaupt[987] – die eigentliche Umgehung technischer Schutzmaßnahmen. Eine genauere Definition, was unter einer Umgehung zu verstehen ist, fehlt.

Bei einer erneuten diplomatischen Konferenz im Dezember 2000 sollte ein Protokoll zum WPPT verabschiedet werden, das Künstlern im Filmsektor und anderen audiovisuellen Bereichen Verwertungs- und Persönlichkeitsrechte auf völkerrechtlicher Ebene zugesteht. Der Entwurf[988] enthielt in Art. 15 eine den Art. 11 WCT und Art. 18 WPPT entsprechende Fassung. Es kam jedoch nicht zum Abschluß dieses Vertrages.[989]

(2) **Sonstige völkerrechtliche Regelungen.** Ein rechtliches Verbot der Umgehung technischer Schutzmaßnahmen kann sich auch aus anderen völkerrechtlichen Regelungen ergeben.

Seit November 1996 arbeitet der Europarat am sogenannten Europäischen Cybercrime-Übereinkommen.[990] Das ambitionierte Projekt will durch eine Mindestharmonisierung eine international effektive strafrechtliche Sanktionierung der „Cyberkriminalität" erreichen. Mit einer Verabschiedung des Übereinkommens wird im Herbst 2001 gerechnet.[991] Es wird erwartet, daß neben den Mitgliedern des Europarats auch assoziierte Länder wie die USA, Kanada, Japan und Südafrika dem Vertrag beitreten.[992] Nach Art. 2 Cybercrime-Übereinkommen (Entwurf) haben

---

[985] S. dazu *Wand*, S. 42 f.

[986] Ursprünglich war geplant, während der diplomatischen Konferenz im Dezember 1996 noch einen dritten WIPO-Vertrag abzuschließen, der den rechtlichen Schutz von Datenbanken betreffen sollte. Der Entwurf (*WIPO Database Treaty Basic Proposal*) enthielt in Art. 10 eine vergleichbare Regelung technischer Schutzmaßnahmen im Datenbankbereich. Aus Zeitmangel und wegen deutlicher Uneinigkeiten über den Vertragsentwurf kam es auf der diplomatischen Konferenz nicht einmal zur Verhandlung dieses Vertrags; s. *v. Lewinski* in: Hoeren/Sieber (Hrsg.), Teil 7.9, Rdnr. 57.

[987] *Koelman*, EIPR 2000, 272, der jedoch auf S. 273 Zweifel anmeldet, ob ein „angemessener Rechtsschutz" i. S. d. Art. 11 WCT nicht auch durch das bloße Verbot vorbereitender Handlungen erreichbar sei; zweifelnd *Wand*, S. 41.

[988] *WIPO Audiovisual Performances Treaty Basic Proposal.*

[989] S. dazu oben bei Fn. 740.

[990] Zur Entstehungsgeschichte s. das Draft Explanatory Memorandum zum Cybercrime-Übereinkommen (Entwurf), Abs. 7 ff.

[991] Die Einzelheiten der Entwürfe sind sehr umstritten. Insbesondere fanden sie Kritik bei Computerherstellern und Bürgerrechtsorganisationen, die durch das Cybercrime-Übereinkommen die Computersicherheitsforschung und Datenschutzrechte beeinträchtigt sahen.

[992] Zum Cybercrime-Übereinkommen allgemein s. *Scheffler/Dressel*, ZRP 2000, 514, 515; <http://www.iris.sgdg.org/actions/cybercrime>; <http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm>.

die Vertragsstaaten strafrechtliche Vorschriften zu erlassen, die den bewußten, unberechtigten Zugang[993] zu Computersystemen sanktionieren.[994] Die fehlende Berechtigung zum Zugang kann sich aus gesetzlichen Vorschriften, Gerichtsurteilen, vertraglichen Bestimmungen und ähnlichem ergeben.[995] Diese Vorschrift, die hauptsächlich gegen das sogenannte „Cracking" gerichtet ist,[996] kann auch Umgehungshandlungen im DRM-Bereich erfassen.

Das zwischen den USA, Kanada und Mexiko geschlossene NAFTA-Abkommen verpflichtet die Mitgliedstaaten in Art. 1707 lit. (b) NAFTA, einen zivilrechtlichen Schutz gegen das unberechtigte Empfangen verschlüsselter Satellitenprogramme zu schaffen.[997] Allerdings wird nur das Empfangen zu gewerblichen Zwecken, nicht das bloße Entschlüsseln

[993] Unter „Zugang" wird „the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data)" verstanden, s. *Draft Explanatory Memorandum* zum Cybercrime-Übereinkommen (Entwurf), Abs. 46.

[994] Art. 2 Cybercrime-Übereinkommen (Entwurf) lautet: „Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."

[995] Vgl. das *Draft Explanatory Memorandum* zum Cybercrime-Übereinkommen (Entwurf), Abs. 38.

[996] *Draft Explanatory Memorandum* zum Cybercrime-Übereinkommen (Entwurf), Abs. 44. „Hackern" geht es nach ihrem Selbstverständnis um die Erforschung der Sicherheit von Computern und Netzwerken, ohne dabei jemandem Schaden zuzufügen. Ein „Cracker" dagegen kompromittiert die Sicherheit von Computersystemen und netzwerken mit Schädigungsabsicht; s. dazu auch *Lessig*, S. 194.

[997] Art. 1707 NAFTA trägt den Titel „Protection of Encrypted ProgramCarrying Satellite Signals" und lautet:

„Within one year from the date of entry into force of this Agreement, each Party shall make it:

(a) a criminal offense to manufacture, import, sell, lease or otherwise make available a device or system that is primarily of assistance in decoding an encrypted program carrying satellite signal without the authorization of the lawful distributor of such signal; and

(b) a civil offense to receive, in connection with commercial activities, or further distribute, an encrypted program carrying satellite signal that has been decoded without the authorization of the lawful distributor of the signal or to engage in any activity prohibited under subparagraph (a).

Each Party shall provide that any civil offense established under subparagraph (b) shall be actionable by any person that holds an interest in the content of such signal."

Mit der Vorschrift sollte insbesondere dem in Mexiko weit verbreiteten Piratenieproblem im Satellitenfernsehbereich begegnet werden. Sie lehnt sich an eine Vorschrift des U.S.-amerikanischen Telekommunikationsrechts (47 U.S.C. § 605) an, s. *Neff/Smallson*, S. 46.

durch einen Privatnutzer erfaßt.[998] Anspruchsberechtiger ist nicht nur, wer das Satellitensignal aussendet, sondern jeder, der ein Interesse an den übertragenen Inhalten hat.[999] Die Vorschrift ist seit dem 1. Januar 1995 in Kraft.

bb) Europäischer Rechtsrahmen

(1) **Allgemeines.** Seit mehreren Jahren wird versucht, auf europäischer Ebene einen umfassenden rechtlichen Schutz technischer Schutzmaßnahmen zu etablieren.[1000] Dies soll durch mehrere Richtlinien erreicht werden, von denen die Richtlinie zum Urheberrecht in der Informationsgesellschaft die Wichtigste ist.[1001]

(2) **Art. 6 Richtlinie zum Urheberrecht in der Informationsgesellschaft.** Das urheberrechtliche Grünbuch der Kommission von 1995[1002] widmete technischen Identifizierungs- und Schutzsystemen einen eigenen Abschnitt. Im Folgedokument zum Grünbuch[1003] trat die Kommission für einen rechtlichen Schutz von technischen Schutz- und Identifizierungssystemen auf Gemeinschaftsebene ein. Im Dezember 1997 legte die Kommission dann einen ersten urheberrechtlichen Richtlinien-Vorschlag vor.[1004] Die weitere Entstehungsgeschichte dieser Richtlinie ist langwierig und verworren. Im Februar 1999 behandelte das Europäische Parlament den Vorschlag in erster Lesung und verlangte eine Reihe von Änderungen.[1005] Darauf legte die Kommission im Mai 1999 einen geänderten Vorschlag vor.[1006] Unter der Ägide des Rats der Europäischen Union folgten mehrere Entwürfe, die nicht veröffentlicht wurden, sondern nur bestimmten „interessierten Kreisen", insbesondere Lobbyisten-Gruppen, zugänglich gemacht wurden.[1007] Am 8. Juni 2000 wurde im COREPER des Rats der Europäischen Union (vgl. Art. 207 EGV) eine politische Einigung über den Richtlinienvorschlag erzielt.[1008] Am 28. September 2000 verabschiedete der Rat formell

---

[998] *Neff/Smallson*, S. 45; *Goolsby*, 4 NAFTA: L. & Bus. Rev. Am. 5, 29 (Autumn 1998).

[999] S. dazu auch *Goolsby*, 4 NAFTA: L. & Bus. Rev. Am. 5, 29 (Autumn 1998).

[1000] Einen historischen Überblick über die Initiativen der Kommission auf diesem Gebiet geben *Marly*, K&R 1999, 106, 107 f.; *Dusollier*, EIPR 1999, 285, 287 f.

[1001] Zu den anderen Richtlinien s. unten Teil 2, D I 2 b bb.

[1002] *Europäische Kommission*, KOM (95) 382 endg.

[1003] *Europäische Kommission*, KOM (96) 568 endg.

[1004] *Europäische Kommission*, KOM (97) 628 endg. Allgemein zum Richtlinienvorschlag s. *Hoeren*, MMR 2000, 515 ff.; *v. Lewinski*, GRUR Int. 1998, 637 ff.; *Flechsig*, ZUM 1998, 150; *Dietz*, ZUM 1998, 438 ff.; *Haller*, S. 77.

[1005] *Europäisches Parlament*, ABl. EG Nr. C 150 vom 28. 5. 1999, S. 171 ff.

[1006] *Europäische Kommission*, KOM (1999) 250 endg. vom 21. 5. 1999.

[1007] Wichtige Fassungen stammen u. a. vom Dezember 1999, März 2000 und vom Mai 2000. Zur Informationspolitik der Kommission und des Rats zu Recht äußerst kritisch *Hoeren*, NJW 2000, 3112, 3113; *ders.*, MMR 2000, 515.

[1008] *Hoeren*, MMR 2000, 515 ff.

einen Gemeinsamen Standpunkt zur Urheberrechts-Richtlinie.[1009] Im Januar und Februar 2001 wurde der Entwurf zur zweiten Lesung im Europäischen Parlament behandelt, zunächst im Auschuß für Recht und Binnenmarkt, später im Plenum. Wie umstritten der Richtlinienvorschlag im einzelnen war,[1010] zeigt sich daran, daß im Rechtsausschuß beinahe 200 Änderungsanträge gestellt wurden.[1011] Am 14. Februar 2001 nahm das Parlament die Richtlinie in zweiter Lesung mit neun Änderungen an.[1012] Außer einer Verkürzung der Umsetzungsfrist auf 18 Monate betreffen die Änderungen allesamt Kleinigkeiten. Nachdem die Kommission Ende März 2001 eine Stellungnahme zum Beschluß des Parlaments abgegeben hatte,[1013] nahm am 9. April 2001 auch der Rat der Europäischen Union die Richtlinie an. Sie trat mit ihrer Veröffentlichung im Amtsblatt am 22. Juni 2001 in Kraft.[1014] Der folgenden Untersuchung liegt die Endfassung der Richtlinie zugrunde; gerade die Vorschriften des rechtlichen Umgehungsschutzes haben im Lauf der Entstehung der Richtlinie deutliche Änderungen erfahren.[1015]

Nach Art. 6 Abs. 1 der Richtlinie zum Urheberrecht in der Informationsgesellschaft sehen die Mitgliedstaaten „einen angemessenen Rechtsschutz gegen die Umgehung wirksamer technischer Maßnahmen durch eine Person vor, der bekannt ist oder den Umständen nach bekannt sein muß, daß sie dieses Ziel verfolgt."[1016] Art. 6 Abs. 3 S. 1 der Richtlinie enthält eine Definition der „technischen Maßnahme". Die Umgehung einer technischen Maßnahme ist nur verboten, wenn die Maßnahme zum

---

[1009] *Rat der Europäischen Union*, ABl. EG Nr. C 344 vom 1. 12. 2000, S. 1 ff.

[1010] Die Kritik an dem Richtlinienvorschlag und der Richtlinie in ihrer endgültigen Fassung ist teilweise durchaus berechtigt. Zum Richtlinienvorschlag in der Fassung des Gemeinsamen Standpunkts des Rats zu Recht äußerst kritisch *Hugenholtz*, EIPR 2000, 499 ff. („The Directive is a badly drafted, compromise-ridden, ambiguous piece of legislation", S. 500); *Vinje*, EIPR 2000, 551 ff. („The initial Commission proposal for the Copyright Directive was seriously flawed, and the text has become even more dramatically defective as it has made its way through the legislative process", S. 551).

[1011] S. *Europäisches Parlament*, Dok. PE 298.368/5–197 vom 17. 1. 2001.

[1012] *Europäisches Parlament*, Dok. PE 300.203 vom 14. 1. 2001, S. 7 ff.

[1013] *Europäische Kommission*, KOM (2001) 170 endg. vom 29. 3. 2001.

[1014] 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, ABl. EG Nr. L 167 vom 22. 6. 2001, S. 10 ff. Einen Überblick über die Richtlinie in der endgültigen Fassung gibt *Kröger*, CR 2001, 316 ff.

[1015] Zu früheren Fassungen der Umgehungsvorschriften s. u. a. *Wand*, S. 93 ff.; *Bechtold* in: Hoeren/Sieber (Hrsg.), Teil 7.11, Rdnr. 36 ff.; *Koelman*, EIPR 2000, 272 ff.; *v. Lewinski*, GRUR Int. 1998, 637, 641 f.; *Freytag*, MMR 1999, 207, 208; *Hoeren*, MMR 2000, 515, 519; *Marly*, K&R 1999, 106, 110f.; zur Entstehungsgeschichte s. a. *Kröger*, CR 2001, 316 f.

[1016] Dagegen hatte sich der ursprüngliche Kommissionsvorschlag 1997 nur auf Vorbereitungshandlungen, nicht auf die tatsächliche Umgehung bezogen; der Wortlaut war jedoch etwas unklar. S. dazu *Koelman*, EIPR 2000, 272 f.

Schutz von Urheberrechten, verwandten Schutzrechten oder dem Sui-Generis-Datenbankrecht, das in Deutschland in §§ 87a ff. UrhG verankert ist, eingesetzt wird, Art. 6 Abs. 3 S. 1. Anders als bei den WIPO-Verträgen ist der Schutz nicht auf Maßnahmen zum Schutz der Rechte von Urhebern, ausübenden Künstlern und Tonträgerherstellern beschränkt, sondern erfaßt neben dem Urheberrecht alle verwandten Schutzrechte.

Eine technische Maßnahme wird nur geschützt, wenn sie „wirksam" ist, Art. 6 Abs. 1 der Richtlinie. Die Definition der Wirksamkeit in Art. 6 Abs. 3 S. 2 ist äußerst weit und zählt beispielhaft die Zugangskontrolle, Verschlüsselung, Verzerrung sowie die Kopierkontrolle auf.[1017] Nach dieser beinahe tautologischen Definition ist nahezu jede technische Maßnahme „wirksam" im Sinne des Art. 6. Nach dem Wortlaut von Art. 6 Abs. 3 S. 2 ist es für die „Wirksamkeit" einer technischen Schutzmaßnahme unerheblich, ob die Schutzmaßnahme sehr einfach oder nur mit großem Aufwand umgangen werden kann. Solange die Schutzmaßnahme beispielsweise auf einem Verschlüsselungsverfahren beruht, handelt es sich um eine geschützte „wirksame" Schutzmaßnahme, sei dieses Verschlüsselungsverfahren wegen sehr kurzer Schlüssellängen auch noch so unsicher.[1018] Auf subjektiver Seite ist erforderlich, daß der Täter

[1017] Zu den technischen Grundlagen dieser Verfahren s. oben Teil 1, C I, und C VIII. Für die Wirksamkeit der Maßnahme trägt der Rechtsinhaber die Beweislast, s. Anm. 1 zu Art. 6 des ursprünglichen Richtlinien-Vorschlag Dezember 1997, *Europäische Kommission*, KOM (97) 628 endg. vom 10. 12. 1997, S. 37. Die Definition der „Wirksamkeit" einer technischen Maßnahme hat gegenüber dem ursprünglichen Entwurf 1997 starke Änderungen erfahren. Im ursprünglichen Kommissionsvorschlag 1997 war eine Maßnahme wirksam, wenn der geschützte Gegenstand nur durch Anwendung eines Zugangsverfahrens „verfügbar" ist. Es kam auf die wirksame Zugangskontrolle an; die englische Fassung verwendete den Begriff „accessible". Danach wären Mechanismen, die nur das Anfertigen von Kopien verhindern und nicht den Zugang im engeren Sinne kontrollieren, nicht erfaßt gewesen; s. *Dusollier*, EIPR 1999, 290; *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 173 f. Im geänderten Kommissionsvorschlag 1999 mußte entweder der Zugang oder die Nutzung des Schutzgegenstandes durch einen Schutzmechanismus kontrolliert werden. In der endgültigen Fassung werden nur noch Maßnahmen erfaßt, die die *Nutzung* kontrollieren. Maßnahmen zur Zugangskontrolle wurden absichtlich gestrichen, da „Fragen betreffend den Zugang zu Werken oder sonstigen Schutzgegenständen außerhalb des Bereichs des Urheberrechts liegen", Begründung Nr. 45, *Rat der Europäischen Union*, ABl. EG Nr. C 344 vom 1. 12. 2000, S. 1, 20. S. zum ganzen ausführlich *Koelman*, EIPR 2000, 272, 275 f. Ganz aufgelöst ist der Konflikt zwischen Nutzungs- und Zugangskontrolle auch in der endgültigen Fassung nicht; in Art. 6 Abs. 3 und 4 kommt das Wort „Zugangskontrolle" weiterhin vor. Zur fragwürdigen Abgrenzung zwischen Zugangs- und Nutzungskonttrolle s. unten Teil 2, D I 2 b bb 3 b.

[1018] Aus technischer Sicht kann bei einer Schlüssellänge von 40 Bit heutzutage nicht mehr von einem sicheren Verschlüsselungsverfahren geredet werden. Dennoch ist ein solches Verfahren ein „wirksame" technische Maßnahme i. S. d. Art. 6 der Richtlinie zum Urheberrecht in der Informationsgesellschaft. Eine technische Maßnahme wird im übrigen auch nicht dadurch „unwirksam", daß sie geknackt wurde. Gerade auf diese Fälle ist der Schutz rechtlicher Umgehungsvorschriften ja zugeschnitten; s. a. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 318 (S.D.N.Y. August 17, 2000);

bei der Umgehung weiß oder wissen müßte, daß er eine unerlaubte Handlung vornimmt, Art. 6 Abs. 1. Insgesamt gewährt Art. 6 Abs. 1 der Richtlinie zum Urheberrecht in der Informationsgesellschaft einen sehr weiten Umgehungsschutz technischer Schutzmaßnahmen.[1019]

cc) Deutscher Rechtsrahmen

Im deutschen Recht bestehen schon de lege lata Ansatzpunkte, nach denen die Umgehung technischer Schutzmaßnahmen verboten sein kann. Daneben besteht ein Reformbedarf, der durch die internationale und europäische Entwicklung ausgelöst wurde.

(1) **Urheberrecht.** Die eigentliche Beseitigung einer technischen Schutzmaßnahme kann eine unberechtigte Bearbeitung im Sinne der §§ 23, 69 c Nr. 2 S. 1 UrhG sein.[1020] Wenn die technische Maßnahme und das zu schützende Werk ein Computerprogramm im Sinne des § 69 a UrhG sind, so ist nicht nur die Veröffentlichung oder Verwertung des Werks ohne technische Schutzmaßnahme, sondern schon die Beseitigung der Maßnahme an sich verboten.[1021] Daneben kann die eigentliche Umgehung einer technischen Schutzmaßnahme zu unerlaubten Vervielfältigungshandlungen führen. Sie kann im Einzelfall nach den Grundsätzen der adäquaten Kausalität auch eine Vorbereitungshandlung für spätere unberechtigte Nutzungshandlungen durch Dritte sein. In beiden Fällen führt dies zu Unterlassungs- und Schadensersatzansprüchen nach § 97 Abs. 1 UrhG.[1022]

Das Bundesjustizministerium hat im Juli 1998 den Diskussionsentwurf eines 5. Urheberrechts-Änderungsgesetzes vorgelegt.[1023] Dieser soll das

unten Fn. 1189. Es ist zwischen einer ex-ante- und einer ex-post-Betrachtung zu unterscheiden: Daß ein Schutzsystem ex post geknackt worden ist, schließt nicht aus, daß es ex ante wirksam war, *Hoeren*, MMR 2000, 515, 520. Für die zweite Lesung der Richtlinie im Europäischen Parlament wurden in dessen Rechts- und Binnenmarktausschuß mehrere Änderungsanträge eingebracht, die die Trennung zwischen der ex-ante- und ex-post-Betrachtung deutlicher in der Richtlinie verankern wollten, s. Änderungsanträge 163–166, *Europäisches Parlament*, Dok. PE 298.368/5–197 vom 17. 1. 2001, S. 101–104. Das Plenum des Parlaments übernahm diese Änderungsanträge jedoch nicht.

[1019] Ebenso *Vinje*, EIPR 2000, 551, 555. Zu den Schrankenbestimmungen des Art. 6 Abs. 4 s. unten Teil 4, D II 3 a aa.

[1020] OLG Karlsruhe, CR 1996, 341 m. Anm. *Raubenheimer*; OLG Düsseldorf, CR 1997, 337; *Hoeren*, MMR 2000, 515, 520; *Raubenheimer*, CR 1996, 69, 76; *Wand*, GRUR Int. 1996, 897, 903 f.; *Dusollier*, EIPR 1999, 285, 286; *Bechtold* in: Hoeren/Sieber (Hrsg.), Teil 7.11, Rdnr. 58; ebenso für die EU-Computerrichtlinie *Kaestner*, S. 9.

[1021] Vgl. den unterschiedlichen Wortlaut von § 23 S. 1 und § 69 c Nr. 2 S. 1 UrhG sowie OLG Karlsruhe, CR 1996, 341 m. Anm. *Raubenheimer*.

[1022] S. a. *Raubenheimer*, CR 1996, 76; *Dusollier*, EIPR 1999, 286.

[1023] *Bundesministerium der Justiz*, Entwurf 5. UrhGÄndG; s. dazu auch *Schöfisch* in: Prütting et al., S. 23 ff.; Wand, S. 163 ff.; Marly, K&R 1999, 106, 108 f. Dieser Entwurf baut u. a. auf dem vom Bundesjustizministerium in Auftrag gegebenen Gut-

deutsche Recht – unter Beachtung der europäischen Entwicklungen – an die Vorgaben der WIPO-Verträge 1996 anpassen.[1024] Nachdem die europäische Richtlinie zum Urheberrecht in der Informationsgesellschaft verabschiedet worden ist, ist nun zu erwarten, daß in in nächster Zeit ein neuer Entwurf eines 5. Urheberrechts-Änderungsgesetzes vorgelegt werden wird.[1025] Da die Vorschriften zum rechtlichen Umgehungsschutz in der Richtlinie seit 1998 stark umgestaltet wurden, ist davon auszugehen, daß der neue Entwurf eines 5. Urheberrechts-Änderungsgesetzes in diesem Bereich ebenfalls stark verändert werden wird.[1026] Dennoch soll im folgenden ein kurzer Überblick über den Diskussionsentwurf in der Fassung vom Juli 1998 gegeben werden. Der Schutz gegen die tatsächliche Umgehung technischer Maßnahmen soll in einem neuen § 96 a UrhG-E verankert werden:

> „Technische Vorrichtungen und Maßnahmen, einschließlich von Computerprogrammen, die zum Schutz vor einer Verletzung eines nach diesem Gesetz geschützten Rechts dienen, dürfen ohne Erlaubnis des Rechtsinhabers nicht umgangen, beseitigt, zerstört oder sonst unbrauchbar gemacht werden."

Die Vorschrift will für alle Werkarten und sonstigen geschützten Gegenstände des UrhG ein einheitliches Umgehungsverbot schaffen.[1027] Es handelt sich um ein Schutzgesetz i. S. d. § 823 Abs. 2 BGB.[1028]

(2) **Strafrecht.** Die Umgehung technischer Schutzmaßnahmen kann eine strafbare Handlung sein. Dies hängt allerdings sehr von den technischen Gegebenheiten und der Art der Umgehungshandlung ab. Hier sollen mögliche Straftatbestände nur erwähnt werden. Nutzt eine Person ein Werk, nachdem sie technische Schutzmaßnahmen entfernt hat, so kann darin ein Computerbetrug zu Lasten des Anbieters i. S. d. § 263 a StGB liegen.[1029] Auch kann ein Erschleichen von Leistungen im Sinne des § 265 a Abs. 1 1. Alt. StGB vorliegen.[1030] Schließlich kann das Manipulieren von technischen Schutzmaßnahmen als Datenveränderung im Sinne des § 303 a

---

achten von *Schricker, Dreier, Katzenberger* und *v. Lewinski*, veröffentlicht als *Schricker* (Hrsg.), Urheberrecht auf dem Weg zur Informationsgesellschaft, sowie dem Zweiten Zwischenbericht der Enquete-Kommission „Zukunft der Medien" des Deutschen Bundestages aus dem Jahr 1997 auf.

[1024] *Bundesministerium der Justiz*, Begründung zum 5. UrhGÄndG-Entwurf, S. 2 f.

[1025] S. dazu schon *Bundesministerium der Justiz*, Begründung zum 5. UrhGÄndG-Entwurf, S. 3.

[1026] Gerade die Formulierung der Umgehungsvorschrift des § 96 a UrhG-E wurde im Diskussionsentwurf 1998 noch nicht als endgültig betrachtet, s. *Schöfisch* in: Prütting et al., S. 23, 26.

[1027] *Bundesministerium der Justiz*, Begründung zum 5. UrhGÄndG-Entwurf, S. 23.

[1028] *Bundesministerium der Justiz*, Begründung zum 5. UrhGÄndG-Entwurf, S. 24.

[1029] S. dazu *Dressel*, MMR 1999, 390, 392; kritisch *Beucher/Engels*, CR 1998, 101, 104.

[1030] *Beucher/Engels*, CR 1998, 101, 104 f.; *Dressel*, MMR 1999, 390, 394.

StGB strafbar sein.[1031] Daneben kann im Einzelfall auch das urheberrechtliche Nebenstrafrecht der §§ 106 ff. UrhG eingreifen.[1032]

dd) U.S.-amerikanischer Rechtsrahmen

In den USA werden Überlegungen zum rechtlichen Schutz technischer Schutzmaßnahmen seit den 80er Jahren angestellt.[1033] Heute sind entsprechende Vorschriften über mehrere Gesetze verstreut, von denen der „Digital Millennium Copyright Act" aus dem Jahr 1998 das wichtigste Gesetz ist.

(1) Digital Millennium Copyright Act (DMCA)

(a) Allgemeines. Im September 1995 veröffentlichte eine Arbeitsgruppe der U.S.-Regierung einen Bericht mit dem Titel „Intellectual Property and the National Information Infrastructure".[1034] Darin wurde ein rechtlicher Umgehungsschutz technischer Schutzmaßnahmen gefordert.[1035] Dadurch und durch die WIPO-Verträge 1996 veranlaßt, erließ der U.S.-Kongreß den sogenannten „Digital Millennium Copyright Act" (DMCA), der am 28. Oktober 1998 in Kraft getreten ist.[1036] Das Gesetz enthält neben Haftungsregelungen für Online-Diensteanbieter, neuen Schrankenregelungen – unter anderem für das sogenannte „Webcasting" von Internet-Radioanstalten – und einem neuen Designschutzrecht[1037] auch Vorschriften zum rechtlichen Schutz von DRM-Komponenten.[1038] Diese Vorschriften sind für eine Untersuchung von DRM-Systemen – neben der allgemeinen Bedeutung der USA für den E-Commerce – deshalb von Bedeutung, weil sie weltweit den ersten umfassenden Versuch einer Regelung technischer Schutzmaßnahmen darstellen, der in Kraft getreten ist.

1031 Vgl. allgemein *Sieber* in: Hoeren/Sieber (Hrsg.), Teil 19, Rdnr. 424 f.

1032 S. allgemein *Sieber* in: Hoeren/Sieber (Hrsg.), Teil 19, Rdnr. 451 ff; zum Pay-TV-Bereich s. *Dressel*, MMR 1999, 392 f.; *Beucher/Engels*, CR 1998, 103; kritisch *Wand* in: Lehmann (Hrsg.), S. 35, 51.

1033 *U.S. Congress, Office of Technology Assessment*, Intellectual Property Rights in an Age of Electronic and Information, S. 23 ff.

1034 *Information Infrastructure Task Force*, Intellectual Property and the National Information Infrastructure.

1035 *Information Infrastructure Task Force*, S. 230 ff. Die damals vorgeschlagene Regelung erfaßte jedoch nur vorbereitende Handlungen, nicht die tatsächliche Umgehung technischer Schutzmaßnahmen, s. *ebda.*, Appendix 1, S. 6.

1036 Public Law 105–304, 112 Stat. 2860. Einen Überblick über die Gesetzgebungsgeschichte geben <http://www.hrrc.org/html/ DMCA-leg-hist.html> und <http://eon.law.harvard.edu/openlaw/DVD/dmca>.

1037 Dabei geht es um einen Designschutz für Schiffsrümpfe (!).

1038 In der amerikanischen Literatur dazu sehr ausführlich *N. B. Nimmer/D. Nimmer*, § 12A und § 12B; *Goldstein*, Copyright, § 5.16 ff., S. 5:241 ff; *D. Nimmer*, 148 U. Penn. L. Rev. 673 ff. (2000); *ders.*, 16 J. Copyright Soc'y U.S.A. 401 ff. (1999); *Samuelson*, 14 Berkeley Tech. L. J. 519 (1999); *Ginsburg*, 23 Colum.-VLA J. L. & Arts 137 ff. (1999); in der deutschen Literatur zum DMCA im Überblick *Freytag*, MMR 1999, 207 ff.; ausführlich *Wand*, S. 218 ff.

Der rechtliche Umgehungsschutz ist in äußerst detaillierten[1039] und zugleich unübersichtlichen Vorschriften geregelt, die als neues Kapitel in den Copyright Act eingefügt wurden. Das Gesetz unterscheidet zwischen Maßnahmen, die den Zugang zu einem Werk kontrollieren (sogenannte „access control", dazu unten b) und Maßnahmen, die ein Verwertungsrecht schützen sollen, das dem Urheber nach dem Copyright Act zusteht (dazu unten c).[1040] Für diese zweite Kategorie hat sich der Begriff „usage control" eingebürgert.[1041] Hinsichtlich der rechtswidrigen Handlungen unterscheidet das Gesetz – wie auf europäischer Ebene – zwischen der Umgehungshandlung selbst und vorbereitenden Handlungen.[1042] Bei einer Verletzung des Umgehungsverbots sieht 17 U.S.C. § 1203 Schadensersatz- und Vernichtungsansprüche vor. Nach 17 U.S.C. § 1204 können Geldstrafen bis zu $ 500.000 und/oder Freiheitsstrafen von bis zu fünf Jahren verhängt werden.[1043]

(b) Zugangskontrolle. 17 U.S.C. § 1201 (a) (1) (A) S. 1 untersagt die tatsächliche Umgehung technischer Schutzmaßnahmen, die den Zugang zu einem urheberrechtlichen Schutzgegenstand wirksam kontrollieren.[1044] Die Definition, was unter einer wirksamen Zugangskontrolle zu verstehen ist, ist denkbar weit gefaßt, s. 17 U.S.C. § 1201 (a) (3) (B).[1045] Wie bei Art. 6 der europäischen Richtlinie zum Urheberrecht in der Informationsgesellschaft ist es für die „Wirksamkeit" einer technischen Schutzmaßnahme unerheblich, ob die Schutzmaßnahme sehr einfach

[1039] In einer amerikanischen Gesetzessammlung belegen die einschlägigen 17 U.S.C. §§ 1201–1205 insgesamt 16 Druckseiten.

[1040] Eine nützliche tabellarische Übersicht findet sich bei *D. Nimmer*, 148 U. Penn. L. Rev. 673, 690 (2000). Zu Abgrenzungsschwierigkeiten s. *Ginsburg*, 23 Colum.-VLA J. L. & Arts 140 ff. (1999). Zum Verhältnis von Verwertungsrechten und Nutzungs- bzw. Zugangskontrolle allgemein s. unten Teil 2, D I 2 b b 3 b.

[1041] Der Begriff wird beispielsweise von der *Library of Congress*, 65 Fed. Reg. 64556, 64568 (October 27, 2000), verwendet. Er ist jedoch nicht exakt, da 17 U.S.C. § 1201 (b) nicht technische Maßnahmen schützen, die jede denkbare „usage" eines Werks betreffen. Vielmehr schützt er nur technische Maßnahmen, die eine „usage" kontrollieren, die unter ein im Copyright Act geregeltes Verwertungsrecht (right of reproduction, right of distribution, right of public performance etc.) fällt. Auch nach U.S.-amerikanischem Verständnis verleiht das Urheberrecht dem Urheber nicht die Kontrolle über die Nutzung seiner Werke an sich, *Elkin-Koren*, 12 Berkeley Tech. L. J. 93, 106 (1997); *Patterson/Lindberg*, S. 187; *Lemley*, 75 Tex. L. Rev. 989, 1014 (1997). Zur gleichen Problematik im europäischen Recht s. unten Fn. 1121.

[1042] Zum Schutz gegen vorbereitende Handlungen s. unten Teil 2, D I 2 b dd 1.

[1043] Zu den Rechtsfolgen s. *N. B. Nimmer/D. Nimmer*, § 12A.11 ff., S. 12A-114 ff.

[1044] S. dazu *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 179 f.

[1045] Anschaulich *U.S. House of Representatives*, H.R. Rep. No. 105–551, Part 1, S. 17: „The act of circumventing a technological protection measure put in place by a copyright owner to control access to a copyrighted work is the electronic equivalent of breaking into a locked room in order to obtain a copy of a book."

oder nur mit großem Aufwand umgangen werden kann.[1046] Die Umgehung einer technischen Schutzmaßnahme wird sehr weit definiert als „to descramble a scramble work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner", 17 U.S.C. § 1201 (a) (3) (A).

Anders als die restlichen Vorschriften des „Digital Millennium Copyright Act" trat das Verbot der tatsächlichen Umgehung nach 17 U.S.C. § 1201 (a) (1) erst mit zweijähriger Verspätung am 28. 10. 2000 in Kraft. Der Kongreß hatte das U.S. Copyright Office der Library of Congress ermächtigt, während dieser Zeit eine Ausnahmeliste von Werkkategorieren zu erstellen, bei denen das Verbot der tatsächlichen Umgehung nach 17 U.S.C. § 1201 (a) (1) nicht greifen soll, 17 U.S.C. § 1201 (a) (1) (B) – (E). Dadurch sollte urheberrechtlichen Schrankenbestimmungen Rechnung getragen werden.[1047]

(c) **Nutzungskontrolle.** Anders als bei Zugangskontrollmaßnahmen existiert bei technischen Maßnahmen zur Nutzungskontrolle kein Verbot der tatsächlichen Umgehungshandlung. Nach Ansicht des Gesetzgebers war dies unnötig, da in diesen Fällen das herkömmliche Urheberrecht mit seinen Verwertungsrechten eingreife.[1048] Der „Digital Millennium Copyright Act" verbietet bezüglich technischer Maßnahmen zur Nutzungskontrolle nur vorbereitende Handlungen.[1049]

(2) **Sonstige Vorschriften.** Seit den späten 70er Jahren gibt es in den USA gerichtliche Auseinandersetzungen über den unberechtigten Empfang verschlüsselter Pay-TV-Programme.[1050] Seit 1984 ist es nach einer kommunikationsrechtlichen Vorschrift (47 U.S.C. § 605) verboten, verschlüsselte Satellitenfernseh-Programme ohne Berechtigung zu empfangen.[1051] Eine

---

[1046] Die Verwendung einer 40-Bit-Verschlüsselung bei CSS ist daher eine Schutzmaßnahme, die den Zugang „wirksam" kontrolliert, Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317 f. (S.D.N.Y. August 17, 2000). S. dazu auch RealNetworks, Inc. v. Streambox, Inc., 2000 WL 127311, S. 9 (W.D.Wash. 2000).

[1047] S. dazu unten Teil 4, D II 3 c aa, und im Überblick *Bechtold* in: Hoeren/Sieber (Hrsg.), Teil 7.11, Rdnr. 71.

[1048] S. den Bericht des Rechtsausschusses des U.S.-Senats, S. Rep. No. 105–190, 105th Cong., 2d Sess. (May 11, 1998), S. 12; s. a. *D. Nimmer*, 148 U. Penn. L. Rev. 673, 690 (2000); *N. B. Nimmer/D. Nimmer*, § 12A.03[D][3], S. 12A-32 f.; *Freytag*, MMR 1999, 207, 208. Die *Library of Congress*, 65 Fed. Reg. 64556, 64557 (October 27, 2000), und *Goldstein*, Copyright, § 5.17.2, S. 5:248, geben als Grund an, daß dadurch urheberrechtliche Schrankenbestimmungen (insb. die „fair use defense") gewahrt bleiben sollten.

[1049] S. dazu unten Teil 2, D I 2 b dd 1 a.

[1050] S. dazu *Thorne/Huber/Kellogg*, § 10.9.3 f., S. 623 ff. m. w. N.; *Portin*, 33 Emory L. J. 825 ff. (1984); *Piscitelli*, 35 Fed. Comm. L. J. 1 (1983). HBO, einer der großen Pay-TV-Anbieter in den USA, begann 1986, sein Fernsehprogramm zu verschlüsseln.

[1051] S. dazu *Thorne/Huber/Kellogg*, § 10.9.4, S. 626 ff.; *Ferris/Lloyd*, § 26.02[1], S. 26–4 ff.; *DeBaun*, 34 UCLA L. Rev. 445 (1986); *Haymer*, 20 Loy. L. A. L. Rev. 145,

weitere einschlägige Vorschrift ist 47 U.S.C. § 553 (a) (1), die das unberechtigte Abhören von Übertragungen über ein Kabelnetzwerk verbietet.[1052] In den einzelnen Bundesstaaten bestehen besondere Vorschriften gegen den unberechtigten Empfang von Pay-TV-Programmen.[1053] Im Einzelfall kann eine Vielzahl allgemeiner Vorschriften des Bundes- oder Landesrechts eingreifen, die in der Praxis jedoch allenfalls eine untergeordnete Rolle spielen.[1054]

Aus den USA sind auch Vorgehensweisen bekannt, bei denen sich die Entwickler technischer Schutzmaßnahmen vor einer Umgehung ihrer Schutzmaßnahmen durch das Patentrecht schützen wollen. So ließ sich das Unternehmen Macrovision, dessen analoge Kopierschutzmechanismen in über 2,5 Milliarden Videokassetten weltweit eingesetzt werden,[1055] nicht nur die Kopierschutzmechanismen patentieren, sondern erhielt auch Patente auf technische Verfahren, mit denen der Kopierschutz umgangen werden kann. Damit hat Macrovision eine Möglichkeit, gegen

161 ff. (1986); *Wand*, S. 214 ff. Die Vorschrift behandelt noch eine Vielzahl anderer Fälle des unberechtigten Abhörens fremder Kommunikation. Sie greift auch ein, wenn die übertragenen Daten nicht mit technischen Schutzmaßnahmen geschützt sind. Nur im Fall des 47 U.S.C. § 605 (a) S. 3 („No person not being entitled thereto shall receive […] any […] communication by radio and use such communication (or any information therein contained) for his own benefit […]") i. V. m. 47 U.S.C. § 605 (b) („The provisions of subsection (a) of this section shall not apply to the interception or receipt by any individual […] of any satellite cable programming for private viewing if (1) the programming involved is not encrypted; […]") stellt die Vorschrift explizit auf das Abhören verschlüsselter Übertragungen ab; s. dazu auch *Ferris/Lloyd*, § 26.02[1][c][ii], S. 26–12 ff. 47 U.S.C. § 605 entspricht seit einer Umnumerierung durch den Cable Communications Policy Act von 1984 dem § 705 Communcations Act; s. dazu *Thorne/Huber/Kellogg*, § 10.9.4, S. 626 Fn. 35. Es ist streitig, ob 47 U.S.C. § 605 neben Satellitenfernsehen auch auf Kabelfernsehen anwendbar ist oder ob in diesen Fällen nur 47 U.S.C. § 553 greift, s. International Cablevision, Inc. v. Sykes, 75 F.2d 123, 129 ff. (2d Cir. 1996).

[1052] Die Vorschrift greift unabhängig davon ein, ob die Kabelsendung mit technischen Schutzmaßnahmen versehen ist oder nicht. S. dazu *Thorne/Huber/Kellogg*, § 10.10.2, S. 635 ff.; *Ferris/Lloyd*, § 26.02[2], S. 26–19 ff.; *Haymer*, 20 Loy. L. A. L. Rev. 145, 155 ff. (1986). 47 U.S.C. § 553 entspricht seit einer Umnumerierung im Jahr 1984 dem § 633 Communications Act.

[1053] S. dazu die Aufzählung in *Ferris/Lloyd*, § 26.03[1], S. 26–31 ff. Viele dieser Vorschriften unterscheiden nicht danach, ob die übertragenen Programme mit technischen Schutzmaßnahmen versehen sind oder nicht. Zur Rechtslage in Kalifornien s. *Haymer*, 20 Loy. L. A. L. Rev. 145, 166 ff. (1986).

[1054] So beispielsweise auf Bundesebene der „Federal Wire Interception and Interception of Oral Communications Act" (18 U.S.C. §§ 2510 ff., s. dazu United States v. Hux, 940 F.2d 314 (8th Cir. 1991)), der „Federal Trade Commission Act", weiterhin Vorschriften zum „Mail and Wire Fraud" (18 U.S.C. §§ 1341 ff.) sowie die „Access Device Statute" (18 U.S.C. § 1029). Auf Landesebene kann das „tort law" (insb. „conversion", „intentional interference with business relations" und „unfair competition") greifen. S. dazu insgesamt *Ferris/Lloyd*, § 26.02[3] ff., S. 26–21 ff.

[1055] Zu den technischen Grundlagen s. oben Fn. 503.

gewerbliche Raubkopierer mit patentrechtlichen Unterlassungs- und Schadensersatzansprüchen vorzugehen.[1056]

b) Verbot vorbereitender Handlungen

Neben der tatsächlichen Umgehung technischer Schutzmaßnahmen betreffen viele rechtliche Umgehungsvorschriften auch sogenannte „vorbereitende Handlungen", also insbesondere Herstellung und Vertrieb von Vorrichtungen, Technologien und Dienstleistungen, mit denen technische Schutzmaßnahmen später tatsächlich umgangen werden können.

aa) Völkerrechtlicher Rechtsrahmen

(1) **WIPO-Verträge.** Der Entwurf der beiden WIPO-Verträge[1057] verbot unter anderem Import, Herstellung und Vertrieb von Geräten oder das Angebot von Dienstleistungen, durch die technische Schutzmaßnahmen umgangen werden können.[1058] Dieser Entwurf, der auf einem Vorschlag der USA aufbaute,[1059] fand bei der diplomatischen Konferenz Ende 1996 wenig Unterstützung.[1060] In der endgültigen Fassung beziehen sich Art. 10 WCT und Art. 18 WPPT nicht mehr auf vorbereitende Handlungen, sondern nur noch auf die eigentliche Umgehungshandlung.[1061] Ein Umgehungsschutz gegen vorbereitende Handlungen fehlt auf dieser völkerrechtlichen Ebene.[1062]

(2) **Zugangskontroll-Übereinkommen des Europarats.** Schon im September 1991 hatte der Europarat seinen Mitgliedstaaten empfohlen, den gewerblichen Handel mit illegalen Pay-TV-Decodern zu untersagen.[1063] Im Oktober 2000 schloß der Europarat Verhandlungen über eine Europäische Konvention zum rechtlichen Schutz von Zugangskontrolldiensten

---

[1056] S. zum ganzen die Aussagen von *Gerry Brill*, Macrovision Corp., in einer Diskussion am Franklin Pierce Law Center 1998, abgedruckt in 39 IDEA 291, 322 f. (1999).

[1057] Allgemein zum WCT und WPPT s. oben Teil 2, D I 2 a aa 1.

[1058] Art. 13 Abs. 1 WCT Basic Proposal lautete: „Contracting Parties shall make unlawful the importation, manufacture or distribution of protection-defeating devices, or the offer or performance of any service having the same effect, by any person knowing or having reasonable grounds to know that the device or service will be used for, or in the course of, the exercise of rights provided under this Treaty that is not authorized by the rightholder or the law."

[1059] S. dazu *Samuelson*, 37 Va. J. Int'l L. 369, 409 ff. (1997); *Lai*, I.P.Q. 1998, 35, 43 f.

[1060] *Samuelson*, 37 Va. J. Int'l L. 369, 414 f. (1997); *Vinje*, EIPR 1999, 192, 201; *Lai*, I.P.Q. 1998, 35, 44.

[1061] Zum Schutz der Umgehungshandlung durch die WIPO-Verträge s. oben Teil 2, D I 2 a aa 1. *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 177 führen diese Einschränkung des Anwendungsbereichs auf die Lobbyarbeit der Unterhaltungselektronik-Industrie zurück. S. weiterhin *v. Lewinski* in: Hoeren/Sieber (Hrsg.), Teil 7.9, Rdnr. 109; *Lai*, I.P.Q. 1998, 35, 48.

[1062] A.A. *Wand*, S. 41, 54.

[1063] *Europarat*, Empfehlung Nr. R(91) 14, aktualisiert durch *Europarat*, Empfehlung Nr. R (95) 1.

ab, die seit Januar 2001 zur Unterzeichnung und Ratifizierung durch die Mitgliedstaaten ausliegt.[1064] Das Übereinkommen weitet im Grunde den Anwendungsbereich der Zugangskontrollrichtlinie der Europäischen Union[1065] auf die Mitgliedstaaten des Europarats aus.[1066] Der Schutzbereich des Übereinkommens ist – entsprechend der Zugangskontrollrichtlinie – sehr weit. Die Vertragsstaaten sollen neben zivilrechtlichen Ansprüchen strafrechtliche, verwaltungsrechtliche oder andere Sanktionen vorsehen, Art. 5 S. 1 Europäisches Zugangskontroll-Übereinkommen. Das Übereinkommen will die Anbieter von Fernseh-, Radio- und Informationsdiensten in ihren Entgeltinteressen schützen.[1067] Dagegen soll der Schutz von Rechteinhabern nicht Gegenstand des Übereinkommens sein.[1068] Für nähere Einzelheiten sei auf die folgenden Auführungen zur Zugangskontrollrichtlinie verwiesen.[1069]

(3) **Sonstige völkerrechtliche Regelungen.** Nach Art. 6 Abs. 1 lit. a Nr. 1 des europäischen Cybercrime-Übereinkommens (Entwurf)[1070] können die Vertragsstaaten Herstellung, Verkauf, Import und Vertrieb von Hard- oder Software strafrechtlich sanktionieren, die zu dem Zweck entwickelt wurden,[1071] eine der in Art. 2 bis 5 genannten Handlungen zu

[1064] European Convention on the Legal Protection of Services Based on, or Consisting of, Conditional Access vom 24. 1. 2001; erhältlich unter <http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=178>. Bis zum 1. 8. 2001 wurde das Übereinkommen von vier Staaten (Frankreich, Luxemburg, Moldavien, Norwegen, Rumänien, Schweiz) unterzeichnet.

[1065] S. dazu unten Teil 2, D I 2 b bb 3.

[1066] Zwischen zwei Mitgliedstaaten der Europäischen Union hat die Zugangskontrollrichtlinie Vorrang, Art. 11 Abs. 4 Europäisches Zugangskontroll-Übereinkommen.

[1067] Anmerkung 17 des *Explanatory Report*.

[1068] Anmerkung 18 S. 1 des *Explanatory Report* lautet: „Other reasons for encrypting services and controlling access, such as security, privacy or the protection of rights holders, are not dealt with unter the scope of the Convention." Dies ist zumindest mißverständlich. Zwar sind nach Art. 7 des Übereinkommens nur die Anbieter der Fernseh-, Radio- und Informationsdienste berechtigt, zivilrechtliche Schadensersatz- und Unterlassungsansprüche geltend zu machen. Diese Anbieter werden regelmäßig nicht die originären Rechteinhaber oder Urheber der übertragenen Inhalte sein. Aufgrund vertraglicher Beziehungen zwischen den Rechteinhabern und den Dienstebetreibern dient jedoch auch ein Schutz der Dienstebetreibern mittelbar den Schutzinteressen der Rechteinhaber.

[1069] S. dazu unten Teil 2, D I 2 b bb 3.

[1070] S. zu dem Übereinkommen allgemein oben Teil 2, D I 2 a aa 2.

[1071] Hier stellte sich das Problem von Allzweck-Vorrichtungen, die zu unterschiedlichen Zwecken eingesetzt werden können (sog. „dual-use"-Problematik). Die Vorschrift erfaßt nach ihrem Wortlaut „a device […] designed or adapted *primarily* for the purpose of committing any of the offences established in accordance with Article 2–5" (Hervorhebung durch den Verfasser). Es war heftig umstritten, ob nur solche Geräte erfaßt werden sollten, die *ausschließlich* für Handlungen i. S. d. Art. 2 ff. benutzt werden können. Letztlich entschied man sich für einen Kompromiß, bei dem solche Geräte erfaßt werden sollen, die *objektiv* für Handlungen i. S. d. Art. 2 ff. entwickelt wurden, s. dazu *Draft Explanatory Memorandum* zum Cybercrime-Übereinkommen (Entwurf), Abs. 73.

begehen.[1072] Da unter Art. 2 Cybercrime-Übereinkommen (Entwurf) der unberechtigte Zugang zu DRM-Systemen subsumiert werden kann,[1073] werden auch vorbereitende Handlungen im DRM-Bereich vom Cybercrime-Übereinkommen erfaßt. Auf subjektiver Seite ist erforderlich, daß der Anbieter der Hard- oder Software beabsichtigt, daß Abnehmer mit Hilfe seiner Produkte technische Schutzmaßnahmen umgehen werden. Nach Art. 6 Abs. 1 lit. b Cybercrime-Übereinkommen (Entwurf) ist auch schon der Besitz solcher Produkte zu bestrafen, solange sie zu einer der in Art. 2 bis 5 genannten Handlungen verwendet werden sollen.[1074]

Das NAFTA-Abkommen[1075] verpflichtet die Mitgliedstaaten in Art. 1707 (a) NAFTA, einen strafrechtlichen Schutz gegen das Herstellen, Importieren, Verkaufen oder sonstige Verfügbarmachen von Geräten oder Systemen zu gewährleisten, die hauptsächlich dazu bestimmt sind, das unberechtigte Entschlüsseln verschlüsselter Satellitenprogramme zu ermöglichen.[1076]

bb) Europäischer Rechtsrahmen

Vorbereitende Handlungen können nach europäischem Recht unter Vorschriften der Richtlinie zum Urheberrecht in der Informationsgesellschaft, der Computerprogramm- sowie der Zugangskontrollrichtlinie fallen.[1077]

(1) **Art. 6 Richtlinie zum Urheberrecht in der Informationsgesellschaft.** Nach Art. 6 Abs. 2 der Richtlinie zum Urheberrecht in der Informationsgesellschaft[1078] ist Herstellung, Einfuhr, Verbreitung, Verkauf, Vermie-

---

[1072] Die Vertragsstaaten sind allerdings nur hinsichtlich der Verbreitung von Paßwörtern u. ä. *verpflichtet*, solche strafrechtlichen Sanktionen zu erlassen, Art. 6 Abs. 3 Cybercrime-Übereinkommen (Entwurf).

[1073] S. dazu oben Teil 2, D I 2 a aa 2.

[1074] Dabei kann die Strafbarkeit auch erst ab dem Besitz einer Mehrzahl solcher Komponenten eingreifen, Art. 6 Abs. 1 lit. b S. 2 Cybercrime-Übereinkommen (Entwurf). Damit zielt dieVorschrift auf professionelle Händler ab.

[1075] S. dazu allgemein oben Teil 2, D I 2 a aa 2.

[1076] Der Wortlaut von Art. 1707 NAFTA findet sich oben unter Fn. 997.

[1077] Im Bereich der gewerblichen Schutzrechte setzen Hersteller zur Bekämpfung der verbreiteten Produkt- und Dienstleistungspiraterie ebenfalls zunehmend auf technische Vorkehrungen, um ihre Produkte bzw. Dienstleistungen zu schützen und als echt zu kennzeichnen. Dabei können Sicherheitshologramme, Chipkarten, Magnetsysteme, biometrische Verfahren, Spezialfarben, Mikrokennzeichnungen usw. eingesetzt werden. Im November 2000 kündigte die EU-Kommission in ihrem Folgedokument zum Grünbuch zur Produkt- und Dienstleistungspiraterie vom Oktober 1998 die Ausarbeitung einer „Richtlinie über Mittel zur Durchsetzung der Rechte des geistigen Eigentums" an, die – ähnlich der Richtlinie zum Urheberrecht in der Informationsgesellschaft – für den Bereich der gewerblichen Schutzrechte die Herstellung und Verteilung illegaler technischer Schutzvorkehrungen verbieten und Rechtsmittel gegen die Manipulation legaler Schutzvorkehrungen vorsehen soll, s. *Europäische Kommission*, KOM (2000) 789 vom 17. 11. 2000, S. 6.

[1078] S. dazu allgemein oben Teil 2, D I 2 a bb 2.

tung, Werbung und der „Besitz zu kommerziellen Zwecken“[1079] von „Vorrichtungen, Erzeugnissen oder Bestandteilen sowie die Erbringung von Dienstleistungen“ verboten.[1080] Die Vorrichtungen etc. müssen entweder als Umgehungshilfsmittel beworben werden (Art. 6 Abs. 2 lit. a) oder neben der Umgehung technischer Maßnahmen nur einen begrenzten wirtschaftlichen Zweck haben (Art. 6 Abs. 2 lit. b)[1081] oder zumindest hautpsächlich als Umgehungsmittel entworfen, hergestellt oder angepaßt worden sein (Art. 6 Abs. 2 lit. c). Für die subjektive Seite ergibt sich aus der Formulierung der einzelnen Alternativen, daß der Täter die Vorrichtung mit dem Ziel späterer Umgehung technischer Maßnahmen hergestellt oder beworben haben muß. Insgesamt handelt es sich um einen sehr weiten Schutz.[1082]

(2) **Computerprogrammrichtlinie.** Die Computerprogrammrichtlinie[1083] behandelt in Art. 7 Abs. 1 lit. c technische Schutzmaßnahmen.[1084] Die Vorschrift wurde durch § 69 f Abs. 2 UrhG ins deutsche Recht umgesetzt.[1085] Der Regelungsbereich von Art. 7 Abs. 1 lit. c Computerprogrammrichtlinie überschneidet sich mit Art. 6 Abs. 2 der Richtlinie zum Urheberrecht in der Informationsgesellschaft.[1086] Nach den Erwägungsgründen der Richtlinie zum Urheberrecht in der Informationsgesellschaft soll Art. 6 der Richtlinie nicht auf technische Schutzmaßnahmen bei Com-

[1079] Diese Klausel wurde erst relativ spät in die Richtlinien-Entwürfe eingeführt, s. *Bechtold* in: Hoeren/Sieber (Hrsg.), Teil 7.11, Rdnr. 43. Den Mitgliedstaaten steht es frei, zusätzlich auch den „privaten Besitz“ zu untersagen, Erwägungsgrund 49 der Richtlinie, ABl. EG Nr. L 167 vom 22. 6. 2001, S. 10, 14.

[1080] Im Rechts- und Binnenmarktausschuß des Europäischen Parlaments wurden für die zweite Lesung mehrere Änderungsanträge eingebracht, nach denen eindeutig auch die Verbreitung von *Informationen* über das Internet erfassen sollen, die zur Umgehung technischer Maßnahmen benützt werden können, s. Änderungsanträge 158–162, *Europäisches Parlament*, Dok. PE 298.368/5–197 vom 17. 1. 2001, S. 97–101. Anlaß für diese Anträge war die Umgehung des CSS-Systems und die anschließende Verbreitung von DeCSS über das Internet, s. dazu oben Teil 1, D II 3 b. Die Änderungsanträge wurden vom Plenum des Europäischen Parlaments jedoch nicht übernommen.

[1081] Durch diese Formulierung soll ein Verbot von Allzweck-Vorrichtungen verhindert werden, die zu unterschiedlichen Zwecken eingesetzt werden können (sog. „dual use“-Problematik); s. dazu *Wand*, S. 111 f., und Anm. 2 zu Art. 6 des ursprünglichen Richtlinien-Vorschlags, *Europäische Kommission*, KOM (97) 628 endg. vom 10. 12. 1997, S. 38; zu der damaligen Fassung kritisch *Dietz*, ZUM 1998, 438, 449; *Haller*, MR 1998, 65; vgl. auch den Bericht über eine Anhörung im Bundesjustizministerium, GRUR 1998, 545.

[1082] Ebenso *Vinje*, EIPR 2000, 551, 555. Zu den Schrankenbestimmungen des Art. 6 Abs. 4 s. unten Teil 4, D II 3 a aa.

[1083] S. oben Fn. 745.

[1084] S. dazu *Marly*, K&R 1999, 106, 107; *Dusollier*, EIPR 1999, 285, 286; *Wand*, S. 64 ff. In Entwürfen der Datenbank-Richtlinie fand sich zeitweise eine dem Art. 7 Abs. 1 lit. c Computerprogramm-Richtlinie entsprechende Regelung, die jedoch nicht in die Endfassung der Richtlinie übernommen wurde, s. *Gaster*, ZUM 1995, 740, 752.

[1085] Daher sei auf die dortigen Ausführungen verwiesen, s. unten Teil 2, D I 2 b cc 1.

[1086] Ebenso *Dusollier*, EIPR 1999, 285, 286.

puterprogrammen Anwendung finden, da diese ausschließlich in Art. 7 Abs. 1 lit. c Computerprogrammrichtlinie behandelt würden.[1087]

(3) Zugangskontrollrichtlinie

(a) Allgemeines. 1994 kündigte die Europäische Kommission die Erarbeitung eines Grünbuchs zum rechtlichen Schutz verschlüsselter Dienste an,[1088] das 1996 vorgelegt wurde.[1089] Im November 1998 verabschiedeten das Europäische Parlament und der Rat die Zugangskontrollrichtlinie.[1090] Die Richtlinie verbietet Herstellung, Vertrieb und Installierung von Vorrichtungen, mit denen zugangskontrollierte Dienste umgangen werden können. Die Richtlinie läßt den Mitgliedsstaaten einen weiten Umsetzungsspielraum; über eine Mindestharmonisierung kommt sie nicht hinaus.[1091]

Die Richtlinie schützt Fernseh- und Radiosendungen[1092] sowie „Dienste der Informationsgesellschaft". Ein „Dienst der Informationsgesellschaft" ist „jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung".[1093] Dabei dürfen die Vertragsparteien nicht gleichzeitig physisch anwesend sein; die Dienstleistung muß vollständig über Draht, Funk, auf optischem oder anderem elektromagnetischem Wege gesendet, weitergeleitet und emp-

---

[1087] Erwägungsgrund 50 der Richtlinie, ABl. EG Nr. L 167 vom 22. 6. 2001, S. 10, 14. In den Verhandlungen über die Richtlinie zum Urheberrecht in der Informationsgesellschaft war lange Zeit umstritten, ob die Computerprogramm- und Datenbankrichtlinien an den Art. 6 der neuen Richtlinie anzupassen seien. In diesem Zusammenhang stellt sich auch die Frage, inwieweit Computerprogramme von anderen urheberrechtlich geschützten Werken bei der zunehmenden Konvergenz überhaupt noch abgegrenzt werden können. So kann beispielsweise eine in HTML geschriebene WWW-Seite als Computerprogramm im urheberrechtlichen Sinne angesehen werden (s. *Bechtold*, ZUM 1997, 427, 428); auch bei den auf DVDs gespeicherten Inhalten (Videos etc.) wird diskutiert, ob es sich dabei nicht um Computerprogramme handelt, s. <http://www.zenadmen.com/anti1201/indextechisscts.htm> (Diskussionen auf der Mailingliste DVD-Discuss im Frühjahr 2000, <http://eon.law.harvard.edu/archive/dvd-discuss>); s. zum ganzen auch *Bechtold*, GRUR 1998, 18, 24; *ders.* in: Hoeren/Sieber (Hrsg.), Teil 7.11, Rdnr. 45.

[1088] *Europäische Kommission*, KOM (94) 347 endg., S. 10.

[1089] *Europäische Kommission*, KOM (96) 76 endg.

[1090] Richtlinie 98/84/EG des Europäischen Parlaments und des Rates vom 20. 11. 1998 über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten, ABl. EG Nr. L 320 vom 28. 11. 1998, S. 54 ff.; zur Entstehungsgeschichte s. *Helberger*, ZUM 1999, 295, 296; *Brenn*, ÖJZ 1999, 81; *Beucher/Engels*, CR 1998, 101, 102, 108 ff.; *Wand*, S. 77 ff.

[1091] Ebenso *Helberger*, ZUM 1999, 295, 305.

[1092] S. dazu *Wand*, S. 81 f.

[1093] Art. 1 Nr. 2 der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. 6. 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft, ABl. EG Nr. L 204 vom 21. 7. 1998, S. 37, geändert durch die Richtlinie 98/48/EG des Europäischen Parlaments und des Rates vom 20. 7. 1998, ABl. EG Nr. L 217 vom 5. 8. 1998, S. 18.

fangen werden.[1094] Somit fällt jeder kommerziell vertriebene Inhalt, der auf Abruf in elektronischer Form – beispielsweise über das Internet – übertragen wird, in den Anwendungsbereich der Richtlinie.[1095] Der Regelungsbereich der Zugangskontrollrichtlinie ist sehr weit.

Alle geschützten Dienste müssen gegen Entgelt erbracht werden, Art. 2 lit. a Zugangskontrollrichtlinie.[1096] Sie müssen einer Zugangskontrolle unterliegen, Art. 2 lit. a Zugangskontrollrichtlinie. Darunter ist „jede technische Maßnahme und/oder Vorrichtung" zu verstehen, „die den Zugang zu einem geschützten Dienst in verständlicher Form von einer vorherigen individuellen Erlaubnis abhängig macht", Art. 2 lit. b der Richtlinie. Die Richtlinie schützt nicht nur Dienste, die einer Zugangskontrolle unterliegen; auch die Zugangskontrolle selbst wird geschützt, „soweit sie als eigenständiger Dienst anzusehen ist", Art. 2 lit. a a. E. der Richtlinie.[1097] Welche Technologie zur Zugangskontrolle eingesetzt wird, ist irrelevant. Dies können Paßwörter, Smartcards, Verschlüsselungsverfahren[1098] und ähnliches sein. Damit erfaßt die Richtlinie auch technische DRM-Komponenten[1099] und betrifft weite Bereiche der über das Internet und DRM-Systeme verbreiteten Inhalte.[1100]

Es ist unerheblich, ob die Inhalte, die im zugangskontrollierten Dienst übertragen werden, urheberrechtlich geschützt sind oder nicht. Die Zugangskontrollrichtlinie schützt unmittelbar den zugangskontrollierten Dienst beziehungsweise die Zugangskontrolle an sich.[1101] Welchem Zweck die Zugangskontrolle dient, ist irrelevant.[1102] Anders als im Rah-

---

[1094] Art. 1 Nr. 2 der Richtlinie 98/34/EG, a. a. O., geändert durch Richtlinie 98/48/EG, a. a. O.

[1095] Als Beispiele mögen Video-on-demand, elektronisches Publizieren, Datenbanken und andere Online-Dienste dienen, *Dusollier*, EIPR 1999, 285, 290; *Wand*, S. 82 ff.; vgl. weiterhin *Helberger*, ZUM 1999, 295, 297, auch zu Abgrenzungsschwierigkeiten gegenüber Telekommunikationsdienstleistungen.

[1096] Zu Abgrenzungsproblemen bei geldwerten Informationen s. *Wand*, S. 85.

[1097] Eine Zugangskontrolle ist als „eigenständiger Dienst" anzusehen, wenn der Anbieter gleichsam an die Stelle des Anbieters des zugangskontrollierten Dienstes tritt und den Zugang in eigener Gesamtverantwortung verwaltet. Die Erbringung bloßer unterstützender und untergeordneter Dienste genügt nicht; s. a. *Wand*, S. 85 f., und *Helberger*, ZUM 1999, 295, 298 f., auch zu den damit verbundenen Auslegungsschwierigkeiten.

[1098] Zu den technischen Grundlagen von Verschlüsselungsverfahren und Paßwörtern s. oben Teil 1, C I, zu Smartcards s. oben Teil 1, C IV 1 b.

[1099] Ebenso *Dusollier*, EIPR 1999, 285, 288, 290; *Heide*, 15 Berkeley Tech. L. J. 903, 1013 Fn. 72 (2000).

[1100] Ebenso *Heide*, 15 Berkeley Tech. L. J. 903, 1044 (2000).

[1101] S. dazu auch *Heide*, 15 Berkeley Tech. L. J. 903, 1018 ff. (2000).

[1102] Zwar sah ein Entwurf der Richtlinie vor, den Schutz nur zu gewähren, wenn die Zugangskontrolle gerade die Entrichtung eines Entgelts sicherstellen sollte, s. Art. 1 lit. b des Vorschlages der *Europäischen Kommission*, KOM (97) 345 endg.; vgl. dazu *Helberger*, ZUM 1999, 297 f.; *Wand*, S. 79 *Brenn*, ÖJZ 1999, 81. Eine solche Einschränkung ist in der endgültigen Richtlinie aber nicht enthalten.

men der WIPO-Verträge und der Richtlinie zum Urheberrecht in der Informationsgesellschaft ist nicht erforderlich, daß die technische Schutzmaßnahme den Zugang „wirksam" kontrolliert.[1103]

Nach Art. 4 Zugangskontrollrichtlinie sind unter anderem Herstellung, Vertrieb, Verkauf, Besitz und Installierung „illegaler Vorrichtungen" verboten.[1104] Die Richtlinie ist nach dem Wortlaut des Art. 4 ausschließlich gegen das kommerzielle Geschäft mit illegalen Vorrichtungen gerichtet.[1105] Eine „illegale Vorrichtung" ist gemäß Art. 2 lit. e der Richtlinie „jedes Gerät oder Computerprogramm, […] das dazu bestimmt oder entsprechend angepaßt ist, um den Zugang zu einem geschützten Dienst in verständlicher Form ohne Erlaubnis des Diensteanbieters zu ermöglichen". Unter diese Definition fallen unter anderem Pay-TV-Piratenkarten und sonstige Hard- und Software-Decoder.

Die Richtlinie war bis zum 28. Mai 2000 in nationales Recht umzusetzen, Art. 6 Abs. 1 der Richtlinie.[1106] Dabei hat der Mitgliedstaat die Wahl, welche Sanktionen auf welchem Rechtsgebiet er vorsieht, Art. 5 Abs. 1 der Richtlinie.[1107] Deutschland hat die Richtlinie bisher noch nicht umgesetzt. Nach einem Mahnschreiben der Kommission stellte die Bundesrepublik in einer Mitteilung an die Kommission dar, daß eine Umsetzung im Fernsehsignalübertragungs-Gesetz (FÜG)[1108] erwogen werde.[1109]

[1103] Vgl. *Helberger*, ZUM 1999, 295, 297.

[1104] Die tatsächliche Umgehung der Zugangskontrolle wird von der Richtlinie nicht erfaßt.

[1105] Vgl. Erwägungsgründe 14 und 21 der Zugangskontrollrichtlinie, S. 55. Das Handeln aus nicht-gewerblichem Interesse – z. B. Hacken als Hobby – wird von der Richtlinie nicht erfaßt; kritisch *Helberger*, ZUM 1999, 295, 299 f.; *Beucher/Engels*, CR 1998, 101, 110; *Wand*, S. 87 f.; s. a. *Heide*, 15 Berkeley Tech. L. J. 993, 1005 (2000).

[1106] Zum Umsetzungsbedarf in Deutschland s. *Helberger*, ZUM 1999, 295, 302.

[1107] Es müssen keine strafrechtlichen Sanktionen vorgesehen werden, Erwägungsgrund 23 der Richtlinie, S. 55.

[1108] Gesetz über die Anwendung von Normen für die Übertragung von Fernsehsignalen, BGBl. I vom 14. 11. 1997, S. 2710.

[1109] *Bundesrepublik Deutschland*, Mitteilung; s. a. *Wand*, S. 186. Danach sollen – neben einer strafrechtlichen Sanktion – u. a. folgende Vorschriften in das FÜG eingefügt werden:

„§ 2 Begriffsbestimmung (Änderung und Ergänzung)

Nr. 4 ein Zugangsberechtigungssystem: jede technische Maßnahme oder Vorrichtung zur Kontrolle des Zugangs zu einem fortgeschrittenen Fernsehdienst

Nr. 6 illegale Vorrichtung: Jedes Gerät oder Computerprogramm, das dazu bestimmt oder entsprechend angepaßt ist, um die Überwindung eines Zugangsberechtigungssystems ohne Erlaubnis des Diensteanbieters zu ermöglichen.

§ 7 a Verbot des Inverkehrbringen illegaler Vorrichtungen (Ergänzung)

Verboten ist

a) Herstellung, Einfuhr, Vertrieb, Verkauf, Vermietung oder Besitz illegaler Vorrichtungen zu gewerblichen Zwecken;

b) Installierung, Wartung oder Austausch illegaler Vorrichtungen zu gewerblichen Zwecken;

In der Literatur wird über eine strafrechtliche Umsetzung nachgedacht.[1110] In Österreich wurde im Juli 2000 ein eigenes Zugangskontrollgesetz erlassen.[1111] Bei Verstößen sieht das österreichische Gesetz zivilrechtliche (Unterlassung, Beiseitigung, Schadensersatz), strafrechtliche und verwaltungsrechtliche Sanktionen vor.[1112] In Großbritannien wurde die Richtlinie in das Urheberrecht integriert.[1113] In anderen Mitgliedstaaten wird die Umsetzung in telekommunikationsrechtliche Vorschriften erwogen.[1114]

(b) Verhältnis zur Richtlinie zum Urheberrecht in der Informationsgesellschaft. Der Regelungsbereich der Zugangskontrollrichtlinie überschneidet sich mit Art. 6 Abs. 2 der Richtlinie zum Urheberrecht in der Informationsgesellschaft. In beiden Regelungen geht es um das rechtliche Verbot vorbereitender Handlungen, die der späteren Umgehung einer technischen Schutzmaßnahme dienen können.[1115] DRM-Komponenten können sowohl durch die Zugangskontrollrichtlinie als auch durch Art. 6 der Richtlinie zum Urheberrecht in der Informationsgesellschaft geschützt sein.[1116]

---

c) Einsatz der kommerziellen Kommunikation zur Förderung des Inverkehrbringen illegaler Vorrichtungen.

§ 10 Schadenersatz (Änderung)

(1) Anbieter von Waren, Rechten oder Dienstleistungen, die vorsätzlich oder fahrlässig gegen die Bestimmungen dieses Gesetzes verstoßen, sofern die Bestimmungen den Schutz des Geschädigten bezwecken, sind dem Geschädigten zum Schadenersatz verpflichtet.

(2) Der Schadenersatzanspruch umfasst zwischen Vertragspartnern pauschal 15 vom Hundert des vertraglich vereinbarten Entgeltes. Die Geltendmachung eines höheren Schadens und ein Anspruch auf eine den gesetzlichen Bestimmungen entsprechende Leistung bleiben unberührt."

[1110] So *Helberger*, ZUM 1999, 295, 302 ff.; *Dressel*, MMR 1999, 390 ff.; *Beucher/Engels*, CR 1998, 101, 103 ff.

[1111] Bundesgesetz über den Schutz zugangskontrollierter Dienste, BGBl. Republik Österreich Teil I vom 11. Juli 2000, S. 739–742. S. dazu *Brenn*, ÖJZ 1999, 81 ff.

[1112] Zu den zivilrechtlichen Ansprüchen s. §§ 5–9 Zugangskontrollgesetz. Der gewerbsmäßige Vertrieb und Verkauf von Umgehungsvorrichtungen wird mit Freiheitsstrafe bis zu zwei Jahren bestraft, § 10 Abs. 1 Zugangskontrollgesetz. Schließlich begeht eine „Verwaltungsübertretung", die mit einer Geldstrafe bis zu 15.000 Euro zu ahnden ist, wer gewerbsmäßig und wissentlich Umgehungsvorrichtungen installiert, wartet, austauscht oder durch Werbung zum Kauf solcher Vorrichtungen anregt, § 13 Abs. 1 Zugangskontrollgesetz.

[1113] Statutory Instrument 2000/1175. Danach wurden § 297A und 298 des Copyright, Designs and Patents Act 1988 mit Wirkung zum 28. 5. 2000 verändert. In § 298 Copyright, Designs and Patents Act 19988 fanden sich schon davor Vorschriften zur Umgehung technischer Schutzmaßnahmen, s. *Beucher/Engels*, CR 1998, 101, 107 f. *Heide*, 15 Berkeley Tech. L. J. 993, 1023 ff. (2000), faßt den Schutz der Zugangskontrollrichtlinie als ein leistungsschutzrechtliches „neighboring right" auf.

[1114] *Heide*, 15 Berkeley Tech. L. J. 993, 1045 (2000).

[1115] Zum Verhältnis beider Richtlinien allgemein s. *Heide*, 15 Berkeley Tech. L. J. 993, 1017 ff. (2000).

[1116] S. dazu *Dusollier*, EIPR 1999, 285, 288.

Da sich beide Regelungen in ihren Voraussetzungen und ihren Rechtsfolgen unterscheiden,[1117] stellt sich die Frage, in welchem Verhältnis die Regelungen zueinander stehen. Der europäische Gesetzgeber hat dieses Spannungsverhältnis gesehen. Grundsätzlich sind beide Regelungen nebeneinander anwendbar.[1118] Jedoch soll der Ansatzpunkt der Richtlinien jeweils ein anderer sein: Die Zugangskontrollrichtlinie biete einen Schutz vor dem unberechtigten *Zugang* zu zugangskontrollierten *Diensten* unabhängig von der Frage, ob die Dienste urheberrechtlich geschützte Werke enthalten oder nicht. Dagegen stelle Art. 6 der Richtlinie zum Urheberrecht in der Informationsgesellschaft gerade auf die unbefugte *Verwertung* eines geschützten *Werks* oder sonstigen Schutzgegenstands ab.[1119]

Es erscheint fraglich, ob dieser Abgrenzungsversuch tragfähig ist. Da die Grenzen zwischen einem Dienst und einem Werk äußerst fließend sind,[1120] ließe sich eine Abgrenzung danach nur erreichen, wenn zwischen

---

[1117] Ein wichtiger Unterschied ist beispielsweise die Regelung zu urheberrechtlichen Schrankenbesitmmungen in Art. 6 Abs. 4 der Richtlinie zum Urheberrecht in der Informationsgesellschaft. Eine vergleichbare Regelung existiert in der Zugangskontrollrichtlinie nicht. S. zu dieser Problematik unten Teil 4, D II 3 a bb.

[1118] Nach Erwägungsgrund 21 der Zugangskontrollrichtlinie läßt die Richtlinie die „Anwendung der gemeinschaftlichen Bestimmungen zum Schutz des geistigen Eigentums unberührt". In der Begründung zur Richtlinie zum Urheberrecht in der Informationsgesellschaft wird darauf hingewiesen, daß „die Fragen betreffend den Zugang zu Werken oder sonstigen Schutzgegenständen außerhalb des Bereichs des Urheberrechts liegen" und daher in dieser Richtlinie nicht behandelt würden; Begründung Nr. 45, *Rat der Europäischen Union*, ABL. EG Nr. C 344 vom 1. 12. 2000, S. 1, 20. Im Erwägungsgrund 35 des geänderten Richtlinienvorschlags zum Urheberrecht in der Informationsgesellschaft vom Mai 1999 fand sich noch eine dem Erwägungsgrund 21 der Zugangskontrollrichtlinie entsprechende Formulierung, *Europäische Kommission*, KOM (1999) 250 endg. vom 21. 5. 1999, S. 19. Dieser Erwägungsgrund wurde in späteren Fassungen des Richtlinienvorschlags gestrichen, s. *Bechtold* in: Hoeren/Sieber (Hrsg.), Teil 7.11, Rdnr. 53. S. zum ganzen auch *Heide*, 15 Berkeley Tech. L. J. 993, 1032 ff. (2000).

[1119] S. Anm. 4 zu Art. 6 des ursprünglichen urheberrechtlichen Richtlinienvorschlags, *Europäische Kommission*, KOM (97) 628 endg. vom 10. 12. 1997, S. 38, sowie die in Fn. 1118 erwähnten Nachweise. Art. 6 der Richtlinie zum Urheberrecht in der Informationsgesellschaft erfaßt in seiner endgültigen Fassung nach dem Wortlaut (Art. 6 Abs. 3 S. 2) nicht (mehr) die Kontrolle des Zugangs zu Werken, s. dazu oben Fn. 1017. Diese Trennung zwischen „access control" und „usage control" findet sich auch im U.S.-amerikanischen DMCA wieder: Während auf europäischer Ebene – grob vereinfacht – die „access control" in der Zugangskontrollrichtlinie und die „usage control" in der Richtlinie zum Urheberrecht in der Informationsgesellschaft geregelt sind, behandelt der DMCA beide Fragen: 17 U.S.C. § 1201 (a) (2) behandelt die „access control", 17 U.S.C. § 1201 (b) die „usage control"; s. dazu auch *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 174 f.

[1120] Sobald ein Werk im Internet zum Abruf bereitgehalten wird, kann es sich um einen Dienst im Sinne der Zugangskontrollrichtlinie handeln; s. a. *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 219.

dem Zugang zu Werken und der Nutzung von Werken[1121] sinnvoll unterschieden werden kann. Selbst wenn dies auf dogmatischer Ebene möglich sein sollte,[1122] ist zu fragen, ob angesichts der zunehmenden Konvergenz der Fernseh-, Telekommunikations- und Informationstechnologie der Zugang zu Werken von dessen Nutzung noch wirtschaftlich sinnvoll abgegrenzt werden kann.[1123] Im digitalen Umfeld geht jeder Nutzung eines Werks notwendigerweise der Zugang zu diesem Werk voraus. Unterliegt dieser Zugang einem Ausschließlichkeitsrecht,[1124] so kann darüber auch die anschließende Nutzungshandlung kontrolliert werden.[1125]

[1121] Unter einer Nutzung von Werken sollen in diesem Zusammenhang Handlungen verstanden werden, die einem der Verwertungsrechte unterfallen, die das Urheberrecht dem Urheber zuweist. Die reine Nutzung eines Werks – beispielsweise das Lesen eines Buches, das Anhören einer Schallplatte oder das Betrachten eines Videofilms – wird vom Urheberrecht traditionellerweise nicht erfaßt, BGH GRUR 1991, 449, 453 – Betriebssystem; BGH CR 1994, 275, 276 – Holzhandelsprogramm; *Marly*, Urheberrechtsschutz, S. 169; *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 189; *Guibault* in: Hugenholtz (Hrsg.), S. 125, 132; zur Frage, ob dies im digitalen Umfeld noch zutrifft s. *Bechtold*, GRUR 1998, 18, 26. Zur gleichen Problematik im Rahmen des U.S.-amerikanischen DMCA s. oben Fn. 1041.

[1122] Nach derzeitiger Rechtslage ist dies zu bezweifeln. In Computersystemen entsteht beim Zugang zu Werken regelmäßig eine Kopie im Arbeitsspeicher des Computers. Nach der herrschenden Meinung fallen solche Kopien unter das Vervielfältigungsrecht des Urhebers gemäß §§ 16, 69c Nr. 1 UrhG (s. oben bei Fn. 761). Dann ist mit jedem Zugang zu einem Werk aber zugleich eine urheberrechtlich relevante Nutzungshandlung verbunden. Die Abgrenzung zwischen Zugangs- und Nutzungshandlung würde damit schwierig; s. dazu *Bechtold*, GRUR 1998, 18, 26 f.; *Koelman*, EIPR 2000, 272, 274 ff.; *Bygrave/Koelman* in: Hugenholtz (Hrsg.), S. 59, 104 f.; *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 218 f.; *Ginsburg*, From Having Copies to Experiencing Works, S. 7 f.; *Wand*, S. 108 Durch die Umsetzung der Richtlinie zum Urheberrecht in der Informationsgesellschaft könnte sich die Rechtslage jedoch ändern und die Abgrenzung leichter fallen, da die Richtlinie in Art. 5 Abs. 1 bestimmte vorübergehende Vervielfältigungshandlungen vom Vervielfältigungsrecht des Urhebers zwingend ausnimmt; s. dazu oben bei Fn. 762. Zur Frage, ob schon im herkömmlichen Urheberrecht ein Recht auf Zugangskontrolle enthalten ist, s. *Heide*, 15 Berkeley Tech. L. J. 993, 1020 ff. (2000).

[1123] Ebenso kritisch *Dusollier*, EIPR 1999, 285, 288; *Vinje*, EIPR 1999, 192, 205 f.; *Bechtold* in: Hoeren/Sieber (Hrsg.), Teil 7.11, Rdnr. 53. Zu entstehenden Zugangs- und Nutzungsrechten allgemein s. *Bechtold*, GRUR 1998, 18, 26 f.; *Koelman*, EIPR 2000, 272, 274 ff.; *Olswang*, EIPR 1995, 215 ff.; *Ginsburg*, From Having Copies to Experiencing Works; *Heide*, 15 Berkeley Tech. L. J. 993, 1020 ff. (2000); *Dusollier*, EIPR 1999, 285, 291; *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 201 f.

[1124] Es ist nach der Zugangskontrollrichtlinie nicht unbedingt erforderlich, daß der Schutz als echtes Ausschließlichkeitsrecht ausgestaltet wird. In Österreich hat sich der Gesetzgeber jedoch für eine solche Lösung entschieden. Die vorliegende Aussage gilt aber auch, wenn es sich um kein Ausschließlichkeitsrecht im rechtstechnischen Sinne handelt.

[1125] *Ginsburg*, From Having Copies to Experiencing Works, S. 7; *dies.*, 23 Colum-VLA J. L. & Arts 137, 143 (1999); *Heide*, I.P.Q. 2000, 215, 221 f.; *ders.*, 15 Berkeley Tech. L. J. 993, 997 (2000); *Wand*, S. 108. Zu der daraus entstehenden Problematik in bezug auf urheberrechtliche Schrankenbestimmungen s. unten Teil 4, D II 3 a bb.

Ein weiterer Abgrenzungsversuch stellt auf den geschützten Adressatenkreis ab. Die Zugangskontrollrichtlinie schützt die Interessen der Anbieter zugangskontrollierter Dienste sowie der Erbringer von Zugangskontrolldiensten, Art. 2 lit. a und Art. 5 Abs. 2 1. Hs. Dagegen werden Urheber und Inhaber von Leistungsschutzrechten vom Schutz der Richtlinie nicht per se erfaßt.[1126] So schützt die Zugangskontrollrichtlinie beispielsweise den Betreiber eines technischen DRM-Systems, da er die Zugangskontrolle als „eigenständigen Dienst" im Sinne des Art. 2 lit. a Zugangskontrollrichtlinie betreibt.[1127] Der Betreiber eines technischen DRM-Systems genießt jedoch nicht unbedingt den Schutz des Art. 6 der Richtlinie zum Urheberrecht in der Informationsgesellschaft. Umgekehrt sind Urheber und Leistungsschutzberechtigte nach der Zugangskontrollrichtlinie nicht notwendigerweise anspruchsberechtigt.

Auch dieser Abgrenzungsversuch hat Schwächen. Einerseits genießen Rechteinhaber den Schutz der Zugangskontrollrichtlinie, wenn sie ihre Inhalte in verschlüsselter Form selbst anbieten.[1128] Andererseits ist zu beachten, daß in DRM-Systemen zwischen den Rechteinhabern und den Betreibern des technischen DRM-Systems regelmäßig vertragliche Beziehungen bestehen. Der Betreiber eines DRM-Zugangskontrolldienstes schützt seinen Dienst mittelbar auch, um die Interessen der Rechteinhaber zu schützen, mit denen er vertraglich verbunden ist und auf deren Inhalte er angewiesen ist. Unter wirtschaftlichen Gesichtspunkten dient die Zugangskontrollrichtlinie auch den Interessen der Rechteinhaber.[1129]

Insgesamt zeigt sich, daß DRM-Komponenten durch beide Richtlinien geschützt werden. Auch wenn sich der Ansatzpunkt beider Richtlinien unterscheidet, liegen zumindest in ihrer wirtschaftlichen Konsequenz weite Überschneidungen vor.

cc) Deutscher Rechtsrahmen

(1) **Urheberrecht.** Ein Schutz gegen vorbereitende Handlungen[1130] kann sich aus den geltenden Vorschriften des deutschen UrhG ergeben. Eine spezielle Vorschrift zu vorbereitenden Handlungen findet sich in § 69 f Abs. 2 UrhG. Mit § 69 f Abs. 2 UrhG wurde Art. 7 Abs. 1 lit. c der Computerprogrammrichtlinie umgesetzt.[1131] Dem Rechteinhaber steht ein

[1126] Dies war eines der umstrittensten Punkte während der Entstehung der Zugangskontrollrichtlinie, vgl. *Vinje*, EIPR 1999, 192, 205; *Heide*, 15 Berkeley Tech. L. J. 993, 1018 f. (2000); *Wand*, S. 89; kritisch *Helberger*, ZUM 1999, 295, 301.

[1127] Ebenso *Dusollier*, EIPR 1999, 285, 290.

[1128] Ebenso *Heide*, 15 Berkeley Tech. L. J. 993, 1013 (2000). In diesem Fall handelt es sich um einen „geschützten Dienst", der gegen Entgelt erbracht wird und einer Zugangskontrolle unterliegt, Art. 2 lit. a Zugangskontrollrichtlinie.

[1129] Ebenso *Dusollier*, EIPR 1999, 285, 290; *Heide*, 15 Berkeley Tech. L. J. 993, 1018 f. (2000). Zurückhaltender *Helberger*, ZUM 1999, 295, 301.

[1130] Zu diesem Begriff s. oben Teil 2, D I 2.

[1131] Zur Richtlinie s. oben Teil 2, D I 2 b bb 2. Zu § 69 f UrhG s. a. *Raubenheimer*, CR 1994, 129 ff; *Wand*, S. 144 ff.

Vernichtungsanspruch gegen den Eigentümer oder Besitzer von Mitteln zu, die allein dazu bestimmt sind, die unerlaubte Beseitigung oder Umgehung technischer Schutzmaßnahmen eines Computerprogramms zu erleichtern.[1132] Als technische Schutzmaßnahme wird jede Vorrichtung angesehen, die die Vervielfältigung oder Veränderung des Programms vereiteln soll oder sich gegen eine urheberrechtlich nicht genehmigte Art und Weise der Nutzung richtet.[1133] Darunter fallen sowohl Hardware- als auch Software-Vorrichtungen.[1134] Auch der Begriff des Mittels zur Beseitigung oder Umgehung des Programmschutzes ist äußerst weit.[1135] Es muß allerdings ausschließlich dazu bestimmt sein, den Programmschutz zu beseitigen oder zu umgehen.

Neben dieser speziellen computerrechtlichen Vorschrift kann sich ein Schutz gegen vorbereitende Handlungen aus allgemeinen urheberrechtlichen Vorschriften ergeben. Herstellung und Vertrieb von Umgehungsvorrichtungen verletzen urheberrechtliche Verwertungsrechte zwar nicht unmittelbar, ermöglichen aber deren Verletzung. Für einen Unterlassungs- oder Schadensersatzanspruch aus § 97 UrhG genügt ein adäquater Kausalzusammenhang zwischen Vorbereitungshandlung und Rechtsverletzung.[1136] Als Mitwirkung kann die Unterstützung eines eigenverantwortlich handelnden Dritten genügen, sofern der in Anspruch Genommene die rechtliche Möglichkeit zur Verhinderung dieser Handlung hatte.[1137] Der BGH hat eine adäquate Verursachung beispielsweise angenommen, wenn Tonband- oder Kopiergeräte zur Verfügung gestellt wurden, weil der bestimmungsgemäße Gebrauch – die Erstellung von Kopien – in der Regel einen Eingriff in die Rechte Dritter mit sich bringe.[1138] Daß diese Geräte im Einzelfall auch ohne Eingriff in Urheberrechte benutzt werden könnten, stehe nicht entgegen, solange sie auf eine Benutzung zugeschnitten seien und zu einem Gebrauch angeboten würden, der im Regelfall zu einem Eingriff in urheberrechtliche Befugnisse führen müsse.[1139] Jedoch

---

[1132] Über die Anforderungen der Computerprogrammrichtlinie hinaus wird auch der Besitz von Umgehungsvorrichtungen für private Zwecke erfaßt.

[1133] *Loewenheim* in: Schricker (Hrsg.), UrhG-Kommentar, § 69 f Rdnr. 9; *Bundesregierung*, BT-Drs. 12/4022 vom 18. 12. 1992, S. 1, 14 f.

[1134] *Loewenheim* in: Schricker (Hrsg.), UrhG-Kommentar, § 69 f Rdnr. 9; *Raubenheimer*, CR 1996, 69, 71.

[1135] *Vinck* in: Fromm/Nordemann (Hrsg.), § 69 f Rdnr. 3; *Loewenheim* in: Schricker (Hrsg.), UrhG-Kommentar, § 69 f Rdnr. 10.

[1136] BGH GRUR 1999, 418, 419 – Möbelklassiker; *Wild* in: Schricker (Hrsg.), UrhG-Kommentar, § 97 UrhG Rdnr. 35; *Nordemann* in: Fromm/Nordemann (Hrsg.), § 97 UrhG Rdnr. 16; *Wand* in: Lehmann (Hrsg.), S. 35, 49. Ausführlich *Wand*, S. 152 ff.

[1137] BGH GRUR 1999, 418, 419 – Möbelklassiker.

[1138] BGHZ 42, 118, 124 ff. – Personalausweise; BGH GRUR 1984, 54, 55 – Kopierläden; *Wild* in: Schricker (Hrsg.), UrhG-Kommentar, § 97 UrhG Rdnr. 37 m. w. N.

[1139] BGHZ 17, 266, 291 f. – Grundig-Reporter; BGH GRUR 1960, 340, 343 f. – Werbung für Tonbandgeräte.

seien Art und Umfang der Maßnahmen, die der Verletzte fordern kann, nach § 242 BGB zu bestimmen; es sei deren Zumutbarkeit und Erforderlichkeit zu untersuchen.[1140] In der Regel genüge ein Hinweis des Herstellers solcher Geräte auf die Möglichkeit der Urheberrechtsverletzung. In besonders gelagerten Fällen seien jedoch strengere Anforderungen an die erforderlichen Sicherungsmaßnahmen des Herstellers zu stellen.[1141]

Solange die bestimmungsgemäße Nutzung einer Vorrichtung zur Umgehung technischer Schutzmaßnahmen in DRM-Systemen regelmäßig zu einer Rechtsverletzung führt, kann das Bereitstellen dieser Vorrichtung Ansprüche auf Schadensersatz und Unterlassung nach § 97 Abs. 1 UrhG auslösen.[1142] Daneben kann sich aus § 99 i. V. m. § 98 UrhG ein verschuldensunabhängiger[1143] Anspruch auf Vernichtung oder Überlassung der Umgehungsvorrichtungen ergeben.[1144] Diese Ansprüche bestehen allerdings nicht, wenn die Umgehungsvorrichtungen in nicht unerheblichem Umfang auch für rechtmäßige Zwecke eingesetzt werden können.[1145]

Daneben wird erwogen, im Rahmen des geplanten 5. Urheberrechts-Änderungsgesetzes[1146] eine allgemeine Regelung bezüglich vorbereitender Handlungen im DRM-Bereich zu schaffen. Danach soll § 99 UrhG insofern erweitert werden, als sich der Vernichtungs- und Überlassungsanspruch auch auf Vorrichtungen erstreckt, die „zur rechtswidrigen Beseitigung, Zerstörung, sonstigen Unbrauchmachung oder Umgehung von technischen Mitteln im Sinne von § 96 a […]“ benutzt werden oder dazu bestimmt sind.[1147]

(2) **Wettbewerbsrecht.** Die Verbreitung von Umgehungsvorrichtungen kann auch zu wettbewersrechtlichen Ansprüchen führen. Bei Pay-TV-Programmen und Computerprogrammen entspricht es ständiger Rechtsprechung, daß der Vertrieb von Decodern, durch die das Programm

---

[1140] BGHZ 42, 118, 129 – Personalausweise; *Kuhlmann*, CR 1989, 177, 179. Zur Frage, ob sich durch die Möbelklassiker-Entscheidung des BGH (GRUR 1999, 418) die dogmatische Konstruktion des angestrebten Ergebnisses ändert, s. *Wand*, S. 158.

[1141] BGHZ 17, 266, 292 f. – Grundig-Reporter, unter Hinweis auf RGZ 146, 26, 29 – Saugrüssel.

[1142] *Wand* in: Lehmann (Hrsg.), S. 35, 50; *ders.*, GRUR Int. 1996, 897, 902; *Kuhlmann*, CR 1989, 177, 179. Zur Rechtslage in den USA s. im Überblick *Koelman/Helberger* in: Hugenholtz (Hrsg.), S. 165, 183.

[1143] *Wild* in: Schricker (Hrsg.), UrhG-Kommentar, § 97 UrhG Rdnr. 1.

[1144] Ebenso *Wand* in: Lehmann (Hrsg.), S. 35, 51; *ders.*, GRUR Int. 1996, 897, 903; vgl. *Bundesregierung*, BT-Drs. 12/4022 vom 18. 12. 1992, S. 1, 14. Dieser Anspruch erfaßt auch handelsübliche Geräte; die Entscheidung BGH ZUM 1988, 532, ist überholt, s. *Wild* in: Schricker (Hrsg.), UrhG-Kommentar, §§ 98/99 Rdnr. 5.

[1145] *Wand*, S. 158. Diese Einschränkung wird wichtig, wenn es um das Spannungsverhältnis zwischen technischen Schutzmaßnahmen und urheberrechtlichen Schrankenbestimmungen geht; s. dazu unten Teil 3, B II 3, und Teil 4.

[1146] S. dazu oben Teil 2, D I 2 a cc 1.

[1147] Zu § 96 a UrhG-E s. ebenfalls oben Teil 2, D I 2 a cc 1.

unberechtigterweise entschlüsselt werden kann, einen Verstoß gegen § 1 UWG in der Form des Behinderungswettbewerbs darstellen kann. Dabei nutze der Anbieter des Decoders die Leistung des Programmanbieters für eigene Zwecke aus.[1148] Eine inhärente Schwäche dieses Schutzes ist, daß rein private Handlungen ohne Verfolgung eines Geschäftszweckes nicht erfaßt werden. Dies ist insofern problematisch, als manche Internet-Nutzer das Knacken technischer Schutzmaßnahmen als bevorzugte Freizeitbeschäftigung betreiben und diesbezügliche Informationen ohne Erwerbsabsicht im Internet veröffentlichen.[1149]

(3) **Allgemeines Deliktsrecht.** Bei vorbereitenden Handlungen zur Umgehung technischer Schutzmaßnahmen kann eine Verletzung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb zu Schadensersatz- und Unterlassungsansprüchen nach §§ 823 Abs. 1, 1004 analog BGB sowie eine vorsätzliche sittenwidrige Schädigung nach § 826 BGB gegeben sein.[1150] Bei Verletzung von Schutzgesetzen kann auch § 823 Abs. 2 BGB eingreifen.[1151]

(4) **Strafrecht.** Herstellung und Vertrieb von Umgehungsvorrichtungen können als Beihilfe zu einer der oben[1152] genannten Straftaten strafbar sein.[1153] Das Auslesen von Dechiffrier-Schlüsseln und ähnlichem kann als Ausspähen von Daten nach § 202 a StGB strafbar sein.[1154] Je nach den Umständen des Einzelfalles mögen auch §§ 269, 270[1155] und § 274 StGB einschlägig sein. Herstellung und Vertrieb einer Umgehungsvorrichtung können nach § 17 Abs. 2 Nr. 1 und 2 UWG strafbar sein; der in einer DRM-Komponente enthaltene technische Schutz (Verschlüsselungsverfahren, Dechiffrier-Schlüssel etc.) kann ein Geschäfts- oder Betriebsge-

---

[1148] BGH CR 1996, 79 m. Anm. *Lehmann*; OLG München, WRP 1992, 661; OLG München, CR 1995, 663 – UNPROTECT; OLG München, CR 1996, 11; OLG Stuttgart, CR 1989, 685 m. Anm. *Lehmann*; OLG Frankfurt, NJW 1996, 264; OLG Düsseldorf, CR 1991, 352; gegen eine Verallgemeinerung dieser Entscheidungen *Marly*, K&R 1999, 110. S. weiterhin *Wand*, S. 158 ff. *Raubenheimer*, CR 1994, 264; *ders.*, NJW-CoR 1996, 174 f.; *ders.*, CR 1996, 69, 77 ff.; *Dressel*, MMR 1999, 390, 392; *Beucher/Engels*, CR 1998, 101, 106; *Hoeren*, MMR 2000, 515, 520; *Wand*, GRUR Int. 1996, 897, 903; *Kuhlmann*, CR 1989, 177, 182 f. Ebenso nach österreischem § 1 UWG OLG Wien, ecolex 1996, 612 f. (Urteil vom 20. 12. 1990).

[1149] Ebenso *Kaestner*, S. 7 f.; *Wand*, S. 161 f.

[1150] OLG Frankfurt, NJW 1996, 264, 265; *Wand* in: Lehmann (Hrsg.), S. 35, 52; *Beucher/Engels*, CR 1998, 101, 106.

[1151] Vgl. dazu *Beucher/Engels*, CR 1998, 101, 106.

[1152] S. Teil 2, D I 2 a cc 2.

[1153] S. dazu *Dressel*, MMR 1999, 390, 392; *Kuhlmann*, CR 1989, 177, 180.

[1154] Vgl. *Sieber* in: Hoeren/Sieber (Hrsg.), Teil 19, Rdnr. 417 ff.; *Beucher/Engels*, CR 1998, 101, 103 f. *Dressel*, MMR 1999, 390, 393 f.; kritisch *Helberger*, ZUM 1999, 295, 302 ff.

[1155] S. dazu *Beucher/Engels*, CR 1998, 101, 105; *Dressel*, MMR 1999, 390, 394 f.

heimnis im Sinne der §§ 17, 18 UWG darstellen.[1156] Auch im strafrechtlichen Bereich werden jedoch Gesetzesänderungen gefordert.[1157]

(5) **Sonstige Vorschriften.** Schließlich wird über eine Ergänzung des Fernsehsignalübertragungs-Gesetzes nachgedacht. Danach würden vorbereitende Handlungen zur Umgehung technischer Schutzmaßnahmen im Pay-TV-Bereich verboten. Durch diese Ergänzung soll die europäische Zugangskontrollrichtlinie in deutsches Recht umgesetzt werden.[1158]

dd) U.S.-amerikanischer Rechtsrahmen

In den USA bestehen mehrere Regelungen, die vorbereitende Handlungen zur Umgehung technischer Schutzmaßnahmen betreffen. Die wichtigsten dieser Regelungen finden sich im „Digital Millennium Copyright Act" von 1998.

(1) **Digital Millennium Copyright Act**

(a) **Zugangs- und Nutzungskontrolle.** Auch hinsichtlich vorbereitender Handlungen unterscheidet der „Digital Millennium Copyright Act" zwischen technischen Schutzmaßnahmen zur Zugangs- und zur Nutzungskontrolle.[1159] 17 U.S.C. § 1201 (a) (2) betrifft vorbereitende Handlungen im Bereich der Zugangskontrolle. Die Vorschrift untersagt unter bestimmten Voraussetzungen Herstellung und Vertrieb von Technologien, Produkten und Dienstleistungen, die hauptsächlich dem Zweck dienen, technische Schutzmaßnahmen zu umgehen, die den Zugang zu einem urheberrechtlich geschützten Werk wirksam kontrollieren. Falls dies nicht der hauptsächliche Zweck der Umgehungsvorrichtung ist, wird sie von dem Verbot dennoch erfaßt, wenn sie neben der Möglichkeit, technische Schutzmaßnahmen zu umgehen, nur einen begrenzten wirtschaftlichen Nutzen aufweist,[1160] oder wenn sie mit dem Wissen vermarktet wird, daß sie zur Umgehung einer technischen Zugangskontrolle eingesetzt werden wird.

17 U.S.C. § 1201 (b) (1) betrifft vorbereitende Handlungen im Bereich der Nutzungskontrolle. Danach sind Herstellung und Vertrieb von Umgehungsvorrichtungen verboten, die hauptsächlich dazu dienen, eine technische Schutzmaßnahme zu umgehen, die wirksam[1161] Handlungen

---

1156 S. dazu *Dressel*, MMR 1999, 390, 391 f.; *Beucher/Engels*, CR 1998, 101, 102; *Raubenheimer*, CR 1994, 264, 267 f.; *Kuhlmann*, CR 1989, 177, 183 f.; vgl. weiterhin *Sieber* in: Hoeren/Sieber (Hrsg.), Teil 19, Rdnr. 440 ff.; *Hefermehl*, § 17 UWG Rdnr. 9 m. w. N.; *Loewenheim* in: Schricker (Hrsg.), UrhG-Kommentar, vor §§ 69 a ff. UrhG, Rdnr. 14; OLG Frankfurt, NJW 1996, 264.

1157 *Dressel*, MMR 1999, 395; *Helberger*, ZUM 1999, 305, jeweils für den Pay-TV-Bereich.

1158 S. dazu oben bei Fn. 1109.

1159 S. zu dieser Unterscheidung oben Teil 2, D I 2 a dd 1 a.

1160 S. dazu *Ginsburg*, 23 Colum-VLA J. L. & Arts 137, 144 ff. (1999).

1161 Wie in anderen Regelungen werden an die Wirksamkeit der geschützten technischen Maßnahme keine hohen Anforderungen gestellt, s. 17 U.S.C. § 1201 (b) (2) (B).

schützt, die unter eines der urheberrechtlichen Verwertungsrechte (z. B. das Recht der Vervielfältigung) fallen.

Ähnlich den Abgrenzungsschwierigkeiten zwischen der europäischen Zugangskontrollrichtlinie und der Richtlinie zum Urheberrecht in der Informationsgesellschaft[1162] ist auch beim „Digital Millennium Copyright Act" die Abgrenzung zwischen der Zugangskontrolle nach 17 U.S.C. § 1201 (a) und der Nutzungskontrolle[1163] nach 17 U.S.C. § 1201 (b) unklar.[1164] Es gibt DRM-Komponenten, die gleichzeitig den Zugang zu digitalen Inhalten und dessen Nutzung kontrollieren.[1165] Auch ist unklar, was unter einer Zugangskontrolle im Sinne des 17 U.S.C. § 1201 (a) zu verstehen ist.[1166]

Daneben findet sich in 17 U.S.C. § 1201 (k) (1) (B) eine spezielle Vorschrift für Videorekorder und -kameras. Nach dieser Vorschrift dürfen

---

[1162] S. dazu oben oben Teil 2, D I 2 b bb 3 b.

[1163] Zur Unschärfe dieses Begriffs s. oben Fn. 1041.

[1164] S. *Ginsburg*, 23 Colum-VLA J. L. & Arts 137, 142 f. (1999). *Dies.*, From Having Copies to Experiencing Works, sieht 17 U.S.C. § 1201 (a) als neuartiges, eigenständiges Zugangskontrollrecht an.

[1165] Das bei DVDs verwendete Verschlüsselungs- und Authentisierungssystem CSS kontrolliert einerseits den Zugang zu Videoinhalten, damit aber gleichzeitig auch dessen Nutzung. Die *Library of Congress*, 65 Fed. Reg. 64556, 64568 (October 27, 2000) spricht diesbezüglich von einem „merger of access and usage control". Die Entscheidung Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. August 17, 2000) geht auf die Zwitterstellung von CSS als Zugangs- und Nutzungskontrolle nicht ein, sondern behandelt CSS ohne nähere Begründung schwerpunktmäßig als Zugangskontrolle, s. dort S. 316 Fn. 133.

[1166] Einerseits wird mit Hinweis auf die Entstehungsgeschichte des Gesetzes vertreten, daß unter „access" nur der *erstmalige* Zugriff auf einen Inhalt zu verstehen sei; habe der Nutzer einmal rechtmäßig Zugang zu dem Inhalt erhalten, so seien technische Schutzmaßnahmen, die die weiteren Zugriffe kontrollieren, nur als Nutzungskontrolle nach 17 U.S.C. § 1201 (b) geschützt; so *N. B. Nimmer/D. Nimmer*, § 12A.03[D][2], S. 12A-31; *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 175. Ebenso meint das *U.S. House of Representatives*, H.R. Rep. No. 105–551, Part 1, S. 18: „Paragraph (a)(1) [von 17 U.S.C. § 1201] does not apply to the subsequent actions of a person once he or she has obtained authorized access to a copy of a work protected under Title 17, even if such actions involve circumvention of additional forms of technological protection measures. In a fact situation where the access is authorized, the traditional defenses to copyright infringement, including fair use, would be fully applicable. So, an individual would not be able to circumvent in order to gain unauthorized access to a work, but would be able to do so in order to make fair use of a work which he or she has acquired lawfully." Andererseits wird vertreten, daß bei *jedem* Zugriff auf einen Inhalt ein „access" im Sinne des 17 U.S.C. § 1201 (a) vorliege; wenn ein Nutzer beispielsweise rechtmäßig ein DRM-geschütztes Video erworben habe, durch eine technische Schutzmaßnahme jedoch an bestimmten Nutzungen gehindert werde, handele es sich dabei um eine Zugangskontrolle, die unter 17 U.S.C. § 1201 (a) falle. Daneben könne aber auch eine Nutzungskontrolle i. S. d. 17 U.S.C. § 1201 (b) vorliegen; so *Goldstein*, Copyright, § 5.17.1, S. 5:245; ebenso *Ginsburg*, 23 Colum.-VLA J. L. & Arts 137, 140 ff. (1999), die diese Auslegung am Wortlaut festmacht und zwischen dem „access to a work" und dem „access to a copy of a work" unterscheidet.

analoge Videorekorder und -kameras, die ursprünglich mit Kopierschutzverfahren von Macrovision versehen waren,[1167] bei denen dieser Schutz aber durch eine Manipulation der Geräte entfernt wurde, nicht mehr in den USA verkauft oder in die USA importiert werden.[1168]

(**b**) **Fallbeispiele.** Für den europäischen Betrachter sind die Regelungen des 17 U.S.C. § 1201 schon deshalb von Interesse, weil es sich international um eine der wenigen Vorschriften zum rechtlichen Umgehungsschutz handelt, zu denen schon Gerichtsentscheidungen vorliegen. Die wichtigsten drei Entscheidungen sollen hier kurz dargestellt werden.[1169]

Nachdem das bei Video-DVDs eingesetzte Schutzsystem CSS im Oktober 1999 von einer deutsch-norwegischen Hackergruppe geknackt worden war,[1170] verklagten acht große amerikanische Filmstudios[1171] vor einem New Yorker Bundesgericht unter Berufung auf Vorschriften des DMCA drei Einzelpersonen, die auf Webseiten das Umgehungsprogramm DeCSS angeboten oder Hyperlinks auf entsprechende Webseiten gesetzt hatten.[1172] Das erstinstanzliche Gericht sah darin eine Verletzung der Zugangskontrollvorschrift des 17 U.S.C. § 1201 (a) (2) und untersagte – nach einer einstweiligen Verfügung, die in die gleiche Richtung gegangen war[1173] – in einem bedeutenden Grundsatzurteil den Beklagten die Verbreitung des Umgehungsprogramms sowie das Setzen entsprechender Hyperlinks.[1174] Derzeit ist das Verfahren vor der zweiten Instanz

---

[1167] Zu den technischen Grundlagen dieser Verfahren s. oben Fn. 503.

[1168] S. dazu im Überblick *Pollack*, 17 Cardozo Arts & Ent. L. J. 47, 103 ff. (1999).

[1169] S. dazu im Überblick *R. T. Nimmer*, § 4.03A[2], S. S4–30 ff.; *Netanel*, 9 Tex. Intell. Prop. L. J. 19 ff. (2000); *Ginsburg*, 24 Colum.-VLA J. L. & Arts 1, 2 ff. (2000). Daneben gibt es eine Entscheidung, in der 17 U.S.C. § 1201 (a) (2) auf illegale Pay-TV-Decoder angewendet wird, CSC Holdings, Inc. v. Greenleaf Electronics, Inc., 2000 WL715601, S. 6 (N.D.Ill., June 2, 2000).

[1170] S. dazu oben Teil 1, D II 3 b.

[1171] Universal City Studios, Paramount Pictures, Metro-Goldwyn-Mayer Studios, Tristar Pictures, Columbia Pictures Industries, Time Warner Entertainmanent, Disney Enterprises und Twentieth Century Fox, unter der Führung der „Motion Pictures Association of America" (MPAA).

[1172] S. dazu im Überblick *Bechtold*, MMR Heft 9/2000, S. XXI; ausführlich *Junger*.

[1173] Universal Citiy Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211 (S.D.N.Y. February 2, 2000).

[1174] Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317 ff. (S.D.N.Y. August 17, 2000). Zur Frage der Einordnung von CSS in die Dichotomie Zugangs-/Nutzungskontrolle s. oben Fn. 1165. Kritisch zur Anwendung des 17 U.S.C. § 1201 (a) (2) auf den Fall insgesamt *Junger*, S. 27 ff. Die Entscheidung wirft u. a. Fragen des Verhältnisses zu urheberrechtlichen Schrankenbestimmungen und zum First Amendment der U.S.-Verfassung sowie der rechtlichen Zulässigkeit von Hyperlinks auf. S. dazu *Ginsburg*, 24 Colum.-VLA J. L. & Arts 1, 5 ff. (2000); *Sparks*, 6 Int. J. Comm. L. & Pol'y (Winter 2000/2001), sowie die unter <http://eon.law.harvard.edu/openlaw/DVD/NY> und <http://www.eff.org/pub/Intellectual_property/MPAA_DVD_cases> erhältlichten Dokumente. Es kann hier nicht auf die Einzelheiten dieser wichtigen und komplexen Entscheidung eingegangen werden. Zur Frage der rechtlichen Zulässigkeit von Hyperlinks s. *Bechtold*, The Link Controversy Page.

anhängig. Teilweise wird damit gerechnet, daß der Fall bis vor den U.S. Supreme Court gelangen wird.

In einem anderen Fall ging es um ein Softwareprogramm, mit dem Audio- und Videoinhalte aus dem Internet abgespielt werden können und das bei Internet-Nutzern weit verbreitet ist.[1175] Das Programm – Realplayer von RealNetworks, Inc. – überträgt digitale Inhalte in einem speziellen Datenformat. Dabei kann der Inhalteanbieter festlegen, daß der Nutzer die Audio- oder Videoinhalte auf seinem Computer nur anhören beziehungsweise anschauen, nicht aber abspeichern kann (sogenannter „Streaming"-Modus). Durch diese Beschränkung sollen Raubkopien verhindert werden. Technisch betrachtet verwendet RealNetworks Authentisierungsverfahren und Metadaten mit Kopierkontrollinformationen, um dieses Ziel zu erreichen.[1176] Daraufhin entwickelte ein anderes Unternehmen – Streambox, Inc. – ein Programm namens „Streambox VCR", mit dem Audio- und Videoinhalte, die im Streaming-Modus mit der RealNetworks-Technologie übertragen wurden, auch permanent abgespeichert werden konnten. Der technische DRM-Schutz des RealPlayers konnte durch dieses Zusatzprogramm umgangen werden.[1177] RealNetworks verklagte Streamworks unter Berufung auf Vorschriften des „Digital Millennium Copyright Act". Das Gericht sah das von RealNetworks verwendete Authentisierungsverfahren als Zugangskontrolle im Sinne des 17 U.S.C. § 1201 (a) (2) und die Kopierkontrollinformationen als Nutzungskontrolle im Sinne des 17 U.S.C. § 1201 (b) an und verbot in einer einstweiligen Verfügung die weitere Herstellung und Vertrieb des „Streambox VCR".[1178]

Die von Sony entwickelte Spielekonsole „Playstation" verfügt über ein System, das verhindern kann, daß in Japan oder USA erworbene Playstation-Speichermedien auf einer in Europa erworbenen Playstation ausgeführt werden können; es ist insofern der bei DVDs eingesetzten „Regional

[1175] Nach Unternehmensangaben ist das Programm weltweit bei über 180 Millionen Internet-Nutzern installiert.

[1176] S. RealNetworks, Inc. v. Streambox, Inc., 2000 WL 127311, S. 1 ff. (W.D.Wash. 2000). Zu den technischen Grundlagen von Authentisierungsverfahren s. oben Teil 1, C III, zu den Grundlagen von Metadaten s. oben Teil 1, C II.

[1177] Zu diesem Zweck gab Streambox VCR dem RealNetworks-System vor, ein authentifizierter Streaming-Player zu sein und beachtete die Metadaten nicht, s. Real Networks, Inc. v. Streambox, Inc., 2000 WL 127311, S. 4 (W.D.Wash. 2000).

[1178] RealNetworks, Inc. v. Streambox, Inc., 2000 WL 127311, S. 7 (W.D.Wash. 2000). Auf den ersten Blick mag erstaunen, daß das Gericht die Metadaten als Nutzungskontrolle auffaßte und nicht unter 17 U.S.C. § 1202 subsumierte. Dazu schreibt das Gericht: „The RealPlayer reads the Copy Switch in the file. If the Copy Switch in the file is turned off, the RealPlayer will not permit the user to record a copy as the file is streamed. Thus, the Copy Switch may restrict others from exercising a copyright holder's exclusive right to copy its work", RealNetworks, Inc. v. Streambox, Inc., 2000 WL 127311, S. 7 (W.D.Wash. 2000). S. zu der Entscheidung auch *Ginsburg*, 24 Colum.-VLA J. L. & Arts 1, 2 ff. (2000).

Code Playback Control" vergleichbar.[1179] Ein kalifornisches Bundesgericht sah es 1999 als einen Verstoß gegen die Zugangskontrollregelung des 17 U.S.C. § 1201 (a) (2) an, wenn ein anderes Unternehmen ein Computerprogramm entwickelt, mit dem dieses Regional-Management-System umgangen werden kann, so daß aus Japan importierte Playstation-Speichermedien auf amerikanischen Playstations abspielbar sind.[1180]

(2) **Audio Home Recording Act.** Neben den umfangreichen Regelungen im „Digital Millennium Copyright Act" existieren noch andere Vorschriften, die vorbereitende Handlungen zur Umgehung technischer Schutzmaßnahmen betreffen. Nach 17 U.S.C. § 1002 (c) – einer Vorschrift, die 1992 durch den „Audio Home Recording Act" in das Urheberrecht eingefügt wurde[1181] – ist Herstellung, Import und Vertrieb von Geräten sowie das Angebot von Dienstleistungen verboten, deren hauptsächlicher Zweck es ist, das in DAT-Geräten enthaltene „Serial Copy Management System" (SCMS)[1182] zu umgehen, zu entfernen oder abzuschalten.

(3) **Trade Secret Law.** DRM-Komponenten wie Verschlüsselungsalgorithmen und Dechiffrier-Schlüssel werden von Unternehmen oftmals als Geschäftsgeheimnisse geschützt.[1183] Veröffentlicht ein Angreifer Computerprogramme oder Informationen, mit denen DRM-Komponenten umgangen werden können, kann ein Verstoß gegen Vorschriften des „trade secret law" vorliegen. In den USA existiert zwar kein einheitlicher Schutz für Geschäftsgeheimnisse. Ein solcher Schutz kann sich aber aus dem common law[1184] oder aus der einzelstaatlichen Umsetzung des „Uniform Trade Secret Act" (UTSA)[1185] ergeben.[1186]

Diese Rechtsgrundlagen zum Schutz technischer Schutzmaßnahmen wurden in den USA auch schon eingesetzt. Nachdem das CSS-System geknackt worden war,[1187] verklagte die DVD Copy Control Association, die CSS lizenziert,[1188] mehrere hundert Einzelpersonen, die das Umge-

---

[1179] S. dazu oben Teil 1, D II 3 e.

[1180] Sony Computer Entertainment America, Inc. v. Gamemasters, Inc. 87 F. Supp. 2d 976, 981 (N.D.Cal. 1999). Auch hier handelt es sich um eine einstweilige Verfügung. Die „Regional Code Playback Control" wird als Zugangskontrolle i. S. d. 17 U.S.C. § 1201 (a) angesehen, s. *Library of Congress*, 65 Fed. Reg. 64555, 64569 (October 27, 2000).

[1181] Zum Audio Home Recording Act allgemein s. unten Teil 2, D II 1 b.

[1182] Zu den technischen Grundlagen von SCMS s. oben Teil 1, D II 1.

[1183] S. dazu oben Teil 2, C I.

[1184] S. dazu Restatement (First) of Torts § 757 (1938) und Restatement (Third) of Unfair Competition § 39 (1995).

[1185] Der UTSA wurde in über 40 Einzelstaaten umgesetzt, z. B. im California Civil Code §§ 3426 ff.

[1186] S. dazu im Überblick *R. T. Nimmer*, § 5.02, S. 5–4 ff.; *Elsing/Van Alstine*, Rdnr. 790 ff.; vgl. a. *Bone*, 86 Cal. L. Rev. 241 ff. (1998).

[1187] S. dazu oben Teil 1, D II 3 b.

[1188] Zur lizenzvertraglichen Seite von CSS s. oben Teil 2, C II.

hungsprogramm DeCSS im Internet angeboten hatten. Im Januar 2000 erließ ein kalifornisches Gericht eine einstweilige Verfügung, nach der es den Beklagten untersagt ist, DeCSS oder sonstige Informationen über CSS (Dechiffrier-Schlüssel etc.) im Internet zu veröffentlichen. Die Schutzkomponente CSS sei als Geschäftsgeheimnis geschützt,[1189] die Veröffentlichung des Umgehungsprogrammes verstoße gegen das kalifornische „trade secret law".[1190]

(4) **Sonstige Vorschriften.** Nach der kommunikationsrechtlichen Vorschrift des 47 U.S.C. § 605[1191] sind Herstellung, Importier und Verkauf von Geräten verboten, die hauptsächlich zum unberechtigten Entschlüsseln von Satellitenprogrammen bestimmt sind, 47 U.S.C. § 605 (e) (4).[1192] Ähnliches regelt 47 U.S.C. § 553 (a) (2) für den Kabelnetzbereich.[1193] Weiterhin kann Herstellung und Vertrieb von Umgehungsprogrammen oder geräten in Einzelfällen unter urheberrechtlichen Gesichtspunkten zu einer „beitragenden Haftung" („contributory infringement") zur späteren Umgehungshandlung durch einen Dritten führen:[1194] Verstößt die tatsächliche Umgehungshandlung gegen urheberrechtliche Vorschriften, so können vorbereitende Handlungen in bestimmten Fällen als „contributory infringement" geahndet werden.[1195]

[1189] Dabei war irrelevant, daß die 40-Bit-Verschlüsselung bei CSS kein besonders wirksamer Schutz ist, DVD Copy Control Ass'n, Inc. v. McLaughlin, 2000 WL 48512, S. 1 (Cal. Super. Jan. 21, 2000). S. dazu auch oben Fn. 1018.

[1190] DVD Copy Control Ass'n, Inc. v. McLaughlin, 2000 WL 48512 (Cal. Super. Jan. 21, 2000), auch erhältlich unter <http://www.eff.org/pub/Intellectual_property/DVDCCA_case/20000120-pi-order.html>. Auf die Einzelheiten kann hier nicht eingegangen werden; so kann ein „Reverse Engineering" – um das es sich letztlich bei der Entwicklung von DeCSS handelte – zulässig sein, solange der Nutzer keine entgegenstehende vertragliche Vereinbarung unterschrieben hat. S. dazu *R. T. Nimmer*, § 4.03A[2], S. S4–32 f.

[1191] S. dazu schon oben Teil 2, D I 2 a dd 2.

[1192] Daneben kann auch 47 U.S.C. § 605 (a) greifen, s. Cable/Home Communcations Corp. v. Network productions, Inc., 902 F.2d 829, 847 f. (11th Cir. 1990); National Subscription Television v. S&H TV, 644 F.2d 820, 826 f. (9th Cir. 1981); Chartwell Communications Group v. Westbrook, 637 F.2d 459, 466 (6th Cir. 1980); *Thorne/Huber/Kellogg*, § 10.10.1, S. 632 ff.; *Ferris/Lloyd*, §26.02[1][c][i], S. 26–11 f.

[1193] Zu weiteren Vorschriften s. oben Teil 2, D I 2 a dd 2.

[1194] Zur parallelen Konstruktion nach deutschem Urheberrecht s. oben Teil 2, D I 2 b cc 1.

[1195] S. dazu Sega Enterprises Ltd. v. MAPHIA, 857 F. Supp. 679, 687 (N.D.Cal. 1994); Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 261 ff. (1988); *Wand*, S. 206 ff. Zum „contributory infringement" allgemein *N. B. Nimmer/D. Nimmer*, § 12.04[A][2], S. 12–72 ff., insb. S. 12–75 ff.; *Goldstein*, Copyright, § 6.1, S. 6:6 ff., insb. § 6.1.2, S. 6:11 ff.; *Rieder*, S. 133 ff., insb. S. 140 f. Praktisch wirft die Subsumption unter die Grundsätze des „contributory infringement" jedoch einige Probleme auf. Einerseits ist die Entscheidung des Supreme Court in Sachen Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984), zu beachten. Danach kann der Hersteller eines Videorekorders nicht für die Urheberrechtsverletzungen haftbar gemacht werden, die seine Käufer mit dem Videorekorder begehen. Dies wurde u. a. damit begründet, daß

3. Verbot der Manipulation von Metadaten

a) Allgemeines

Metadaten[1196] sind in DRM-Systemen unerläßlich. Eine dauerhafte Identifizierung von Inhalten, Rechteinhabern, Nutzungsbedingungen und Nutzern ist die Grundlage für die Einräumung von Nutzungsrechten sowie für die Nutzungskontrolle und vergütung in DRM-Systemen.[1197] Authentizität und Integrität von Metadaten sind eine der Grundvoraussetzungen, damit ein DRM-System eine sichere Vertriebsplattform für digitale Inhalte bieten kann.[1198] Zwar existieren unterschiedliche technische Verfahren, die diese Schutzziele verwirklichen sollen.[1199] Der technische Schutz von Metadaten ist jedoch nicht perfekt.[1200] Es wird Angreifern in DRM-Systemen immer gelingen, in bestimmten Fällen Metadaten zu verändern oder zu löschen. Dadurch kann ein Angreifer eventuell digitale Inhalte im DRM-System nutzen, ohne dafür ein Entgelt entrichten zu müssen. Manipulationen an Metadaten können zu Rechtsverletzungen und Vermögensbeeinträchtigungen führen.[1201] In dieser Lage wird zunehmend auf einen rechtlichen Schutz von Metadaten gesetzt. Dabei wird die Manipulation von Metadaten gesetzlich verboten.

Bei allen Unterschieden im Detail lassen sich Grundstrukturen des rechtlichen Schutzes von Metadaten ausmachen.[1202] So bezieht sich der

---

der Videorekorder nicht nur für Urheberrechtsverletzungen benutzt werden könne, sondern daß daneben auch gewichtige andere Nutzungsmöglichkeiten bestünden („significant noninfringing uses"), beispielsweise das private Aufnehmen von Fernsehsendungen, um diese zeitlich versetzt ansehen zu können (sog. „time shifting"). S. zum ganzen *N. B. Nimmer/D. Nimmer*, § 12.04[A][2][b], S. 12–77 ff.; *Goldstein*, Copyright, § 6.1.2, S. 6:11 f.; *Rieder*, S. 145 f.; Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 263 ff. (1988); *Wand*, S. 209 ff.; zu den Auswirkungen dieser Entscheidung auf die Herstellung illegaler Pay-TV-Decoder s. *Sciorra*, 11 Cardozo Arts & Ent. L. J. 905, 945 ff. (1993). Andererseits ist problematisch, welche Anforderungen beim „contributory infringement" an die subjektive Seite des Täters zu stellen sind (s. dazu allgemein *Rieder*, S. 133 ff., und in Bezug auf die Herstellung illegaler Pay-TV-Decoder ausführlich *Sciorra*, a. a. O., S. 934 ff.). Schließlich ist fraglich, ob eine Haftung nach den Grundsätzen des „contributory infringement" nur eintritt, wenn ein „direct infringement" durch einen Dritten tatsächlich nachgewiesen werden kann, s. *N. B. Nimmer/D. Nimmer*, §12.04[A][3][a], S. 12–82 ff.

[1196] Die Arbeit verwendet einheitlich den Begriff „Metadaten", der insbesondere in der technischen Literatur gebraucht wird. In der juristischen Literatur werden Metadaten oft als „Informationen über die Rechtewahrnehmung" bezeichnet.

[1197] Zu den technischen Grundlagen von Metadaten s. ausführlich oben Teil 1, C II.

[1198] S. dazu oben Teil 1, C III 1 b.

[1199] Metadaten können durch digitale Wasserzeichen auf robuste und sichere Weise mit dem entsprechenden digitalen Inhalt verbunden werden; s. dazu oben Teil 1, C II 2 b bb. Zum Schutz der Authentizität und Integrität von Metadaten s. oben Teil 1, C III 1 b.

[1200] S. dazu auch oben Teil 2, D I 1.

[1201] *V. Lewinski*, GRUR Int. 1997, 667, 677.

[1202] S. dazu auch *de Kroon* in: Hugenholtz (Hrsg.), S. 229, 259 ff.

rechtliche Schutz nicht auf alle Arten von Metadaten. Bei Metadaten in DRM-Systemen läßt sich zwischen Informationen über den Inhalt selbst, über dessen Rechteinhaber, über die Nutzungsbedingungen sowie über die Nutzer unterscheiden.[1203] Die Schutzvorschriften beziehen sich nur auf die Metadaten zur Identifizierung von Inhalten, Rechteinhabern und Nutzungsbedingungen (dazu unten b). Aus datenschutzrechtlichen Gründen sind Metadaten zur Identifizierung der Nutzer vom Rechtsschutz regelmäßig ausgeschlossen (dazu unten c). Die Einführung eines rechtlichen Schutzes von Metadaten ist bei weitem nicht so umstritten wie die Einführung des Umgehungsschutzes allgemeiner technischer Schutzmaßnahmen.

b) Metadaten hinsichtlich Inhalt, Rechteinhaber und Nutzungsbedingungen

Regelmäßig ist die Entfernung oder Veränderung richtiger Metadaten verboten (dazu unten aa). Entfernt ein Angreifer ein digitales Wasserzeichen mit Informationen über den Inhalt und dessen Nutzungsbedingungen, so können solche Regelungen eingreifen.[1204] Mitunter wird auch das Bereitstellen falscher Metadaten verboten (dazu unten bb). Dabei fügt ein Angreifer zu einem digitalen Inhalt falsche Metadaten hinzu, um so technische Schutzmaßnahmen zu umgehen. Vereinzelt finden sich Vorschriften, die Herstellung und Vertrieb von Vorrichtungen verbieten, mit denen Metadaten verändert oder entfernt werden können („vorbereitende Handlungen",[1205] dazu unten cc).

aa) Verbot der Entfernung oder Veränderung richtiger Metadaten

(1) Völkerrechtlicher Rechtsrahmen

(a) WIPO-Verträge. Art. 12 WCT enthält eine detaillierte Regelung hinsichtlich des Schutzes von Metadaten, die dort „Informationen über die Rechtewahrnehmung" genannt werden. Während Art. 12 WCT Metadaten betrifft, die von Urhebern eingesetzt werden, enthält Art. 19 WPPT eine entsprechende Vorschrift für ausübende Künstler und Tonträgerhersteller.[1206] Anders als die Vorschriften zur Umgehung allgemeiner technischer Schutzmaßnahmen[1207] waren die Vorschriften zum Schutz von Metadaten bei den Verhandlungen der WIPO-Verträge wenig umstritten.

[1203] S. oben Teil 1, C II 1.

[1204] Je nach konkreter Ausgestaltung können daneben noch andere Vorschriften zum Schutz technischer Schutzmaßnahmen eingreifen.

[1205] Zu diesem Begriff s. oben Teil 2, D I 2.

[1206] Im folgenden wird Art. 12 WCT dargestellt; für Art. 19 WPPT gilt Entsprechendes. Die Vorschriften basieren hauptsächlich auf Vorschlägen der U.S.-amerikanischen Delegation bei der diplomatischen Konferenz, s. *Samuelson*, 37 Va. J. Int'l L. 369, 415 f. (1997). S. zum ganzen auch *v. Lewinski*, GRUR Int. 1997, 667, 676 f.; *Wand*, S. 45 ff. Der Entwurf eines „WIPO Audiovisual Performances Treaty Basic Proposal" (s. dazu oben Teil 2, D I 2 a aa 1) enthielt in Art. 16 eine entsprechende Vorschrift, s. *WIPO Audiovisual Performances Treaty Basic Proposal*, S. 64 ff.

[1207] Zu Art. 11 WCT und Art. 18 WPPT s. oben Teil 2, D I 2 a aa 1.

Man konnte sich auf eine detaillierte Regelung einigen, die zum konkreten Vorbild für viele nationale Vorschriften zum Schutz von Metadaten wurde.[1208] Metadaten sind nach Art. 12 Abs. 2 WCT einerseits kennzeichende Informationen über das Werk selbst sowie über dessen Urheber und sonstige Rechteinhaber. Anderseits werden auch – anders als noch im Entwurf des WCT[1209] – Informationen über die Nutzungsbedingungen des Werks erfaßt.

Art. 12 Abs. 1 WCT untersagt die unbefugte Entfernung oder Änderung dieser Metadaten sowie die unbefugte Verbreitung, Einfuhr, Funksendung oder öffentliche Wiedergabe von Werken, bei denen diese Metadaten unbefugt entfernt oder geändert wurden. Für die subjektive Seite ist Voraussetzung, daß der Täter weiß oder (bei zivilrechtlicher Sanktion) wissen muß, daß sein Handeln eine Verletzung eines unter den WCT oder die RBÜ fallenden Rechts herbeiführt, ermöglicht, erleichtert oder verbirgt.[1210]

(b) Sonstige völkerrechtliche Regelungen. Nach Art. 4 des Cybercrime-Übereinkommen (Entwurf)[1211] sind die Vertragsstaaten verpflichtet, das unberechtigte Beschädigen, Löschen, Verändern oder Unterdrücken von Computerdaten strafrechtlich zu sanktionieren.[1212] Unter den Begriff der Computerdaten können auch Metadaten in DRM-Systemen fallen.[1213]

(2) Europäischer Rechtsrahmen. Art. 7 der Richtlinie zum Urheberrecht in der Informationsgesellschaft[1214] lehnt sich an die dargestellten Regelungen der WIPO-Verträge an. Anders als Art. 6 der Richtlinie[1215] blieb die Vorschrift zum rechtlichen Schutz von Metadaten während der langen Entstehungsgeschichte der Richtlinie im wesentlichen unverändert.[1216]

Nach Art. 7 Abs. 2 Unterabs. 1 der Richtlinie werden Metadaten geschützt, die zur Identifikation der Werke und ihrer Rechteinhaber dienen

---

[1208] S. *Samuelson*, 36 Va. J. Int'l L. 369, 417 (1997).

[1209] Art. 14 *WCT basic Proposal*, S. 58 f.

[1210] Dabei reicht die Verletzung bloßer Vergütungsansprüche aus, s. die gemeinsame Erklärung der Vertragsstaaten zu Art. 12 WCT und Art. 19 WPPT, erhältlich unter <http://www.wipo.int/eng/iplex>.

[1211] S. dazu allgemein oben Teil 2, D I 2 a aa 2.

[1212] Art. 4 Abs. 1 Europäisches Cybercrime-Übereinkommen (Entwurf) lautet: „Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right."

[1213] „Computer data" werden in Art. 1 lit. b Europäisches Cybercrime-Übereinkommen (Entwurf) definiert als „any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function."

[1214] Dazu allgemein s. oben Teil 2, D I 2 a bb 2.

[1215] S. dazu oben Fn. 1015.

[1216] *Bechtold* in: Hoeren/Sieber (Hrsg.), Teil 7.11, Rdnr. 79.

oder Informationen über Nutzungsbedingungen enthalten.[1217] Es werden nur Metadaten geschützt, die sich auf urheberrechtliche Werke oder auf Gegenstände beziehen, die durch verwandte Schutzrechte oder die Datenbank-Richtlinie geschützt sind, Art. 7 Abs. 2 Unterabs. 1 der Richtlinie.[1218] Anders als die WIPO-Verträge stellt die Vorschrift klar, daß die Metadaten vom Rechteinhaber stammen müssen, Art. 7 Abs. 2 Unterabs. 1 der Richtlinie. Sie müssen mit einem Vervielfältigungsexemplar verbunden sein oder während der Wiedergabe erscheinen, Art. 7 Abs. 2 Unterabs. 2 der Richtlinie.

Die Vorschrift verbietet einerseits die Entfernung oder Änderung solcher Metadaten. Andererseits wird die Verbreitung, Einfuhr, Sendung, öffentliche Wiedergabe oder öffentliche Zugänglichmachung[1219] von Vervielfältigungsstücken sanktioniert, bei denen die Metadaten unbefugt entfernt oder verändert wurden, Art. 7 Abs. 1 der Richtlinie. Dabei muß der Täter unbefugt handeln.[1220] Es ist unerheblich, ob der Täter zu geschäftlichen Zwecken handelt oder nicht.[1221] Auf subjektiver Seite setzt die Vorschrift voraus, daß der Täter weiß oder wissen muß, daß er durch seine Handlung die Verletzung von Urheberrechten oder Leistungsschutzrechten veranlaßt, ermöglicht oder erleichtert. Durch diese subjektive Voraussetzung wird eine Verbindung zum herkömmlichen Urheberrecht hergestellt.

(3) **Deutscher Rechtsrahmen.** In Deutschland existieren derzeit keine speziellen Vorschriften, welche die Manipulation von Metadaten in DRM-Systemen verbieten. Jedoch enthält der Entwurf eines 5. UrhG-Änderungsgesetzes[1222] in § 96 b UrhG-E eine Vorschrift, die die Vorgaben der WIPO-Verträge und der Richtlinie zum Urheberrecht in der Informa-

[1217] Dabei werden nicht nur vollständige Metadaten erfaßt, sondern kurze Identifizierungsnummern, die auf einen vollständigen Metadatensatz in einer Datenbank verweisen, Art. 7 Abs. 2 Unterabs. 1 a. E. („Zahlen oder Codes, durch die derartige Informationen ausgedrückt werden"); zu der Unterscheidung zwischen „dumb" und „intelligent identifiers" s. oben bei Fn. 138. Sonstige Informationen, die an einem Werk angebracht werden können, werden nicht erfaßt, Anm. 1 zur Art. 7 des ursprünglichen Richtlinienvorschlags 1997, *Europäische Kommission*, KOM (97) 628 endg. vom 10. 12. 1997, S. 38.

[1218] Gegenüber den WIPO-Verträgen erstreckt sich der Schutz damit auf alle gesetzlich geschützten Leistungsschutzrechte, nicht nur auf jene der ausübenden Künstler und Tonträgerhersteller, wie dies in Art. 19 WPPT der Fall ist.

[1219] Damit ist das „right to make available to the public" in Art. 3 Abs. 2 der Richtlinie gemeint; s. dazu oben bei Fn. 767.

[1220] Dies ist nicht der Fall, wenn der Rechteinhaber zugestimmt hat, die Entfernung gesetzlich zulässig oder sogar (z. B. aus Datenschutzgründen) gesetzlich vorgeschrieben ist, Anm. 2 zu Art. 7 des ursprünglichen Richtlinienvorschlags 1997, *Europäische Kommission*, KOM (97) 628 endg. vom 10. 12. 1997, S. 38.

[1221] Ebenso *Kaestner*, S. 12 f.

[1222] S. dazu oben Teil 2, D I 2 a cc 1.

tionsgesellschaft umsetzen will.[1223] Anders als nach den WIPO-Verträgen und der europäischen Richtlinie ist nicht erforderlich, daß der Täter weiß, daß seine Handlung zur Verletzung des Urheberrechs oder verwandten Schutzrechten führt oder diese ermöglicht. Damit sollen schwierige Abgrenzungsfragen im Einzelfall vermieden werden.[1224]

Auch nach den allgemeinen geltenden Vorschriften kann das Entfernen oder Verändern richtiger Metadaten unzulässig sein. Das Entfernen von Metadaten kann dazu führen, daß ein digitaler Inhalt ohne Angaben über die Rechteinhaber sowie die Nutzungsbedingungen vertrieben und daraufhin unberechtigt genutzt und vervielfältigt wird. Nach den oben dargestellten Grundsätzen des adäquaten Kausalzusammenhangs[1225] kann in Einzelfällen schon das Entfernen von Metadaten zu Ansprüchen aus § 97 Abs. 1 UrhG führen.[1226] Die Entfernung einer Urheberkennzeichnung kann gegen das Urheberpersönlichkeitsrecht auf Anerkennung der Urheberschaft nach § 13 S. 2 UrhG verstoßen.[1227] In Einzelfällen mögen §§ 1, 3 UWG unter dem Gesichtspunkt der Herkunftstäuschung weiterhelfen.[1228] Schließlich können strafrechtliche Tatbestände wie §§ 303 a, 263 a, 269 und 270 StGB erfüllt sein.[1229]

[1223] Danach soll ein neuer § 96 b UrhG lauten:

„(1) Zur Rechtewahrnehmung erforderliche Informationen, die in dem Original oder einem Vervielfältigungsstück eines Werkes oder einer Datenbank oder in einem Bild- oder Tonträger verkörpert sind, oder die im Zusammenhang mit der öffentlichen Wiedergabe eines Werkes, einer Datenbank oder eines Bild- oder Tonträgers verwendet werden, dürfen ohne Erlaubnis des Rechtsinhabers nicht beseitigt oder verändert werden.

(2) Originale oder Vervielfältigungsstücke eines Werkes oder einer Datenbank sowie Bild- oder Tonträger, bei denen zur Rechtewahrnehmung erforderliche Informationen rechtswidrig beseitig oder verändert worden sind, dürfen nicht verbreitet oder zur öffentlichen Wiedergabe benutzt werden.

(3) Zur Rechtewahrnehmung erforderliche Informationen im Sinne dieses Gesetzes sind Daten, die Informationen enthalten, die zur Identifizierung des Gegenstandes oder des Inhabers eines nach diesem Gesetz geschützten Rechts oder des Inhabers eines Nutzungsrechts an einem solchen Gegenstand dienen oder die sich auf die Bedingungen beziehen, unter denen ein Nutzungsrecht an einem solchen Gegenstand eingeräumt wird."

[1224] *Bundesministerium der Justiz*, Begründung zum 5. UrhGÄndG-Entwurf, S. 24. Insgesamt wird keine Kenntnis des Täters verlangt. Dies entspreche dem allgemeinen deutschen Haftungssystem bei Unterlassungs- und Beseitigungsansprüchen, vgl. *ebda*.

[1225] S. dazu oben Teil 2, D I 2 b cc 1.

[1226] Vgl. *de Kroon* in: Hugenholtz (Hrsg.), S. 229, 242 f.

[1227] Zweifelnd *de Kroon* in: Hugenholtz (Hrsg.), S. 229, 245, für den Fall, daß die Metadaten nicht direkt im Inhalt eingebettet sind, sondern aus einer zentralen Datenbank abgerufen werden. Diese Anspruchsgrundlage hilft allenfalls bezüglich der Metadaten zur Identifikation der Urheber, nicht bezüglich der Metadaten zur Definition von Nutzungsbedingungen u. ä., s. *ebda*.

[1228] Vgl. *de Kroon* in: Hugenholtz (Hrsg.), S. 229, 246, die auch für einen markenrechtlichen Schutz bestimmter Metadaten plädiert.

[1229] S. a. *de Kroon* in: Hugenholtz (Hrsg.), S. 229, 248 f.

(4) **U.S.-amerikanischer Rechtsrahmen.** Durch den „Digital Millennium Copyright Act“[1230] wurden in den „Copyright Act“ Vorschriften zum Schutz gegen die Entfernung oder Veränderung von Metadaten eingefügt. 17 U.S.C. § 1202 schützt Metadaten, die dort „copyright management information“ genannt werden. Unter diese Vorschrift fallen Metadaten zur Identifikation des Inhalts, der Rechteinhaber sowie Nutzungsbedingungen, 17 U.S.C. § 1202 (c).[1231] 17 U.S.C. § 1202 (b) (1) und (3) enthalten das Verbot, solche Metadaten zu entfernen oder zu verändern und derartig manipulierte Werke zu verbreiten oder wiederzugeben.[1232] Weiterhin ist es gemäß 17 U.S.C. § 1202 (b) (2) verboten, die Metadaten selbst zu verbreiten, die von einem Werk entfernt oder verändert wurden. In allen Fällen muß der Täter unbefugt handeln.[1233] Er muß wissen oder hätte – hinsichtlich zivilrechtlicher Rechtsbehelfe – zumindest wissen müssen, daß er durch die Entfernung oder Veränderung der Metadaten eine Urheberrechtsverletzung ermöglicht, erleichtert oder verbirgt.[1234]

Neben dieser allgemeinen Vorschrift des „Digital Millennium Copyright Act“ wurde schon 1992 durch den „Audio Home Recording Act“[1235] eine Vorschrift in den Copyright Act eingefügt, nach der Metadaten – hier: SCMS-Informationen[1236] – bei der Übertragung digitaler Inhalte nicht verändert werden dürfen, s. 17 U.S.C. § 1002 (e) S. 2. Seit 1995 enthält der Copyright Act weiterhin eine Vorschrift, nach der bei Übertragungen von Audioinhalten über das Internet bestimmte Metadaten nicht entfernt werden dürfen, s. 17 U.S.C. § 114 (d) (2) (A) (iii).[1237]

[1230] Zum DMCA allgemein s. oben Teil 2, D I 2 a dd 1.

[1231] *Ginsburg*, 23 Colum.-VLA J. L. & Arts 137, 157 f. (1999), vertritt die Auffassung, daß diese Regelung den Anforderungen des Art. 12 WCT nicht gerecht werde. S. zur Vorschrift ausführlich *D. Nimmer*, 46 J. Copyright Soc'y U.S.A. 401, 412 ff. (1999). Dabei reicht es nicht aus, wenn die Metadaten neben einem Werk auf einer Webseite angezeigt werden, ohne mit dem Werk selbst in irgendeiner Weise verbunden zu sein, Kelly v. Arriba Soft Corp., 77 F. Supp. 2d. 1116, 1122 (1999). Identifizierungsnummern, die auf Metadatensätze in Datenbanken verweisen (zur Unterscheidung zwischen „dumb“ und „intelligent identifiers“ s. oben bei Fn. 138), werden jedoch erfaßt, 17 U.S.C. § 1202 (c) (7); s. dazu *D. Nimmer*. 46 J. Copyright Soc'y U.S.A. 401, 415 (1999).

[1232] *Ginsburg*, 23 Colum.-VLA J. L. & Arts 137, 158 f. (1999), vertritt die Auffassung, daß eine Veränderung der Metadaten auch dann vorliege, wenn die Metadaten selbst nicht manipuliert werden, sondern der digitale Inhalt manipuliert werde, auf den sich die Metadaten beziehen.

[1233] 17 U.S.C. § 1202 (b) spricht von „without the authority of the copyright owner or the law.“

[1234] Zu den Auslegungsproblemen, die dieses subjektive (!) Tatbestandsmerkmal bietet, s. *D. Nimmer*, 46 J. Copyright Soc'y U.S.A. 401, 423 ff. (1999).

[1235] Allgemein zum „Audio Home Recording Act“ s. unten Teil 2, D II 1 b.

[1236] Zu den technischen Grundlagen von SCMS s. oben Teil 1, D II 1.

[1237] Die Einzelheiten der Vorschrift, die durch den „Digital Performance Rights in Sound Recordings Act of 1995“ eingefügt wurden, sind recht komplex, s. dazu *D. Nimmer*, 93 Nw. U. L. Rev. 195, 198 (1999); *N. B. Nimmer/D. Nimmer*, § 8.22[C][1][b].

In Einzelfällen kann schließlich die lauterkeitsrechtliche Vorschrift des § 43 (a) Lanham Act (15 U.S.C. § 1125 (a)) eingreifen.[1238]

bb) Verbot des Bereitstellens falscher Metadaten

Es zeigt sich, daß umfassende Regelungen bestehen, die das Entfernen und Verändern von Metadaten verbieten, die von den Inhalteanbietern in digitale Inhalte integriert wurden. Dagegen sind Regelungen sehr viel seltener, die das bloße Bereitstellen falscher Metadaten durch einen Angreifer sanktionieren. Das ist insofern erstaunlich, als es durchaus Fälle gibt, in denen das Bereitstellen falscher Metadaten nicht gleichzeitig als Verändern richtiger Metadaten interpretiert werden kann und daher von den dargestellten Regelungen nicht erfaßt werden.[1239] Auch kann in DRM-Systemen in Interesse daran bestehen, daß der Urheber selbst digitale Inhalte nicht mit unzutreffenden Metadaten versieht. Weder die WIPO-Verträge noch die dargestellten europäischen Richtlinien enthalten Vorschriften bezüglich des Bereitstellens falscher Metadaten.

(1) **Deutscher Rechtsrahmen.** Auch in Deutschland bestehen keine speziellen Regelungen zur Bereitstellung falscher Metadaten in DRM-Systemen. Dies soll sich durch den Entwurf eines 5. Urheberrechts-Änderungsgesetzes[1240] nicht ändern. Jedoch kann sich ein Schutz gegen die Bereitstellung falscher Metadaten aus allgemeinen Vorschriften ergeben. Versucht ein Angreifer, in Metadaten eines Inhalts einen falschen Urheber (beispielsweise einen bekannten Komponisten oder Autor) anzugeben, kann das „droit de non-paternité" eingreifen, das sich aus § 12 S. 1 BGB und dem allgemeinen Persönlichkeitsrecht in Verbindung mit §§ 823 Abs. 1, 1004 analog BGB ergibt.[1241] Auch kann die Rechtsprechung zu sogenannten „Meta-Tags" herangezogen werden.[1242] Die Verwendung

[1238] Zu der Vorschrift allgemein s. *Elsing/Van Alstine*, Rdnr. 761. Bei Metadaten über Nutzungsbedingungen hilft die Vorschrift nicht weiter, s. *Samuelson*, 37 Va. J. Int'l L. 369, 418 Fn. 277 (1997); *N. B. Nimmer/D. Nimmer*, § 12A.08[B], S. 12A-91; *de Kroon* in: Hugenholtz (Hrsg.), S. 229, 241.

[1239] Dies ist beispielsweise der Fall, wenn ein Angreifer das Werk eines fremden Rechteinhabers digitalisiert, das bisher mit keinerlei Metadaten versehen war (Beispiel: herkömmliche CD-Aufnahme), es mit falschen Metadaten (falscher Rechteinhaber, falsche Nutzungsbedingungen etc.) ausstattet und dann in ein DRM-System einschleust.

[1240] S. dazu oben Teil 2, D I 2 a cc 1.

[1241] Dieses Persönlichkeitsrecht, das ein Abwehrrecht gegen das „Unterschieben" eines fremden Werks gewährt, folgt nicht aus § 13 UrhG, s. *Schack*, Rdnr. 41. Zum „droit-de-non-paternité" allgemein s. *Seemann*, UFITA 128 (1995), 31 ff., auch zum marken- und wettbewerbsrechtlichen Schutz der Urheberbezeichnung.

[1242] Zu den technischen Grundlagen von Meta-Tags s. oben Fn. 196. Dabei integriert ein Anbieter (A) bei der Erstellung einer WWW-Seite in sog. „Meta-Tags" dieser Seite fremde Marken oder sonstige fremde Kennzeichen von Wettbewerbern (W). Diese Meta-Tags werden von Suchmaschinen im Internet zur Erstellung von Suchindices ausgewertet. Gibt ein Nutzer bei einer Suchmaschine das Kennzeichen des Wettbewerbers als Suchbegriff ein, so kann es vorkommen, daß die Suchmaschine dem Nutzer als Suchergebnis an erster Stelle nicht die WWW-Seite des tatsächlichen Kennzeicheninha-

einer fremden Marke oder einer fremden geschäftlichen Bezeichnung in einem Meta-Tag kann gegen §§ 14 Abs. 2, 15 Abs. 2 MarkenG verstoßen.[1243] Dazu existieren in Deutschland inzwischen mehrere Gerichtsurteile.[1244] Daneben kann ein Verstoß gegen §§ 1, 3 UWG gegeben sein.[1245] In Einzelfällen lassen sich die rechtlichen Grundsätze von Meta-Tags auf Metadaten von DRM-Systemen übertragen.[1246]

(2) **U.S.-amerikanischer Rechtsrahmen.** Dagegen existieren in den USA spezielle gesetzliche Vorschriften, die das Bereitstellen falscher Metadaten betreffen. Nach 17 U.S.C. § 1202 (a) ist es verboten, falsche Metadaten zu verwenden oder zu verbreiten.[1247] Der Täter muß die Absicht haben, dadurch eine Urheberrechtsverletzung zu ermöglichen, erleichtern oder zu verbergen.[1248] Die Vorschrift gilt auch für den Rechteinhaber selbst, dem das Anbringen falscher Metadaten ebenfalls verboten ist. Eine ähnliche Vorschrift, die sich vornehmlich auf das bei DAT-Geräten eingesetzte „Serial Copy Management System"[1249] bezieht, ist in 17 U.S.C. § 1002 (d) (1) enthalten. Danach ist es verboten, in digitalen Audioinhalten falsche Informationen darüber einzubetten, ob die Audioinhalte urheberrechtlich geschützt sind und ob die Inhalte vom Nutzer kopiert werden dürfen.

Im U.S.-amerikanischen Copyright Act ist seit 1991 ein „droit de nonpaternité" für bildende Künstler explizit in 17 U.S.C. § 106A (a) (1) (B) geregelt.[1250] Für sonstige Rechteinhaber kann in Einzelfällen § 43 (a) Lanham Act (15 U.S.C. § 1125 (a)) weiterhelfen.[1251] Schließlich existiert auch in den USA Rechtsprechung zu der Frage, ob in einem Meta-Tag fremde Kennzeichen verwendet werden dürfen. Dies kann unter marken- und wettbewerbsrechtlichen Gesichtspunkten unzulässig sein.[1252]

---

bers W, sondern das Angebot des Anbieters A anzeigt. Mit Hilfe von Meta-Tags können Kundenströme auf das eigene Angebot im Internet umgelenkt werden; s. dazu *Viefhues*, MMR 1999, 336 f.; *Menke*, WRP 1999, 982, 983.

[1243] Im einzelnen stellen sich mehrere Probleme. So ist umstritten, ob die Verwendung einer Marke in einem Meta-Tag eine (eventuell auch kennzeichenmäßige) Benutzungshandlung darstellt; s. dazu *Kur*, CR 2000, 448 ff.; *Viefhues*, MMR 1999, 336, 337 ff.; *Menke*, WRP 1999, 982, 984 ff.

[1244] LG Mannheim, CR 1998, 306 – ARWIS (s. dazu *Menke*, WRP 1999, 982 f.); LG Frankfurt, CR 2000, 462; OLG München, WRP 2000, 775 – Hanseatic.

[1245] LG Hamburg, MMR 2000, 46, 47; *Viefhues*, MMR 1999, 336, 340 f.; *Menke*, WRP 1999, 982, 989 f.

[1246] Wie bei Meta-Tags kann ein Inhalteanbieter in einem DRM-System durch falsche Metadaten versuchen, die Aufmerksamkeit der Kunden auf sein Angebot zu lenken.

[1247] Dabei ist nicht nur die „public distribution", sondern jede Verbreitung an Dritte gemeint, *D. Nimmer*, 46 J.Copyright Soc'y U.S.A. 401, 417 (1999).

[1248] Zu den Auslegungsproblemen, die dieses subjektive Tatbestandsmerkmal bietet, s. *D. Nimmer*, 46 J.Copyright Soc'y U.S.A. 401, 418 ff. (1999).

[1249] Zu den technischen Grundlagen von SCMS s. oben Teil 1, D II 1.

[1250] S. dazu *N. B. Nimmer/D. Nimmer*, § 8D.06[B][1], S. 8D-70 ff.

[1251] S. dazu *N. B. Nimmer/D. Nimmer*, § 8D.03[B][1], S. 8B-40 ff.

[1252] Hinweise zu entsprechenden Urteilen finden sich in der deutschen Literatur in *Kochinke/Geiger*, K&R 2000, 594, 595 f.; *Viefhues*, MMR 1999, 336, 337; s. in der

cc) Verbot vorbereitender Handlungen

Die bisher dargestellten Vorschriften zum Schutz von Metadaten betreffen die tatsächliche Manipulation von Metadaten. Wie beim rechtlichen Umgehungsschutz allgemeiner technischer Schutzmaßnahmen[1253] stellt sich bei Metadaten die Frage, ob nicht auch Vorrichtungen und Dienstleistungen verboten werden sollten, die zur Entfernung oder Veränderung von Metadaten benutzt werden können („vorbereitende Handlungen"). Ein solches Verbot vorbereitender Handlungen findet sich im Bereich von Metadaten nur sehr vereinzelt. Nach Art. 6 Abs. 1 lit. a Nr. 1 des europäischen Cybercrime-Übereinkommens (Entwurf)[1254] sind die Vertragsstaaten verpflichtet, die Herstellung, Verkauf, Import und Vertrieb von Hard- oder Software strafrechtlich zu sanktionieren, die entwickelt wurde, um eine der in Art. 4 genannten Handlungen zu begehen. Da unter Art. 4 des Übereinkommens auch das Beschädigen, Löschen, Verändern oder Unterdrücken von Metadaten fallen kann,[1255] erfaßt Art. 6 vorbereitende Handlungen im Bereich von Metadaten.[1256] Für die subjektive Seite ist erforderlich, daß der Anbieter der Hard- oder Software gerade beabsichtigt, daß seine Käufer die Geräte zu einer der in Art. 4 genannten Handlungen verwenden. Nach Art. 6 Abs. 1 lit. b Cybercrime-Übereinkommen (Entwurf) ist auch schon der bloße Besitz solcher Komponenten zu bestrafen, solange sie zu einer der in Art. 4 genannten Handlungen verwendet werden sollen.[1257]

In Deutschland finden sich keine speziellen Vorschriften zu dieser Frage. Nach dem Entwurf eines 5. Urheberrechts-Änderungsgesetzes[1258] soll § 99 UrhG aber insofern erweitert werden, als sich der Vernichtungs- und Überlassungsanspruch auch auf Vorrichtungen erstreckt, die „zur rechtswidrigen Beseitigung oder Veränderung von zur Rechtewahrnehmung erforderlichen Informationen" benützt werden oder bestimmt sind.[1259] Dadurch würde – im internationalen Vergleich recht außergewöhnlich – im deutschen UrhG ein Schutz vorbereitender Handlungen im Metadaten-Bereich verankert.

U.S.-amerikanischen Literatur *R. T. Nimmer*, § 6.16[2][b], S. S6–82 f.; *Lastowka*, 86 Va. L. Rev. 835 ff. (2000); *McCuaig*, 18 J. Marshall J. Computer & Info. L. 643 ff. (2000); *Paylago*, 40 IDEA 451 ff. (2000).

1253 S. dazu oben Teil 2, D I 2.

1254 S. dazu allgemein Teil 2, D I 2 a aa 2.

1255 S. dazu oben Teil 2, D I 3 b aa 1 b.

1256 Die Vertragsstaaten sind jedoch nicht verpflichtet, einen solchen Schutz gesetzlich zu verankern, Art. 6 Abs. 3 Cybercrime-Übereinkommen (Entwurf).

1257 Dabei kann die Strafbarkeit auch erst ab dem Besitz einer Mehrzahl solcher Komponenten eingreifen, Art. 6 Abs. 1 lit. b S. 2 Cybercrime-Übereinkommen (Entwurf). DieVorschrift zielt auf professionelle Händler ab.

1258 S. dazu oben Teil 2, D I 2 a cc 1.

1259 Nach geltender Rechtslage wird ein Anspruch aus § 99 UrhG regelmäßig ausscheiden, s. *Wand*, GRUR Int. 1996, 897, 903.

c) Metadaten hinsichtlich der Nutzer

Die dargestellten Regelungen zum Schutz von Metadaten beziehen sich immer nur auf Metadaten, die den digitalen Inhalt und dessen Rechteinhaber identifizieren und Nutzungsbedingungen definieren. Keine der Regelungen verbietet die Entfernung oder Veränderung von Metadaten, durch die ein DRM-System Nutzer identifiziert.[1260] Metadaten zur Nutzeridentifizierung werfen datenschutzrechtliche Probleme auf, da sie zur Erstellung umfangreicher Nutzerprofile verwendet werden können. Zwar existieren technische Ansätze, die das Spannungsverhältnis zwischen Identifizierung und Anonymität lösen sollen.[1261] Dennoch haben sich die Gesetzgeber weltweit entschlossen, Metadaten zur Nutzeridentifizierung vom rechtlichen Schutz durch Umgehungsvorschriften auszunehmen. Das bedeutet, daß ein Angreifer nicht gegen Umgehungsvorschriften verstößt, wenn er nutzeridentifizierende Metadaten verändert, entfernt oder falsche Metadaten bereitstellt.[1262]

Die europäische Richtlinie zum Urheberrecht in der Informationsgesellschaft betont, daß Identifizierungssysteme den Schutz der Privatspähre gemäß der EG-Datenschutzrichtlinie[1263] wahren müssen.[1264] Die U.S.-amerikanische Regelung des 17 U.S.C. § 1202 stellt in Abs. c ausdrücklich fest, daß Metadaten zur Nutzeridentifizierung nicht erfaßt sind. Dadurch sollte ebenfalls datenschutzrechtlichen Bedenken begegnet werden.[1265]

II. Obligatorischer Einsatz von DRM-Komponenten

1. Obligatorischer Einsatz technischer Schutzmaßnahmen

Neben den dargestellten umfangreichen Regelungen, die die Umgehung technischer Schutzmaßnahmen verbieten,[1266] bestehen mitunter Vorschriften, die den Einsatz technischer Schutzmaßnahmen gesetzlich vorschreiben. Danach müssen beispielsweise Endgeräte über bestimmte DRM-Komponenten verfügen. Durch solche Vorschriften will der Gesetzgeber entweder erreichen, daß sich ein DRM-System am Markt durchsetzt. Oder es soll erreicht werden, daß Endgeräte, die nicht über

---

[1260] Zu dieser Einsatzmöglichkeit von Metadaten s. oben Teil 1, C II 3.

[1261] S. dazu oben Teil 1, E V.

[1262] Unabhängig von speziellen Umgehungsvorschriften können solche Handlungen jedoch u. U. sonstige Rechtsvorschriften verletzen.

[1263] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. 10. 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG Nr. L 281 vom 23. 11. 1995, S. 31 ff.

[1264] Erwägungsgrund 57 der Richtlinie, ABl. EG Nr. L 167 vom 22. 6. 2001, S. 10, 15.

[1265] *U.S. House of Representatives*, H.R. Rep. No. 105–551, Part 1, S. 22; *N. B. Nimmer/D. Nimmer*, § 12A.08[C][2][a], S. 12A-96 f.; s. a. 17 U.S.C. § 1205.

[1266] S. dazu oben Teil 2, D I 2.

DRM-Komponenten verfügen und mit denen der Schutz eines bestehenden DRM-Systems umgangen werden könnte, am Markt nur schwierig erhältlich sind. Dadurch kann die Sicherheit dieses DRM-Systems erhöht werden.

Gesetzliche Regelungen zum obligatorischen Einsatz technischer Schutzmaßnahmen sind selten und regelmäßig auf enge Anwendungsfelder beschränkt. Die wichtigen Umgehungsvorschriften – die europäische Richtlinie zum Urheberrecht in der Informationsgesellschaft und der U.S.-amerikanische „Digital Millennium Copyright Act" – stellen jeweils klar, daß die Verwendung technischer Schutzmaßnahmen nicht gesetzlich vorgeschrieben ist.[1267] Auch im U.S.-amerikanischen Pay-TV-Bereich besteht keine gesetzliche Verpflichtung, ein bestimmtes Schutzsystem einzusetzen.[1268] Diese Zurückhaltung der Gesetzgeber ist auch ein Ergebnis jahrelanger Diskussionen der beteiligten Industriebranchen. Bisher hat sich die Computerindustrie immer zurückhaltend bis abweisend gezeigt, wenn sie von der Musik- und Filmindustrie aufgefordert wurde, technische Schutzmaßnahmen in Konsumenten-PCs einzubauen.[1269] Im folgenden sollen die gesetzlichen Vorschriften dargestellt werden, die dennoch eine solche Verpflichtung vorsehen.

a) Europäischer und deutscher Rechtsrahmen

Im Oktober 1995 erließen das Europäischen Parlament und der Rat eine Richtlinie zur Übertragung von Fersehsignalen („Ferhsehsignalübertragungs-Richtlinie").[1270] Die Richtlinie behandelt Normierungsfragen im

[1267] Bezüglich der Richtlinie s. Erwägungsgrund 48 der Richtlinie, ABl. EG Nr. L 167 vom 22. 6. 2001, S. 10, 14. Beim DMCA ist zu unterscheiden: Zwar sieht der DMCA für analoge Videorekorder und -kameras obligatorische Schutzmaßnahmen vor, s. dazu unten Teil 2, D II 1 b. Die allgemeinen Regelungen des DMCA in 17 U.S.C. § 1201 (a) und (b) enthalten aber keine gesetzliche Verpflichtung, technische Schutzmaßnahmen einzusetzen, s. 17 U.S.C. § 1201 (c) (3). S. zum ganzen *N. B. Nimmer/D. Nimmer*, § 12A.05[C], S. 12A-59 ff.

[1268] Im analogen Pay-TV-Bereich wäre die FCC nach 47 U.S.C. § 605 (h) berechtigt gewesen, einen allgemeinen Verschlüsselungsstandard für Satelliten-Pay-TV verbindlich festzulegen. 1990 lehnte sie dies jedoch ab, s. *Federal Communications Commission*, 5 FCC Rcd. 2710 (F.C.C. Apr. 25, 1990), und erkannte statt dessen den „Videocipher II"-Industriestandard als de-facto-Standard an. Im digitalen Pay-TV-Bereich hat die FCC ebenfalls keinen Standard verbindlich festgelegt. Jedoch verfolgt sie eng die Aktivitäten der OpenCable-Initiative, die einen de-facto-Standard entwickelt, s. oben Fn. 909 f.

[1269] S. dazu auch *Marks/Turnbull*, EIPR 2000, 198, 203 f., 205. In den USA liegt dies zumindest auch an einem bestimmten, in der Computerbranche weit verbreiteten Verständnis der Aufgaben des Staates im High-Tech-Sektor. Nach dieser Auffassung war die Entwicklung der U.S.-Computerindustrie deshalb so erfolgreich, weil der Staat und damit auch der Gesetzgeber in die gesamte Entwicklung möglichst wenig eingegriffen hat, s. *Marks/Turnbull*, EIPR 2000, 198, 205.

[1270] Richtlinie 95/47/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 über die Anwendung von Normen für die Übertragung von Fernsehsignalen, ABl. EG Nr. L 281 vom 23. 11. 1995, S. 51 ff.

Bereich des Breitbildschirm-Formats 16:9 sowie des digitalen Fernsehens. Dabei wurde es für notwendig erachtet, bestimmte technische Rahmenbedingungen und technische Einzelsysteme zu standardisieren. Die Kommission sprach sich angesichts früherer negativer Erfahrungen im HDTV-Bereich gegen technische Standardisierungen hoheitlicher Natur aus, sondern wollte dies den Marktkräften überlassen.[1271] Daher ging dem Erlaß der Richtlinie ein breiter Konsultations- und Kooperationsprozeß mit den betroffenen Unternehmen und technischen Normierungsgremien voraus. Im Rahmen dieses Prozesses kamen unter der Leitung des „European Project for Digital Video Broadcasting" mehrere Vereinbarungen über Zugangskontrollsysteme beim digitalen Pay-TV zustande.[1272] Unter anderem einigte man sich darauf, in Pay-TV-Systemen einen einheitlichen Standard zur Ver- und Entschlüsselung der Videodaten zu verwenden („Common Scrambling Algorithm").[1273]

In Art. 4 lit. a der Fernsehsignalübertragungs-Richtlinie wird vorgeschrieben, daß alle Pay-TV-Decoder, die in der Europäischen Gemeinschaft verkauft oder vermietet werden und verschlüsselte Pay-TV-Signale entschlüsseln können, den „Common Scrambling Algorithm" verwenden müssen. Die Einzelheiten des „Common Scrambling Algorithm" werden in der Richtlinie nicht standardisiert.[1274] Zusätzlich wird verlangt, daß

[1271] S. dazu *Weisser*, ZUM 1997, 877, 888; *Europäische Kommission*, KOM (94) 455 endg. vom 25. 10. 1994, S. 3 ff.

[1272] Zu den technischen Grundlagen solcher „Conditional Access"-Systeme s. oben Teil 1, D II 2.

[1273] Der „Common Scrambling Algorithm" setzt sich aus einer Verschlüsselungs- („Scrambling Technology") und einer Entschlüsselungskomponente („Common Descrambling System") zusammen. Er ist für sich allein noch kein vollständiges Pay-TV-„Conditional Access"-System, da er nur bei der Verschlüsselung der Videodaten selbst, nicht bei der Verschlüsselung der sogenannten „Entitlement Control Messages" (ECMs) eingesetzt wird; s. dazu oben Fn. 522.

[1274] Art. 4 Fernsehsignalübertragungs-Richtlinie lautet wörtlich:

„Hinsichtlich der Zugangsberechtigung der Fernsehzuschauer zu digitalen Fernsehdiensten in der Europäischen Gemeinschaft gilt, unabhängig vom Übertragungsweg, folgendes:

a) Alle Kundengeräte, die in der Europäischen Gemeinschaft verkauft, vermietet oder in anderer Weise zur Verfügung gestellt werden und die verwürfelte digitale Fernsehsignale dekodieren können, müssen in der Lage sein,
   – solche Signale entsprechend dem gemeinsamen europäischen Verwürfelungs-Algorithmus, für den eine anerkannte europäische Normenorganisation als Verwalter fungiert, zu dekodieren; […]"

Mit dem „europäischen Verwürfelungs-Algorithmus" ist der „Common Scrambling Algorithm" gemeint, der von vier Unternehmen (Canal+ SA, dem Centre Commun d'Etudes de Télédiffusion et Télécommunications, Irdeto BV, New Datacom Ltd.) entwickelt wurde, und vom ETSI als anerkannter Normenorganisation verwaltet wird, s. *European Telecommunications Standards Institute*, DVB Scrambling Technology Licence and Non-Disclosure Agreement, S. 1; <http://www.etsi.org/dvbandca/DVB/Explanatorynote.doc>. Details des Algorithmus sind nicht veröffentlicht worden, können aber nach Abschluß eines „Non-Disclosure Agreements" vom ETSI als Verwalter be-

die Pay-TV-Decoder auch unverschlüsselte Videodaten wiedergeben können, Art. 4 lit. a 2. Spiegelstrich Fernsehsignalübertragungs-Richtlinie. Danach ist es unzulässig, Pay-TV-Decoder oder Fernseher auf den Markt zu bringen, die nur zum Empfang von Pay-TV und nicht von Free-TV geeignet sind.[1275]

Art. 4 lit. a Fernsehsignalübertragungs-Richtlinie wurde in § 5 Abs. 3 Fernsehsignalübertragungs-Gesetz (FÜG) sinngemäß in deutsches Recht umgesetzt.[1276] Aus sonstigen Vorschriften läßt sich in Deutschland keine Verpflichtung zum Einsatz technischer Schutzsysteme herleiten.[1277] Dies gilt jedenfalls für den hier interessierenden urheberrechtlichen Einsatzbereich von DRM-Systemen. In anderen Bereichen existieren dagegen gesetzliche Verpflichtungen zum Einsatz technischer Schutzmaßnahmen. So sind private Fernsehsender nach dem Rundfunkstaatsvertrag verpflichtet, jugendgefährdende Sendungen mit einer zusätzlichen Verschlüsselung zu versehen, wenn die Sendung tagsüber ausgestrahlt werden sollen. Dadurch soll verhindert werden, daß Kinder und Jugendliche die Sendungen anschauen können.[1278]

---

zogen werden, s. <http://www.etsi.org/dvbandca/DVB/DVBINTRO.htm>; s. zum ganzen auch *Cutts*, Electronics & Communications Engineering Journal 21, 25 (Februar 1997). Hinter dieser Vorschrift stehen wettbewerbsrechtliche Überlegungen: Die EG-Kommission, auf deren Vorschlag die Vorschrift in die Richtlinie aufgenommen wurde (*Europäische Kommission*, KOM (94) 455 endg. vom 25. 10. 1994, S. 5), wollte sicherstellen, daß der Anbieter eines Pay-TV-Dienstes nicht ein proprietäres Verschlüsselungssystem in die von ihm vertriebenen Pay-TV-Decoder einbaut und dessen Kunden dadurch nur noch den Pay-TV-Dienst dieses Anbieters nutzen können. Durch die Verwendung des „Common Scrambling Algorithm" soll der Wettbewerb unter den Pay-TV-Anbietern ermöglicht werden, s. Erwägungsgrund 17 der Fernsehsignalübertragungs-Richtlinie, S. 51, 52. Durch die Richtlinie werden nur die Hersteller von Pay-TV-Decodern verpflichtet, die Decoder DRM-kompatibel auszugestalten und DRM-geschützte Inhalte anzuzeigen, wenn sich der Inhalteanbieter eines solchen Schutzes bedient. Dagegen sind die Inhalteanbieter nicht verpflichtet, ihre Inhalte mit einem DRM-Schutz zu versehen.

[1275] Diese Vorschrift wurde vom Europäischen Parlament in der zweiten Lesung eingeführt. S. dazu *Ladeur*, ZUM 1998, 261, 267, der dies als Schutzklausel für den öffentlich-rechtlichen Rundfunk auffaßt.

[1276] Gesetz über die Anwendung von Normen für die Übertragung von Fernsehsignalen, BGBl. I vom 14. 11. 1997, S. 2710. In § 5 Abs. 3 FÜG wird der „Common Scrambling Algorithm" nicht explizit erwähnt, sondern nur umschrieben. Eine Regelung durch Rechtsverordnung wurde nicht für sinnvoll gehalten, s. Begründung zu § 5 des FÜG-Entwurfs, *Bundesregierung*, BT-Drs. 13/7337 vom 25. 3. 1997, S. 8.

[1277] Insbesondere läßt sich eine Verpflichtung, in Endgeräte technische Schutzmaßnahmen zu integrieren, nicht aus § 97 I 1 UrhG, § 1004 BGB herleiten, solange die fraglichen Geräte nicht ausschließlich für urheberrechtsverletzende Vervielfältigungen benutzt werden, s. *Wiechmann*, ZUM 1989, 111, 115 ff.; *Schack*, Rdnr. 683.

[1278] Zu den Einzelheiten s. § 3 Abs. 5 RfStV i. V. m. der übereinstimmenden Satzung der Landesmedienanstalten vom 19. 5. 2000 zur Gewährleistung des Jugendschutzes in digital verbreiteten Programmen des privaten Fernsehens, erhältlich unter <http://www.alm.de/aktuelles/presse/jusatz.doc>, sowie *Weisser*, NJW 2000, 3526, 3528 f.

b) U.S.-amerikanischer Rechtsrahmen

Auch in den USA wird die Verwendung technischer Schutzmaßnahmen vereinzelt vorgeschrieben. Nach jahrelangen Verhandlungen hatten sich 1989 führende Unterhaltungselektronik-Unternehmen mit der Tonträgerindustrie im Rahmen des sogenannten „Athens Agreement" darauf geeinigt, in DAT-Geräten für den privaten Konsumentenmarkt das „Serial Copy Management System" (SCMS) einzubauen.[1279] Dadurch sollten die Bedenken der Tonträgerindustrie zerstreut werden, ein digitales Aufnahmesystem für den privaten Konsumentenmarkt führe im Musiksektor zu unkontrollierbaren Raubkopien. Im „Athens Agreement" wurde auch vereinbart, in den einzelnen Ländern auf die Verabschiedung gesetzlicher Vorschriften zu drängen, die die Verwendung von SCMS in DAT-Geräten gesetzlich vorschreiben sollten.[1280]

Die Vereinbarungen des „Athens Agreement" und weitere Kompromisse zwischen Musikverlagen und Unterhaltungselektronikherstellern wurden zur Grundlage für den „Audio Home Recording Act" (AHRA), der in den USA 1992 in Kraft trat.[1281] Nach 17 U.S.C. § 1002 (a) müssen alle in den USA hergestellten, vertriebenen oder in die USA importierten digitalen Aufnahmegeräte, die für den privaten Konsumenten bestimmt sind,[1282] mit SCMS ausgestattet sein.[1283] Faktisch werden von dieser Vor-

---

[1279] Zu den technischen Grundlagen von SCMS s. oben Teil 1, D II 1.

[1280] S. *U.S. Congress, Office of Technology Assessment*, Copyright & Home Copying, S. 28. Zu früheren Gesetzgebungsvorschlägen aus dem Jahr 1987 in bezug auf geplante DAT-Kopierschutzmechanismen s. *U.S. Congress, Office of Technology Assessment*, a. a. O., S. 57 f.; *Lutzker*, 11 Cardozo Arts & Ent. L. J. 145, 171 ff. (1992); *Sciorra*, 11 Cardozo Arts & Ent. L. J. 905, 924 ff. (1993).

[1281] Pub. L. No. 102–563, 106 Stat. 424, kodifiziert in 17 U.S.C. §§ 1001–1010. Zum AHRA allgemein s. *N. B. Nimmer/D. Nimmer*, § 8B.01, S. 8B-5 ff.; *McKuin*, 16 Hastings Comm/Ent L.J. 311 ff. (1994); *Lutzker*, 11 Cardozo Arts & Ent. L. J. 145 ff. (1992); Wand, S. 195 ff. Zur Entstehungsgeschichte, die durch starken Lobbyismus geprägt war, wodurch das Gesetz faktisch den Inhalt des „Athens Agreement" und eines Vergleich zwischen Musikverlegern und Sony nach einer Klage der Verleger übernahm, s. *McKuin*, a. a. O., S. 322; *Lutzker*, a. a. O., S. 145 ff.; *N. B. Nimmer/D. Nimmer*, § 8B.01, S. 8B-6 ff.; *U.S. Congress, Office of Technology Assessment*, Copyright & Home Copying, S. 28; *Marks/Turnbull*, EIPR 2000, 198, 203; *Garnett* in: World Intellectual Property Organization (Hrsg.), S. 101, 108; *Wand*, S. 196 f. Im Frühjahr 1996 versuchte die Film- und Unterhaltungselektronikindustrie, sich mit der Computerindustrie auf einen ähnlichen Gesetzgebungsvorschlag im Filmsektor (mitunter als „Video Home Recording Act" bezeichnet) zu einigen. Danach hätten alle Geräte, die Videoinhalte aufnehmen können, eingebettete Kopierkontrollinformationen erkennen und beachten müssen. Die Computerindustrie wehrte sich heftig gegen diesen Vorschlag, der dann auch nicht verwirklicht wurde; s. *Marks/Turnbull*, EIPR 2000, 198, 205.

[1282] Professionelle Geräte sind ausgenommen, s. 17 U.S.C. § 1001 (3) (A) und § 1001 (10).

[1283] Gem. 17 U.S.C. § 1002 (a) (2) und (3) können die Geräte grundsätzlich auch mit einem anderen, äquivalenten Schutzsystem ausgestattet sein; diese Regelung hat in der Praxis keine Rolle gespielt. Während in Gesetzesentwürfen noch geplant war, eine

schrift nur DAT-Geräte erfaßt, da sich andere digitale Aufnahmegeräte entweder nicht am Markt durchsetzen konnten[1284] oder nicht unter die Vorschrift fallen.[1285] Die Verpflichtung trifft nur die Hersteller von digitalen Aufnahmegeräten. Die Anbieter von Audioinhalten sind nicht verpflichtet, SCMS auch zu verwenden.[1286] Auch in der Europäischen Union wurde darauf hingewirkt, die Verwendung von Kopierschutzverfahren wie SCMS in Endgeräten gesetzlich vorzuschreiben.[1287] Anders als in den USA konnten sich diese Vorschläge in Europa nicht durchsetzen.[1288]

Der U.S.-amerikanische Digital Millennium Copyright Act fügte 1998 eine Regelung in den Copyright Act ein, nach der alle analogen Videorekorder und -kameras, die in die Vereinigten Staaten importiert beziehungsweise dort hergestellt oder verkauft werden, mit analogen Kopierschutzverfahren des Unternehmens Macrovision versehen sein müssen, 17 U.S.C. § 1201 (k) (1) (A) und (B) S. 2.[1289] Danach müssen die Geräte die entsprechenden Kopierschutzinformationen in Videodaten auslesen, dürfen geschützte Videoinhalte nicht kopieren und müssen ihrerseits die Kopierschutzverfahren in aufgenommene Videoinhalte einbetten können, 17 U.S.C. § 1201 (k) (4) (C). Professionelle Film- und Fernsehausrüstung wird von der Regelung ausdrücklich ausgenommen, 17 U.S.C. § 1201 (k) (3) (B). Schon vor dieser gesetzlichen Regelung waren die Kopierschutzverfahren von Macrovision in den USA weit verbreitet.

2. Obligatorischer Einsatz von Metadaten

Wie gezeigt wurde, bestehen vereinzelt Regelungen, die die Verwendung technischer Schutzmaßnahmen in Endgeräten gesetzlich vorschreiben.

---

genaue technische Definition des SCMS festzulegen, ist eine solche in der endgültigen Fassung nicht enthalten, s. *N. B. Nimmer/D. Nimmer*, § 8B.03[B], S. 8B-46.

[1284] So die „Digital Compact Cassette" (DCC) von Philips und letztlich auch die MiniDisc von Sony.

[1285] So entschied der 9th Circuit Court of Appeals in Kalifornien im Jahr 1999 in einer wegweisenden Entscheidung, daß MP3-Player nicht unter den Anwendungsbereich des AHRA fallen, s. Recording Industry Association of America, Inc. v. Diamond Multimedia Systems, Inc., 180 F.3d 1072 (9th Cir. 1999), auf deutsch abgedruckt in GRUR Int. 1999, 974. S. zu dieser wichtigen Entscheidung *Allemann*, 79 Tex. L. Rev. 189 (2000); *Webb*, 7 Rich. J. L. & Tech. 5 (2000); *Gonzalez*, 15 Berkeley Tech. L. J. 67 (2000).

[1286] S. dazu unten Teil 2, D II 2.

[1287] Ein entsprechender Vorschlag findet sich im urheberrechtlichen Grünbuch der *Europäischen Kommission*, KOM (88) 172 endg. vom 7. 6. 1988, S. 129 ff.; s. dazu *Wand*, S. 95 ff.

[1288] *Wiechmann*, ZUM 1989, 111, 112.

[1289] Zu den technischen Grundlagen dieser Verfahren („automatic gain control" und „Colorstripe") s. oben Fn. 503. Diese Kopierschutzverfahren müssen nicht beim Filmen mit einer Videokamera eingesetzt werden, 17 U.S.C. § 1201 (k) (3) (A). Auch bezieht sich die Regelung nicht auf Videorekorder, die vor dem Inkrafttreten des DMCA hergestellt wurden, 17 U.S.C. § 1201 (k) (3) (C). S. zur gesamten Regelung im Überblick *Pollack*, 17 Cardozo Arts & Ent. L. J. 47, 103 ff. (1999).

Dagegen existiert keine Regelung, in der den Inhalteanbietern oder DRM-Systembetreibern die Verwendung von Metadaten gesetzlich vorgeschrieben wird.[1290] Der U.S.-amerikanische „Audio Home Recording Act" stellt in 17 U.S.C. § 1002 (d) (2) klar, daß das bei DAT-Geräten eingesetzte „Serial Copy Management System" die Anbieter von Audioinhalten nicht verpflichtet, ihre Inhalte mit SCMS zu versehen. Auch der durch den „Digital Millennium Copyright Act" eingefügte 17 U.S.C. § 1202[1291] enthält keine solche Verpflichtung.[1292] Die europäische Richtlinie zum zum Urheberrecht in der Informationsgesellschaft äußert sich nicht direkt zu dieser Frage. Sie begrüßt nur die internationale Normierung von Metadaten; Normierungsinitiativen sollten gefördert werden, um Inkompatibilitäten von DRM-Systemen zu verhindern.[1293]

III. Zusammenfassung

In den letzten Jahren haben die Gesetzgeber weltweit Regelungen geschaffen, die die Umgehung technischer Schutzmaßnahmen verbieten.[1294] Dabei werden regelmäßig die tatsächliche Umgehung technischer Schutzmaßnahmen, die Herstellung und Verbreitung von Umgehungsvorrichtungen („vorbereitende Handlungen") sowie die Veränderung oder Entfernung von Metadaten verboten. Daneben bestehen sehr vereinzelt

[1290] Vgl. *v. Lewinski*, GRUR Int. 1997, 677; *de Kroon* in: Hugenholtz (Hrsg.), S. 229, 253, 257; Anmerkung 14.06 zu Art. 14 *WCT Basic Proposal*; gemeinsame Erklärung der Vertragsstaaten zu Art. 12 WCT, erhältlich unter <http://www.wipo.int/eng/iplex>; s. a. 17 U.S.C. § 1002 (d) (2).

[1291] S. dazu oben Teil 2, D I 3 b aa 4.

[1292] S. *N. B. Nimmer/D. Nimmer*, § 12A.08, S. 12A-89; *D. Nimmer*, 46 J. Copyright Soc'y U.S.A. 401, 417 (1999).

[1293] Erwägungsgrund 54 der Richtlinie, ABl. EG Nr. L 167 vom 22. 6. 2001, S. 10, 15.

[1294] Im Rahmen dieser Untersuchung wurde nur auf die völkerrechtliche, europarechtliche, deutsche und U.S.-amerikanische Rechtslage eingegangen. In vielen anderen Ländern existieren ähnliche Regelungen. So entschied der australische High Court 1992 in einer umstrittenen Entscheidung, daß die Herstellung eines illegalen Dongles eine Kopie des Dongle-Prüfprogramms bedinge und daher das Vervielfältigungsrecht des Urhebers des Dongle-Prüfprogramms verletze, Autodesk, Inc. v. Dyason, 173 Commonwealth Law Reports 330 (1991–1992); s. dazu *Prescott*, EIPR 1992, 191 ff.; *Lahore*, EIPR 1992, 482, 431 f. Zur Rechtslage in Australien nach Umsetzung der WIPO-Verträge s. *Fitzpatrick*, EIPR 2000, 214, 224; zur Rechtslage in Frankreich s. Art. L. 122–6–2 Code de la Propriété Intellectuelle; *Beucher/Engels*, CR 1998, 101, 107; *Debbasch*, Rdnr. 716 ff.; zur (inzwischen veränderten) Rechtslage in Großbritannien s. *Beucher/Engels*, CR 1998, 101, 107 f.; zur Rechtslage in Japan s. Art. 120bis UrhG, erhältlich unter <http://www.cric.or.jp/cric_e/ecolj/cl78.html>; zur Rechtslage in Italien s. <http://www.softwarelibero.it/docs/siae-en.shtml>; zur Rechtslage in Ungarn s. *Hegyi*, GRUR Int. 2000, 325, 342. Einen Überblick über die Rechtslage in Kanada, Finnland, Frankreich, Italien, den Niederlanden, der Schweiz und Schweden gibt *Dellebeke* (Hrsg.), S. 343 ff.

Regelungen, die den Einsatz technischer Schutzmaßnahmen in Endgeräten gesetzlich vorschreiben.

Dieser Regelungskomplex ist bemerkenswert, da die generelle Einsicht, das Urheberrecht hinke dem technischen Fortschritt hinterher,[1295] in diesem Bereich nur eingeschränkt zutrifft. Wenn im Jahr 1996 auf völkerrechtlicher Ebene ein rechtlicher Schutz gegen die Umgehung technischer Schutzmaßnahmen vereinbart wurde, ohne daß nennenswerte Erfahrungen mit solchen Regelungen auf nationaler Ebene bestanden, und ohne daß sichere Prognosen darüber angestellt werden konnten, welche Bedeutung technische Schutzmaßnahmen in Zukunft haben werden, so zeigt dies den enormen rechtspolitischen Willen, die Informationsgesellschaft schon in ihrer Anfangsphase zu formen.

Der Regelungskomplex berührt grundsätzliche Fragen. Der rechtliche Umgehungsschutz hat mit dem Urheberrecht im klassischen Sinne sehr wenig zu tun.[1296] Mitunter wird der Begriff „paracopyright" gebraucht.[1297] In den europäischen Staaten finden sich Vorschriften des rechtlichen Umgehungsschutzes in Strafgesetzen, in Urheberrechtsgesetzen, in Wettbewerbsgesetzen sowie in Telekommunikations- und Rundfunkgesetzen.[1298] Allenfalls der Zusammenhang mit der Ausübung oder Verletzung von Urheber- und Leistungsschutzrechten rechtfertigt die Aufnahme solcher Regelungen in Urheberrechtsgesetze. Eine Integration der Vorschriften zum Umgehungsschutz in das Urheberrecht ist nicht unproblematisch. Der rechtliche Umgehungsschutz befaßt sich unter anderem mit technischen Schutzmaßnahmen, die den Zugang zu digitalen Inhalten kontrollieren. Der Zugang zu Information an sich wird von den traditionellen urheberrechtlichen Verwertungsrechten nicht erfaßt. Das Verhältnis zwischen einem Recht auf Zugangskontrolle und den Verwertungsrechten ist weitgehend unklar.[1299]

Der Regelungskomplex betrifft Fragen des Zugangs und der Nutzung von Information im weitesten Sinne. Fragen des Investitionsschutzes gewinnen immer größere Bedeutung.[1300] Der Schwerpunkt der Vorschriften zum rechtlichen Umgehungsschutz liegt auf dem Verbot vorbereitender

---

[1295] Vgl. nur *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, Einl., Rdnr. 1.

[1296] So auch das Committee of Commerce des U.S.-Repräsentantenhauses: „These […] provisions have little, if anything, to do with copyright law.", H.R. Rep. No. 105–551, Part 2, 105th Cong., 2d Sess. (July 22, 1998), S. 24; s. weiterhin *Wand*, S. 36.

[1297] *Nimmer*, § 12A.17[B], S. 12A-125.

[1298] S. dazu *Helberger*, ZUM 1999, 295, 305; *Beucher/Engels*, CR 1998, 101, 107 f.; *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 214 ff. Einen Überblick über Umgehungsvorschriften außerhalb des Urheberrechts gibt *Dusollier*, Anti Circumvention Protection Outside Copyright.

[1299] Ebenso *Dusollier*, EIPR 1999, 285, 291; s. a. *Bechtold*, GRUR 1998, 18, 26 f.

[1300] *Dusollier*, EIPR 1999, 285, 296. Dies zeigt auch die Zugangskontrollrichtlinie, die u. a. erlassen wurde, um die Rentabilität der geschützten Dienste zu gewährleisten, s. Erwägungsgrund 6 der Zugangskontrollrichtlinie, S. 54.

Handlungen, die aus Sicht der Rechteinhaber die größte Gefahr darstellen.[1301] Dies führt zu einer Akzentverschiebung: Während das klassische Urheberrecht primär die unberechtigte Nutzungshandlung an sich sanktioniert, geht es beim rechtlichen Umgehungsschutz an erster Stelle um die Kontrolle der Herstellung von Vorrichtungen, die diese unberechtigten Nutzungshandlungen erst ermöglichen.[1302] Darin läßt sich ein Trend zu indirekter Regulierung erkennen.[1303]

[1301] *N. B. Nimmer/D. Nimmer*, § 12A.03, S. 12A-15.
[1302] Ebenso *R. T. Nimmer*, § 12A.03, S. 12A-15.
[1303] S. dazu auch unten Teil 5.

Teil 3: Vom Urheber- zum Informationsrecht

In den beiden ersten Teilen dieser Arbeit wurden die technischen und rechtlichen Grundlagen von DRM-Systemen dargestellt. In vorliegenden dritten Teil werden zunächst die Ergebnisse der beiden vorangegangenen Teile zusammengeführt, um danach – darauf aufbauend – darzulegen, welche Auswirkungen DRM-Systeme auf das herkömmliche Urheberrecht haben.[1304] Diese Frage wird unter rechtlichen (dazu unten A II) und rechtsökonomischen Gesichtspunkten (dazu unten A III) untersucht. Dabei zeigt sich ein Paradigmenwechsel im Schutz der Inhalteanbieter. Um die rechtsökonomische und rechtliche Bewertung dieses Paradigmenwechsels geht es in den darauf folgenden Abschnitten B I und B II.

Vorab sei ein Hinweis gestattet, wie die folgenden Ausführungen zu verstehen sind. DRM-Systeme sind kein monolithisches Phänomen. Sie können sich aus zahllosen verschiedenen technischen Komponenten zusammensetzen. Auch existiert eine Vielzahl unterschiedlicher rechtlicher Schutzmöglichkeiten und gesetzlicher Vorschriften, die im DRM-Bereich einschlägig sein können. Die daraus resultierende Vielfalt unterschiedlicher DRM-Systeme macht es schwierig, allgemeine Aussagen über die Implikationen des Digital Rights Management zu machen. Wenn dies im folgenden dennoch versucht wird, so ist zu bedenken, daß es sich dabei um Aussagen über ein modellhaftes DRM-System handelt, das möglichst viele der dargestellten technischen und rechtlichen Schutzmechanismen in sich vereint.[1305] In der Realität werden viele Systeme nur über einen Ausschnitt dieser technischen und rechtlichen Schutzmechanismen verfügen. Auf solche Systeme trifft die folgende Analyse ebenso zu, wenn auch teilweise in abgeschwächter Form. Die folgenden Ausführungen orientieren sich bewußt an einem möglichst umfassenden DRM-System mit einem hohen Schutzniveau, da die Implikationen des Digital Rights Management auf das Urheberrecht in einem solchen System am deutlichsten hervortreten. Dabei nimmt die Untersuchung die Gefahren in Kauf, die

---

[1304] Dabei werden bewußt Ergebnisse der vorangegangenen Teile erneut aufgegriffen und im Überblick dargestellt, um Querverbindungen zwischen unterschiedlichen Bereichen zu verdeutlichen.

[1305] Die Skizzierung umfassender DRM-Systeme in der Einführung zu dieser Untersuchung (s. bei Fn. 5) kommt einem solchen Modellsystem am nächsten. Auch kommen die umfangreichen Schutzmechanismen in DVDs dem Modellsystem näher als der bloße Kopierschutz in DAT-Geräten.

aus den notwendigen Abstraktionen und Vereinfachungen einer Modellbetrachtung resultieren.[1306]

A. Paradigmenwechsel

I. Allgemeines

1. These vom Tod des Urheberrechts

> *Information wants to be free.*[1307]
>
> *Copyright law is totally out of date. It is a Gutenberg artifact. Since it is a reactive process, it will probably have to break down completely before it is corrected.*[1308]

Prominente Protagonisten des „Cyberspace" – insbesondere *John Perry Barlow*, der Mitbegründer der „Electronic Frontier Foundation", aber auch *Nicholas Negroponte*, der Leiter des MIT Media Lab – verbreiten die These, das Urheberrecht habe im Internet keine Zukunft mehr. Das herkömmliche Urheberrecht sei auf den Schutz von Werken fokussiert, die in einem physischen Werkexemplar (Buch, Schallplatte etc.) verkörpert seien. In einer digitalisierten, vernetzten Umgebung bestünden keine dauerhaften Werkverkörperungen mehr. Ein Werk sei in einem Computernetzwerk nur noch eine Ansammlung elektrischer Spannungszustände.[1309] Darauf sei das herkömmliche Urheberrecht nicht zugeschnitten. Hinzu trete die Schwierigkeit der Rechtsdurchsetzung von Urheberrechten im digitalen Bereich, die durch die Internationalität des Internet bedingt sei.[1310]

[1306] Auch ist darauf hinzuweisen, daß sich viele Literaturstellen, die im folgenden zitiert werden, nicht explizit mit DRM-Systemen beschäftigen. Vielmehr behandeln sie oftmals Fragen des vertraglichen oder aber des technischen Schutzes von Inhalteanbietern. Diese Schutzmechanismen sind Ausschnitte eines umfassenden DRM-Systems, das u. a. auf einem technischen und vertraglichen Schutz aufbaut. Auch wenn die Literaturstellen damit nur Teilaspekte von DRM-Systemen behandeln, können sie für die vorliegende Untersuchung voll verwertet werden. Aus Gründen der Übersichtlichkeit wird im folgenden nicht immer explizit darauf hingewiesen, daß sich eine zitierte Literaturstelle nur mit einem Teilaspekt von DRM-Systemen beschäftigt.

[1307] *Brand*, S. 202. Dieses oft angeführte Zitat aus dem Jahre 1988 ist verkürzt. *Brand* schreibt vollständig: „Information wants to be free. Information also wants to be expensive. Information wants to be free because it has become so cheap to distribute, copy, and recombined – too cheap to meter. It wants to be expensive, because it can be immeasurably valuable to the recipient. That tension will not go away. It leads to endless wrenching debates about price, copyright, ‚intellectual property', and the moral rightness of casual distribution, because each round of new devices makes the tension worse, not better", *ebda.*

[1308] *Negroponte*, S. 58.

[1309] *Barlow*, Wired 2.03, S. 84, 86 (März 1994).

[1310] *Barlow*, Wired 2.03, S. 84, 86 (März 1994). Diese urheberrechtliche Diskussion bettet sich in die allgemeinere Diskussion ein, ob das Internet überhaupt staatlich regulierbar ist. Daran zweifeln viele der Protagonisten des Cyberspace, beispielsweise der

Die Krise des Urheberrechts zeige sich auch daran, daß Urheberrechtsverletzungen gesellschaftlich nur noch als Kavaliersdelikte betrachtet würden.[1311] Das herkömmliche Urheberrecht sei zum Scheitern verdammt.[1312] Was an seine Stelle trete, sei noch unklar.[1313]

Auch wenn die Schlußfolgerungen der Protagonisten im einzelnen überzogen sein mögen, trifft doch die Analyse der Symptome in vielen Fällen zu.[1314] Im digitalen Umfeld ist es ein leichtes, Kopien digitaler Inhalte zu erstellen – Original und Kopie sind nicht mehr voneinander zu unterscheiden. Das Internet und P2P-Systeme wie Napster ermöglichen heute jedem Jugendlichen die Verbreitung digitaler Inhalte an ein Millionenpublikum. Dies war früher großen Medienkonzernen mit entspre-

---

EFF-Mitgründer *John Gilmore* („The Net interprets censorship as damage and routes around it"; s. <http://www.toad.com/gnu>) und *John Perry Barlow*, s. insbesondere seine „Declaration of the Independence of Cyberspace" („Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. […] I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. […] Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions. […] You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions. […] Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.") S. zu diesen und anderen Aussagen *Greenleaf*, 21 U. New South Wales L. J. 593, 594 ff. (1998); s. dazu aus juristischer Sicht *Johnson/Post*, 48 Stan. L. Rev. 1367 (1996), sowie *Lessig*, S. 192 f.; *Netanel*, 79 Tex. L. Rev. 447, 448 (2000); *ders.*, 88 Cal. L. Rev. 395 ff. (2000); *N.N.*, 112 Harv. L. Rev. 1574, 1680 ff. (1999); *Shapiro*, 8 Seton Hall. Const. L. J. 703 ff. (1998); *Spar* in: Cutler/Haufler/Porter (Hrsg.), S. 31 ff.; *Goldsmith*, 65 U. Chi. L. Rev. 1199 ff. (1998); *Lemley*, 73 Chi.-Kent L. Rev. 1257, 1265 f. (1998).

1311 *Barlow*, Wired 2.03, S. 84, 88 (März 1994), weist auf das verbreitete Raubkopieren von Computersoftware hin und meint: „Whenever there is such profound divergence between law and social practice, it is not society that adapts"; s. a. *ebda.*, S. 129. Als weiteres Beispiel nennt *Barlow* den überragenden Erfolg des P2P-Systems Napster, s. *Barlow*, Wired 8.10, S. 240 (Oktober 2000).

1312 *Negroponte*, S. 58; in diese Richtung auch *Kelsey/Schneier*, S. 3 f. Noch extremer *Barlow*, Wired 2.03, S. 84, 89 (März 1994): „It may well be that when the current system of intellectual property law has collapsed, as seems inevitable, that no new legal structure will arise in its place."

1313 *Barlow*, Wired 8.10, S. 240, 252 (Oktober 2000). S. zum ganzen auch *Masson*, 71 Ind. L. J. 1049 ff. (1996); *Gimbel*, 50 Stan. L. Rev. 1671, 1672 ff. (1998).

1314 Der Verfasser teilt nicht die in juristischen Kreisen wohl verbreitete Auffassung, daß man die extremen Thesen von *Barlow* und anderen am besten einfach ignorieren sollte. Die Entwicklung der letzten Jahre – u. a. der Erfolg von Napster – hat gezeigt, daß diese Thesen zumindest wert sind, diskutiert zu werden. Sie haben eine Vielzahl von wissenschaftlichen Arbeiten und politischen Diskussionen beeinflußt; ebenso *Netanel*, 88 Cal. L. Rev. 395, 398 (2000); *Shapiro*, 8 Seton Hall Const. L. J. 703, 706 f. (1998); s. a. *Wittgenstein*, UFITA 2000, 39 ff.

chenden finanziellen Ressourcen vorbehalten.[1315] Bedenkt man zusätzlich die Internationalität des Internet, so erscheint ein effektiver Schutz durch das herkömmliche Urheberrecht in Datennetzen zumindest schwer möglich.[1316]

Daher ist es nicht verwunderlich, daß Inhalteanbieter im digitalen Umfeld zunehmend auf Schutzmechanismen außerhalb des herkömmlichen Urheberrechts setzen. Gerade in DRM-Systemen entstehen neben dem Urheberrecht andere Schutzmechanismen, die die Schwächen des Urheberrechts im digitalen Umfeld zumindest abzumildern versprechen:[1317] „The answer *to* the machine is *in* the machine."[1318]

2. Unterschiedliche Schutzmechanismen für digitale Inhalte

Will ein Urheber seine Verwertungsinteressen schützen – beispielsweise das Interesse, die Erstellung unberechtigter Kopien von Werken zu verhindern –, so stehen ihm dafür neben dem Schutz durch die Ausschließlichkeitsrechte, die das Urheberrecht dem Urheber gewährt, grundsätzlich mehrere Schutzmechanismen zur Verfügung.[1319] Er kann mit den einzelnen Nutzern Verträge abschließt, in denen die Bedingungen der Nutzung des Werks geregelt sind (*vertraglicher Urheberschutz*).[1320] Weiterhin können die Interessen der Urheber durch technische Gegebenheiten geschützt sein (*faktischer Urheberschutz*): Vor der Entwicklung von Fotokopiergeräten stellte das Vervielfältigen von Schriftwerken für Urheber keine ernstzunehmende Gefahr dar; das Abschreiben von Texten ist

---

[1315] *Barlow*, Wired 8.10, S. 240 (Oktober 2000); in diese Richtung auch *Negroponte*, S. 59 f.; *Kelsey/Schneier*, S. 4.

[1316] Trotzdem muß man sich der Eindimensionalität solcher Aussagen bewußt sein: Zwar steigt im Internet die Gefahr von Raubkopien digitaler Inhalte wegen gesunkener Kopierkosten stark an. Andererseits sinken für die Anbieter die Kosten der Distribution, Vervielfältigung und Vermarktung digitaler Inhalte. Auch können spezielle Suchmaschinen die Rechtsverfolgung erleichtern. Um festzustellen, welche Auswirkungen das Internet auf die finanzielle Lage der Inhalteanbieter hat, müssten diese beiden Positionen gegeneinander abgewogen werden, s. *Boyle*, 53 Vand. L. Rev. 2007, 2017 (2000); *Koelman*, The Protection of Technological Measures, S. 3 f.

[1317] Ebenso *Gimbel*, 50 Stan. L. Rev. 1671, 1672 (1998): „The danger is not that copyright law will be infringed but that it will be supplanted". Auch *Barlow* bleibt nicht bei der These vom Tod des Urheberrechts stehen, s. *Barlow*, Wired 8.10, S. 240, 252 (Oktober 2000); vgl. weiterhin *Lessig*, S. 124 ff.

[1318] So der bekannte Titel eines Aufsatzes von *Clark* in: Hugenholtz (Hrsg.), S. 139 ff.

[1319] S. zum folgenden *Hardy*, 1996 U. Chi. Legal F. 21, 223 ff.

[1320] Darunter sind nicht Nutzungsverträge im streng urheberrechtlichen Sinne (§§ 31 ff. UrhG) zu verstehen. Vielmehr geht es um die Frage, wie ein Urheber seine Verwertungsinteressen schützen könnte, wenn ein Urheberrecht nicht existieren würde. In diesem Fall könnte der Urheber versuchen, seine Werke auf rein vertraglicher Basis zu schützen. Dies erinnert an die Stellung des Inhabers eines Geschäftsgeheimnisses, der das Geschäftsgeheimnis ebenfalls auf vertraglicher Basis schützt, indem er in Know-How-Lizenzverträge bestimmte Nutzungsbedingungen und beschränkungen einfügt.

zu zeitaufwendig. Mit der Verbreitung von Fotokopiergeräten fiel dieser faktische Urheberschutz weg.[1321] Daneben kann ein Urheber auch versuchen, seine Verwertungsinteressen gezielt durch technische Maßnahmen zu schützen; hier kommen DRM-Systeme ins Spiel (*technischer Urheberschutz*).[1322]

Ein Urheber kann seine Interessen durch eine Vielzahl unterschiedlicher Schutzmechanismen schützen. Das Urheber*recht* ist nur einer unter mehreren Schutzmechanismen. Dabei wird der Urheber durch die Summe aller Schutzmechanismen geschützt.[1323] Die Bedeutung eines bestimmten Schutzmechanismus kann im Verlauf der Zeit variieren. Vor der Verbreitung von Fotokopiergeräten bestand ein faktischer Urheberschutz gegen die massenhafte Vervielfältigung von Büchern und Zeitschriften. Als sich das Fotokopieren zunehmend auch im privaten Bereich verbreitete, fiel dieser faktische Urheberschutz weg. Der Gesetzgeber reagierte darauf im Jahr 1985 durch die Einführung einer Vergütungspflicht für die Betreiber von Kopiergeräten.[1324] Daran zeigt sich, daß zwar die Bedeutung eines bestimmten Schutzmechanismus' (hier: faktischer Urheberschutz) im Verlauf der Zeit abnehmen kann. Jedoch kann ein gleichbleibendes Schutzniveau gewährleistet werden, wenn zum Ausgleich andere Schutzmechanismen gestärkt werden.[1325]

Eine ähnliche Entwicklung läßt sich bei digitalen Medien beobachten. Dort wird die Erstellung von Kopien zum Kinderspiel. Original und Ko-

[1321] *Hardy*, 1996 U. Chi. Legal F. 217, 224 f. Den Unterschied zwischen analogen und digitalen Kopien und deren unterschiedliche Auswirkungen auf den Schutz des Urhebers analysiert aus ökonomischer Sicht *Shy*, S. 167 ff. Auf die Bedeutung dieses „faktischen" Kopierschutzes für die ökonomische Analyse des Urheberrechts weisen auch *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69, 105 f., und *Landes/Posner*, 18 J. Legal Stud. 325, 329 (1989), hin.

[1322] Neben den hier aufgeführten Schutzmechanismen bestehen noch weitere Schutzmechanismen. So spielt die Wahrscheinlichkeit, mit der eine Urheberrechtsverletzung entdeckt und verfolgt wird, eine Rolle: Je höher diese Wahrscheinlichkeit ist, desto besser sind die Interessen des Urhebers geschützt, s. *Hardy*, 1996 U. Chi. Legal F. 216, 223, Fn. 12. Auch können soziale Normen eine Rolle spielen. So ist die Hemmschwelle, ganze Bücher illegal zu kopieren, größer als die Hemmschwelle, Software oder MP3-Dateien zu kopieren. *Lemley*, 22 U. Dayton L. Rev. 547, 578 (1997), weist zu Recht daraufhin, daß im Bereich des Urheberrechts die Vorstellung des Laien, was er darf und was nicht, oftmals erheblich von der tatsächlichen Rechtslage abweicht.

[1323] *Hardy*, 1996 U. Chi. Legal F. 217, 226; *Lessig*, S. 87 f., 124 f.

[1324] Bei Verabschiedung des UrhG im Jahre 1965 waren Fotokopien im privaten Bereich noch ohne nennenswerte Bedeutung, *Bundesregierung*, BT-Drs. 10/837 vom 22. 12. 1983, S. 7, 9. Im Rahmen der Urheberrechtsnovelle 1985 wurde festgestellt, daß die Vervielfältigung urheberrechtlich geschützter Werke durch Fotokopierer ein solches Ausmaß angenommen habe, daß von einer neuen Nutzungsart gesprochen werden müsse, *Bundesregierung*, a. a. O., S. 10. Die damals eingeführte Betreiberabgabe des § 54 Abs. 2 UrhG a. F. wurde inzwischen erweitert und findet sich in §§ 54, 54 a UrhG wieder. Zu der vor 1985 geltenden Vergütungspflicht für Vervielfältigungen zu gewerblichen Zwecken nach § 54 Abs. 2 UrhG a. F. s. *Bundesregierung*, a. a. O., S. 21.

[1325] S. *Hardy*, 1996 U. Chi. Legal F. 217, 226 f.

pie unterscheiden sich qualitativ in keiner Weise. Der früher bestehende „faktische Urheberschutz", der durch praktische Probleme bei der Erstellung von Kopien entstand, fällt in digitalen Medien fast vollständig weg. Als Ausgleich könnte versucht werden, den rechtlichen Schutz des Urhebers zu verstärken. Tatsächlich wird die Verfolgung von Urheberrechtsverletzungen im digitalen Medien und internationalen Computernetzwerken jedoch immer schwieriger. Damit fällt in digitalen Medien nicht nur der „faktische Urheberschutz" aus, vielmehr verliert auch der Schutz durch das herkömmliche Urheberrecht deutlich an Effektivität.[1326] Ist in einem solchen Umfeld kann es sinvoll sein, auf andere Schutzmechanismen auszuweichen, deren Schutz im digitalen Umfeld effektiver und kostengünstiger ist.[1327]

Hinter dieser übergreifenden Betrachtungsweise des Urheberrechts steht eine Auffassung, die versucht, rechtliche Regulierungsmechanismen in bezug zu anderen Regulierungsmechanismen zu setzen. So kann die Freiheit des Einzelnen neben rechtlichen Beschränkungen auch durch Marktprozesse,[1328] durch soziale Normen[1329] und durch die Architektur des Raumes, in dem sich der Einzelne bewegt,[1330] beschränkt werden.[1331] Sollen in einem solchen Umfeld bestimmte Regulierungsziele erreicht werden, kann dies grundsätzlich durch jeden der unterschiedlichen Regulierungsmechanismen oder durch eine Kombination dieser Mechanismen erreicht werden.[1332] Dabei beeinflussen sich die Regulierungsmechanismen untereinander, sie können nicht getrennt voneinander betrachtet werden. Regulierungsziele können nicht nur erreicht werden, indem das menschliche Verhalten reguliert wird. Vielmehr ist es auch möglich, mit Hilfe eines Regulierungsmechanismus einen anderen Regulierungsme-

---

[1326] *Lessig*, S. 125.

[1327] *Lessig*, S. 122 f.

[1328] Der Preis eines Gutes beschränkt die Fähigkeit des Einzelnen, dieses Gut in beliebiger Anzahl zu erwerben, *Lessig*, 27 J. Legal Stud. 661, 663 (1998).

[1329] S. dazu aus rechtssoziologischer Sicht *Raiser*, S. 184 ff., auch zur Abgrenzung zwischen Recht und sozialer Norm. Aus der Sicht der ökonomischen Analyse des Rechts ist das grundlegende Werk von *Ellickson* zu nennen. Zur Entstehung sozialer Normen im Internet s. *Major*, 78 Wash. U. L. Q. 59 ff. (2000); *Lemley*, 73 Chi.-Kent L. Rev. 1257, 1261 ff. (1998).

[1330] Dies trifft nicht nur auf den Cyber*space* zu; s. *Lessig*, S. 91 f. und S. 123 („There are special laws about the theft of automobiles, planes, and boats. There are no special laws about the theft of skyscrapers. Cars, planes, and boats need protection. Skyscrapers pretty much take care of themselves.")

[1331] *Lessig*, 27 J. Legal Stud. 661, 662 (1998); *ders.*, S. 85 ff.; s. a. *Mitchell*, S. 159.

[1332] *Lessig*, 27 J. Legal Stud. 661, 664 (1998); *Lessig*, S. 92 f., führt als Beispiel das Regulierungsziel an, die Diebstahlshäufigkeit von Autoradios zu senken. Zu diesem Zweck kann die Strafandrohung für solche Taten erhöht werden (rechtliche Regulierung). Auch können Autoradios mit einem Sicherheitscode ausgestattet werden, durch den gewährleistet wird, daß das Autoradio nur in einem bestimmten Auto funktioniert (technische Regulierung).

chanismus zu beeinflussen, der dann wiederum das menschliche Verhalten beeinflußt. Dies eröffnet die Möglichkeit indirekter Regulierung.[1333]

Diese Überlegungen sind Teil des theoretischen Fundaments einer neueren Forschungsrichtung im U.S.-amerikanischen Internet-Recht.[1334] Diese Richtung vertritt die These, daß die technische Architektur des Internet – also die Ausgestaltung der verwendeten Hard- und Software – in ihren regulativen Auswirkungen einer rechtlichen Regulierung gleich kommen kann („Code is Law").[1335] Vor diesem theoretischen Hinter-

[1333] Staatlich unterstützte Aufklärungs- und Werbekampagnen können soziale Normen verändern. Baurechtliche Vorschriften verändern die Architektur des „Raumes", in dem sich die Bürger bewegen. Steuern und Subventionen beeinflussen Marktprozesse; s. dazu *Lessig*, 27 J. Legal Stud. 661, 666 ff. (1998). Als weiteres Beispiel führt *Lessig*, S. 92 f., das Regulierungsziel an, daß Autofahrer sich häufiger anschnallen sollen. Zu diesem Zweck könnte ein Gesetz erlassen werden, daß das Fahren ohne Gurt unter Strafe stellt (direkte rechtliche Regulierung des Verhaltens des Individuums). Der Staat könnte Kampagnen unterstützen, in denen für das Fahren mit Gurt geworben wird (indirekte rechtliche Regulierung sozialer Normen). Der Staat könnte Autoversicherer dazu anhalten, günstigere Prämien an Autofahrer zu vergeben, die angeschnallt fahren (indirekte rechtliche Regulierung von Marktprozessen). Schließlich könnten Gurtsysteme vorgeschrieben werden, die das Autofahren ohne angelegten Gurt technisch verhindern (indirekte rechtliche Regulierung der technischen Architektur). Zur Beeinflussung sozialer Normen durch das Recht s. *Sunstein*, 144 U. Pa. L. Rev. 2021 ff. (1996) und *ders.*, 96 Colum. L. Rev. 903, 953 ff. (1996), der dies als die „expressive Funktion des Rechts" bezeichnet; s. a. *Scott*, 86 Va. L. Rev. 1603, 1623 ff. (2000). Mit der Interaktion unterschiedlicher Regulierungsmechanismen und den Folgen indirekter Regulierung befaßt sich in den USA eine Bewegung, die manchmal unter dem Stichwort „New Chicago School" zusammengefaßt wird, so von *Lessig*, 27 J. Legal Stud. 661, 671 (1998), der auf S. 673 ff. noch weitere Vertreter dieser Richtung aufzählt. Auch unter diesen Vertretern ist jedoch umstritten, ob sich ihre Arbeit unter einem einheitlichen Begriff zusammenfassen läßt. Kritisch *Tushnet*, 1998 Wis. L. Rev. 579 ff.

[1334] Dabei soll nicht verschwiegen werden, daß in den USA umstritten ist, ob ein eigenständiges Rechtsgebiet des „cyberlaw" oder des Internet-Rechts überhaupt existiert; verneinend *Easterbrook*, 1996 U. Chi. Legal F. 207 ff.; *ders.*, 4 Tex. Rev. L. & Pol. 103 ff. (1999); *Sommer*, 15 Berkeley Tech. L. J. 1145 ff. (2000); bejahend *Lessig*, 113 Harv. L. Rev. 501 ff. (1999); *Shapiro*, 8 Seton Hall Const. L. J. 703, 716 ff. (1998).

[1335] Der wichtigste Vertreter dieses Ansatzes ist *Lawrence Lessig*, der diese These insbesondere in seinem 1999 erschienen Buch „Code and Other Laws of Cyberspace" entwickelt. Das Buch baut auf einer Vielzahl früherer Veröffentlichungen *Lessigs* auf, u. a. *Lessig*, 9 Fordham Intell. Prop. Media & Ent L. J. 405 ff. (1999); *ders.*, 27 J. Legal Stud. 661 ff. (1998); *ders.*, 11 St. John's J. L. Commentary 635 ff. (1996); *ders.*, 45 Emory L. J. 869 ff. (1996); *ders.*, 14 Berkeley Tech. L. J. 759 ff. (1999); *ders.*, 104 Yale L. J. 143 (1995). *Lessigs* Buch hat in den USA – nicht nur unter Juristen – zu einer breiten Debatte geführt; zu der juristischen Diskussion s. die teilweise berechtigte Kritik von *Post*, 52 Stan. L. Rev. 1439 ff. (2000); s. weiterhin *Nunziato*, 15 Berkeley Tech. L. J. 753 ff. (2000); *Fried*, 114 Harv. L. Rev. 606 ff. (2000); *Netanel*, 79 Tex. L. Rev. 447 ff. (2000); *Nadel*, 52 Fed. Comm. L. J. 821 ff. (2000); *Berman*, 71 U. Colo. L. Rev. 1263 ff. (2000); *Schwartz*, 2000 Wis. L. Rev. 743 ff.; *Hetcher*, 98 Mich. L. Rev. 1916 ff. (2000). Grundlegend zur technischen Regulierung im Cyberspace auch *Reidenberg*, 76 Tex. L. Rev. 553 ff. (1998); *ders.*, 45 Emory L. J. 911, 926 ff. (1996); *Mitchell*, S. 111 f. S. weiterhin *Shapiro*, 8 Seton Hall Cont. L. J. 703, 715 ff. (1998); *Greenleaf*, 21 U. New South Wales L. J. 593 ff. (1998); *N.N.*, 112 Harv. L. Rev. 1574, 1634 ff. (1999).

grund sollen im folgenden die Implikationen von DRM-Systemen betrachtet werden.[1336]

II. Auswirkungen des DRM aus rechtlicher Sicht

DRM-Systeme bauen auf einer Vielzahl unterschiedlicher Schutzkomponenten auf (dazu unten 1). Diese ineinandergreifenden Schutzkomponenten könnten Aufgaben des herkömmlichen Urheberrechts übernehmen (dazu unten 2).

1. Komponenten des Schutzes

a) Schutz durch Technik

aa) Allgemeines

DRM-Systeme können eine umfassende technische Plattform zum kontrollierten Vertrieb digitaler Inhalte in Online- und Offline-Umgebungen zur Verfügung stellen. Ein zentraler Bestandteil technischer DRM-Systeme ist die Kontrolle über den Zugang zu und die Nutzung von digitalen Inhalten. Dafür werden insbesondere Verschlüsselungsverfahren eingesetzt.[1337] Mit „digitalen Containern" ist beim Nutzer ein dauerhafter Verschlüsselungsschutz möglich.[1338] DRM-Systeme schützen digitale Inhalte nicht nur im digitalen Bereich. Die Inhalte werden auch noch geschützt, wenn sie auf ein analoges Medium kopiert wurden.[1339] Mit Hilfe der „Superdistribution" ist es auch möglich, den dezentralen Austausch digitaler Inhalte unter den Nutzern in einer sicheren DRM-Umgebung durchzuführen.[1340]

Welche Nutzungen in einem DRM-System zulässig sind, kann der Inhalteanbieter in inhaltlicher, persönlicher, räumlicher und zeitlicher Hinsicht nahezu beliebig ausgestalten und ausdifferenzieren.[1341] DRM-Systeme können gewährleisten, daß die übertragenen Inhalte auch tatsächlich von demjenigen stammen, der sich als Inhalteanbieter ausgibt (Authentizität). Ein DRM-System kann sicherstellen, daß die Inhalte auf dem Übertragungsweg nicht von einem Dritten verändert wurden (Inte-

---

[1336] Eine solche Betrachtung von DRM-Systemen ist nicht unumstritten. So meint *Sommer*, 15 Berkeley Tech. L. J. 1145, 1223 (2000), daß die Probleme von DRM-Systemen nicht auf dem Hintergrund eines – nach seiner Meinung nicht existierenden – Internet- oder Informationsrechts zu betrachten seien. Vielmehr handele es sich um normale Probleme des herkömmlichen Immaterialgüterrechts, dessen Begründung zwischen utilitaristischen und kulturell-persönlichkeitsrechtlichen Ansätzen schwanke.

[1337] Zu den technischen Grundlagen s. oben Teil 1, C I.

[1338] Zu den technischen Grundlagen s. oben Teil 1, C I 1 b aa.

[1339] Zu den technischen Grundlagen s. oben Teil 1, C VIII.

[1340] Zu den technischen Grundlagen s. oben Teil 1, E I.

[1341] Zu „rights management languages" s. oben Teil 1, C II 2 a bb. Zur geographischen Beschränkung der Nutzungsmöglichkeit durch die „Regional Code Playback Control" in DVDs s. oben Teil 1, D II 3 e.

grität).[1342] Dadurch können auch urheberpersönlichkeitsrechtliche Interessen (Schutz gegen die Entstellung des Werks gem. § 14 UrhG) gewahrt werden.

Die technischen Schutzmaßnahmen eines DRM-Systems können mit einem oder mehreren Zahlungssystemen gekoppelt werden. Dabei ist auch die Abrechnung von Kleinstbeträgen – bis zu Pfennigbruchteilen – möglich („Micropayment").[1343] Die einzelnen DRM-Komponenten werden regelmäßig in ein XML-basiertes E-Commerce-System eingebettet, das die Vertragsanbahnung, abschluß und -abwicklung elektronisch abbilden kann.[1344] Mit Hilfe von Software-Agenten können diese Prozesse sogar vollständig automatisiert werden („agent-mediated electronic commerce").[1345]

DRM-Systeme beinhalten Mechanismen, die die Sicherheit des DRM-Systems an sich gewährleisten sollen. Dafür existieren Verfahren, die die Authentizität und Integrität der DRM-Systemkomponenten gewährleisten.[1346] Auch wird manipulationssichere Hard- und Software eingesetzt, die einem Angreifer die Kompromittierung des Systems zumindest deutlich erschwert.[1347] Gelingt es einem Angreifer dennoch, ein Endgerät zu kompromittieren, kann dieses von der weiteren Nutzung des DRM-Systems ausgeschlossen werden („device revocation").[1348] Dafür sind unter anderem Verfahren erforderlich, mit denen die Nutzer und Endgeräte individuell identifiziert werden können.[1349]

DRM-Systeme bieten nicht nur einen passiven Schutz digitaler Inhalte. Sie können auch aktiv Rechtsverletzungen verhindern oder zu ihrer Aufklärung beitragen. Mit Hilfe von „fair exchange"-Protokollen kann auf technischem Wege verhindert werden, daß ein Nutzer von einem DRM-System digitale Inhalte beziehen kann, ohne dafür gleichzeitig bezahlen zu müssen.[1350] Spezielle Suchmaschinen können manipulierte Inhalte im

---

[1342] Zu den technischen Grundlagen s. oben Teil 1, C III. Zu den Implementierungen in IPSec, DTCP, HDCP, CPSA, MPEG, OPIMA und TCPA s. oben Teil 1, D III und IV.

[1343] Zu den technischen Grundlagen der Zahlungssysteme insgesamt s. oben Teil 1, C VI.

[1344] Zu den technischen Grundlagen s. oben Teil 1, C VII.

[1345] Zu den technischen Grundlagen s. oben Teil 1, E III.

[1346] Dafür werden neben digitalen Signaturen insbesondere „Challenge-Response-Verfahren" eingesetzt. Zu den technischen Grundlagen s. oben Teil 1, C II 2. Zu den Implementierungen in IPSec, DTCP, HDCP, CPSA, MPEG, OPIMA und TCPA s. oben Teil 1, D III und IV.

[1347] Zu den technischen Grundlagen s. oben Teil 1, C IV.

[1348] Zu den technischen Grundlagen s. oben Teil 1, C I 1 b bb.

[1349] Zu den technischen Grundlagen s. oben Teil 1, C II 3. Diese Identifizierungsverfahren können derart ausgestaltet werden, daß ein Angreifer sich nicht fälschlicherweise als berechtigter Nutzer ausgeben kann (Authentizität von Nutzern), zu den technischen Grundlagen s. oben Teil 1, C III 1 c. Zur erleichterten Nutzeridentifizierung bei mobilen Endgeräten s. oben Teil 1, E II.

[1350] Zu den technischen Grundlagen s. oben Teil 1, E III.

Internet aufspüren.[1351] Es existieren sogar Verfahren, mit denen sich ein digitaler Inhalt nach einer Manipulation im Wege einer „Selbstkorrektur" automatisch wieder in den Ausgangszustand zurückversetzen kann.[1352]

Es zeigt sich, daß die technischen Komponenten eines DRM-Systems einen umfassenden und nahezu beliebig konfigurierbaren Schutz digitaler Inhalte bieten. Natürlich hat auch dieser Schutz seine Schwächen.[1353] Insgesamt können technische Schutzmaßnahmen in DRM-Systemen jedoch einen sehr weitgehenden Schutz verleihen.

bb) Unterstützender rechtlicher Umgehungsschutz

Die Gesetzgeber haben die Schwächen technischer Schutzmaßnahmen erkannt und gehen zunehmend dazu über, technische Schutzmaßnahmen mit einem rechtlichen Schutz zu flankieren, nach dem die Umgehung technischer Schutzmaßnahmen verboten ist.[1354] Dabei wird regelmäßig schon Herstellung und Vertrieb von Vorrichtungen untersagt, mit denen später technische Schutzmaßnahmen umgangen werden können.[1355] Rechtliche Umgehungsverbote finden sich in Vorschriften des Urheber-, Straf-, Wettbewerbs-, Telekommunikations-, Rundfunk- und Deliktsrechts sowie anderen Vorschriften. In seiner Gesamtheit handelt es sich um einen sehr engmaschigen rechtlichen Schutz, der nahezu alle möglichen Umgehungshandlungen und vorrichtungen im DRM-Bereich abdeckt.[1356] Durch den rechtlichen Umgehungsschutz werden sowohl Verwertungs- als auch urheberpersönlichkeitsrechtliche Interessen geschützt.

Technische Schutzmaßnahmen bieten in der Kombination mit dem rechtlichen Umgehungsschutz einen umfassenden und effektiven Schutz digitaler Inhalte.

b) Schutz durch Nutzungsverträge

aa) Allgemeines

Contracting will be ubiquitous.[1357]

In DRM-Systemen schützen Inhalteanbieter ihre Interessen zunehmend durch eine vertragliche Bindung der Endnutzer.[1358] In diesen Verträgen

[1351] Zu den technischen Grundlagen s. oben Teil 1, C V 2.

[1352] Zu den technischen Grundlagen s. oben Teil 1, C III 2 c.

[1353] Einerseits können technische Schutzmaßnahmen immer umgangen werden; s. oben Teil 1, F. Andererseits lassen sich manche sehr sicheren Schutzmaßnahmen auf dem Markt nicht durchsetzen, da sie die Nutzung digitaler Inhalte erschweren und dadurch vom Konsumenten nicht akzeptiert werden; s. *Sander*, S. 4 ff.

[1354] S. dazu oben Teil 2, D I 2 a.

[1355] S. dazu oben Teil 2, D I 2 b.

[1356] Der umfassende rechtliche Schutz zeigt sich an der Überschneidung vieler Regelungen. Man denke nur an die Überschneidungen zwischen der Richtlinie zum Urheberrecht in der Informationsgesellschaft und der Zugangskontrollrichtlinie oben Teil 2, D I 2 b bb 3 b; zur umstrittenen Abgrenzung zwischen der Zugangs- und Nutzungskontrolle beim U.S.-amerikanischen DMCA s. oben Teil 2, D I 2 b dd 1 a.

[1357] *Merges*, 12 Berkeley Tech. L. J. 115, 118 (1997).

[1358] S. dazu oben Teil 2, B.

wird in differenzierter Weise geregelt, zu welchen Nutzungen des digitalen Inhalts der Nutzer berechtigt ist.[1359] Solche Regelungen sind in recht weitem Umfang wirksam.[1360] Daneben enthalten solche Verträge Klauseln, in denen sich der Nutzer verpflichtet, die technischen Schutzkomponenten des DRM-Systems nicht zu umgehen, zu verändern oder dies auch nur zu versuchen.[1361] Die Verträge können wirksam über das Internet – sogar vollautomatisch mit Hilfe von Software-Agenten – geschlossen werden.[1362] Der Abschluß solcher Verträge ist mit minimalen Kosten verbunden: Während es früher schon aus Kostengründen unmöglich erschien, daß ein Urheber mit allen Nutzern seiner Werke in vertraglicher Beziehung steht, wird in DRM-Systemen die Abdeckung eines gesamten Markts durch Nutzungsverträge möglich.[1363]

Das Besondere an diesen Nutzungsverträgen ist, daß sie Klauseln enthalten, durch die Verwertungsinteressen der Inhalteanbieter geschützt werden sollen. Trotzdem können Nutzungsverträge in DRM-Systemen nicht unbedingt mit Nutzungsverträgen im streng urheberrechtlichen Sinne (§§ 31 ff. UrhG) gleichgesetzt werden. Durch einen Nutzungsvertrag im urheberrechtlichen Sinne räumt der Urheber dem Vertragspartner ein Nutzungsrecht an einem urheberrechtlich geschützten Werk ein. Das Urheberrecht ist somit Ausgangspunkt des urheberrechtlichen Nutzungsvertrags. Dagegen ist ein Nutzungsvertrag in einem DRM-System streng genommen auf das Urheberrecht nicht angewiesen. Bei diesem Nutzungsvertrag geht es primär um die *Einräumung einer rein faktischen Nutzungsmöglichkeit* eines digitalen Inhalts. Schließt der Nutzer keinen DRM-Nutzungsvertrag ab, kann der Inhalteanbieter auf technischem Wege verhindern, daß der Nutzer den fraglichen Inhalt nutzen kann. Nutzungsverträge in DRM-Systemen betreffen primär die faktische Überlassung digitaler Inhalte, nicht die Lizenzierung bestimmter Rechtspositionen. Dies wird besonders deutlich, wenn man bedenkt, daß in DRM-Systemen auch digitale Inhalte vertrieben werden können, die dem urheberrechtlichen Schutz nicht unterfallen, beispielsweise bloße Daten,

[1359] Beispiele solcher Vertragsklauseln finden sich oben Teil 2, B I.

[1360] Die Einzelheiten hängen von der konkreten Ausgestaltung der Nutzungsverträge ab. Zur rechtlichen Wirksamkeit solcher s. Verträge oben Teil 2, B II; zur Möglichkeit der Einräumung beschränkter Nutzungsrechte im Speziellen s. oben Teil 2, B II 2 c.

[1361] S. dazu oben Teil 2, B I.

[1362] S. dazu oben Teil 2, B II 2 b und B II 3 b.

[1363] *Reichman/Franklin*, 147 U. Penn. L. Rev. 875, 898 (1999). Dabei muß nicht unbedingt eine direkte vertragliche Beziehung zwischen dem Inhalteanbieter und dem Nutzer bestehen. So kann eine vertragliche Beziehung zwischen dem Inhalteanbieter und einem Zwischenhändler bestehen, der dann den digitalen Inhalt dem Nutzer gegen Abschluß eines Nutzungsvertrags überläßt. In DRM-Systemen können somit mehrstufige Vertragsketten vorliegen. Es wird eine vertragliche Beziehung zwischen allen Teilnehmern eines DRM-Systems möglich. Dadurch entsteht eine Art Vertragsnetz; s. dazu *Brennan*, 36 Hous. L. Rev. 61, 109 (1999); *Hugenholtz*, 26 Brooklyn J. Int'l L. 77, 79 f. (2000).

amtliche Werke (s. § 5 UrhG) oder Werke, bei denen der urheberrechtliche Schutz erloschen ist (s. § 64 UrhG). Die Nutzung all dieser Inhalte wird in DRM-Systemen durch Nutzungsverträge geregelt, obwohl es sich dabei um keine Nutzungsverträge im urheberrechtlichen Sinn handelt.

Die Stellung des Inhalteanbieters in einem DRM-System ähnelt insofern dem Inhaber eines Geschäftsgeheimnisses, der das Geschäftsgeheimnis ebenfalls auf rein vertraglicher Basis schützt, ohne daß ihn das Gesetz mit einem umfassenden Ausschließlichkeitsrecht ausgestattet hätte. Es ist für den weiteren Verlauf der Untersuchung wichtig zu erkennen, daß ein Inhalteanbieter seine Verwertungsinteressen in einem DRM-System durch Nutzungsverträge auch schützen könnte, wenn gar kein Urheberrecht existieren würde. Zwar werden Nutzungsverträge in DRM-Systemen regelmäßig auch Nutzungsverträge im urheberrechtlichen Sinn sein, soweit die geschützten Inhalte dem urheberrechtlichen Schutz unterliegen. Es ist jedoch wichtig, daß dies lediglich an der Ausgestaltung des geltenden Urheberrechts liegt und der vertragliche Schutz in DRM-Systemen davon weitgehend unabhängig operiert. Nutzungsverträge in DRM-Systemen stellen einen alternativen Schutzmechanismus neben dem herkömmlichen Urheberrecht dar.[1364]

bb) Unterstützender technischer Schutz

Die Klauseln eines DRM-Nutzungsvertrags, die die Bedingungen festlegen, zu denen ein Nutzer den digitalen Inhalt nutzen darf, können in einem DRM-System auch in maschinenlesbarer Form ausgedrückt werden. Zu diesem Zweck können mit Metadaten digitale Inhalte, ihre Rechteinhaber und ihre Nutzer identifiziert werden;[1365] daneben ermöglichen „rights management languages", vertragliche Nutzungsbedingungen in maschinenlesbaren Metadaten abzubilden.[1366] Mit ihnen kann nahezu jede denkbare Nutzungsmöglichkeit in beliebiger Weise individuell definiert und äußerst differenziert kontrolliert werden.[1367] Solche Metadaten sind eine in maschinenlesbare Sprache gegossene Beschreibung der DRM-Nutzungsverträge. Metadaten ermöglichen, daß der Nutzer an die Bedingungen von des Nutzungsverträgs nicht nur *rechtlich* gebunden ist, sondern daß das DRM-System *technisch* sicherstellen kann, daß der Nutzer sich an die Bedingungen des Nutzungsvertrags hält. Ist der Nutzer nach einem DRM-Nutzungsvertrag berechtigt, einen digitalen Inhalt insgesamt zehn Mal zu nutzen oder ein Mal zu kopieren, so stellt das DRM-

[1364] Näher dazu unten Teil 3, A II 2 b bb, und A II 3. Dennoch besteht sowohl unter rechtsökonomischen als auch rechtlichen Gesichtspunkten eine enge Verbindung zwischen DRM-Nutzungsverträgen und dem Urheberrecht; s. dazu unten Teil 3, B I 3, und B II 2.

[1365] Zu den technischen Grundlagen s. oben Teil 1, C II 2 a aa.

[1366] Zu den technischen Grundlagen s. oben Teil 1, C II 2 a bb.

[1367] Für die Einzelheiten und Beispiele sei auf die obigen Aufführungen, Teil 1, C II 2 a b 2 und 3, verwiesen.

System mit Hilfe von Metadaten auf technischem Weg sicher, daß sich der Nutzer an diese Bedingungen des Nutzungsvertrags auch tatsächlich hält. Es ist dann technisch einfach nicht möglich, den Inhalt mehr als zehn Mal zu nutzen oder zwei Mal zu kopieren.

Zu diesem Zweck werden die Metadaten, die DRM-Nutzungsverträge maschinenlesbar abbilden, ihrerseits technisch geschützt. Mit Hilfe digitaler Wasserzeichen können Metadaten so robust in digitale Inhalte eingebettet werden, daß eine Entfernung der Metadaten unmöglich ist, ohne den Inhalt selbst zu beschädigen.[1368] Selbst wenn der digitale Inhalt teilweise verändert wurde, sind regelmäßig noch genügend Informationen vorhanden, um das Wasserzeichen und die Metadaten zu rekonstruieren.[1369] DRM-Systeme können auch die Authentizität und Integrität von Metadaten gewährleisten.[1370]

Mit Metadaten kann damit erreicht werden, daß der Nutzer die Bedingungen eines DRM-Nutzungsvertrags einhält. Im Idealfall werden die Nutzungsbedingungen durch Metadaten untrennbar mit dem digitalen Inhalt verbunden; dadurch kann ausgeschlossen werden, daß der Inhalt ohne die zugehörigen Vertragsbedingungen vertrieben wird. Schließlich kann das DRM-System auch die Authentizität und Integrität der Vertragsbedingungen gewährleisten. Der Schutz durch Nutzungsverträge wird in DRM-Systemen also durch einen unterstützenden technischen Schutz ergänzt.

cc) Unterstützender rechtlicher Umgehungsschutz

Trotz dieses unterstützenden technischen Schutzes wird es Angreifern in DRM-Systemen mitunter gelingen, Metadaten zu verändern oder zu entfernen. In diesem Fall greifen rechtliche Regelungen ein, nach denen die Entfernung oder Veränderung von Metadaten verboten ist.[1371] So kann die Entfernung digitaler Wasserzeichen unter die Vorschriften bezüglich der Entfernung von Metadaten fallen.[1372] Vereinzelt wird auch das Bereit-

[1368] Zu den technischen Grundlagen s. oben Teil 1, C II 2 b bb. Oftmals werden nicht die vollständigen Metadaten in den Inhalt eingebettet, sondern nur eine kurze Identifizierungsnummer, die auf eine Datenbank verweist, von der der vollständige Metadatensatz bezogen werden kann; zu dieser Unterscheidung zwischen „dumb" und „intelligent identifiers" s. oben bei Fn. 138.

[1369] S. oben bei Fn. 283.

[1370] S. oben Teil 1, C III 1 b und C III 2. Auch können Metadaten Bestandteil des Dechiffrierschlüssels sein, s. oben Fn. 371.

[1371] S. dazu oben Teil 2, D I 3 b aa.

[1372] Ebenso *Lai*, EIPR 1999, 171, 173; a. A. bezüglich 17 U.S.C. § 1202 teilweise *D. Nimmer*, 46 J. Copyright Soc'y U.S.A. 401, 463 f. (1999), der aber nicht scharf zwischen unterschiedlichen Arten von Wasserzeichen unterscheidet. Wenn Wasserzeichen Teil eines Kopierschutzverfahrens sind (wie beispielsweise bei der Audio-DVDs, kann ihre Entfernung auch als Umgehung einer technischen Schutzmaßnahme angesehen werden, s. dazu *D. Nimmer*, a. a. O., S. 462, der dies als einen möglichen Verstoß gegen 17 U.S.C. § 1201 (b) (1), nicht aber gegen 17 U.S.C. § 1201 (a) (1) ansieht; zweifelnd *Lai*, a. a. O., S. 173.

stellen falscher Metadaten[1373] und die Herstellung und Vertrieb von Umgehungsvorrichtungen verboten.[1374]

Insgesamt betrachtet können Inhalteanbieter in DRM-Systemen ihre Interessen durch eine vertragliche Bindung der einzelnen Nutzer wahren (vertraglicher Schutz). Die Bedingungen dieser Nutzungsverträge binden die Nutzer nicht nur rechtlich; vielmehr stellt das DRM-System technisch sicher, daß die Nutzungsbedingungen eingehalten werden (unterstützender technischer Schutz). Versucht ein Nutzer, diesen technischen Schutz zu umgehen, verstößt er gegen spezielle rechtliche Vorschriften (unterstützender rechtlicher Umgehungsschutz).

c) Schutz durch Technologie-Lizenzverträge

Neben dem Schutz durch Technik (dazu oben a) und dem Schutz durch Nutzungsverträge (dazu oben b) besteht in DRM-Systemen noch ein dritter Schutzpfeiler, durch den Inhalteanbieter ihre Interessen wahren können. Technologie-Lizenzverträge, die die Hersteller DRM-kompatibler Endgeräte regelmäßig abschließen müssen, enthalten umfangreiche Bestimmungen zum Schutz digitaler Inhalte.[1375] In Technologie-Lizenzverträgen wird vorgeschrieben, mit welchen anderen DRM-Technologien die lizenzierte Technologie in Endgeräten gekoppelt werden muß.[1376] Es wird vorgeschrieben, daß die Endgeräte Metadaten, die von den Inhalteanbieter festgelegt wurden, beachten müssen.[1377] Daneben enthalten DRM-Technologie-Lizenzverträge Klauseln, die die Sicherheit des DRM-Systems an sich gewährleisten sollen.[1378] Dazu werden der Lizenzgeber sowie Filmstudios und Tonträgerunternehmen unter anderem berechtigt, bestimmte Geräte von der weiteren Nutzung des DRM-Systems auszuschließen („device revocation").[1379] Weiterhin wird den Lizenznehmern verboten, Hard- oder Software herzustellen, mit denen technische Schutzmaßnahmen umgangen werden können.[1380]

Solche Klauseln in DRM-Technologie-Lizenzverträgen dienen mittelbar den Interessen der Inhalteanbieter. Inhalteanbieter nehmen regelmäßig auch Einfluß auf die Ausgestaltung der Technologie-Lizenzverträge.[1381] Es soll erreicht werden, daß verschiedene DRM-Komponenten nahtlos ineinander greifen und dadurch eine umfassende und sichere DRM-Schutzarchitektur vom Inhalteanbieter bis zum Konsumenten-

[1373] S. dazu oben Teil 2, D I 3 b bb.
[1374] S. dazu oben Teil 2, D I 3 b cc.
[1375] S. dazu oben Teil 2, C II.
[1376] S. dazu oben Teil 2, C II 2 b.
[1377] S. dazu oben Teil 2, C II 2 c.
[1378] S. dazu oben Teil 2, C II 2 d.
[1379] S. dazu oben Teil 2, C II 2 e.
[1380] S. dazu oben Teil 2, C II 2 f.
[1381] S. dazu oben Teil 2, C I.

Endgerät entsteht.[1382] Inhalteanbieter können in DRM-Systemen ihre Interessen mittelbar durch Technologie-Lizenzverträge schützen.

d) Ergebnis

Es zeigt sich, daß sich Inhalteanbieter in DRM-Systemen nicht nur durch das Urheberrecht schützen können. Vielmehr können sie sich durch technische Schutzmaßnahmen schützen, die ihrerseits durch einen rechtlichen Umgehungsschutz geschützt werden. Auch können sie sich durch Nutzungsverträge schützen, die ihrerseits durch technische Schutzmaßnahmen und einen darauf bezogenen rechtlichen Umgehungsschutz geschützt werden. Schließlich können sich Inhalteanbieter durch Technologie-Lizenzverträge schützen. Damit ergibt sich für die unterschiedlichen Schutzmechanismen in DRM-Systemen vorläufig[1383] folgendes Bild (siehe Abbildung 7):

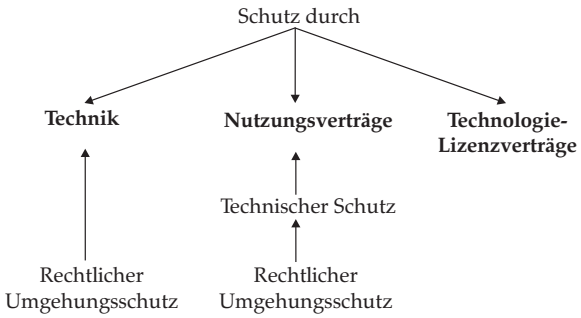


Abbildung 7: Unterschiedliche Schutzmechanismen in DRM-Systemen (1)

2. Folgen

Im folgenden soll untersucht werden, welche Auswirkungen die unterschiedlichen Schutzmechanismen in DRM-Systemen haben. Es zeigt sich, daß viele Schutzinteressen der Inhalteanbieter gleichzeitig durch mehrere ineinandergreifende Schutzmechanismen geschützt werden (dazu unten a). Dies führt zur Entstehung eines neuen privaten absoluten „Rechts" (dazu unten b).

a) Ineinandergreifen der Schutzmechanismen

Die unterschiedlichen Schutzmechanismen in DRM-Systemen greifen ineinander, wenn es um den Schutz bestimmter Interessen der Inhalteanbieter geht. Dies wird im folgenden an mehreren Beispielen dargestellt.

[1382] *Federal Communications Commission*, 15 FCC Rcd. 18,199 (September 18, 2000), Abs. 16.

[1383] Diese Abbildung wird im weiteren Verlauf der Untersuchung noch erweitert werden.

1. Inhalteanbieter haben ein starkes Interesse daran, die Nutzer von DRM-Systemen daran zu hindern, daß diese digitale Inhalte unbeschränkt kopieren können. Dadurch wollen Inhalteanbieter die Erstellung unbezahlter Raubkopien verhindern. Zu diesem Zweck existieren technische Systeme, die kontrollieren, wie viele Kopien der Nutzer auf welchen Speichermedien erstellen kann.[1384] Bei Einsatz dieser Systeme ist es technisch gar nicht möglich, eine große Anzahl von Kopien zu erstellen (*technischer Schutz*).[1385] Gelingt es einem Angreifer, diesen technischen Kopierschutz zu umgehen, so verstößt er dabei gegen den *rechtlichen Umgehungsschutz* technischer Schutzmaßnahmen. Je leichter die technischen Schutzmaßnahmen umgangen werden können, desto wichtiger ist dieser rechtliche Umgehungsschutz.[1386] Daneben wird der Nutzer in dem DRM-Nutzungsvertrag verpflichtet, nur eine bestimmte Anzahl von Kopien zu erstellen oder den Inhalt nur auf bestimmte, geschützte Speichermedien zu kopieren (*vertraglicher Schutz*).[1387] Diese Bedingungen des Nutzungsvertrags werden im DRM-System in Metadaten ausgedrückt. Dadurch stellt das DRM-System auf technischem Weg sicher, daß sich der Nutzer an die Bedingungen des Nutzungsvertrags hält (*technischer Schutz der Nutzungsverträge*). Die Metadaten können in speziellen Bereichen des Datenformats gespeichert oder mit Hilfe digitaler Wasserzeichen direkt in die Inhalte eingebettet werden. Bei der Verwendung robuster Wasserzeichen können die Metadaten von Angreifern nicht entfernt werden (ebenfalls *technischer Schutz der Nutzungsverträge*).[1388] Gelingt es einem Angreifer dennoch, die Metadaten zu entfernen oder zu verändern, so verstößt er gegen den *rechtlichen Umgehungsschutz* des technischen Schutzes des Nutzungsverträge. Schließlich werden die

[1384] Zu den technischen Grundlagen s. oben Teil 1, C I 2; zur Kopierkontrolle bei DAT (SCMS) s. oben Teil 1, D II 1, zum bei DVDs eingesetzten CGMS s. oben Teil 1, D II 3 c.

[1385] Bei SCMS wird nur die Erstellung einer digitalen Kopie der zweiten Generation verhindert; steht das digitale Original zur Verfügung, können von diesem Original unbegrenzt viele Kopien erstellt werden. Es geht im vorliegenden Zusammenhang aber nicht um die Einzelheiten von SCMS. Vielmehr geht es grundsätzlich um die Möglichkeiten technischer Kopierkontroll-Systeme.

[1386] Ebenso *Lai/Buonaiuti* in: Katzenbeisser/Petitcolas (Hrsg.), S. 195. Die Interdependenz zwischen technischem und rechtlichem Schutz findet erst dort ihre Grenze, wo völlig unwirksame oder unbrauchbare technische Schutzmaßnahmen eingesetzt werden, die dann keinen rechtlichen Schutz mehr genießen. Diese Grenze ist angesichts der gängigen Definition „wirksamer" technischer Schutzmaßnahmen in Umgehungsvorschriften regelmäßig sehr niedrig; s. nur oben Fn. 1018.

[1387] So beispielsweise im Rahmen der „Schedule A – Business Rules" des „End User License Agreement" des Universal Music Group-Projekts „Bluematter", s. dazu oben Fn. 781. In Schutzhüllenverträgen für Computersoftware finden sich regelmäßig Klauseln, nach denen der Nutzer die Software nur zur Erstellung einer Sicherheitskopie kopieren darf. Die Erstellung sonstiger Kopien wird dem Nutzer vertraglich untersagt.

[1388] S. dazu auch oben Teil 3, A II 1 b bb.

Hersteller DRM-kompatibler Geräte in Technologie-Lizenzverträgen verpflichtet, daß die von ihnen hergestellten Geräte diese Metadaten auslesen und befolgen müssen (*Schutz durch Technologie-Lizenzverträge*).[1389] Zur Verhinderung unberechtigter Kopien können DRM-Systeme digitale Inhalte auf physischen Speichermedien auch individualisiert verschlüsselt abspeichern, so daß eine Kopie auf ein anderes Speichermedium unmöglich ist (*technischer Schutz*).[1390] Die Hersteller DRM-kompatibler Geräte werden dann in Technologie-Lizenzverträgen dazu verpflichtet, diese Verfahren in ihren Geräten auch einzusetzen (*Schutz durch Technologie-Lizenzverträge*). Das Interesse der Inhalteanbieter, eine Kontrolle über die Anzahl der Kopien zu haben, die ein Nutzer von einem geschützten digitalen Inhalt erstellen kann, wird in einem DRM-System also durch bis zu sechs unterschiedliche Schutzmechanismen sichergestellt.

2. Ein Inhalteanbieter kann ein Interesse daran haben, unterschiedlichen Nutzern digitale Inhalte zu unterschiedlichen Konditionen oder in unterschiedlichen Versionen anzubieten. Für diese Zwecke bieten DRM-Systeme vielfältige Möglichkeiten der Angebotsdifferenzierung.[1391] So können digitale Inhalte in unterschiedlichen Qualitätsstufen angeboten und unterschiedlich verschlüsselt werden („multiresolution encryption“).[1392] Dadurch können Nutzer mit unterschiedlichen individuellen Zahlungsbereitschaften befriedigt werden: Ein Nutzer mit hoher individueller Zahlungsbereitschaft wählt den digitalen Inhalt in einer hohen Qualität. Dafür muß er aber auch mehr zahlen als ein Nutzer, der den Inhalt in einer niedrigen Qualität wählt. Auch können solche Verfahren für Werbezwecke eingesetzt werden. Beispielweise kann ein teilweise verschlüsselter Videofilm in einem DRM-System derart angeboten werden, daß alle Nutzer den Film in schlechter Qualität kostenlos anschauen können. Sagt der Film einem Nutzer zu, so kann er einen Dechiffrier-Schlüssel erwerben und damit den Film in HiFi-Qualität entschlüsseln.[1393] Dieser *technische Schutz* eines ausdifferenzierten Geschäftsmodells wird seinerseits durch einen *rechtlichen Umgehungsschutz* geschützt: Nutzt ein Angreifer den digitalen Inhalt in einer Qualitätsstufe, für die er kein Entgelt entrichtet hat, kann dies gegen rechtliche Umgehungsvorschriften verstoßen. Daneben kann eine solche Angebotsdifferenzierung auch in Nutzungsverträgen weitergeführt werden. So finden sich oft Klauseln, die die Nutzer verpflichten, Inhalte nur zu privaten Zwecken zu verwenden. Für gewerb-

[1389] S. oben Teil 2, C II 2 c.
[1390] Zu diesem bei CPRM eingesetzten Verfahren s. oben Teil 1, D II 4.
[1391] Zur Preisdiskriminierung in DRM-Systemen aus ökonomischer Sicht s. unten Teil 3, A III 3 b.
[1392] Zu den technischen Grundlagen s. oben Teil 1, C I 1 b cc.
[1393] S. oben bei Fn. 112.

liche Nutzer existieren dann andere Nutzungsverträge mit regelmäßig höheren Nutzungsentgelten (Angebotsdifferenzierung durch *vertraglichen Schutz*).[1394] Solche Angebotsdifferenzierungen in Nutzungsverträgen können durch entsprechende Metadaten unterstützt werden (*technischer Schutz der Nutzungsverträge*).[1395] Gelingt es einem Angreifer, diese Metadaten zu entfernen oder zu verändern und die Inhalte entgegen der Angebotsdifferenzierung zu nutzen, so kann darin ein Verstoß gegen den *rechtlichen Umgehungsschutz* des technischen Schutzes des Nutzungsverträge liegen. Schließlich können die Hersteller DRM-kompatibler Geräte in Technologie-Lizenzverträgen verpflichtet werden, daß die von ihnen hergestellten Geräte diese Angebotsdifferenzierungen beachten (*Schutz durch Technologie-Lizenzverträge*). DRM-Systeme bieten die Möglichkeit einer stark ausgeprägten Nutzungsdifferenzierung in inhaltlicher, zeitlicher, räumlicher und persönlicher Hinsicht, die von bis zu sechs Schutzmechanismen unterstützt wird.

3. Auch die urheberpersönlichkeitsrechtlichen Interessen werden in DRM-Systemen durch mehrere Mechanismen geschützt. DRM-Systeme können die Integrität digitaler Inhalte gewährleisten und damit das Werk gegen Entstellung schützen, s. § 14 UrhG (*technischer Schutz*).[1396] Die Umgehung eines solchen technischen Schutzes kann rechtlich unzulässig sein (*rechtlicher Umgehungsschutz* des technischen Schutzes). In *Nutzungsverträgen* kann der Inhalteanbieter auch festlegen, zu welchen Bearbeitungen der Nutzer berechtigt ist. Diese Bedingungen können in Metadaten ausgedrückt werden,[1397] die ihrerseits durch *technische Schutzmaßnahmen* und einen dazugehörigen *rechtlichen Umgehungsschutz* geschützt werden.
4. Um eine zuverlässige Vertriebsplattform für digitale Inhalte bieten zu können, muß in DRM-Systemen ein möglichst hohes Sicherheitsniveau gewährleistet sein. Zu diesem Zweck verfügt ein DRM-System regelmäßig über technische Komponenten, die die Umgehung des

---

[1394] So beispielsweise im „End User License Agreement" des DRM-Pilotprojekts der Universal Music Group „Bluematter", s. oben Fn. 781. § 5 des Agreements bestimmt u. a. „Content, when it is made available to you, is only for your personal use." Ein solches Vorgehen lag auch der ProCD-Entscheidung zugrunde, s. dazu unten Teil 3, A III b aa.

[1395] So kann in Metadaten vorgesehen werden, daß die digitalen Inhalte nur auf bestimmten Geräten ausgegeben werden können. Damit kann beispielsweise erreicht werden, daß ein Film nur auf digitalen Projektionsgeräten angezeigt werden kann, die für den Heimgebrauch bestimmt sind. Für professionelle Kino-Aufführungen wird das Werk in einer anderen Version mit anderen Nutzungsbedingungen vertrieben; s. dazu oben bei Fn. 223.

[1396] S. dazu oben bei Fn. 1342.

[1397] Zur Festlegung von Bearbeitungsrechten in Metadaten s. oben Teil 1, C II 2 a b 2 a.

DRM-Systems verhindern oder zumindest erschweren. Dazu wird auf Integritäts- und Authentizitätsprüfungen der Systemkomponenten sowie auf manipulationssichere Hard- und Software gesetzt (*technischer Schutz*). Die Umgehung solcher Systemkomponenten durch einen Angreifer verletzt *rechtliche Umgehungsvorschriften*. Weiterhin verpflichten sich Nutzer in DRM-Nutzungsverträgen regelmäßig, die technischen Schutzkomponenten eines DRM-Systems nicht zu umgehen, zu verändern oder dies auch nur zu versuchen (*vertraglicher Schutz*).[1398] Schließlich werden die Hersteller DRM-kompatibler Geräte in Technologie-Lizenzverträgen verpflichtet, die Geräte so auszugestalten, daß Angreifer die integrierten technischen Schutzmaßnahmen nicht umgehen können. Weiterhin wird den Herstellern untersagt, selbst Komponenten herzustellen, mit denen technische Schutzmaßnahmen umgangen werden können (*Schutz durch Technologie-Lizenzverträge*). Um die Systemsicherheit zu gewährleisten, ist es in DRM-Systemen oftmals technisch möglich, kompromittierte Nutzergeräte von der weiteren Nutzung des DRM-Systems auszuschließen (*technischer Schutz* durch sogenannte „device revocation"). In Technologie-Lizenzverträgen werden die Lizenzgeber und bestimmte Rechteinhaber gegenüber den Geräteherstellern berechtigt, diese „device revocation" zu veranlassen (*Schutz durch Technologie-Lizenzverträge*). Damit greifen bezüglich der Sicherheit von DRM-Systemen bis zu vier unterschiedliche Schutzmechanismen ineinander.

5. Inhalteanbieter haben ein Interesse daran, daß in Unterhaltungselektronik-Geräten technische Schutzmaßnahmen eingesetzt werden. Dadurch können Raubkopien verhindert werden. Zu diesem Zweck existieren vereinzelt Vorschriften, in denen die Verwendung technischer Schutzmaßnahmen gesetzlich vorgeschrieben wird. Beispielsweise ist in den USA bei analogen Videorekordern und -kameras die Verwendung der analogen Kopierschutzverfahren von Macrovision gesetzlich vorgeschrieben (*rechtlicher Schutz*).[1399] Andererseits sieht auch die CSS-Lizenz vor, daß die Hersteller von DVD-Geräten diese Kopierschutzverfahren in die Endgeräte integrieren müssen (*Schutz durch Technologie-Lizenzverträge*).[1400]

[1398] S. dazu oben Teil 2, A II 1 b aa. So verletzte das Knacken des CSS-Algorithmus die entsprechende „click-wrap license", die vor der Nutzung des DVD-Software-Decoders, in dem CSS enthalten war, abgeschlossen werden mußte; s. *Hoy*, S. 4; *Eddy*, S. 3.

[1399] S. dazu oben Teil 2, D II 1 b.

[1400] S. dazu oben Teil 2, C II 2 b. Zwar sind auf den ersten Blick die regulatorischen Auswirkungen einer Verpflichtung in einem Technologie-Lizenzvertrag weit weniger einschneidend als eine gesetzliche Verpflichtung. Im Fall des Technologie-Lizenzvertrags steht es dem Hersteller des Endgeräts immerhin frei, ob er die Bedingungen des Technologie-Lizenzvertrags akzeptiert und diesen abschließt. Und tatsächlich bleibt es dem Hersteller von DVD-Geräten unbenommen, ein DVD-Gerät auf den Markt zu bringen, das weder CSS noch die Macrovision-Verfahren unterstützt: CSS ist nicht Teil

6. Das Ineinandergreifen rechtlicher und technischer Schutzmechanismen zeigt sich auch bei der Übertragung und Einräumung von Nutzungsrechten. Wird einem Nutzer in einem DRM-System vertraglich ein urheberrechtliches Nutzungsrecht eingeräumt, so hat er ein Interesse zu erfahren, ob sein Vertragspartner zur Einräumung dieses Nutzungsrechts überhaupt berechtigt war. Dieses Interesse wird vom deutschen Urheberrecht nicht geschützt: Ein gutgläubiger Erwerb urheberrechtlicher Nutzungsrechte ist nicht möglich.[1401] Der Grund dafür ist, daß es bei urheberrechtlichen Nutzungsrechten – wie bei Forderungen im allgemeinen Zivilrecht – an einer geeigneten Rechtsscheinsgrundlage fehlt: Der Erwerber eines urheberrechtlichen Nutzungsrechts kann nur auf das Wort seines Vertragspartners vertrauen, daß dieser zur Einräumung des Nutzungsrechts befugt ist.[1402] Allerdings werden für DRM-Systeme Verfahren entwickelt, die es auf *technischem Weg* verhindern, daß beispielsweise ein Zwischenhändler ei-

---

der technischen DVD-Format-Spezifikationen, s. oben bei Fn. 897. Es ist jedoch zu beachten, daß die Filmstudios ihre Filme zur Veröffentlichung auf DVDs nur freigeben, wenn diese mit CSS geschützt werden. Da sich DVD-Geräte nur verkaufen lassen, wenn sie Hollywood-Filme abspielen können, sind die Hersteller solcher Geräte faktisch gezwungen, CSS zu benutzen und den entsprechenden Technologie-Lizenzvertrag abzuschließen, s. oben bei Fn. 898. Damit besteht für die Hersteller von DVD-Geräten – vermittelt über den CSS-Know-How-Lizenzvertrag – ein faktischer Zwang, die Kopierschutzverfahren von Macrovision zu verwenden. In ihren faktischen Auswirkungen unterscheidet sich die dargestellte Verpflichtung in einem Technologie-Lizenzvertrag damit nicht von einer gesetzlichen Verpflichtung, die Macrovision-Verfahren einzusetzen.

1401 *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, § 34 Rdnr. 13, vor §§ 28 ff. Rdnr. 63; s. a. BGHZ 5, 116, 119 – Parkstraße 13.

1402 *Schack*, Rdnr. 537, 556; *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, vor §§ 28 ff. Rdnr. 63. Im U.S.-amerikanischen Urheberrecht ist die Rechtslage ähnlich. Ein gutgläubiger Erwerb urheberrechtlicher Nutzungsrechte wird von U.S.-amerikanischen Gerichten regelmäßig abgelehnt, so in Microsoft Corp. v. Harmony Computers & Electronics, Inc., 846 F. Supp. 208, 211, 213 f. (E.D.N.Y. 1994; auf S. 214: „[…] if defendants purchased their Products from Microsoft licensees who were acting outside the scope of their licenses by selling the Products stand-alone, any distribution of the Products by defendants […] would constitute copyright infringement"); Major League Baseball Promotion v. Colour-Tex, 729 F. Supp. 1035, 1042 f. (D. N.J. 1990; auf S. 1042: „[…] the reasonable or good faith use of material by a sublicensee does not alone insulate the sublicensee from a claim of infringement […]"); *N. B. Nimmer/D. Nimmer*, §10.15[A], S. 10–121. Im Anwendungsbereich des UCITA ergibt sich dies für die Übertragung von Nutzungsrechten aus § 506 (a) S. 2 und (b) UCITA („[…] a transferee acquires no more than the contractual interest or other rights than the transferor was authorized to transfer"); s. dazu *Lemley*, 87 Cal. L. Rev. 111, 148 (1999). S. weiterhin den Official Comment No. 3 zu § 506 UCITA, *UCITA*, S. 217: „[…] neither copyright nor patent recognize concepts of protecting a buyer in the ordinary course […] by giving that person greater rights than were authorized to be transferred […]. Transfers that exceed or are otherwise unlicensed by a patent or copyright owner create no rights of use in the transferee."; vgl. schließlich *Lunney*, 1 Tulane J. Tech. & Intell. Prop. 1 (1999), Abs. 25 ff.

nem Nutzer vertraglich urheberrechtliche Nutzungsrechte einräumt, die ihm selbst gar nicht eingeräumt wurden (sogenannte „distribution chain security").[1403] Dadurch wird gleichsam auf technischem Weg ein verläßlicher Rechtsscheinträger geschaffen.[1404]

Es zeigt sich, daß die unterschiedlichen Schutzinteressen der Inhalteanbieter in DRM-Systemen regelmäßig durch mehrere Schutzmechanismen gewahrt werden, die nebeneinander eingreifen. Jede dieser Schutzmechanismen kann für sich genommen schon ein recht hohes Schutzniveau gewährleisten. Dennoch ist es nicht ausgeschlossen, daß Angreifer einzelne Schutzmechanismen umgehen können. Das Charakteristische an DRM-Systemen ist jedoch, daß eine Vielzahl unterschiedlicher Schutzmechanismen ineinandergreift, so daß in einem Fall der Umgehung eines Schutzmechanismus' regelmäßig ein anderer Schutzmechanismus unterstützend eingreift. Die Stärke von DRM-Systemen liegt damit nicht in dem technischen beziehungsweise dem vertraglichen Schutz oder dem rechtlichen Umgehungsschutz. Sie liegt vielmehr in der Kombination zahlloser ineinandergreifender Schutzmechanismen, die sich gegenseitig ergänzen.

b) Schaffung eines privaten absoluten „Rechts"

aa) Allgemeines

Wenn in DRM-Systemen zahllose Schutzmechanismen ineinandergreifen, die sich gegenseitig ergänzen, so muß untersucht werden, welche Implikationen dies für den Schutz der Inhalteanbieter hat. Insbesondere soll

---

1403 Zu den technischen Grundlagen s. oben Teil 1, E IV.

1404 Weiterhin können Nutzungsbedingungen als Metadaten durch digitale Wasserzeichen und ähnliches dauerhaft mit den digitalen Inhalten verbunden werden. Damit kann einem digitalen Inhalt direkt entnommen werden, unter welchen Bedingungen er benutzt werden darf. Damit unterscheiden sich derart markierte digitale Inhalte von herkömmlichen Immaterialgütern durch einen „Rechtsscheinträger", dem die eingeräumte Nutzungsrechte entnommen werden können. Enthielte dieser Rechtsscheinträger irreführende Informationen über Nutzungsrechte, so könnte zu überlegen sein, ob auch ein gutgläubiger Erwerb dieser Nutzungsrechte zulässig sein sollte. Vgl. dazu in etwas anderem Zusammenhang *Merges*, 12 Berkeley Tech. L. J. 115, 122 (1997). Eine ähnliche Konstellation existiert im U.S.-amerikanischen Urheberrecht. Zwar ist auch nach dieser Rechtsordnung grundsätzlich kein gutgläubiger Erwerb urheberrechtlicher Nutzungsrechte möglich. Eine Ausnahme wird jedoch gemacht, wenn ein Rechtsscheinträger existiert: Hat der Urheber das Urheberrecht an einen Dritten übertragen und räumt er danach einem Vierten ein einfaches Nutzungsrecht ein, so ist diese Einräumung wirksam, wenn die Übertragung des Urheberrechts noch nicht im Register des U.S. Copyright Office (s. 17 U.S.C. § 408) eingetragen wurde, 17 U.S.C. § 205 (e). Insofern ist das Register, zu dessen Benutzung die Urheber seit dem Beitritt der USA zur RBÜ nicht mehr verpflichtet sind, mit negativer Publizität ausgestattet; s. *Schack*, Rdnr. 538; *N. B. Nimmer/D. Nimmer*, §10.07[B], S. 10–60 ff.; *Bodewig* in: Beier/Götting/Lehmann/Moufang (Hrsg.), S. 833, 852 f. Anders als im deutschen Urheberrecht besteht in diesem Fall mit dem Register ein Rechtsscheinträger, so daß ein gugläubiger Erwerb möglich ist.

analysiert werden, in welchem Verhältnis der Schutz in solchen DRM-Systemen zum Schutz durch das herkömmliche Urheberrecht steht.

Dabei sind einige grundsätzliche Charakteristika des Schutzes durch das Urheberrecht zu bedenken. Das Urheberrecht vermittelt eine der Sachherrschaft (§ 903 BGB) vergleichbare „Werkherrschaft", die dem Urheber die freie Entscheidung darüber beläßt, ob und zu welchen Bedingungen er bestimmten Dritten die Nutzung seines Werks erlaubt (§§ 15 ff. UrhG).[1405] Die Herrschaft über das Werk äußert sich in der Befugnis, mit dem Werk nach Belieben zu verfahren, insbesondere es zu verwerten (positives Nutzungsrecht) und Dritte von der Einwirkung auszuschließen (negatives Verbotsrecht).[1406] Das Urheberrecht ist damit – wie alle Immaterialgüterrechte – ein „Herrschaftsrecht".[1407] Charakteristikum eines Herrschaftsrechts ist die Möglichkeit, auf ein bestimmtes Rechtsobjekt einzuwirken und andere von der Einwirkung auszuschließen.[1408] Herrschaftsrechten kommt absolute Wirkung zu.[1409] Ein absolutes Recht wirkt gegen jedermann, ist von jedermann zu respektie-

[1405] *Schack*, Rdnr. 4.

[1406] *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, Einl. Rdnr. 19. Diese Kategorisierung ist eine Vereinfachung. So bestehen Vergütungsansprüche (z. B. im Rahmen der §§ 26, 27, 49, 54 ff. UrhG), die weder positives Nutzungsrecht noch negatives Verbotsrecht sind, sondern entweder das Relikt eines eingeschränkten negativen Verbotsrechts sind oder eigenständige Rechte darstellen.

[1407] *Larenz/Wolf*, § 15 Rdnr. 8; *Schack*, Rdnr. 4.

[1408] *Schönherr* in: Brügger (Hrsg.), S. 57, 68 f.; *Larenz/Wolf*, § 14 Rdnr. 14, § 15 Rdnr. 2; *Seiler* in: Staudinger (Begr.), § 903 Rdnr. 2; Einl. zu §§ 854 ff. Rdnr. 18. Ausschließlichkeitsrechte sind die negative Komponente des Herrschaftsrechts. Die positive Seite besteht in der Befugnis des Berechtigten, den Gegenstand zu nutzen, sowie in der Verfügungsmacht, also in der rechtlich gesicherten Möglichkeit, über die Sache durch Rechtsgeschäft zu verfügen, s. *Schönherr,* a. a. O., S. 69, 71. Es ist umstritten, ob sich der rechtliche Gehalt von Herrschaftsrechten nicht schon im negativen Verbotsrecht erschöpft; zu dieser Ansicht und der damit zusammenhängenden Imperativen-Theorie, nach der alle Rechtssätze ein Ge- oder Verbot zum Ausdruck bringen, s. *Larenz*, S. 253 ff.; *Schönherr*, a. a. O., S. 69 f.

[1409] *Medicus*, Rdnr. 66 f.; *Larenz/Wolf*, § 15 Rdnr. 2. In diesem Umfeld ist auch der Begriff des „subjektiven Rechts" zu erwähnen. Dieser Begriff und seine Stellung im Gesamtgefüge des Privatrechts sind seit langem umstritten, s. *Medicus*, Rdnr. 70 ff.; *Larenz/Wolf*, § 14 Rdnr. 3 ff. Nach h. M. verschafft das subjektive Recht der einzelnen Person eine zwecks Befriedigung seiner Bedürfnisse durch die Rechtsordnung zuerkannte und gesicherte Willensmacht, *Larenz/Wolf*, § 14 Rdnr. 11. Dieser auf die Willensherrschaft abstellende Ansatz wurde im 19. Jahrhundert u. a. von *Savigny* und *Windscheid* vertreten. Dagegen betonte *von Ihering* den Zweck der Machtverleihung, nämlich die Befriedigung bestimmter Interessen; s. dazu *Medicus*, Rdnr. 70; *Larenz/Wolf*, § 14 Rdnr. 11 ff. Zur Begriffsbestimmung wird oft auf die Imperativen-Theorie zurückgegriffen, s. dazu oben Fn. 1408. Den Gegensatz zum subjektiven Recht bildet das objektive Recht, das die generell geltenden, abstrakten Vorschriften und Verhaltensanweisungen umfaßt, *Larenz/Wolf*, § 14 Rdnr. 1.

ren und daher gegen jedermann geschützt.[1410] Zu diesem Zweck sehen Herrschaftsrechte bei unbefugten Eingriffen in ihren Schutzbereich Abwehr- und Ersatzansprüche vor.[1411] Das Urheberrecht ist – sowohl in seiner verwertungsrechtlichen als auch in seiner persönlichkeitsrechtlichen Seite – ein absolutes Recht, das vor rechtswidriger Verletzung spezialgesetzlich in §§ 97 ff. UrhG und als sonstiges Recht durch § 823 Abs. 1 BGB geschützt wird.[1412] Den Gegensatz zu absoluten Rechten bilden relative Rechte, die nur gegen eine bestimmte Person wirken. Darunter fallen insbesondere Forderungen.[1413]

Das Urheberrecht ist auch ein gegenständliches oder „quasi-dingliches" Recht.[1414] Dingliche Rechte weisen eine Sache an eine Person derart zu, daß ihr Wille hinsichtlich dieser Sache von der Rechtsordnung grundsätzlich als maßgeblich anerkannt wird.[1415] Immaterialgüterrechte beziehen sich – wie Sachenrechte – auf ein von der Person zu unterscheidendes Objekt, das indessen kein körperlicher, sondern ein unkörperlicher Gegenstand ist.[1416] Daher läßt sich das Urheberrecht als ein „quasi-dingliches" Recht bezeichnen.[1417] Den Gegensatz zum dinglichen Recht bildet das relative oder obligatorische Recht: Während ein dingliches Recht zu

[1410] *Medicus*, Rdnr. 62; *Seiler* in: Staudinger (Begr.), Einl. zu §§ 854 ff. Rdnr. 37. *Wieling* zählt zu den absoluten Rechten die dinglichen Rechte, das Persönlichkeitsrecht, die persönlichen Familienrechte und die Immaterialgüterrechte, *Wieling*, § 1 II 2, S. 13.

[1411] *Larenz/Wolf*, § 15 Rdnr. 17; ebenso *Canaris* in: Jakobs et al. (Hrsg.), S. 371, 373, der als wesentliches Charakteristikum eines absoluten Rechts den umfassenden Klageschutz gegenüber beliebigen Dritten ansieht. Nach *Canaris* tritt jedoch ergänzend der Verfügungs-, insbesondere der Sukzessionsschutz hinzu, *ebda.*, S. 373 f.

[1412] *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, Einl. Rdnr. 18; *Schönherr* in: Brügger (Hrsg.), S. 57, 63. Auch hierbei handelt es sich um eine Vereinfachung. Die Ansprüche des Urhebers nach §§ 27, 49, 54 ff. UrhG wirken gegenüber jedermann, also absolut. Es sind aber bloße Vergütungsansprüche, denen keine Ausschließungswirkung zukommt. Deswegen unterscheidet *Schönherr*, a. a. O., S. 64, zwischen der absoluten Wirkung (Wirkung gegenüber jedermann) und der Ausschließungswirkung (ius excludendi).

[1413] *Larenz/Wolf*, § 15 Rdnr. 44; s. a. *Schmidt* in: Staudinger (Begr.), Einl. zu §§ 241 ff., Rdnr. 438 ff.

[1414] *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, Einl. Rdnr. 19.

[1415] *Larenz/Wolf*, § 15 Rdnr. 5; *Westermann*, § 2 II 1 a, S. 9; *Baur/Stürner*, § 2 Rdnr. 2. Nach dieser „Zuordnungstheorie" bestimmt sich der Charakter dinglicher Rechte nach *Vorgang und Art der Rechtsgewährung*. Andere verstehen unter einem dinglichen Recht die Vermittlung der Rechtsmacht über Sachen, stellen also stärker auf den *Rechtsinhalt* ab. Dabei wird stärker der absolute Charakter dinglicher Rechte, also deren Ausschließungsfunktion, betont. S. dazu *Eichler*, S. 1 ff.; *Fabricius*, AcP 162 (1963), 456, 467 ff.; *Kühne*, AcP 140 (1935), 1, 10 ff. Nicht immer wird scharf zwischen Dinglichkeit und Absolutheit unterschieden, s. nur *Kühne*, a. a. O., S. 11. Zu dieser eher rechtstheoretischen Frage s. a. *Seiler* in: Staudinger (Begr.), Einl. zu §§ 854 ff. Rdnr. 18 f.

[1416] *Larenz/Wolf*, § 15 Rdnr. 8.

[1417] *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, Einl. Rdnr. 19.

einer unmittelbaren Zuordnung des betreffenden Gegenstandes zu einer Person führt, schafft ein obligatorisches Recht lediglich ein Band zwischen zwei Personen.[1418] Dingliche Rechte sind eine Hauptgruppe der absoluten Rechte.[1419] Dennoch ist der Begriff des dinglichen Rechts nicht mit dem Begriff des absoluten Rechts deckungsgleich.[1420]

Zwischen den beiden Idealtypen des „absoluten" und des „obligatorischen" Rechts bestehen Mischformen, die unter dem Stichwort „Verdinglichung obligatorischer Rechte" zusammengefaßt werden. In diesen Fällen genießt ein obligatorisches Recht in gewissem Umfang auch Schutz gegenüber Dritten, wird also insoweit einem absoluten Recht angenähert.[1421] Darunter fallen unter anderem die Vormerkung (siehe §§ 883 Abs. 2, 888 BGB),[1422] das Recht zum Besitz aus Schuldverhältnissen (siehe § 986 Abs. 2)[1423] sowie die Grundstücksmiete (siehe § 571 BGB).[1424] Verdinglichte obligatorische Rechte stehen regelmäßig im Schnittfeld zwischen Schuld- und Sachenrecht. Auch wenn der Begriff der „Verdinglichung" genau genommen nicht korrekt ist,[1425] hat er sich eingebürgert und wird auch im weiteren Verlauf dieser Arbeit verwendet werden.

[1418] *Canaris* in: Jakobs et al. (Hrsg.), S. 371, 373; *Wieling*, § 1 II, S. 10 f.; *Baur/Stürner*, § 2 Rdnr. 2. Anders als ein dingliches Recht ordnet eine Forderung nicht einen außerhalb ihrer selbst liegenden Gegenstand zu, *Canaris*, a. a. O., S. 373. Die Unterscheidung zwischen dinglichem und obligatorischem Recht geht auf die Unterscheidung zwischen der actio in rem und der actio in personam im älteren römischen Recht zurück, s. *Wieling*, § 1 II 1, S. 11.

[1419] *Seiler* in: Staudinger (Begr.), Einl. zu §§ 854 ff., Rdnr. 18; *Baur/Stürner*, § 2 Rdnr. 2; *Canaris* in: Jakobs et al. (Hrsg.), S. 371, 375. Wie andere absoluten Rechte sind dingliche Rechte auch Herrschaftsrechte, *Seiler*, a. a. O., Rdnr. 37.

[1420] So existieren einerseits nicht-dingliche Rechte, die absolut wirken, z. B. das Persönlichkeitsrecht sowie die persönlichen Familienrechte, s. *Wieling*, § 1 II 2, S. 13. Andererseits ist nicht jedes dingliche Recht zwingend ein absolutes Recht. So hat der Ersitzungsbesitzer nach §§ 937, 1007 BGB ein nur relativ wirkendes dingliches Recht: Er ist gegenüber allen geschützt, ausgenommen gegenüber dem Eigentümer, s. *Wieling*, § 1 II 4 b, S. 20.

[1421] Zur Verdinglichung obligatorischer Rechte ausführlich *Canaris* in: Jakobs et al. (Hrsg.), S. 371 ff.; *Weitnauer* in: Canaris/Diederichsen (Hrsg.), S. 705 ff.

[1422] S. dazu *Canaris* in: Jakobs et al. (Hrsg.), S. 371, 381 ff.

[1423] S. dazu *Canaris* in: Jakobs et al. (Hrsg.), S. 371, 392 ff.

[1424] *Medicus*, Rdnr. 64.

[1425] In den Fällen einer „Verdinglichung obligatorischer Rechte" geht es nicht darum, daß relative Rechte eine engere Zuordnung zu einer Sache erfahren, also verdinglicht werden. Vielmehr geht es darum, daß diese relativen Rechte gewisse Rechtswirkungen gegenüber Dritten entfalten, also einem absoluten Recht angenähert werden. Der Begriff „Verabsolutierung relativer Rechte" wäre daher korrekter. Der Begriff „Verdinglichung obligatorischer Rechte" hat sich wohl eingebürgert, weil dingliche Sachenrechte der wichtigste Unterfall absoluter Rechte sind. S. zum ganzen *Larenz/Wolf*, § 15 Rdnr. 62; deutlich auch *Quack* in: Münchener Kommentar, Einl. zu §§ 854 ff., Rdnr. 26: „Die Fragestellung, ob eine bestimmte Position ‚verdinglicht' werden kann […], ist damit die Frage, ob sie als Inhalt einer Person-Sachbeziehung und damit als absolut, d. h. gegenüber jedermann wirkend gestaltet werden kann", *Westermann*, § 2

bb) Vom vertraglichen Schutz zum absoluten „Recht"

Wie oben dargestellt wurde, schützen Inhalteanbieter ihre Interessen in DRM-Systemen zunehmend durch eine vertragliche Bindung der Endnutzer. Diese Nutzungsverträge können Nutzungsverträge im urheberrechtlichen Sinn sein, müssen es aber nicht. Das Charakteristische von Nutzungsverträgen in DRM-Systemen ist, daß der Inhalteanbieter dem Nutzer erst nach Abschluß des Nutzungsvertrags die faktische Nutzungsmöglichkeit einräumt.[1426]

DRM-Systeme sind auf den Massenmarkt zugeschnitten. Es geht um den Vertrieb digitaler Inhalte an Millionen von Nutzern. Nutzungsverträge werden in einem großen DRM-System millionenfach abgeschlossen. Zwar schafft jeder einzelne Nutzungsvertrag nur eine relativ wirkende Rechtsbeziehung zwischen dem Inhalteanbieter (bzw. dem DRM-Systembetreiber oder einem Dritten)[1427] und dem Nutzer. Dennoch erscheint fraglich, ob nicht die Summe all dieser Nutzungsverträge zu einem Schutz führt, der einem absolut wirkenden Recht – insbesondere dem Urheberrecht – vergleichbar ist.

In den USA wird diese Frage seit der Entscheidung des 7th Circuit Court of Appeals in Sachen ProCD, Inc. v. Zeidenberg[1428] heftig diskutiert. Judge *Easterbrook* vertrat in der Entscheidung die Auffassung, daß der parallele Abschluß zahlloser Nutzungsverträge in seinen Auswirkungen dem urheberrechtlichen Schutz nicht vergleichbar sei.[1429] In der U.S.-amerikanischen Literatur wurde dieser Passus der Entscheidung überwiegend heftig kritisiert.[1430] Diese Kritik kann auch für die vorliegende Frage fruchtbar gemacht werden.

II 1 b, S. 10: „Für die Einordnung [als verdinglichtes obligatorisches Recht] ist entscheidend, daß das Objekt des Rechts dem Berechtigten in mindestens einer Beziehung mit absoluter Wirkung zugeordnet ist" und *Weitnauer* in: Canaris/Diederichsen (Hrsg.), S. 705, 721: „Die Verdinglichung bedeutet, daß solche Vereinbarungen, ohne ihren schuldrechtlichen Charakter zu verändern oder zu verlieren, nicht nur zwischen denjenigen Parteien wirken, die sie geschlossen haben, sondern auch für und gegen einen Sondernachfolger […]".

[1426] S. dazu oben Teil 3, A II 1 b aa.

[1427] Es wurde schon oben in Fn. 1363 darauf hingewiesen, daß Nutzungsverträge in DRM-Systemen nicht notwendigerweise direkt zwischen dem Inhalteanbieter und dem Nutzer abgeschlossen werden müssen.

[1428] S. dazu oben Teil 2, B II 3 a aa.

[1429] Die Frage der Vergleichbarkeit von „copyright" und „contract" stellte sich dort im Rahmen der „preemption" i. S. d. 17 U.S.C. § 301; s. dazu unten Teil 4, B III 1. Judge *Easterbrook* schreibt: „A copyright is a right against the world. Contracts, by contrast, generally affect only their parties; strangers may do as they please, so contracts do not create ‚exclusive rights'", ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1454 (7th Cir. 1996).

[1430] S. die Nachweise in den folgenden Fußnoten. Dagegen begrüßen *Mercer*, 30 Creighton L. Rev. 1287, 1344 f. (1997), und *Monroe*, 1 Marq. Intell. Prop. L. Rev. 143 (1997), diesen Passus der Entscheidung, wiederholen jedoch nur die in der Entscheidung vorgebrachten Gründe. *Gomulkiewicz*, 12 Berkeley Tech. L. J. 891, 896 (1998),

Nutzungsverträge in DRM-Systemen zeichnen sich durch zwei Eigenschaften aus: Zum einen handelt es sich um standardisierte Verträge, die millionenfach in gleicher Form abgeschlossen werden: DRM-Nutzungsverträge sind allgemeine Geschäftsbedingungen. Zum anderen hat der Nutzer – wie bei allgemeinen Geschäftsbedingungen üblich – faktisch keinen Einfluß auf den Inhalt der Nutzungsverträge.[1431]

Jeder Nutzer, der in einem DRM-System digitale Inhalte nutzen will, wird gezwungen, vor der Nutzung einen Nutzungsvertrag abzuschließen. Damit steht der Inhalteanbieter (oder ein Dritter) in einem DRM-System bezüglich jedes Inhalts mit allen Nutzern in einer vertraglichen Beziehung. Idealiter gibt es keinen einzigen Nutzer, der den digitalen Inhalt nutzen kann, ohne gleichzeitig an die Bedingungen des entsprechenden Nutzungsvertrags gebunden zu sein. Zwar entfaltet der Nutzungsvertrag zwischen dem Inhalteanbieter und jedem Nutzer nur eine relative Rechtswirkung. Nimmt man alle Nutzungsverträge zusammen, so entfalten sie in ihrer Summe Rechtswirkungen zwischen dem Inhalteanbieter und *allen* Nutzern eines DRM-Systems.

Dagegen ließe sich einwenden, daß es immer Nutzer geben wird, die einen digitalen Inhalt nutzen, ohne den entsprechenden Nutzungsvertrag abgeschlossen zu haben. Dies läßt sich am Beispiel der Computersoftware zeigen: Auch wenn Softwarehersteller versuchen, ihre Interessen durch eine vertragliche Bindung *aller* Nutzer der Software zu schützen,[1432] gibt es Nutzer, die die Software raubkopiert haben und in keiner vertraglichen Bindung zu dem Softwarehersteller stehen. Hier scheint der vertragliche Schutz zu versagen.[1433]

In einem DRM-System wird jedoch verhindert, daß es zu einem solchen Fall überhaupt kommen kann. Dabei ist das Ineinandergreifen der unterschiedlichen Schutzmechanismen eines DRM-Systems zu beachten. Ein DRM-System stellt auf technischem Weg sicher, daß ein Nutzer auf einen digitalen Inhalt nur Zugriff erhält, wenn er davor einen Nutzungsvertrag wirksam abgeschlossen hat (*technischer Schutz*).[1434] Gelingt es einem Angreifer, diesen technischen Schutz zu umgehen und den Inhalt ohne Abschluß eines Nutzungsvertrags zu nutzen, so kann darin eine Verletzung des *rechtlichen Umgehungsschutzes* liegen. Weiterhin ist zu beachten, daß Bedingungen von Nutzungsverträgen in DRM-Systemen mit Hilfe

---

ein Microsoft-Anwalt, begrüßt die Entscheidung und weist darauf hin, daß die Entscheidung langjähriger gängiger Praxis in der Softwarebranche entspreche. Begrüßend auch *O'Rourke*, 12 Berkeley Tech. L. J. 53 (1997).

[1431] *Merges*, 93 Mich. L. Rev. 1570, 1613 (1995).

[1432] Dies soll durch Schutzhüllenverträge erreicht werden, s. dazu oben Teil 2, B II 2 a.

[1433] Vgl. dazu in etwas anderem Zusammenhang *Marly*, Softwareüberlassungsverträge, Rdnr. 115.

[1434] Ebenso *Heide*, 15 Berkeley Tech. L. J. 993, 1012 (2000).

von „rights management languages“ in maschinenlesbare Metadaten ausgedrückt werden. Dadurch kann ein DRM-System technisch sicherstellen, daß ein Nutzer sich an die Bedingungen des Nutzungsvertrags hält. Will ein Angreifer dies verhindern, kann er versuchen, die Metadaten zu entfernen oder zu verändern. Metadaten können jedoch mit Hilfe digitaler Wasserzeichen direkt in die Inhalte eingebettet werden. Bei der Verwendung robuster Wasserzeichen ist es für einen Angreifer sehr schwer, die eingebetteten Metadaten zu entfernen. Die Nutzungsverträge werden also ihrerseits *technisch geschützt*.[1435] Selbst wenn dem Angreifer die Entfernung der Metadaten gelingt, verletzt er dadurch Vorschriften des *rechtlichen Umgehungsschutzes*.[1436] Schließlich werden die Hersteller DRM-kompatibler Geräte in *Technologie-Lizenzverträgen* verpflichtet, daß die von ihnen hergestellten Geräte die eingebetteten Metadaten beachten.[1437]

Durch eine Kombination vertraglicher, technischer und gesetzlicher Mechanismen stellt ein DRM-System also sicher, daß ein digitaler Inhalt *immer* nur in Kombination mit dem entsprechenden Nutzungsvertrag erhältlich ist. Digitaler Inhalt und Nutzungsvertrag sind nahezu untrennbar miteinander verknüpft. Der Fall, daß ein Nutzer einen digitalen Inhalt nutzen kann, ohne an die Bedingungen des entsprechenden Nutzungsvertrags gebunden zu sein, wird in einem solchen idealisierten DRM-System gar nicht vorkommen.[1438]

Das Ineinandergreifen unterschiedlicher Schutzmechanismen führt also dazu, daß *jede* Person, die einen digitalen Inhalt nutzen will, an den entsprechenden Nutzungsvertrag gebunden ist.[1439] Außenstehende Dritte, die den digitalen Inhalt nutzen können, existieren in einem solchen idealisierten DRM-System nicht. Nimmt man alle Nutzungsverträge sowie die erwähnten anderen Schutzmechanismen zusammen, so entfaltet dieses Konglomerat in seiner Summe Rechtswirkungen zwischen dem Inhalteanbieter und *allen* Nutzern eines DRM-Systems. Da dieser Schutz gegenüber jedem wirkt, der mit dem digitalen Inhalt in Berührung kommt, ähnelt er in seinen Wirkungen einem absolut wirkenden Recht. Zwar handelt es sich bei diesem Schutz um kein „Recht“ im herkömmlichen Sinne. Der Inhalteanbieter wächst durch das Ineinandergreifen vertraglicher, technischer und gesetzlicher Schutzmechanismen vielmehr in eine faktische Position hinein, die der Position des Inhabers eines absolu-

1435 S. dazu oben Teil 3, A II 1 b bb, und A II 2 a.
1436 S. dazu oben Teil 3, A II 1 b cc, und A II 2 a.
1437 S. dazu oben Teil 3, A II 1 c, und A II 2 a.
1438 Ebenso *Elkin-Koren*, 12 Berkeley Tech. L. J. 93, 103 f. (1997).
1439 Dies ist naturgemäß eine Vereinfachung. Selbst wenn jeder Nutzer einen Nutzungsvertrag abschließen mußte, kann dieser Vertragsschluß bei einzelnen Nutzern immer noch rechtlich unwirksam sein, beispielsweise wegen Minderjährigkeit, Willensmängeln oder Sittenwidrigkeit. Zu dieser Frage s. unten Teil 3, B II 2.

ten Rechts sehr ähnelt: Absolute Rechte wirken gegenüber jedermann; es gibt niemanden, der nicht von der Wirkung des absoluten Rechts betroffen wäre. Darin unterscheiden sich absolute von relativen Rechten. Zwar ist ein einzelner Nutzungsvertrag in einem DRM-System grundsätzlich ein relatives Recht. Nimmt man alle Nutzungsverträge in einem DRM-System zusammen und bedenkt man den unterstützenden technischen, gesetzlichen und vertraglichen[1440] Schutz, so gibt es auch in einem DRM-System niemanden, der nicht von der Wirkung dieses Schutzkonglomerats betroffen wäre.[1441]

In ihrer Gesamtheit und in Kombination mit unterstützenden Schutzmechanismen wirken Nutzungsverträge in DRM-Systemen gleichsam absolut.[1442] Man kann insoweit von einer „Verdinglichung" der Nutzungsverträge sprechen, die aus der Kombination mehrerer Schutzmechanismen resultiert.[1443] Überzieht ein Inhalteanbieter oder DRM-Systembetreiber ein gesamtes DRM-System mit einem vorformulierten, einheitlichen Nutzungsvertrag, auf dessen Inhalt der Nutzer keinen Einfluß hat („take it or leave it"), so nähert sich dieser „relative" Schutz durch Vertrag in seinen faktischen Auswirkungen einem absoluten Schutz an.[1444] Da die Nutzer keinen direkten Einfluß auf den Vertragsinhalt ha-

---

[1440] Hier sind Technologie-Lizenzverträge gemeint.

[1441] Ebenso *Cohen*, 97 Mich. L. Rev. 462, 487 (1998); *Ginsburg*, 42 Representations 53, 63 (1993): „[…] if copying could be electronically tracked or prevented, no ‚third parties' to the contract would exist."

[1442] Ebenso in Ansätzen *Elkin-Koren*, 12 Berkeley Tech. L. J. 93, 104 f. (1997): „Even though this [contractual] right is established ‚merely' against a party to a contract, no one may gain access to the work without being subject to a contract. With on-line dissemination, contractual arrangements converge with physical means of exclusion, monitoring, and control to create a de facto property right"; *Gimbel*, 50 Stan. L. Rev. 1671, 1683 f. (1998); *Heide*, 15 Berkeley Tech. L. J. 993, 1012 (2000); s. weiterhin *Lemley*, 87 Cal. L. Rev. 111, 148 (1999); *Lessig*, S. 135; *Hugenholtz*, 6 Maastricht Journal of European and Comparative Law 308, 309 (1999). Der Schutz versagt allerdings, wenn der abgeschlossene Nutzungsvertrag unwirksam ist; s. dazu oben Fn. 1439.

[1443] Zur Unschärfe des Begriffs der „Verdinglichung" s. oben Fn. 1425. Es sei ausdrücklich betont, daß diese „Verdinglichung" nicht bezüglich der Gesamtheit der Nutzungsverträge an sich eintritt. Überzieht ein Hersteller einen Markt mit allgemeinen Geschäftsbedingungen, so entsteht dadurch noch kein „verdinglichtes" Recht. Erst die Kombination vertraglicher, technischer und gesetzlicher Schutzmechanismen führt in DRM-Systemen zur „Verdinglichung". Diese wichtige Differenzierung wird auch in der U.S.-amerikanischen Diskussion zu DRM-Systemen regelmäßig unterschlagen.

[1444] *Covotta/Sergeef*, 13 Berkeley Tech. L. J. 35, 49 (1998); *Merges*, 93 Mich. L. Rev. 1570, 1613 (1995); *Bott*, 67 U. Cin. L. Rev. 237, 254 (1998); *O'Rourke*, 12 Berkeley Tech. L. J. 53, 80 (1997); *Nimmer/Brown/Frischling*, 87 Cal. L. Rev. 17, 60 f. (1999); *Warlick*, 45 J. Copyright Soc'y U.S.A. 158, 170 (1997); *McManis*, 87 Cal. L. Rev. 173, 183 (1999); *Garon*, 17 Cardozo Arts & Ent. L. J. 491, 550 f. (1999). S. a. *Reichman/Franklin*, 147 U. Penn. L. Rev. 875, 910, 949 (1999); *Lessig*, S. 197. A. A. *Gordon*, 41 Stan. L. Rev. 1343, 1415 ff. (1989), die an dieser Position aber wohl nicht mehr festhält, s. *Gordon*, 73 Chi.-Kent L. Rev. 1367, 1381 (1998). An der Möglichkeit des

ben, wird auch von einer „privaten Gesetzgebung“ gesprochen.[1445] Der Inhalteanbieter kann sich in einem DRM-System durch dieses absolut wirkende Konglomerat aus Nutzungsverträgen und unterstützenden Schutzmechanismen schützen. Fraglich erscheint, welche Bedeutung dem ebenfalls absolut wirkenden Urheberrecht in diesem Umfeld noch zukommt.

cc) Vom technischen Schutz zum absoluten „Recht“

> *Code can, and increasingly will, displace law as the primary defense of intellectual property in cyberspace.*[1446]

Dieser Bedeutungsverlust des Urheberrechts in DRM-Systemen wird noch deutlicher, wenn man technische Schutzmechanismen betrachtet. Sie ermöglichen eine umfassende Zugangs- und Nutzungskontrolle digitaler Inhalte. Durch Verschlüsselungsverfahren und andere technische Schutzmaßnahmen wird sichergestellt, daß ein Nutzer auf den Inhalt nur Zugriff erhält, wenn er ein entsprechendes Entgelt entrichtet hat (*technischer Schutz*). Dabei wird es Angreifern durch technische Schutzmaßnahmen erschwert, diese Zugangs- und Nutzungskontrolle zu umgehen (*technischer Schutz*).[1447] Selbst wenn einem Angreifer die Umgehung gelingt, verstößt er dadurch gegen den *rechtlichen Umgehungsschutz*. Weiterhin werden alle berechtigten Nutzer in Nutzerverträgen verpflichtet, die technischen Schutzkomponenten eines DRM-Systems nicht zu umgehen, zu verändern oder dies auch nur zu versuchen (*vertraglicher Schutz*). Schließlich werden die Hersteller DRM-kompatibler Geräte in Technologie-Lizenzverträgen verpflichtet, daß in ihren Endgeräten ein bestimmtes Sicherheitsniveau gewährleistet ist (*Schutz durch Technologie-Lizenzverträge*).

Durch eine Kombination technischer, vertraglicher und gesetzlicher Mechanismen erhält der Inhalteanbieter in einem DRM-System also die Möglichkeit, die Nutzung seiner Inhalte genau zu kontrollieren und unberechtigte Dritte von der Nutzung auszuschließen. Der Fall, daß ein Dritter einen digitalen Inhalt nutzen kann, ohne daß die Zugangs- und Nutzungskontrolle des DRM-Systems greift, wird in einem solchen idealisierten DRM-System gar nicht vorkommen.

---

flächendeckenden Einsatzes von Nutzungsverträgen zweifeln wohl *Landes/Posner*, 18 J. Legal Stud. 325, 330 (1989).

[1445] Der Gedanke, daß Software-Schutzhüllenverträge eine Art „private legislation“ seien, wurde das erste Mal von *Robert Merges* in 93 Mich. L. Rev. 1570, 1613 (1995), formuliert; s. a. *Merges*, 12 Berkeley Tech. L. J. 115, 126 f. (1997). Dabei bezieht sich *Merges* auf Arbeiten von *Friedrich Kessler* aus den 40er Jahren, der in „adhesion contracts“ (Standardverträge mit einseitig auferlegten Bedingungen) eine „private legislation“ sah, s. *Merges*, 12 Berkeley Tech. L. J. 115, 126 Fn. 38 (1997) m. w. N. S. weiterhin *Nimmer/Brown/Frischling*, 87 Cal. L. Rev. 17, 61 (1999); *Gimbel*, 50 Stan. L. Rev. 1671, 1685 (1998); *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1164 f. (1998).

[1446] *Lessig*, S. 126.

[1447] Diesem Zweck dient u. a. manipulationssichere Hard- und Software.

Das Ineinandergreifen unterschiedlicher Schutzmechanismen führt also dazu, daß *jede* Person, die einen digitalen Inhalt nutzen will, an die technischen Schutzmaßnahmen gebunden ist. Durch das Ineinandergreifen technischer, vertraglicher und gesetzlicher Schutzmechanismen wächst der Inhalteanbieter in eine faktische Position hinein, die der Position des Inhabers eines absoluten Rechts sehr ähnelt: Es gibt in einem DRM-System niemanden, der nicht von der Wirkung dieses Schutzkonglomerats betroffen wäre. In ihren Auswirkungen schaffen die ineinandergreifenden Schutzmechanismen faktisch ein absolutes „Recht"[1448] der Zugangs- und Nutzungskontrolle digitaler Inhalte.[1449]

Wie das Schutzkonglomerat um DRM-Nutzungsverträge[1450] wirken technische Schutzmaßnahmen in Kombination mit unterstützenden Schutzmechanismen gleichsam absolut. Da die Inhalteanbieter und DRM-Systembetreiber die Einzelheiten des technischen Schutzes relativ autonom festlegen können, wird auch hier von „privater Gesetzgebung" gesprochen.[1451]

3. Ergebnis

DRM-Systeme bieten durch das Ineinandergreifen mehrerer Schutzmechanismen – Schutz durch Technik mit unterstützendem rechtlichem Umgehungsschutz, Schutz durch Vertrag mit unterstützendem technischem und darauf bezogenem rechtlichem Umgehungsschutz sowie Schutz durch Technologie-Lizenzverträge – neue Möglichkeiten, den Zugang zu digitalen Inhalten und deren Nutzung zu kontrollieren und unberechtigte Dritte von der Nutzung auszuschließen. Das Besondere an DRM-Systemen ist das Ineinandergreifen dieser Schutzmechanismen; in ihrer Kombination schaffen sie ein Schutzniveau, das dem eines absolut wirkenden

[1448] Wie bei dem Schutz durch DRM-Nutzungsverträge handelt es sich hier um kein „Recht" im herkömmlichen Sinne. Der Inhalteanbieter wächst durch das Ineinandergreifen technischer, vertraglicher und gesetzlicher Schutzmechanismen vielmehr in eine faktische Position hinein, die der Position des Inhabers eines absoluten Rechts sehr ähnelt. Auch an dieser Stelle sei betont, daß dieser Effekt nicht bezüglich der technischen Schutzmaßnahmen an sich eintritt. Erst die Kombination technischer Schutzmaßnahmen mit unterstützenden gesetzlichen und vertraglichen Schutzmechanismen verleiht dem Inhalteanbieter eine Position, die einem absolut wirkenden Recht ähnelt.

[1449] Ebenso in Ansätzen *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1158, 1164 (1998); *Lessig*, S. 130; *N.N.*, 112 Harv. L. Rev. 1574, 1652 (1999); sowie *Heide*, 15 Berkeley Tech. L. J. 993, 1010 f. (2000) in bezug auf ein neuartiges „property right" durch die Kombination von technischen Schutzmaßnahmen und der europäischen Zugangskontrollrichtlinie; s. a. *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 205, 258. Zu den Grenzen dieses Schutzes s. unten Teil 3, B II 2.

[1450] S. dazu oben Teil 3, A II 2 b bb.

[1451] *Lessig*, 113 Harv. L. Rev. 501, 529: „Trusted systems […] are forms of privatized law".

Rechts – dem Urheberrecht – ähnelt.[1452] In ihrer stärksten Ausgestaltung sind DRM-Systeme praktisch ein in Silikon gegossenes Urheberrecht, dessen Umfang und Ausgestaltung von denjenigen festgelegt werden, die die Systeme entwickeln und zum Schutz digitaler Inhalte einsetzen.

DRM-Systeme können verwendet werden, um Inhalte zu schützen, die vom urheberrechtlichen Schutz nicht erfaßt werden. DRM-Systeme können die Nutzung digitaler Inhalte in sehr differenzierter Weise kontrollieren. Eine solche Nutzungskontrolle ist dem herkömmlichen Urheberrecht fremd.[1453] Weiterhin kann ein Raubkopierer das urheberrechtlich geschützte Werk eines Dritten vervielfältigen und unter seinem Namen in einem DRM-System vertreiben.[1454]

Auch sonst bestehen deutliche Unterschiede zwischen dem Schutz durch DRM-Systeme und durch das herkömmliche Urheberrecht. Bei einer Verletzung urheberrechtlicher Vorschriften stehen dem Urheber Ansprüche auf Schadensersatz sowie Unterlassung und Beseitigung zur Verfügung, §§ 97 ff. UrhG. Mit Ausnahme des vorbeugenden Unterlassungsanspruches handelt es sich um einen Schutz, der erst nach Eintritt der Rechtsverletzung greift (*Schutz ex post*). Technische Schutzmaßnahmen in DRM-Systemen verhindern dagegen schon den Eintritt der Rechtsverletzung. Im Idealfall kommt es aufgrund des technischen *ex-ante-Schutzes* gar nicht zum Eintritt eines Schadens, der mit Hilfe rechtlicher Ansprüche ausgeglichen werden müßte.[1455] In einem DRM-System

---

[1452] Ebenso *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1158 (1998); ebenfalls in diese Richtung *Hugenholtz*, 6 Maastricht Journal of European and Comparative Law 308, 312 (1999). Damit ist nicht gemeint, daß die Kombination der Schutzmechanismen zu einem neuartigen „absoluten Recht" im rechtstechnischen Sinne führt. Dies wird bezüglich einzelner rechtlicher Umgehungsvorschriften teilweise bejaht, s. beispielsweise *Heide*, 15 Berkeley Tech. L. J. 993, 1010 f. (2000) und *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 205, 258; in Österreich enthält das Zugangskontrollgesetz ein absolut wirkendes Recht. In der vorliegenden Untersuchung soll vielmehr dargestellt werden, welche Folgen das Ineinandergreifen mehrerer Schutzmechanismen in DRM-Systemen hat. Ein „absolutes *Recht*" kann schon aus begrifflichen Gründen nicht entstehen, da manche der dargestellten Schutzmechanismen *technischer* Natur sind.

[1453] S. dazu oben Fn. 1121 und *Bechtold*, GRUR 1998, 18, 26 f.

[1454] Dabei besteht die Gefahr, daß der wirkliche Urheber davon gar nichts erfährt: Solange der Raubkopierer das plagiierte Werk mit technischen Schutzmaßnahmen versieht und sicherstellt, daß der wirklichen Urheber nicht auf eine dechiffrierte Version zugreifen kann, wird der wirkliche Urheber gar nicht bemerken, daß sein Werk plagiiert wurde; s. dazu auch *Collberg/Thomborson/Low*, S. 31.

[1455] Ebenso *Gimbel*, 50 Stan. L. Rev. 1671, 1685 (1998); *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1157 Fn. 5 (1998); *Lessig*, 45 Emory L. J. 869, 899 (1996); *ders.*, 113 Harv. L. Rev. 501, 530 f. (1999); *Elkin-Koren/Salzberger*, 19 Int. Rev. L. & Econ., 553, 575 (1999); *Cohen*, 13 Berkeley Tech. L. J. 1089, 1134 f. (1998). Bestes Beispiel dafür sind „fair exchange"-Protokolle, s. dazu oben Teil 1, E III. Dieses Charakteristikum von DRM-Systemen ist ein allgemeines Merkmal technischer Regulierungsmechanismen, s. *Reidenberg*, 76 Tex. L. Rev. 553, 580 f. (1998). *Thornburg*, 34 U.C. Davis L. Rev. 151, 195 f. (2000) vergleicht die Wirkungen eines DRM-Systems mit einer einstweiligen Verfügung.

wird technisch verhindert, daß ein Nutzer gegen Bedingungen des Nutzungsvertrags verstoßen kann.[1456] Selbst wenn sich ein Nutzer einer technischen Schutzmaßnahme widersetzen will, ist ihm dies im Extremfall einfach nicht möglich.[1457] DRM-Systeme bieten damit ein Schutzniveau, welches das Schutzniveau des herkömmlichen Urheberrechts an Effektivität und Sicherheit bei weitem übertrifft.[1458] In der technischen Literatur zu DRM-Systemen sind Aussagen weit verbreitet, der Schutz in DRM-Systemen überwinde die Schwächen des rechtlichen Schutzes, vollziehe sich sogar ganz außerhalb des Rechts („self-enforcing protection").[1459]

Dies alles zeigt, daß DRM-Systeme mit dem Urheberrecht im klassischen Sinne nicht mehr viel zu tun haben.[1460] DRM-Systeme setzen hauptsächlich auf Schutzmechanismen außerhalb des herkömmlichen Urheberrechts. Der urheberrechtliche Schutz wird zunehmend durch einen Schutz

---

[1456] *Gimbel*, 50 Stan. L. Rev. 1671, 1683 f. (1998), meint: „Coupled with the technology of trusted systems, this dynamic [based on a contractual protection] threatens to create the ultimate contracts of adhesion – unbreachable agreements which amount to self-executing private law"; s. weiterhin *Thornburg*, 34 U.C. Davis L. Rev. 151, 176 (2000).

[1457] *Gimbel*, 50 Stan. L. Rev. 1671, 1685 (1998).

[1458] *Lessig*, 45 Emory L. J. 869, 899 f. (1996), meint plastisch, um ein vergleichbares Schutzniveau mit Hilfe des herkömmlichen Urheberrechts zu erreichen, müßte der Staat hinter jede Werkkopie einen Polizisten stellen, der die Nutzung des Werks genau kontrolliert und bei einer Rechtsverletzung sofort *ex ante* einschreitet. Ein solches Vorgehen sei völlig undenkbar. Mit Hilfe von DRM-Systemen und ihren technischen Schutzarchitekturen werde jedoch ein solches Schutzniveau hergestellt.

[1459] So meinen *Mori/Kawahara*, E 73 Transactions of the IEICE 1133 (1990), zu ihrem Superdistribution-Konzept (s. dazu oben Teil 1, E I): „Superdistribution relies neither on law nor ethics to achieve these protections; instead it is achieved through a combination of electronic devices, software, and administrative arrangements whose global design we call the ‚Superdistribution Architecture'." *Nelson* schreibt zu seinem Xanadu-Projekt (s. dazu oben Teil 1, B) in Literary Machines 93.1, S. 2/42: „To bypass some legal problems, we foresee establishing copyright convention *internal to the network* and contractually agreed upon by all participants." Hinsichtlich eBooks meint die *Electronic Book Exchange Working Group*, S. 9: „Electronic books may be able to avoid the fine print [as in shrink-warp software license agreements, which are seen as frustrating to the consumer] by making automatic what you can and cannot do with a copyrighted work". *Sandholm* meint in bezug auf Multi-Agentensysteme (s. dazu oben Teil 2, E III) in: Klusch/Weiß (Hrsg.), S. 113, 130: „In conventional commerce, deals are usually enforced by law. […] However, such enforced protocols are problematic in electronic commerce, e.g. over the Internet. First, adequate laws for ecommerce may be lacking, or the transacting agents (human or computational) may be governed by different laws, e.g. they may be sited in different countries. Also, the laws might not be strictly enforced, or enforcing them – e.g. by litigation – might be impractically expensive. We would like the agents' ecommerce transactions to work properly independent of such fluctuations in enforcement."

[1460] Ebenso *Goldstein*, 45 J. Copyright Soc'y U.S.A. 151 (1997): „Contracts and encryption today exist entirely outside of copyright; they are substitutes for, not supplements to, copyright"; *Gimbel*, 50 Stan. L. Rev. 1671, 1672 (1998): „The danger is not that copyright law will be infringed but that it will be supplanted."

aus Technik, Nutzungsverträgen und Technologie-Lizenzverträge ersetzt.[1461] Der Gesetzgeber unterstützt die Entwicklung solcher Schutzmechanismen, indem er gesetzliche Vorschriften zum rechtlichen Umgehungsschutz technischer Schutzmaßnahmen einführt.[1462] In DRM-Systemen deutet sich ein Paradigmenwechsel im Schutz der Inhalteanbieter an.

Grundsätzlich ist diese Entwicklung zu begrüßen. Im Vergleich zum herkömmlichen Urheberrecht bieten die Schutzmechanismen eines DRM-Systems bisher ungekanntes Maß an Flexibilität. Technische Schutzmaßnahmen können individuell auf die Bedürfnisse der Inhalteanbieter angepaßt werden und neuartige Geschäftsmodelle unterstützen.[1463] Auch der vertragliche Schutz kann den Bedürfnissen der Vertragsparteien sehr viel genauer angepaßt werden kann als das notwendigerweise pauschalierende Urheberrecht. Solche Schutzmechanismen können regelmäßig auch schneller auf neue technische Herausforderungen reagieren als das Urheberrecht, das zu diesem Zweck erst in langwierigen Gesetzgebungsverfahren geändert werden muß.[1464]

Daher stellt sich die Frage, welche Bedeutung dem Urheberrecht in diesem Umfeld noch zukommt.[1465] Inhalteanbieter werden sich in DRM-Systemen zunehmend durch alternative Mechanismen außerhalb des Urheberrechts schützen. Das Urheberrecht als Mechanismus zum Schutz des Urhebers wird in diesem Umfeld an Bedeutung verlieren. Damit soll nicht der These vom Tod des Urheberrechts das Wort geredet werden. Auch in DRM-Systemen werden dem Urheberrecht weiterhin wichtige Aufgaben

---

[1461] In diese Richtung auch *Goldstein*, 45 J. Copyright Soc'y U.S.A. 151 ff. (1997); *Vinje*, EIPR 1999, 192, 207; *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1157 (1998); *dies.*, 12 Berkeley Tech. L. J. 93, 94 (1997); *Elkin-Koren/Salzberger*, 19 Int. Rev. L. & Econ., 553, 575 (1999); *Fisher*, 73 Chi.-Kent L. Rev. 1203 (1998); *Lessig*, S. 126; *ders.*, 113 Harv. L. Rev. 501, 529 (1999); *Hugenholtz*, 26 Brooklyn J. Int'l L. 77 ff. (2000); *ders.*, 6 Maastricht Journal of European and Comparative Law 308 ff. (1999); *Vinje*, EIPR 1996, 431, 437 (1996); *Burk/Cohen*, S. 8; s. a. *Reichman/Franklin*, 147 U. Penn. L. Rev. 875, 929 (1999); in bezug auf das Verhältnis zwischen Urheberrecht und Vertrag s. a. *Lunney*, 1 Tulane J. Tech. & Intell. Prop. 1 (1999); *Merges*, 12 Berkeley Tech. L. J. 115, 118 (1997).

[1462] *Burk/Cohen*, S. 8 f. Zwar werden diese Vorschriften teilweise in Urheberrechtsgesetze integriert. Das ändert aber nichts an der Tatsache, daß sie mit dem Urheberrecht im herkömmlichen Sinne wenig zu tun haben, s. dazu oben bei Fn. 1296 und *Bechtold* in: Hoeren/Sieber (Hrsg.), Teil 7.11, Rdnr. 25.

[1463] Hier sei nur nochmals auf die ausdifferenzierten „rights management languages" hingewiesen, s. dazu oben Teil 1, C II 2 a bb. S. a. *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1159 (1998).

[1464] *Merges*, 12 Berkeley Tech. L. J. 115, 119 (1997); *Lunney*, 1 Tulane J. Tech. & Intell. Prop. 1 (1999), Abs. 36 ff.

[1465] S. *Hugenholtz*, 6 Maastricht Journal of European and Comparative Law 308, 317 (1999): „In a totally controlled system no need for protection *erga omnes* [i.e. through copyright] will remain."

zukommen. Allerdings wird sich die Bedeutung des Urheberrechts wandeln.[1466]

III. Auswirkungen des DRM aus rechtsökonomischer Sicht

1. Allgemeines

Betrachtet man DRM-Systeme mit den Methoden der ökonomischen Analyse des Rechts, so könnte sich der dargestellte Paradigmenwechsel bestätigen. Im Vergleich zum anglo-amerikanischen Rechtskreis spielt die ökonomische Analyse des Rechts im Deutschland eine geringe Rolle.[1467] Das gilt in besonderem Maße für das Urheberrecht. Ökonomische Untersuchungen des Urheberrechts sind in Deutschland rar.[1468] In den USA ist die ökonomische Betrachtung des „copyright law" dagegen weit verbreitet.[1469] Dieser unterschiedliche Stellenwert des „law and economics"-Ansatzes liegt – neben dem grundsätzlich anderen Stellenwert in der U.S.-amerikanischen Rechtswissenschaft – an der unterschiedlich ausgestalteten Begründung des Urheberrechts.[1470] Während das U.S.-amerikanische „copyright law" sehr stark von utilitaristischen Gedanken geprägt ist, liegt die Begründung des deutschen und kontinentaleuropäischen Urheberrechts zu einem großen Teil in persönlichkeitsrechtlichen Überlegungen.[1471]

[1466] S. dazu unten Teil 3, B II 2, und B II 3. Diese Thesen dürfen nicht als generelle Aussage über die zukünftige Bedeutung des Urheberrechts mißverstanden werden. Die vorliegende Arbeit beschäftigt sich ausschließlich mit den Implikationen von DRM-Systemen. Außerhalb von DRM-Systemen wird das Urheberrecht auch in Zukunft notwendig sein, um Urheber und Leistungsschutzberechtigte zu schützen. Es sei nur im „analogen" Bereich an öffentliche Aufführungen und Ausstellungen erinnert (s. §§ 18, 19 UrhG). Allerdings werden in Zukunft immer mehr Werke in digitaler Form angeboten und vertrieben werden. Mit der zunehmenden Digitalisierung weiter Lebensbereiche steigt der potentielle Anwendungsbereich von DRM-Systemen an. DRM-Systeme könnten zu einem wichtigen Grundpfeiler der entstehenden Informationsgesellschaft werden. Insofern sind die Thesen der Arbeit auf einen Bereich der urheberrechtlichen Werkverwertung anwendbar, der in Zukunft stark anwachsen und herkömmliche Arten der Werkverwertung verdrängen wird.

[1467] Grundlegend zur ökonomischen Analyse des Rechts in Deutschland *Eidenmüller*; *Schäfer/Ott*.

[1468] Solche Analysen finden sich bei *Kulle*; *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69 ff.; *Koboldt/Schmidtchen*, Ordo 42 (1991), 295 ff.; *Pethig*, 144 JITE 462 ff. (1988).

[1469] Grundlegend *Landes/Posner,* 18 J. Legal Stud. 325 (1989). Einen Überblick über die dortige Diskussion geben *Gordon/Bone* in: Bouckaert/De Geest (Hrsg.), Band II, Kap. 1610, S. 189 ff.

[1470] Zu weiteren Gründen s. *Dreyfuss*, 53 Vand. L. Rev. 1821 ff. (2000).

[1471] Die utilitaristische Ausrichtung des U.S.-amerikanischen „copyright law" wird schon aus der U.S.-Verfassung deutlich. Section 8 des Art. 1 der Verfassung lautet in Auszügen: „The Congress shall have Power […] *to promote the Progress of Science and useful Arts*, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries". Auch ein bekanntes urheberrechtliches Standardwerk in den USA baut explizit auf einem ökonomischen Verständnis des Ur-

Jedoch ist auch im kontinentaleuropäischen Rechtskreis zu beobachten, daß sich der Akzent des Urheberrechts zunehmend von einem Kulturzu einem Industrierecht verschiebt.[1472] Fragen des Investitionsschutzes werden immer wichtiger.[1473] Daher dürfte der ökonomischen Analyse des Urheberrechts in Zukunft auch im kontinentaleuropäischen Raum eine gesteigerte Bedeutung zukommen.[1474] Man muß man sich aber der Grenzen der ökonomischen Analyse des Urheberrechts bewußt sein. Sie kann kein abschließendes normatives Modell für die rechtliche Ausgestaltung des Urheberschutzes bieten.[1475] Auch sind die Prämissen der ökonomischen Analyse des Urheberrechts nicht unumstritten.[1476] Trotz alledem zeigt sich, daß die ökonomische Analyse von DRM-Systemen interessante Ergebnisse liefern kann, die auch für das juristische Verständnis dieser Systeme einen deutlichen Erkenntnisgewinn versprechen.

Die nachfolgenden Ausführungen wollen keine umfassende ökonomische Analyse des Urheberrechts leisten. Vielmehr werden nur jene Bereiche behandelt, die für den Untersuchungsgegenstand der Arbeit von

heberrechts auf, s. *Goldstein*, Copyright, § 1.14, S. 1:40 ff. In der deutschen Urheberrechtslehre hat sich in diesem Jahrhundert die sog. „monistische Theorie" durchgesetzt. Danach ist das Urheberrecht ein einheitliches Recht, in welchem persönlichkeits- und vermögensrechtliche Befugnisse untrennbar miteinander verwoben sind. Dies wird aus § 11 UrhG deutlich; s. dazu *Schack*, Rdnr. 306; *Vogel* in: Schricker (Hrsg.), UrhG-Kommentar, Einl. Rdnr. 72. Dem geht ein jahrhundertelanger Theorienstreit über die Begründung des Urheberrechts voraus, der von der naturrechtlichen Begründung eines „geistigen Eigentums" über die Theorie eines Persönlichkeitsrechts und die Theorie vom Immaterialgüterrecht bis zur dualistischen Theorie reichte; s. dazu *Rehbinder*, Rdnr. 20 ff.; *Vogel*, a. a. O., Einl. Rdnr. 62 ff.; *Leinemann*, S. 17 ff. Zu den Unterschieden zwischen dem anglo-amerikanischen „copyright law" und dem kontinentaleuropäischen „droit d'auteur" s. im Überblick *Götting/Fikentscher* in: Assmann/Bungert (Hrsg.), Kap. 7, Rdnr. 209.

1472 S. dazu *Schricker* (Hrsg.), Urheberrecht auf dem Weg zur Informationsgesellschaft, S. 142; *Schricker*, GRUR 1992, 242 ff.; *Dreier*, CR 2000, 45, 46; *Bechtold*, GRUR 1998, 18, 24.

1473 *Wiebe*, GRUR 1994, 233, 244 f.

1474 Ebenso *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 190. In den USA läßt sich derzeit geradezu eine Renaissance der „economic analysis of copyright law" beobachten.

1475 *Wiebe*, GRUR 1994, 233, 243. *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69, 110, meint: „Sicherlich kann die ökonomische Analyse keine eindeutigen Vorgaben machen, wie ein Urheberrechtssystem ausgestaltet sein sollte. Sie kann aber Hilfestellungen geben." *Lemley/McGowan*, 86 Cal. L. Rev. 479, 610 (1998), schreiben: „There is a difference between law *and* economics, an estimable discipline, and law *as* economics, an unrealistic construct" (Hervorhebungen im Original). Vgl. weiterhin *Fisher*, 101 Harv. L. Rev. 1659, 1696 ff. (1988).

1476 Eine Auseinandersetzung mit diesen Einwänden würde den Rahmen der vorliegenden Untersuchung sprengen. S. dazu im Überblick *Gordon/Bone* in: Bouckaert/De Geest (Hrsg.), Band II, Kap. 1610, S. 189, 200 f.

unmittelbarem Interesse sind.[1477] Zunächst wird das Potential von DRM-Systemen aus rechtsökonomischer Sicht dargestellt: DRM-Systeme bieten neue Möglichkeiten der Ausschließbarkeit (dazu unten 2) und der Preisdiskriminierung (dazu unten 3). Sie haben das Potential, Transaktionskosten zu senken (dazu unten 4).

In diesen drei Abschnitten wird die Position, daß DRM-Systeme tiefgreifende ökonomische Änderungen mit sich bringen, zunächst unkritisch referiert. In einem zweiten Teil wird auf die Schwachstellen dieser Position hingewiesen und dargelegt, daß unter ökonomischen Gesichtspunkten eine Begrenzung des DRM-Schutzes sinnvoll sein kann (dazu weiter unten B I).

2. Digitale Inhalte als öffentliches Gut

a) Allgemeines

Digitale Inhalte unterscheiden sich – wie jede Information – von körperlichen Gütern durch ihre Nicht-Rivalität in der Nutzung und Nicht-Exklusivität im Angebot. Ein Gut ist *nicht-rivalisierend*, wenn der Konsum durch eine Person den Nutzen des Guts für andere Personen nicht schmälert. Das Gut ist – sobald es einmal vorhanden ist – grenzkostenlos[1478] mehrnutzbar, das heißt nicht knapp.[1479] Information[1480] läßt sich unendlich oft kopieren, ohne daß dabei die Information selbst aufgezehrt wird.[1481] Damit unterscheidet sich Information von körperlichen Gütern: Ißt A einen Apfel, kann B diesen Apfel nicht auch essen (rivalisierendes Gut); hört A eine Wagner-Oper, kann B diese Oper dennoch hören (nicht-rivalisierendes Gut).[1482] Ein Gut ist *nicht-exklusiv*, wenn es unmöglich ist, nichtzahlende Konsumenten von der Nutzung des Guts auszu-

[1477] Beispielsweise wird nicht auf das Verhältnis zwischen ökonomischer Analyse und Urheberpersönlichkeitsrechten eingegangen. Zur Anwendung der ökonomischen Analyse in diesem Bereich s. *Hansmann/Santilli*, 26 J. Legal Stud. 95 ff. (1997); *van den Bergh*, I.P.Q. 1998, 17, 30 ff.; *Landes/Posner*, 18 J. Legal Stud. 325, 327 (1989).

[1478] Die Grenzkosten sind der Kostenanstieg, der sich aus der Herstellung einer zusätzlichen Produktionseinheit eines Guts ergibt, *Pindyck/Rubinfeld*, S. 80; *Cooter/Ulen*, S. 21; *Varian*, S. 263 f.

[1479] *Cooter/Ulen*, S. 42, 126; *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69, 73; *Detering*, S. 21. Anders ausgedrückt sind bei einem nicht-rivalisierenden Gut die Grenzkosten – also die Kosten, das Gut einem zusätzlichen Konsumenten zur Verfügung zu stellen – für jeden Outputlevel gleich Null, *Pindyck/Rubinfeld*, S. 644.

[1480] Wenn im folgenden von „Information" gesprochen wird, so ist dies im weitesten Sinne zu verstehen. Darunter fallen alle Arten urheberrechtlich geschützter Werke, aber auch bloße Daten und Fakten. Unter „Information" fallen alle digitalen Inhalte, die einem DRM-System vertrieben werden können.

[1481] *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69, 72 f.; *Fisher*, 101 Harv. L. Rev. 1659, 1700 (1988).

[1482] *Benkler*, 53 Vand. L. Rev. 2063, 2065 f. (2000).

schließen.[1483] Für den Produzenten von Information wäre es ohne das Urheberrecht oder äquivalente Schutzmechanismen unmöglich zu verhindern, daß Dritte die Information nutzen, ohne dafür ein Entgelt zu entrichten.

Güter, die diese beiden Eigenschaften aufweisen, werden „öffentliche Güter" genannt.[1484] Daraus ergibt sich, daß Information – also auch digitale Inhalte – öffentliche Güter sind.[1485] Streng genommen ist zwischen dem Informationsgut selbst und dem Informationsträger zu unterscheiden:[1486] Die Information selbst ist ein öffentliches Gut mit den eben beschriebenen Eigenschaften. Wird diese auf einem Informationsträger (CD, Schallplatte, Buch) gespeichert, so ist dieses Trägermedium ein normales privates, das heißt rivalisierendes und exklusives Gut: Ein bestimmtes Buchexemplar kann nicht gleichzeitig von mehreren Lesern genutzt werden.[1487] Jedoch ist es regelmäßig möglich, das Informationsgut vom Informationsträger abzukoppeln und auf einen neuen Informationsträger zu kopieren.[1488] Weiterhin kann in DRM-Systemen Information

[1483] *Pindyck/Rubinfeld*, S. 645. Dies ist eine Vereinfachung: Nahezu jedes Gut ist mit entsprechendem Aufwand exkludierbar. Mit der Aussage, ein Gut sei nicht-exklusiv, ist nur gemeint, daß die Kosten der Exkludierbarkeit so hoch wären, daß dies faktisch nicht in Frage kommt; s. *Jasay* in: Newman (Hrsg.), Band 3, S. 95, 100.

[1484] Klassische Beispiele öffentlicher Güter sind Leuchttürme und die Landesverteidigung. Es ist umstritten, ob bei der Definition des öffentlichen Guts nur auf dessen Nicht-Rivalität oder zusätzlich auf dessen Nicht-Exklusivität abzustellen ist. Im ersteren Sinne *Demsetz*, 13 J. L. & Econ. 293, 295 (1970); *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69, 72; im letzteren Sinne *Pindyck/Rubinfeld*, S. 645. Die vorliegende Arbeit folgt der umfassenderen Definition, wonach öffentliche Güter nicht-rivalisierend und nicht-exklusiv sind. Zu Theorie der öffentlichen Güter allgemein s. *McNutt* in: Bouckaert/De Geest (Hrsg.), Band I, Kap. 0750, S. 927 ff. Mitunter wird auch das Internet selbst als öffentliches Gut angesehen, s. dazu *Hallgren/McAdams* in: McKnight/Bailey (Hrsg.), S. 455, 466 ff. *Elkin-Koren* und *Salzberger* meinen, daß die Gewährung von Rechtsschutz durch den Staat ein öffentliches Gut ist: Kein Bürger kann auf praktikable Weise vom Rechtsschutz ausgeschlossen werden, und die Inanspruchnahme des Rechtsschutzes durch einen Bürger hindert andere Bürger nicht an der Inanspruchnachme. Der technische Schutz von DRM-Systemen übernehme diese Funktion des Rechtsschutzes und wandele ihn in ein privates Gut, s. *Elkin-Koren/Salzberger*, 19 Int. Rev. L. & Econ. 553, 576 (1999).

[1485] *Lemley*, 75 Tex. L. Rev. 989, 994 (1997); *Pindyck/Rubinfeld*, S. 645; *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69, 72; *Shy*, S. 163; *Watt*, S. 3; *Elkin-Koren/Salzberger*, 19 Int. Rev. L. & Econ. 553, 559 (1999); *Gordon/Bone* in: Bouckaert/De Geest (Hrsg.), Band II, Kap. 1610, S. 189, 191. Manche Autoren fassen Information nicht unter den Begriff des öffentlichen Guts, sondern meinen, Information teile nur die Merkmale eines öffentlichen Guts, so *Cooter/Ulen*, S. 126. Das ist allenfalls ein begrifflicher Unterschied.

[1486] *Messerschmitt/Szyperski*, S. 4 f., differenzieren weiterhin zwischen normalen Informationsgütern und Computersoftware, die teilweise andere Eigenschaften aufweist.

[1487] *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69, 72 f.; *Kulle*, S. 80; *Koboldt/Schmidtchen*, Ordo 42 (1991), 295, 297; *Watt*, S. 4; s. a. *Gordon* in: Ott/Schäfer (Hrsg.), S. 328, 330 Fn. 5.

[1488] *Kulle*, S. 80; s. a. *Watt*, S. 5.

verbreitet werden, ohne überhaupt jemals an ein physikalisches Trägermedium gebunden zu sein. Information wird zum bloßen elektronischen Signal.[1489] Damit trifft die Charakterisierung von Information als öffentlichem Gut für den vorliegenden Untersuchungsgegenstand zu.

Aufgrund der Nicht-Exklusivität und Nicht-Rivalität von Information kann jedermann, der in den Besitz der Information kommt, diese vervielfältigen und selbst als Anbieter der Information auftreten.[1490] Die Eigenschaften von Information schließen es aus, daß der ursprüngliche Informationsproduzent dies verhindern kann.[1491] Diese Kopisten bieten die Information auf dem Markt in Konkurrenz zum ursprünglichen Informationsproduzenten an. Während der Informationsproduzent Ressourcen in die Produktion der Information gesteckt hat, haben die Kopisten nur die vergleichsweise geringen Kosten der Vervielfältigung zu tragen:[1492] Es ist teuer, Information zu produzieren, aber billig, sie zu kopieren.[1493] Daher können die Kopisten die Information zu einem geringeren Preis anbieten. Die Konsumenten, die die Information zum günstigsten Preis erwerben wollen, weichen auf das Angebot der Kopisten aus. Auf dem Markt würde dadurch ein Preis für die Information entstehen, der den Grenzkosten[1494] der Informationsvervielfältigung durch die Kopisten entspricht, die Gewinnerwartungen der Informationsproduzenten aber weit enttäuschen würde.[1495] Mitunter werden Konsumenten die Information auch gar nicht erwerben. Sie verheimlichen ihre wirklichen Präferenzen und ihre Zahlungsbereitschaft bezüglich dieses Guts in der Hoffnung, daß andere Konsumenten das Gut kaufen und sie es dann aufgrund der Nicht-Exklusivität und Nicht-Rivalität des Guts mitnutzen können. Es ensteht ein typisches Trittbrettfahrer-Problem (sogenannte „free rider"-Problematik).[1496]

[1489] *Elkin-Koren/Salzberger*, 19 Int. Rev. L. & Econ. 553, 559 f. (1999); s. a. o. bei Fn. 1309.

[1490] *Cooter/Ulen*, S. 126; *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69, 73.

[1491] Wegen der Nicht-Exklusivität kann der Informationsproduzent nicht verhindern, daß ein Dritter in den Besitz der Information kommt. Wegen der Nicht-Rivalität behindert die Nutzung der Information durch den Dritten auch keine anderen Personen.

[1492] *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69, 73.

[1493] *Landes/Posner*, 18 J. Legal Stud. 325, 326 (1989); *Cooter/Ulen*, S. 126; *Shapiro/Varian*, S. 3. Anders ausgedrückt: Die Produktion von Information führt zu hohen versunkenen Kosten, aber niedrigen Grenzkosten, *Shapiro/Varian*, S. 3; *European Communication Council* (Hrsg.), S. 165; *Shy*, S. 5. Zum Begriff der versunkenen Kosten s. unten Fn. 1498.

[1494] Zum Begriff s. oben Fn. 1478.

[1495] *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69, 73 f.; *Landes/Posner*, 18 J. Legal Stud. 325, 326 ff. (1989); *Gordon*, 73 Chi.-Kent L. Rev. 1367, 1370 f. (1998); *Lemley*, 75 Tex. L. Rev. 989, 995 (1997); *Netanel*, 106 Yale L. J. 283, 292 (1996); *Cooter/Ulen*, S. 126; *Posner*, Economic Analysis of Law, S. 43, mit Zahlenbeispiel.

[1496] *Cooter/Ulen*, S. 107; *Schäfer/Ott*, S. 96. Allgemein zeichnet sich Trittbrettfahrerverhalten dadurch aus, daß eine Person ihre Präferenzen für ein Gut nicht kundtut, weil sie glaubt, das Gut werde auch produziert und finanziert, ohne daß sie ihren Wunsch danach äußert und einen anteiligen Finanzierungsbeitrag leistet; s. *Müller*, S. 36.

In einem solchen Umfeld, in dem die Information auf dem Markt zu Grenzkostenpreisen angeboten wird, wäre eine optimale Nutzung der Information gewährleistet. Aufgrund der Nicht-Rivalität von Information sollte nämlich jeder, der eine positive Zahlungsbereitschaft für die Information aufweist, diese auch nutzen können. Da die Grenzkosten bei der Vervielfältigung von Information nahezu Null sind, könnte beim Angebot der Information zu Grenzkostenpreisen jeder Konsument mit einer Zahlungsbereitschaft über Null die Information nutzen.[1497]

Dabei wird jedoch vernachlässigt, daß der ursprüngliche Informationsproduzent bei einem Marktpreis zu Grenzkosten die versunkenen Kosten,[1498] die die Informationsproduktion mit sich brachte – also die Kosten der Werkschöpfung –, nicht wieder einspielen könnte. Die erwarteten Gewinne würden nicht ausreichen, um den Informationsproduzenten überhaupt zur Produktion der Information zu bewegen.[1499] Aufgrund der Nicht-Rivalität und Nicht-Exklusivität von Information bestünde daher kein (monetärer) Anreiz zur ressourcenverbrauchenden Herstellung von Information. Dies würde am Markt zu einer suboptimalen Produktion von Information führen.[1500] Es würde weniger Information produziert, als die Konsumenten tatsächlich zu erwerben bereit wären.[1501] Öffentliche Güter, zu denen Information zählt, stellen einen Fall des Marktversagens[1502] dar.

Um dieses Marktversagen zu beseitigen und die Produktion von Information zu maximieren, wird dem potentiellen Informationsproduzenten das Urheberrecht im Sinne eines „property right“[1503] gewährt.[1504] Durch

---

1497 *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69, 74.

1498 „Versunkene Kosten“ sind Ausgaben, die nach ihrer Aufwendung nicht mehr rückgängig gemacht werden können, *Pindyck/Rubinfeld*, S. 205. Davon sind „Fixkosten“ zu unterscheiden; darunter sind Kosten zu verstehen, die nicht mit dem Produktionsniveau variieren, s. *Pindyck/Rubinfeld*, S. 206 f. In der ökonomischen Analyse des Urheberrechts werden beide Begriffe oft miteinander vermengt, s. *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69, 75 Fn. 17.

1499 *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69, 74; *Lemley*, 75 Tex. L. Rev. 989, 995 (1997).

1500 *Cooter/Ulen*, S. 126; *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69, 73 f.; *Koboldt/Schmidtchen*, Ordo 42 (1991), 295, 297.

1501 *Gordon*, 17 U. Dayton L. Rev. 853, 854 (1992).

1502 Marktversagen kennzeichnen Fälle, in denen der Markt nicht zu optimalen Ergebnissen führt. Marktversagen können durch unterschiedliche Ursachen entstehen, insbesondere Marktmacht, externe Effekte, öffentliche Güter, und asymmetrische Informationen; s. dazu allgemein *Pindyck/Rubinfeld*, S. 591 f.; *Cooter/Ulen*, S. 40 ff.; *Schäfer/Ott*, S. 96 ff.; *Müller*, S. 32 ff. Zur Bedeutung von Marktversagen im Internet s. *Elkin-Koren/Salzberger*, 19 Int. Rev. L. & Econ., 553, 555 ff. (1999).

1503 Die Übersetzung von „property right“ schwankt in der deutschen Literatur zwischen Handlungs-, Verfügungs- und Herrschaftsrechten. Die Übersetzung als „Eigentumsrecht“ ist zu eng. S. zum Begriff *Lehmann* in: Neumann (Hrsg.), S. 519, 520.

1504 Die Gewährung eines „property right“ ist nicht die einzig mögliche Antwort auf das vorliegende Marktversagen. Herkömmliche öffentliche Güter werden regelmäßig

das „property right" erhält der Urheber die Möglichkeit, nicht-zahlende Konsumenten von der Nutzung seiner Werke auszuschließen. Potentielle Kopisten müssen dem Urheber ein Entgelt entrichten, um in den Besitz eines Werkexemplars zu gelangen, das sie dann kopieren können. Dadurch werden die Kosten der Kopisten künstlich erhöht. Das Urheberrecht sorgt also dafür, daß das technisch problemlose Vervielfältigen von Information für Unbefugte künstlich verteuert wird.[1505] Dadurch kann der Urheber am Markt für sein Werk Preise über den Grenzkosten verlangen und die Kosten der Werkschöpfung wieder einspielen. Damit schafft das Urheberrecht letztlich einen Anreiz zur Schaffung von Werken.[1506] Unter dem Blickwinkel der Information als öffentlichem Gut beseitigt das Urheberrecht – in den Grenzen der effektiven Rechtsdurchsetzung – das Merkmal der Nicht-Exklusivität von Information.[1507]

---

vom Staat bereitgestellt (Beispiel: Landesverteidigung) oder zumindest staatlich subventioniert. Auch bei Information sind solche Ansätze denkbar (Beispiel: staatliche Bereitstellung von Wettervorhersagen, staatliche Unterstützung privater Forschungseinrichtungen), *Cooter/Ulen*, S. 126. Im klassischen Anwendungsbereich des Urheberrechts wird jedoch aus mehreren Gründen (u. a. fehlende objektive Bewertungsmaßstäbe ästhetischer Fragen, Zensurpotential) auf solche „staatsnahen" Ansätze verzichtet, *Gordon* in: Ott/Schäfer (Hrsg.), S. 328, 331; *dies.*, 82 Colum. L. Rev. 1600, 1611 f. (1982); s. aber *Shavell/van Ypersele*. In der ökonomischen Analyse ist umstritten, ob und in welchem Umfang das Urheberrecht zur Anreizschaffung überhaupt notwendig ist. Für den Informationsproduzenten bestehen auch andere Möglichkeiten der Refinanzierung. So kann in Einzelfällen der zeitliche Vorsprung ausreichen, den er am Markt vor seinen Nachahmern hat („lead time"), um seine Investitionen zu amortisieren, vgl. *Schäfer/Ott*, S. 587. Weitere Finanzierungsstrategien bestehen in der Koppelung mit anderen, exklusiven Gütern, speziellen Vermarktungsstrategien und ähnlichem. S. dazu insgesamt *Breyer*, 84 Harv. L. Rev. 281, 293 ff. (1970); *Palmer*, 12 Hamline L. Rev. 261 ff. (1989); *van den Bergh*, I.P.Q. 1998, 17, 22 ff.; *Boyle*, 53 Vand. L. Rev. 2007, 2015 f. (2000); *Koboldt/Schmidtchen*, Ordo 42 (1991), 295, 300; in bezug auf DRM-Systeme und das Internet s. *Schlachter*, 12 Berkeley Tech. L. J. 15, 23 ff. (1997). Ein umfassender Institutionenvergleich der unterschiedlichen Anreizsysteme im urheberrechtlichen Bereich fehlt bislang, *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69, 111.

[1505] *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69, 75; *Cooter/Ulen*, S. 128; *Lemley*, 75 Tex. L. Rev. 989, 996 (1997); *Sterk*, 94 Mich. L. Rev. 1197, 1207 (1996).

[1506] Vgl. *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69, 76.

[1507] *Watt*, S. 3 f.; *Gordon*, 82 Colum. L. Rev. 1600, 1612 (1982); *Gordon/Bone* in: Bouckaert/De Geest (Hrsg.), Band II, Kap. 1610, S. 189, 193; *Gordon* in: Ott/Schäfer (Hrsg.), S. 328, 332; *dies.*, 17 U. Dayton L. Rev. 853, 854 f. (1992). Auch bei einem Schutz durch das Urheberrecht bleibt Information immer noch nicht-rivalisierend. Dies führt zu einer suboptimalen Nutzung der Information, s. dazu unten Teil 3, A III 2 c aa. Neben dem hier vorgestellten Ansatz bestehen innerhalb der ökonomischen Analyse noch andere Ansätze zur Begründung des Urheberrechts. So läßt sich das Urheberrecht spieltheoretisch begründen, s. *Gordon*, 17 U. Dayton L. Rev. 853, 860 ff. (1992). Die Spieltheorie beschäftigt sich mit der Analyse strategischer Interaktionen mehrerer Beteiligter. Danach wird es zur sog. „dominanten Strategie", selbst keine Werke zu schaffen, sondern nur fremde Werke zu kopieren. Die Einführung des Urheberrechts dient der Veränderung der Auszahlungsmatrix und verändert dadurch die Strategien der Beteiligten, *Gordon*, 17 U. Dayton L. Rev. 853, 864 f. (1992). Zu den Grundlagen der

b) Neue Möglichkeiten der Ausschließbarkeit

Wenn das Urheberrecht Information zu einem exklusiven Gut macht, um so einen Anreiz zur Informationsproduktion zu geben, stellt sich die Frage, welche Aufgabe dem Urheberrecht im DRM-Bereich zukommt. Die technischen Schutzkomponenten von DRM-Systemen ermöglichen eine umfassende Zugangs- und Nutzungskontrolle von digitalen Inhalten. In Kombination mit unterstützenden vertraglichen und gesetzlichen Schutzmechanismen ermöglichen sie es, nicht-zahlende Dritte von der Nutzung digitaler Inhalte auszuschließen.[1508] Daneben führen Nutzungsverträge in Kombination mit unterstützenden technischen und gesetzlichen Schutzmechanismen ebenfalls zu einem Schutzniveau, das dem eines absolut wirkenden Rechts vergleichbar ist.[1509] Die ineinandergreifenden Schutzmechanismen eines DRM-Systems – allen voran technische Schutzmaßnahmen – ermöglichen die Kontrolle darüber, welche Nutzer digitale Inhalte nutzen können. Damit machen DRM-Systeme digitale Inhalte vom nicht-exklusiven zum exklusiven Gut.[1510]

Aus ökonomischer Sicht kommt DRM-Systemen somit die gleiche Aufgabe zu wie dem Urheberrecht. Da der Schutz von DRM-Systemen umfassender und und sicherer ist als der Schutz des Urheberrechts,[1511] ist ihre Anreizwirkung sogar stärker.[1512] Dann stellt sich aber die Frage, welche

---

Spieltheorie im Überblick s. *Pindyck/Rubinfeld*, S. 461 ff.; *Varian*, S. 477 ff.; *Cooter/Ulen*, S. 34 ff. Ein wiederum anderer Ansatz der ökonomischen Analyse des Urheberrechts findet sich bei *Lunney*, 49 Vand. L. Rev. 483 ff. (1996).

[1508] S. dazu oben Teil 3, A II 2 b cc.

[1509] S. dazu oben Teil 3, A II 2 b bb. Zu dem komplexen Zusammenspiel der unterschiedlichen Schutzmechanismen insgesamt s. oben Teil 3, A II.

[1510] Ebenso in Ansätzen *Elkin-Koren/Salzberger*, 19 Int. Rev. L. & Econ., 553, 559 (1999); *Heal* in: Kaul/Grunberg/Stern (Hrsg.), S. 220, 222; *Pindyck/Rubinfeld*, S. 645; *DeLong/Froomkin* in: Kahin/Varian (Hrsg.), S. 6, 37; *Burk*, 21 Cardozo L. Rev. 121, 168 (1999); *Benkler*, 53 Vand. L. Rev. 2063, 2065 (2000); *Bonus* in: Dettling (Hrsg.), S. 129, 148 f. Mitunter wird ein solches Gut als „teilweise öffentliches Gut" bezeichnet, da nur noch die Nicht-Rivalität des Guts besteht; so für den Bereich des Pay-TV *Bonus*, a. a. O., S. 148 f. Die These, daß DRM-Systeme digitale Inhalte zum exklusiven Gut machen, hängt allerdings stark von der Sicherheit des betreffenden DRM-Systems ab; ebenso *Elkin-Koren/Salzberger*, 19 Int'l. Rev. L. & Econ. 553, 561 (1999), die aus diesem Grund die Ansicht vertreten, die herkömmlichen ökonomischen Methoden zur Analyse öffentlicher Güter seien für digitale Inhalte nur bedingt brauchbar. Technische Entwicklungen müßten als endogene Variablen in die ökonomische Analyse mit einbezogen werden, *Elkin-Koren/Salzberger*, a. a. O., S. 561, 578 f. Bei anderen öffentlichen Gütern lassen sich ähnliche Entwicklungen beobachten. So könnten Leuchttürme durch verschlüsselte Funksignale ersetzt werden, die nur noch von den berechtigten Empfängern entschlüsselt werden könnten; bei Fernstraßen kann die Nutzung mit Hilfe elektronischer Mautsysteme kontrolliert werden. In beiden Fällen würde die Nicht-Exklusivität des öffentlichen Guts entfallen, dessen Nicht-Rivalität aber bestehen bleiben; s. dazu *Schäfer/Ott*, S. 525.

[1511] S. dazu oben Teil 3, A II 2.

[1512] Vgl. *Elkin-Koren/Salzberger*, 19 Int. Rev. L. & Econ., 553, 575 (1999); *Bell*, 76 N.C. L. Rev. 557, 579 f. (1998).

Bedeutung das Urheberrecht in diesem Umfeld noch hat: Das Marktversagen, aufgrund dessen das Urheberrecht geschaffen wurde – die Nicht-Exklusivität von Information – besteht bei DRM-Systemen nicht mehr.[1513] Zwar bedeutet dies nicht, daß das Urheberrecht in DRM-Systemen aus ökonomischer Sicht bedeutungslos ist.[1514] Auch aus ökonomischer Sicht wird sich seine Bedeutung aber wandeln.[1515] Insgesamt zeigen sich deutliche Parallelen zwischen der rein juristischen und der rechtsökonomischen Analyse von DRM-Systemen.[1516]

c) „Deadweight loss" bei DRM-Systemen

Wie dargelegt wurde, zielen das Urheberrecht und DRM-Systeme darauf ab, das Marktversagen, das aus der Nicht-Exklusivität von Information herrührt, zu beseitigen und einen Anreiz zur Informationsproduktion zu schaffen. Es stellt sich die Frage, ob diese Ansätze zur Beseitigung des Marktversagens nicht mit irgendwelchen Nachteilen verbunden sind. Tatsächlich kann gezeigt werden, daß das Urheberrecht wie auch DRM-Systeme aufgrund eines sogenannten „deadweight loss" zu einer suboptimalen Nutzung der Information führen. Zur Erklärung dieser These muß etwas ausgeholt werden. Dafür wird zunächst – unter Rückgriff auf Effizienzgesichtspunkte des Monopols – der „deadweight loss" dargestellt, der durch die Schaffung des Urheberrechts auftritt (dazu unten aa). Anschließend wird dieses Ergebnis auf DRM-Systeme übertragen (dazu unten bb).

[1513] Ebenso in Ansätzen *Elkin-Koren/Salzberger*, 19 Int. Rev. L. & Econ., 553, 560 (1999); *Elkin-Koren*, 12 Berkeley Tech. L. J. 93, 105 (1997); *Dowell*, 86 Cal. L. Rev. 843, 854 Fn. 45 (1998); *Cooter/Ulen*, S. 136; *Watt*, S. 57 („[…] self-protection strategies are in fact substitutes to copyright law […]"); *Bell*, Escape from Copyright, S. 15.

[1514] S. dazu unter rechtlichen Gesichtspunkten schon bei Fn. 1466. Für eine ökonomische Untermauerung der These, daß das Urheberrecht in DRM-Systemen an Bedeutung verlieren sollte, wäre ein umfassender institutioneller Vergleich des Schutzes durch das Urheberrecht mit dem Schutz durch DRM-Systeme notwendig. DRM-Systeme wären gegenüber dem Urheberrecht zu bevorzugen, wenn die gesamten Kosten, die durch das Urheberrecht enstehen – unter anderem Rechtsdurchsetzung, staatlicher Schutz durch Gerichte u. ä. –, höher wären als die Kosten von DRM-Systemen. Diese These vertreten *Elkin-Koren/Salzberger*, 19 Int. Rev. L. & Econ., 553, 575 (1999). S. zu diesem Vergleich auch *Watt*, S. 58; *Fisher*, 73 Chi.-Kent L. Rev. 1203, 1232 (1998); *Gordon*, 17 U. Dayton L. Rev. 853, 856 f. (1992): „If the desired incentives could be forthcoming even *without* an intellectual property rule in place, it is probably wasteful for the courts and legislature to become involved" (Hervorhebung im Original). Zu den diesbezüglichen Kosten des Urheberrechts s. *Gordon/Bone* in: Bouckaert/De Geest (Hrsg.), Band II, Kap. 1610, S. 189, 196. Für einen solchen Vergleich wären auch empirische Daten notwendig. Die Verfügbarkeit statistischer Daten bezüglich des Urheberrechts ist traditionell aber recht dürftig. Die vorliegende Arbeit will und kann einen solchen Vergleich daher nicht leisten.

[1515] S. dazu unten Teil 3, B I 2, und B I 3. S. dazu unter rechtlichen Gesichtspunkten unten Teil 3, B II 2, und B II 3.

[1516] Vgl. die vorliegenden Ausführungen mit den Ausführungen oben Teil 3, A II 3.

aa) Effizienzverluste beim Urheberrecht

In der Ökonomie ist das Phänomen des „deadweight loss" insbesondere aus der Effizienzanalyse von Monopolmärkten bekannt. Die ökonomische Analyse des Urheberrechts greift regelmäßig auf diese Überlegungen zurück, wenn sie vergleichbare Phänomene im urheberrechtlichen Bereich untersucht.

In der rechtsökonomischen Literatur findet sich oft die Aussage, das Urheberrecht führe – wie andere Immaterialgüterrechte auch – zu einer Monopolstellung des Berechtigten.[1517] Das trifft in dieser Allgemeinheit nicht zu: In den meisten Fällen führt das Urheberrecht zu keinem Monopol im ökonomischen Sinne.[1518] Das Urheberrecht verleiht ein Monopol im ökonomischen Sinne nur in den Fällen, in denen für das geschützte Werk kein nahes Substitut[1519] erhältlich ist.[1520] Kann der Konsument bei gleichen Präferenzen auf andere Werke ausweichen, verfügt der Urheber eines Werks über keine Monopolstellung im ökonomischen Sinn. Die Frage, ob das Urheberrecht zu einem Monopol im ökonomischen Sinne führt, hängt damit von der Art des geschützten Werks und dem Markt ab, auf dem das Werk verkauft wird: Ein absoluter Kino-Kassenschlager hat wenige, mitunter gar keine Substitute. Bei einem Dreigroschen-Roman bestehen dagegen viele nahe Substitute. In den meisten Fällen existieren für urheberrechtlich geschützte Werke keine perfekten Substitute, in vielen Fällen nicht einmal nahe Substitute.[1521]

Wenn im folgenden Effizienzverluste des Monopols dargestellt und diese Ergebnisse auf das Urheberrecht übertragen werden, so ist zu bedenken, daß sich der Urheber regelmäßig in einem Markt befindet, dessen Struktur zwischen vollkomenemem Wettbewerb und Monopol angesiedelt ist. Auch in solchen Märkten einer monopolistischen Konkur-

---

[1517] In diese Richtung *Cooter/Ulen*, S. 128; *Posner*, Economic Analysis of Law, S. 299; *Netanel*, 106 Yale L. J. 283, 293 (1996); *Elkin-Koren/Salzberger*, 19 Int. Rev. L. & Econ., 553, 559 Fn. 13 (1999); *Gordon/Bone* in: Bouckaert/De Geest (Hrsg.), Band II, Kap. 1610, S. 189, 194. Auch in der ökonomischen Literatur finden sich solche Aussagen, so bei *Varian*, S. 410, in bezug auf Patente und bei *Kulle*, S. 83, in bezug auf das Urheberrecht.

[1518] *Lemley*, 75 Tex. L. Rev. 989, 996 Fn. 26, 1066 (1997); *Kitch*, 53 Vand. L. Rev. 1727, 1734 (2000). Ein Monopol im ökonomischen Sinne liegt vor, wenn in einem Markt nur ein Verkäufer existiert, *Pindyck/Rubinfeld*, S. 327 f.

[1519] Zwei Güter sind perfekte Substitute, wenn der Konsument bereit ist, ein Gut für das andere zu einem konstanten Verhältnis zu tauschen, *Varian*, S. 36, 105 f. Bei Substituten führt die Erhöhung des Preises für das eine Gut zur Erhöhung der Nachfrage des anderen Guts, *Pindyck/Rubinfeld*, S. 22 f.

[1520] *Fisher*, 73 Chi.-Kent L. Rev. 1203, 1234 (1998); *Easterbrook*, 13 Harv. J. L. & Pub. Pol'y 108, 109 (1990); *Kitch*, 53 Vand. L. Rev. 1727, 1730 (2000); *van den Bergh*, I.P.Q. 1998, 17, 25.

[1521] S. a. *Cohen*, 97 Mich. L. Rev. 462, 520 ff. (1998); *dies.*, 53 Vand. L. Rev. 1799, 1811 (2000); *Fisher*, 101 Harv. L. Rev. 1659, 1702 f. (1988); *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1184 (1998).

renz[1522] können jedoch – wenn auch in abgeschwächter Form – Effizienzverluste des Monopols auftreten.[1523] Urheber und Monopolist sind in mancher Hinsicht vergleichbar. So können beide für ihre Produkte Preise über den Grenzkosten verlangen.[1524] Bis zu einem gewissen Maß verleiht das Urheberrecht Monopolmacht.[1525] Daher lassen sich die darzustellenden Effekte bis zu einem gewissen Maß auch im urheberrechtlichen Bereich beobachten.[1526]

Will ein Unternehmen ein bestimmtes Gut anbieten, so stellt sich die Frage, in welcher Menge es das Produkt produzieren soll. Die Volkswirtschaftslehre geht davon aus, daß private Unterehmen ihre Gewinne maximieren wollen. Der Gewinn eines Unternehmens ergibt sich aus der Differenz zwischen Erlös und Kosten.[1527] Ein Unternehmen wird die Produktion eines Guts solange ausweiten, bis die Kosten der Herstellung einer zusätzlichen Produktionseinheit (sogenannte „Grenzkosten") nicht mehr niedriger sind als der Erlös aus der Herstellung dieser zusätzlichen Produktionseinheit (sogenannter „Grenzerlös"). Es ist daher die allgemeine Bedingung für ein Gewinnmaximum, daß gilt

Grenzkosten = Grenzerlös.[1528]

Auf einem Konkurrenzmarkt hat der einzelne Anbieter keinen Einfluß auf den Preis des Guts, das er verkauft. Der Preis ergibt sich vielmehr aus

---

[1522] Und darum handelt es sich bei Urheberrechten, s. *Koboldt/Schmidtchen*, Ordo 42 (1991), 295, 300; *Merges*, 53 Vand. L. Rev. 1857, 1859 (2000); zum Begriff der „monopolistischen Konkurrenz" allgemein s. *Varian*, S. 434 ff.; *Pindyck/Rubinfeld*, S. 423 ff.

[1523] *van den Bergh*, I.P.Q. 1998, 17, 26; *Sterk*, 94 Mich. L. Rev. 1197, 1205 Fn. 45 (1997); s. a. *Varian*, S. 436; *Pindyck/Rubinfeld*, S. 424.

[1524] Zum Urheberrecht s oben Teil 3, A III 2 a, S. 220 ff. Auch der Monopolist kann aufgrund seiner Monopolmacht Preise über den Grenzkosten verlangen, s. *Pindyck/Rubinfeld*, S. 327. Zu der Vergleichbarkeit s. *Benkler*, 53 Vand. L. Rev. 2063, 2070 f. (2000).

[1525] *Gordon*, 73 Chi.-Kent L. Rev. 1367, 1388 Fn. 76 (1998); *Benkler*, 53 Vand. L. Rev. 2063, 2068 (2000): „To the extent that we observe a transaction for an information good at a positive price, we are observing a situation where the seller has ‚market power' to engage at least to some extent in above marginal cost pricing." *Fikentscher*, S. 41, spricht anschaulich von „property rights" als „kleinen Monopolen". Kritisch zu der Gleichsetzung von Immaterialgüterrechten mit Monopolen *Kitch*, 53 Vand. L. Rev. 1727, 1729 ff. (2000); allgemein kritisch zu diesem Ansatz *Easterbrook*, 13 Harv. J. L. & Pub. Pol'y 108 ff. (1990).

[1526] Auf die Gefahren dieser Betrachtung, die in der ökonomischen Analyse des Urheberrechts weit verbreitet ist, weist – aus dem Blickwinkel der Neuen Institutionenökonomie und unter stärkerer Berücksichtigung des Patentrechts als des Urheberrechts – *Merges*, 53 Vand. L. Rev. 1857, 1858 ff. (2000), hin. Insgesamt ist die folgende Analyse als Untersuchung eines Referenzmodells zu verstehen.

[1527] *Varian*, S. 314; *Schäfer/Ott*, S. 7S. 79.

[1528] *Schäfer/Ott*, S. 79; *Varian*, S. 401; *Pindyck/Rubinfeld*, S. 255 f.; *Cooter/Ulen*, S. 26 f.

dem Aufeinandertreffen von Angebot und Nachfrage. Anbieter sind in einem Konkurrenzmarkt sogenannte „Preisnehmer".[1529] Daher wird der Anbieter auf einem Konkurrenzmarkt die Produktion eines Guts so lange ausdehnen, wie der Preis, den er am Markt antrifft, höher ist als die Kosten einer zusätzlichen Produktionseinheit. Im Konkurrenzmarkt gilt daher für das Gewinnmaximum des Anbieters die speziellere Bedingung

Grenzkosten = Preis.[1530]

In einem Konkurrenzmarkt bestimmt also der Marktpreis das Angebot des einzelnen Anbieters. Da der Anbieter für jede beliebige Höhe des Marktpreises ein Outputniveau wählen wird, bei dem die Grenzkosten dem Marktpreis entsprechen, ist die Grenzkostenkurve eines Anbieters im Konkurrenzmarkt seine Angebotskurve.[1531] Faßt man die Nachfragekurven aller Konsumenten und die Angebotskurven aller Unternehmen, die das gleiche Gut nachfragen beziehungsweise herstellen, durch Horizontaladdition zusammen, erhält man die Marktnachfrage- und Marktangebotskurve für dieses Gut.[1532] Beide sind in Abbildung 8 (S. 294) dargestellt.[1533]

In einem Konkurrenzmarkt ergibt sich die angebotene Menge und der Preis eines Guts aus dem Schnittpunkt von Angebots- und Nachfragekurve: In Abbildung 8 wird das Gut in der Menge Q_c zum Preis P_c hergestellt. Bei diesem sogenannten Gleichgewichtspreis werden genau so viel Güter angeboten, wie Güter nachgefragt werden.[1534]

[1529] *Pindyck/Rubinfeld*, S. 252; *Varian*, S. 275, 363; *Schäfer/Ott*, S. 79. Dies liegt daran, daß im Modell der vollständigen Konkurrenz eine große Anzahl von Anbietern auf dem Markt tätig sind („atomistischer Markt"), so daß die Möglichkeiten des einzelnen Anbieters, durch eine Änderung seines eigenen Preises den Marktpreis zu verändern, vernachlässigbar klein sind. Zu den weiteren Annahmen des Modells der vollständigen Konkurrenz s. unten Fn. 1671.

[1530] *Schäfer/Ott*, S. 79; *Pindyck/Rubinfeld*, S. 257 f.

[1531] Anders ausgedrückt: Der Marktpreis entspricht genau den Grenzkosten, solange jeder Anbieter auf seinem gewinnmaximierenden Niveau produziert, s. *Varian*, S. 366; *Pindyck/Rubinfeld*, S. 263; *Schäfer/Ott*, S. 79.

[1532] *Schäfer/Ott*, S. 82; *Varian*, S. 253 ff.; *Pindyck/Rubinfeld*, S. 116 f.

[1533] Es sei darauf hingewiesen, daß es sich bei diesen Ausführungen um die Darstellung eines Referenzmodells handelt. Beispielsweise läßt sich die Abbildung nicht exakt auf die Produktion von Information übertragen. Bei der Informationsproduktion sind die Grenzkosten regelmäßig sehr gering; auch wird die Grenzkostenkurve über weite Strecken keinen ansteigenden Verlauf nehmen. Aus Gründen einer anschaulichen Erklärung im weiteren Verlauf wird die übliche Darstellungsweise verwendet, ohne daß an dieser Stelle auf die Besonderheiten der Informationsproduktion eingegangen wird. Solche Modifikationen werden bis zu einem gewissen Maß von *Cohen*, 53 Vand. L. Rev. 1799, 1802 (2000), berücksichtigt.

[1534] S. dazu allgemein *Varian*, S. 3 ff.; *Pindyck/Rubinfeld*, S. 23 f. Es kann gezeigt werden, daß bei vollständiger Konkurrenz auf allen Märkten im Gleichgewicht Pareto-Effizienz erreicht wird (sogenanntes erstes Wohlfahrtstheorem); s. dazu *Varian*, S. 16, 292 ff., 494 ff.; *Pindyck/Rubinfeld*, S. 572 ff.; *Schäfer/Ott*, S. 83. Zum Begriff der Pareto-Effizienz s. unten Fn. 1553.

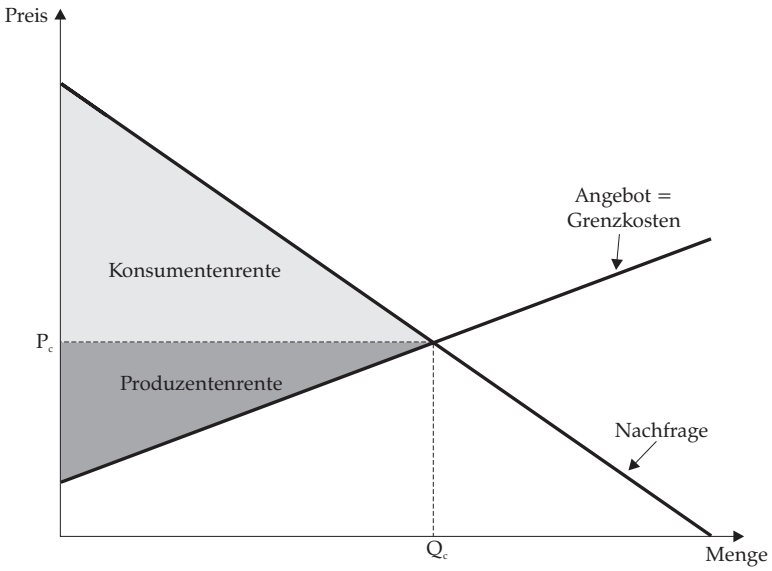


Abbildung 8: Angebot und Nachfrage bei vollkomenem Wettbewerb

Dieser Betrachtung des Konkurrenzmarkts ist der Monopolmarkt gegenüberzustellen. Während für Unternehmen auf Konkurrenzmärkten der Preis ein nicht beeinflußbarer Parameter ist, kann ein Monopolist den Preis eines Guts grundsätzlich beliebig festsetzen.[1535] Dabei muß er jedoch die Auswirkungen der Preisänderung auf die Nachfrage berücksichtigen: Will der Monopolist eine höhere Menge absetzen, so muß er – wegen der grundsätzlich fallenden Nachfragekurve[1536] – dafür den Preis senken.[1537] Dabei muß der Monopolist grundsätzlich den Preis für *alle* abgesetzten Güter (und nicht nur für die zusätzliche Outputmenge) senken.[1538] Diese Wechselwirkung hat zur Folge, daß die Grenzerlöskurve des Monopolisten stärker absinkt als die Nachfragefragekurve (s. Abbildung 9).[1539]

[1535] *Varian*, S. 400; *Pindyck/Rubinfeld*, S. 328.

[1536] Grundsätzlich steigt mit sinkendem Preis eines Guts die Nachfrage nach diesem Gut an und vice versa. Anderes gilt ausnahmsweise bei sog. „Giffen-Gütern"; s. *Varian*, S. 90 ff., 101.

[1537] *Cooter/Ulen*, S. 32; *Schäfer/Ott*, S. 85.

[1538] *Varian*, S. 401 f.; *Cooter/Ulen*, S. 32; *Sterk*, 94 Mich. L. Rev. 1197, 1206 (1996). Einen Ausweg bietet die Preisdiskriminierung, s. dazu unten Teil 3, A III 3.

[1539] *Cooter/Ulen*, S. 32; *Posner*, Economic Analysis of Law, S. 295 Fn. 1; *Pindyck/Rubinfeld*, S. 329; *Sterk,* 94 Mich. L. Rev. 1197, 1206 (1996). Die mathematische Herleitung würde hier zu weit führen, s. dazu *Varian*, S. 402 f.

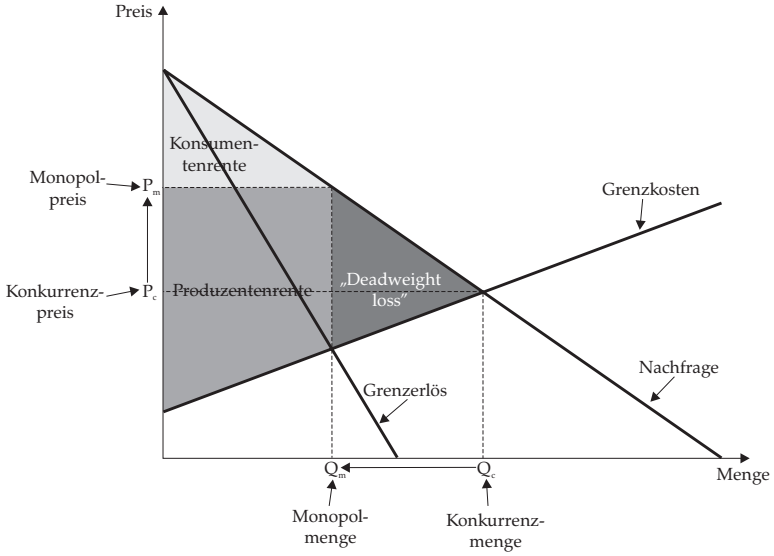


Abbildung 9: Angebot und Nachfrage bei monopolistischem Anbieter

Weiterhin unterscheidet sich ein Anbieter im Monopolmarkt von einem Anbieter im Wettbewerbsmarkt insofern, als der Gewinn des Monopolisten nicht maximiert wird, wenn die Grenzkosten dem Preis des Guts entsprechen.[1540] Anders als im Wettbewerbsmarkt muß ein Monopolist den Preis nicht als Datum hinnehmen, sondern kann ihn selbst festsetzen.[1541] Auch für den Monopolisten gilt jedoch der allgemeine Grundsatz, daß er seinen Gewinn maximiert, wenn die Grenzkosten dem Grenzerlös entsprechen.[1542] Wie Abbildung 9 zeigt, maximiert der Monopolist seinen Gewinn daher, wenn er die Menge Q_m des Guts produziert, da sich an diesem Punkt die Grenzkostenkurve mit der Grenzerlöskurve schneidet.[1543] Bei dieser Outputmenge kann der Monopolist das Gut bei gegebener Nachfragekurve zum Preis P_m absetzen. Der Monopolist bietet das Gut damit zu einem Preis an, der über den Grenzkosten des Guts liegt.

Damit ist in einem Monopolmarkt der Preis höher und die Ausbringungsmenge niedriger als in einem Wettbewerbsmarkt.[1544] Der Monopo-

[1540] Zu dieser Bedingung für ein Gewinnmaximum, die nur im Wettbewerbsmarkt gilt, s. oben bei Fn. 1530.

[1541] *Cooter/Ulen*, S. 31 f.

[1542] S. dazu oben bei Fn. 1528.

[1543] S. *Varian*, S. 403; *Pindyck/Rubinfeld*, S. 329 ff.; *Posner*, Economic Analysis of Law, S. 297 f.

[1544] Vgl. in Abbildung 9 den Unterschied zwischen P_m und P_c sowie zwischen Q_m und Q_c; s. *Cooter/Ulen*, S. 33; *Schäfer/Ott*, S. 85.

list beschränkt den verfügbaren Output, um seinen Gewinn zu maximieren.[1545] In einer Monopolbranche sind Konsumenten typischerweise schlechter und der Anbieter typischerweise besser gestellt als in einer Wettbewerbsbranche.[1546] Dies zeigt sich an der Veränderung der sogenannten „Konsumenten-" und „Produzentenrenten". Die Konsumentenrente ist ein Maß der Vorteile, die sich für alle Konsumenten zusammengenommen aus einem Gütertausch ergeben. Sie läßt sich als die Differenz zwischen dem höchsten Preis, den der jeweilige Konsument beim Kauf des Guts gerade noch zu akzeptieren bereit wäre (sogenannter „Vorbehaltspreis"), und dem Preis begreifen, den der Konsument tatsächlich zahlt.[1547] Dagegen ist die Produzentenrente das Maß des Nettonutzens aller Produzenten und läßt sich als die Differenz zwischen dem Betrag, zu dem der jeweilige Produzent das Gut tatsächlich verkauft hat, und dem Betrag begreifen, zu dem der Produzent das Gut gerade noch verkaufen würde (also den Grenzkosten).[1548] In Abbildung 8 ist die Konsumentenrente die hellgraue Fläche unterhalb der Nachfragekurve und oberhalb des Marktpreises P_c.[1549] Die Produzentenrente ist die mittelgraue Fläche oberhalb der Angebotskurve und und unterhalb des Marktpreises.[1550] Ein Vergleich des Wettbewerbs- und des Monopolmarkts zeigt, daß die Konsumentenrente im Monopolmarkt zu Gunsten der Produzentenrente sinkt (vgl. die hell- und mittelgrau schraffierten Flächen in den Abbildungen 8 und 9). In einem Monopolmarkt kommt es zu einer Wohlstandsumverteilung von den Konsumenten auf den Monopolisten.

Zwar führt diese Wohlstandsumverteilung an sich noch zu keinem Effizienzverlust.[1551] Allerdings ist zu beachten, daß die Konsumenten, deren Vorbehaltspreis für das Gut zwischen Q_m und Q_c liegt, im Monopolmarkt das Gut nicht erwerben können, da der Monopolist zu wenig Einheiten des Guts produziert. Vergleicht man die Abbildungen 8 und 9, so zeigt sich,

---

1545 *Varian*, S. 13; *Pindyck/Rubinfeld*, S. 347; *Cooter/Ulen*, S. 32 f.

1546 *Varian*, S. 406.

1547 *Pindyck/Rubinfeld*, S. 123, 288; *Schäfer/Ott*, S. 70. Dabei muß zwischen der Untersuchung eines einzelnen Konsumenten am Markt und dessen sog. „Nettorente des Konsumenten" und der aggregierten Untersuchung aller Konsumenten am Markt und deren sog. „Konsumentenrente" unterschieden werden, s. *Varian*, S. 238 f.

1548 *Varian*, S. 2S. 248; *Pindcyk/Rubinfeld*, S. 289. Auch hier muß zwischen der Untersuchung eines einzelnen Unternehmens am Markt und dessen sog. „Nettorente des Produzenten" und der aggregierten Untersuchung aller Unternehmen am Markt und deren sog. „Produzentenrente" unterschieden werden, s. *Varian*, S. 247 f.

1549 S. *Pindyck/Rubinfeld*, S. 288 f.

1550 S. *Pindyck/Rubinfeld*, S. 289.

1551 S. *Pindyck/Rubinfeld*, S. 348; Schäfer/*Ott*, S. 86; *Posner*, Economic Analysis of Law, S. 302. Zu dem Unterschied zwischen Allokationseffizienz und Verteilungsgerechtigkeit s. *Schäfer/Ott*, S. 6 f., 31, ausführlich zum Verhältnis s. *Eidenmüller*, S. 273 ff. Denkmodelle wie die Pareto-Effizienz und das Kaldor-Hicks-Kriterium treffen nur eine Aussage über die Effizienz, nicht aber über die Verteilungsgerechtigkeit einer Allokation, s. *Posner*, Economic Analysis of Law, S. 15; *Varian*, S. 541.

daß im Monopolmarkt gegenüber dem Konkurrenzmarkt die Summe aus Konsumenten- und Produzentenrente um eine Fläche verringert ist, die in Abbildung 9 dunkelgrau schraffiert wurde. Dieser Effizienzverlust wird als „deadweight loss" bezeichnet.[1552] Ein Monopolmarkt ist weder nach dem Pareto-Kriterium[1553] noch nach dem Kaldor-Hicks-Kriterium[1554] effi-

[1552] S. *Varian*, S. 409; *Pindyck/Rubinfeld*, S. 347 f.; *Posner*, Economic Analysis of Law, S. 301 ff.; *Schäfer/Ott*, S. 85 f. Genau genommen besteht der „deadweight loss" nur aus der Differenz zwischen der in Abbildung 9 dunkelgrau schraffierten Fläche und der Konsumentenrente, die die Konsumenten erhalten, wenn sie ihr an zweiter Stelle präferiertes Gut kaufen. Dadurch ist der „deadweight loss" tatsächlich kleiner als oben eingezeichnet. An der grundsätzlichen Aussage der Analyse ändert sich aber nichts; s. dazu *Fisher*, 73 Chi.-Kent L. Rev. 1203, 1236 Fn. 78 (1998); *Easterbrook*, 13 Harv. J. L. & Pub. Pol'y 108, 110 (1990). *Posner*, S. 301, erklärt den „deadweight loss" damit, daß durch den erhöhten Preis des Monopolisten manche Konsumenten auf (mehr oder minder nahe) Substitute ausweichen werden, deren Grenzkosten höher sind als die Grenzkosten des monopolistischen Gutes. Dadurch werden vermehrt Güter konsumiert, die höhere Produkionskosten als das monopolistische Gut haben. Diese erhöhten Kosten führen zu dem „deadweight loss".

[1553] Ein Zustand ist Pareto-effizient, wenn die Besserstellung einer Person nur gelingt, wenn dadurch mindestens eine andere Person einen Nachteil erleidet, *Schäfer/Ott*, S. 26; *Varian*, S. 14, 291; *Posner*, Economic Analysis of Law, S. 14; *Eidenmüller*, S. 48. Nachdem der Monopolist alle Q_m Einheiten des Guts abgesetzt hat, wäre er grundsätzlich bereit, zusätzliche Einheiten zu einem Preis zwischen P_m und P_c – was seinen Grenzkosten entspricht – zu verkaufen. Dadurch würden sowohl der Monopolist als auch der Konsument besser gestellt, der das zusätzlich produzierte Gut erwerben würde; eine Pareto-Verbesserung wäre möglich. Ein Monopolmarkt ist daher Pareto-ineffizient, *Varian*, S. 16, 407 f. Daß der Monopolist die zusätzliche marginale Einheit nicht verkauft, liegt daran, daß er beim Verkauf dieser Einheit zu einem niedrigeren Preis als P_m den Preis für alle „inframarginalen" Einheiten des Guts, die er derzeit verkauft, senken müßte. Dies würde insgesamt zu einer Gewinnverminderung führen. Der Monopolist will den *zusätzlichen* Output also nicht erzeugen, da dadurch der Erlös, den er für den *gesamten* Output erhalten könnte, verringert würde; s. *Varian*, S. 407 f., 419, und oben bei Fn. 1538 f. Der Monopolist kann dieses Problem nur mit Hilfe der sog. Preisdiskriminierung vermeiden, s. dazu unten Teil 3, A III 3. Zur Kritik am Konzept der Pareto-Effizienz s. *Posner*, Economic Analysis of Law, S. 14 f.; *Eidenmüller*, S. 48 ff.

[1554] Im Gegensatz zum Pareto-Kriterium liegt nach dem Kaldor-Hicks-Kriterium auch dann eine Verbesserung vor, wenn durch eine Änderung zwar bestimmte Personen schlechter gestellt werden, aber der Vorteil der Bessergestellten insgesamt höher ist als der Nachteil der Schlechtergestellten. In diesem Fall könnten die Bessergestellten nämlich den Schlechtergestellten Ersatz leisten und wären danach immer noch bessergestellt, s. *Cooter/Ulen*, S. 44; *Posner*, Economic Analysis of Law, S. 14; *Eidenmüller*, S. 51; *Schäfer/Ott*, S. 32 ff., auch zur Kritik an diesem Kriterium. Das Kaldor-Hicks-Kriterium verlangt nur, daß alle Schlechtergestellten entschädigt werden *können*, nicht aber, daß sie auch tatsächlich entschädigt *werden* – in diesem Fall läge schon eine Paretoverbesserung vor, *Schäfer/Ott*, S. 32; *Eidenmüller*, S. 51. Da beim Übergang vom Monopolmarkt zum Wettbewerbsmarkt die Summe der Konsumentenrente und der Produzentenrente um die Fläche des „deadweight loss" zunimmt, ist der Zuwachs der Konsumentenrente größer als die Gewinnminderung des Produzenten durch den Verlust der Monopolstellung. Die Konsumenten könnten aus diesem Zuwachs die Verluste des Monopolisten kompensieren und hätten immer noch einen Nettovorteil. Damit ist ein Wettbewerbsmarkt nach dem Kaldor-Hicks-Kriterium effizienter, s. *Schäfer/Ott*, S. 86.

zient.[1555] Der „deadweight loss" des Monopolmarkts stellt gegenüber dem Wettbewerbsmarkt einen echten Wohlfahrtsverlust und damit die sozialen Kosten des Monopols dar.[1556]

Diese Analyse der Allokationsineffizienz von Monopolmärkten läßt sich – mit den oben erwähnten Einschränkungen[1557] – auf das Urheberrecht übertragen.[1558] Dem Monopolisten insofern vergleichbar, erlaubt das Urheberrecht dem Urheber, für Werkausgaben Preise zu verlangen, die über deren Grenzkosten liegen.[1559] Damit werden aber nicht alle potentiellen Nutzer mit positiver Zahlungsbereitschaft in den Genuß des Werks kommen.[1560] Wie das Monopol führt das Urheberrecht zu einem „deadweight loss", also zu einem Wohlfahrtsverlust.[1561] Der notwendige Produktionsanreiz wird mit dem Verzicht auf eine optimale Nutzung einmal bereitgestellter Informationsgüter erkauft.[1562] Das Urheberrecht verringert durch seine Anreizwirkung den Wohlfahrtsverlust durch Unterproduktion („social welfare loss due to underproduction") unter Inkaufnahme eines Wohlfahrtsverlusts durch Unternutzung („social welfare loss due to underutilization").[1563] Anders ausgedrückt bedeutet das: Je geringer der Urheberschutz ist, desto geringer ist der Anreiz, schöpfe-

[1555] Zusätzlich kann ein Monopol ineffizient sein, weil der Monopolist Ressourcen aufwendet, um seine Monopolstellung zu erreichen und aufrechtzuerhalten – Ressourcen, die ansonsten wirtschaftlich sinnvollere Aktivitäten investiert werden könnten, s. *Posner*, Economic Analysis of Law, S. 306.

[1556] *Posner*, Economic Analysis of Law, S. 302.

[1557] S. oben bei Fn. 1517 ff.

[1558] S. dazu auch *Fisher*, 73 Chi.-Kent L. Rev. 1203, 1234 ff. (1998); *Netanel*, 106 Yale L. J. 283, 293 (1996); *Gordon*, 41 Stan. L. Rev. 1343, 1437 Fn. 399 (1989); *Liebowitz*, S. 3 ff.; *Gordon/Bone* in: Bouckaert/De Geest (Hrsg.), Band II, Kap. 1610, S. 189, 194 f.; *Benkler*, 53 Vand. L. Rev. 2063, 2070 f. (2000); *Fisher*, 101 Harv. L. Rev. 1659, 1700 ff. (1988); *Meurer*, Copyright and Price Discrimination; *Detering*, S. 32 f.

[1559] S. dazu oben Teil 3, A III 2 a.

[1560] *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69, 76; *Netanel*, 106 Yale L. J. 283, 293 (1996).

[1561] *Schäfer/Ott*, S. 577; *DeLong/Froomkin* in: Kahin/Varian (Hrsg.), S. 6, 14; *Detering*, S. 32 f.; *Netanel*, 106 Yale L. J. 283, 293 (1996).

[1562] Das Urheberrecht hindert die Allgemeinheit, die Nicht-Rivalität des geschützten Werks voll auszunutzen, *Gordon* in: Ott/Schäfer (Hrsg.), S. 328, 330, 334; s. weiterhin *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69, 76; *Koboldt/Schmidtchen*, ORDO 42 (1991), 295, 307 f.; *van den Bergh*, I.P.Q. 1998, 17, 21; *Lemley*, 75 Tex. L. Rev. 989, 996 (1997); *Meurer*, 45 Buff. L. Rev. 845, 858 (1997); *Cooter/Ulen*, S. 128; *Benkler*, 53 Vand. L. Rev. 2063, 2066 (2000); *Fisher*, 101 Harv. L. Rev. 1659, 1701 f. (1988). Neben dem entstehenden „deadweight loss" verursacht das Urheberrecht noch weitere Kosten, etwa eine Anreizhemmung gegenüber zukünftigen Schöpfern, Transaktionskosten zum Abschluß von Nutzungs- und Verwertungsverträgen sowie Kosten der Verwaltung und Durchsetzung des Urheberrechts; s. dazu insgesamt *Gordon/Bone* in: Bouckaert/De Geest (Hrsg.), Band II, Kap. 1610, S. 189, 194 ff.

[1563] *Koboldt* in: Ott/Schäfer (Hrsg.), S. 69, 76; *Watt*, S. 12; *Fisher*, 101 Harv. L. Rev. 1659, 1703 (1988).

risch tätig zu werden; je höher der Urheberschutz ist, desto weniger Nutzer wird das Werk erreichen, weil ihnen die Kosten dafür zu hoch sein werden. Aufgabe des Gesetzgebers ist es, einen angemessenen Ausgleich zwischen diesen beiden Polen – Unterproduktion und Unternutzung – zu schaffen.[1564]

bb) Effizienzverluste bei DRM-Systemen

Fraglich ist, ob sich die beschriebene Allokationsineffizienz des Urheberrechts auch beim Schutz durch DRM-Systeme beobachten läßt. Dabei ist zu beachten, daß durch DRM-Systeme – wie durch das Urheberrecht – das Charakteristikum der Nicht-Exklusivität von Information beseitigt wird.[1565] Wie das Urheberrecht erlauben DRM-Systeme dem Inhalteanbieter, für digitale Inhalte Preise zu verlangen, die über deren Grenzkosten liegen. Unter dem Blickwinkel der vorliegenden Effizienzanalyse sind damit der Schutz durch das Urheberrecht und durch DRM-Systeme vergleichbar:[1566] Auch DRM-Systeme führen zu einem „deadweight loss" und zu einer Unternutzung der produzierten Information.[1567] Diese Parallelität findet ihre Ursache darin, daß der Wohlfahrtsverlust durch Unternutzung in der Nicht-Rivalität der Information begründet ist:[1568] Ein Gut wird nur dann auf einem gesellschaftlich optimalen Niveau konsumiert, wenn jeder Konsument, dessen Vorbehaltspreis mindestens den Grenzkosten entspricht, das Gut konsumieren kann. Bei nicht-rivalisierenden Gütern betragen die Grenzkosten jedoch Null.[1569] Dann müßte das nicht-rivalisierende Gut nahezu jedem zur Verfügung stehen. Da sowohl das Urheberrecht als auch DRM-Systeme die Grenzkosten aus Anreizgründen künstlich erhöhen, wird eine solch weite Verbreitung des nicht-rivalisierenden Guts jedoch gerade verhindert.[1570]

[1564] *Landes/Posner*, 18 J. Legal Stud. 325, 326 (1989); *Fisher*, 101 Harv. L. Rev. 1659, 1703 (1988); *Liebowitz*, S. 5. S. dazu auch unten Teil 3, B I 2.

[1565] S. oben Teil 3, A III 2 b.

[1566] Ebenso *Watt*, S. 57 („[… copyright and self-protection strategies] both have the effect of imposing greater expected costs upon pirates").

[1567] Vgl. *Benkler*, 53 Vand. L. Rev. 2063, 2066 (2000).

[1568] Vgl. *DeLong/Froomkin* in: Kahin/Varian (Hrsg.), S. 6, 13 f.; *Benkler*, 53 Vand. L. Rev. 2063, 2066 (2000).

[1569] S. dazu die Definition der „Nicht-Rivalität" in Fn. 1479. Tatsächlich liegen die Grenzkosten bei digitalen Inhalten regelmäßig über Null. Selbst wenn die Kosten, eine Kopie eines digitalen Inhalts zu erstellen, tatsächlich Null sein sollten, heißt das noch nicht, daß die gesamten Grenzkosten auch Null sind; s. *Kitch*, 53 Vand. L. Rev. 1727, 1737 (2000).

[1570] Grundsätzlich könnte mit DRM-Systemen auch die Nicht-Rivalität von Information beseitigt werden: Würde eine Softwarekomponente kontrollieren, daß ein bestimmter digitaler Inhalt zu einem bestimmten Zeitpunkt immer nur von einer Person weltweit genutzt werden könnte, wäre der Inhalt ein rivalisierendes Gut. Dies würde jedoch die Nutzungsmöglichkeit des Inhalts noch in viel höherem Maße beschränken, als wenn der Inhalt exklusiv, aber nicht-rivalisierend wäre, s. *DeLong/Froomkin* in: Kahin/Varian (Hrsg.), S. 6, 38. Diese Beschränkung des Informationsflusses ist daher nicht wünschenswert; zu diesem Zweck werden DRM-Systeme nicht eingesetzt.

3. Möglichkeit der Preisdiskriminierung

Wenn DRM-Systeme grundsätzlich zu einem Wohlfahrtsverlust führen, könnte man die Frage stellen, ob sich dieser nicht vermeiden läßt. Um die Frage zu beantworten, ist wiederum auf die ökonomische Analyse des Monopolmarkts zurückzugreifen. Dort kann der „deadweight loss" mit Hilfe einer sogenannten „Preisdiskriminierung" vermindert, theoretisch sogar ganz beseitigt werden (s. dazu unten a). Diese Überlegungen lassen sich auf DRM-Systeme übertragen (s. dazu unten b).

a) Preisdiskriminierung beim Monopol

Die Ineffizienz des Monopols zeigt sich daran, daß die Konsumenten mit einem Vorbehaltspreis zwischen P_m und P_c (s. oben Abbildung 9, S. 295) das Gut nicht erwerben können. Zwar wären sie bereit, einen Preis über den Grenzkosten P_c zu zahlen. Der Monopolist will diesen *zusätzlichen* Output aber nicht erzeugen, da dadurch der Erlös, den er für den *gesamten* Output erhält, verringert würde.[1571] Dies liegt daran, daß ein Monopolist das Gut an alle Konsumenten normalerweise zum gleichen Preis verkaufen muß: Würde der Monopolist unterschiedliche Preise berechnen, so könnte ein Konsument, dem der Monopolist einen niedrigen Preis berechnet, das Gut kaufen und an einen anderen Konsumenten weiterverkaufen, dem der Monopolist selbst einen höheren Preis berechnen würde. Durch diese sogenannten „Arbitrage"-Geschäfte[1572] würde die differenzierte Preispolitik des Monopolisten effektiv unterlaufen.[1573]

Mitunter kann der Monopolist aber solche Arbitrage-Geschäfte verhindern. So kann dem Konsumenten der Weiterverkauf des Guts vertraglich verboten sein oder technisch unterbunden werden. In diesen Fällen ist es dem Monopolisten grundsätzlich möglich, verschiedene Outputeinheiten eines Guts zu unterschiedlichen Preisen verkaufen. Dieses Vorgehen wird als „Preisdiskriminierung" bezeichnet.[1574] Es kann zwischen drei Arten der Preisdiskriminierung unterschieden werden. Bei einer „Preisdiskriminierung ersten Grades" (auch: „perfekte" Preisdiskriminierung) verkauft der Monopolist das Gut an jeden Konsumenten jeweils zu dem Preis, der dessen individueller Zahlungsbereitschaft entspricht. Bei einer „Preisdiskriminierung zweiten Grades" hängt der Preis vom Verhalten des Konsumenten ab; so verkauft der Monopolist das Gut beispielsweise in unterschiedlichen Mengeneinheiten, wobei der Preis des Guts zwischen den einzelnen Mengeneinheiten differiert (insbesondere Mengenrabatte). Bei einer „Preisdiskriminierung dritten Grades" bietet der Monopolist das

---

1571 S. dazu oben Fn. 1553.
1572 Zum Begriff s. *Pindyck/Rubinfeld*, S. 8.
1573 *Posner*, Economic Analysis of Law, S. 305.
1574 *Varian*, S. 419 f.; *Pindyck/Rubinfeld*, S. 370 f.

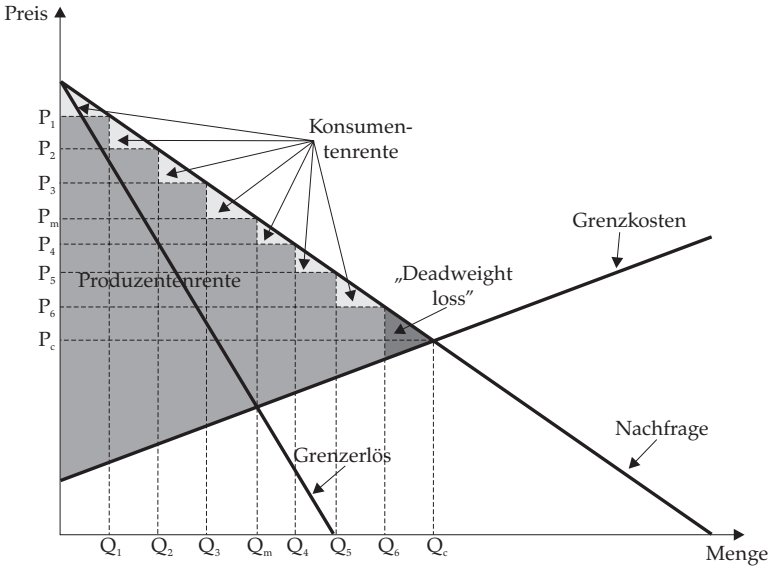


Abbildung 10: Angebot und Nachfrage bei monopolistischem Anbieter mit Preisdiskriminierung

Gut unterschiedlichen Personengruppen (Pensionär, Student, bestimmter Wohnort etc.) zu unterschiedlichen Preisen an.[1575]

Im Idealfall der Preisdiskriminierung ersten Grades verlangt der Monopolist von jedem Konsumenten genau den Preis, den der Konsument gerade noch zu zahlen bereit ist (also dessen Vorbehaltspreis). Im Gegensatz zum nicht-preisdiskriminierenden Monopolisten kann in einem solchen Fall auch das Marktsegment jener Konsumenten bedient werden, deren Vorbehaltspreis zwischen P_m und P_c liegt. Die Gefahr, daß dadurch der Gesamterlös des Monopolisten absinkt,[1576] ist durch die Preisdiskriminierung gebannt. Damit führt die Preisdiskriminierung zu einer starken Verringerung des „deadweight loss": In Abbildung 10 ist die dunkelgrau schraffierte Fläche sehr viel kleiner als in Abbildung 9 (S. 295).[1577]

1575 *Varian*, S. 420; *Pindyck/Rubinfeld*, S. 371 ff.; *Bailey*, S. 113.

1576 S. oben bei Fn. 1571.

1577 Bei einer perfekten Preisdiskriminierung wird der „deadweight loss" sogar ganz beseitigt. Auch fällt die Konsumentenrente weg; vielmehr wird die gesamte Rente vom Produzenten abgeschöpft, *Varian*, S. 420. Zur Veranschaulichung ist in Abbildung 10 jedoch eine geringe Konsumentenrente eingetragen. Dies entspricht eher der Realität. Auch der eingezeichnete „deadweight loss" wird in der Realität bestehen bleiben. Eine perfekte Preisdiskriminierung ist nämlich faktisch nicht durchführbar. Will ein Anbieter Preisdiskriminierung betreiben, so entstehen ihm dadurch Kosten: Er muß verschiedene Marktsegmente oder Kundengruppen identifizieren, denen das Gut zu unterschiedlichen Preisen angeboten wird. Er muß auch Maßnahmen ergreifen – sei es durch

Es zeigt sich, daß eine Preisdiskriminierung die Wohlfahrtsverluste des Monopols stark minimieren kann.[1578] Zwar führt die Preisdiskriminierung im Vergleich zum nicht-preisdiskriminierenden Monopolmarkt zu einer weiteren Umverteilung von der Konsumenten- zur Produzentenrente (vgl. die Abbildungen 9 und 10). Damit ist aber nichts über die Effizienz beider Marktmodelle gesagt.

Vielmehr ist ein Monopolmarkt mit Preisdiskriminierung im Gegensatz zum Monopolmarkt ohne Preisdiskriminierung Pareto-effizient:[1579] Bei einem diskriminierenden Monopolisten erhalten alle Konsumenten das Gut, deren Vorbehaltspreis über den Grenzkosten liegt. Wie beim Konkurrenzmarkt kommt es nachfolgend zu keinen Tauschhandlungen unter den Konsumenten. Zwar müssen die meisten Konsumenten im Monopolmarkt mit Preisdiskriminierung für das Gut mehr zahlen als im Konkurrenzmarkt, wodurch sich völlig unterschiedliche Einkommensverteilungen ergeben.[1580] Dies ändert jedoch nichts daran, daß ein Monopolmarkt mit Preisdiskriminierung genauso Pareto-effizient ist wie ein Konkurrenzmarkt.[1581] Der Wohlfahrtsverlust, der beim nicht-preisdiskriminierenden Monopolisten aus der suboptimalen Güterproduktion herrührt, wird beim preisdiskriminierenden Monopolisten beseitigt: Im Vergleich zum nicht-diskriminierenden Monopolisten kann das Gut von mehr Konsumenten erworben werden.[1582]

Technik, Verträge oder Marketingmaßnahmen –, um eine Arbitrage unter den verschiedenen Kunden zu vermeiden. Die Kosten der Etablierung von Preisdiskriminierung begrenzen die Granularität der Preisdiskriminierung. Es wird immer eine Anzahl von Konsumenten geben, deren Vorbehaltspreis für das Gut nur knapp über dessen Grenzkosten liegt. Diese Konsumenten werden das Gut in der Realität auch bei einer Preisdiskriminierung nicht erhalten, da die Kosten der Identifizierung dieser Konsumenten und der Verhinderung einer Arbitrage zwischen diesen und anderen Konsumenten höher sind als der Erlös bei Bedienung dieses Marktsegments. Für den Monopolisten lohnt es sich in der Realität auch bei einer Preisdiskriminierung nicht, dieses untere Preissegment zu bedienen. Daher wird er den Konsumenten mit einem Vorbehaltspreis zwischen P_c und P_6 (s. Abbildung 10) das Gut nicht verkaufen. Dadurch ergibt sich der eingezeichnete „deadweight loss" zwischen Q_6 und Q_c. Anders als beim theoretischen Ideal einer perfekten Preisdiskriminierung bleibt in der Realität bei einer Preisdiskriminierung immer ein gewisser „deadweight loss" bestehen. S. zum ganzen *Benkler*, 53 Vand. L. Rev. 2063, 2072 f. (2000).

[1578] Dies gilt allerdings nur, wenn die Kosten, um eine Preisdiskriminierung durchzuführen, nicht höher sind als die Wohlfahrtsverluste beim nichtdiskriminierenden Monopol.

[1579] Zu diesem Begriff s. oben Fn. 1553.

[1580] Diese Wohlfahrtsumverteilung zeigt sich an den unterschiedlich ausgestalteten Konsumenten- und Produzentenrenten in den Abbildungen 8 und 10.

[1581] *Varian*, S. 16, 421; *Boyle*, 53 Vand. L. Rev. 2007, 2025 (2000).

[1582] *Fisher*, 73 Chi.-Kent L. Rev. 1203, 1239 (1998). Diese allgemeine Aussage trifft jedoch nur für den idealisierten Fall der perfekten Preisdiskriminierung zu. Beispielsweise hängt bei einer Preisdiskriminierung dritten Grades die Frage, ob dadurch der Produktionsoutput erhöht wird, von der Ausgestaltung der einzelnen Gruppen und deren individuellen Präferenzen ab. Eine allgemeine Aussage ist dabei nicht mehr mög-

b) Preisdiskriminierung bei DRM-Systemen

Diese Überlegungen lassen sich auf DRM-Systeme übertragen.[1583] Wie beim Monopol entsteht beim Schutz durch DRM-Systeme ein „deadweight loss". Dieser Effizienzverlust rührt daher, daß der DRM-Schutz dem Inhalteanbieter ermöglicht, die Preise für seinen digitalen Inhalt über deren Grenzkosten zu setzen; dies führt zu einer Unternutzung des digitalen Inhalts.[1584] Wie beim Monopol könnte eine Preisdiskriminierung diesen Effizienzverlust beseitigen oder zumindest vermindern.[1585] Gleichzeitig würde sie zu einer Erhöhung der Produzentenrente führen.[1586] Dies hätte in DRM-Systemen eine Verstärkung des Anreizes zur Informationsproduktion zur Folge und wäre insofern mit einer Verstärkung des Urheberschutzes vergleichbar.[1587] Unter diesen Gesichtspunkten scheinen Ansätze begrüßenswert, die in DRM-Systemen und im herkömmlichen Urheberrecht eine Preisdiskriminierung umsetzen.[1588]

---

lich, vielmehr handelt es sich um eine empirische Frage; s. *Posner*, Economic Analysis of Law, S. 306. Auch wenn die idealisierte perfekte Preisdiskriminierung aus Effizienzgesichtspunkten zu bevorzugen ist, kann nicht gesagt werden, daß die Preisdiskriminierung beim Monopolisten immer zu befürworten sei. Dies hängt insbesondere mit den völlig anderen Wohlfahrtsverteilungen beim preisdiskriminierenden Monopolisten zusammen. Weiterhin ist von diesen theoretischen Modellen die geltende Rechtslage zu unterscheiden. Nach geltendem Kartellrecht kann eine Preisdiskriminierung nach § 20 Abs. 1 GWB unzulässig sein, da sie beispielsweise von marktmächtigen Lieferanten gezielt als Kampfmittel gegen schwächere Konkurrenten und Newcomer eingesetzt werden kann; s. dazu *Markert* in: Immenga/Mestmäcker (Hrsg.), GWB-Kommentar, § 20 Rdnr. 9, 176 ff.

[1583] S. dazu insbesondere den einflußreichen Beitrag von *Fisher*, 73 Chi.-Kent L. Rev. 1203, 1234 ff. (1998); s. weiterhin *Bell*, 76 N.C. L. Rev. 557, 589 Fn. 142 (1998); *Friedman*, 13 Berkeley Tech. L. J. 1151, 1168 ff. (1998); *O'Rourke*, 12 Berkeley Tech. L. J. 53, 62, 70 f. (1997); *Meurer*, 45 Buff. L. Rev. 845 ff. (1997); *Burk*, 21 Cardozo L. Rev. 121, 169 f. (1999); *Benkler*, 53 Vand. L. Rev. 2063, 2071 ff. (2000). Der Beitrag von *Fisher* hat in den USA zu einer kontroversen Diskussion über grundlegende Fragen der ökonomischen Analyse des Urheberrechts geführt, s. nur *Gordon*, 73 Chi.-Kent L. Rev. 1367 ff. (1998); *Benkler*, 53 Vand. L. Rev. 2063 ff. (2000); *Boyle*, 53 Vand. L. Rev. 2007 ff. (2000); *Cohen*, 53 Vand. L. Rev. 1799 ff. (2000). Eine grundlegende Analyse der Auswirkungen der Preisdiskriminierung auf die Produktion öffentlicher Güter findet sich bei *Demsetz*, 13 J. L. & Econ. 293 ff. (1970).

[1584] S. dazu oben Teil 3, A III 2 c bb.

[1585] S. a. *Gordon*, 17 U. Dayton L. Rev. 853, 855 Fn. 9 (1992); *dies.*, 41 Stan. L. Rev. 1343, 1350 Fn. 23 (1989).

[1586] S. oben bei Fn. 1580.

[1587] *Fisher*, 73 Chi.-Kent L. Rev. 1203, 1240 (1998); *Meurer*, 45 Buff. L. Rev. 845, 876 ff. (1997). *Fisher* begrüßt diese Entwicklung und empfiehlt, aufgrund der Effizienzsteigerungen auf diesen Schutzmechanismus umzusteigen, s. *Fisher*, a. a. O., S. 1234 ff. Eine Preisdiskriminierung kann nicht nur den „deadweight loss" von DRM-Systemen, sondern auch den „deadweight loss" des herkömmlichen Urheberrechts beseitigen.

[1588] Die vorstehende Analyse läßt sich auch im Bereich des Urheberrechts anwenden. Schon heute wird im herkömmlichen urheberrechtlichen Bereich die Preisdiskriminierung eingesetzt: Wissenschaftliche Zeitschriften werden Bibliotheken oft zu weit höhe-

In den USA waren diese Effizienzüberlegungen bezüglich einer Preisdiskriminierung im Umfeld von DRM-Systemen eine der tragenden Gründe für die Entscheidung des 7th Circuit Court of Appeals in Sachen ProCD, Inc. v. Zeidenberg (dazu unten aa). Fraglich erscheint, ob in DRM-Systemen eine Preisdiskriminierung praktisch durchführbar ist. Dafür muß es dem Inhalteanbieter möglich sein, unterschiedliche Marktsegmente zu identifizieren und Arbitrage-Geschäfte zu verhindern (dazu unten bb).

aa) ProCD, Inc. v. Zeidenberg

Die Auswirkungen der Preisdiskriminierung auf den urheberrechtlichen Bereich waren Gegenstand der U.S.-amerikanischen zweitinstanzlichen Entscheidung in Sachen ProCD, Inc. v. Zeidenberg.[1589] Das Unternehmen ProCD, Inc., bot damals mehrere CD-ROMs an, die ein elektronisches Telefonbuch der Vereinigten Staaten enthielten. ProCD hatte mit einem finanziellen Aufwand von etwa 10 Millionen $ über 95 Millionen Einträge aus 3000 Telefonbüchern zusammengetragen. Der Beklagte Zeidenberg hatte die CD-ROMs 1994 erworben, gründete ein Unternehmen, kopierte die Telefondaten auf einen WWW-Server, schrieb eine eigene Suchsoftware und stellte die Telefondaten und die Suchsoftware der Öffentlichkeit über das Internet zur Verfügung.[1590] ProCD fürchtete um den Absatz seiner CD-ROMs und ging gegen Zeidenberg vor.[1591]

ProCD konnte sich allerdings nicht auf eine Verletzung urheberrechtlicher Verwertungsrechte berufen. Der U.S. Supreme Court hatte 1991 in einer grundlegenden Entscheidung – entgegen der langjährigen Entscheidungspraxis vieler unterinstanzlicher Gerichte – die sogenannte „sweat of

ren Abonnementpreisen angeboten als Privatpersonen. Das Angebot von Büchern in gebundenen und Paperback-Ausgaben und die zeitlich gestaffelte Verwertung von Filmen in Kinos, Videokassetten, Fernsehen etc. sind weitere Formen der Preisdiskriminierung, *Landes/Posner*, 18 J. Legal Stud. 325, 328 (1989); zur Preisdiskriminierung im Filmbereich s. *Waterman* in: Gerbard (Hrsg.), S. 181, 185 ff. Zum Argument, daß das Urheberrechtsgesetz selbst schon eine Art Preisdiskriminierung ermögliche, s. a. *Gordon*, 73 Chi.-Kent L. Rev. 1367, 1370 ff. (1998). S. weiterhin umfassend *Meurer*, Copyright Law and Price Discrimination.

[1589] ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996). Diese Entscheidung war schon im Zusammenhang mit der zivilrechtlichen Wirksamkeit von „shrinkwrap licenses" erwähnt worden, s. oben Teil 2, B II 3 a aa. Daneben wirft die Entscheidung unter dem Gesichtspunkt der „federal preemption" Fragen beim Verhältnis zwischen „copyright law" und „contract law" auf, s. dazu unten Teil 4, B III 1 b.

[1590] Aus der erst- und zweitinstanzlichen Entscheidung geht nicht klar hervor, ob Zeidenberg die Datenbank im Internet kostenlos oder nur gegen Entgelt anbot. Während die erstinstanzliche Entscheidung schreibt, der Zugriff sei kostenlos gewesen – ProCD, Inc. v. Zeidenberg, 908 F. Supp. 640, 646 (W. D. Wis. 1996) –, schreibt die zweitinstanzliche Entscheidung, der Benutzer hätte ein Entgelt zahlen müssen – ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1450 (7th Cir. 1996).

[1591] Eine ausführliche Darstellung des Sachverhalts findet sich im erstinstanzlichen Urteil ProCD, Inc. v. Zeidenberg, 908 F.Supp. 640, 643 ff. (W.D.Wis. 1996); s. a. ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996).

the brow"-Doktrin abgelehnt und entschieden, daß die bloße Ansammlung von Daten mangels eines Mindestmaßes an Kreativität keinen urheberrechtlichen Schutz genieße.[1592] Damit genoß die Datensammlung von ProCD keinen urheberrechtlichen Schutz.[1593] Zwar wird in den USA seit vielen Jahren über Gesetzesvorschläge zur Schaffung eines urheberrechtlichen Datenbankschutzes diskutiert.[1594] Ein entsprechendes Gesetz wurde aber bis heute nicht erlassen.

Zum Schutz seiner Datensammlung mußte ProCD daher auf einen anderen Schutzmechanismus zurückgreifen: Nutzungsverträge.[1595] ProCD legte den verkauften CD-ROMs einen Schutzhüllenvertrag bei, in dem bestimmte Nutzungsbedingungen abgedruckt waren. Weitere Nutzungsbedingungen wurden vor der Nutzung der Software auf dem Bildschirm angezeigt.[1596] Danach war der Nutzer der CD-ROMs nur berechtigt, die Daten für persönliche Zwecke zu kopieren. Eine Weitergabe der Daten an Dritte war untersagt. Ausdrücklich wurde dem Nutzer verboten, die Daten ganz oder teilweise in Netzwerkumgebungen anzubieten.[1597] ProCD verkaufte diese Fassung der CD-ROMs zu einem Preis von $ 150,–. Daneben bot ProCD die gleichen Daten für kommerzielle Kunden zu einem höheren Preis an. In dieser Fassung fanden sich keinerlei Nutzungsbeschränkungen.[1598]

In dem Rechtsstreit war nun fraglich, ob die Nutzungsbeschränkungen, denen Zeidenberg in dem Schutzhüllenvertrag zugestimmt hatte, wirk-

[1592] Feist Publications, Inc. v. Rural Telephone Service Co., Inc., 499 U.S. 340 (1991) = GRUR Int. 1991, 933 m. Anm. *Hoebbel*.

[1593] ProCD, Inc. v. Zeidenberg, 908 F.Supp. 640, 647 (W.D.Wis. 1996). Etwas zurückhaltender die zweitinstanzliche Entscheidung ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996).

[1594] S. nur *Gaster*, CR 1999, 669 ff.; *Benkler*, 15 Berkeley Tech. L. J. 535 ff. (2000); *Reichman/Samuelson*, 50 Vand. L. Rev. 51 ff. (1997).

[1595] In diesem Fall ging es also nicht um ein vollständiges DRM-System, sondern vielmehr nur um einen Schutz durch Nutzungsverzträge. Da dieser Schutzmechanismus der Teil eines umfassenderen DRM-Systems sein kann, sind die Überlegungen der Entscheidung aber auch auf DRM-Systeme anwendbar. Ein ähnliches Vorgehen ließ sich früher in Deutschland beobachten, als der BGH sehr hohe Anforderungen an die urheberrechtliche Schutzfähigkeit von Computersoftware stellte. Damals wichen viele Softwarehersteller auf vertragliche Schutzmechanismen aus, s. *Marly*, Softwareüberlassungsverträge, Rdnr. 114 ff., 914 ff., 1034; *Hoeren*, Rdnr. 64 f. *Lehmann*, NJW 1993, 1822 f., spricht plastisch von einer „vertraglichen Armierung" und einem „feingesponnenen Vertragskokon", das die Softwarehersteller um die Software herumlegten. Seit der UrhG-Novelle 1993 unterliegen fast alle Computerprogramme dem Schutz durch das Urheberrecht, so daß sich das Problem nicht mehr stellt.

[1596] Die zivilrechtliche Wirksamkeit dieser vertraglichen Vereinbarungen wurde in zweiter Instanz bejaht; s. dazu oben Teil 2, B II 3 a aa.

[1597] ProCD, Inc. v. Zeidenberg, 908 F.Supp. 640, 644 f. (W.D.Wis. 1996).

[1598] Schließlich bot ProCD die Datenbank im Online-Dienst „America Online" für eine stündliche Nutzungsgebühr von $ 3,- an. Diese Fassung war wiederum auf den privaten Sektor zugeschnitten; s. ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996).

sam waren und ProCD somit die Veröffentlichung der Telefondaten im Internet vertraglich untersagen konnte.[1599] Das Gericht zweiter Instanz stützte sich in seiner Entscheidung stark auf eine ökonomische Analyse des Sachverhalts. Der vorsitzende Richter Judge *Easterbrook* – ein prominenter Anhänger der „Chicago School" – argumentierte, wenn ProCD die CD-ROMs nur zu einem einheitlichen Preis anbieten würde, müßte dieser Preis deutlich höher als $ 150,– sein, um die Kosten zu decken.[1600] Dann würden aber sowohl Privat- als auch Geschäftskunden schlechter dastehen als bei der vorliegenden Preisdiskriminierung: Die Privatkunden würden das Produkt wegen des höheren Preises nicht mehr erwerben. Die Geschäftskunden müßten für das gleiche Produkt einen deutlich höheren Preis zahlen. Dieser Preis fiele um so höher aus, da nun für den Hersteller die Einnahmen aus dem privaten Käufersektor bei gleichbleibenden Produktionskosten wegfielen. Durch die Preisdiskriminierung könne ProCD die CD-ROMS den Privatkunden zu einem niedrigeren Preis anbieten. Dadurch würden die CD-ROMS weiter verbreitet, als wenn man die Preisdiskriminierung verhindern würde.[1601] Eine Preisdiskriminierung, wie sie ProCD betreibe, sei daher im Interesse aller Käufer, die dadurch entweder das Produkt überhaupt erst oder zumindest zu einem günstigeren Preis erwerben könnten.[1602]

Um eine solche Preisdiskriminierung zu ermöglichen, müsse ProCD jedoch die Möglichkeit haben, Arbitrage-Geschäfte[1603] zu unterbinden. Solche Geschäfte verhindere ProCD, indem sie Privatkunden eine Weitergabe der Daten vertraglich verbiete.[1604] Die Nutzungsbeschränkung im Schutzhüllenvertrag sei damit notwendig, um eine Preisdiskriminierung überhaupt durchführen zu können. Insgesamt sei die Preisdiskriminierung von ProCD und die dazu notwendige vertragliche Beschränkung der Nutzungsmöglichkeiten bei Privatkunden zu begrüßen.[1605]

[1599] In diesem Zusammenhang ging es nicht um die allgemeine zivilrechtliche Wirksamkeit von „shrinkwrap licenses". Dies hatte die Gerichtsentscheidung schon in einem früheren Abschnitt bejaht, s. oben Teil 2, B II 3 a aa. Vielmehr ging es um die Frage, ob aus urheberrechtlicher Sicht solche vertraglichen Nutzungsbeschränkungen wirksam sind. Nach U.S.-amerikanischem Recht kann dies unter dem Gesichtspunkt des „preemption doctrine" fraglich sein; s. dazu unten Teil 4, B III 1.

[1600] *Easterbrook* begründet seine These, ein einheitlicher Preis müsse *deutlich* über $ 150,- liegen, mit der hohen Nachfrageelastizität der CD-ROMs im Privatkunden-Bereich, s. ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996).

[1601] ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1455 (7th Cir. 1996).

[1602] ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996).

[1603] Zu diesem Begriff s. oben bei Fn. 1572.

[1604] ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1450 (7th Cir. 1996).

[1605] In deutschen Gerichtsurteilen wird die Problemdimension regelmäßig völlig verkannt. So läßt sich beispielsweise der Vertrieb von Standard-Software in unterschiedlichen Versionen (sog. OEM- und Vollversionen) unter dem Gesichtspunkt der Preisdiskriminierung erklären.Obwohl sich der BGH kürzlich mit der Zulässigkeit von OEM-Softwarelizenzen zu beschäftigen hatte (näher bei Fn. 2005), blendete er diese

bb) Möglichkeiten von DRM-Systemen

Wenn eine Preisdiskriminierung in DRM-Systemen aus rechtsökonomischer Sicht wünschenswert erscheint, weil durch sie der „deadweight loss" eines DRM-Systems verringert werden kann, stellt sich die Frage, ob eine solche in DRM-Systemen überhaupt möglich ist. Dafür müssen grundsätzlich zwei Voraussetzungen erfüllt sein. Einerseits muß es dem Anbieter möglich sein, zwischen unterschiedlichen Konsumenten oder zumindest zwischen unterschiedlichen Konsumentengruppen zu unterscheiden, um diesen unterschiedliche Preise in Rechnung stellen zu können (*Identifizierungs-Problem*). Andererseits muß es dem Anbieter möglich sein zu verhindern, daß die Konsumenten die Güter später unbegrenzt untereinander austauschen können (*Arbitrage-Problem*). Im folgenden soll gezeigt werden, daß beide Voraussetzungen durch DRM-Systeme in vollem und teilweise ungekanntem Ausmaß erfüllt werden.

Bezüglich des *Identifizierungs-Problems* ist zu beachten, daß Anbieter in DRM-Systemen genaue Informationen über die Nutzungsgewohnheiten der einzelnen Konsumenten erhalten können. Diese Nutzungsprofile können zur Grundlage einer Preisdiskriminierung gemacht werden. So können digitale Inhalte für unterschiedliche Nutzungsintensitäten zu unterschiedlichen Preisen angeboten werden: Hört ein bestimmter Nutzer ein Musikstück insgesamt zwei Mal an, so wird ihm ein niedrigerer Preis berechnet als einem Nutzer, der das Stück fünf Mal pro Tag anhört.[1606] Nutzungsprofile können auch verwendet werden, um das Angebot individuell auf den jeweiligen Nutzer zuzuschneiden.[1607] Personalisierte Informationsangebote werden immer wichtiger.[1608] Durch die digitale Form von Inhalten ist es vergleichsweise einfach, die Inhalte in einzelnen Eigenschaften (Leistungsumfang, Qualität, Nutzungsbeschränkungen, Aktualität, Erscheinungsdatum,[1609] Präsentationsform und ähnliches) zu variie-

ökonomischen Überlegungen völlig aus und erwähnte in seiner Entscheidung gar nicht die potentiellen Vorteile einer Preisdiskriminierung, die auf einer Spaltung der Vertriebswege aufbauen kann. Vielmehr meint er, es sei „von vornherein nicht ersichtlich", warum Microsoft Softwareprogramme an bestimmte Kunden als sog. „OEM-Version" zu günstigeren Preisen verkaufe als an andere Kunden als (teurere) Vollversion; s. BGH, CR, 2000, 651, 654.

[1606] Vgl. *Meurer*, 45 Buff. L. Rev. 845, 879 (1997). Dabei ist allerdings fraglich, ob hier tatsächlich eine Preisdiskriminierung vorliegt, s. unten Teil 3, B I 1 b.

[1607] Dies kann bis zum sog. „one-to-one marketing" reichen, *Bakos*, 41 (8) Comm. ACM, 35, 37 (1998). S. weiterhin *Shapiro/Varian*, S. 33 ff.; *Smith/Bailey/Brynjolfsson* in: Brynjolfsson/Kahin (Hrsg.), S. 99, 113; *Bakos/Brynjolfsson* in: Kahin/Varian (Hrsg.), S. 114 ff.; *Burk*, 21 Cardozo L. Rev. 121, 169 (1999); *Bailey*, S. 115 ff. Zu entsprechenden Ansätzen im derzeitigen Internet s. *Chang/Kannan/Whinston*, 4 Intern. J. Electr. Comm. 85 ff. (1999).

[1608] *Shapiro/Varian*, S. 6 ff.; *European Communication Council* (Hrsg.), S. 18.

[1609] Dies läßt sich auch im Buchsektor beobachten, wo gebundene Ausgaben für Kunden mit einem hohen Vorbehaltspreis regelmäßig früher auf dem Markt erscheinen als Paperback-Ausgaben für Kunden mit einem niedrigeren Vorbehaltspreis.

ren und unterschiedlich zu vermarkten.[1610] Auch können digitale Inhalte in unterschiedlichen Qualitätsstufen angeboten werden: DRM-Systeme unterstützen eine solche Angebotsdifferenzierung durch Verfahren, die eine teilweise Verschlüsselung der Inhalte in unterschiedlichen Qualitätsstufen ermöglichen („multiresolution encryption").[1611]

Auf dieser Produktdifferenzierung, die auch als „versioning" bezeichnet wird,[1612] kann eine Preisdiskriminierung aufbauen: Die unterschiedlichen Versionen eines digitalen Inhalts bedienen verschiedene Marktsegmente zu unterschiedlichen Preisen.[1613] Der Konsument wählt jene Versions-Preis-Kombination, die seinen individuellen Präferenzen am besten entspricht. Dies hat für den Anbieter den Vorteil, daß er die einzelnen Konsumenten nicht im voraus bestimmten Marktsegmenten zuordnen muß.[1614] Vielmehr wählen die Konsumenten selbst das gewünschte Marktsegment aus.[1615] Man kann dies auch als „Selbstsegmentierung" des Markts bezeichnen.[1616]

[1610] *Shapiro/Varian*, S. 32 f., 55 ff.; *Varian* in: Kahin/Varian (Hrsg.), S. 190 ff.; *European Communication Council* (Hrsg.), S. 19, 187 ff.; *Bakos*, 41 (8) Comm. ACM, 35, 37 ff. (August 1998).

[1611] S. dazu oben bei Fn. 1391 ff. und Teil 1, C I 1 b cc. Schon heute läßt sich eine Preisdiskriminierung beobachten, die auf einer solchen Qualitätsdifferenzierung aufbaut: Videofilme werden in in hoher Qualität auf digitalen DVDs und in schlechterer Qualität auf analogen Videokassetten angeboten. DVDs werden regelmäßig teurer angeboten als die Videokassetten, obwohl ihre Herstellungs- und Verpackungskosten billiger sind; vgl. *Waterman* in: Gerbarg (Hrsg.), S. 181, 191 f. Bei Computersoftware gibt es oft eine billige Version mit eingeschränktem Funktionsumfang und eine teurere professionelle Version mit Zusatzfunktionen.

[1612] S. nur *Shapiro/Varian*, S. 53 ff.

[1613] *European Communication Council* (Hrsg.), S. 19; *Shapiro/Varian*, S. 37 ff.; *Varian* in: Kahin/Varian (Hrsg.), S. 190; *Bakos*, 41 (8) Comm. ACM, 35, 39 f. (August 1998); *Messerschmitt/Szyperski*, S. 34 f.; *Detering*, S. 159; s. a. *Meurer*, 45 Buff. L. Rev. 845, 869 (1997): „Price discrimination means that consumers of an identical product are charged different prices by the same seller, or that consumers of similar products made by the same seller are charged a price differential unrelated to cost."

[1614] Dies kann für den Anbieter schwierig sein, wenn ihm keine ausreichenden Informationen über den einzelnen Konsumenten zur Verfügung stehen.

[1615] *Varian* in: Kahin/Varian (Hrsg.), S. 190, 193.

[1616] So *Detering*, S. 157; *Varian*, S. 423; vgl. weiterhin *Meurer*, 45 Buff. L. Rev. 845, 872 (1997). Diese Vorgehensweise läßt sich als Preisdiskriminierung zweiten Grades begreifen, *Shapiro/Varian*, S. 39, 53 ff. Zwar geht es im Hauptfall der Preisdiskriminierung zweiten Grades um Mengenrabatte u. ä. Grundsätzliches Charakteristikum einer Preisdiskriminierung zweiten Grades ist jedoch, daß nicht der Anbieter den Konsumenten einem bestimmten Marktsegment zuweist, sondern daß der Konsument unter mehreren Preis-Produkt-Kombinationen auswählt und sich damit selbst einem Marktsegment zuweist. Daneben kann die Veränderung der Qualität eines Produkts auch als Veränderung der Menge Produkts interpretiert werden, s. *Varian*, S. 424; *Detering*, S. 157 ff.; *Meurer*, 45 Buff. L. Rev. 845, 872 f. (1997). Bis zu einem gewissen Maß ist in DRM-Systemen auch eine Preisdiskriminierung ersten Grades möglich: Mit Hilfe von Nutzungsprofilen könnte der Inhalteanbieter sein Angebot auf jeden einzelnen Nutzer individuell zuschneiden und individuelle Preise festsetzen.

Bezüglich des *Arbitrage-Problems* ist zwischen zwei Problemlagen zu unterscheiden: Einerseits muß der Anbieter verhindern, daß ein Konsument, dem der Monopolist einen niedrigen Preis berechnet, das Gut kauft und an einen anderen Konsumenten weiterverkauft, dem der Monopolist selbst einen höheren Preis berechnen würde (klassisches Arbitrage-Geschäft). Technische Schutzmaßnahmen können das Austauschen digitaler Inhalte in DRM-Systemen erschweren und damit Arbitrage-Geschäfte verhindern.[1617] Es sei nur an Kopierschutzmaßnahmen oder an die kryptographische Bindung digitaler Inhalte an ein bestimmtes Speichermedium erinnert.[1618] Auch können dem Nutzer Arbitrage-Geschäfte in Nutzungsverträgen untersagt werden.[1619]

Andererseits ist ein spezielles Problem des „versioning" digitaler Inhalte zu beachten. Bietet ein Anbieter in einem DRM-System einen digitalen Inhalt in unterschiedlichen Versionen an, so unterscheiden sich die Versionen in technischer Sicht regelmäßig nur minimal.[1620] Es muß daher

---

[1617] *Meurer*, 45 Buff. L. Rev. 845, 879 (1997); *Boyle*, 53 Vand. L. Rev. 2007, 2025 (2000).

[1618] Zu Kopierschutzmaßnahmen s. oben Teil 1, C I 2, zur kryptographischen Bindung an ein bestimmtes Speichermedium im Rahmen von CPRM s. oben Teil 1, D II 4.

[1619] *Meurer*, 45 Buff. L. Rev. 845, 874 ff. (1997). Auch der Schutzhüllenvertrag, welcher der ProCD-Entscheidung zugrundelag, enthielt eine solche Klausel, s. oben bei Fn. 1597. Mitunter setzt das Urheberrecht den Bemühungen des Inhalteanbieters, Arbitrage-Geschäfte zu verhindern, eine Grenze. So kann ein Urheber wegen des Erschöpfungsgrundsatzes den Weiterverkauf eines einmal in den Verkehr gebrachten Werkexemplars nicht verhindern. Durch den Erschöpfungsgrundsatz werden Arbitrage-Geschäfte unter den Konsumenten möglich, *Cohen*, 53 Vand. L. Rev. 1799, 1804 f. (2000). Im deutschen und europäischen Urheberrecht entspricht es herrschender Meinung, daß der Erschöpfungsgrundsatz im Online-Bereich nicht greift, s. dazu *Loewenheim* in: Schricker (Hrsg.), UrhG-Kommentar, § 17 Rdnr. 37; *Bechtold*, Multimedia und das Urheberrecht, S. 18 f.; a. A. *Koehler*. Im U.S.-amerikanischen Urheberrecht ist umstritten, ob die „first sale doctrine" im Online-Bereich anwendbar ist, s. nur *U.S. Department of Commerce/National Telecommunications and Information Administration; R. T. Nimmer*, § 4.08[2][a], S. 4–30 f., S. S4–51 f.; *Nimmer/Brown/Frischling*, 87 Cal. L. Rev. 17, 39 f. (1999).

[1620] In einem Sachverhalt, welcher der Entscheidung des LG Düsseldorf, CR 1996, 737, zugrundelag, bot ein Softwarehersteller sein Computerprogramm in sechs Varianten an, die sich jeweils in ihrer Leistungsfähigkeit unterschieden. Das Programm war durch einen Dongle technisch geschützt. Faktisch erhielt aber jeder Konsument unabhängig davon, welche Variante er wählte, das Vollprogramm. Die Varianten wurden nur mit unterschiedlichen Dongles ausgeliefert, die die jeweiligen Programmteile sperrte, zu deren Nutzung der Konsument nicht berechtigt war. Um dieses Geschäftsmodell nicht zu gefährden, muß der Softwarehersteller verhindern können, daß der Konsument durch eine Manipulation des Dongles eine hochwertige Version des Computerprogramms nutzen kann, obwohl er nur für eine leistungsschwächere Version bezahlt hat. In anderen Bereichen lassen sich ähnliche Problem beobachten. So bot IBM lange Zeit einen Laserdrucker in zwei Versionen an: Eine schnelle Version mit einer Druckgeschwindigkeit von 10 Seiten pro Minute sowie eine langsame Version mit einer Druckgeschwindigkeit von 5 Seiten pro Minute. Technisch unterschieden sich beide Versionen nur dadurch, daß in der langsameren Version ein Chip eingefügt wurde, der

verhindert werden, daß ein Konsument eine kostengünstige Version des Inhalts erwirbt, diese Version manipuliert und dadurch eine hochwertige, teurere Version erhält, ohne das entsprechende Entgelt gezahlt zu haben. Auch hier könnten technische Schutzmaßnahmen eingesetzt werden, die solche Manipulationen verhindern oder zumindest erschweren. Regelmäßig werden dem Konsumenten solche Manipulationen zusätzlich in Nutzungsverträgen untersagt.[1621]

Es zeigt sich, daß DRM-Systeme umfangreiche Möglichkeiten bieten, um das beschriebene Identifizierungs- und das Arbitrage-Problem zu lösen. Damit eignen sie sich in besonderem Maße für eine Preisdiskriminierung. Auch die sonstigen Parameter von DRM-Systemen und des E-Commerce begünstigen ein solches Geschäftsmodell. Bei einer Preisdiskriminierung muß der Anbieter relativ häufig die Preise seiner angebotenen Güter ändern. Preisänderungen verursachen für den Anbieter Kosten, die auch als „Menükosten" bezeichnet werden. Im herkömmlichen Handel bestehen Menükosten insbesondere in den Kosten, die Güter mit neuen Preisauszeichnungen zu versehen.[1622] Je höher die Menükosten sind, desto weniger lohnt es sich für Anbieter, häufige oder kleine Preisänderungen durchzuführen. Hohe Menükosten beschränken damit die Möglichkeit der Preisdiskriminierung.[1623] Im Vergleich zum herkömmlichen Handel sind Menükosten im Internet und in DRM-Systemen viel geringer: Eine Preisänderung besteht regelmäßig nur noch in der bloßen Änderung eines Eintrags in einer zentralen Datenbank.[1624] In DRM-Systemen können Preisänderungen vollautomatisch und dyna-

---

den Drucker künstlich verlangsamte. Damit wollte IBM sein Konzept der Produktdifferenzierung und Preisdiskriminierung aufrechterhalten. Zu diesem Zweck muß aber verhindert werden, daß der Nutzer nach dem Erwerb der langsameren Version den Chip problemlos entfernen kann. S. zum ganzen *Shapiro/Varian*, S. 59, 64; *Varian* in: Kahin/Varian (Hrsg.), S. 190, 194 ff.

[1621] *Meurer*, 45 Buff. L. Rev. 845, 874 ff. (1997). Sind die Kosten der Manipulation höher als die Preisdifferenz zwischen den beiden Versionen, so lohnt sich die Manipulation für den Käufer auch nicht.

[1622] Daneben fallen unter die Menükosten auch die Kosten der Neuerstellung von Katalogen, Preislisten u. ä. Nach einer Untersuchung in den USA betragen die Menükosten für eine Preisänderung in einem U.S.-amerikanischen Supermarkt im Durchschnitt $ 0,52. In der Summe machen die Menükosten 35,2% der Nettogewinnspanne eines Supermarkts aus, *Levy/Bergen/Dutta/Venable*, 112 Quarterly Journal of Economics 791, 821, 831 (1997).

[1623] Vgl. *Smith/Bailey/Brynjolfsson* in: Brynjolfsson/Kahin (Hrsg.), S. 99, 103.

[1624] *Bailey*, S. 115; *Smith/Bailey/Brynjolfsson* in: Brynjolfsson/Kahin (Hrsg.), S. 99, 103; *Brynjolfsson/Smith*, 46 Management Science 563, 572 (2000). Daraus resultiert auch die Experimentierfreudigkeit von Online-Anbietern mit neuartigen Preismodellen. Im Herbst 2000 bot der Online-Buchhändler Amazon.com für mehrere Wochen unterschiedlichen Kunden DVDs zu verschiedenen Preisen an, um herauszufinden, welche Auswirkungen der Preis auf die Nachfrage hat.

misch durchgeführt werden.[1625] Es läßt sich auch empirisch belegen, daß Anbieter im Internet häufigere und kleinere Preisänderungen durchführen als der herkömmliche Handel; dies kann auf niedrigere Menükosten zurückgeführt werden.[1626] Da in DRM-Systemen Menükosten sinken, wird die Einführung einer Preisdiskriminierung erleichtert.

c) Ergebnis

Mit Hilfe einer Preisdiskriminierung kann der „deadweight loss" verringert werden, der bei DRM-Systemen – ähnlich wie beim Urheberrecht und beim Monopol – entsteht. Dies erhöht die Allokationseffizienz von DRM-Systemen. Eine Preisdiskriminierung ist in DRM-Systemen nicht nur wünschenswert, sondern auch möglich. Die technischen und vertraglichen Schutzmechanismen von DRM-Systemen bieten dafür umfassende Möglichkeiten.[1627] Mit diesen Schutzmechanismen können Arbitrage-Geschäfte erschwert oder gar verhindert werden. Je größer die Freiheit für die Anbieter ist, sich durch Technik und Vertrag zu schützen, desto größer sind die Möglichkeiten der Preisdiskriminierung.[1628] Am Beispiel der sogenannten „multiresolution encryption" zeigt sich, in welcher Perfektion die ineinandergreifenden Schutzmechanismen von DRM-Systemen das „versioning" digitaler Inhalte und eine darauf aufbauende Preisdiskriminierung ermöglichen.[1629] In DRM-Systemen kann die Preisdiskriminierung automatisiert werden und nahezu in Echtzeit auf Veränderungen der Nachfrage oder des Angebots reagieren.[1630] Ein preisdiskriminierendes DRM-System scheint das Beste aus zwei Bereichen – Anreizwirkung und Allokationseffizienz – zu vereinen.[1631]

[1625] Vgl. *Bailey*, S. 115; *Smith/Bailey/Brynjolfsson* in: Brynjolfsson/Kahin (Hrsg.), S. 99, 113.

[1626] *Bailey* kommt bei einem Vergleich für Bücher, CDs und Software in den Jahren 1997 und 1998 zu dem Ergebnis, daß Online-Händler ihre Preise im Vergleich zu herkömmlichen Händler mehr als doppelt so oft ändern, s. *Bailey*, S. 93 ff. *Brynjolfsson/Smith*, 46 Management Science 563, 572 f. (2000), kommen bei einem ähnlichen Vergleich für Bücher und CDs von Februar 1998 bis Mai 1999 zu dem Ergebnis, daß die Höhe der Preisänderung bei Internet-Händlern um bis zum Faktor 100 kleiner sind als bei herkömmlichen Händlern.

[1627] Vgl. *Meurer*, 45 Buff. L. Rev. 845, 872 ff. (1997); *Netanel*, 106 Yale L. J. 283, 293 Fn. 30 (1996).

[1628] *Boyle*, 53 Vand. L. Rev. 2007, 2024 f. (2000). Sind beispielsweise urheberrechtliche Schrankenbestimmungen vertraglich abdingbar, kann dieser Bereich ebenfalls zur Produktdifferenzierung verwendet werden, *Cohen*, 53 Vand. L. Rev. 1799, 1805 (2000).

[1629] S. dazu bei Fn. 1391 ff.

[1630] *Shapiro/Varian*, S. 42.

[1631] Auf die Kritik an dieser These wird unten, Teil 3, B I 1 b, eingegangen. S. weiterhin unten Teil 3, B I 3.

4. Niedrigere Transaktionskosten

a) Allgemeines

DRM-Systeme ermöglichen einen vollautomatischen Vertrieb digitaler Inhalte. Dadurch könnten sogenannte „Transaktionskosten“[1632] deutlich gesenkt werden, was aus ökonomischer Sicht unter vielen Aspekten begrüßenswert erscheint. Es lassen sich unterschiedliche Arten von Transaktionskosten unterscheiden: Such- und Informationskosten, Verhandlungs- und Entscheidungskosten sowie Überwachungs- und Durchsetzungskosten.[1633] *Suchkosten* entstehen, wenn man nach einem geeigneten Partner für eine Markttransaktion sucht; darunter können Kommunikationskosten und Werbekosten fallen.[1634] *Informationskosten* entstehen unter anderem bei der Sammlung von Informationen über die Preise, die von verschiedenen Anbietern für dasselbe Gut gefordert werden.[1635] *Verhandlungskosten* umfassen unter anderem die Kosten, die beim Aushandeln von Vertragsbestimmungen durch die Vertragsparteien entstehen; dies benötigt Zeit, eventuell ist auch eine Rechtsberatung notwendig.[1636] *Entscheidungskosten* umfassen die Kosten der Aufbereitung sämtlicher Informationen, die Kosten der Entscheidungsfindung und ähnliches.[1637] *Überwachungs-* und *Durchsetzungskosten* entstehen bei der Überwachung der Qualität und Menge gelieferter Produkte und bei der Durchsetzung von Vertragsbestimmungen.[1638]

Im Vergleich zum herkömmlichen Handel könnten diese Transaktionskosten in DRM-Systemen sinken. Durch Suchsysteme und das Internet können in DRM-Systemen Such- und Informationskosten deutlich gesenkt werden.[1639] Metadaten ermöglichen die weitgehende Automatisierung von Transaktionen in DRM-Systemen und tragen ebenfalls zur

---

[1632] *Cooter/Ulen*, S. 87, definieren „Transaktionskosten“ als die „costs of exchange“. *Schäfer/Ott*, S. 5, definieren „Transaktionskosten“ als „die Kosten, die potentielle Vertragspartner an Information und Koordination aufwenden müssen, um den Vertrag abzuschließen und durchzusetzen.“ Zum Begriff der Transaktionskosten insgesamt s. *Richter/Furubotn*, S. 45 ff. Der Begriff bleibt in der rechtsökonomischen Literatur recht schwammig, *Eidenmüller*, S. 97 ff. Grundlegend *Coase*, 3 J. L. & Econ. 1 ff. (1960).

[1633] *Richter/Furubotn*, S. 51, 318 ff.; s. a. *Merges*, 12 Berkeley Tech. L. J. 115, 116 (1997). Alle diese Transaktionskosten lassen sich unter dem Begriff „Markttransaktionskosten“ zusammenfassen. Daneben kann man noch Unternehmenstransaktionskosten und politische Transaktionskosten identifizieren, s. *Richter/Furubotn*, S. 49 f.

[1634] *Richter/Furubotn*, S. 51.

[1635] *Richter/Furubotn*, S. 51.

[1636] *Richter/Furubotn*, S. 52.

[1637] *Richter/Furubotn*, S. 52.

[1638] *Richter/Furubotn*, S. 52.

[1639] *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1170 Fn. 50 (1998); *Brynjolfsson/Smith*, 46 Management Science 563, 568 (2000); *Bakos*, 41 (8) Comm. ACM, 35, 39 (August 1998); *Greenwald/Kephart* in: Dean (Hrsg.), S. 506; *Merges*, 12 Berkeley Tech. L. J. 115, 116 (1997); *O'Rourke*, 53 Vand. L. Rev. 1965, 1969 (2000).

Senkung der Transaktionskosten bei.[1640] Auch Verhandlungs- und Entscheidungskosten sinken;[1641] dies zeigen schon die Kommunikationskosten, die durch moderne Kommunikationsmedien drastisch gesunken sind.[1642] Durch technische Schutzmaßnahmen werden schließlich die Überwachungs- und Durchsetzungskosten deutlich vermindert: DRM-Systeme sind „self-enforcing" und verhindern schon den Eintritt einer Rechtsverletzung.[1643] Durch digitale Fingerabdrücke, „traitor tracing", Suchsysteme und andere Verfahren werden die Kosten der Identifizierung von Rechtsverletzern geringer.[1644] Falls sich Software-Agenten durchsetzen, könnten mit ihrer Hilfe Informations-, Such- und Verhandlungskosten nochmals deutlich gesenkt werden. Ein Software-Agent könnte nicht nur die Preise mehrerer Anbieter, sondern auch unterschiedlich ausgestaltete Nutzungsverträge vergleichen und das für den Konsumenten beste Angebot aussuchen.[1645] Selbst wenn man Software-Agenten außer acht läßt, die zu einem großen Teil noch Zukunftsmusik sind, zeigt sich, daß in DRM-Systemen Transaktionskosten deutlich sinken können.[1646] Dies ist ein allgemeines Charakteristikum des Internet und der Digitalisierung.[1647]

b) Auswirkungen auf urheberrechtliche Schrankenbestimmungen

Unter urheberrechtlichen Gesichtspunkten ist das Verhältnis von Transaktionskosten zu urheberrechtlichen Schrankenbestimmungen von Interesse. Sinkende Transaktionskosten in DRM-Systemen können Aus-

[1640] *Merges*, 84 Cal. L. Rev. 1293, 1387 (1996); *Hardy*, 1996 U. Chi. Legal F. 217, 237. *Merges*, 12 Berkeley Tech. L. J. 115, 127 f. (1997) meint hinsichtlich der Metadaten, die einen „friktionslosen" Markt ermöglichen: „They are, in a sense, the ultimate in Newtonian lawmaking."

[1641] *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1170 f. (1998). A. A. *Merges*, 12 Berkeley Tech. L. J. 115, 116 (1997), der betont, daß das Internet die Kosten des *Aushandelns* von Vertragsbedingungen nicht senke; unverändert sei die Mitwirkung von Menschen notwendig. Dies trifft zwar zu, vernachlässigt aber die Senkung der Kommunikationskosten. Die Kosten des *Aushandelns* von Vertragsbedingungen könnten zudem mit Software-Agenten deutlich gesenkt werden.

[1642] *Hardy*, 1996 U. Chi. Legal F. 217, 237.

[1643] S. dazu oben Teil 3, A II 3; vgl. weiterhin *Elkin-Koren/Salzberger*, 19 Int. Rev. L. & Econ., 553, 570 (1999); *Fisher*, 73 Chi.-Kent L. Rev. 1203, 1233 (1998); *Merges*, 12 Berkeley Tech. L. J. 115, 116 (1997).

[1644] *Merges*, 12 Berkeley Tech. L. J. 115, 117 (1997).

[1645] *Brennan*, 36 Hous. L. Rev. 61, 114 f. (1999); *dies.*, 20 Miss. C. L. Rev. 27, 35 (1999); s. a. *Netanel*, 79 Tex. L. Rev. 447, 480 (2000); *Easterbrook*, 1996 U. Chi. Legal F. 207, 215.

[1646] *Bell*, 76 N. C. L. Rev. 557, 579 (1998).

[1647] *Shapiro/Varian*, S. 127; *Easterbrook*, 4 Tex. Rev. L. & Pol. 103, 111 (1999); *Hardy*, 1996 U. Chi. Legal F. 217, 236 ff.; *O'Rourke*, 53 Vand. L. Rev. 1965, 1969 ff. (2000). Diese Entwicklung ist grundsätzlich zu begrüßen, da sie sich dem ökonomischen Ideal einer Welt ohne Transaktionskosten annähert, wie sie von *Ronald Coase* beschrieben wurde; s. a. *Easterbrook*, 4 Tex. Rev. L. & Pol. 103, 111 f. (1999). Zum *Coase*-Theorem s. unten Fn. 1658.

wirkungen auf die Notwendigkeit urheberrechtlicher Schrankenbestimmungen haben.[1648]

In einem grundlegenden Aufsatz aus dem Jahr 1982 stellte *Wendy Gordon* die These auf, daß die „fair use doctrine"[1649] des U.S.-amerikanischen Urheberrechts eingreife, wenn ein Marktversagen vorliege.[1650] Auf einem idealen Markt räumt der Urheber jeder Person ein Nutzungsrecht ein, deren Vorbehaltspreis[1651] über dem Preis liegt, den der Urheber für die Einräumung des Nutzungsrechts verlangt.[1652] Eine solche Transaktion kann jedoch durch prohibitiv hohe Transaktionskosten verhindert werden: Sind die Transaktionskosten höher als der Nutzen, den beide Parteien aus der Transaktion zu ziehen hoffen, so wird die Transaktion nicht durchgeführt.[1653] Hohe Transaktionskosten führen zu einem Marktversagen.[1654] Verhindern prohibitiv hohe Transaktionskosten die Einräumung eines Nutzungsrechts, so sollte nach *Gordon* eine urheberrechtliche Schrankenbestimmung eingreifen, die dem Nutzer die Nutzung des Werks erlaubt, ohne daß eine vorherige Transaktion mit dem Urheber notwendig ist.[1655]

Als Beispiel mag das Erstellen von Fotokopien durch private Nutzer dienen. Müßte ein Nutzer vor dem Kopieren einer Seite aus einem Buch zunächst die Erlaubnis des Urhebers einholen, würde der Nutzer die Seite regelmäßig gar nicht kopieren: Die Transaktionskosten – Identifizierung und Kontaktierung des Urhebers, Vertragsverhandlung und ähnliches –

[1648] Es sei nochmals darauf hingewiesen, daß in diesem Abschnitt die Position, daß DRM-Systeme tiefgreifende ökonomische Änderungen mit sich bringen, zunächst unkritisch referiert wird. Kritische Anmerkungen finden sich weiter unten, s. Teil 3, B I 1 c, und B I 2 a.

[1649] Die „fair use doctrine" ist eine umfassende Schrankenbestimmung des U.S.-amerikanischen Urheberrechts, die sich seit über 100 Jahren im common law herausgebildet hat und 1976 in 17 U.S.C. § 107 kodifiziert wurde. Auch wenn sie mitunter mit § 53 UrhG verglichen wird, ist die „fair use doctrine" sehr viel umfangreicher und offener als einzelne deutsche Schrankenbestimmungen. S. zum ganzen *Goldstein*, Copyright, § 10, S. 10:1 ff.; *Rieder*, S. 195 ff.

[1650] *Gordon*, 82 Colum. L. Rev. 1600 ff. (1982). Daß die vorliegende Arbeit diesen Erklärungsansatz der „fair use doctrine" betont, liegt daran, daß sich dieser Aspekt in die Analyse von DRM-Systemen sehr gut einfügt. Auch in der U.S.-amerikanischen Literatur bestehen Ansätze, die „fair use doctrine" anders zu erklären oder diesen Erklärungsansatz zumindest zu erweitern; s. nur *Fisher*, 101 Harv. L. Rev. 1659, 1744 ff. (1988).

[1651] Zu dem Begriff s. oben bei Fn. 1547.

[1652] *Gordon*, 82 Colum. L. Rev. 1600, 1615 (1982).

[1653] *Gordon*, 82 Colum. L. Rev. 1600, 1628 f. (1982).

[1654] Zum Begriff des Marktversagens s. oben Fn. 1502.

[1655] Tatsächlich sind die Bedingungen, die *Gordon* für das Eingreifen der „fair use defense" aufstellt, komplexer; s. *Gordon*, 82 Colum. L. Rev. 1600, 1614 ff. (1982). Die Verbindung zwischen der „fair use defense" und prohibitiv hohen Transaktionskosten stellen auch *Landes/Posner*, 18 J. Legal Stud. 325, 357 f. (1989), *Posner*, 21 J. Legal Stud. 67, 69 (1992), und *Watt*, S. 13, her.

wären regelmäßig viel höher als der Nutzen, den der Nutzer aus der erstellten Kopie ziehen würde.[1656] Bei solch prohibitiv hohen Transaktionskosten macht es aus ökonomischer Sicht keinen Sinn, das Kopieren urheberrechtlich geschützter Werke zu verbieten: Dadurch würde eine gesellschaftlich wertvolle Nutzung des Werks unterbunden, ohne dem Urheber einen finanziellen Vorteil zu bringen.[1657] Also greift eine Schrankenbestimmung, die dem Nutzer das Kopieren erlaubt und eine Transaktion mit dem Urheber entbehrlich macht.

Nach diesem Ansatz hängt die Reichweite urheberrechtlicher Schrankenbestimmungen somit von der Höhe der Transaktionskosten ab.[1658]

[1656] Bei dieser theoretischen Betrachtung bleiben alternative Ansätze wie die Einschaltung von Verwertungsgesellschaften oder die Einführung von Geräte- und Betreiberabgaben zunächst außen vor.

[1657] *Gordon/Bone* in: Bouckaert/De Geest (Hrsg.), Band II, Kap. 1610, S. 189, 202.

[1658] *Bell*, 76 N. C. L. Rev. 557, 583 (1998). In diesem Zusammenhang sind zwei für die Neue Institutionenökonomie maßgebliche Arbeiten zu beachten. Dies ist zum einen die grundlegende Arbeit von *Coase*, die auf die Bedeutung von Transaktionskosten für die Mikroökonomie und die ökonomische Analyse des Rechts aufmerksam machte; s. *Coase*, 3 J. L. & Econ. 1 ff. (1960). Nach dem – später so genannten – „*Coase*-Theorem" ist für eine effiziente Nutzung von Ressourcen keine bestimmte Zuweisung von „property rights" erforderlich, solange die Transaktionskosten null sind. In einer Gesellschaft, in der die „property rights" eindeutig spezifiziert und frei übertragbar sind und in der keine Transaktionskosten bestehen, ist die letztendliche Ressourcenallokation Pareto-effizient und unabhängig von der ursprünglichen Zuweisung der „property rights": Durch nachfolgende Transaktionen werden die ursprünglich an eine bestimmte Person zugewiesenen „property rights" weiterübertragen und wandern zu der Person mit der höchsten Zahlungsbereitschaft („bester Wirt"), *Schäfer/Ott*, S. 90; *Cooter/Ulen*, S. 82 ff.; *Eidenmüller*, S. 59 ff. Das heißt aber auch, daß die Zuweisung von „property rights" für eine effiziente Nutzung relevant wird, wenn die Transaktionskosten so hoch sind, daß spätere Tauschgeschäfte verhindert werden, *Cooter/Ulen*, S. 85. Das *Coase*-Theorem ist mitunter scharf kritisiert worden, vgl. *Schäfer/Ott*, S. 92 ff. m. w. N. Auch ist die beschränkte Aussagekraft des *Coase*-Theorems zu beachten: Bei fehlenden Transaktionskosten beeinflußt die Zuweisung der „property rights" zwar nicht die effiziente Nutzung, wohl aber die Wohlfahrtsverteilung, s. *Cooter/Ulen*, S. 111. Jedenfalls lenkte das *Coase*-Theorem den Blick der ökonomischen Analyse auf die Bedeutung von Transaktionskosten. Im vorliegenden Zusammenhang noch wichtiger ist die Untersuchung von *Calabresi* und *Melamed* zwischen „property rules" und „liability rules", die auf der Schrift von *Coase* aufbaut; s. *Calabresi/Melamed*, 85 Harv. L. Rev. 1089 ff. (1972); dazu im Überblick *Schäfer/Ott*, S. 516 f.; *Cooter/Ulen*, S. 103 ff. *Calabresi* und *Melamed* unterscheiden zwischen „property", „liability" und „inalienability rules", von denen im vorliegenden Zusammenhang nur die beiden ersten Kategorien von Interesse sind. Beide Kategorien stellen unterschiedliche Arten des Schutzes von „property rights" dar. Bei „property rules" – man mag dies mit „Abwehransprüchen" übersetzen, so *Schäfer/Ott*, S. 516 – darf in die geschützte Rechtsposition nur eingegriffen werden, wenn der Inhaber der Rechtsposition dem ex ante zustimmt. Der Inhaber kann jeden Eingriff in die Rechtsposition abwehren. Vor einem Eingriff wird es daher regelmäßig zu einer Zahlung des Eingreifenden an den Inhaber der Rechtsposition kommen. Bei „liability rules" – man mag dies mit „haftungsrechtlichen Ansprüchen" übersetzen, so *Schäfer/Ott*, S. 517 – kann der Inhaber der Rechtsposition einen Eingriff in die Position nicht *ex ante* abwehren, vielmehr steht ihm nur

Und tatsächlich haben in den letzten Jahren mehrere U.S.-amerikanische Gerichte den Standpunkt bezogen, daß sich der Nutzer eines urheberrechtlich geschützten Werks nicht auf die „fair use defense" berufen könne, wenn ein zumutbarer Weg bestehe, auf vertraglichem Wege ein Nutzungsrecht zu erwerben; bei niedrigen Transaktionskosten sei eine Schrankenbestimmung unnötig.[1659]

Diese Überlegungen lassen sich auch für das deutsche Urheberrecht fruchtbar machen. Ein wichtiger Grund für die Einführung des § 53 UrhG war, daß ein Verbot der Vervielfältigung und eine Vergütungspflicht der Nutzer im privaten Bereich praktisch kaum durchgesetzt werden kann.[1660] Auch die Beschränkung der Verwertungsrechte des Urhebers auf bloße Vergütungsansprüche, Geräte- und Betreiberabgaben nach § 49 Abs. 1 S. 2 sowie §§ 54, 54 a i. V. m. § 54 h Abs. 1 UrhG, können unter dem Gesichtspunkt prohibitiv hoher Transaktionskosten erklärt werden. Wegen hoher Transaktionskosten können diese Ansprüche zudem nur von einer Verwertungsgesellschaft geltend gemacht werden.[1661] Wäre es notwendig, für jedes Zitat aus einem fremden Werk ein entsprechendes Nutzungsrecht vom Urheber zu erwerben, so würden Autoren wegen zu hoher Transaktionskosten auf die Mehrzahl der Zitate verzichten. Auch die Schrankenbestimmung des § 51 UrhG läßt sich daher mit diesem Transaktionskostenansatz erklären.

---

ex post ein Schadensersatzanspruch zu; *Calabresi/Melamed*, 85 Harv. L. Rev. 1089, 1092 (1972). In dem von *Calabresi* und *Melamed* aufgestellten Konzept wird die Höhe der Entschädigung von einem Gericht festgelegt; dies kann aber auch durch andere Institutionen geschehen, s. dazu *Merges*, 84 Cal. L. Rev. 1293, 1303 (1996). *Calabresi* und *Melamed* stellten die These auf, daß bei niedrigen Transaktionskosten „property rules" angemessen seien, während bei hohen Transaktionskosten „liability rules" die effizientere Lösung böten. Dies liegt daran, daß bei hohen Transaktionskosten das Aushandeln der Summe, die der Eingreifende an den Inhaber der Rechtsposition zu zahlen hat, unter den Beteiligten ineffizienter ist als die nachträgliche Festlegung einer Schadenssumme durch ein Gericht, *Calabresi/Melamed*, 85 Harv. L. Rev. 1089, 1110, 1118 f. (1972). S. dazu mit Zahlenbeispiel *Cooter/Ulen*, S. 104; weitere Beispiele finden sich bei *Calabresi/Melamed*, 85 Harv. L. Rev. 1089, 1106 ff. (1972). Diese Analyse läßt sich auch auf urheberrechtliche Schrankenbestimmungen übertragen. So faßt *Hardy*, 1996 U. Chi. Legal F. 217, 233, die „fair use defense" als „liability rule" auf, die wegen hoher Transaktionskosten effizienter sei als eine „property rule". Obwohl der Urheber beim Eingreifen der „fair use defense" keine Entschädigung erhalte, handele es sich dennoch um eine „liability rule", die Entschädigung sei nur Null, s. *Hardy*, 1996 U. Chi. Legal F. 217, 233. A.A. wohl *Gordon*, 82 Colum. L. Rev. 1600, 1622 ff. (1982). Zur Kritik an der „property rule/liability rule"-Analyse s. unten Fn. 1744.

[1659] American Geophysical Union v. Texaco, Inc., 60 F.3d 913 (2d Cir. 1994), *cert. dismissed*, 116 S. Ct. 592 (1995); Princeton University Press v. Michigan Document Services, Inc., 99 F.3d 1381 (6th Cir. 1996), *cert. denied*, 117 S. Ct. 1336 (1997); s. zu beiden Entscheidungen *Loren*, 5 J. Intell. Prop. L. 1, 32 ff. (1997); *Bell*, 76 N.C. L. Rev. 557, 567 ff. (1998); s. weiterhin *Guibault* in: Hugenholtz (Hrsg.), S. 125, 141 f.

[1660] Vgl. *Bundesregierung*, BT-Drs. IV/270 vom 23. 3. 1962, S. 71; *Schack*, Rdnr. 494; *Guibault* in: Hugenholtz (Hrsg.), S. 125, 140; *Wand*, S. 58.

[1661] S. dazu *Pethig*, 144 JITE 462, 489 ff. (1988).

Aufgrund niedrigerer Transaktionskosten und neuer technischer Überwachungsmöglichkeiten sinkt die Wahrscheinlichkeit solcher Marktversagen in DRM-Systemen jedoch deutlich.[1662] Danach könnten Schrankenbestimmungen in DRM-Systemen nur noch eine untergeordnete Rolle spielen.[1663]

5. Ergebnis

Die bisherige ökonomische Analyse von DRM-Systemen zeigt, daß DRM-Systeme bis zu einem gewissen Maß das Urheberrecht ersetzen könnten. Wie das Urheberrecht beseitigen DRM-Systeme die Nicht-Exklusivität von Information und schaffen damit einen Anreiz zur Informationsproduktion. Wie beim Urheberrecht entstehen dadurch zwar Wohlfahrtsverluste. Durch eine Preisdiskriminierung, die in DRM-Systemen in besonderen Maße möglich erscheint, könnte dieser „deadweight loss" jedoch verringert, idealiter sogar ganz beseitigt werden. DRM-Systeme können weiterhin zu einer Senkung von Transaktionskosten führen, was Auswirkungen auf die Notwendigkeit urheberrechtlicher Schrankenbestimmungen haben könnte.

Die dargestellten Argumente werden von einer bestimmten Richtung in der ökonomischen Analyse von DRM-Systemen vorgebracht, die sich von DRM-Systemen im Vergleich zum klassischen Urheberrecht umfassende Verbesserungen hinsichtlich der Allokationseffizienz und der Anreizwirkung versprechen. Die Anhänger dieser Richtung stehen DRM-Systemen damit sehr positiv gegenüber.[1664] Danach bieten DRM-Systeme den Inhalteanbietern einen besseren Schutz als das herkömmliche Urheberrecht und führen damit zu einer größeren Anreizwirkung. Der bessere Schutz führe in Verbindung mit einem Wettbewerb zwischen unterschiedlichen Inhalteanbietern zu niedrigeren Preisen für die Verbraucher und zu einer quantitativen Erhöhung sowie einer qualitativen Verbesserung – bessere Organisation, Aktualität und Verifikation – der angebotenen In-

[1662] So schon *Möschel/Bechtold*, MMR 1998, 571, 575. Die europäische Richtlinie zum Urheberrecht in der Informationsgesellschaft erkennt dieses Abhängigkeitsverhältnis zwischen der Schrankenbestimmung der privaten Vervielfältigungen und DRM-Systemen ebenfalls an, s. Art. 5 Abs. 2 lit.b und Art. 6 Abs. 4 Unterabs. 2 der Richtlinie sowie Erwägungsgrund 39 der Richtlinie, Abl. EG Nr. L 167 vom 22. 6. 2001, S. 10, 13; s. dazu *Bechtold* in: Hoeren/Sieber (Hrsg.), Kap. 7.11, Rdnr. 44.

[1663] *Elkin-Koren/Salzberger*, 19 Int. Rev. L. & Econ., 553, 569 (1999); *Hardy*, 1996 U. Chi. Legal F. 217, 241 f.; *Bell*, 76 N. C. L. Rev. 557, 583 f., 600 ff. (1998); *Goldstein*, Copyright's Highway, S. 224; *Wand*, S. 58; s. a. *Merges*, 12 Berkeley Tech. L. J. 115, 132 (1997). Zur Kritik an dieser These s. unten Teil 3, B I 2 a.

[1664] Deutlichste Vertreter dieser Richtung sind *Bell*, 76 N. C. L. Rev. 557 ff. (1998); *Hardy*, 1196 U. Chi. Legal F. 217 ff. (1996) ff.; sowie – in abgeschwächter Form und mit unterschiedlichen Nuancierungen – *Fisher*, 73 Chi.-Kent L. Rev. 1203 ff. (1998); *O'Rourke*, 12 Berkeley Tech. L. J. 53 ff. (1997); *Merges*, 12 Berkeley Tech. L. J. 115 ff. (1997).

halte.[1665] DRM-Systeme würden zu niedrigeren Transaktionskosten und damit zu höherer Allokationseffizienz führen.[1666] Zwar müsse der Nutzer künftig für die meisten Nutzungen digitaler Inhalte ein Entgelt entrichten.[1667] Im Gegenzug könnten die Inhalte jedoch von einer größeren Zahl von Nutzern benutzt werden, der nicht-rivalisierende Charakter von Information werde so voll ausgenützt.[1668] Indem sich Inhalteanbieter durch technische und vertragliche Mechanismen selbst schützen könnten, werde die Entscheidung über Umfang und Ausgestaltung des Schutzes digitaler Inhalte aus den Händen des Gesetzgebers genommen und in die Hände der Beteiligten gelegt. Auf dieser „dezentralen" Ebene seien die besseren Informationen vorhanden, in welchem Umfang und auf welche Weise digitale Inhalte geschützt werden sollten. DRM-Systeme würden damit das herkömmliche Informationsproblem des Gesetzgebers beseitigen.[1669]

Ob diese Thesen und die bisher dargestellten ökonomischen Gesichtspunkte in dieser Reinheit zutreffen oder ob nicht vielmehr Einschränkungen zu machen und Prämissen in Frage zu stellen sind, soll im nächsten Abschnitt untersucht werden.

B. Notwendigkeit des Urheberrechts

In der Tendenz scheinen die bisherigen rechtlichen und rechtsökonomischen Untersuchungen die These zu bestätigen, daß DRM-Systeme zunehmend Aufgaben des Urheberrechts übernehmen könnten, ja sogar einen Ersatz für den urheberrechtlichen Schutz bieten, und daß diese Entwicklung grundsätzlich zu begrüßen ist. Im folgenden soll untersucht werden, ob diese These unter rechtsökonomischen (dazu unten I) und rechtlichen (dazu unten II) Gesichtspunkten wirklich haltbar ist oder ob bestimmte Einschränkungen zu machen sind.

[1665] *Bell*, 76 N. C. L. Rev. 557, 580, 588 f. (1998).

[1666] *Bell*, 76 N. C. L. Rev. 557, 587 f. (1998).

[1667] *Bell*, 76 N. C. L. Rev. 557, 596 ff. (1998).

[1668] *Bell*, 76 N. C. L. Rev. 557, 589 (1998).

[1669] Vgl. *Easterbrook*, 4 Tex. Rev. L. & Pol.'y 103 ff. (1999); *ders.*, 1996 U. Chi. Legal F. 207, 210 f.; *Bell*, 76 N. C. L. Rev. 557, 592 (1998); s. weiterhin *Merges*, 12 Berkeley Tech. L. J. 115 ff. (1997); *ders.*, 84 Cal. L. Rev. 1293 ff. (1996); *Benkler*, 53 Vand. L. Rev. 2063, 2067 f. (2000); *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1166 f. (1998). *Easterbrook*, 1996 U. Chi. Legal F. 207, 215 f. meint: „Error in legislation is common, and never more so than when the technology is galloping forward. Let us not struggle to match an imperfect legal system to an evolving world that we understand poorly. Let us instead do what is essential to permit the participants in this evolving world to make their own decisions. That means three things: make rules clear; create property rights where now there are none; and facilitate the formation of bargaining institutions. Then let the world of cyberspace evolve as it will, and enjoy the benefits."

I. Rechtsökonomische Überlegungen

Im folgenden soll untersucht werden, ob die dargestellte rechtsökonomische Analyse von DRM-Systemen und ihre Prämissen einer kritischen Überprüfung standhalten (dazu unten 1). Anschließend wird der Frage nachgegangen, ob aus rechtsökonomischer Sicht eine Beschränkung des Schutzes von DRM-Systemen notwendig erscheint, und durch welche Institution diese Beschränkung gegebenfalls erfolgen sollte (dazu unten 2).

1. Kritikpunkte

a) Allgemeines

Auch wenn die dargestellten ökonomischen Überlegungen plausibel klingen mögen, geben sie doch kein vollständiges Bild der ökonomischen Zusammenhänge in DRM-Systemen.[1670] Die Überlegungen gehen oftmals zu stark von einem Idealmodell der vollständigen Konkurrenz aus.[1671] Zwar können DRM-Systeme bestimmte Marktversagen lindern; dies gilt insbesondere hinsichtlich der Nicht-Exklusivität von Information sowie – bis zu einem gewissen Maß – hinsichtlich prohibitiv hoher Transaktionskosten.[1672] Bei einer solchen Betrachtung wird jedoch vernachlässigt, daß DRM-Systeme ihrerseits zu neuen Marktversagen führen können; hier sind insbesondere Informationsasymmetrien und Netzwerkeffekte zu nennen.[1673] Hinter der Auffassung der rechtsökono-

[1670] Eine umfassende Kritik in diese Richtung stammt von *Cohen*, 97 Mich. L. Rev. 462 ff. (1998), die den dargestellten Ansätzen vorwirft, durch unrealistische Prämissen das Ergebnis ihrer Untersuchung schon im voraus festgelegt zu haben. Sie stützt sich in ihrer eigenen Analyse stark auf Arbeiten aus dem Bereich der politischen Ökonomie und der „public choice"-Theorie; auch ihre Untersuchung muß sich jedoch einiges an Kritik gefallen lassen. Ebenfalls kritisch zur dargestellten ökonomischen Analyse von DRM-Systemen *Benkler*, 53 Vand. L. Rev. 2063 ff. (2000); *Boyle*, 53 Vand. L. Rev. 2007 ff. (2000).

[1671] Im Modell der vollständigen Konkurrenz gibt es eine große Anzahl von Anbietern und Nachfragern („atomistischer Markt"), wodurch der Einzelne keinen Einfluß auf den Marktpreis besitzt, verhalten sich Anbieter und Nachfrager rational im Sinne einer Gewinn- und Nutzenmaximierung, besitzen Anbieter und Nachfrager vollkommene Informationen über jedes verfügbare Gut und über jeden Preis eines jeden Guts, haben die Nachfrager keine räumlichen, zeitlichen, persönlichen oder sachlichen Präferenzen hinsichtlich der Anbieter und vice versa, existieren homogene Güter, ist der Markt vollkommen transparent, sind die Produktionsfaktoren und die produzierten Güter voll teilbar und beweglich, bestehen weder rechtliche noch tatsächliche Marktzutritts- oder Marktaustrittsschranken, ist die Reaktionsgeschwindigkeit von Anbietern und Nachfragern unendlich groß, erfolgen keine Eingriffe in den freien Preisbildungsprozeß von staatlicher oder anderer Seite, und existieren keine Externalitäten; s. dazu im Überblick *I. Schmidt*, S. 5; *O'Rourke*, 53 Vand. L. Rev. 1965, 1967 f. (2000); *Pindyck/Rubinfeld*, S. 252 f.

[1672] S. dazu oben Teil III, A III 2, und A III 4.

[1673] S. dazu unten Teil 3, B I 2 b bb 2, und B I 2 b cc 2; vgl. a. *Cohen*, 97 Mich. L. Rev. 462, 560 (1998), die auf S. 523 meint, in DRM-Systemen seien Marktversagen die Regel, nicht die Ausnahme.

mischen Protagonisten von DRM-Systemen[1674] steht ein bestimmtes Verständnis von den Aufgaben des Staates in einer Marktwirtschaft. Es wird eine prinzipielle Überlegenheit vollständig privater Regulierung gegenüber staatlicher Regulierung postuliert.[1675]

Zwar mag *Julie Cohen* in ihrer Kritik zu weit gehen, wenn sie meint: „the cybereconomists assume too much and prove too little about the rightness of their desired regime."[1676] Dennoch ist zu bedenken, daß es bis heute kein umfassendes ökonomisches Wettbewerbsmodell für Informationsgüter gibt.[1677] Empirische Arbeiten fehlen in diesem Bereich fast vollständig.[1678] Auch die ökonomische Analyse des Internet-Rechts steht erst in ihren Anfängen.[1679] Selbst das herkömmliche Urheberrecht bietet der ökonomischen Analyse noch einiges an Forschungsbedarf.[1680] Weder der Gesetzgeber noch die Wissenschaft können heute sagen, welcher Ausgleich im digitalen Umfeld zwischen dem Immaterialgüterschutz – als Investitionsanreiz – und den Beschränkungen dieses Schutzes – zum Schutz des freien Wettbewerbs und der Allgemeinheit – erforderlich ist.[1681] Auch wenn sich solche Fragen niemals mit mathematischer Präzision beant-

---

1674 S. dazu die Nachweise in Fn. 1664.

1675 Vgl. dazu *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1166 ff. (1998); *Benkler*, 53 Vand. L. Rev. 2063, 2067 (2000). *Cohen*, 97 Mich. L. Rev. 462, 464, 468 ff., 494 f. (1998), zeigt deutliche Parallelen zwischen diesen Protagonisten von DRM-Systemen und einer Entscheidung des U.S. Supreme Courts aus dem Jahr 1905 – Lochner v. New York, 198 U.S. 45 (1905) –, in der das Gericht ein Gesetz, das die zulässige Arbeitszeit für Bäcker begrenzte, mit der Begründung für unwirksam erklärte, das Gesetz stelle einen unberechtigten Eingriff in die Vertragsfreiheit der beteiligten Parteien dar. Insgesamt zieht sich der Streit um das Verhältnis zwischen privater und staatlicher Regulierung quer durch das gesamte U.S.-amerikanische Internet-Recht.

1676 *Cohen*, 97 Mich. L. Rev. 462, 560 (1998).

1677 Vgl. *Fishburn/Odlyzko/Siders* in: Kahin/Varian (Hrsg.), S. 167, 170 f.; *Fishburn/Odlyzko*, 13 Economic Theory 447, 448 (1999); *Cohen*, 97 Mich. L. Rev. 462, 540, 544 f. (1998); *Benkler*, 53 Vand. L. Rev. 2063 (2000); *ders.*, 74 N.Y.U. L. Rev. 354, 424 (1999): „We have no idea how a world in which information goods are perfectly excludable – as technological protection measures promise to make them – will look." Aus diesem Grund äußerst kritisch *Easterbrook*, 4 Tex. Rev. L. & Pol. 103, 104 ff. (1999). S. a. *Boyle*, 53 Vand. L. Rev. 2007, 2014 (2000), der darauf hinweist, daß es bisher wenige Ansätze gibt, die unterschiedlichen Standpunkte der ökonomischen Analyse des Urheberrechts im DRM-Bereich in einem einheitlichen Modell zu vereinen.

1678 *Benkler*, 53 Vand. L. Rev. 2063 f., 2067 (2000); *Boyle*, 53 Vand. L. Rev. 2007, 2016 f. (2000); *Messerschmitt/Szyperski*, S. 4.

1679 Einen ersten Überblick über neuartige Probleme verschaffen *Elkin-Koren/Salzberger*, 19 Int. Rev. L. & Econ., 553 ff. (1999). In Bezug auf Software s. *Messerschmitt/Szyperski*.

1680 S. dazu nur die Kritik von *Kitch*, 53 Vand. L. Rev. 1727 ff. (2000); s. weiterhin *Easterbrook*, 1996 U. Chi. Legal F. 207, 208, der auf S. 210 meint, es sei unmöglich, rechtsökonomische Fragen des Internet-Rechts zu behandeln, wenn die rechtsökonomischen Grundlagen von Immaterialgüterrechten noch überhaupt nicht verstanden seien.

1681 *Reichman/Franklin*, 147 U. Penn. L. Rev. 875, 916, 966 (1999).

worten lassen werden, ist man selbst von einer nur näherungsweisen Beantwortung noch weit entfernt.

In den folgenden Abschnitten sollen einige Einwände gegen die bisherige ökonomische Betrachtung von DRM-Systemen näher ausgeführt werden, um ein differenzierteres Bild der Problematik zu vermitteln.

b) Preisdiskriminierungs-Argument

Wie oben dargelegt wurde, führen DRM-Systeme zu einem „deadweight loss", der allerdings durch eine Preisdiskriminierung verringert werden könnte. Idealiter wäre ein preisdiskriminierendes DRM-System genauso effizient wie das Modell des vollkommenen Wettbewerbs.[1682] Die Prämissen dieser Betrachtung sind jedoch unter mehreren Gesichtspunkten angreifbar.

Die Argumentation baut auf der These auf, daß der Schutz von DRM-Systemen zu einem „deadweight loss" führt, der dem Wohlfahrtsverlust bei einem Monopolmarkt vergleichbar ist. Man darf aber nicht vergessen, daß das Urheberrecht und DRM-Systeme nur in den seltensten Fällen zu einem wirklichen Monopol im ökonomischen Sinne führen werden. Tatsächlich bewegt sich der Schutz von DRM-Systemen irgendwo zwischen den beiden Extremen der vollkommenen Konkurrenz und des monopolistischen Anbieters.[1683] In einer solchen Situation kann die Allokationsineffizienz der teilweise monopolistischen Struktur zwar durchaus verringert werden, indem das DRM-System eine Preisdiskriminierung einsetzt. Wie das wirkliche Monopol im ökonomischen Sinne als Referenzmodell zeigt, können dadurch Wohlfahrtsverluste beseitigt werden. In einer Situation zwischen vollkommenem Wettbewerb und monopolistischen Anbieter kann die Allokationsineffizienz der teilweise monopolistischen Struktur aber auch verringert werden, indem die monopolistische Struktur selbst abgebaut wird. Mit anderen Worten: Wenn sich der Schutz von DRM-Systemen irgendwo zwischen den beiden Extremen der vollständigen Konkurrenz und des monopolistischen Anbieters bewegt, so kann die Allokationseffizienz erhöht werden, wenn man DRM-Systeme an eines von zwei Extremen – einerseits vollständige Konkurrenz, andererseits monopolistischer Anbieter mit Preisdiskriminierung – annähert. In beiden Fällen käme es zu einer Pareto-Verbesserung.[1684] Dies bedeutet, daß sowohl die Einführung einer Preisdiskriminierung, die zu einer Erhöhung des Schutzniveaus führt,[1685] als auch die Absenkung des Schutzniveaus zu einer Erhöhung der Allokationseffizienz in DRM-Systemen führen kann.

[1682] S. dazu oben Teil 3, A III 3 b.

[1683] S. oben bei Fn. 1518 ff.

[1684] *Boyle*, 53 Vand. L. Rev. 2007, 2026 f. (2000); *Cohen*, 53 Vand. L. Rev. 1799, 1806 (2000).

[1685] S. oben bei Fn. 1586 f.

Nun kann man vertreten, daß eine Erhöhung des Schutzniveaus in DRM-Systemen wünschenswert ist, da sie die Anreizwirkung für die Informationsproduktion erhöht.[1686] Dabei wird jedoch die Frage außer acht gelassen, ob eine solche Anreizerhöhung überhaupt notwendig und wünschenswert ist. Das Urheberrecht muß einen Ausgleich zwischen den Interessen der Urheber, den Nutzern, der Allgemeinheit und zukünftigen Urhebern schaffen. Ökonomisch läßt sich der Schutz durch das Urheberrecht und äquivalente Schutzmechanismen wie DRM-Systeme nur in dem Umfang rechtfertigen, in dem eine Anreiz- und Belohnungswirkung zur Schaffung neuer Werke notwendig ist. Darüber hinaus wird eine Begründung aus ökonomischer Sicht schwierig.[1687] Mit anderen Worten: Die Ansicht, eine Preisdiskriminierung bei DRM-Systemen führe zu einer erhöhten Anreizwirkung, indem sich der Inhalteanbieter die Konsumentenrente einverleiben könne, läßt die grundlegende Frage außer acht, ob eine solche Wohlstandsumverteilung überhaupt wünschenswert und notwendig ist.[1688]

Wenn es also zumindest nicht offensichtlich ist, daß in DRM-Systemen eine Erhöhung des Schutzniveaus unter Anreizgesichtspunkten notwendig ist, so kann eine Verminderung von Allokationsineffizienzen grundsätzlich auch durch eine Verringerung[1689] des Schutzniveaus erreicht werden. Der Gesetzgeber kann entscheidende Impulse geben, welche Richtung eingeschlagen wird: Weitet er den urheberrechtlichen Schutz aus, erkennt er die Wirksamkeit von „Enter"-Verträgen an[1690], senkt er das Datenschutzniveau[1691] oder führt er einen rechtlichen Umgehungsschutzs für technische Schutzmaßnahmen ein, so stärkt er im DRM-Bereich monopolistische Strukturen und fördert Maßnahmen der Preisdiskriminierung.[1692] Um die Frage zu beantworten, welche Richtung der

[1686] S. dazu oben bei Fn. 1586 f. Durch eine Preisdiskriminierung wird genau dieser Effekt erreicht. Im Gegensatz zum Konkurrenzmarkt und zum nicht-preisdiskriminierenden Monopolmarkt fällt bei perfekter Preisdiskriminierung die *gesamte* am Markt entstehende Rente ausschließlich dem monopolistischen Produzenten zu, *Varian*, S. 421; *Boyle*, 53 Vand. L. Rev. 2007, 2025 f. (2000). Damit kommt eine Preisdiskriminierung einer Verstärkung des Urheberrechts gleich. Ein Monopolist setzt die Preisdiskriminierung ein, um sich die Konsumentenrente möglichst vollständig einzuverleiben, *Pindyck/Rubinfeld*, S. 370. Sowohl der Konkurrenzmarkt als auch der preisdiskriminierende Monopolmarkt sind effizient; sie unterscheiden sich jedoch deutlich in der Wohlfahrtsverteilung, s. *Boyle*, 53 Vand. L. Rev. 2007, 2025 (2000).

[1687] Darauf wird unter rechtsökonomischen Gesichtspunkten unten Teil 3, B I 2 a, unter rechtlichen Gesichtspunkten unten Teil 3, B II 3 a, eingegangen.

[1688] *Cohen*, 97 Mich. L. Rev. 462, 510 Fn. 183 (1998).

[1689] Das hieße z. B. Einsatz weniger umfangreicher oder weniger sicherer technischer Schutzmaßnahmen in DRM-Systemen.

[1690] S. dazu oben Teil 2, B II 2 b.

[1691] Die Absenkung des Datenschutzniveaus würde DRM-Anbietern erlauben, umfangreichere Nutzungsprofile anzulegen. Diese Informationen könnten wiederum für eine bessere Preisdiskriminierung verwendet werden.

[1692] *Boyle*, 53 Vand. L. Rev. 2007, 2026 (2000).

Gesetzgeber aus ökonomischer Sicht am besten einschlagen sollte, müßten die Kosten beider alternativer Vorgehensweisen miteinander verglichen werden. Dies ist ein komplexes Unterfangen, müßten doch neben den eigentlichen Kosten der Umstellung – Gesetzesänderungen, Verwaltungskosten und ähnliches – auch dynamische Effekte auf den künftigen Innovationsprozeß und exogen festgelegte Rechte – beispielsweise Datenschutz und freie Meinungsäußerung – berücksichtigt werden.[1693]

Bevor man für eine Ausdehnung des DRM-Schutzes durch eine Preisdiskriminierung plädiert, müßten solche Fragen angesprochen werden, die schwierige theoretische wie empirische Probleme aufweisen. Dies ist bisher nicht der Fall gewesen.[1694] Mit anderen Worten: Man kann nicht durch die Etablierung des Urheberrechts und von DRM-Systemen zunächst Wohlfahrtsverluste schaffen, um dann die Preisdiskriminierung und damit eine Erhöhung des Schutzniveaus als Lösung anzupreisen, wenn eine Verringerung des Schutzniveaus die Wohlfahrtsverluste ebenfalls beseitigen würde. Eine solche Argumentation kommt einer *petitio principii* nahe.[1695]

Diese argumentative Schwäche läßt sich auch in der ProCD-Entscheidung nachweisen.[1696] Judge *Easterbrook* meinte, die Preisdiskriminierung von ProCD führe zu Effizienzgewinnen. Dabei verglich er implizit die Allokationseffizienz eines nicht-preisdiskriminierenden Monopolisten mit der eines preisdiskriminierenden Monopolisten. Dagegen stellte er nicht die Frage, ob ProCD überhaupt ein wie auch immer geartetes Ausschließlichkeitsrecht zustehen sollte. Die USA kennen gerade keinen immaterialgüterrechtlichen Schutz für Datenbanken. Es erscheint zweifelhaft, ob ein vertraglicher Schutz für Datenbanken mit ähnlichen Anreizwirkungen überhaupt wünschenswert oder rechtlich zulässig ist.[1697] Mit anderen Worten: Judge *Easterbrook* hätte in seiner ökonomischen Analyse nicht nur den nicht-preisdiskriminierenden mit dem preisdiskriminierenden Monopolmarkt, sondern auch beide Modelle mit dem Konkurrenzmarkt vergleichen müssen.[1698]

[1693] *Boyle*, 53 Vand. L. Rev. 2007, 2027 (2000).

[1694] *Boyle*, 53 Vand. L. Rev. 2007, 2027 (2000); vgl. weiterhin *Kitch*, 53 Vand. L. Rev. 1727, 1729 ff., 1736 (2000).

[1695] Vgl. dazu auch *Gordon*, 73 Chi.-Kent L. Rev. 1367, 1381, 1386 ff. (1998).

[1696] Zu dieser Entscheidung s. oben Teil 3, A III 3 b a.

[1697] Diese Frage spielt auch unter dem Gesichtspunkt der „federal preemption" nach 17 U.S.C. § 301 eine Rolle, s. dazu unten Teil 4, B III 1.

[1698] S. dazu *Gordon*, 73 Chi.-Kent L. Rev. 1367, 1381, 1383 ff. (1998). Daneben wird Judge *Easterbrook* vorgeworfen, dem Copyright Act ließe sich nicht entnehmen, daß solche ökonomischen Überlegungen bei der Auslegung des geltenden Urheberrechts überhaupt heranzuziehen seien; so *Nimmer/Brown/Frischling*, 87 Cal. L. Rev. 17, 61 f. (1999) unter Bezug auf eine neuere Entscheidung des Supreme Court, in der dieser schreibt: „[…] whether or not we think it would be wise policy to provide statutory protection for such price discrimination is not a matter that is relevant to our duty to interpret the text of the Copyright Act"; s. Quality King Distribs., Inc. v. L'Anza Research

Neben diesem grundsätzlichen Einwand gegen das Preisdiskriminierungs-Argument bei DRM-Systemen ist zu beachten, daß es oft von der Betrachtungsweise abhängt, ob überhaupt eine Preisdiskriminierung vorliegt.[1699] In der obigen Analyse wurde beispielsweise dargelegt, eine Preisdiskriminierung liege vor, wenn je nach Nutzungsintensität für digitale Inhalte ein unterschiedlicher Preis berechnet werde: Hört ein Nutzer ein DRM-geschütztes Musikstück insgesamt zwei Mal an, so wird ihm ein niedrigerer Preis berechnet als dem Nutzer, der das Stück fünf Mal pro Tag anhört.[1700] Ob eine solche Differenzierung tatsächlich eine Preisdiskriminierung darstellt, hängt davon ab, was man als das Gut betrachtet, das der Anbieter verkauft. Versteht man unter dem Gut den digitalen Inhalt, so wird es tatsächlich zu unterschiedlichen Preisen angeboten: Ein Nutzer, der den Inhalt häufig nutzt, muß für das Gut mehr zahlen als ein Nutzer, der das Gut selten nutzt. Versteht man unter dem Gut dagegen die Nutzungsdauer eines digitalen Inhalts, so berechnet der Anbieter allen Nutzern den gleichen Preis; die Nutzer konsumieren das Gut nur in unterschiedlichen Mengen. Da digitale Inhalte in Online-Umgebungen zunehmend nicht mehr als diskrete Produkte, sondern als kontinuierliche Dienstleistung angeboten werden, könnte dieser Einwand zunehmend an Bedeutung gewinnen.

Es geht an dieser Stelle nicht darum, die einzelnen Argumente für oder gegen die Preisdiskriminierung in DRM-Systemen abschließend zu bewerten oder zu widerlegen. Es soll nur gezeigt werden, daß die theoretischen und empirischen Grundlagen der These, eine Preisdiskriminierung sei in DRM-Systemen aus ökonomischer Sicht zu begrüßen, lückenhaft sind.

c) Transaktionskosten-Argument

Wie oben dargestellt wurde, könnten DRM-Systeme und der E-Commerce im allgemeinen zu einer deutlichen Senkung von Transaktionskosten führen, was unter anderem Auswirkungen auf die Notwendigkeit urheberrechtlicher Schrankenbestimmungen haben könnte.[1701] Auch hier stellt sich jedoch die Frage, ob die These in dieser Allgemeinheit haltbar ist. So muß die Aussage kritisch hinterfragt werden, das Internet und DRM-Systeme würden zu einer deutlichen Senkung von Transaktionskosten führen.

Zum einen gibt es im Internet Entwicklungen, die sogar zu einer Erhöhung von Transaktionskosten führen können. Wenn in DRM-Systemen

---

Int'l, Inc., 118 S. Ct. 1125, 1134 (1998); dagegen *O'Rourke*, 12 Berkeley Tech. L. J. 53, 87 f. (1997). Zu weiteren Kritikpunkten an der ökonomischen Argumentation *Easterbrooks* s. *Meurer*, Copyright Law and Price Discrimination, S. 17 ff., 40 ff.

[1699] S. zum folgenden *Kitch*, 53 Vand. L. Rev. 1727, 1738 (2000).

[1700] S. oben bei Fn. 1607.

[1701] S. oben Teil 3, A III 4.

für jede Nutzung eines digitalen Inhalts entsprechende Nutzungsverträge abgeschlossen werden müßten, so könnte allein die Anzahl der notwendigen Verträge zu einer Erhöhung der Transaktionskosten führen.[1702] In diesem Zusammenhang sind die Vielzahl von überlappenden Nutzungsrechten und von Rechteinhabern – Stichwort: Multimedia – zu beachten.[1703] Weiterhin können in DRM-Systemen auch kleinste Einheiten digitaler Inhalte einzeln vertrieben werden. In einem solchen Fall kann das Verhältnis zwischen Transaktionskosten und Transaktionswert ungünstiger sein als bei einer herkömmlichen Transaktion.[1704] Zumindest derzeit sind im Internet und in DRM-Systemen noch keine umfassenden Mechanismen praktisch verfügbar, um die Integrität und Authentizität angebotener Inhalte zu überprüfen und Rechteinheber digitaler Inhalte zu identifizieren. Solange technische Lösungsmöglichkeiten nur auf dem Reißbrett existieren, können auch diese Aspekte zu hohen Transaktionskosten führen.[1705]

DRM-Systeme und der E-Commerce im allgemeinen versprechen insbesondere, durch unterschiedliche Arten von Suchsystemen Suchkosten zu senken.[1706] Suchsysteme können bei stark individualisierten digitalen Inhalten oft nicht weiterhelfen. Individualisierte Produktangebote erschweren den Vergleich zwischen unterschiedlichen Anbietern. Aus Sicht der Anbieter ist eine zu starke Vergleichbarkeit mit Wettbewerbern oft gar nicht erwünscht. Die Individualisierung des Produktangebots dient mitunter gerade dem Zweck, die Vergleichbarkeit zu erschweren und damit Transaktionskosten zu erhöhen.[1707] Zu diesem Zweck blockieren Anbieter mit höheren Preisen im Internet beispielsweise automatische Preisvergleichsysteme, um einen effizienten Preisvergleich der Konsumenten zu verhindern.[1708] Dies alles wirkt dem Trend zu einem „friktionslosen" E-Commerce entgegen.[1709]

[1702] So *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1195 (1998); *Elkin-Koren/Salzberger*, 19 Int. Rev. L. & Econ., 553, 568 (1999); s. a. *Dreier*, CR 2000, 45, 47.

[1703] *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1197 (1998); s. a. *Lemley*, 75 Tex. L. Rev. 989, 1068 (1997); *Bailey*, S. 102.; *Möschel/Bechtold*, MMR 1998, 571. Diese Probleme sollen bei Multimedia-Werken durch „One-Stop-Shops" der Verwertungsgesellschaften gelöst werden, s. dazu oben Teil 1, D V.

[1704] So *Hardy*, 1996 U. Chi. Legal F. 217, 239 f.

[1705] *Elkin-Koren/Salzberger*, 19 Int. Rev. L. & Econ., 553, 562 f. (1999); *Burk*, 21 Cardozo L. Rev. 121, 152 ff. (1999).

[1706] S. oben bei Fn. 1639.

[1707] *Shapiro/Varian*, S. 168; *Farag/Van Alstyne* in: Proceedings of the 2nd ACM Conference on Electronic Commerce 2000, S. 135 ff.

[1708] *DeLong/Froomkin* in: Kahin/Varian (Hrsg.), S. 6, 25; *Burk*, 21 Cardozo L. Rev. 121, 156 (1999); *ders.*, 4 J. Small & Emerg. Bus. L. 27 (2000); eBay v. Bidder's Edge, 100 F. Supp.2d 1058 (C.D. Cal. 2000). S. dazu umfassend *O'Rourke*, 53 Vand. L. Rev. 1965, 1975 ff. (2000).

[1709] *Burk*, 21 Cardozo L. Rev. 121, 156 (1999).

Auch das Argument, daß der Einsatz von Software-Agenten zu einer drastischen Senkung von Transaktionskosten führt,[1710] ist mit Vorsicht zu genießen. In den meisten Fällen handelt es sich bei Software-Agenten noch um Zukunftsmusik.[1711] Auch treten bei der Interaktion großer Populationen von Software-Agenten – es kann sich um mehrere hunderttausend oder gar Millionen von Software-Agenten handeln – neue Effekte auf, die von der Internet-Ökonomie bisher noch in keiner Weise befriedigend erklärt sind.[1712] Schließlich ist ein Software-Agent nur dann sinnvoll, wenn er die Präferenzen des Konsumenten, der den Software-Agenten einsetzt, adäquat repräsentiert. Dafür muß der Konsument den Software-Agenten mit entsprechenden Informationen über seine Präferenzen versorgen. Die Erfahrung zeigt, daß viele Nutzer von Software – beispielsweise Filtersoftware im Jugendschutz- oder Software im Datenschutzbereich – die Standardeinstellungen des Herstellers übernehmen, ohne die Software entsprechend der eigenen Präferenzen zu personalisieren.[1713] Beim Einsatz von Software-Agenten, die mit den Voreinstellungen des Software-Herstellers ausgestattet sind, treten mögliche Effizienzgewinne aber nicht auf.

Neben diesen theoretischen Einwänden ist auch auf empirischer Seite alles andere als geklärt, welche Auswirkungen der E-Commerce und das Internet auf die Höhe von Transaktionskosten haben. Derzeit ist zumindest unklar, ob sich die These empirisch belegen läßt, daß das Internet zu mehr Wettbewerb, zu einer Effizienzsteigerung, zu geringeren Transaktionskosten und damit zu niedrigeren Preisen führt.[1714] Studien, die die Preise von Büchern und CDs im traditionellen Handel mit den Preisen bei Internet-Händlern vergleichen, kommen zu widersprüchlichen Ergebnissen: Teilweise wird festgestellt, daß die Preise im Internet-Handel um 9–16% geringer seien als die Preise für die identischen Produkte im herkömmlichen Handel.[1715] Teilweise wird festgestellt, daß sich die Preise

---

[1710] S. oben bei Fn. 1645.

[1711] S. oben Teil 1, E III; diesen Gesichtspunkt vernachlässigt *Brennan*, 20 Miss. C. L. Rev. 27 ff. (1999). *Samuelson*, 87 Cal. L. Rev. 1, 4 (1999), bezweifelt, ob Software-Agenten im zukünftigen E-Commerce überhaupt eine bedeutende Stellung haben werden.

[1712] Näher dazu beispielsweise *Netanel*, 79 Tex. L. Rev. 447, 481 ff. (2000); *Kephart/Hanson/Greenwald*, 32 Computer Networks 731 ff. (2000).

[1713] Ebenso *Netanel*, 79 Tex. L. Rev. 447, 482 (2000); *Schwartz*, 2000 Wis. L. Rev. 743, 754 f.

[1714] Danach sollen die Preise im Internet fallen, da die Konsumenten aufgrund gesunkener Such- und Informationskosten bessere Preisvergleiche zwischen mehreren Anbietern eines Guts durchführen können. S. dazu die grundlegende Untersuchung von *Bailey*.

[1715] Dies ist das Ergebnis einer von *Brynjolfsson* und *Smith* in den USA durchgeführten Studie, die zwischen Februar 1998 und Mai 1999 u. a. die Preise für Bücher und CDs zwischen herkömlichen Händlern und Angeboten im Internet verglichen; s. *Brynjolfsson/Smith*, 46 Management Science 563, 564 f. (2000).

nicht unterscheiden; andere Studien kommen zum Ergebnis, die Preise im herkömlichen Handel seien sogar günstiger.[1716] Die Vorhersage, daß gesunkene Such- und Informationskosten im Internet zu einem verstärkten Preiswettbewerb führen, wodurch die Produkte tendenziell zu einem einheitlichen Preis angeboten werden,[1717] läßt sich empirisch bis heute nicht bestätigen.[1718]

Insgesamt zeigt sich, daß die Aussagen, im Online-Umfeld seien Transaktionskosten vernachlässigbar klein, weit übertrieben sind.[1719] Man muß deutlich zwischen einer kurzfristigen und einer langfristigen Perspektive unterscheiden: Zwar bieten DRM-Systeme und der E-Commerce zahlreiche Möglichkeiten, durch die Transaktionskosten deutlich gesenkt werden können. Allerdings handelt es sich dabei oft um bloße Potentiale, die noch nicht realisiert sind. Eine realistischere Einschätzung ist daher, daß das Internet und DRM-Systeme das *Potential* haben, Transaktionskosten deutlich zu senken, daß dieses Potential bisher aber allenfalls in Ansätzen realisiert wurde. Damit steht aber auch die These, die Notwendigkeit urheberrechtlicher Schrankenbestimmungen würde durch gesunkene Transaktionskosten entfallen, zumindest derzeit auf wackeligen Füßen. Langfristig mag sie freilich einiges für sich haben.[1720]

[1716] *Bailey* kommt bei einem Vergleich von U.S.-Preisen für Bücher, CDs und Software in den Jahren 1997 und 1998 zu dem Ergebnis, daß die Preise bei Online-Händlern nicht geringer sind als in herkömmlichen Geschäften, s. *Bailey*, S. 83 ff., 101 ff. Zu einem ähnlichen Ergebnis kommt eine in den USA im April 1999 durchgeführten Studie, die die Preise von Internet-Buchhändlern mit den Preisen in normalen Buchläden verglich, s. *Clay/Krishnan/Wolff/Fernandes*, S. 3 f., 10 ff. Wenn man die Versandkosten und die „sales tax" berücksichtige, seien die Preise in herkömmlichen Buchläden sogar günstiger als in Online-Buchläden, s. *Clay/Krishnan/Wolff/Fernandes*, S. 4, 13 ff. Einen Überblick über diese und weitere empirische Studien geben *Smith/Bailey/Brynjolfsson* in: Brynjolfsson/Kahin (Hrsg.), S. 99, 100 ff.

[1717] Diese Vorhersagen bauen regelmäßig auf dem Preiswettbewerbsmodell von *Bertrand* auf, einem Oligopolmodell, in dem die Unternehmen ein homogenes Gut produzieren, jedes Unternehmen den Preis seiner Wettbewerber als gegeben ansieht und alle Unternehmen gleichzeitig ihre Preise setzen. In diesem Modell werden alle Unternehmen ihre Preise in Höhe der Grenzkosten setzen; s. dazu, auch zur Kritik an dem Modell, *Borrmann/Finsinger*, S. 68 ff.; *Pindyck/Rubinfeld*, S. 437 f.

[1718] S. *Clay/Krishnan/Wolff* in: Proceedings of the 2nd ACM Conference on Electronic Commerce 2000, S. 44 ff., die zwischen August 1999 und Januar 2000 die Preise von 315 Büchern in 32 U.S.-amerikanischen Online-Buchläden untersuchten. S. weiterhin *Farag/Van Alstyne* in: Proceedings of the 2nd ACM Conference on Electronic Commerce 2000, S. 135 ff.

[1719] Ebenso *Merges*, 12 Berkeley Tech. L. J. 115, 116 (1997); s. a. *Brynjolfsson/Smith*, 46 Management Science 563, 569 (2000).

[1720] Dann ist allerdings immer noch zu fragen, ob die Fokussierung auf eine Transaktionskostenanalyse die Problematik urheberrechtlicher Schrankenbestimmungen vollständig erfaßt; s. dazu sogleich im Text.

2. Beschränkung des DRM-Schutzes

In DRM-Systemen kann der Inhalteanbieter Umfang, Intensität und Dauer des DRM-Schutzes und der einzelnen Schutzmechanismen (Technik, Nutzungsverträge, Technologie-Lizenzverträge) grundsätzlich selbst festlegen. Er kann einen digitalen Inhalt technisch und vertraglich schützen, obwohl dessen urheberrechtlicher Schutz schon erloschen ist (s. § 64 UrhG). Er kann auch das Erstellen von Kopien zum privaten Gebrauch technisch verhindern oder vertraglich untersagen, selbst wenn der Nutzer dazu nach einer urheberrechtlichen Schrankenbestimmung berechtigt sein sollte. Da Inhalteanbieter und DRM-Systembetreiber in der Ausgestaltung des DRM-Schutzes grundsätzlich keinen Beschränkungen unterliegen, werden sie versuchen, ein möglichst umfassendes und sicheres Schutzsystem zu verwenden. Das Bestreben nach einer möglichst weitgehenden Kontrolle bringt es aber mit sich, daß in einem solchen System urheberrechtliche Schrankenbestimmungen nicht beachtet werden. Es entsteht ein Spannungsverhältnis zwischen dem Schutz durch DRM-Systeme und urheberrechtlichen Schrankenbestimmungen.[1721]

Das Urheberrecht verleiht dem Urheber keine unbeschränkten Verwertungsrechte. Vielmehr finden sich zahllose Schrankenbestimmungen, die in Deutschland in §§ 45 ff. UrhG enthalten und in der europäischen Richtlinie zum Urheberrecht in der Informationsgesellschaft in Art. 5 geregelt sind.[1722] Trifft die These zu, daß DRM-Systeme bei digitalen Inhalten in gewissem Umfang den Schutz durch das Urheberrecht ersetzen könnten, so stellt sich die Frage, ob der Schutz durch DRM-Systeme in ähnlicher Weise beschränkt werden sollte, wie der urheberrechtliche Schutz durch Schrankenbestimmungen beschränkt wird. Dieser Frage soll im folgenden unter rechtsökonomischen Gesichtspunkten nachgegangen werden. In einem späteren Abschnitt geht die Untersuchung auf rechtliche Aspekte dieser Frage ein.[1723]

a) Notwendigkeit einer Beschränkung

Um die Frage zu beantworten, ob unter dem Blickwinkel der ökonomischen Analyse eine Beschränkung des DRM-Schutzes – ähnlich den urheberrechtlichen Schrankenbestimmungen – notwendig ist, muß zunächst auf Funktionen von Schrankenbestimmungen im Bereich des Urheberrechts eingegangen werden.

Wie oben dargelegt wurde, verringert das Urheberrecht durch seine Anreizwirkung den Wohlfahrtsverlust durch Unterproduktion („social welfare loss due to underproduction"), nimmt aber gleichzeitig einen

---

[1721] S. dazu ausführlich unten Teil 3, B II 3.

[1722] In den USA finden sich wichtige Schrankenbestimmungen unter anderem in 17 U.S.C. § 107 („fair use defense") und § 109 („first sale doctrine").

[1723] S. dazu unten Teil 3, B II 3.

Wohlfahrtsverlust durch Unternutzung („social welfare loss due to underutilization") in Kauf.[1724] Es ist die zentrale Aufgabe des Urheberrechts, zwischen diesen beiden Polen – Unterproduktion und Unternutzung oder Anreiz zur Werkschöpfung und Zugang zum geschöpften Werk – einen angemessenen Ausgleich zu finden.[1725] Der urheberrechtliche Schutz muß aus diesen Gründen beschränkt werden. Ökonomisch läßt sich der Schutz durch das Urheberrecht nur in dem Umfang rechtfertigen, in dem eine Anreiz- und Belohnungswirkung zur Schaffung neuer Werke notwendig ist. Darüber hinaus wird eine Begründung aus ökonomischer Sicht schwierig.[1726]

[1724] S. dazu ausführlich oben Teil 3, A III 2 c.

[1725] *Landes/Posner*, 18 J. Legal Stud. 325, 326 (1989); *Fisher*, 101 Harv. L. Rev. 1659, 1703 (1988); *Liebowitz*, S. 5; *Elkin-Koren*, 12 Berkeley Tech. L. J. 93, 99 f. (1997).

[1726] Vgl. *van den Bergh*, I.P.Q. 1998, 17, 21; *Lemley*, 75 Tex. L. Rev. 989, 997 (1997); *Sterk*, 94 Mich. L. Rev. 1197, 1209 (1996); *Lehmann*, GRUR Int. 1983, 356, 362. Seit einiger Zeit ist dies in der ökonomischen Analyse der Immaterialgüterrechte allerdings nicht mehr unumstritten (s. *Merges*, 21 AIPLA Q. J. 305, 306 (1993): „[…] the literature has progressed beyond the point where a crude ‚incentive' story passes for analysis in every case"). So wird vertreten, dem Urheber sollten möglichst umfangreiche „property rights" verliehen werden, da nur so die effiziente Verwertung der geschützten Güter gewährleistet sei. Nach dieser Auffassung ist das Urheberrecht nicht nur ein Produktionsanreiz, sondern ermöglicht zusätzlich einen Markt, auf dem Nutzungsrechte an die Nutzer mit der höchsten Zahlungsbereitschaft wandern. Danach ist es nicht so sehr die Aufgabe des Urheberrechts, einen Produktionsanreiz zu schaffen, sondern vielmehr soll das Urheberrecht dem Urheber ermöglichen festzustellen, was seine Werkschöpfungen am Markt wert sind. Durch die bessere Einschätzung der Nachfrage kann der Urheber Werke schaffen, die am Markt Erfolg haben. Das Urheberrecht und andere Immaterialgüterrechte dient daher der besseren Ressourcenallokation; vgl. *Netanel*, 106 Yale L. J. 283, 309 (1996); *Koelman*, The Protection of Technological Measures, S. 3. Nach diesem Ansatz sind urheberrechtliche Schrankenbestimmungen weniger wichtig. Vielmehr wird in solchen Fällen auf Transaktionen zwischen dem Urheber und den Nutzern gesetzt; diese Transaktionen sollen durch eine Zuweisung umfassender „property rights" als Ausgangspunkt erleichtert werden. Die Ressourcenallokation sollte weitesmöglich dem Markt überlassen werden, was zu einer Effizienzsteigerung führe; s. *Netanel*, a. a. O., S. 309 f., 318 f., m. w. N. Im Ergebnis unterscheidet sich dieser – mitunter „neoklassissch" genannte – Ansatz vom anreizbasierten Ansatz hauptsächlich durch den *Umfang* der „property rights", die durch das Urheberrecht verliehen werden sollen: Während der anreizbasierte Ansatz den urheberrechtlichen Schutz begrenzt, favorisiert der „neoklassische" Ansatz umfassende Urheberrechte und überläßt die Allokation dieser Rechte dann dem Markt, *Netanel*, a. a. O., S. 310; *Lemley*, a. a. O., S. 1044. Dieser Ansatz wurde zuerst für das Patentrecht als sog. „prospect theory" entwickelt von *Kitch*, 20 J. L. & Econ. 265 ff. (1977). Er stellt Parallelen zur Begründung von „property rights" durch das Sachenrecht her. Dort werden umfangreiche „property rights" regelmäßig mit der sog. „Tragödie der Allmende" begründet, die zu einer Übernutzung knapper Ressourcen führt; s. dazu unten Fn. 1743. Wenn auch der Schwerpunkt der bisherigen Untersuchungen des „neoklassischen Ansatzes" im Patentrecht liegt, wird der Ansatz auch im Urheberrecht vertreten; s. *Gordon*, 41 Stan. L. Rev. 1343, 1389, 1435 ff. (1989); *Easterbrook*, 13 Harv. J. L. & Pub. Pol'y 108, 113 (1990); *ders.*, 4 Tex. Rev. L. & Pol. 103, 111 f. (1999); *ders.*,

Urheberrechtliche Schrankenbestimmungen wollen diesen Ausgleich zwischen Unterproduktion und Unternutzung herstellen. Dabei ist zu beachten, daß Schrankenbestimmungen auch den Interessen der Urheber selbst dienen. Die meisten urheberrechtlich geschützten Werke bauen in hohem Maß auf früheren Werken auf.[1727] Je stärker und länger diese früheren Werke urheberrechtlich geschützt werden, desto höher sind die Kosten, nachfolgende Werke zu schaffen.[1728] Es entspricht daher dem eigenen Interesse der Urheber, daß das Urheberrecht keinen allzu umfassenden Schutz bietet.[1729]

Urheberrechtliche Schrankenbestimmungen dienen auch dem Interesse Dritter und Interessen der Allgemeinheit. Dies zeigt sich, wenn man sich eine Rechtslage vorstellt, in der ein umfassendes Urheberrecht ohne Schrankenbestimmungen besteht. Wollte in einem solchen System ein Kritiker Ausschnitte aus einem Buch in seiner Buchkritik zitieren, so müßte er dafür einen urheberrechtlichen Nutzungsvertrag mit dem Urheber abschließen. Selbst wenn man die Problematik der Transaktionskosten vernachlässigt, ist zu beachten, daß von diesem Zitat nicht nur der

1996 U. Chi. Legal F. 207, 212 („Create property rights, where now there are none [… in order] to make bargains possible"); *Dam*, 24 J. Legal Stud. 321, 332 bei Fn. 44 (1995); *Merges*, 12 Berkeley Tech. L. J. 115, 127, 131 (1997). Nach diesem Ansatz internalisiert das Urheberrecht positive externe Effekte, da es dem Urheber erlaubt, den Nutzen abzuschöpfen, den das geschaffene Werk bei Dritten schafft, *Demsetz*, 57 Am. Econ. Rev. Papers & Proc. 347, 359 (1967); *Gordon*, 41 Stan. L. Rev. 1343, 1348 Fn. 21, 1437 ff. (1989); *Netanel*, a. a. O., S. 312. Anhänger der Neuen Institutionenökonomik vertreten ähnliche Positionen; s. nur *Richter/Furubotn*, S. 131; *Netanel*, a. a. O., S. 312 ff. Einen Überblick über den „neoklassischen" Ansatz sowie kritische Anmerkungen geben *Lemley*, a. a. O., S. 1044 ff.; *Netanel*, a. a. O., S. 308 ff.; *Hardy*, 1996 U. Chi. Legal F. 217, 132 ff. In der deutschsprachigen rechtsökonomischen Literatur betont insbesondere *Lehmann* in seinen Abhandlungen zu „property rights" die Parallelen zwischen dem Urheberrecht und dem Sacheigentum, s. *Lehmann* in: Neumann (Hrsg.), S. 519, 533; *ders.*, GRUR Int. 1983, 356 ff.; s. a. *Wiebe*, GRUR 1994, 233, 242. Kritisch zur Übertragbarkeit der „Tragödie der Allmende"-Analyse auf das Urheberrecht, das sich mit nicht-rivalisierender Information beschäftigt, *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1191 (1998). Die Kritik an der ökonomischen Analyse urheberrechtlicher Schrankenbestimmungen, die in diesem Abschnitt geäußert wird, ist auch und gerade auf den „neoklassischen" Ansatz anwendbar.

[1727] Man kann insofern davon sprechen, daß Information nicht nur nicht-rivalisierend und nicht-exklusiv, sondern auch „kumulativ" ist, s. *Gordon/Bone* in: Bouckaert/De Geest (Hrsg.), Band II, Kap. 1610, S. 189, 195.

[1728] *Lemley*, 75 Tex. L. Rev. 989, 997 ff. (1997); *Netanel*, 106 Yale L. J. 283, 295 f. (1996); *Landes/Posner*, 18 J. Legal Stud. 325, 332 (1989); *Posner*, Economic Analysis of Law, S. 47; *van den Bergh*, I.P.Q. 1998, 17, 22; *Sterk*, 94 Mich. L. Rev. 1197, 1207 (1996); *Gordon/Bone* in: Bouckaert/De Geest (Hrsg.), Band II, Kap. 1610, S. 189, 195; *Mahajan*, 67 Fordham L. Rev. 3297, 3331 (1999); *O'Rourke*, 12 Berkeley Tech. L. J. 53, 80 (1997).

[1729] *Landes/Posner*, 18 J. Legal Stud. 325, 333 (1989); *Cohen*, 97 Mich. L. Rev. 462, 498 (1998); *Loren*, 5 J. Intell. Prop. L. 1, 24 f. (1997); kritisch *O'Rourke*, 12 Berkeley Tech. L. J. 53, 80, 83 f. (1997).

Kritiker profitiert. Vielmehr profitieren davon auch die Leser seiner Kritik. Gleiches gilt bei einem Künstler, der auf einem bestehenden Werk aufbaut und ein neues Werk schöpft. Es ist nicht nur der Künstler, der profitiert, wenn er das frühere Werk als Grundlage für sein neues Werk verwenden kann. Es sind auch Dritte, wenn sie das neu geschaffene Werk betrachten oder nutzen.[1730]

In all diesen Fällen, in denen es um das Verhältnis zwischen bestehenden Werken und Neuschöpfungen geht, wäre es zwar grundsätzlich denkbar, daß der nachfolgende Urheber – im Beispiel also der Kritiker oder der Künstler – mit dem ursprünglichen Urheber einen entsprechenden Nutzungsvertrag abschließt. Überlegt sich der nachfolgende Urheber, diesen Nutzungsvertrag abzuschließen, so berücksichtigt er dabei aber nur die Vorteile, die er selbst aus dem Nutzungsvertrag ziehen würde, nicht aber die Vorteile Dritter, die ihn für diese Vorteile nicht kompensieren würden. Dies führt dazu, daß der nachfolgende Urheber für die Nutzung eines bestehenden Werks eine geringere Zahlungsbereitschaft besitzt, als deren gesamtgesellschaftlicher Nutzen ist.[1731] Durch die Neuschöpfung von Werken entstehen sogenannte „positive externe Effekte",[1732] die der nachfolgende Urheber bei Abschluß eines Nutzungsvertrags mit dem ursprünglichen Urheber nicht berücksichtigt, das heißt nicht „internalisiert".[1733] Dies kann dazu führen, daß der nachfolgende Urheber ein bestehendes Werk nicht verwendet oder sogar überhaupt kein neues Werk schöpft, da er den daraus resultierenden Verlust geringer einschätzt, als der gesamtgesellschaftliche Verlust tatsächlich ist.[1734] Positive externe Effekte, die nicht internalisiert werden, können zu einer suboptimalen Produktion neuer Werke führen.[1735]

[1730] Vgl. *Loren*, 5 J. Intell. Prop. L. 1, 49 (1997); *Burk/Cohen*, S. 3.

[1731] *Dowell*, 86 Cal. L. Rev. 843, 864 (1998); *Loren*, 5 J. Intell. Prop. L. 1, 49 (1997); s. dazu auch *Landes/Posner*, 18 J. Legal Stud. 325, 358 f. (1989). Mit anderen Worten: Die gesamte Konsumentenrente, die aus dem Verzicht auf eine vertragliche Nutzungsbeschränkung herrührt, ist größer als die Rente des einzelnen potentiellen Urhebers, der vor der Entscheidung steht, ob er sich der vertraglichen Beschränkung unterwirft, *Lemley*, 87 Cal. L. Rev. 111, 170 (1999).

[1732] Ein externer Effekt tritt bei einer Handlung eines Konsumenten oder Produzenten auf, die andere Produzenten oder Konsumenten beeinflußt, sich aber nicht auf den Marktpreis auswirkt; *Pindyck/Rubinfeld*, S. 294. Die hier auftretenden positiven externen Effekte spiegeln sich nicht im Preis des Werks wieder und werden daher auch nicht durch den Preismechanismus gesteuert bzw. werden dem Urheber nicht über den Preis zugerechnet; s. *Müller*, S. 37.

[1733] *Loren*, 5 J. Intell. Prop. L. 1, 49 (1997); *Lemley*, 87 Cal. L. Rev. 111, 170 (1999).

[1734] *Lemley*, 87 Cal. L. Rev. 111, 170 (1999); *Cohen*, 97 Mich. L. Rev. 462, 547 (1998); *Burk/Cohen*, S. 3.

[1735] S. dazu *Lemley*, 75 Tex. L. Rev. 989, 1056 ff. (1997); *Gordon*, 82 Colum. L. Rev. 1600, 1630 f. (1982); *Cohen*, 97 Mich. L. Rev. 462, 547 (1998); *dies.*, 53 Vand. L. Rev. 1799, 1812 (2000).

Auch in anderen Fällen können positive externe Effekte ein Grund für urheberrechtliche Schrankenbestimmungen sein. Das Kopieren von Werken zu Unterrichtszwecken (s. § 53 Abs. 3 UrhG) kann zu einem höheren Bildungsniveau der Unterrichteten führen. Müßte der Lehrer vor dem Kopieren eines Zeitschriftenbeitrags für den Schulunterricht eine Erlaubnis des Urhebers einholen, würde dieser positive externe Effekt in dem entsprechenden Nutzungsvertrag nicht hinreichend berücksichtigt.[1736]

Urheberrechtliche Schrankenbestimmungen berücksichtigen damit positive externe Effekte, die in einem Schutzregime, das auf einem umfassenden Urheberrecht basiert, unberücksichtigt blieben. Zwar kann man die Auffassung vertreten, daß der nachfolgende Urheber in manchen der dargestellten Fälle die positiven externen Effekte, die durch seine Neuschöpfung entstehen, internalisieren kann, indem er später von den Dritten, bei denen diese positiven externen Effekte entstehen, ein entsprechendes Entgelt verlangt. Dies wird aber nicht in allen Fällen funktionieren. Teilweise kann der nachfolgende Urheber diese Dritten gar nicht identifizieren, teilweise – wie im Beispiel des § 53 Abs. 3 UrhG – sind die positiven externen Effekte diffus auf die Allgemeinheit verteilt.

Hier zeigen sich auch die Grenzen der herkömmlichen ökonomischen Analyse des Urheberrechts. So wird es Urheber geben, die gar kein Interesse an einer solchen Refinanzierung haben, da sie nicht wegen eines monetären Anreizes schöpferisch tätig werden. Dennoch können ihre Neuschöpfungen zu positiven externen Effekten für die Allgemeinheit führen.[1737] Erfolg im Massenmarkt ist nicht das einzige Kriterium, mit dem unsere Gesellschaft den Wert kultureller Schöpfungen mißt.[1738] Weiterhin wird es in einem System des umfassenden Urheberrechts ohne Schrankenbestimmungen Fälle geben, in denen ein Urheber die Einräumung eines Nutzungsrechts aus Gründen verweigert, die von der herkömmlichen ökonomischen Analyse nicht adäquat erfaßt werden. So kann sich ein Urheber aus prinzipiellen Gründen weigern, einem Dritten vertraglich das Recht einzuräumen, sein Werk zu parodieren[1739] oder zu

[1736] *Loren*, 5 J. Intell. Prop. L. 1, 52 (1997); s. a. *Benkler*, 53 Vand. L. Rev. 2063, 2077 (2000).

[1737] S. *Cohen*, 53 Vand. L. Rev. 1799, 1812 (2000). In diesen Fällen stellt sich unter ökonomischen Gesichtspunkten allerdings auch schon die Frage, warum solche Urheber überhaupt unter den urheberrechtlichen Schutz fallen.

[1738] *Cohen*, 53 Vand. L. Rev. 1799, 1814 (2000), die auf S. 1816 f. meint: „The imperfect correspondence between pricing and value to consumers is a vital structural underpinning of the copyright system."

[1739] Eine Parodie eines Werks kann nach deutschem Urheberrecht als freie Benutzung nach § 24 UrhG ohne Zustimmung des Urhebers zulässig sein; sie kann aber auch eine zustimmungspflichtige Bearbeitung i. S. d. § 23 UrhG sein; s. dazu *Loewenheim* in: Schricker (Hrsg.), UrhG-Kommentar, § 24 Rdnr. 22 ff. Bei Musikstücken ist § 24 Abs. 2 UrhG zu beachten.

zitieren.[1740] In solchen Fällen kann ein Interesse der Allgemeinheit daran bestehen, dem Dritten die Nutzung des Werks trotz der Weigerung des Urhebers zu erlauben.[1741] Für urheberrechtliche Schrankenbestimmungen bestehen auch außerökonomische Gründe, deren Erfassung in einer ökonomischen Analyse zumindest schwierig ist.[1742]

Die vorliegende Arbeit will und kann keine umfassende ökonomische Analyse urheberrechtlicher Schrankenbestimmungen liefern. Es zeigt sich aber, daß die Begründung und Reichweite urheberrechtlicher Schrankenbestimmungen unter dem Gesichtspunkt der ökonomischen Analyse des Urheberrechts noch zu großen Teilen unklar ist.[1743] Inwieweit die ökono-

[1740] Diesbezüglich für die meisten Fälle a. A. *Bell*, 76 N. C. L. Rev. 557, 601 ff. (1998); s. weiterhin *Posner*, 21 J. Legal Stud. 67 ff. (1992).

[1741] S. dazu *Merges*, 21 AIPLA Q.J. 305, 310 (1993); *ders.*, 12 Berkeley Tech. L. J. 115, 133 (1997); *Lemley*, 75 Tex. L. Rev. 989, 1060 (1997); *Gordon*, 82 Colum. L. Rev. 1600, 1632 ff. (1982). Allerdings kann nicht von jeder Weigerung des Urhebers, ein Nutzungsrecht einzuräumen, auf ein Marktversagen geschlossen werden, s. *Gordon*, a. a. O., S. 1634 f.

[1742] *Gordon*, 82 Colum. L. Rev. 1600, 1631 f. (1982); *Lunney*, 1 Tulane J. Tech. & Intell. Prop. Abs. 41 (1999). Dies erkennt auch *Bell*, 76 N. C. L. Rev. 557, 594 (1998), an. Gemeinhin geht die Mikroökonomie davon aus, daß die Menschen rational handeln und ihren Nutzen maximieren (*homo oeconomicus)*; Leitmodell ist der „resourceful, evaluative, maximizing man"; s. zu dieser „REMM-Hypothese" *Schäfer/Ott*, S. 56 ff.; *Eidenmüller*, S. 29 ff., jeweils auch zur Kritik daran; s. weiterhin *Posner*, Economic Analysis of Law, S. 3 ff. Gerade im Bereich des Urheberrechts ist diese Hypothese oftmals eine Fiktion. Eine neuere Richtung innerhalb der „Law and Economics"-Bewegung, die mitunter als „Behavioral Law and Economics" bezeichnet wird, versucht deshalb, die Schwachstellen dieser Hypothese zu beseitigen; s. dazu *Jolls/Sunstein/Thaler*, 50 Stan. L. Rev. 1471 ff. (1998); *Korobkin/Ulen*, 88 Cal. L. Rev. 1051 ff. (2000).

[1743] Neben den hier dargestellten gibt es noch andere Kritikansätze. Ein Ansatz firmiert unter dem Schlagwort „tragedy of the anticommons". Dabei handelt es sich um ein Konzept, das *Heller* 1998 in 111 Harv. L. Rev. 622 ff. (1998) auf die Eigentumsverteilung im postsozialistischen Rußland anwandte. Dem liegt die Analyse der „tragedy of the commons" – zu deutsch: Tragödie der Allmende – zugrunde: Die „tragedy of the commons" entsteht, wenn zu viele Personen berechtigt sind, eine knappe Ressource zu nutzen. Aufgrund fehlender „property rights" kommt es zu einer Übernutzung der Ressource, es entstehen negative externe Effekte. Durch die Schaffung von Privateigentum kann dieses Marktversagen behoben, die negativen externen Effekte „internalisiert" werden; s. dazu *Schäfer/Ott*, S. 520 f.; *Varian*, S. 569 ff.; *Lehmann*, GRUR Int. 1983, 356 ff.; *Pindyck/Rubinfeld*, S. 638 ff. *Heller* versteht unter einem „anticommons property" ein System von „property rights", in dem mehrere Berechtigte wirksame Ausschließlichkeitsrechte an *einer gemeinsamen* knappen Ressource haben; s. *Heller*, a. a. O., S. 668; *Depoorter/Parisi*, S. 13 f. Diese Ausschließlichkeitsrechte können sich überlappen oder nebeneinander bestehen. Eine „tragedy of the anticommons" entsteht – spiegelbildlich zur „tragedy of the commons" –, wenn zu viele Personen Ausschließlichkeitsrechte an einer Ressource haben. Verglichen mit dem sozialen Optimum kann es durch rationales Parallelverhalten der einzelnen Personen zu einer Unternutzung der Ressource kommen; s. dazu näher *Heller*, a. a. O., S. 622 ff., 670; *Parisi/Depoorter/Schulz*, S. 2. Dies liegt an negativen Externalitäten zwischen den Ausschließlichkeitsrechten: Die Ausübung eines Ausschließlichkeitsrechts kann den Wert eines anderen Ausschließlichkeitsrechts vermindern. Muß ein Nutzer von mehreren

mische Analyse überhaupt eine umfassende Erklärung von Schrankenbestimmungen liefern kann oder ob sich hier vielmehr die Grenzen der ökonomischen Analyse zeigen, ist ein umstrittenes und noch weithin offenes Feld. Es ist wohl inzwischen anerkannt, daß der Ansatz, urheberrechtliche Schrankenbestimmungen nur aufgrund prohibitiv hoher Transaktionskosten zu erklären, zu kurz greift.[1744] Bei einer solchen Be-

Inhabern von Ausschließlichkeitsrechten Nutzungsrechte erwerben, so werden diese nutzenmaximierend dafür einen Preis verlangen, der höher ist, als wenn die Ausschließlichkeitsrechte nur einem Inhaber zugeordnet wären; dies führt im Ergebnis zu einer Unternutzung, *Depoorter/Parisi*, S. 14 ff. Würden sich die Rechteinhaber zusammenschließen, so könnten sie durch Koordination einen höheren Gewinn erzielen; Koordinationsmöglichkeiten fehlen jedoch meist. Dadurch tritt ein Phänomen auf, das dem sog. „Gefangenendilemma" gleicht, s. *Depoorter/Parisi*, S. 19 f. Diese Probleme werden auch bei niedrigen Transaktionskosten nicht beseitigt, *Depoorter/Parisi*, S. 25. Dieses Modell läßt sich auch im immaterialgüterrechtlichen Bereich anwenden: *Depoorter/Parisi* wenden die Theorie im Urheberrecht, *Heller/Eisenberg*, 280 Science 698 ff. (1998), im Schnittfeld von biomedizinischer Forschung und Patentrecht an; s. a. *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1192 ff. (1998). Auch in DRM-Systemen könnte diese Analyse von Interesse sein. Die vertraglichen und technischen Schutzmechanismen von DRM-Systemen erlauben es, an einem digitalen Inhalt zahlreiche Ausschließlichkeitsrechte nebeneinander zu etablieren, *Elkin-Koren*, a. a. O., S. 1196 f. Die nebeneinander bestehenden Ausschließlichkeitsrechte könnten – im Sinne einer „tragedy of the anticommons" – zu einer Unternutzung der geschützten Werke führen. Nach diesem Ansatz dienen Schrankenbestimmungen dazu, ein Marktversagen zu korrigieren, das aus dem strategischen Verhalten von Rechteinhabern in „anticommons"-Situationen resultiert, *Depoorter/Parisi*, S. 25. Die Aussagen dieses Ansatzes treffen aber nur zu, wenn der Nutzer von mehreren Rechteinhabern Nutzungsrechte erwerben *muß*, diese Nutzungsrechte also komplementär sind, *Depoorter/Parisi*, S. 18. Eine ähnliche Theorie stellt *Cohen* auf. Danach sind die Nutzungen, die durch Schrankenbestimmungen erlaubt sind, wie die urheberrechtlich geschützten Werke ebenfalls öffentliche Güter: Da die Schrankenbestimmungen regelmäßig für jedermann gelten, seien sie nicht-exklusiv. Da ihre Ausübung durch eine Person die Ausübung durch eine andere Person in keiner Weise behindert, seien sie nicht-rivalisierend. Dies könne zu einer suboptimalen Ausnutzung der Schrankenbestimmungen führen, *Cohen*, 97 Mich. L. Rev. 462, 550 (1998). Überträgt man diese Analyse auf DRM-Systeme, so könnte man annehmen, daß DRM-Systeme zwar das Problem des öffentlichen Guts von Information beseitigen, nicht aber das Problem des öffentlichen Guts von Schrankenbestimmungen.

[1744] Auch die Thesen von *Calabresi* und *Melamed* zu „property" und „liability rules", die bei Schrankenbestimmungen mitunter verwendet werden (s. dazu oben Fn. 1658), sind umstritten. Im Bereich des Immaterialgüterrechts argumentiert *Merges*, daß bei hohen Transaktionskosten die Gewährung von „property rules" dazu führen kann, daß die Betroffenen selbst Institutionen schaffen, um Transaktionskosten zu senken. Danach trifft die These, daß bei hohen Transaktionskosten der Staat „liability rules" schaffen sollte, nicht immer zu. Vielmehr schaffen sich die Beteiligten ihre eigenen „liability rules". *Merges* nennt diese Entwicklung „Contracting into Liability Rules" und weist sie an urheberrechtlichen Verwertungsgesellschaften und Patent-Pools nach; *Merges*, 84 Cal. L. Rev. 1293 ff. (1996). Auch werden in den letzten Jahren zunehmend Einwände gegen die allgemeine Thesen von *Calabresi* und *Melamed* vorgebracht. Die Wahl zwischen „property rules" und „liability rules" hänge nicht nur von der Höhe der Transaktionskosten, sondern auch von einer Reihe anderer Faktoren ab. Teilweise wird argumentiert, daß nach verschiedenen Einsatzbereichen zu trennen sei;

trachtungsweise werden insbesondere die Auswirkungen des urheberrechtlichen Schutzes auf spätere Werkschöpfungen nicht hinreichend berücksichtigt. Ausführliche ökonomische Untersuchungen über die Auswirkungen des Urheberrechts auf den dynamischen Innovationsprozeß sind rar. Erst in den letzten Jahren wurde diesen Fragen zunehmend Aufmerksamkeit gewidmet.[1745] Dies führt dazu, daß solche Aspekte urheberrechtlicher Schrankenbestimmungen in der wissenschaftlichen Diskussion regelmäßig unterrepräsentiert sind.[1746]

Diese Betrachtung des Urheberrechts läßt sich auf DRM-Systeme übertragen. Wie das Urheberrecht führen DRM-Systeme zu einem Wohlfahrtsverlust durch Unternutzung („social welfalre loss due to underutilization"). Sie nehmen diesen Wohlfahrtsverlust in Kauf, weil sie dadurch eine Unterproduktion digitaler Inhalte („social welfare loss due to underproduction") verhindern.[1747] Auch in DRM-Systemen muß daher grundsätzlich ein Ausgleich zwischen diesen beiden Polen – Unterproduktion und Unternutzung beziehungsweise Anreiz zur Inhalteproduktion und Zugang zum produzierten Inhalt – gefunden werden. Ein solcher Ausgleich wäre nur dann nicht erforderlich, wenn das Unternutzungsproblem in DRM-Systemen auf andere Weise gelöst werden könnte. Eine weitgehende Preisdiskriminierung verspricht genau dies.[1748] Es erscheint jedoch mehr als fraglich, ob man der Ansicht, daß eine Preisdiskriminierung den „deadweight loss" in DRM-Systemen verhindern könnte, angesichts ihrer theoretischen Brüche derzeit folgen sollte.[1749] Folgt man der Ansicht nicht, muß in DRM-Systemen ein Ausgleich zwischen Unterpro-

so legen *Kaplow/Shavell*, 109 Harv. L. Rev. 713 ff. (1996), dar, daß in der Regel (aber nicht immer) bei der Regulierung negativer Externalitäten „liability rules" und bei der Regulierung von Verfügungsrechten an Sachen „property rules" zu bevorzugen seien. Andere bringen vor, daß unter gewissen Voraussetzungen bei geringen Transaktionskosten entgegen *Calabresi* und *Melamed* „liability rules" zu bevorzugen seien; s. dazu näher *Ayres/Talley*, 104 Yale L. J. 1027 ff., 1058 ff. (1995); kritisch *Merges*, a. a. O., S. 1304 ff.; *Kaplow/Shavell*, 105 Yale L. J. 221 ff. (1995); weitere neuere Beiträge zur Arbeit von *Calabresi* und *Melamed* finden sich in einem Tagungsband des Yale Law Journal ab 106 Yale Law Journal 2091 (1997). Aus diesen Gründen lassen sich die Thesen *Calabresis* und *Melameds* im vorliegenden Zusammenhang nicht unkritisch übernehmen; ebenso *Cohen*, 97 Mich. L. Rev. 462, 502 f. (1998).

[1745] S. aber *Lemley*, 75 Tex. L. Rev. 989 ff. (1997). Auf die fehlende Durchdringung dieser Frage weist auch *Kitch*, 53 Vand. L. Rev. 1727, 1738 f. (2000), hin.

[1746] Ebenso *Cohen*, 97 Mich. L. Rev. 462, 544 (1998); s. a. *Perlman*, 53 Vand. L. Rev. 1831, 1838 f. (2000); *Dreyfuss*, 53 Vand. L. Rev. 1821, 1825 (2000). *Cohen*, 53 Vand. L. Rev. 1799, 1817 (2000), meint gar: „Where complexity is central […] and models overly reductionist, economic modeling may do more harm than good. It may cause harm, in particular, if it causes us to focus on and emphasize those aspects of the process that are least important – to overlook what is most vital in favor of what is easier to describe or model."

[1747] S. dazu oben Teil 3, A III 2 c bb.

[1748] S. dazu oben Teil 3, A III 3.

[1749] S. dazu oben Teil 3, B I 1 b.

duktion und Unternutzung geschaffen werden. Selbst wenn man der Ansicht folgt, muß man immer noch untersuchen, ob in dem Modell eines preisdiskriminierenden DRM-Systems alle relevanten Faktoren urheberrechtlicher Schrankenbestimmungen berücksichtigt werden.

Wie die vorstehende Analyse gezeigt hat, ist dies nicht der Fall. Die Gründe für eine Beschränkung des Schutzes in DRM-Systemen können vielgestaltig sein. Würden DRM-Systeme einen umfassenden Schutz verleihen, so müßte für jede Nutzung digitaler Inhalte ein entsprechender Nutzungsvertrag abgeschlossen werden. Bei diesen Nutzungsverträgen würden jedoch positive externe Effekte nicht berücksichtigt, was zu einer Unterproduktion digitaler Inhalte führen kann. Daneben wird ein Inhalteanbieter den Abschluß eines Nutzungsvertrags mitunter aus Gründen verweigern, die mit dem herkömmlichen Instrumentarium der ökonomischen Analyse schwer erfaßt werden können.

Es zeigt sich, daß der Schutz in DRM-Systemen in vielerlei Hinsicht mit dem urheberrechtlichen Schutz vergleichbar ist und in beiden Fällen eine Beschränkung dieses Schutzes notwendig erscheint. Im Rahmen der vorliegenden Arbeit ist es nicht möglich, im einzelnen zu untersuchen, in welchen Fällen aus ökonomischer Sicht der Schutz in DRM-Systemen beschränkt werden sollte und inwieweit zu diesem Zweck urheberrechtliche Schrankenbestimmungen auf DRM-Systeme anwendbar sein sollten. Es soll nur gezeigt werden, daß es aus ökonomischer Sicht gewichtige und unterschiedliche Gründe dafür gibt, den Schutz von DRM-Systemen zu beschränken. Ohne eine Beschränkung kann ein Inhalteanbieter den DRM-Schutz entsprechend seinen eigenen Präferenzen maximieren; dabei werden aber Interessen Dritter oder der Allgemeinheit vernachlässigt. In diesem Umfeld könnte sich die Bedeutung urheberrechtlicher Schrankenbestimmungen wandeln: Schrankenbestimmungen, die auf prohibitiv hohen Transaktionskosten aufbauen, werden in DRM-Systemen an Bedeutung verlieren. Schrankenbestimmungen, die andere Zielsetzungen verfolgen, insbesondere Interessen Dritter oder der Allgemeinheit wahren sollen, werden dagegen wichtiger werden.[1750]

[1750] *Merges*, 12 Berkeley Tech. L. J. 115, 134 (1997), der auf S. 135 meint: „Essentially, my point is that in the realm of cyberspace […,] rather than focusing on whether a market might form for the copyrighted work, we should assume it will. The only relevant questions are: (1) which class(es) of users should be allowed to bypass the presumptive market; and (2) how much revenue should the copyright holder be forced to forego to serve the goals of fair use?". S. weiterhin *Bell*, 76 N. C. L. Rev. 557, 584 (1998). Zum Verhältnis von Effizienz und Verteilungsgerechtigkeit allgemein s. die Nachweise oben Fn. 1551.

b) Beschränkung durch den Markt oder den Gesetzgeber

aa) Allgemeines

Bevor man aus den vorangegangenen Ausführungen schließen kann, daß es notwendig ist, den Schutz von DRM-Systemen gesetzlich zu beschränken, ist zu untersuchen, ob solche Beschränkungen nicht auch durch andere Institutionen als den Gesetzgeber erreicht werden könnten. So könnten die Probleme eines zu weitreichenden DRM-Schutzes schon durch den Wettbewerb zwischen Anbietern verschiedener Inhalte und verschiedener DRM-Systeme gelöst werden. Tatsächlich wird in den USA von vielen vertreten, das Einschreiten des Gesetzgebers oder der Gerichte sei aus diesem Grund unnötig. In einem Wettbewerbsmarkt würden Anbieter keine überbordenden Schutzmaßnahmen einsetzen, da diese zu starken Nutzungsbeschränkungen führen, die Konsumenten dies nicht akzeptieren, daher auf andere Anbieter ausweichen und damit die Nachfrage nach zu stark geschützten Inhalten sinkt.

Diese Argumentation läßt sich sowohl hinsichtlich vertraglicher als auch hinsichtlicher technischer Schutzmaßnahmen in DRM-Systemen anführen. Hinsichtlich vertraglicher Schutzmechanismen meint Judge *Easterbrook* in der ProCD-Entscheidung,[1751] Nutzungsbedingungen seien genauso Teil des verkauften „Produkts" wie dessen unmittelbare Qualitätseigenschaften. Der Wettbewerb unter mehreren Anbietern könne – neben dem Preis und der Qualität des Produkts – auch über unterschiedlich liberale Nutzungsbedingungen ausgetragen werden.[1752] Hinsichtlich technischer Schutzmaßnahmen wird angeführt, daß verschiedene Inhalteanbieter und verschiedene Anbieter von DRM-Systemen unterschiedlich restriktive technische Schutzmaßnahmen verwenden würden. Dies führe zu einer unterschiedlichen Nachfrage nach diesen Schutzmaßnahmen und damit zu einem Wettbewerb um das Schutzniveau in DRM-Systemen. Die Konsumenten würden jene Schutzmaßnahme aussuchen, die ihren Präferenzen am ehesten entsprechen. In einem Wettbewerbsmarkt werde das – nur hypothetische – Problem eines zu weitreichenden DRM-Schutzes durch den Wettbewerb gelöst.[1753] Diese These wird im folgenden hinsichtlich des vertraglichen Schutzes (dazu unten bb) und des technischen Schutzes (dazu unten cc) auf ihre Stichhaltigkeit untersucht.

[1751] S. dazu oben Teil 3, A III 3 b aa.

[1752] ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1453 (7th Cir. 1996); ähnlich *Easterbrook*, 1996 U. Chi. Legal F. 207, 214 f.; *O'Rourke*, 82 Minn. L. Rev. 609, 703 (1998); *dies.*, 12 Berkeley Tech. L. J. 53, 83 (1997); *Bell*, 76 N.C. L. Rev. 557, 608 (1998); *Lemley*, 35 Jurimetrics J. 311, 320 (1995); *Monroe*, 1 Marq. Intell. Prop. L. Rev. 143, 149 (1997); *Gomulkiewicz*, 13 Berkeley Tech. L. J. 891, 901 (1998); *Elkin-Koren/Salzberger*, 19 Int. Rev. L. & Econ., 553, 570 (1999); *Posner*, Economic Analysis of Law, S. 127 f.

[1753] *Post*, 52 Stan. L. Rev. 1439, 1453 ff. (2000); *Samuelson*, 14 Berkeley Tech. L. J. 519, 566 (1999); s. weiterhin *Bell*, 76 N.C. L. Rev. 557 ff. (1998). *Post* kritisiert dabei

bb) Vertraglicher Schutz

(1) **Allgemeines.** Verwendet ein Inhalteanbieter in einem DRM-System Nutzungsverträge, die für den Nutzer vergleichsweise ungünstig sind, weil sie ihm beispielsweise die Ausübung urheberrechtlicher Schrankenbestimmungen untersagen, erscheint fraglich, ob der Inhalteanbieter damit am Wettbewerbsmarkt Erfolg haben wird. In DRM-Systemen könnte ein Wettbewerb zwischen unterschiedlichen Nutzungsverträgen entstehen.[1754] Nach dieser Ansicht reflektieren Nutzungsverträge – wie allgemein Verträge – lediglich die Interessen der Vertragsparteien.[1755] Wenn ein Konsument einen Vertrag abschließe, der ihm nur wenige Vorteile bringe, so sei dies nicht zu beanstanden, solange dadurch keine Dritten geschädigt würden.[1756] Dies sei Ausdruck der Vertragsfreiheit. Selbst wenn ein DRM-Nutzungsvertrag für den Nutzer „ungünstig"[1757] sei, müsse dies hingenommen werden, da sich der Nutzer ja selbst auf den Vertrag eingelassen habe. In einer Marktwirtschaft werde der Konsument nicht durch eine richterliche oder gesetzliche Kontrolle von Nutzungsbedingungen, sondern durch den Wettbewerb zwischen verschiedenen Anbietern geschützt.[1758] Der Wettbewerb könne dazu führen, daß sich DRM-Nutzungsverträge, die die Präferenzen der Nutzer zu wenig berücksichtigen, am Markt nicht durchsetzen.

Im folgenden soll untersucht werden, ob diese Thesen unter ökonomischen Gesichtspunkten zutreffen. Nutzungsverträge in DRM-Systemen sind regelmäßig allgemeine Geschäftsbedingungen. Die Frage, ob ein Wettbewerb unterschiedlicher Nutzungsverträge möglich erscheint, ist ein spezieller Anwendungsfall des allgemeineren Problems eines Wettbewerbs allgemeiner Geschäftsbedingungen. In Deutschland wurde insbesondere in den 70er Jahren vor Erlaß des AGB-Gesetzes vertreten, ein AGB-Gesetz sei unnötig, da der Verbraucher durch einen Wettbewerb unterschiedlicher

---

Lessig's Ausführungen zu DRM-Systemen in *Lessig*, S. 122 ff. Die Kritik ist insofern berechtigt, als *Lessig* auf die Frage, ob das weitreichende Schutzpotential von DRM-Systemen mit den damit verbundenen Gefahren überhaupt ausgenützt werden wird, nicht eingeht. Insgesamt vernachlässigt *Lessig* in seiner – trotz alledem bahnbrechenden – Analyse zum Verhältnis zwischen technischer und rechtlicher Regulierung im Internet die Einflüsse des Wettbewerbs als Beschränkungsmechanismus technischer Regulierung.

[1754] So die unter Fn. 1752 Genannten.

[1755] *Bell*, 76 N. C. L. Rev. 557, 591 (1998).

[1756] *Merges*, 12 Berkeley Tech. L. J. 115, 126 (1997): „If a licensee wants to five up its future right to use information in exchange for the present right to use it, why not permit such action? Unless third parties are harmed, this tradeoff seems reasonable".

[1757] Dabei ist schon problematisch, nach welchem Referenzsystem beurteilt werden soll, wann ein Nutzungsvertrag „ungünstig" ist.

[1758] ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1453 (7th Cir. 1996). Die einzige Grenze – in den USA – bilde das kodifizierte Vertragsrecht des UCC sowie die Sittenwidrigkeit, *ebda.*, S. 1449.

allgemeiner Geschäftsbedingungen geschützt werde.[1759] Dafür hat sich der Begriff „Konditionenwettbewerb" eingebürgert. Fraglich ist, ob ein solcher Konditionenwettbewerb realistisch ist.[1760]

(2) **Asymmetrische Information.** Die These, ein Konditionenwettbewerb sei möglich und daher ein Einschreiten des Gesetzgebers oder der Gerichte unnötig, baut implizit auf dem Modell der vollständigen Konkurrenz auf. Danach verfügen alle Marktteilnehmer über die vollständigen Informationen, die sie zur Entscheidungsfindung benötigen.[1761] Unter dieser Voraussetzung ist die Entscheidung der Marktteilnehmer, eine bestimmte vertragliche Bindung einzugehen, zu respektieren. In Geschäften des Massenmarktes, die auf allgemeinen Geschäftsbedingungen basieren, ist jedoch fraglich, ob diese Prämisse zutrifft. In einem solchen Umfeld wissen bestimmte Marktteilnehmer oft mehr als andere – es treten sogenannte „Informationsasymmetrien" auf.[1762]

Informationsasymmetrien könnten einen wirksamen Konditionenwettbewerb verhindern. Um dies zu zeigen, muß etwas ausgeholt werden. Die Auswirkungen asymmetrischer Informationsverteilung lassen sich an einem klassischen Beispiel verdeutlichen, das in der U.S.-amerikanischen Literatur als „market for lemons"-Problem bekannt ist und erstmals von *Akerlof* beschrieben wurde.[1763] In diesem Beispielsmarkt bieten Verkäufer Gebrauchtwagen in zwei unterschiedlichen Qualitätsstufen in jeweils gleicher Menge an: Einerseits gut erhaltene Autos (sogenannte „plums"), andererseits schlecht erhaltene (sogenannte „lemons").[1764] Die Verkäufer eines guten Gebrauchtwagens sind bereit, ihn für 2.000 Euro zu verkaufen, die Verkäufer eines schlechten Wagens wollen sich für 1.000 Euro von ihm trennen. Die Käufer sind bereit, 2.400 Euro für einen guten und 1.200 Euro für einen schlechten Wagen zu bezahlen. Wenn es für die Käufer unproblematisch ist, die Qualität der Wagen festzustellen, wird es auf dem Markt keine Probleme geben: Die guten Wagen werden für einen Preis zwischen 2.000 Euro und 2.400 Euro, die schlechten Wagen für einen Preis zwischen 1.000 Euro und 1.200 Euro verkauft. Dadurch entsteht eine Pareto-effiziente Güterverteilung.[1765]

[1759] So insbesondere *Grunsky*, BB 1971, 1113, 1115 ff.; s. dazu auch *Schäfer/Ott*, S. 478 f.

[1760] Eine grundlegende Analyse des Konditionenwettbewerbs in deutscher Sprache liefert *Adams* in: Neumann (Hrsg.), S. 655 ff.

[1761] Zu den weiteren Voraussetzungen des Modells der vollständigen Konkurrenz s. oben Fn. 1671.

[1762] *Pindyck/Rubinfeld*, S. 595; *Cooter/Ulen*, S. 43.

[1763] *Akerlof*, 84 Quarterly Journal of Economics 488 ff. (1970). S. zum folgenden *Varian*, S. 628 ff.; *Pindyck/Rubinfeld*, S. 596 ff.; *Richter/Furubotn*, S. 236 ff.; *Schäfer/Ott*, S. 321 ff.; *Müller*, S. 39 ff.

[1764] Im Amerikanischen ist „Plum" die umgangssprachliche Bezeichnung für einen guten und „Lemon" die Bezeichnung für einen schlechten Gebrauchtwagen.

[1765] Zum Begriff der Pareto-Effizienz s. oben Fn. 1553.

Anders ist die Lage, wenn es für die Käufer schwierig ist, die Qualität der Gebrauchtwagen einzuschätzen. Dann fehlen ihnen – im Gegensatz zu den Verkäufern – die Informationen, die eigentlich für die Transaktion erforderlich wären; es liegt eine Informationsasymmetrie vor. Für potentielle Käufer ist es oft schwierig, durch das bloße Betrachten eines Gebrauchtwagens dessen Qualität zu beurteilen. Daher können die Käufer den Wert des Gebrauchtwagens nur schätzen. Da die Wahrscheinlichkeit, daß es sich um einen guten oder schlechten Wagen handelt, im Beispielsmarkt gleich groß ist,[1766] mitteln die Käufer ihre Vorbehaltspreise[1767] für beide Wagenarten und sind bereit, für alle Wagen einheitlich 1.800 Euro zu zahlen, da

(1.200 Euro + 2.400 Euro) x 0,5 = 1.800 Euro.

Zu diesem Preis sind die Verkäufer guter Gebrauchtwagen aber nicht bereit, ihre Wagen zu verkaufen, verlangen sie doch mindestens 2.000 Euro. Auf einem solchen Markt mit asymmetrischer Informationsverteilung werden die guten Gebrauchtwagen also niemals verkauft. Zwar wären die Käufer bereit, den entsprechenden Kaufpreis für das höherwertige Produkt zu zahlen, sie können aber das höherwertige Produkt nicht von dem schlechteren Produkt unterscheiden.[1768] Es besteht ein externer Effekt zwischen den Verkäufern der guten und der schlechten Wagen: Wenn ein Verkäufer versucht, einen schlechten Wagen zu verkaufen, beeinflußt das die Wahrnehmung der Käufer über die Qualität des durchschnittlichen Wagens auf dem Markt. Dies senkt den Preis, den die Käufer bereit sind, für den durchschnittlichen Wagen zu zahlen, und benachteiligt jene Verkäufer, die gute Wagen verkaufen wollen. Um überhaupt Wagen verkaufen zu können, werden Verkäufer, die bisher Gebrauchtwagen guter Qualität verkaufen wollten, daher die Qualität ihrer zu verkaufenden Wagen senken. Mit der Verschlechterung der durchschnittlichen Produktqualität sinkt wiederum die Erwartung der Käufer, was zu einer weiteren Verringerung der Zahlungsbereitschaft führt.[1769] Es findet eine negative Auslese („adverse selection"), ein „race to the bottom" statt, in dem die Erzeugnisse von geringer Qualität jene von hoher Qualität verdrängen. Der Markt richtet sich nach der schlechtesten Qualität.[1770] Damit führen Informationsasymmetrien zu einem Marktversagen.[1771]

1766 Es wird eine gleich große Anzahl guter wie schlechter Wagen angeboten.

1767 Zu diesem Begriff s. oben bei Fn. 1547.

1768 *Varian*, S. 629; *Pindyck/Rubinfeld*, S. 598.

1769 *Schäfer/Ott*, S. 323 f.

1770 *Varian*, S. 632; *Pindyck/Rubinfeld*, S. 598; *Schäfer/Ott*, S. 323 f.; *Müller*, S. 56.

1771 *Varian*, S. 629 f. Zum Begriff und anderen Fällen des Marktversagens s. oben Fn. 1502. Grundsätzlich bestehen allerdings Möglichkeiten, dieses Marktversagen aus Informationsasymmetrien zu beheben. So können die Anbieter von Produkten hoher Qualität den Käufern signalisieren, welche Qualität ihr Produkt hat. Dies ermöglicht

Dieses „market for lemons"-Modell kann auf allgemeine Geschäftsbedingungen übertragen werden.[1772] Dazu ist zwischen „guten" und „schlechten" Geschäftsbedingungen zu unterscheiden. „Gute" Geschäftsbedingungen sind solche, die einem vollständig und individuell ausgehandelten Vertrag zwischen dem Verwender und dem Kunden entsprechen. Im Vergleich dazu benachteiligen „schlechte" Geschäftsbedingungen den Kunden, wenn man die Transaktion in ihrer Gesamtheit betrachtet.[1773] Ein Wettbewerb unterschiedlicher Geschäftsbedingungen – und damit auch unterschiedlicher Nutzungsverträge in DRM-Systemen – würde funktionieren, wenn der Kunde die Geschäftsbedingungen der unterschiedlichen Anbieter vergleichen und dies seine Kaufentscheidung beeinflussen würde. Zu diesem Zweck müßte er unter anderem vergleichen, wie in den einzelnen Geschäftsbedingungen die jeweiligen Schadensrisiken geregelt sind, mit welcher Wahrscheinlichkeit sich diese Risiken bei ihm verwirklichen werden und wie hoch in diesem Fall der zu erwartende Schaden wäre. Die daraus ermittelte Bewertung der einzelnen Geschäftsbedingung müßte zum jeweiligen Produktpreis addiert werden. Nach einem Vergleich der unterschiedlichen Summen würde der Kunde die für ihn „beste" Geschäftsbedingung wählen. Unter diesen Voraussetzungen wäre ein Wettbewerb um allgemeine Geschäftsbedingungen möglich.[1774]

Auch wenn diese Anforderungen modellhaft überspitzt sein mögen, zeigt sich die Fragwürdigkeit der These, bei allgemeinen Geschäftsbedingungen im Massenmarkt sei ein Konditionenwettbewerb möglich. Die Lektüre und der Vergleich mehrerer Geschäftsbedingungen verursacht

---

den Käufern, gute Qualität von schlechter Qualität zu unterscheiden und beseitigt damit das Marktversagen. Ein Beispiel für ein solches Signal ist das Anbieten einer Garantie (s. dazu *Varian*, S. 636 f.; *Pindyck/Rubinfeld*, S. 601 ff.; *Richter/Furubotn*, S. 240) oder das Aufbauen einer guten Reputation (s. dazu *Schäfer/Ott*, S. 472 ff.; *Richter/Furubotn*, S. 240).

[1772] S. zum folgenden *Schäfer/Ott*, S. 479 f.; *Adams* in: Neumann (Hrsg.), S. 655, 664 f.; *Katz* in: Newman (Hrsg.), Band 3, S. 502, 504 f.

[1773] „Gute" Geschäftsbedingungen maximieren nicht unbedingt die rechtliche Position des Kunden. Denn jede Besserstellung des Kunden erhöht mittelbar den Preis des angebotenen Produkts. „Gute" Geschäftsbedingungen sind vielmehr solche Bedingungen, die den Gesamtnutzen des Kunden maximieren, der vom Produktpreis, von der Qualität des angebotenen Produkts sowie dem Inhalt der Geschäftsbedingungen abhängt; s. *Schäfer/Ott*, S. 479. Dahinter steht das Modell des „vollständigen Vertrags". In diesem Modell einigen sich die Vertragsparteien vor Vertragsabschluß über die Zuordnung aller Risiken, die mit der Durchführung des Vertrags verbunden sind. Dabei werden die Vertragsparteien die Risiken nicht beliebig unter sich verteilen. Vielmehr wird bei rationalem Verhalten jede Vertragspartei die Risiken übernehmen, die sie im Vergleich zur anderen Vertragspartei mit einem geringeren Aufwand vermeiden, versichern oder auf sonstige Weise bewältigen kann. Dies liegt daran, daß der Preisaufschlag, den diese Vertragspartei für die Übernahme des Risikos verlangt, geringer sein wird, als wenn die andere Vertragspartei das Risiko übernimmt. Vollständige Verträge sind Pareto-effizient. S. dazu *Schäfer/Ott*, S. 373 ff.; *Cooter/Ulen*, S. 205 f.

[1774] *Schäfer/Ott*, S. 480.

für den Konsumenten Kosten, die aufzubringen sich nicht lohnt.[1775] Der Vergleich unterschiedlicher Geschäftsbedingungen ist ungleich schwieriger als der Vergleich unterschiedlicher Preise.[1776] Die Wahrscheinlichkeit, daß beim Konsumenten ein in den Geschäftsbedingungen unterschiedlich geregeltes Schadensereignis eintritt, ist so gering, daß die Kosten, diese unterschiedlichen Regelungen zu identifizieren und zu vergleichen, außer Verhältnis zu dem sich daraus ergebenden Nutzen stehen.[1777] Die in allgemeinen Geschäftsbedingungen geregelten Risiken realisieren sich beim einzelnen Konsumenten oftmals entweder erst nach langer Zeit oder aber gar nicht. Geschäftsbedingungen sind damit Güter, deren Qualität sich dem Konsumenten nur schwer oder erst nach langer Zeit erschließen.[1778] Während es sich für den Konsumenten aus diesen Gründen nicht lohnt, sich näher mit den Geschäftsbedingungen zu beschäftigen, stellt sich die Lage beim Verwender regelmäßig anders dar: Anders als der Konsument schließt er eine hohe Anzahl gleicher Verträge ab, während der Konsument mit einem einzelnen Anbieter nur vereinzelt Verträge abschließt. Dadurch besteht für den Anbieter ein größerer Anreiz, sich über die rechtlichen Auswirkungen der Geschäftsbedingungen zu informieren, als für den Konsumenten.[1779] Dies führt zu einer Informationsasymmetrie.

Die hohen Informations- und Suchkosten beim Vergleich unterschiedlicher Geschäftsbedingungen schließen es aus, daß die Konsumenten ihre Kaufentscheidung von der Ausgestaltung der jeweiligen Geschäftsbedingung abhängig machen.[1780] Zwar wären die Kunden bereit, für ein Pro-

---

[1775] *Basedow* in: Münchener Kommentar, AGBG Einl. Rdnr. 5; *Köndgen*, NJW 1989, 943, 946 f.; *Adams* in: Neumann (Hrsg.), S. 655, 662 f.; *Kötz*, ZVersWiss 1993, 57, 66; *Schlosser* in: Staudinger (Begr.), Einl. zum AGBG Rdnr. 4; *Ulmer* in: Ulmer/Brandner/Hensen (Hrsg.), Einl. Rdnr. 6.

[1776] *Cohen*, 97 Mich. L. Rev. 462, 488 (1998).

[1777] Vgl. *Adams* in: Neumann (Hrsg.), S. 655, 663; *Basedow* in: Münchener Kommentar, AGBG Einl. Rdnr. 5; *Kötz*, S. A 32. Die Informationskosten können für den Konsumenten sogar den Wert der mit dem *gesamten* Vertrag verbundenen Vorteile übersteigen.

[1778] Man kann daher allgemeine Geschäftsbedingungen auch als „Erfahrungsgüter" betrachten. Ein Erfahrungsgut ist ein Gut, dessen Charakteristika der Konsument erst einschätzen kann, wenn er es benutzt; s. *Shapiro/Varian*, S. 5, 85 f.; *Schäfer/Ott*, S. 466; *Detering*, S. 17 ff., auch zu *Arrows* Informationsparadoxon. Zu Geschäftsbedingungen als Erfahrungsgut s. *Schäfer/Ott*, S. 324; *Adams* in: Neumann (Hrsg.), S. 655, 663 ff.; wohl auch *Coester* in: Staudinger (Begr.), § 9 AGBG, Rdnr. 94; s. weiterhin *Wein*, ZVersWiss 86 (1997), 103, 111.

[1779] *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1182 (1998); s. a. *Wolf* in: Wolf/Horn/Lindacher (Hrsg.), Einl. Rdnr. 3; *Kötz*, S. A 31 f.

[1780] Es kann daher auch nicht argumentiert werden, die Konsumenten würden die Geschäftsbedingungen nicht vergleichen, weil sie diesen bei der Bildung der persönlichen Präferenzen keine große Bedeutung beimessen würden. Dies wäre eine petitio principii: Die Konsumenten verfügen gar nicht über die notwendigen Informationen, um beurteilen zu können, ob die Geschäftsbedingungen für die Präferenzbildung relevant sind oder nicht; ebenso *Cohen*, 97 Mich. L. Rev. 462, 488 Fn. 88 (1998).

dukt mit „guten" Geschäftsbedingungen einen höheren Preis zu zahlen, sie können aber nicht zwischen „guten" und „schlechten" Geschäftsbedingungen unterscheiden.[1781] Für den Kunden sind aus diesen Gründen die unmittelbaren Produkteigenschaften und der Preis viel wichtiger als die Einzelheiten der Geschäftsbedingungen, mag diese subjektive Bewertung auch nicht mit der objektiven Gewichtung übereinstimmen.[1782] Wenn ein Verwender seine Geschäftsbedingungen „verschlechtert", spart er dadurch Kosten und erhöht seinen Gewinn. Mit einer Abwanderung von Konsumenten muß er nicht rechnen, weil den Konsumenten wegen der hohen Informationskosten gar nicht bewußt ist, daß die Konkurrenz ein besseres Preis-Leistungs-Verhältnis bietet.[1783] Wie im dargestellten „market for lemons"-Modell wird der Verwender „guter" Geschäftsbe-

[1781] Vgl. *Adams* in: Neumann (Hrsg.), S. 655, 665. Dagegen wird mitunter eingewandt, der Anbieter werde in einem DRM-System dem Nutzer die Nutzungsbedingungen in verständlicher Weise vermitteln, da er ein starkes Interesse daran habe, daß der Nutzer die Nutzungsbedingungen versteht. Nur so sei eine wirksame Preisdiskriminierung möglich; s. *O'Rourke*, 12 Berkeley Tech. L. J. 53, 85 f. (1997); *Gomulkiewicz*, 13 Berkeley Tech. L. J. 891, 901 Fn. 58 (1998). Dabei ist jedoch zu beachten, daß Nutzungsverträge nicht die einzige Möglichkeit in DRM-Systemen sind, um eine Preisdiskriminierung durchzuführen; Anbieter können zu diesem Zweck auch technische Schutzmaßnahmen einsetzen. Weiterhin ist auch das Preisdiskriminierungs-Argument selbst mit Schwächen behaftet, s. oben Teil 3, B I 1 b.

[1782] *Müller*, S. 289.

[1783] *Schäfer/Ott*, S. 480; *Adams* in: Neumann (Hrsg.), S. 655, 664 f. Gegen diese Analyse könnte man einwenden, daß der Konsument zwar wegen der Informationsasymmetrie die unterschiedlichen Geschäftsbedingungen nicht vergleichen könne; dies sei aber gar nicht notwendig, da nachteilige Klauseln für den Konsumenten zu einem günstigeren Preis des Produkts führen könnten. Die Qualität der Geschäftsbedingungen spiegelt sich also im Preis des Produkts wider (sogenanntes „Preisargument"; s. dazu *Brandner* in: Ulmer/Brandner/Hensen (Hrsg.), § 9 Rdnr. 109 f.; *Basedow* in: Münchener Kommentar, § 9 AGBG Rdnr. 19; *Coester* in: Staudinger (Begr.), § 9 AGBG, Rdnr. 94 ff.; *Kötz*, S. A 27 ff.; *Kliege*, S. 48 ff.). Zwar trifft es grundsätzlich zu, daß sich ungünstigere Geschäftsbedingungen in günstigeren Preisen niederschlagen und daher für den Kunden auch vorteilhaft sein können. Das hier vorgestellte Modell hat jedoch eine „schlechte" Geschäftsbedingung anders definiert: Eine „schlechte" Geschäftsbedingung liegt vor, wenn das *Bündel* aus Produkteigenschaften, Produktpreis und begleitenden Geschäftsbedingungen eine Allokation vornimmt, die im Vergleich zur Allokation eines vollständigen Vertrags für den Kunden nachteilhaft ist; s. dazu oben bei Fn. 1773. Mit anderen Worten: Der Einwand, daß Geschäftsbedingungen, die für den Kunden ungünstig sind, zu einem für ihn günstigeren Preis führen können, ist in dem hier angewandten Modell schon berücksichtigt. Daneben ist zu beachten, daß es regelmäßig nicht nachweisbar ist, ob ein Anbieter eine Kostensenkung, die bei ihm aufgrund veränderter Geschäftsbedingungen eingetreten ist, überhaupt oder in vollem Umfang an den Kunden weitergibt; s. dazu ausführlich *Kliege*, S. 54 ff.; vgl. weiterhin *Coester* in: Staudinger (Begr.), § 9 AGBG, Rdnr. 94; *Kötz*, S. A 28. Auch nach der Rechtsprechung des BGH zum AGB-Recht kann die unangemessene Benachteiligung des Vertragspartners grundsätzlich nicht mit einem entsprechend geringeren Preis gerechtfertigt werden, BGHZ 22, 90, 98; NJW 1993, 2442, 2444; VersR 1997, 319. Jedoch wird dieser Grundsatz von der Rechtsprechung in einigen Fällen durchbrochen, s. *Coester*, a. a. O., Rdnr. 95 ff.; *Basedow*, a. a. O., Rdnr. 19 f.

dingungen gezwungen, auf das kostenminimierende Niveau „schlechter" Geschäftsbedingungen umzustellen.[1784] Es findet ein „race to the bottom" statt. Die prohibitiv hohen Transaktionskosten führen zu einer Informationsasymmetrie und damit zu einem Marktversagen.[1785] Für die Anbieter fehlt der Anreiz, bei der Ausgestaltung der Geschäftsbedingungen in einen Überflügelungswettbewerb zum Vorteil der Verbraucherseite einzutreten.[1786]

Die Informationsasymmetrie führt auch dazu, daß die These von der Allokationseffizienz von Verträgen bei allgemeinen Geschäftsbedingungen nicht zutrifft: Kann eine Vertragspartei aufgrund fehlender Informationen nicht einschätzen, ob die beabsichtigte Transaktion für sie nutzenmaximierend ist, und stellt der Markt diese Informationen auch nicht zur Verfügung, kann nicht davon ausgegangen werden, daß eine solche Transaktion Pareto-effizient ist.[1787] Jedenfalls in Konsumgütermärkten ist der Wettbewerb nicht in der Lage, von sich aus zu einer angemessenen Ausgestaltung von allgemeinen Geschäftsbedingungen gegenüber Endverbrauchern beizutragen.[1788] Daraus erklärt sich die Notwendigkeit einer gesetzlichen Kontrolle allgemeiner Geschäftsbedingungen.[1789] Um das Problem der Informationsasymmetrie zu beseitigen, sieht das Gesetz über allgemeine Geschäftsbedingungen Vorschriften vor, die den Verwender darin beschränken, welche Klauseln er in Geschäftsbedingungen verwenden darf.[1790]

Diese ökonomische Analyse allgemeiner Geschäftsbedingungen läßt sich auf Nutzungsverträge in DRM-Systemen übertragen. Die Beschreibung der Nutzungsmöglichkeiten in DRM-Nutzungsverträgen ist oft

---

1784 *Adams* in: Neumann (Hrsg.), S. 655, 664 f.

1785 *Basedow* in: Münchener Kommentar, AGBG Einl. Rdnr. 5; *Kötz*, ZVersWiss 1993, 57, 66; *Schlosser* in: Staudinger (Begr.), Einl. zum AGBG Rdnr. 4.

1786 *Ulmer* in: Ulmer/Brandner/Hensen (Hrsg.), Einl. Rdnr. 6. Für den Verwender werden die Wettbewerbsvorteile, die der Verwender durch eine „gute" Geschäftsbedingungen erzielen kann, regelmäßig geringer sein als die Kosten, die dadurch für ihn entstehen, *Kötz*, S. A 35.

1787 *Meyerson*, 24 Ga. L. Rev. 583, 603 (1990).

1788 Ganz h. M.; *Ulmer* in: Ulmer/Brandner/Hensen (Hrsg.), Einl. Rdnr. 6; *Schlosser* in: Staudinger (Begr.), Einl. zum AGBG Rdnr. 4; *Basedow* in: Münchener Kommentar, AGBG Einl. Rdnr. 6; *Behrens*, S. 172; ausführlich *Adams* in: Neumann (Hrsg.), S. 655 ff.; *Kötz*, S. A 33 ff.; s. weiterhin *Eisenberg*, 47 Stan. L. Rev. 211, 243 f. (1995); *Meyerson*, 24 Ga. L. Rev. 583, 605 (1990).

1789 *Schäfer/Ott*, S. 480. Ein ähnliches Problem ergibt sich bei Versicherungsverträgen, s. dazu *Müller*, S. 228 f.; *Wein*, ZVersWiss 86 (1997), 103 ff. Klauseln, die der Kontrolle des AGB-Gesetzes unterliegen, erfüllen im Vergleich zu gesetzlich unkontrollierten Klauseln das Kaldor-Hicks-Kriterium, s. dazu *Schäfer/Ott*, S. 480.

1790 Vgl. *Katz* in: Newman (Hrsg.), Band 3, S. 502, 504. Nach diesem Erklärungsansatz besteht eine Notwendigkeit für eine gesetzliche Regelung jedoch nicht hinsichtlich solcher Klauseln, deren Wert vom Kunden mit vertretbarem Informationsaufwand erkannt und innerhalb des Gesamtverhältnisses von Leistung und Gegenleistung richtig eingeordnet werden kann, s. *Schäfer/Ott*, S. 480.

komplex, die Informationskosten, um die Nutzungsbedingungen richtig einschätzen zu können, sind für den Nutzer hoch, und der Wert der Transaktion regelmäßig vergleichsweise gering.[1791] Wenn aus diesen Gründen auf Konsumentenseite keine Nachfrage nach bestimmten Klauseln in Nutzungsverträgen besteht, existiert auf der Anbieterseite auch kein Anreiz, solche Klauseln anzubieten.[1792] Außerdem ist zu berücksichtigen, daß für digitale Inhalte, die in DRM-Systemen vertrieben werden, oftmals keine nahen Substitute bestehen.[1793] Je stärker der Inhalteanbieter mit einer monopolartigen Stellung ausgestattet ist, desto weniger ist er einem eventuellen Konditionenwettbewerb ausgesetzt.[1794] Bei Nutzungsverträgen in DRM-Systemen, die im Massenmarkt eingesetzt werden,[1795] ergibt sich damit, daß ein Konditionenwettbewerb aufgrund von Informationsasymmetrien unwahrscheinlich ist.

Gegen diese Analyse könnten zwei Einwände vorgebracht werden. Einerseits könnte die Vereinheitlichung der Konditionen unterschiedlicher Anbieter in DRM-Systemen sogar wünschenswert sein. Es wird vertreten, daß bei einer Vereinheitlichung allgemeiner Geschäftsbedingungen der Wettbewerb auf den Preis und die Qualität des Produkts verlagert werde, was die Vergleichbarkeit der Angebote fördern werde. Der denkbare Nebenleistungswettbewerb (um Geschäftsbedingungen) werde auf einen Wettbewerb um die Hauptleistung konzentriert. Indem sich der Wettbewerb bei einheitlichen allgemeinen Geschäftsbedingungen auf andere, weniger komplexe Wettbewerbsparameter konzentrieren könne, habe eine Konditionenvereinheitlichung *wettbewerbsfördernden* Charakter.[1796] Die wettbewerbstheoretischen Grundlagen dieser These sind jedoch äußerst fraglich.[1797] Im vorliegenden Zusammenhang ist noch wich-

[1791] *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1182 (1998); *Perlman*, 53 Vand. L. Rev. 1831, 1838 (2000).

[1792] *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1184 (1998); *Meyerson*, 24 Ga. L. Rev. 583, 605 (1990).

[1793] S. dazu oben Teil 3, A III 2 c aa.

[1794] S. *Cooter/Ulen*, S. 277; *Posner*, Economic Analysis of Law, S. 128; s. dazu unter kartellrechtlichen Gesichtspunkten *Immenga* in: Immenga/Mestmäcker (Hrsg.), GWB-Kommentar, § 2 Abs. 2 Rdnr. 4.

[1795] Vorliegend geht es um Geschäftsbedingungen in DRM-Systemen, mit denen digitale Inhalte zu relativ niedrigen Preisen an ein Massenpublikum verkauft werden. In dieser Konstellation treten die beschriebenen Informationsasymmetrien auf. In anderen Einsatzbereichen von DRM-Systemen mag sich ein differenzierteres Bild ergeben.

[1796] Vgl. dazu *Kliege*, S. 121; *Cooter/Ulen*, S. 279. Dies war für den deutschen Gesetzgeber ein Grund für die Zulassung von Konditionenkartellen im Rahmen des § 2 Abs. 2 GWB, s. *Immenga* in: Immenga/Mestmäcker (Hrsg.), GWB-Kommentar, § 2 Abs. 2 Rdnr. 5. Zu einer ähnlichen These im Bereich des Versicherungsvertragsrechts s. *Wein*, ZVersWiss 86 (1997), 103, 105.

[1797] Vgl. dazu *Monopolkommission*, XI. Hauptgutachten, Rdnr. 955; *Möschel*, Rdnr. 262; *Emmerich*, S. 65 f.; *Immenga* in: Immenga/Mestmäcker (Hrsg.), GWB-Kommentar, § 2 Abs. 2 Rdnr. 7 f.; *Koller*, ZHR 136 (1972), 139, 141 ff., 150.

tiger, daß zweifelhaft ist, ob überhaupt sinnvoll zwischen einem Hauptleistungs- und einem Nebenleistungswettbewerb differenziert werden kann. Bedingungen in DRM-Nutzungsverträgen betreffen nicht nur Nebenleistungen, sondern definieren erst die Hauptleistung: Bei einem körperlichen Gut definiert sich der Umfang des Guts und die an ihm bestehenden Rechte aus der physischen Existenz des Guts. Allgemeine Geschäftsbedingungen betreffen dann nur Nebenleistungen. Dagegen definiert sich der Umfang eines digitalen Inhalts und die an ihm bestehenden Rechte erst durch ein Rechtebündel, das durch einen Nutzungsvertrag verliehen wird, sowie durch technische Schutzmaßnahmen: „The license is the product."[1798] Eine Dichotomie zwischen Haupt- und Nebenleistung besteht bei DRM-Nutzungsverträgen nicht. Die These, daß eine Konditionenvereinheitlichung mit Konzentration auf den Hauptleistungswettbewerb wünschenswert sei, kann schließlich deshalb nicht überzeugen, weil dadurch das Problem vertraglicher Schutzmaßnahmen in DRM-Systemen nicht beseitigt würde: Hier geht es um die Frage, ob durch einen Wettbewerb von Nutzungsbedingungen ein zu weitreichender vertraglicher Schutz der Inhalteanbieter vermieden werden kann. Dadurch soll es Dritten ermöglicht werden, die Inhalte ohne Zustimmung der Rechteinhaber in einer Weise zu nutzen, die zu positiven externen Effekten für die Allgemeinheit führt. Bei einer Vereinheitlichung der Nutzungsbedingungen und einer Konzentration des Wettbewerbs auf Preis und Qualität würde man aber die einzige Wettbewerbsdimension beseitigen, in der – wenn überhaupt – die positiven externen Effekte entstehen können. Das Modell der Konzentration auf den Hauptleistungswettbewerb berücksichtigt diesen Aspekt nicht.

Die dargestellte Analyse könnte wegen eines zweiten Einwands zu modifizieren sein. In einem DRM-System kann es vorkommen, daß ein Nutzer mehrfach beim gleichen Anbieter digitale Inhalte erwirbt. Das „markets for lemon"-Modell geht davon aus, daß die Konsumenten lediglich einzelne isolierte Verträge mit einzelnen Anbietern abschließen. Der Anbieter erwartet nicht, daß der Konsument nochmals mit ihm weitere Verträge abschließt.[1799] Die Beurteilung des „market for lemon"-Modells könnte sich ändern, wenn ein Konsument bei einem Anbieter oftmals hintereinander Verträge abschließen und damit nach und nach bessere

[1798] *Gomulkiewicz*, 13 Berkeley Tech. L. J. 891 (1998); s. weiterhin *O'Rourke*, 14 Berkeley Tech. L. J. 635, 648 (1999); Official Comment No. 3 zu § 209 UCITA, *UCITA*, S. 125 („License terms define the product"); *R. T. Nimmer*, 36 Hous. L. Rev. 1, 4 (1999); *Dodd*, 36 Hous. L. Rev. 195, 215, 217 (1999); *Cohen*, 13 Berkeley Tech. L. J. 1089, 1115 (1998). Man kann digitale Inhalte daher auch als „Rechtsprodukt" auffassen; s. dazu *Müller*, S. 266. Ähnliche Entwicklungen lassen sich beim Versicherungsschutz beobachten: Versicherungsverträge definieren den Umfang der Versicherung. Versicherungen sind damit ein Rechtsprodukt; s. dazu *Roth*, VersR 1993, 129, 135, und *Müller*, S. 286 ff.

[1799] S. *Adams*, BB 1989, 781, 784.

Informationen über die rechtliche Qualität der verwendeten allgemeinen Geschäftsbedingungen erhalten würde.[1800] In DRM-Systemen, die auf den Massenmarkt ausgerichtet sind, sind solche wiederholten Vertragsbeziehungen durchaus denkbar. Je nach Umfang und Schnelligkeit, mit der neue Verträge von denselben oder auch von anderen Konsumenten abgeschlossen werden, kann die Informationsverbesserung, die sich für die Konsumenten aus diesen Wiederholungskäufen ergibt, zu einer Verringerung der dargestellten Informationsasymmetrie führen.[1801] Es ist im vorliegenden Zusammenhang nicht möglich, auf die einzelnen Bedingungen dieser Modellerweiterung einzugehen. Die Voraussetzungen, daß durch Wiederholungskäufe das Marktversagen beseitigt wird, sind jedoch relativ eng und von den einzelnen Gegebenheiten des Markts abhängig.[1802] Auch unter Berücksichtigung dieser Modellerweiterung sind gesetzliche Beschränkungen allgemeiner Geschäftsbedingungen immer noch vorzugswürdig.[1803]

Aus all diesen Gründen kann auch die Argumentation Judge *Easterbrooks* in der ProCD-Entscheidung[1804] nicht überzeugen.[1805] Ein Wettbe-

[1800] *Adams* in: Neumann (Hrsg.), S. 655, 665 f.

[1801] Dies setzt voraus, daß die Konsumenten zu irgendeinem Zeitpunkt nach dem Kauf die jeweilige Qualität der allgemeinen Geschäftsbedingung feststellen und dem richtigen Anbieter zuordnen. Ein Anbieter würde es dann in Erwartung eines zukünftigen Absatzrückgangs schon in der ersten Kaufperiode unterlassen, schlechte Geschäftsbedingungen anzubieten. Ob der Anbieter dies tut, hängt maßgeblich davon ab, ob die durch die bessere Qualität zusätzlich erzeugten, zukünftigen Gewinne höher sind als diejenigen Gewinne, die zum jetzigen Zeitpunkt durch die Verkäufe an ahnungslose Kunden bei der Produktion minderwertiger Qualität eingestrichen werden können. Zu diesem „Good will"-Kontrollverfahren s. *Adams*, BB 1989, 781, 785; *ders.* in: Neumann (Hrsg.), S. 655, 665 ff.

[1802] Kriterien, daß Wiederholungskäufe bei allgemeinen Geschäftsbedingungen zu einer Lösung des „market for lemons"-Problems führen, sind u. a. die Geschwindigkeit, mit der die Konsumenten die Qualität der Geschäftsbedingungen erkennen und darauf reagieren, die Marktstruktur, die Existenz von Informationsvermittlern oder Testzeitschriften, die Möglichkeit der Qualitätsdiskriminierung durch die Anbieter und insbesondere das Bestehen von Marktzutrittsschranken. Ausführlich zum ganzen *Adams* in: Neumann (Hrsg.), S. 655, 665 ff., sowie – inhaltlich identisch, aber weniger formal dargestellt – *ders.*, BB 1989, 781, 784 ff.

[1803] Vorteile eines AGB-Gesetzes sind u. a. die Tatsache, daß die gesetzliche AGB-Kontrolle schneller greift als ein auf Wiederholungskäufen basierendes Kontrollsystem, die Herstellung der Einzelfallgerechtigkeit durch Verhinderung von Qualitätsdiskriminierung durch die Anbieter und insbesondere eine deutliche Verminderung der Such- und Kontrollkosten beim einzelnen Konsumenten. Diese Vorteile müssen gegenüber den Vorteilen eines Konditionenwettbewerbs abgewogen werden. S. zum ganzen *Adams*, BB 1989, 781, 787 f.; *ders.* in: Neumann (Hrsg.), S. 655, 674 ff.

[1804] S. dazu oben bei Fn. 1752.

[1805] S. dazu *Madison*, 67 Fordham L. Rev. 1025, 1113 ff. (1998); *Elkin-Koren*, 12 Berkeley Tech. L. J. 93, 110 (1997). Daneben bestehen noch weitere Aspekte, die einen Konditionenwettbewerb verhindern können. So wird die These vertreten, Netzwerkeffekte verhinderten einen Konditionenwettbewerb. Zum Begriff der Netzwerkeffekte s. unten Teil 3, B I 2 b cc 2 a. Die Auswirkungen von Netzwerkeffekten auf Stan-

werb verschiedener Nutzungsverträge in DRM-Systemen scheint wenig realistisch.[1806] Dies könnte sich ändern, wenn in Zukunft Software-Agenten für die Nutzer autonom die Nutzungsbedingungen unterschiedlicher Anbieter vergleichen würden.[1807] Das erscheint jedoch zweifelhaft: Der Einsatz solcher Software-Agenten im Massenmarkt ist auf absehbare Zeit Zukunftsmusik, und es stellt sich das Problem, daß Software-Agenten in der Realität oftmals nicht entsprechend der Präferenzen der Nutzer personalisiert werden.[1808]

Wie oben[1809] dargestellt wurde, bestehen aus ökonomischer Sicht vielfältige Gründe, die Bestrebungen von Inhalteanbietern, sich durch DRM-Systeme einen umfassenden und unbegrenzten Schutz zu verschaffen, skeptisch zu beurteilen. Im Bereich der vertraglichen Schutzmechanismen können die Probleme eines überbordenden DRM-Schutzes auch nicht durch einen Wettbewerb zwischen unterschiedlichen Anbietern von Inhalten oder DRM-Systemen gelöst werden.

cc) Technischer Schutz

(1) Allgemeines. Ein Inhalteanbieter kann auch durch technische Schutzmaßnahmen einen umfassenden und nahezu unbegrenzten Schutz erreichen. Wie bei vertraglichen Schutzmechanismen stellt sich hier die

dardverträge wurde insbesondere von *Klausner* im gesellschaftsrechtlichen Bereich untersucht; s. *Klausner*, 81 Va. L. Rev. 757, 775 ff. (1995). Diese Analyse läßt sich auf allgemeine Geschäftsbedingungen übertragen, s. dazu *Kahan/Klausner*, 83 Va. L. Rev. 713 ff. (1997). Kommt es bei der Klausel einer Geschäftsbedingung zu einem Streit über Bedeutung und Auslegung, so rufen die Parteien ein Gericht an, das den Streit entscheidet. Diese Entscheidung kommt aber nicht nur den Prozeßbeteiligten zugute; vielmehr trägt sie faktisch zur Klärung der Rechtslage für jeden bei, der die betreffende Klausel in seinen allgemeinen Geschäftsbedingungen verwendet. Je mehr Produzenten eine bestimmte Klausel verwenden, desto wahrscheinlicher ist eine zukünftige gerichtliche Klärung der Bedeutung dieser Klausel, was zu einer Erhöhung der Rechtssicherheit für die Verwender führt. Der Nutzen, eine bestimmte Klausel zu verwenden, steigt also mit der Anzahl der anderen Verwender, *Klausner*, 81 Va. L. Rev. 757, 776 (1995); *Kahan/Klausner*, 83 Va. L. Rev. 713, 726 (1997). Dieser Effekt, der sich auch als „interpretativer Netzwerkeffekt" bezeichnen läßt, führt zu einer Standardisierung allgemeiner Geschäftsbedingungen, *Kahan/Klausner*, 83 Va. L. Rev. 713, 729 (1997); *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1184 (1998); *Perlman*, 53 Vand. L. Rev. 1831, 1838 (2000); *Katz* in: Newman (Hrsg.), Band 3, S. 502, 503. Diese Standardisierung kann auch zu einem Lock-in auf suboptimalen Vertragsklauseln führen, s. *Klausner*, 81 Va. L. Rev. 757, 798 ff. (1995); *Kahan/Klausner*, 83 Va. L. Rev. 713, 734 f. (1997). Das Modell der „interpretativen Netzwerkeffekte" hat jedoch einige Schwächen; solche Netzwerkeffekte werden bei allgemeinen Geschäftsbedingungen allenfalls schwach ausgeprägt sein; s. zur Kritik ausführlich *Lemley/McGowan*, 86 Cal. L. Rev. 479, 571 (1998); zu den Folgen dieser Kritik s. unten Fn. 1858. Zu weiteren Kritikpunkten an der These des Konditionenwettbewerbs s. *Cohen*, 97 Mich. L. Rev. 462, 518 ff. (1998).

[1806] Ebenso *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1184 (1998).

[1807] Vgl. *Elkin-Koren/Salzberger*, 19 Int. Rev. L. & Econ., 553, 561 (1999).

[1808] S. dazu oben bei Fn. 1713; kritisch auch *Gimbel*, 50 Stan. L. Rev. 1671, 1684 (1998).

[1809] S. oben Teil 3, B I 2 a.

Frage, ob ein Wettbewerb zwischen unterschiedlichen Anbietern dazu führen könnte, daß sich Schutzmaßnahmen, die einseitig nur die Interessen der Inhalteanbieter wahren, am Markt nicht durchsetzen können.[1810]

Als Beleg dieser These werden oft die Erfahrungen mit Kopierschutzmaßnahmen bei Computersoftware in den 80er Jahren angeführt. Damals versuchten viele Softwarehersteller, ihre Produkte durch Dongles und andere Schutzmaßnahmen vor unberechtigter Vervielfältigung zu schützen. Nach einigen Jahren verschwanden Dongles jedoch wieder vom Massenmarkt.[1811] Ein Grund für diesen Mißerfolg sei, so wird vorgebracht, daß Dongles vom Konsumenten nicht akzeptiert wurden.[1812] Es ist fraglich, ob sich dieser Erklärungsansatz ohne Abstriche auf heutige DRM-Systeme übertragen läßt. Dongles wurden von den Konsumenten nicht akzeptiert, weil durch sie die Benutzung der Software kompliziert wurde[1813] und weil Dongles mitunter nicht ordnungsgemäß funktionierten.[1814] Dagegen versprechen DRM-Systeme, daß der Konsument von den technischen Schutzmaßnahmen gar nichts mehr bemerkt. Sie werden derart in die Hard- oder Softwareumgebung des Konsumenten integriert, daß sich die Nutzung eines DRM-Systems von der Nutzung eines ungeschützten Systems nicht unterscheidet.[1815] Auch Fehlfunktionen sollen vermieden werden. Heutige technische Schutzmaßnahmen in DRM-Systemen unterscheiden sich in ihrer Perfektion und Integration deutlich von früheren Dongles. Schließlich eröffnen DRM-Systeme Nutzungsmöglichkeiten, die bisher undenkbar erschienen. Nutzer können auf digitale Inhalte zu jeder Tageszeit von jedem Ort aus sofort zugreifen. Inhalte können individualisiert werden. Im Gegensatz zu Dongles erweitern heutige DRM-Systeme die Nutzungsmöglichkeiten in beträchtlichem Maße und erhöhen damit die Attraktivität für den Nutzer.[1816] Die empirischen Belege für das Scheitern eines rudimentären Schutzkonzepts in den 80er Jahren können daher nicht ohne weiteres auf heutige DRM-Systeme übertragen werden.

[1810] S. zu diesem Erkenntnisinteresse allgemein oben Teil 3, B I 2 b aa.

[1811] Sie werden heute noch bei spezieller oder besonders teurer Software eingesetzt.

[1812] *Gilmore*, c't 4/2001, S. 64; *DeLong/Froomkin* in: Kahin/Varian (Hrsg.), S. 6, 10 f.; *Manasse*, S. 9; *Barlow*, Wired 8.10, S. 240, 241 (Oktober 2000); *Barlow*, Wired 2.03, S. 84, 129 (März 1994). Ein anderer Erklärungsansatz wird unten Teil 3, B I 2 b cc 2 d, dargestellt.

[1813] Besaß der Nutzer unterschiedliche Softwareprogramme, die jeweils durch Dongles geschützt waren, so mußte vor der Nutzung eines Programms eventuell ein Dongle am Computer umgesteckt werden.

[1814] Beim parallelen Betrieb mehrerer Dongles konnte es zu Fehlfunktionen kommen. Auch verweigerte das geschützte Programm manchmal seine Dienste, obwohl der Dongle ordnungsgemäß eingesetzt war. Schließlich wurde mitunter das Erstellen von Sicherungskopien verhindert; s. zum ganzen *Cohen*, 97 Mich. L. Rev. 462, 524 f. (1998).

[1815] *Sander*, S. 3 f.

[1816] S. a. *Cohen*, 97 Mich. L. Rev. 462, 525 (1998).

Aus theoretischer Sicht lassen sich für die Frage, ob ein Wettbewerb zwischen verschiedenen technischen Schutzmaßnahmen mit unterschiedlichem Schutzniveau möglich ist, zwei Konstellationen zu unterscheiden. In der *ersten Konstellation* werden in einem einheitlichen DRM-System verschiedene Inhalte angeboten, die technisch unterschiedlich stark geschützt sind. Beispielsweise wird ein Musikstück eines bekannten Künstlers mit umfangreichem Kopierschutz angeboten, während ein Stück eines unbekannteren Künstlers mit einem geringeren technischen Schutz angeboten wird. Da die Nutzer zwischen beiden Inhalten wählen können, könnte auf diese Weise mittelbar ein Wettbewerb zwischen unterschiedlichen technischen Schutzniveaus entstehen. Jedoch ist zweierlei zu beachten: Einerseits hängt der Wettbewerb zwischen verschiedenen digitalen Inhalten, die unterschiedlich stark geschützt sind, davon ab, inwieweit die Inhalte substitutierbar sind. Die Frage, ob und inwieweit urheberrechtlich geschützte Werke Substitute haben, ist umstritten und letztlich nur im Einzelfall mit Hilfe empirischer Untersuchungen zu klären.[1817] Selbst wenn die verschiedenen Inhalte nahe Substitute darstellen, ist immer noch fraglich, ob dies zu einem Wettbewerb unterschiedlicher DRM-Schutzniveaus führt. Der Nutzer wird beim Erwerb des digitalen Inhalts oftmals gar nicht im einzelnen erfahren, wie und in welchem Umfang der Inhalt genau geschützt ist. Dies macht technische Schutzmaßnahmen zum Erfahrungsgut[1818] und hindert den Nutzer an einem Vergleich unterschiedlicher Schutzniveaus vor dem Erwerb der Inhalte. Die einzelne Ausgestaltung der technischen Schutzmaßnahmen eines digitalen Inhalts ist komplex, die Informationskosten, um deren Auswirkungen richtig einschätzen zu können, sind hoch, und der Wert der Transaktion regelmäßig vergleichsweise gering. Wie bei vertraglichen Schutzmechanismen entsteht daher auch bei technischen Schutzmechanismen eine Informationsasymmetrie.[1819] Wenn aus diesen Gründen auf Konsumentenseite keine Nachfrage nach bestimmten Schutzniveaus besteht, existiert auf der Anbieterseite auch kein Anreiz, diese Schutzniveaus anzubieten. Ein Wettbewerb unterschiedlicher Schutzniveaus erscheint unter diesen Voraussetzungen unwahrscheinlich.

Davon ist eine *zweite Konstellation* zu unterscheiden. In diesem Fall wählt der Nutzer nicht zwischen unterschiedlich geschützten Inhalten eines *einheitlichen* DRM-Systems. Vielmehr wählt er zwischen *unterschiedlichen* DRM-Systemen. Beispielsweise sind am Markt zwei Systeme verfügbar, mit denen Konsumenten zu Hause Videofilme betrachten können: Einerseits das analoge VHS-System, in dem Videofilme relativ unge-

[1817] S. dazu allgemein oben Teil 3, A III 2 c aa.
[1818] Zum Begriff s. oben Fn. 1778.
[1819] S. dazu ausführlich oben Teil 3, B I 2 b bb 2.

schützt vertrieben werden,[1820] andererseits das digitale DVD-System, das über umfangreiche technische Schutzmaßnahmen verfügt.[1821] Ein Wettbewerb zwischen solchen unterschiedlichen DRM-Systemen könnte dazu führen, daß sich nur solche Systeme am Markt durchsetzen, die keinen maximalen Schutz bieten, sondern bestimmte Interessen der Nutzer und der Allgemeinheit – insbesondere urheberrechtliche Schrankenbestimmungen – respektieren. Im Gegensatz zur ersten Konstellation geht es hier also nicht um einen Wettbewerb unterschiedlich geschützter digitaler Inhalte innerhalb eines einheitlichen DRM-Systems, sondern um einen Wettbewerb unterschiedlich schützender DRM-Systeme, innerhalb derer oft die gleichen Inhalte angeboten werden. Fraglich ist, ob in dieser Konstellation der Wettbewerb funktioniert. Auch hierbei ist auf Informationsasymmetrien hinzuweisen: Bevor sich der Konsument für ein bestimmtes DRM-System entscheidet, wird er oftmals gar nicht die Einzelheiten des Schutzniveaus der unterschiedlichen Systeme erfahren. Diese sind regelmäßig komplex, die Informationskosten, um deren Auswirkungen richtig einschätzen zu können, sind hoch. Verschiedene DRM-Systeme weisen regelmäßig noch viele andere Unterschiede auf, die mit dem technischen Schutzniveau nichts zu tun haben; für den Konsumenten stehen Fragen der Qualität der in dem System verfügbaren Inhalte, der Kompatibilität zu schon bestehenden Systemen und ähnliches im Vordergrund. Dies kann dazu führen, daß der Konsument die Ausgestaltung der technischen Schutzmaßnahmen in einem DRM-System nicht in seine Entscheidungsfindung einbezieht, welches System er anschaffen sollte. Diese Informationsasymmetrie kann einen Wettbewerb unterschiedlich ausgestalteter DRM-Systeme verhindern.

Neben solchen Effekten,[1822] die schon ausführlich bei vertraglichen Schutzmechanismen geschildert wurden, können in dieser zweiten Konstellation aber noch weitere Fälle des Marktversagens auftreten: Netzwerkeffekte und Lock-In-Effekte können den Wettbewerb unterschiedlicher DRM-Systeme verhindern. Dies soll in den folgenden beiden Abschnitten dargestellt werden.

(2) Netzwerkeffekte

(a) Allgemeines. Auf einem herkömmlichen Markt ist die Nachfrage eines Konsumenten nach einem Gut unabhängig von der Nachfrage anderer Konsumenten nach diesem Gut.[1823] Dies trifft aber nicht auf allen Märkten zu. So existieren Güter, bei denen die Nachfrage eines Konsumenten von der Anzahl der weiteren Konsumenten abhängt, die dieses

[1820] Der einzige Schutz bei gekauften analogen Videokassetten sind analoge Kopierschutzverfahren von Macrovision; s. dazu oben Fn. 503.

[1821] S. dazu oben Teil 1, D II 3.

[1822] S. oben Teil 3, B I 2 b bb.

[1823] *Pindyck/Rubinfeld*, S. 127.

Gut ebenfalls gekauft haben. Man spricht dann von einem „Netzwerkeffekt".[1824] Ein „positiver" Netzwerkeffekt liegt vor, wenn die Nachfrage eines Konsumenten nach einem Gut mit der steigenden Anzahl anderer Konsumenten, die das Gut erworben haben, ansteigt.[1825] In Märkten mit positiven Netzwerkeffekten steigt der Wert eines Guts mit seiner zunehmenden Verbreitung an.[1826]

Bestes Beispiel für Netzwerkeffekte ist das Telefon. Der Nutzen des Telefons ist für den einzelnen Konsumenten umso höher, je mehr Konsumenten an das Telefonnetz angeschlossen sind.[1827] Daher steigt der Vorbehaltspreis[1828] jedes Konsumenten für das Telefon mit der Anzahl der anderen Konsumenten, die ein Telefon besitzen.[1829] Netzwerkeffekte treten oft in „physikalischen" Netzwerken (Telefon, Fax, Internet) auf. Sie können aber auch in „virtuellen" Netzwerken auftreten.[1830] Ein Beispiel dafür stellen bestimmte Arten von Computersoftware dar.[1831] So unterliegt Textverarbeitungssoftware starken Netzwerkeffekten: Durch ein einheitliches Dateiformat können die Nutzer einer bestimmten Textverarbeitungssoftware die Dateien untereinander tauschen und auf ihrem Computer weiterverarbeiten. Damit steigt der Nutzen der Software für

[1824] Grundlegend *Katz/Shapiro*, 75 Am. Econ. Rev. 424 ff. (1985). Mitunter werden auch die Begriffe „Netzeffekt" und „Netzwerk-Externalität" verwendet, s. *European Communication Council* (Hrsg.), S. 157; *Pindyck/Rubinfeld*, S. 127; *Shy*, S. 3. Man kann Netzwerkeffekte auch als „externe Effekte im Konsum" bezeichnen; s. *Varian*, S. 592; *European Communication Council* (Hrsg.), S. 157; *Shy*, S. 17; *Lemley/McGowan*, 86 Cal. L. Rev. 479, 483 (1998). Ein externer Effekt im Konsum liegt vor, wenn ein Konsument direkt durch die Produktion oder den Konsum eines anderen Akteurs berührt wird, *Varian*, S. 554. Teilweise wird zwischen „Netzwerkeffekten" und „Netzwerk-Externalitäten" unterschieden: Während erstere Situationen mit steigenden Skalenerträgen kennzeichnen, bezeichnen zweitere Situationen, in denen Effizienzverluste auftreten; s. dazu *Lemley/McGowan*, 86 Cal. L. Rev. 479, 482 Fn. 5 (1998). Ob es sich bei Netzwerkeffekten tatsächlich um eine „Externalität" handelt, hängt auch von der Definition des Begriffs „Externalität" ab, s. *Gröhn*, S. 28 f.; *Liebowitz/Margolis*, 8 (2) J. Econ. Persp. 133, 136 ff. (1994).

[1825] *Katz/Shapiro*, 75 Am. Econ. Rev. 424 (1985). Dagegen liegt ein negativer Netzwerkeffekt vor, wenn die Nachfrage des Konsumenten dadurch absinkt, z. B. bei exklusiven Luxusgütern, s. *Pindyck/Rubinfeld*, S. 127; *Monopolkommission*, IX. Hauptgutachten, Tz. 819.

[1826] *European Communication Council* (Hrsg.), S. 159.

[1827] Vgl. *Lemley/McGowan*, 86 Cal. L. Rev. 479, 488 f. (1998); *Monopolkommission*, IX. Hauptgutachten, Tz. 818.

[1828] S. zu diesem Begriff oben bei Fn. 1547.

[1829] *Varian*, S. 592 f. Der Vorbehaltspreis des „marginalen" Konsumenten nimmt wieder ab, wenn die Zahl der schon angeschlossenen Personen sehr hoch ist, da dann alle Konsumenten, die das Gut höher schätzen, bereits angeschlossen sind, *Varian*, S. 593.

[1830] S. zu der Unterscheidung *Lemley/McGowan*, 86 Cal. L. Rev. 479, 488 ff. (1998).

[1831] S. dazu *Gröhn*; *Shy*, S. 51 ff.; *Shy* in: Kahin/Varian (Hrsg.), S. 97, 104 f. m. w. N. Ein anderes Beispiel für Netzwerkeffekte in virtuellen Netzwerken ist das Kreditkartensystem, s. *Lemley/McGowan*, 86 Cal. L. Rev. 479, 492 f., 512 ff. (1998).

den einzelnen Konsumenten in dem Maße, in dem andere Konsumenten die gleiche Software benutzen; die Möglichkeit des Datenaustauschs führt zu Netzwerkeffekten.[1832] Netzwerkeffekte sind ein Erklärungsansatz für die hohen Marktanteile von Microsoft im Softwarebereich.[1833]

Weiterhin lassen sich „direkte" und „indirekte" Netzwerkeffekte unterscheiden. Bei einem direkten Netzwerkeffekt steigt der Wert des Guts mit der Zahl seiner Nutzer, wie in den vorangegangenen Beispielen gezeigt wurde. Bei einem indirekten Netzwerkeffekt entsteht der Netzwerkeffekt durch ein komplementäres Gut.[1834] So kaufen umso mehr Konsumenten einen IBM-kompatiblen PC, je mehr Software für diesen Hardware-Standard verfügbar ist. Computerhardware unterliegt damit starken Netzwerkeffekten, die aber nicht durch die Hardware selbst hervorgerufen wird, sondern durch die – komplementäre – Software, die auf der Hardware ausgeführt werden kann; es liegt ein indirekter Netzwerkeffekt vor.[1835] Indirekte Netzwerkeffekte treten bei vielen Komplementärgütern auf:[1836] Der Nutzen des Betriebssystems eines Computers steigt für den Konsumenten mit der Masse der Anwendungssoftware, die für dieses

[1832] *Lemley/McGowan*, 86 Cal. L. Rev. 479, 491 (1998); *Shapiro/Varian*, S. 174; *Elkin-Koren/Salzberger*, 19 Int. Rev. L. & Econ., 553, 558 (1999). Dies gilt jedoch nur für bestimmte Arten von Software. Ein weiteres Beispiel ist Tabellenkalkulations-Software, s. dazu *Shy*, S. 44 ff. Starke Netzwerkeffekte treten auch bei „Instant Messaging"-Programmen auf. Dagegen treten z. B. bei Formular- oder Informationsmanagementsoftware sowie bei kleineren Hilfsprogrammen weniger starke Netzwerkeffekte auf; s. dazu unter empirischen Aspekten *Gröhn*, S. 108 ff.

[1833] *Pindyck/Rubinfeld*, S. 131. Ein weiteres bekanntes – wenn auch seit einigen Jahren umstrittenes – Beispiel für Netzwerkeffekte ist das sog. QWERTY-Tastaturlayout bei Schreibmaschinen und Computertastaturen. QWERTY beschreibt die übliche Anordnungen von Buchstaben auf einer anglo-amerikanischen Computer- oder Schreibmaschinentastatur. Es wird die These vertreten, diese Anordnung sei um 20 bis 40% weniger effizient als eine alternative Anordnung („Dvorak Simplified Keyboard"). Wegen der Netzwerkeffekte habe sich die QWERTY-Anordnung jedoch durchgesetzt; s. dazu *Shapiro/Varian*, S. 185 f.; *Shy*, S. 43 f.; *Gröhn*, S. 142 f.; *Monopolkommission*, IX. Hauptgutachten, Tz. 833. Teilweise wird diese Interpretation jedoch angezweifelt; so sei nicht erwiesen, daß andere Tastatur-Anordnungen effizienter seien. S. dazu und zu anderen Einwänden *Liebowitz/Margolis*, S. 19 ff.; *Margolis/Liebowitz* in: Newman (Hrsg.), Band 3, S. 17, 21 f.

[1834] Zwei Güter sind *komplementär*, wenn sie vom Konsumenten üblicherweise zusammen genutzt werden. In diesen Fällen kauft der Konsument statt einzelner Güter ganze Systeme. Um zwei komplementäre Produkte zu produzieren, müssen diese untereinander *kompatibel* sein. Zur Herstellung der Kompatibilität ist regelmäßig ein *Standard* erforderlich. Beispiele solcher komplementärer Güter sind die Computerhardware und Computersoftware, Fotokamera und Film, Kassettengerät und Kassette, CD-Spieler und CD usw.; s. zum ganzen *Shy*, S. 2; *Gröhn*, S. 28; *Pindyck/Rubinfeld*, S. 23.

[1835] S. dazu *Shy*, S. 52; *Gupta/Jain/Sawhney*, 18 Marketing Science 396, 397 (1999); *Katz/Shapiro*, 75 Am. Econ. Rev. 424 (1985). Daneben bestehen auch innerhalb der Computerhardware (teilweise direkte) Netzwerkeffekte, auf die hier nicht eingegangen wird; s. dazu *Shy*, S. 13 ff.

[1836] *Varian*, S. 592; *European Communication Council* (Hrsg.), S. 157 f.

Betriebssystem angeboten wird.[1837] Die Nachfrage nach Videokassetten hängt von der Anzahl der verkauften Videorekorder ab und vice versa.[1838] Ein CD-Spieler ist nutzlos ohne CDs; die Nachfrage nach CD-Spielern steigt mit der Anzahl der verfügbaren CDs.[1839] Indirekte Netzwerkeffekte entstehen hauptsächlich bei Systemprodukten. Unterliegt ein Gut indirekten Netzwerkeffekten, so wird der Netzwerkeffekt nicht durch das Gut selbst, sondern durch ein anderes, komplementäres Gut vermittelt.[1840]

Netzwerkeffekte sind für die ökonomische Analyse des Internet-Rechts von hoher Bedeutung.[1841] Netzwerkmärkte stellen keine Wettbewerbsmärkte im herkömmlichen Sinn dar. Sie unterscheiden sich von herkömmlichen Märkten oftmals durch die Existenz komplementärer und kompatibler Produkte, durch die Bedeutung von Standards, durch hohe Kosten eines Anbieterwechsels (sogenannte „switching costs"), durch Lock-in-Effekte und durch bedeutende Größenvorteile.[1842] In Netzwerkmärkten tritt der originäre Wert des angebotenen Guts in den Hintergrund. Der Konsument kauft nicht mehr nur das Gut, sondern vielmehr den Zugang zu einem Netzwerk, den er durch das Gut erhält.[1843]

Netzwerkmärkte können unterschiedliche Arten von Marktversagen aufweisen.[1844] Bei Gütern mit Netzwerkeffekten liegen steigende Skalenerträge vor.[1845] Unternehmen, die ein Gut mit starken Netzwerkeffekten auf den Markt bringen wollen, versuchen in besonderem Maße, schon früh im Lebenszyklus des Guts die Nachfrage anzuregen, um schnell eine

---

[1837] *Cohen*, 97 Mich. L. Rev. 462, 543 (1998); *Rubinfeld*, GRUR Int. 1999, 479 f.

[1838] *Varian*, S. 592; *Katz/Shapiro*, 75 Am. Econ. Rev. 424 (1985).

[1839] Vgl. *Shy*, S. 2.

[1840] *Rubinfeld*, GRUR Int. 1999, 479; *Gupta/Jain/Sawhney*, 18 Marketing Science 396, 397 f. (1999). Teilweise wird dieser Effekt auch „horizontaler Netzwerkeffekt" genannt, so *Gröhn*, S. 27.

[1841] S. dazu die grundlegende Untersuchung von *Lemley/McGowan*, 86 Cal. L. Rev. 479 ff. (1998), die die Theorie der Netzwerkeffekte im Bereich des Kartell-, Urheber-, Telekommunikations-, Internet-, Gesellschafts- und Vertragsrechts untersuchen. Unter <http://www.stern.nyu.edu/networks/site.html> bietet *Economides* eine Vielzahl von Literaturhinweisen und Hyperlinks zum Thema.

[1842] *Shy*, S. 1 ff.

[1843] *European Communication Council* (Hrsg.), S. 157.

[1844] *Shy*, S. 6; s. weiterhin *European Communication Council* (Hrsg.), S. 157 ff.; *Rubinfeld*, GRUR Int. 1999, 479 ff.

[1845] *Lemley/McGowan*, 86 Cal. L. Rev. 479, 484 (1998). Ein steigender Skalenertrag liegt vor, wenn bei einer Vermehrung aller Produktionsfaktoren um einen bestimmten Prozentsatz die Produktion eine darüberliegende prozentuale Steigerung erfährt, s. *Varian*, S. 312 f.; *Pindyck/Rubinfeld*, S. 198. Dieses Charakteristikum verbindet Netzwerkgüter mit natürlichen Monopolen. Dennoch sind beide Phänomene nicht gleichzusetzen: Während es bei natürlichen Monopolen um Größenvorteile auf *Angebots*seite geht, handelt es sich bei Netzwerkeffekten um Größenvorteile auf *Nachfrage*seite, *Lemley/McGowan*, 86 Cal. L. Rev. 479, 595 ff. (1998); s. a. *Posner*, Antitrust in the New Economy, S. 2; *Shapiro/Varian*, S. 179 ff.; *Mestmäcker*, ZUM 2001, 185.

kritische Masse von Konsumenten zu erreichen. Nach Überwinden der kritischen Masse wird das Gut weitgehend zum „Selbstläufer" (sogenanntes „tipping"): Mit zunehmender Größe steigt die Attraktivität des Netzwerkguts. Dies wiederum veranlaßt weitere Nutzer, sich dem Netzwerk anzuschließen, was erneut zur Verstärkung des Netzwerkeffekts führt. Es treten sogenannte „positive Rückkoppelungen" auf.[1846] Deshalb investieren Unternehmen anfangs massiv in den Erwerb von Marktanteilen.[1847] Die positiven Rückkoppelungen von Netzwerkeffekten führen dazu, daß der Marktanteil des Marktbeherrschers immer mehr ansteigt, während der Marktanteil von Wettbewerbern immer mehr absinkt: Deren Marktanteil wird vom Marktbeherrscher förmlich aufgesogen.[1848] Netzwerkeffekte können in einem Markt zu de-facto-Standards, auch zu einer Monopolstellung eines Anbieters führen.[1849]

Eine solche Entwicklung ist unter ökonomischen Gesichtspunkten nicht a priori zu verurteilen. Wenn aufgrund der ökonomischen Besonderheiten eines Markts ein einheitlicher Standard effizienter ist als mehrere konkurrierende Standards, so ist eine einheitliche Standardisierung wünschenswert.[1850] Selbst wenn ein einheitlicher Standard zu bevorzugen ist, heißt das aber noch nicht, daß nur ein einziges Unternehmen Produkte

---

[1846] *Monopolkommission*, IX. Hauptgutachten, Tz. 831. Mitunter wird auch von „positivem Feedback" gesprochen, s. *European Communication Council* (Hrsg.), S. 159; *Shapiro/Varian*, S. 173 ff.

[1847] *Varian*, S. 597 f.; *Katz/Shapiro*, 8 (2) J. Econ. Persp. 93, 107 (1994); s. a. *European Communication Council* (Hrsg.), S. 16 f. Um die kritische Masse zu erreichen, gehen Unternehmen sogar dazu über, das Produkt zu verschenken: Ene schnelle Marktdurchdringung ist wichtiger als ein schneller Gewinn. Bekanntestes Beispiel ist die kostenlose Abgabge der Internet-Browser durch Netscape und Microsoft. Andere Fälle sind die kostenlose Abgabe des Adobe Acrobat Reader, des Real Audio Player und der Star Office Suite; s. zum ganzen *Parker/Van Alstyne* in: Proceedings of the 2nd ACM Conference on Electronic Commerce 2000, S. 107 ff.; *European Communication Council* (Hrsg.), S. 191 ff.; *Varian*, S. 597 f.; *Rubinfeld*, GRUR Int. 1999, 479, 481. Bei den positiven Rückkoppelungen spielt auch die Erwartungshaltung der Nutzer hinsichtlich der künftigen Entwicklung des Netzwerks eine große Rolle. Rechtzeitige Vorankündigungen von Produktinnovationen können die Durchsetzung am Markt daher beschleunigen beziehungsweise überhaupt erst ermöglichen; *European Communication Council* (Hrsg.), S. 160 f.; *Shapiro/Varian*, S. 181; *Rubinfeld*, a. a. O., S. 481. Im Amerikanischen wird die verfrühte Vorankündigung von Softwareprodukten als „vaporware" bezeichnet.

[1848] *Shapiro/Varian*, S. 176; *Rubinfeld*, GRUR Int. 1999, 479, 480. Daher wird auch gefordert, daß der Schutz durch das Urheberrecht in Märkten mit Netzwerkeffekten zu verringern sei. Dies sei ein Ausgleich für die Verstärkung des urheberrechtlichen Schutzes aufgrund der Netzwerkeffekte; s. dazu *Farrell* in: Kahin/Abbate (Hrsg.), S. 368 ff.; *Gordon/Bone* in: Bouckaert/De Geest (Hrsg.), Band II, Kap. 1610, S. 189, 197.

[1849] *Katz/Shapiro*, 8 (2) J. Econ. Persp. 93, 105 (1994); *Rubinfeld*, GRUR Int. 1999, 479, 480. Beispiel für einen solchen de-facto-Standard, der aus Netzwerkeffekten resultiert, ist die VHS-Videokassette, *Shapiro/Varian*, S. 229.

[1850] *European Communication Council* (Hrsg.), S. 216; *Rubinfeld*, GRUR Int. 1999, 479, 484 f.

nach diesem Standard anbieten sollte. Es ist auch denkbar und mitunter effizienter, wenn mehrere Unternehmen Produkte anbieten, die alle einem gemeinsamen Standard entsprechen und untereinander kompatibel sind.[1851]

Netzwerkeffekte bergen die Gefahr einer Innovationsbehinderung. Nachdem sich ein System aufgrund von Netzwerkeffekten am Markt durchgesetzt hat, können ökonomisch effizientere oder technisch überlegene und innovativere Lösungen am Markt scheitern, da sie sich neben dem Marktbeherrscher nicht durchsetzen können.[1852] Dadurch können Netzwerkeffekte dazu führen, daß sich am Markt langfristig ein suboptimales System durchsetzt. Es entsteht ein sogenannter „Lock-In" auf das suboptimale System.[1853] Als Beispiele für solche suboptimalen Systeme werden der Erfolg der QWERTY-Tastatur[1854] und die Durchsetzung des VHS-Videoformats gegenüber dem Betamax-Format genannt.[1855]

Netzwerkeffekte sind komplexe und faktenspezifische Phänomene, die einer fundierten empirischen Analyse bedürfen. Generalisierende Aussagen über Netzwerkeffekte laufen Gefahr, mit der Realität nichts mehr zu tun zu haben.[1856] So können Netzwerkeffekte unterschiedlich stark ausgeprägt sein. In physikalischen Netzwerken wirken sie regelmäßig viel stärker als in virtuellen Netzwerken.[1857] Netzwerkeffekte können so schwach sein, daß sie für die rechtsökonomische Analyse praktisch vernachlässigt werden können.[1858] In der ökonomischen Literatur sind die

---

[1851] *Lemley/McGowan*, 86 Cal. L. Rev. 479, 497 (1998); *Rubinfeld*, GRUR Int. 1999, 479, 480 f. S. dazu auch unten Teil 4, D I 1.

[1852] *Monopolkommission*, IX. Hauptgutachten, Tz. 831; *European Communication Council* (Hrsg.), S. 216; *Rubinfeld*, GRUR Int. 1999, 479, 480; *Katz/Shapiro*, 8 (2) J. Econ. Persp. 93, 106 (1994); *Lemley/McGowan*, 86 Cal. L. Rev. 479, 497 (1998); *Gröhn*, S. 48 ff.

[1853] S. dazu auch unten Teil 3, B I 2 b cc 3.

[1854] S. oben Fn. 1833.

[1855] Sowohl die empirischen wie theoretischen Grundlagen dieser Aussage sind aber nicht unumstritten; s. dazu *Gröhn*, S. 48 ff.; *Lemley/McGowan*, 86 Cal. L. Rev. 479, 497 (1998).

[1856] *Lemley/McGowan*, 86 Cal. L. Rev. 479, 487, 594, 609 f. (1998); s. a. *Rubinfeld*, GRUR Int. 1999, 479, 480.

[1857] Vgl. *Lemley/McGowan*, 86 Cal. L. Rev. 479, 590 f., 592, 601 (1998).

[1858] *Lemley/McGowan*, 86 Cal. L. Rev. 479, 601 (1998), bringen als Beispiel die Anbringung von Tankdeckeln an Autos: An manchen Autotypen ist der Tankdeckel auf der rechten Seite, an manchen Autotypen auf der linken Seite angebracht. Dies führt dazu, daß die Autofahrer an Tankstellen mitunter mit der falschen Wagenseite an der Zapfsäule halten. Man könnte argumentieren, daß aufgrund von Netzwerkeffekten eine einheitliche Anbringung der Tankdeckel effizienzsteigernd wäre. Dennoch kommt es nicht zu dieser Vereinheitlichung. Die Entscheidung eines Konsumenten, einen bestimmten Autotyp zu kaufen, wird nämlich von der Anbringung des Tankdeckels nicht beeinflußt. Konsumenten kaufen Autos, keine Tankdeckel. Die eventuell bestehenden Netzwerkeffekte sind zu schwach, um irgendeine rechtlich relevante Auswirkung zu haben.

Auswirkungen von Netzwerkeffekten auf theoretischer wie auf empirischer Ebene umstritten.[1859] Sie sollten in rechtsökonomischen Analysen mit Vorsicht verwendet werden. Vor einer unkritischen Anwendung neuer, noch teilweise ungeklärter Konzepte ist zu warnen.[1860]

Trotz dieser Vorbehalte soll im folgenden untersucht werden, welche Aussagen das Konzept der Netzwerkeffekte zu der Frage beisteuern kann, ob ein Wettbewerb zwischen verschiedenen DRM-Systemen mit unterschiedlich ausgestalteten technischen Schutzniveaus denkbar erscheint. Würden in diesem Bereich Netzwerkeffekte greifen, könnte ein solcher Wettbewerb verhindert werden und ein möglicherweise Lock-In auf ein gesellschaftlich suboptimales DRM-System entstehen. Im folgenden sollen drei unterschiedliche Arten von Netzwerkeffekten untersucht werden, die in DRM-Systemen auftreten können.

(**b**) **Indirekte Netzwerkeffekte bei DRM-Systemen.** Um digitale Inhalte ein DRM-Systems zu nutzen, muß der Konsument bei sich eine oder mehrere DRM-Komponenten installieren. Diese Komponenten können entweder spezielle Hardwaregeräte (DVD-Player, Set-Top-Box, digitaler Videorekorder) oder eine spezielle Abspielsoftware sein. Man kann diese Komponenten auch als Endgeräte bezeichnen. In einem DRM-System werden die Inhalte in einem besonderen Dateiformat angeboten werden, das nur mit Hilfe DRM-kompatibler Endgeräte benutzt werden kann. Zwischen den Inhalten und dem Endgerät besteht ein Komplementärverhältnis: Die Inhalte lassen sich nur mit Hilfe des DRM-Endgeräts nutzen, und das DRM-Endgerät ist für den Konsumenten nur nützlich, wenn dafür entsprechende Inhalte verfügbar sind. Für den Konsumenten steigt der Nutzen des Endgeräts wie auch des DRM-Systems insgesamt mit der Anzahl der Inhalte, die in diesem DRM-System und für dieses DRM-Endgerät angeboten werden.[1861] Das ist vergleichbar mit den indirekten Netzwerkeffekten bei Betriebssystemen, Videorekordern und CD-Playern, die oben dargestellt wurden:[1862] In allen Fällen steigt der Nutzen eines bestimmten technischen Systems mit der Anzahl der Inhalte, die in diesem System genutzt werden können. Diese indirekten Netzwerkeffekte führen bei DRM-Systemen dazu, daß die Anzahl der Konsumenten des DRM-

[1859] Vgl. *Liebowitz/Margolis*, 8 (2) J. Econ. Persp. 133, 149 (1994): „Although network *effects* are pervasive in the economy, we see scant evidence of the existence of network *externalities*. [… Network effects] carry no special likelihood of market failure, or externaility. […] the *a priori* case for network externalities is treacherous and the empirical case is yet to be presented" (Hervorhebungen im Original); *Lemley/McGowan*, 86 Cal. L. Rev. 479, 485, 591 (1998), die auf S. 610 meinen: „We do not know nearly as much as we would like about how networks work and what they mean for market structure; what we do know suggests that network ‚effects' may have either positive or negative ramifications depending on a whole host of factors."

[1860] Ebenso *Lemley/McGowan*, 86 Cal. L. Rev. 479, 486 (1998).

[1861] S. a. *Messerschmitt/Szyperski*, S. 8.

[1862] S. Teil 3, B I 2 b cc 2 a.

Systems umso höher ist, je höher die Anzahl der für das System verfügbaren Inhalte ist. Mit steigender Zahl der Konsumenten steigt aber wieder die Anzahl der Inhalte. Dies führt zu den beschriebenen positiven Rückkoppelungen. Der Netzwerkeffekt verselbständigt sich und führt dazu, daß sich die Stellung des dominanten DRM-Systems am Markt verstärkt und konkurrierende DRM-Systeme zunehmend vom Markt verdrängt werden.[1863] Indirekte Netzwerkeffekte können einen Wettbewerb unterschiedlicher DRM-Systeme verhindern.[1864]

(c) **Auswirkungen indirekter Netzwerkeffekte des Betriebssystems.** Computerbetriebssysteme unterliegen starken indirekten Netzwerkeffekten. Der Nutzen eines Betriebssystems steigt für den Konsumenten mit der Zahl der Anwendungssoftware, die für dieses Betriebssystem angeboten wird.[1865] Dies führt zu einem Lock-in[1866] der Konsumenten auf ein einheitliches Betriebssystem. Diese Situation kann der Anbieter des Betriebssystems ausnutzen. Wenn er in das etablierte Betriebssystem ein DRM-

[1863] Die Praxis scheint dies zu bestätigen. Das DVD-System verfügt über mehrere DRM-Komponenten, s. dazu oben Teil 1, D II 3. In den letzten Jahren hat sich die DVD als de-facto-Standard für digitale Videoinhalte durchgesetzt. Eine Alternative, auf die ein Konsument ausweichen könnte, wenn er mit der Ausgestaltung der DRM-Komponenten nicht einverstanden wäre, existiert nicht. Das einzige alternative DRM-System für DVDs, das in den USA unter dem Namen „Divx" angeboten wurde, wurde mangels Erfolg nach nur einem Jahr wieder vom Markt genommen. Divx-DVDs konnten auf einem normalen DVD-Spieler nicht abgespielt werden; s. dazu oben Fn. 538. Diese Betrachtung hängt allerdings davon ab, welche Systeme man als Substitute für DVDs betrachtet. So könnte man vertreten, analoge Videokassetten seien Substitute für DVDs und verfügten über ein anderes DRM-Schutzniveau. Inwieweit DVDs und Videokassetten substitutierbar sind, erscheint aufgrund der Qualitätsunterschiede sowie der Zusatzfunktionen von DVDs aber fraglich. Letztlich handelt es sich um eine empirische Frage.

[1864] Bei softwarebasierten DRM-Systemen ist es dem Konsumenten oft möglich, mehrere DRM-Systeme parallel auf seinem Computer zu installieren. Es könnte eingewandt werden, daß der dargestellte Netzwerkeffekt in einer solchen Umgebung nicht ins Gewicht falle: Wenn in mehreren DRM-Systemen unterschiedliche Inhalte angeboten würden, könne der Konsumenten ja alle DRM-Clientprogramm parallel installieren. Dies sei unproblematisch möglich, würden die entsprechenden DRM-Clientprogramme doch regelmäßig sogar kostenlos angeboten. Dabei wird jedoch außer acht gelassen, daß die Installation eines DRM-Clients zeitaufwendig und mit Lernkosten verbunden ist. Weiterhin finanzieren sich die DRM-Systemanbieter regelmäßig durch eine prozentuale Beteiligung an jeder Transaktion digitaler Inhalte, die über dieses DRM-System getätigt werden. Das kostenlose Angebot der DRM-Clientprogramme ist nur ein Marketingzug. Außerdem ist die Tatsache, daß DRM-Clients kostenlos angeboten werden, gerade ein Indiz für das Vorliegen von Netzwerkeffekten; s. dazu oben Fn. 1847. Schließlich besteht selbst bei Betriebssystemen die Möglichkeit, mehrere Betriebssysteme parallel auf einem Rechner zu betreiben (entweder mit Hilfe sog. „Boot Loader" oder mit speziellen Programmen wie VMware, s. <http://www.vmware.com>). Dennoch unterliegen Betriebssysteme augenscheinlich starken Netzwerkeffekten. Trotz alledem ist zuzugestehen, daß der Netzwerkeffekt bei rein softwarebasierten DRM-Clients nicht so stark ausgeprägt sein wird wie bei Betriebssystemen.

[1865] S. dazu oben bei Fn. 1837.

[1866] Zum Begriff s. unten Teil 3, B I 2 b cc 3.

System integriert, so kann er das DRM-System an den Netzwerkeffekt des Betriebssystems koppeln: Das DRM-System wird sich schnell bei einer großen Anzahl von Nutzern verbreiten. Derzeit läßt sich ein solches Vorgehen bei Microsoft beobachten.[1867] Der Anbieter eines Betriebssystems, das aufgrund starker indirekter Netzwerkeffekte über eine große Kundenbasis verfügt, kann also einem DRM-System auf einen Schlag eine ähnlich große Kundenbasis verschaffen, wenn er das DRM-System in das Betriebssystem integriert. Hat das DRM-System eine gewisse Verbreitung gefunden, greifen zusätzlich die indirekten Netzwerkeffekte des DRM-Systems selbst.[1868] Durch diese Sonderkonstellation bei Betriebssystemen kann der Hersteller eines Betriebssystems den Wettbewerb zwischen verschiedenen DRM-Systemen mit unterschiedlichen technischen Schutzniveaus verhindern.[1869]

(d) **Auswirkungen direkter Netzwerkeffekte digitaler Inhalte.** Die Frage, warum Softwarehersteller Ender der 80er Jahre zunehmend davon abkamen, ihre Produkte mit Kopierschutzverfahren und Dongles technisch zu schützen,[1870] wird auch unter dem Aspekt der Netzwerkeffekte ökonomisch untersucht. Nach diesen Untersuchungen läßt sich der Verzicht auf technische Schutzmaßnahmen bei Computersoftware durch Netzwerkeffekte erklären. Es sei wegen Netzwerkeffekten für Softwarehersteller ertragreicher gewesen, Software ohne technische Schutzmaßnahmen zu vertreiben. Diese Argumentation soll im folgenden überblicksartig dargestellt werden.[1871] Ihre Ergebnisse könnte sich auf heutige DRM-Systeme übertragen lassen.

[1867] Microsoft entwickelt DRM-Technologien, die in den Windows Media Player integriert sind, der wiederum an das Betriebssystem gekoppelt ist. Insbesondere plant Microsoft, den Media Player 8 nur noch in Verbindung mit der neuen Betriebssystem-Version „Windows XP" und nicht mehr als getrenntes Produkt zu vertreiben; s. dazu *Procomp*.

[1868] S. oben Teil 3, B I 2 b cc 2 b.

[1869] Dahinter verbirgt sich die allgemeine Problematik, daß der Anbieter eines Betriebssystems aufgrund starker Netzwerkeffekte eine neue Funktionalität am Markt durchsetzen kann, indem er sie in das Betriebssystem integriert; s. dazu *Rubinfeld*, GRUR Int. 1999, 479, 485 f. Dieser Sondereinfluß ist Gegenstand des Kartellprozesses gegen Microsoft, bei dem es unter anderem um die Frage geht, ob Microsoft Funktionen des „Internet Explorer" in sein Betriebssystem integrieren darf. Eine Darstellung der Problematik solcher Koppelungspraktiken, die im Schnittfeld von Kartell- und Urheberrecht anzusiedeln ist, würde hier zu weit führen. Es soll nur darauf hingewiesen werden, daß auch diese Sonderkonstellation bei Betriebssystemen den Wettbewerb zwischen unterschiedlichen DRM-Systemen beschränken kann. S. zur Betriebssystems- und Microsoft-Problematik die Beiträge in *Eisenach/Lenard* (Hrsg.) und *Lemley/McGowan*, 86 Cal. L. Rev. 479, 500 ff. (1998); *Shelanski/Sidak*, 68 U. Chi. L. Rev. 1, 7 ff. (2001); *Economides*; *Meier-Wahl/Wrobel*, WuW 1999, 28 ff.; *Gröhn*, S. 62 ff.

[1870] S. dazu schon oben Teil 3, B I 2 b cc 1.

[1871] S. zum folgenden *Shy* in: Kahin/Varian (Hrsg.), S. 97, 104 ff.; *Shy/Thisse*, 8 (2) Journal of Economics & Management Strategy 163 ff. (1999); *Conner/Rumelt*, 37 Management Science 125 ff. (1991).

Dabei ist die Situation, in der ein Hersteller beispielsweise eine Textverarbeitungssoftware mit einem Kopierschutz vertreibt, mit der Situation zu vergleichen, in der er den Kopierschutz entfernt hat. Entfernt der Hersteller den Kopierschutz, so erhöht sich dadurch faktisch die Anzahl der Nutzer der Software: Konsumenten mit geringen Vorbehaltspreisen, die nicht bereit sind, die Software zu dem Preis zu erwerben, zu dem der Hersteller die Software anbietet, können die Software nun (unberechtigterweise) kopieren und ebenfalls nutzen (unberechtigte Nutzer). Wie oben dargelegt wurde,[1872] unterliegt Textverarbeitungssoftware starken Netzwerkeffekten: Der Nutzen der Textverarbeitung steigt für den einzelnen Konsumenten in dem Maße, in dem er mit anderen Konsumenten Daten austauschen kann. Entfernt der Softwarehersteller bei einer Textverarbeitungssoftware den Kopierschutz, so vergrößert sich dadurch nicht nur die Nutzerschaft. Vielmehr erhöht sich aufgrund des Netzwerkeffekts der Nutzen der Textverarbeitungssoftware für *alle* Konsumenten, also die berechtigten wie auch die unberechtigten. Dadurch erhöht sich aber auch der Vorbehaltspreis der berechtigten Konsumenten für die Software: Steigt die Anzahl der (berechtigten und unberechtigten) Konsumenten der Software, so sind die berechtigten Konsumenten bereit, mehr für die Software zu zahlen, da ihr Nutzen höher ist.

Die Entfernung des Kopierschutzes bei Textverarbeitungssoftware hat damit drei Auswirkungen: Erstens wird nun eine Anzahl von Konsumenten, die die Software davor nicht erworben haben, die Software ebenfalls – wenn auch unberechtigt – nutzen. Zweitens steigt dadurch aufgrund von Netzwerkeffekten der Vorbehaltspreis der zahlenden Konsumenten. Drittens wird eine gewisse Anzahl von Konsumenten, die früher die Software gekauft haben, sich nun entschließen, die Software nicht mehr zu erwerben, sondern auf eine Raubkopie zurückgreifen. Der Gesamteffekt dieser beiden entgegengesetzten Auswirkungen (höherer Vorbehaltspreis der zahlenden Konsumenten, aber gleichzeitige Verringerung der zahlenden Konsumenten) hängt davon ab, wieviele früher zahlende Konsumenten bei der Beseitigung des Kopierschutzes zu Raubkopierern werden („Wechsel-Konsumenten"). Dies hängt wiederum davon ab, wie hoch die zahlenden Konsumenten Zusatzdienstleistungen schätzen, die der Softwarehersteller nur zahlenden Konsumenten zur Verfügung stellt. Dazu können Handbücher, telefonischer Support und ähnliches zählen. Legen zahlende Konsumenten großen Wert auf solche Zusatzdienstleistungen, so werden viele von ihnen auch bei einer Entfernung des Kopierschutzes die Software weiterhin käuflich erwerben und nicht auf eine Raubkopie ausweichen. Wie beschrieben, steigt der Vorbehaltspreis dieser weiterhin zahlenden Konsumenten durch einen Netzwerkeffekt an. Ist die Erhöhung dieser Vorbehaltspreise größer als die

[1872] S. bei Fn. 1832.

Verluste, die dem Hersteller aus den „Wechsel-Konsumenten" erwachsen, so erhöht die Entfernung des Kopierschutzes den Gewinn des Herstellers. Mit anderen Worten: Der Verlust, der dem Softwarehersteller durch Konsumenten entsteht, die bei einer Entfernung des Kopierschutzes zu Raubkopierern werden, ist in diesem Fall geringer als der zusätzliche Gewinn, den er erhält, weil die berechtigten Konsumenten, die weiterhin die Software käuflich erwerben, aufgrund der Netzwerkeffekte bereit sind, für die Software mehr zu zahlen. Es kann gezeigt werden, daß in einem Softwaremarkt, in dem alle Softwarehersteller ihre Produkte mit einem Kopierschutz versehen, der Gewinn eines Herstellers erhöht werden kann, indem er den Kopierschutz seiner Software entfernt.[1873]

Es zeigt sich, daß Netzwerkeffekte auch dazu führen können, daß ein Inhalteanbieter nicht das höchstmögliche technischen Schutzniveau wählt, weil er seinen Gewinn bei einem niedrigeren Schutzniveau maximieren kann. Insofern könnten die Bedenken, DRM-Systeme würden Inhalteanbietern einen zu weitgehenden Schutz verleihen, übertrieben sein. Grundsätzlich sind die dargestellten Effekte auch in DRM-Systemen denkbar. Jedoch ist zu beachten, daß das Modell von recht engen Annahmen ausgeht, die zudem auf Spezifika der Softwarebranche aufbauen. Einerseits hängen seine Aussagen davon ab, daß bei einem Computerprogramm Zusatzleistungen wie Support oder Handbücher angeboten werden, wodurch vermieden wird, daß bei einer Entfernung des Kopierschutzes zu viele bisher zahlende Nutzer zu Raubkopierern werden. Durch Zusatzdienstleistungen werden die Nutzer gleichsam „bei der Stange" gehalten, ihr höherer Vorbehaltspreis wird abgeschöpft und gleicht die Verluste aus den „Wechsel-Konsumenten" aus. Selbst wenn das Modell bei bestimmten Arten von Computersoftware zutreffen mag,[1874] existieren bei digitalen Inhalten wie Video- und Audiodaten oder Text regelmäßig wenig Zusatzdienstleistungen, die zudem für Konsumenten bei weitem nicht so wichtig sind wie Support oder Handbücher bei Computersoftware. Damit ist für die Konsumenten bei einer Entfernung des Kopierschutzes solcher Inhalte der Anreiz ungemein größer, auf Raubkopien auszuweichen. Andererseits hängen die Aussagen des Modells davon ab, daß bei Textverarbeitungssoftware starke Netzwerkeffekte bestehen. Dadurch erhöht sich der Vorbehaltspreis der zahlenden Konsumenten bei einer Vergrößerung der Nutzerschaft in starkem Maße. Dagegen werden bei vielen Audio- oder Videoinahlten und ähnlichem nur sehr schwache bis gar keine Netzwerkeffekte auftreten: Während die Möglichkeit, Da-

[1873] S. zum ganzen *Shy* in: Kahin/Varian (Hrsg.), S. 97, 106 ff. mit einfachem Zahlenbeispiel; formaler *ders.*, S. 67 ff.; s. weiterhin *Shy/Thisse*, 8 (2) Journal of Economics & Management Strategy 163 ff. (1999); s. weiterhin *Watt*, S. 60 f.; *Conner/Rumelt*, 37 Management Science 125 ff. (1991).

[1874] Ob dies der Fall ist, ist letztlich eine empirische Frage.

teien auszutauschen, eines der zentralen Funktionsmerkmale von Textverarbeitungssoftware ist, geht es bei sonstigen digitalen Inhalten um die bloße Nutzung dieser Inhalte.[1875]

Insgesamt können Netzwerkeffekte grundsätzlich auch dazu führen, daß ein Inhalteanbieter auf die Verwendung eines maximalen Schutzes verzichtet. Unter dem Gesichtspunkt, daß ein DRM-System in der Praxis keinen schrankenlosen Schutz gewähren sollte, scheint dies begrüßenswert. Allerdings wird dieser Effekt nur bei ganz bestimmten digitalen Inhalten und unter sehr engen Voraussetzungen eintreten.[1876]

(e) **Zusammenfassung.** Die Frage, ob in DRM-Systemen Netzwerkeffekte auftreten und welche Auswirkungen dies hat, ist komplex und hängt stark von der tatsächlichen Ausgestaltung des jeweiligen DRM-Systems ab. Eine umfassende Analyse müßte einzelne Fallgruppen von DRM-Systemen unterscheiden. So müßte nach Art der vertriebenen Inhalte oder danach unterschieden werden, ob auf einen Software- oder einen Hardware-Schutz gesetzt wird. Trotz dieser Unterschiede zeigt sich, daß die These, ein Wettbewerb zwischen unterschiedlichen DRM-Systemen führe dazu, daß Anbieter keine überbordenden technischen Schutzmaßnahmen einsetzen würden, allzu stark vereinfacht. Netzwerkeffekte können einen Wettbewerb zwischen unterschiedlichen DRM-Systemen verhindern. Selbst wenn die Durchsetzung eines einheitlichen DRM-Standards aus ökonomischer Sicht grundsätzlich zu begrüßen ist, können Netzwerkeffekte dazu führen, daß sich am Markt eine suboptimale Lösung durchsetzt. Qualitätsaspekte einer Technologie sind nicht immer entscheidend für ihren Markterfolg.[1877]

(3) **Lock-in.** Ein Wettbewerb zwischen unterschiedlichen DRM-Systemen setzt voraus, daß ein Konsument, der sich einmal für ein bestimmtes DRM-System entschieden hat, später auf ein anderes DRM-System umsteigen kann, wenn er dies will.[1878] Ein solcher Systemwechsel kann durch hohe Kosten verhindert werden. Sind die Kosten für einen Wechsel der Systemarchitektur („switching costs") größer als der durch den Wechsel

---

[1875] Grundsätzlich können auch bei digitalen Inhalten wie Videos, Musik, Texten u. ä. direkte Netzwerkeffekte bestehen. Einerseits erwerben Konsumenten bestimmte „Kassenschlager" mitunter aus dem Grund, weil alle anderen Konsumenten den „Kassenschlager" auch haben. *Pindyck/Rubinfeld*, S. 127, bezeichnen dies als „bandwagon effect" (Mitläufer-Effekt); s. aber *Pindyck/Rubinfeld*, S. 129 f., zur Begrenzung durch den „Snob-Effekt". Wie stark dieser Netzwerkeffekt ist, hängt vom einzelnen digitalen Inhalt ab und ist letztlich eine empirische Frage.

[1876] Letztlich ist es auch eine empirische Frage, ob dieser Effekt eintritt. So ist fraglich, wie hoch zahlende Nutzer tatsächlich den Nutzern von Zusatzleistungen bei solchen Produkten einschätzen. Davon hängt aber die Aussage des Modells ab.

[1877] S. dazu *Monopolkommission*, XI. Hauptgutachten, Tz. 752.

[1878] Es geht im vorliegenden Abschnitt immer noch um die Konstellation, in der ein Wettbewerb zwischen zwei unterschiedlich schützenden DRM-Systemen besteht; s. dazu allgemein oben Teil 3, B I 2 b cc 1.

entstehende Nutzen, so befinden sich Konsumenten in einer sogenannten „Lock-in"-Situation.[1879] Lock-in-Effekte führen zu einer sehr unelastischen Nachfrage.[1880] Dadurch können Systemanbieter die Preise ihrer Komponenten in die Höhe treiben, ohne Gefahr zu laufen, daß sie Konsumenten verlieren. Bei Lock-In-Effekten können Unternehmen die Konsumentenrente abschöpfen.[1881] Lock-in-Effekte geben dem Unternehmen bis zu einem gewissen Maß eine Monopolstellung.[1882]

Lock-in-Effekte mit entsprechenden „switching costs" sind im E-Commerce-Bereich weit verbreitet.[1883] Sie können auch bei DRM-Systemen auftreten. Die Kosten, von einem DRM-System zu einem anderen zu wechseln, können beträchtlich sein. Dazu gehören die Kosten der Anschaffung neuer Soft- und Hardware sowie der Aufwand, die Benutzung des neuen Systems zu erlernen.[1884] Ein Nutzer hat sich eventuell an die Bedienung und Funktionalität eines DRM-Systems gewöhnt und scheut die Umstellung auf ein anderes System.[1885] In DRM-Systemen werden digitale Inhalte in speziellen Dateiformaten abgespeichert. Wechselt ein Konsument das DRM-System, ist wegen der mangelnden Kompatibilität der unterschiedlichen Systeme nicht unbedingt gewährleistet, daß die Inhalte auch unter dem neuen System genutzt werden können. Mitunter ist eine Konvertierung zwar möglich, aber sehr zeitaufwendig. Bei einem

[1879] *European Communication Council* (Hrsg.), S. 162; *Varian*, S. 589; *Shapiro/Varian*, S. 104; *Shy*, S. 4.

[1880] Bei einer elastischen Nachfrage reagiert die nachgefragte Menge stark auf den Preis: Wenn man den Preis um ein Prozent erhöht, sinkt die nachgefragte Menge um mehr als ein Prozent. Hat ein Gut viele nahe Substitute, so weist es regelmäßig eine elastische Nachfrage auf, während Güter mit wenig nahen Substituten eine unelastische Nachfrage aufweisen, s. *Varian*, S. 259.

[1881] *Varian*, S. 589; *European Communication Council* (Hrsg.), S. 162.

[1882] Befinden sich Konsumenten in einer Lock-In-Situation, so kann das entsprechende Unternehmen den Produktpreis über die Grenzkosten anheben, bis der Preis über der Summe von Grenzkosten und „Switching costs" liegt. Erst ab diesem Preis lohnt es sich für den Konsumenten, zu einem anderen Anbieter auszuweichen; s. *Shy*, S. 5, 15. Hat ein Unternehmen einmal einen solchen Lock-in-Effekt erreicht, stehen ihm unterschiedliche Möglichkeiten zur Verfügung, um diesen Effekt und die Kundenbindung aufrechtzuerhalten. Beispiel dafür sind Vielfliegerprogramme von Fluggesellschaften, die Einführung neuer proprietärer Funktionen, der Verkauf komplementärer Produkte etc.; s. dazu *Shapiro/Varian*, S. 127 ff., 156 ff.

[1883] Vgl. *Shapiro/Varian*, S. 105 ff. Lock-in-Situationen überschneiden sich mitunter mit Situationen der Pfadabhängigkeit und von Netzwerkeffekten. Bei einer Pfadabhängigkeit hängt das derzeitige Verhalten der Konsumenten von ihren früheren Entscheidungen ab. Zum Begriff der Pfadabhängigkeit s. *Margolis/Liebowitz* in: Newman (Hrsg.), Band 3, S. 17 ff.; zur Abgrenzung zwischen Netzwerkeffekten und Pfadabhängigkeit allgemein *Lemley/McGowan*, 86 Cal. L. Rev. 479, 597 f. (1998).

[1884] *Varian*, S. 589; *Shapiro/Varian*, S. 104, 116 ff.; *Shy*, S. 4 f.; *Lemley*, 28 Conn. L. Rev. 1041, 1050 (1996).

[1885] Vgl. *Shapiro/Varian*, S. 121 f.

Wechsel des DRM-Systems verliert der Nutzer also eventuell sein persönliches Musik-/Video-/Buch-Archiv. Auch dies führt zu einem Lock-in.[1886]

In DRM-Systemen können damit hohe „switching costs" zu einem Lock-in führen. Dadurch werden Konsumenten gehindert, von einem DRM-System auf ein anderes umzusteigen. Dies behindert einen Wettbewerb zwischen unterschiedlichen DRM-Systemen.

c) Ergebnis

Auch wenn die ökonomischen Grundlagen urheberrechtlicher Schrankenbestimmungen noch in weiten Teilen unklar und umstritten sind, läßt sich festhalten, daß Schrankenbestimmungen im Bereich des Urheberrechts aus ökonomischer Sicht vielfältige und wichtige Aufgaben übernehmen. Unter anderem unterstützen sie dynamische Innovationsprozesse. Der Schutz durch DRM-Systeme ist dem urheberrechtlichen Schutz in vielen Aspekten vergleichbar. Auch die Gründe, warum das Urheberrecht durch Schrankenbestimmungen beschränkt wird, sind auf DRM-Systeme übertragbar.

Wegen der weitreichenden Schutzpotentiale von DRM-Systemen könnten Inhalteanbieter in DRM-Systemen ein umfassendes und nahezu unbegrenztes Schutzniveau etablieren. Setzen DRM-Systeme urheberrechtliche Schrankenbestimmungen auf technischem oder vertraglichem Weg außer Kraft, erscheint dies aus ökonomischer Sicht problematisch. Zwar wird die These vertreten, daß sich der Wettbewerb zwischen unterschiedlichen Inhalteanbietern und DRM-Systemen dieses Problems annehmen werde. Der Wettbewerb werde dazu führen, daß sich überbordende vertragliche und technische Schutzmechanismen am Markt nicht durchsetzen können. Diese These vernachlässigt jedoch unterschiedliche Marktversagen, die bei DRM-Systemen auftreten können. Zwar sind die Auswirkungen von Informationsasymmetrien, Netzwerkeffekten und Lock-In-Situationen komplex und oft von den einzelnen Gegebenheiten eines DRM-Systems abhängig. Es spricht jedoch einiges dafür, daß ein Wettbewerb zwischen Inhalteanbietern und DRM-Systemen nicht ausreicht, um urheberrechtlichen Schrankenbestimmungen im DRM-Umfeld Geltung zu verschaffen.

3. Funktion des herkömmlichen Urheberrechts

Die bisherigen rechtsökonomischen Untersuchungen haben ergeben, daß DRM-Systeme zunehmend Aufgaben des Urheberrechts übernehmen könnten. Die ineinandergreifenden Schutzmechanismen eines DRM-Systems können digitale Inhalte vom nicht-exklusiven zum exklusiven Gut machen. Aus ökonomischer Sicht kommt DRM-Systemen damit die glei-

[1886] *Shapiro/Varian*, S. 122 f.; *Kulle*, S. 253; *Shy*, S. 4, 15. Man mag dies – wie *Lemley*, 28 Conn. L. Rev. 1041, 1050 (1996) – auch als „Pfadabhängigkeit" bezeichnen; s. dazu oben Fn. 1883.

che Aufgabe zu wie dem Urheberrecht. Dann stellt sich aber die Frage, welche Bedeutung das Urheberrecht in diesem Umfeld noch hat: Das Marktversagen, aufgrund dessen das Urheberrecht geschaffen wurde – die Nicht-Exklusivität von Information – besteht in DRM-Systemen nicht mehr.[1887] Im folgenden soll gezeigt werden, daß dem herkömmlichen Urheberrecht aus rechtsökonomischer Sicht auch in diesem Umfeld noch eine Aufgabe zukommen kann.

DRM-Systeme können auf einem vertraglichen Schutz aufbauen. Der Inhalteanbieter räumt den Nutzern nach Abschluß eines Nutzungsvertrags die faktische Möglichkeit ein, einen bestimmten Inhalt auf eine bestimmte Weise zu nutzen.[1888] Das herkömmliche Urheberrecht kann diesen vertraglichen Schutz unterstützen. Würde ein Inhalteanbieter seine digitalen Inhalte alleine auf vertraglicher Basis schützen, ohne daß ihm unterstützend ein Urheberrecht zur Verfügung stünde,[1889] so müßten in den Nutzungsverträgen umfangreiche Bestimmungen über die erlaubten Nutzungen enthalten sein. Ohne das Urheberrecht wäre beispielsweise nicht festgelegt, wer Inhaber des Vervielfältigungsrechts ist, was unter einer Vervielfältigung zu verstehen ist und welche Fälle unter diesen Begriff fallen. Müßten sich die Vertragsparteien vor Abschluß eines DRM-Nutzungsvertrags erst über solche Fragen einigen, könnte dies zu einer starken Erhöhung der Transaktionskosten führen. In einem solchen Umfeld kann es aus ökonomischer Sicht sinnvoll sein, den Vertragsparteien gesetzlich klare Rechtebündel zuzuweisen, die als Ausgangspunkt für Nutzungsverträge genommen werden können. Zugewiesene „property rights“ können als Ausgangspunkt für Transaktionen dienen und, sofern sie eindeutig zugewiesen und klar definiert sind, Transaktionskosten senken.[1890] Sie ermöglichen es den Parteien unabhängig davon, wem die „property rights“ zugewiesen wurden, durch Tausch eine Pareto-effiziente Allokation zu erzielen.[1891] Gerade im Massenmarkt, in dem eine Vielzahl von Nutzungsverträgen auftreten, können klar definierte „property rights“ effizienzsteigernd wirken.[1892]

[1887] S. dazu ausführlich Teil 3, A III 2 b.

[1888] Dabei können Nutzungsverträge in DRM-Systemen nicht grundsätzlich mit urheberrechtlichen Nutzungsverträgen gleichgesetzt werden, s. dazu oben Teil 3, A II 1 b aa.

[1889] Dies ist in DRM-Systemen grundsätzlich denkbar. Inhalteanbieter in DRM-Systemen sind insofern Inhabern eines Geschäftsgeheimnisses vergleichbar, die das Geschäftsgeheimnis auf rein vertraglicher Basis schützen, ohne daß ihnen das Gesetz ein umfassendes Ausschließlichkeitsrecht zugewiesen hätte. S. dazu schon oben Teil 3, A II 1 b aa.

[1890] S. dazu *Cooter/Ulen*, S. 89; *Gordon/Bone* in: Bouckaert/De Geest (Hrsg.), Band II, Kap. 1610, S. 189, 195; *Easterbrook*, 1996 U. Chi. Legal F. 207, 209, 211.

[1891] Vgl. *Varian*, S. 558.

[1892] S. a. *Merges* in: Mowery (Hrsg.), S. 272, 282 f., der Immaterialgüterrechte in diesem Zusammenhang als „off-the-rack-contract“ bezeichnet. Zu den darauf aufbauenden neoklassischen Erklärungsansätzen des Urheberrechts s. oben Fn. 1726.

Auf die einzelnen Auswirkungen und Grenzen dieser Argumentation kann hier nicht eingegangen werden.[1893] Es spricht jedoch einiges dafür, daß das herkömmliche Urheberrecht im DRM-Bereich zwar nicht mehr primäres Schutzinstrument ist, daß es aber die Effizienz eines anderen Schutzinstruments – nämlich des Schutzes durch Nutzungsverträge – deutlich erhöht.

Auch im Bereich technischer Schutzmaßnahmen zeigt sich aus ökonomischer Sicht, daß Schutzmechanismen des Gesetzgebers im DRM-Bereich zunehmend die Aufgabe zukommt, die Effektivität anderer Schutzmechanismen zu erhöhen: Viele technische Schutzmaßnahmen in DRM-Systemen können umgangen werden. Um dies zu verhindern, werden große finanzielle Aufwendungen getätigt, um immer sicherere tech-

[1893] So scheint es keinesfalls Voraussetzung für einen vertraglichen Schutz von Information zu sein, daß diese Information durch ein „property right" geschützt wird. Heute wird eine Vielzahl von Information auf vertraglicher Basis geschützt, ohne gleichzeitig durch ein Immaterialgüterrecht geschützt zu sein. Als Beispiele sei Know-How oder – in den USA – bloße Daten einer Datenbank genannt. Seit der Entscheidung des U.S. Supreme Courts in Sachen Feist (s. oben Fn. 1592) sind U.S.-amerikanische Datenbankhersteller hauptsächlich auf vertragliche Schutzmechanismen angewiesen, s. *Reichman/Franklin*, 147 U. Penn. L. Rev. 875, 884 f., 888 f. (1999). Trotz dieses geringen immaterialgüterrechtlichen Schutzniveaus ist der Weltmarktanteil von U.S.-Datenbankherstellern sehr hoch; unter Einbeziehung gedruckter Informationen gehen Schätzungen von bis zu 70% aus, *Reichman/Franklin*, a. a. O., S. 895 Fn. 76. Zum Teil wird vertreten, daß gerade dieses geringe Schutzniveau zur heutigen Dominanz der U.S.-Anbeiter geführt habe, s. *Reichman/Franklin*, a. a. O., S. 895 f., 912; *Garon*, 17 Cardozo Arts & Ent. L. J. 491, 571 ff., 606 (1999). Daneben untersuchte *Merges* die Effizienz des japanischen Softwaremarkts, der stark von der „keiretsu"-Unternehmensstruktur geprägt ist. Er versuchte zu zeigen, daß der Softwareschutz in diesem System, der auf einem vertraglichen Schutz aufbaut, ineffizienter sei als der im Westen vorherrschende Softwareschutz durch ein Immaterialgüterrecht; s. dazu *Merges* in: Mowery (Hrsg.), S. 272, 282 f.; *ders.*, 93 Mich. L. Rev. 1570, 1587 ff. (1995). Die Richtigkeit dieser Analyse und der ihr zugrundliegenden Annahmen wird jedoch bezweifelt, s. *Mashima*, 33 Int'l Law. 119 ff. (1999); *dies.*, 82 J. Pat. & Trademark Off. Soc'y 203 ff. (2000). Weiterhin werden allgemeine Zweifel an der These vorgebracht, daß klar definierte „property rights" effizienzsteigernd wirken. So legen *Ayres/Talley*, 104 Yale L. J. 1027 ff. (1995), im Umfeld des Systems der „property rules" und „liability rules" von *Calabresi* und *Melamed* dar, daß die Aufteilung von „property rights" auf mehrere Inhaber sowie deren unklare oder geteilte Zuweisung die Beteiligten dazu anregen kann, eine Lösung auf vertraglichem Wege zu finden. Im Gegensatz zur Zuweisung umfassender klarer „property rights" könnten in einem solchen System das strategische Verhalten der Vertragsparteien gemindert werden und letztlich effizientere Ergebnisse erzielt werden. Im urheberrechtlichen Bereich vertritt *Burk* die These, bei unklaren Zuweisungen von „property rights" – von ihm „muddy entitlements" genannt – seien die Beteiligten gezwungen, auf vertraglichem Wege eine effiziente Verteilung zu erreichen. Die amerikanische „fair use defense" sei eine solche unklare Zuweisung: Es sei vor einem Gerichtsprozeß praktisch unmöglich zu bestimmen, ob eine bestimmte Nutzungshandlung unter die „fair use defense" falle oder nicht. Eine solche Zuweisungsstruktur sei zu bevorzugen; s. *Burk*, 21 Cardozo L. Rev. 121, 139 (1999); s. a. *Johnston*, 11 J. L. Econ. & Org. 256 ff. (1995). Die These, klar definierte „property rights" hätten eine effizienzsteigernde Wirkung, müßte zunächst diese Einwände entkräften.

nische Schutzmaßnahmen zu entwickeln. Gleichzeitig passen sich Angreifer dieser Entwicklung an und verwenden immer mehr Zeit und Energie, um diese neuen Schutzmaßnahmen zu knacken.[1894] Dadurch entsteht ein Technologie-Wettbewerb zwischen den Entwicklern technischer Schutzmaßnahmen und den Entwicklern von Umgehungsvorrichtungen.[1895] Die in diesem Technologie-Wettbewerb getätigten finanziellen Aufwendungen werden anderen, produktiveren Bereichen – beispielsweise der Erstellung der Inhalte selbst – entzogen. Es erscheint daher sinnvoll, mit Hilfe staatlicher Intervention den Technologie-Wettbewerb zu stoppen beziehungsweise zu kontrollieren. Diesem Zweck dienen rechtliche Vorschriften, die die Umgehung technischer Schutzmaßnahmen verbieten: Sie erhöhen die Kosten der Entwickler von Umgehungsvorrichtungen auf ein Niveau, in dem diese aus dem Technologie-Wettbewerb aussteigen.[1896]

Insgesamt zeigt sich, daß das Urheberrecht auch in DRM-Systemen wichtige Aufgaben übernimmt, seine Aufgabe als primäres Schutzinstrument jedoch sinkt.

4. Zusammenfassung

Die ökonomische Analyse von DRM-Systemen ist komplex und führt zu ambivalenten Ergebnissen.[1897] Die ökonomischen Zusammenhänge des Urheberrechts und von DRM-Systemen sind teilweise unklar oder werden – je nach Zielsetzung – in einer bestimmten Richtung instrumentalisiert.[1898] Wir sind weit davon entfernt, die Zusammenhänge einer Informationsökonomie zu verstehen. Heute kann niemand sagen, welche Art von Ausschließlichkeitsrechten mit welchem Schutzniveau in einer Informationsgesellschaft aus ökonomischer Sicht optimal sind.

Die Arbeit kann keine abschließende Antwort auf die umfangreichen ökonomischen Fragen geben, die sich im Zusammenhang mit DRM-Systemen stellen. Manche Bestandteile der ökonomischen Analyse von

---

1894 Vgl. *Smith/Weingart*, 31 Computer Networks 831, 838 (1999).

1895 *Elkin-Koren/Salzberger*, 19 Int'l. Rev. L. & Econ. 553, 560 (1999); *Watt*, S. 57.

1896 *Elkin-Koren/Salzberger*, 19 Int'l. Rev. L. & Econ. 553, 560 f. (1999); *Fisher*, 73 Chi.-Kent L. Re. 1203, 1233 (1998); *Burk*, 73 Chi.-Kent L. Rev. 943, 994 (1998); *Hardy*, 1996 U. Chi. Legal F. 217, 251; ähnlich *Wand*, S. 2; kritisch *Burk*, 21 Cardozo L. Rev. 121, 172 f. (1999).

1897 *Easterbrook*, 4 Tex. Rev. L. & Pol. 103, 107 (1999), meint in diesem Zusammenhang lakonisch: „If firms that put millions of dollars on the line cannot make reliable decisions about technology, what whould make us think that scholars with *no* money on the line do well at devising legal rules to govern technology?" (Hervorhebung im Original).

1898 *Boyle*, 53 Vand. L. Rev. 2007, 2037 (2000), meint: „Intellectual property policy has consistently under-valued the public domain, over-emphasized the threats and under-emphasized the opportunities presented by new technologies, ignored the extent to which information and information goods are actually bundled with other more excludable phenomena, exaggerated the role that incentives have in producing innovation while minimizing their negative effects, and so on."

DRM-Systemen sind in ihrem theoretiscchen Fundament derzeit noch lückenhaft. Das gilt beispielsweise für das Preisdiskriminierungs- und das Transaktionskosten-Argument. Relativ klar scheint dagegen zu sein, daß aus rechtsökonomischer Sicht Beschränkungen des DRM-Schutzes notwendig sind.[1899] Die These, daß ein Wettbewerb zwischen unterschiedlichen Inhalteanbietern oder DRM-Systemen zu einem ausgewogenen Schutzniveau führt, vernachlässigt Informationsasymmetrien, Netzwerkeffekte, Kompatibilitäts-Erfordernisse und Lock-in-Effekte, die alle wettbewerbshindernde Wirkung haben können.

Wie der DRM-Schutz und urheberrechtliche Schrankenbestimmungen aus ökonomischer Sicht am besten ineinandergreifen sollten, ist eine schwierige Frage. *William Fisher* schlägt in seiner Analyse von DRM-Systemen[1900] eine Kombination aus umfangreicher Preisdiskriminierung und umfangreichen Schrankenbestimmungen vor: Indem DRM-Systeme umfangreiche Möglichkeiten der Preisdiskriminierung böten, sei ihre Anreizwirkung im Vergleich zum Urheberrecht deutlich stärker.[1901] Um einen zu weitgehenden Schutz der Inhalteanbieter zu vermeiden, müsste daher im Gegenzug der Anwendungsbereich urheberrechtlicher Schrankenbestimmungen deutlich ausgeweitet werden. Nur in diesem Fall sei im Ergebnis der Schutz des Inhalteanbieters durch DRM-Systeme dem ausgewogenen Schutz des Urhebers durch das Urheberrecht vergleichbar.[1902]

[1899] Auch diese Aussage ist jedoch mit Vorsicht zu genießen. Selbst wenn ein Wettbewerb zwischen DRM-Systemen oder Inhalteanbietern unrealistisch ist, heißt das nicht notwendigerweise, daß ein Eingreifen des Gesetzgebers unter ökonomischen Gesichtspunkten vorzuziehen wäre. Dies läßt sich schon im Bereich des Urheberrechts aufzeigen. Es ist eine gängige These, das Urheberrecht schaffe einen gerechten Ausgleich zwischen den Interessen der Urheber und der Allgemeinheit. Bedenkt man die Aussagen der „Public Choice"-Theorie, so könnte man an dieser These zweifeln. So wird vorgebracht, die ständige Ausdehnung der Dauer, Umfang und Stärke des Urheberrechts in den letzten Jahrzehnten zeige, daß das geltende Urheberrecht allenfalls einen politischen Kompromiß zwischen unterschiedlichen Lobbyistengruppen darstelle. Ein starker Lobbyismus führe zu einer Konzentration von Sondervorteilen bei den Mitgliedern organisierter Interessengruppen und zu einer breiten Streuung der Nachteile, auch auf weniger organisierte Gesellschaftsteile (sog. „rent seeking"). Dies führe zu einem „Politikversagen"; so *Bell*, Escape from Copyright, S. 32 f., 38; s. dazu allgemein *Van den Hauwe* in: Bouckaert/De Geest (Hrsg.), Band I, Kap. 0610, S. 615 f.; *Kirsch*, S. 301 f.; *Müller*, S. 70; *Monopolkommission*, Systemwettbewerb, S. 12 ff, Tz. 7. Von einem gerechten Ausgleich aller Interessen könne beim Urheberrecht keine Rede sein. Selbst wenn der Gesetzgeber einen gerechten Ausgleich finden wollte, sei ihm dies aufgrund starker Informationsdefizite gar nicht möglich, *Bell*, Escape from Copyright, S. 38 f. Eine vollständige Analyse im Bereich des Urheberrechts und von DRM-Systemen müßte diese beiden Imperfektionen – Marktversagen und Politikversagen – gewichten und gegeneinander abwägen. Zur „Public Choice"-Theorie allgemein s. *Kirsch*; im Überblick *Van den Hauwe* in: Bouckaert/De Geest (Hrsg.), Band I, Kap. 0610, S. 603 ff.; *Müller*, S. 68 ff.

[1900] S. dazu auch oben bei Fn. 1583 ff.

[1901] *Fisher*, 73 Chi.-Kent L. Rev. 1203, 1240, 1251 (1998).

[1902] *Fisher*, 73 Chi.-Kent L. Rev. 1203, 1240, 1251 f. (1998).

Im Vergleich zum Schutz durch das Urheberrecht sei dieses DRM-Szenario sogar zu bevorzugen: Wegen der Möglichkeit der Preisdiskriminierung entfalle in DRM-Systemen der „deadweight loss", der im Urheberrecht zu Wohlfahrtsverlusten führt.[1903] Damit würden preisdiskriminierende DRM-Systeme das Beste aus beiden Welten vereinen: Einerseits eine optimale Anreizwirkung für potentielle Inhalteanbieter (das heißt kein Wohlfahrtsverlust durch Unterproduktion), andererseits eine optimale Nutzung der Inhalte durch die Konsumenten (das heißt kein Wohlfahrtsverlust durch Unternutzung).[1904] Träfen die Annahmen des Preisdiskriminierungs-Arguments tatsächlich zu und könnten seine konzeptionellen Schwächen beseitigt werden,[1905] wäre dieser Vorschlag unter ökonomischen Gesichtspunkten eine verblüffend elegante Lösung des Problems der Information als öffentlichem Gut.

II. Rechtliche Überlegungen

1. Allgemeines

> *What we face, in a word, is the imminent privatization, or „shrink-wrapping", of […] copyright law.*[1906]

Im Vergleich zum Urheberrecht bieten DRM-Systeme für den Inhalteanbieter einige Vorteile. Vertragliche und technische Schutzmechanismen können individueller auf die Vorstellungen des Inhalteanbieters abgestimmt werden und sind damit flexibler als das notwendigerweise pauschalierende Urheberrecht.[1907] Vertragliche und technische Schutzmechanismen könnten bei grenzübergreifenden Transaktionen einen besseren Schutz bieten als das Urheberrecht. Das Urheberrecht unterliegt dem Territorialitätsprinzip, wodurch sich in verschiedenen Ländern unterschiedliche Schutzniveaus ergeben können. Der Urheber hat auf die Rechtsordnung, durch die sein Werk jeweils geschützt wird, aber nur geringen Einfluß.[1908] DRM-Systeme ermöglichen dem Inhalteanbieter einen weltweit einheitlichen Schutz ohne jeglichen Niveauunterschied.[1909]

[1903] S. dazu oben Teil 3, A III 2 c.

[1904] *Fisher*, 73 Chi.-Kent L. Rev. 1203, 1252 (1998); kritisch *Cohen*, 53 Vand. L. Rev. 1799, 1815 ff. (2000).

[1905] S. dazu oben Teil 3, B I 1 b.

[1906] *McManis*, 87 Cal. L. Rev. 173 (1999).

[1907] Ebenso *Merges*, 12 Berkeley Tech. L. J. 115, 119 (1997). Die hohe Flexibilität ist ein allgemeines Charakteristikum technischer Regulierungsmechanismen, *Reidenberg*, 76 Tex. L. Rev. 553, 579 f. (1998).

[1908] S. zu diesem Themenkreis *Intveen*; *Hoeren* in: Hoeren/Sieber (Hrsg.), Teil 7.10; *Bechtold*, GRUR 1998, 18, 22 f.

[1909] Auch dies ist ein allgemeiner Vorteil technischer Regulierungsmechanismen, s. *Reidenberg*, 76 Tex. L. Rev. 553, 577 ff. (1998), der auf S. 578 meint: „[…] the jurisdiction of Lex Informatica is the network itself."

Es ist daher nicht verwunderlich, daß Inhalteanbieter zunehmend auf technische und vertragliche Schutzmechanismen setzen. DRM-Systeme schaffen durch das Ineinandergreifen mehrerer Schutzmechanismen ein Schutzniveau, das dem eines absoluten Rechts entspricht. Sie stellen in ihrer stärksten Ausgestaltung praktisch ein in Silikon gegossenes Urheberrecht dar.[1910] Das Besondere an DRM-Systemen ist, daß der Inhalteanbieter bei mehreren Schutzmechanismen (Schutz durch Technik, Schutz durch Nutzungsverträge, Schutz durch Technologie-Lizenzverträge) selbst den Schutzumfang und das Schutzniveau festlegen kann. Er muß nicht auf eine gesetzliche Ausgestaltung des Schutzmechanismus zurückgreifen, sondern kann den Schutzmechanismus in weiten Grenzen selbständig gestalten.[1911]

Wir bewegen uns damit von einer Situation, in der Schutzumfang und -intensität durch das Urheberrecht festgelegt wurde, hin zu einer Situation, in der Schutzumfang und intensität durch private Parteien festgelegt werden, die sich zu diesem Zweck einer Kombination aus technischen Schutzmaßnahmen, Nutzungsverträgen und Lizenzverträgen bedienen.[1912] Das Recht unterstützt diese Entwicklung, indem zunehmend Nutzungsverträge als wirksam anerkannt werden und der Gesetzgeber die Umgehung technischer Schutzmaßnahmen verbietet. DRM-Systeme stellen für die Schutzinteressen der Inhalteanbieter eher einen Ersatz als eine Ergänzung des Urheberrechts dar. Ausschließlichkeitsrechte werden nicht mehr durch den Gesetzgeber, sondern durch private Parteien mit Hilfe technischer und vertraglicher Schutzmechanismen definiert.[1913] Wie auch in anderen Bereichen des Internet-Rechts[1914] läßt sich eine *Privatisierung des Rechtsschutzes* beobachten.[1915]

In diesem Umfeld stellt sich die Frage, welche Bedeutung dem Urheberrecht aus rechtlicher Sicht noch zukommt. Einerseits könnte das Urheberrecht bedeutsam werden, wenn technische oder vertragliche Schutzmechanismen versagen (dazu unten 2). Andererseits könnte dem

---

[1910] S. dazu ausführlich oben Teil 3, A II 2 b.

[1911] Die Grenzen ergeben sich bei technischen Schutzmechanismen aus der technischen Machbarkeit und der Durchsetzbarkeit einer Schutzmaßnahme am Markt, bei vertraglichen Schutzmechanismen aus der Notwendigkeit, daß die vertraglichen Verpflichtungen wirksam sind und beispielsweise nicht gegen Vorschriften des BGB, des AGBG oder des GWB verstoßen.

[1912] Ebenso *Benkler*, 53 Vand. L. Rev. 2063, 2078 (2000).

[1913] *Thornburg*, 34 U.C. Davis L. Rev. 151, 176 (2000).

[1914] S. dazu im Überblick unten Teil 5.

[1915] Ebenso *Lessig*, S. 130, 135; *ders.*, 113 Harv. L. Rev. 501, 529 (1999); s. a. *Radin/Wagner*, 73 Chi.-Kent L. Rev. 1295, 1315 f. (1998); *Elkin-Koren*, 73 Chi.-Kent L. Rev. 1155, 1160 ff. (1998); *Vinje*, EIPR 1996, 431, 437 (1996); *Burk/Cohen*, S. 8; *McManis*, 87 Cal. L. Rev. 173, 176 (1999).

Urheberrecht die Funktion zukommen, technische und vertragliche Schutzmechanismen zu begrenzen (dazu unten 3).[1916]

2. Funktion des herkömmlichen Urheberrechts

Die einzelnen Schutzmechanismen eines DRM-Systems bieten keinen perfekten Schutz. Versagt der vertragliche oder der technische Schutz eines DRM-Systems, so könnte das Urheberrecht unterstützend eingreifen.

Schützt ein Inhalteanbieter seine Inhalte durch Nutzungsverträge,[1917] so kann er in DRM-Systemen durch eine Kombination mit unterstützenden Schutzmechanismen (Technik, rechtlicher Umgehungsschutz und Technologie-Lizenzverträge) ein Schutzniveau erreichen, das dem eines absolut wirkenden Rechts ähnelt („Verdinglichung" der Nutzungsverträge).[1918] Jedoch hilft der Schutz der „verdinglichten" Nutzungsverträge nicht weiter, wenn die Verträge unwirksam sind.[1919] Unter anderem können zivilrechtliche Unwirksamkeitsgründe (Anfechtung, beschränkte Geschäftsfähigkeit, mangelnde Vollmachten und ähnliches) vorliegen, auch kann ein Verstoß gegen das AGB-Gesetz vorliegen. In all diesen Fällen versagt der vertragliche Schutz.[1920] Die oben aufgestellte These, daß „verdinglichte" Nutzungsverträge in ihrer Gesamtheit in DRM-Systemen ein Schutzniveau schaffen, das dem eines absoluten Rechts vergleichbar ist,[1921] muß daher modifiziert werden: Der „verdinglichte" vertragliche Schutz in DRM-Systemen versagt, wenn die einzelnen Nutzungsverträge

[1916] Damit behandelt der folgende rechtliche Teil Fragen, die weiter oben schon unter rechtsökonomischen Gesichtspunkten untersucht wurden; s. dazu oben Teil 3, B I 2, und B I 3.

[1917] Hier ist wieder ein DRM-Nutzungsvertrag im Sinne der Einräumung einer rein faktischen Nutzungsmöglichkeit gemeint. Dies muß nicht identisch mit einem Nutzungsvertrag im urheberrechtlichen Sinne sein, s. oben Teil 3, A II 1 b aa.

[1918] S. dazu oben Teil 3, A II 2 b bb.

[1919] S. dazu schon oben bei Fn. 1439. Dagegen kommt der Fall, daß der vertragliche Schutz versagt, da ein Nutzer den Inhalt in einem DRM-System ohne begleitenden Nutzungsvertrag erhält, aufgrund technischer und lizenzvertraglicher Schutzmaßnahmen idealiter nicht vor. S. dazu oben Teil 3, A II 1 b, und A II 2 b bb.

[1920] Dieses Problem potenziert sich, wenn zwischen dem Inhalteanbieter und dem Nutzer keine direkte, sondern nur eine indirekte vertragliche Beziehung in Form einer mehrgliedrigen Vertragskette besteht; s. dazu oben Fn. 1363. Räumt ein Urheber beispielsweise ein ausschließliches Nutzungsrecht an einem Inhalt einem Intermediär ein, der diesen Inhalt in einem DRM-System an Nutzer vertreibt, muß der vertragliche Schutz des Urhebers „mitlaufen"; *Merges*, 12 Berkeley Tech. L. J. 115, 119 (1997). Ist ein Vertrag mit einem Intermediär unwirksam oder der Intermediär unerreichbar, insolvent oder nicht kooperationswillig, so kann dies bedeuten, daß der Inhaltenanbieter seine durch die Vertragskette geschützten Interessen gegenüber dem Nutzer nicht durchsetzen kann. Dieser Nachteil wiegt umso schwerer, je länger die Vertragskette wird: Die Wahrscheinlichkeit, daß eines der Glieder in der Vertragskette rechtlich unwirksam oder faktisch wirkungslos ist, steigt mit der Länge der Vertragskette; *Merges*, a. a. O., S. 119 f.

[1921] S. dazu oben Teil 3, A II 2 b bb.

unwirksam sind. Insofern besteht ein wichtiger Unterschied zwischen diesem vertraglichen Schutz und einem echten absoluten Recht, das nicht von der Wirksamkeit einer Vielzahl obligatorischer Rechtsbeziehungen abhängig ist.[1922] Daher wird es in DRM-Systemen faktisch vorkommen, daß Nutzer digitale Inhalte nutzen können, ohne gleichzeitig an einen Nutzungsvertrag gebunden zu sein. Um diese Schutzlücke zu schließen, bietet sich ein wirklich absolut wirkendes Recht an, das seine Wirkung gegenüber jedermann entfaltet, ohne eine vertragliche Bindung vorauszusetzen: das Urheberrecht.[1923]

Ein ähnliches Problem kann bei technischen Schutzmaßnahmen auftreten. Kein technisches Schutzsystem ist perfekt.[1924] Gelingt es einem Angreifer, eine technische Schutzmaßnahme zu umgehen, so können Inhalte des DRM-Systems genutzt werden, ohne daß dafür das entsprechende Entgelt gezahlt wird. Zwar kann das Vorgehen des Angreifers gegen rechtliche Umgehungsvorschriften verstoßen. Der rechtliche Umgehungsschutz greift jedoch nicht in allen Fällen. So wird er oftmals nur den eigentlichen Angreifer, nicht aber Dritte erfassen, die den geknackten Inhalt später nutzen oder ihrerseits im Internet anbieten.[1925] Aus diesem Grund wird es in DRM-Systemen vorkommen, daß Nutzer digitale Inhalte nutzen können, ohne gleichzeitig durch technische Schutzmaßnahmen kontrolliert zu werden. Zwar können hier noch andere Schutzmechanismen wie der rechtliche Umgehungsschutz eingreifen. Dies wird aber nicht in allen Fällen weiterhelfen. Um diese Schutzlücke zu schließen, bietet sich wiederum ein absolut wirkendes Recht an, das seine Wirkung ausnahmslos gegenüber jedermann entfaltet: das Urheberrecht.[1926]

Inhalteanbieter verlassen sich in DRM-Systemen zunehmend auf Schutzmechanismen außerhalb des herkömmlichen Urheberrechts. Jeder dieser neuartigen Schutzmechanismen hat jedoch seine Schwächen. Es wird immer Fälle geben, in denen Nutzer unberechtigterweise Inhalte in DRM-Systemen nutzen, ohne daß dies durch einen der neuartigen Schutzmechanismen verhindert wird. Diese Schutzlücke wird durch das herkömmliche Urheberrecht mit seinen gegenüber jedermann wirkenden Ausschließlichkeitsrechten geschlossen. Das Urheberrecht[1927] greift da-

[1922] Vgl. a. *Merges*, 12 Berkeley Tech. L. J. 115, 119 (1997).

[1923] Die Verbindung zwischen dem Schutz durch Nutzungsverträge und dem Urheberrecht wurde in dieser Deutlichkeit zuerst von *Merges*, 12 Berkeley Tech. L. J. 115, 119 ff. (1997), hergestellt.

[1924] S. oben Teil 1, F.

[1925] Bei diesen Dritten können beispielsweise subjektive Tatbestandsvoraussetzungen fehlen.

[1926] Ebenso *Gimbel*, 50 Stan. L. Rev. 1671, 1683 (1998).

[1927] An dieser Stelle sei nochmals darauf hingewiesen, daß die Arbeit mit der Verwendung des Begriffs „Urheberrecht“ in diesem Zusammenhang aus Gründen der einfacheren Darstellung die Summe der Ausschließlichkeitsrechte meint, die beispielsweise in Deutschland im UrhG geregelt sind. Darunter können auch Ausschließlichkeitsrech-

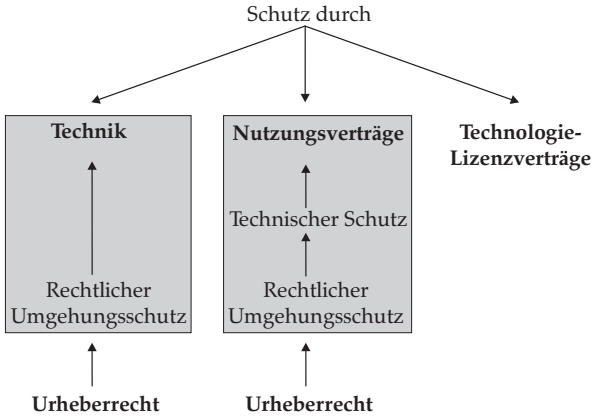


Abbildung 11: Unterschiedliche Schutzmechanismen in DRM-Systemen (2)

nach als eine Art „Sicherheitsnetz" ein, wenn andere Schutzmechanismen des DRM-Systems versagen (s. Abbildung 11).[1928]

Damit deutet sich ein Wandel des Urheberschutzes an. Inhalteanbieter in DRM-Systemen verlassen sich primär auf den Schutz durch technische Schutzmaßnahmen, Nutzungsverträge und Technologie-Lizenzverträge. Versagt eine dieser Schutzmaßnahmen, so können sie auf einen rechtlichen und technischen Schutz dieser Schutzmaßnahmen zurückgreifen. Erst wenn auch diese Schutzebene versagt, kommt das Urheberrecht im klassischen Sinne ins Spiel. In DRM-Systemen verliert das Urheberrecht seine Funktion als zentrales Schutz- und Anreizinstrument für geistige Schöpfungen.[1929]

---

te von Leistungsschutzberechtigten fallen. Die Differenzierung zwischen Urhebern und Leistungsschutzberechtigten tut für den vorliegenden Untersuchungsansatz nichts zur Sache; s. dazu schon die Anmerkungen in der Einführung zu dieser Untersuchung.

[1928] S. zu dieser Abbildung schon Abbildung 7, S. 263.

[1929] Wie viele Thesen stellt diese naturgemäß eine Vereinfachung des komplexen Ineinandergreifens unterschiedlicher Schutzmechanismen dar. Beispielsweise schützen DRM-Systeme in der Tendenz stärker die Verwertungsinteressen der Inhalteanbieter als deren Urheberpersönlichkeitsinteressen (wenn auch technische Maßnahmen existieren, um Urheberpersönlichkeitsrechte zu wahren, s. nur oben bei Fn. 1340 und 1396). Daher könnte das Urheberrecht in DRM-Systemen hinsichtlich des Schutzes des Urheberpersönlichkeitsrechts wichtiger sein als hinsichtlich des Schutzes von Verwertungsinteressen. Weiterhin darf die These nur als Aussage hinsichtlich der Stellung des Urheberrechts innerhalb von DRM-Systemen verstanden werden, womit sich die vorliegende Arbeit beschäftigt. Selbstverständlich wird das Urheberrecht außerhalb von DRM-Systemen weiterhin eine zentrale Rolle spielen; man denke nur an den gesamten Bereich der öffentlichen Aufführungen sowie analoger Vervielfältigungen. Sobald es aber um digitale Inhalte geht, können DRM-Systeme eingesetzt werden. In diesem gesteckten Rahmen sind die Einsatzmöglichkeiten von DRM-Systemen äußerst umfangreich. Diesem Bereich gilt die vorliegende Untersuchung.

3. Beschränkung des DRM-Schutzes

a) Notwendigkeit einer Beschränkung

> *We should not be handing out monopolies like confetti while muttering „this won't hurt".*[1930]

Wie die Abbildung 11 zeigt, kann der Inhalteanbieter in DRM-Systemen insgesamt auf sieben unterschiedliche Schutzmechanismen zurückgreifen: Schutz durch Technik, durch Nutzungsverträge, durch technischen Schutz der Nutzungsverträge, durch rechtlichen Umgehungsschutz der beiden technischen Schutzmechanismen, durch Technologie-Lizenzverträge und durch das Urheberrecht. Das Schlagwort von der „hyperprotection" scheint angebracht.[1931] Man mag sich fragen, ob es all dieser Mechanismen zum Schutz von Inhalteanbietern überhaupt bedarf. Diese Frage wird in der rechtspolitischen Diskussion allerdings selten gestellt.[1932]

Neben dieser quantitativen Verstärkung erreicht der Schutz in DRM-Systemen auch eine neue Qualität. DRM-Systeme gleichen einem „self-executing law", dessen Umfang von denjenigen bestimmt wird, die durch das System geschützt werden.[1933] DRM-Systeme ermöglichen dem Inhalteanbieter, gleichsam sein eigenes Urheberrechtsgesetz zusammenzuschustern und dessen Reichweite selbst zu bestimmen.[1934] Dies kann dazu führen, daß Inhalteanbieter ihre Interessen in DRM-Systemen maximal schützen, ohne auf gegenläufige Interessen Dritter und der Allgemeinheit Rücksicht zu nehmen.[1935] Es besteht die Gefahr, daß DRM-Systeme –

[1930] *Laddie*, EIPR 1996, 253, 260.

[1931] *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 222, Fn. 264 m. w. N.

[1932] S. aber *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 221 f.: „Is it really necessary for rights-holders to be (cumulatively) protected by copyright, database protection, contract law, technical protection and an additional layer of [technological measure] procetion? *Wand* has observed, rather cynically, that ‚three times stitched holds better'. Perhaps, one might add: five times is overdoing it"; *Koelman*, EIPR 2000, 272, 279; *Vinje*, EIPR 1999, 192, 200 f.; *ders.*, EIPR 1996, 431, 438; *ders.*, EIPR 2000, 551, 556. Auch existieren beispielsweise keine empirischen Daten zu der Frage, ob Inhalteanbieter den rechtlichen Umgehungsschutz technischer Schutzmaßnahmen überhaupt benötigen; Vgl. a. *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 221; *Hugenholtz*, 6 Maastricht Journal of European and Comparative Law 308, 314 f. (1999); *ders.*, 26 Brooklyn J. Int'l L. 77, 86 (2000); *Bell*, 76 N.C. L. Rev. 557, 561 (1998). Schließlich weist *Koelman*, The Protection of Technological Measures, S. 4, darauf hin, daß sich durch die Schaffung neuer Schutzmechanismen bekannte Probleme nur verschieben könnten: Wenn im DRM-Umfeld nicht mehr Vorschriften des Urheberrechts, sondern des rechtlichen Umgehungsschutzes massenhaft verletzt werden, so wäre für die Effektivität der Rechtsdurchsetzung nichts gewonnen.

[1933] S. dazu oben bei Fn. 1459; s. a. *Gimbel*, 50 Stan. L. Rev. 1671, 1685 (1998); *Thornburg*, 34 U.C. Davis L. Rev. 151, 176 (2000); *Lessig*, S. 129 f.

[1934] S. a. *Burk/Cohen*, S. 8: „Rights-holders can effectively write their own intellectual property statute in computer code"; *Möschel/Bechtold* in: Pfitzmann/Roßnagel (Hrsg.), S. 4 f.

[1935] *Reichman/Franklin*, 147 U. Penn. L. Rev. 875, 898 (1999); *Vinje*, EIPR 1996, 431, 437 (1996).

insbesondere technische Schutzmaßnahmen und Nutzungsverträge – urheberrechtliche Schrankenbestimmungen unterlaufen.[1936]

Dies sind keine theoretischen Überlegungen ohne praktische Relevanz. Schon bei heutigen DRM-Systemen zeigt sich das Spannungsverhältnis zwischen dem Schutz durch DRM-Systeme und urheberrechtlichen Schrankenbestimmungen. Bei einer eBook-Version eines Texts von *Jules Verne*, die käuflich erworben werden kann, ist dem Nutzer beispielsweise nur erlaubt, alle zehn Tage jeweils zehn Seiten des Texts auszudrucken. Weiterhin ist ihm verboten, den Text an Dritte weiterzugeben. Beide Nutzungsbedingungen werden durch technische Schutzmaßnahmen gesichert; ein vollständiger Ausdruck oder die Weitergabe des eBooks an Dritte wird technisch verhindert.[1937] *Jules Verne* ist 1905 gestorben, das Urheberrecht auf seine Texte längst abgelaufen (s. § 64 UrhG). In anderen Fällen wird das Ausdrucken oder Kopieren einzelner Textstellen sogar gänzlich verboten.[1938] Ein weiteres Beispiel zeigt Abbildung 12 (S. 376), in der die Nutzungsbedingungen für eine DRM-geschützte eBook-Fassung des Kinderbuch-Klassikers „Alice im Wunderland" von *Lewis Carroll* abgedruckt sind. Die eBook-Fassung ist eine exakte

[1936] Ebenso *Guibault* in: Hugenholtz (Hrsg.), S. 125, 160; *Vinje*, EIPR 1996, 431, 436 (1996); *Denicola*, 47 J. Copyright Soc'y U.S.A. 193, 196 (2000); *Lessig*, 113 Harv. L. Rev. 501, 529 (1999); *Burk/Cohen*, S. 6, 8; *Koelman/Herberger* in: Hugenholtz (Hrsg.),. 165, 191; *Vinje*, EIPR 2000, 551, 555; *Hoeren*, MMR 2000, 3, 4; *Kröger*, CR 2001, 316 321; s. a. *Dreier*, CR 2000, 45, 46 f. Diese Erkenntnis ist nicht neu. Schon der 1986 erschienene Bericht des *U.S. Congress, Office of Technology Assessment*, Intellectual Property Rights in an Age of Electronics and Information, meint auf S. 119: „However, from the point of view of public policy, technological protection may be a poor way to protect intellectual property rights because it ignores part of the constitutional compromise between the public welfare and the profit-making of intellectual creators." Einen Überblick über die Problematik der Nutzungsverträge, die urheberrechtliche Schrankenbestimmungen unterlaufen, gibt *Guibault*, a. a. O., S. 125 ff.; s. weiterhin *Elkin-Koren* und *Dreier* in: Dreyfuss/Zimmerman/First (Hrsg.), S. 191 ff., 295 ff. Extreme Beispiele einer Welt, bei der Information nur noch auf der Basis von Verträgen und Technik verbreitet wird, geben *Nimmer/Brown/Frischling*, 87 Cal. L. Rev. 17, 20 f., 54 ff. (1999). Diese Beispiele werden von *Wolfson*, 87 Cal. Rev. 79, 104 ff. (1999) zu Recht als übertrieben kritisiert. DRM-Systeme können im Übrigen das Prozeßrisiko verlagern: Beging früher ein Nutzer eine unberechtigte Nutzungshandlung, so mußte der Rechteinhaber den Nutzer auf Unterlassung und/oder Schadensersatz verklagen. In DRM-Systemen wird die unberechtigte Nutzungshandlung von vornherein verhindert. Will ein Nutzer von einer urheberrechtlichen Schrankenbestimmung Gebrauch machen, so hindert ihn das DRM-System unter Umständen daran. Dann bleibt dem Nutzer nichts anderes übrig, als den Rechteinhaber zu verklagen; s. dazu *Thornburg*, 34 U.C. Davis L. Rev. 151, 177, 195 (2000).

[1937] Es handelt sich um englische Fassung des Buches mit dem Titel „A Journey to the Center of the Earth", die der Verfasser im April 2001 bei Amazon.com erworben hat.

[1938] So in einer deutschen eBook-Fassung von *Robert Louis Stevenson's* „Der befremdliche Fall von Dr. Jekyll & Mr. Hyde", die der Verfasser im Mai 2001 bei <http://www.dibi.de> erworben hat. *Stevenson* ist 1894 gestorben.

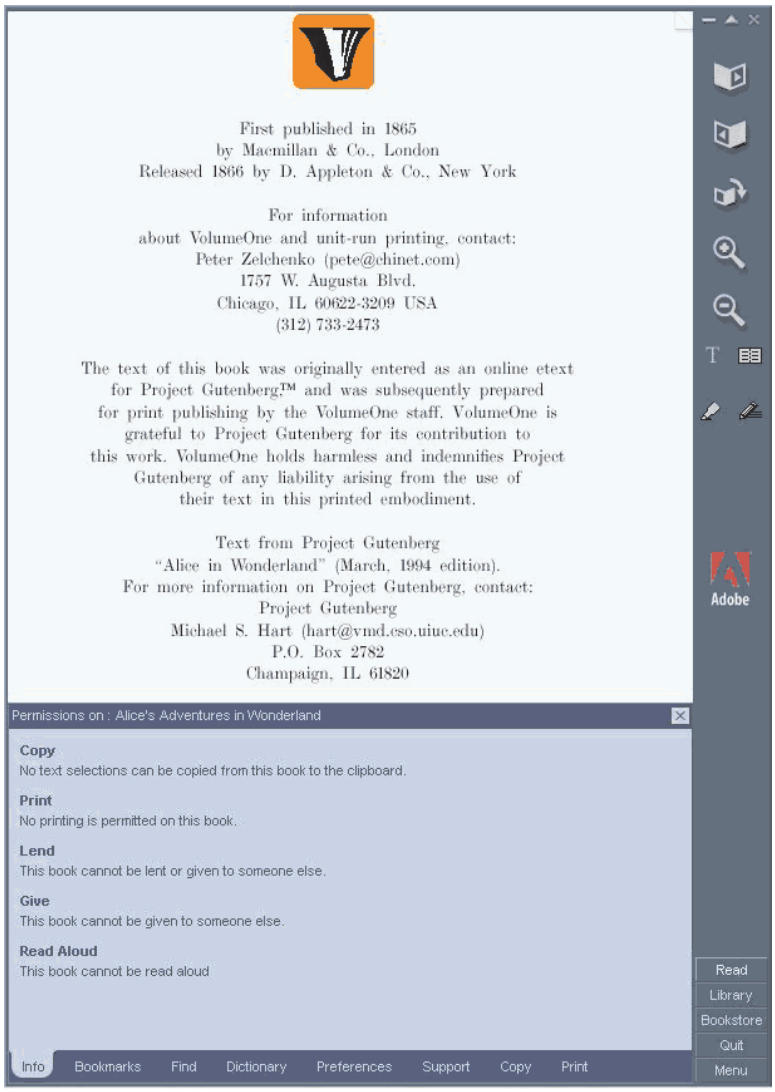


Abbildung 12: Urheberrechtliche Schrankenbestimmungen und DRM-Systeme

elektronische Reproduktion der britischen Erstausgabe des Buchs aus dem Jahr 1865. Nach den Nutzungsbedingungen dürfen aus der eBook-Fassung keine Ausschnitte kopiert werden. Auch kann der Text nicht ausgedruckt, an einen Dritten ausgeliehen oder weitergegeben wer-

den.[1939] Selbst wenn ein Nutzer zu einer dieser Nutzungen nach einer urheberrechtlichen Schrankenbestimmung berechtigt sein sollte, verhindert das DRM-System des eBook-Software-Readers diese Nutzung auf technischem Weg. *Carroll* ist 1898 verstorben.

Die angebebenen Beispiele stammen zwar sämtlich aus dem Bereich der eBooks und dem U.S.-amerikanischen Markt. Dies darf aber nicht darüber hinwegtäuschen, daß das Spannungsverhältnis zu urheberrechtlichen Schrankenbestimmungen ein allgemeines Phänomen aller DRM-Systeme ist. So können auch die in DVD-Geräten und Speichermedien eingebauten Schutzmechanismen das Kopieren geschützter Inhalte in digitaler und analoger Form verhindern oder zumindest erschweren. Ähnliches gilt für Conditional-Access-Systeme im Pay-TV-Bereich.

Auch DRM-Technologie-Lizenzverträge können mittelbar Auswirkungen darauf haben, ob die Nutzer eines DRM-Systems von urheberrechtlichen Schrankenbestimmungen Gebrauch machen können.[1940] So werden die Hersteller von Computern und Unterhaltungselektronik in DRM-Technologie-Lizenzverträgen verpflichtet, bestimmte Standard-Nutzungsbedingungen einzuhalten. Danach darf ein Endgerät beispielsweise digitale Inhalte nur einmal auf ein anderes Gerät kopieren. Die Gerätehersteller werden weiterhin verpflichtet, daß ihre Geräte die Metadaten, die von den Inhalteanbietern festgelegt wurden und die ihrerseits urheberrechtliche Schrankenbestimmungen aushebeln können, beachten. Mitunter verlangen Technologie-Lizenzverträge auch, daß beim Kopieren digitaler Inhalte deren Qualität deutlich verschlechtert wird. Wie alle Schutzmechanismen eines DRM-Systems müssen Technologie-Lizenzverträge nicht notwendigerweise dazu führen, daß die Nutzer bestimmte Nutzungen nicht mehr vornehmen können, zu denen sie nach urheberrechtlichen Schrankenbestimmungen berechtigt sind. Wie alle Schutzmechanismen haben Technologie-Lizenzverträge aber dieses Potential.[1941]

[1939] Die weitere Beschränkung „This book cannot be read aloud" bezieht sich auf eine Funktion des Adobe eBook Readers, der Texte grundsätzlich durch eine synthetisierte Sprachausgabe vorlesen kann. Im Internet und der Presse war der Fall im Dezember 2000 bekannt geworden, da Adobe vorgeworfen wurde, durch diese Bestimmung vertraglich verhindern zu wollen, daß Eltern das eBook ihren Kindern selbst laut vorlesen. Dies trifft natürlich nicht zu. In der Folgezeit lockerte Adobe die Nutzungsbedingungen des eBooks. S. zum ganzen <http://slashdot.org/yro/00/12/14/1515228.shtml>; <http://www.thestandard.com/article/0,1902,22914,00.html>; *Junger*, S. 17 ff. Abbildung 12 ist im WWW an mehreren Stellen erhältlich, beispielsweise unter <http://www.pigdogs.org/art/adobe.html>.

[1940] Zu solchen Technologie-Lizenzverträgen im allgemeinen s. oben Teil 2, C.

[1941] Daher soll hier auch nicht gesagt sein, daß in allen der erwähnten Technologie-Lizenzklauseln urheberrechtliche Schrankenbestimmungen eingreifen würden. Es geht im vorliegenden Rahmen nur darum, das Potential solcher Schutzmechanismen aufzuzeigen.

DRM-Systeme können Inhalte schützen, deren urheberrechtliche Schutzfrist schon abgelaufen ist; sie ermöglichen ein „unendliches Urheberrecht".[1942] DRM-Systeme können auch Inhalte schützen, die gar keinem urheberrechtlichen Schutz unterliegen.[1943] Sie können ferner eingesetzt werden, um den Nutzer an der Ausübung urheberrechtlicher Schrankenbestimmungen – beispielsweise dem Zitierrecht nach § 51 UrhG oder dem Recht auf private Vervielfältigungen nach § 53 UrhG – zu hindern. Zwar müssen DRM-Systeme nicht notwendigerweise in dieser Art und Weise konfiguriert sein. Inwieweit Interessen der Nutzer und der Allgemeinheit in DRM-Systemen berücksichtigt werden, hängt von der genauen Ausgestaltung der Nutzungs- und Technologielizenzverträge sowie von den Metadaten und technischen Schutzmaßnahmen ab. Jedoch haben DRM-Systeme das Potential, das Kräfteverhältnis zwischen Rechteinhabern und Nutzern zugunsten der ersten Gruppe zu verschieben. Auch aus ökonomischer Sicht spricht einiges dafür, daß Inhalteanbieter in DRM-Systemen ihren eigenen Nutzen maximieren und dabei auf urheberrechtliche Schrankenbestimmungen keine Rücksicht nehmen.

Diese Entwicklung ist aus rechtlicher Sicht problematisch, kommen urheberrechtlichen Schrankenbestimmungen doch wichtige Aufgaben zu. Nach allen Urheberrechtsgesetzen muß sich der Urheber gewisse Einschränkungen seines ausschließlichen Herrschaftsrechts über das von ihm geschaffene Werk im Interesse Dritter und der Allgemeinheit gefallen lassen.[1944] Zu diesem Zweck sieht das deutsche UrhG verschiedene Einschränkungen des Urheberrechts vor, die von einer ersatzlosen Aufhebung des ausschließlichen Verwertungsrechts über eine gesetzliche Lizenz oder eine Zwangslizenz bis zu einer Verwertungsgesellschaftspflichtigkeit eines Zahlungsanspruchs gehen können.[1945]

[1942] Vgl. *Mahajan*, 67 Fordham L. Rev. 3297, 3330 (1999); *Cohen*, 97 Mich. L. Rev. 462, 472 (1998); *Vinje*, EIPR 1996, 431, 436 (1996).

[1943] Dieses Problem stellt sich weniger in Europa als in den USA, wo es keinen sui-generis-Schutz von reinen Datensammlungen gibt, wie er inzwischen in §§ 87 a ff. UrhG enthalten ist.

[1944] *Melichar* in: Schricker (Hrsg.), UrhG-Kommentar, vor §§ 45 ff. Rdnr. 1. Dies wird in Deutschland auch mit Hinweis auf die verfassungsrechtliche Lage begründet. Nach der Rechtsprechung des Bundesverfassungsgerichts stellt das geschaffene Werk und die darin verkörperte Leistung in vermögensrechtlicher Hinsicht Eigentum des Urhebers im Sinne des Art. 14 Abs. 1 S. 1 GG dar, BVerfGE 31, 229, 239 – Kirchen- und Schulgebrauch; BVerfGE 49, 382, 392 – Kirchenmusik; s. zu diesem Themenkomplex ausführlich *Leinemann*, S. 55 ff. Damit unterliegt das das Urheberrecht wie das Sacheigentum der Sozialbindung, BVerfGE 31, 229, 241, 243 – Kirchen- und Schulgebrauch; *Melichar*, a. a. O., vor §§ 45 ff. Rdnr. 1; *Nordemann* in: Fromm/Nordemann, vor § 45 Rdnr. 1; *Leinemann*, S. 61 ff. Selbst die herrschende deutsche Lehre, die urheberrechtliche Schrankenbestimmungen traditionell eng auslegt, anerkennt die Notwendigkeit dieser Bestimmungen, s. nur *Melichar*, a. a. O., vor §§ 45 ff. Rdnr. 13.

[1945] S. dazu *Melichar* in: Schricker (Hrsg.), UrhG-Kommentar, vor §§ 45 ff. Rdnr. 6; *Leinemann*, S. 92 f.

Urheberrechtliche Schrankenbestimmungen dienen unter anderem der Informationfreiheit,[1946] dem Datenschutz,[1947] der Aufrechterhaltung des freien Wettbewerbs[1948] und der Ausbildungs- und Kulturförderung.[1949] Urheberrechtliche Schrankenbestimmungen dienen der Informationsfreiheit,[1950] wenn die Verwertungsrechte bei der Vervielfältigung von Zeitungsartikeln in bestimmten Fällen auf eine gesetzliche Lizenz begrenzt werden, § 49 UrhG. Gleiches gilt, wenn öffentlich gehaltene Reden trotz des urheberrechtlichen Schutzes ohne Zustimmung des Urhebers öffentlich wiedergegeben werden dürfen, § 48 UrhG. Sie unterstützen die freie geistige Auseinandersetzung,[1951] wenn das Zitieren aus fremden Werken ohne Zustimmung des Urhebers erlaubt wird, § 51 UrhG. Sie dienen den Interessen eines freien Wettbewerbs,[1952] wenn sie die Dekompilierung von Computerprogrammen ermöglichen, die zur Erstellung von Substitutionsprodukten notwendig ist, § 69 e UrhG. Die Beschränkungen des Urheberrechts unterstützen die Schaffung neuer Werke und fördern die geistige Auseinandersetzung,[1953] indem die „freie Benutzung" eines bestehenden Werks von dessen Urheber nicht verhindert werden kann, § 24 UrhG.[1954] Sie fördern die Schaffung neuer Werke und dienen der Informationsfreiheit, wenn die Schutzdauer des Urheberrechts auf 70 Jahre *post mortem auctoris* begrenzt wird, § 64 UrhG.[1955]

[1946] S. dazu *Guibault* in: Hugenholtz (Hrsg.), S. 125, 131.

[1947] *Guibault* in: Hugenholtz (Hrsg.), S. 125, 131 ff.

[1948] *Guibault* in: Hugenholtz (Hrsg.), S. 125, 135 ff.

[1949] S. dazu *Guibault* in: Hugenholtz (Hrsg.), S. 125, 137 ff. S. zum ganzen aus rechtsvergleichender Sicht *Davies*; vgl. weiterhin *Pahud*, UFITA 2000, 99, 116 ff.; *Vinje*, EIPR 1999, 192, 193; *Burk/Cohen*, S. 2 ff.

[1950] S. dazu *Melichar* in: Schricker (Hrsg.), UrhG-Kommentar, § 48 Rdnr. 1 und § 49 Rdnr. 1; *Leinemann*, S. 97 ff.; *Fechner*, S. 348 ff. Zu diesem Gesichtspunkt im europäischen Urheberrecht s. *Guibault* in: Hugenholtz (Hrsg.), S. 125, 128 ff.

[1951] S. dazu *Schack*, Rdnr. 482; *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, § 51 Rdnr. 6; *Leinemann*, S. 100.

[1952] S. dazu *Loewenheim* in: Schricker (Hrsg.), UrhG-Kommentar, § 69 e Rdnr. 1; *Marly*, Softwareüberlassungsverträge, Rdnr. 1048; *Guibault* in: Hugenholtz (Hrsg.), S. 125, 135 f., 150; *Vinje*, EIPR 1999, 192, 193 f.

[1953] S. dazu *Schack*, Rdnr. 482.

[1954] S. dazu *Leinemann*, S. 99 f.; *Loewenheim* in: Schricker (Hrsg.), UrhG-Kommentar, § 24 Rdnr. 2.

[1955] S. dazu *Leinemann*, S. 117 f.; *Schack*, Rdnr. 466. Daneben dienen Schrankenbestimmungen auch anderen Interessen, beispielsweise im Falle der §§ 45, 87 c Abs. 2 UrhG dem Interesse der Rechtspflege und der öffentlichen Sicherheit. Eine Auflistung der unterschiedlichen Schrankenbestimmungen und der jeweiligen Interessen der Allgemeinheit, die durch sie geschützt werden, findet sich bei *Leinemann*, S. 94 ff. Das deutsche UrhG läßt in der Aufzählung der teilweise äußerst speziellen Schrankenbestimmungen ab § 45 UrhG eine wirkliche Systematik vermissen. *Schack*, Rdnr. 480, meint zu Recht, daß „manchmal als Geltungsgrund der Schranken eher die politische Duchsetzungskraft einzelner Verwerterinteressen […] als leitende Prinzipien des Urheberrechts" zu vermuten seien; s. a. *Vinje*, EIPR 1999, 192, 193.

Diese Erwägungen, aufgrund derer das Urheberrecht beschränkt ist, bleiben auch in DRM-Systemen relevant.[1956] DRM-Systeme laufen Gefahr, urheberrechtlichenSchrankenbestimmungen zu unterlaufen. Nimmt man die Bedeutung der Schrankenbestimmungen ernst, so kommt man nicht umhin, daß sie bei Schutzmechanismen außerhalb des Urheberrechts – Technik, Nutzungsverträge, Technologie-Lizenzverträge, rechtlicher Umgehungsschutz – ein wie auch immer geartetes Äquivalent haben müssen.[1957] Zwar geht es beim Spannungsverhältnis zwischen DRM-Sy-

[1956] So auch *Burk/Cohen*, S. 10: „Where [technological protection measures] attempt to impose restrictions on informational content that would be prohibited in a contractual agreement, the restrictions should be viewed as equally repugnant to public policy and equally void." Jedoch könnte sich die Bedeutung einzelner Schrankenbestimmungen in DRM-Systemen wandeln. Ein wichtiger Grund für die Einführung des heutigen § 53 UrhG war, daß ein Verbot der Vervielfältigung und eine Vergütungspflicht der Nutzer im privaten Bereich praktisch kaum durchgesetzt werden konnte, s. dazu oben bei Fn. 1660. Durch sinkende Transaktionskosten könnte diese Kontrolle in DRM-Systemen möglich werden, s. dazu oben Teil 3, A III 4. Damit könnte *diese* Begründung § 53 UrhG entfallen; ebenso *Leinemann*, S. 150; *Möschel/Bechtold*, MMR 1998, 571, 575; *Wand*, S. 58. Dagegen läßt sich zwar schon aus ökonomischer Sicht einiges anführen, s. oben Teil 3, B I 1 f, und B I 2 a. Aus juristischer Sicht ist jedoch zu beachten, daß die Schrankenbestimmunge des § 53 UrhG noch anderen Zwecken dient. Durch § 53 UrhG wird verhindert, daß der Urheber Informationen über einzelne Kopiervorgänge aus der privaten Sphäre des Nutzers erfährt – es geht um Datenschutz im weitesten Sinne. In DRM-Systemen könnte sich die Bedeutung des § 53 UrhG damit von einer Vorschrift, durch die an erster Stelle prohibitiv hohe Transaktionskosten vermieden werden sollen, zu einer Vorschrift wandeln, durch die an erster Stelle die Erhebung personenbezogener Daten verhindert werden soll. Grundsätzlich können datenschutzrechtliche Bedenken den Umfang urheberrechtlicher Verwertungsrechte beschränken; s. dazu *Guibault* in: Hugenholtz (Hrsg.), S. 125, 142; *Bygrave/Koelman* in: Hugenholtz (Hrsg.), S. 59, 98 ff. In der Gesetzesbegürdung zum UrhG wird ein ähnlicher Aspekt angesprochen, wenn auf den in Art. 13 GG ausgesprochenen Grundsatz der Unverletzlichkeit der Wohnung Bezug genommen wird, s. *Bundesregierung*, BT-Drs. IV/270 vom 23. 3. 1962, S. 71; s. a. BGH GRUR 1965, 104, 107 f. – Personalausweise. Zu datenschutzrechtlichen Problemen von DRM-Systemen s. a. die Nachweise in Fn. 39.

[1957] Ebenso *Vinje*, EIPR 1999, 192, 196: „Even if legislators succeed in retaining an appropriate balance between rights, limits and exceptions, to what avail will this be if rightholders can effectively replace this copyright regime with a private one of their own making that takes no account of copyright limits and exceptions?"; *Gimbel*, 50 Stan. L. Rev. 1671, 1680 ff., 1686 (1998); *Lessig*, S. 127; *Vinje*, EIPR 1996, 431, 434, 436; *Burk/Cohen*, S. 10; *Cohen*, 12 Berkeley Tech. L. J. 161, 183 (1997); s. weiterhin *Goldstein*, 45 J. Copyright Soc'y U.S.A. 151, 157 (1997). Daneben können auch andere Rechtsgebiete eine Beschränkung des DRM-Schutzes gebieten. So können kartellrechtliche Bestimmungen die Ausübung von Verwertungsrechten beschränken; dazu grundlegend die „Magill"-Entscheidung des EuGH, Urteil vom 6. 4. 1995 in den verbundenen Rechtssachen C-241/91 P und C-242/91 P, Slg. 1995, I-743 – RTE und ITP/Kommission; s. dazu *R. Bechtold*, EuZW 1995, 345 ff.; *Götting*, JZ 1996, 307 ff. In den USA ist derzeit das Verhältnis zwischen dem rechtlichen Umgehungsschutz und dem Schutz der freien Meinungsäußerung, der sich aus dem ersten Zusatzartikel zur U.S.-Verfassung ergibt, äußerst umstritten; s. dazu nur Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d. 294, 325 ff. (S.D.N.Y. 2000); *Benkler*, 74 N.Y.U. L. Rev.

stemen und dem Urheberrecht nicht nur um urheberrechtliche Schrankenbestimmungen: Erlaubt ein DRM-Nutzungsvertrag einem Nutzer, den digitalen Inhalt insgesamt nur fünf Mal zu bestimmten Uhrzeiten auf einem bestimmten Endgerät zu nutzen, so können solche vertraglichen Nutzungsbeschränkungen zwar nicht wegen eines Verstoßes gegen urheberrechtliche Schrankenbestimmungen, aber wegen eines Verstoßes gegen sonstige urheberrechtliche Grundsätze unwirksam sein.[1958] Der wichtigste Bereich, in dem sich ein Spannungsverhältnis zwischen DRM-Systemen und dem Urheberrecht ergibt, sind jedoch urheberrechtliche Schrankenbestimmungen.

Gegen eine solche gesetzliche Beschränkung technischer und vertraglicher Schutzmechanismen wird mitunter vorgebracht, daß DRM-Systeme gar nicht zu einer Aushöhlung urheberrechtlicher Schrankenbestimmungen führten. Werde ein Videofilm beispielsweise auf einer DVD gespeichert und mit den für DVDs üblichen technischen Schutzmaßnahmen versehen, so könne ein Nutzer zwar den Videoinhalt weder kopieren noch daraus Ausschnitte entnehmen. Dennoch bestünden für ihn Möglichkeiten, um von urheberrechtlichen Schrankenbestimmungen Gebrauch zu machen: So könne er den Videofilm von der DVD abspielen, auf einem Fernseher anzeigen lassen und mit einer Videokamera abfilmen. Auch sei der Videofilm regelmäßig im Handel neben der DVD-Fassung auf einer nicht kopiergeschützten analogen Videokassette erhältlich, bei der die entsprechenden Nutzungen problemlos vorgenommen werden könnten. DRM-Systeme würden daher urheberrechtliche Schrankenbestimmungen nicht aushöhlen. Sie führten nur dazu, daß der Nutzer die Schrankenbestimmungen nicht bei einer perfekten digitalen und DRM-geschützten Version des Inhalts ausnützen könne. Allenfalls würden DRM-Systeme die Ausübung von Schrankenbestimmungen bei der Version des Inhalts mit der besten verfügbaren Qualität verhindern. Gerade in den USA wird dieses Argument in letzter Zeit verstärkt vorgebracht. Eine Beschränkung des Schutzes von DRM-Systemen sei nicht zulässig. Das U.S.-amerikanische Recht sehe kein „fair use of the best quality available" vor.[1959] Auch in Deutschland finden sich inzwischen Äußerungen, die in diese Richtung gehen.[1960] Insgesamt steht die Diskus-

354, 420 ff. (1999). Zu diesem Aspekt aus europäischer Sicht s. *Hugenholtz* in: Dreyfuss/Zimmerman/First (Hrsg.), S. 343 ff.; *Wand*, S. 136, 185 f.

[1958] S. dazu unten Teil 4, B.

[1959] S. dazu *Library of Congress*, 65 Fed. Reg. 64556, 64568 (October 27, 2000) und die mündliche Verhandlung in zweiter Instanz in Sachen Universal City Studios, Inc., v. Reimerdes vom 1. 5. 2001, erhältlich unter <http://www.eff.org/IP/Video/MPAA_DVD_cases/20010501_ny_hearing_transcript.html> (Befragung von *Kathleen Sullivan*); s. weiterhin die Diskussionsbeiträge in *Benkler* (Hrsg.), 11 Fordham Intell. Prop. Media & Ent. L. J. 317, 331, 348, 356 (2001), und *Stefik*, The Internet Edge, S. 96.

[1960] *Wand*, S. 59, 245.

sion dazu erst ganz am Anfang. Gerichtsentscheidungen zu der Frage existieren nicht.

Gegen diese Argumentation ist einzuwenden, daß Inhalte zunehmend nur noch in DRM-Systemen veröffentlicht werden könnten. Ein Ausweichen auf alternative analoge Publikationsmedien wäre dann nicht mehr möglich. In ferner Zukunft könnte auch das Abfilmen und Wiederaufnehmen DRM-geschützter Inhalte nicht mehr möglich sein;[1961] praktikabel ist es schon heute nicht. Außerdem erscheint problematisch, einen Nutzer, der von urheberrechtlichen Schrankenbestimmungen Gebrauch machen will, auf technisch inferiore Versionen des Inhalts zu verweisen. Warum soll der Inhalteanbieter zum Schutz seiner berechtigten Interessen von den neuen Möglichkeiten eines DRM-Systems Gebrauch machen können, während der Nutzer zur Ausübung seiner berechtigten Interessen auf eine in der Qualität schlechtere und mitunter veraltete Versionen des Inhalts zurückgreifen muß? Eine solche Argumentation ist abzulehnen. Sie wäre der Systematik der Schrankenbestimmungen des deutschen UrhG auch fremd.

b) Vom Urheber- zum Nutzerschutz

Es zeigt sich, daß der „privatisierte" Rechtsschutz von DRM-Systemen den Inhalteanbietern weitgehende Schutzmöglichkeiten verleiht, bei dem Interessen Dritter und der Allgemeinheit nicht ausreichend berücksichtigt werden. Sowohl unter ökonomischen[1962] als auch rechtlichen[1963] Gesichtpunkten erscheint eine gesetzliche Beschränkung des Schutzes von DRM-Systemen notwendig. Dabei geht es um eine Beschränkung aller Schutzmechanismen in einem DRM-System – Technik, Nutzungsverträge, Technologie-Lizenzverträge, rechtlicher Umgehungsschutz und Urheberrecht.[1964] Abstrakt betrachtet geht es im vorliegenden Fall darum, daß die Privatautonomie der Inhalteanbieter aus Gründen des öffentlichen Interesses eingeschränkt wird. Das vollständige Schutzgefüge in DRM-Systemen stellt sich damit wie in Abbildung 13 (S. 384) dar.

Während DRM-Systeme hinsichtlich des Schutzes der Inhalteanbieter das Urheberrecht ersetzen könnten,[1965] bleibt hinsichtlich des Schutzes der Nutzer und der Allgemeinheit ein gesetzgeberisches Eingreifen notwendig. Im Bereich der DRM-Systeme wird sich das Urheberrecht damit mehr und mehr von einem *Urheber-* zu einem *Nutzerschutz* wandeln.[1966]

[1961] Dies wäre dann der Fall, wenn digitale Wasserzeichen so robust wären, daß sie auch eine Digital-Analog-Wandlung sicher überstehen; s. dazu oben Teil 1, C II 2 b bb 4.

[1962] S. dazu oben Teil 3, B I 2 b.

[1963] S. dazu oben Teil 3, B II 3 a.

[1964] Zum Zusammenspiel dieser Schutzmechanismen im Überblick s. oben Abbildung 11, S. 373.

[1965] S. dazu aus juristischer Sicht oben Teil 3, A II 3, aus rechtsökonomischer Sicht oben Teil 3, A III 2 b.

[1966] Ebenso *Elkin-Koren*, 12 Berkeley Tech. L. J. 93, 105 f., 113 (1997); *Lemley*, 87 Cal. L. Rev. 111, 114 f., 171 f. (1999) m. w. N.; *Koelman/Herberger* in: Hugenholtz

Zwar verkürzt diese plakative These notwendigerweise die Komplexität der gesamten Problematik.[1967] In der Tendenz trifft sie freilich zu.[1968]

(Hrsg.), S. 165, 200 f. *Lessig*, S. 127, meint: „The problem will center not on copy-right but on copy-*duty* – the duty of owners of protected property to make that property accessible" (Hervorhebung im Original).

[1967] So geht es bei urheberrechtlichen Schrankenbestimmungen nicht immer unmittelbar um den Schutz des Nutzers. Schrankenbestimmungen schützen auch den Wettbewerb oder allgemeine öffentliche Interessen, s. dazu oben Teil 3, B II 3 a. Weiterhin ist fraglich, ob zwischen dem hier propagierten „Nutzerschutz" und dem herkömmlichen „Verbraucherschutz" unterschieden werden muß. Schließlich könnte die These die Frage aufwerfen, ob urheberrechtliche Schrankenbestimmungen als „Rechter der Nutzer" den „Rechten der Urheber" gegenübergestellt werden können; s. dazu *Vinje*, EIPR 1999, 192, 195. Von der in Deutschland herrschenden Meinung wird die Charakterisierung von Schrankenbestimmungen als „Rechten der Nutzer" abgelehnt; vgl. nur *Melichar* in: Schricker (Hrsg.), UrhG-Kommentar, vor §§ 45 ff. Rdnr. 2; zum Verhältnis zwischen technischen Schutzmaßnahmen und § 53 UrhG s. in diesem Zusammenhang auch – mit einer nicht überzeugenden begrifflichen Argumentation – *Wiechmann*, ZUM 1989, 111, 118. Auch in den USA besteht Streit hinsichtlich der Frage, ob das Urheberrecht nicht nur Rechte der Urheber, sondern auch Rechte der Nutzer festlege. So wird vertreten, die in 17 U.S.C. § 107 enthaltene „fair use"-Doktrin sei nicht nur ein Verteidigungsmittel gegen urheberrechtliche Ansprüche, sondern kodifiziere ein positives Recht des Nutzers, in bestimmten Fällen das urheberrechtlich geschützte Werk ohne Zustimmung des Urhebers zu nutzen; s. *Patterson/Lindberg* und die Nachweise in *Brennan*, 36 Hous. L. Rev. 61, 77 (1999); *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 191 Fn. 119. Von der überwiegenden Meinung wird diese Sichtweise jedoch ebenfalls abgelehnt. Die Tatsache, daß Nutzungen im Anwendungsbereich der „fair use"-Doktrin keine Urheberrechtsverletzung darstellen, sage noch nichts über deren Rechtmäßigkeit aus, da sie noch nach anderen Gesetzen rechtswidrig sein könnten; *Brennan*, 36 Hous. L. Rev. 61, 77 ff. (1999); s. a. *Nimmer/Brown/Frischling*, 87 Cal. L. Rev. 17, 76 (1999); Bateman v. Mnemonics, Inc., 79 F.2d 1532, 1542 Fn. 22 (11th Cir. 1996); *Bell*, Escape from Copyright, S. 28 f.; vgl. weiterhin *N. B. Nimmer/D. Nimmer*, § 12A.07[B], S. 12A-82 ff.; *D. Nimmer*, 148 U. Penn. L. Rev. 673, 714 f. (2000); *Information Infrastructure Task Force*, S. 231, mit berechtigter Kritik von *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 199. Für die vorliegenden Zwecke ist es aber gar nicht notwendig, sich der Ansicht von den Schrankenbestimmungen als Nutzer*rechten* anzuschließen; ebenso *Nimmer/Brown/Frischling*, a. a. O., S. 76. Das Urheberrecht stellt einen Ausgleich zwischen den Interessen der Urheber und der Nutzer bzw. der Allgemeinheit dar. Auch wenn man die Schrankenbestimmungen als bloße inhaltliche Beschränkungen der Verwertungsrechte des Urhebers auffaßt, ist eine Übertragung der Schrankenbestimmungen auf andere Schutzmechanismen in DRM-Systemen geboten, da diesen solche Beschränkungen nicht inhärent sind. Bei der Beschränkung des Schutzes von DRM-Systemen geht es also nicht darum, dem Nutzer irgendwelche feststehenden „Rechte" im rechtlichen Sinn zu verleihen, sondern es geht um die Aufrechterhaltung des Interessenausgleichs, wie er sich im Urheberrecht wiederfindet. Die Bevorzugung der Inhalteanbieter in DRM-Systemen hat einfach faktisch zur Folge, daß Fragen des Nutzerschutzes immer wichtiger werden. In großem Umfang handelt sich sich bei der ganzen Frage auch nur um einen Streit um Begriffe.

[1968] So läßt sich die Entwicklung der letzen Jahre in den USA und Europa, in das Urheberrecht zunehmend Bestimmungen einzuführen, die zum Schutz der Nutzer durch vertragliche Vereinbarungen nicht abgeändert werden können, mit dieser These erklären; s. dazu unten Teil 4, B.

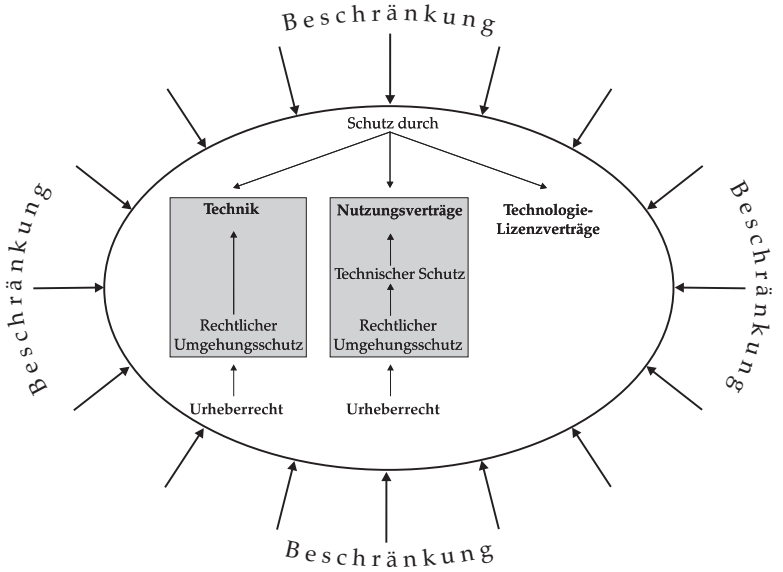


Abbildung 13: Unterschiedliche Schutzmechanismen in DRM-Systemen (3)

C. Ergebnis

Sowohl eine rechtliche als auch eine rechtsökonomische Untersuchung von DRM-Systemen ergibt, daß die ineinandergreifenden Schutzmechanismen von DRM-Systemen das Urheberrecht ersetzen könnten.[1969] Zwar wird das Urheberrecht auch in DRM-Systemen weiterhin für den Schutz der Inhalteanbieter sorgen. Es verliert jedoch den Status als primärer Schutzmechanismus, sondern unterstützt vielmehr andere Schutzmechanismen.[1970] Dagegen zeigt die rechtliche und rechtsökonomische Untersuchung, daß urheberrechtliche Schrankenbestimmungen auch in DRM-Systemen von zentraler Bedeutung sind.[1971] Überspitzt ausgedrückt bedeutet dies, daß die Begründung für das Urheberrecht als Schutzmechanismus für den Inhalteanbieter wegfällt, während die Begründung für urheberrechtliche Schrankenbestimmungen bestehen

[1969] S. dazu aus juristischer Sicht oben Teil 3, A II 2, aus rechtsökonomischer Sicht oben Teil 3, A III 2 b.

[1970] S. dazu aus juristischer Sicht oben Teil 3, B II 2, aus rechtsökonomischer Sicht oben Teil 3, B I 3.

[1971] S. dazu aus juristischer Sicht oben Teil 3, B II 3 a, aus rechtsökonomischer Sicht oben Teil 3, B I 2.

bleibt.[1972] Im Bereich von DRM-Systemen wandelt sich das Urheberrecht von einem Urheber- zu einem Nutzerschutz. Die Definition solcher Beschränkungen von DRM-Systemen könnte die Aufgabe eines zukünftigen Informationsrechts werden.[1973] Ob und inwieweit die bestehenden Regelungen dieser Aufgabe gerecht werden, soll im folgenden Teil untersucht werden.

[1972] Ebenso *Lessig*, S. 129: „[DRM systems] thus achieve what copyright law achieves. But it can achieve this protection *without the law doing the restricting*" (Hervorhebung im Original). Dabei handelt es sich natürlich um eine grobe Vereinfachung. Auf den Modellcharakter der vorliegenden Untersuchung sei erneut hingewiesen, s. oben bei Fn. 1305 f.

[1973] Ebenso *Hugenholtz*, 26 Brooklyn J. Int'l L. 77, 78 f. (2000): „The combination of contract and technology poses a direct threat to the copyright system as we know it, and may require an entirely new body of information law to safeguard the public domain"; *van den Bergh*, I.P.Q. 1998, 17, 34: „Defining the boundaries of freedom to contract to safeguard access to information may become the primary goal of the copyright law of the 21st century."

Teil 4: Recht als Beschränkung des DRM-Schutzes

Die vorangegangene rechtliche und rechtsökonomische Untersuchung hat ergeben, daß DRM-Systeme den Inhalteanbietern einen zu weitgehenden Schutz verleihen können, bei dem Interessen Dritter und der Allgemeinheit unzureichend berücksichtigt werden. Daher ist eine Beschränkung des DRM-Schutzes notwendig, wie auch immer diese Beschränkung im einzelnen aussehen mag. Es geht um eine Beschränkung aller Schutzmechanismen in einem DRM-System – Technik, Nutzungsverträge, Technologie-Lizenzverträge und rechtlicher Umgehungsschutz. Dem Inhalteanbieter ist es unbenommen, diese Schutzmechanismen kumulativ einzusetzen. Es existieren weder faktische noch rechtliche Beschränkungen, die Schutzmechanismen in einem umfassenden DRM-System zu kombinieren.[1974] Alle diese Schutzmechanismen können dazu führen, daß

[1974] Eine solche gesetzliche Beschränkung wird in den USA insbesondere von *Bell* gefordert. Er vertritt die These, die Kombination aus DRM-Schutz – insbesondere technischem und vertraglichem Schutz – und dem Schutz durch das Urheberrecht verleihe den Inhalteanbietern zu weitgehende Schutzmöglichkeiten. Daher müsse das Recht den Inhalteanbietern die Möglichkeit geben, zwischen diesen beiden Schutzmechanismen – DRM-Schutz und Urheberrecht – zu wählen. Schütze sich ein Inhalteanbieter durch ein DRM-System selbst, müsse ein „exit from copyright" ermöglicht werden: „Why, after all, should we continue to offer the owners of expressive works the benefits of an intellectual property welfare program that they no longer need?"; *Bell*, Escape from Copyright, S. 3, 15, 47 f.; s. auch schon *ders.*, 76 N.C. L. Rev. 557, 615 (1998). Im vorliegenden Zusammenhang kann die These *Bells* nicht überzeugen. *Bell* geht davon aus, daß die *Kombination* des Schutzes durch DRM-Systeme (technischer und vertraglicher Schutz) mit dem Schutz durch das Urheberrecht dem Inhalteanbieter einen zu weitgehenden Schutz verleiht; s. nur *Bell*, Escape from Copyright, S. 53. Diese Analyse trifft jedoch nicht die Problematik von DRM-Systemen. Wie oben dargelegt, verleihen nur schon die typischen Schutzmechanismen von DRM-Systemen (Technik, Nutzungsvertrag, Technologie-Lizenzvertrag) einen zu weitgehenden Schutz. Das Urheberrecht spielt als Schutzmechanismus für den Inhalteanbieter nur noch eine untergeordnete Rolle. Durch einen Verzicht auf das Urheberrecht würde damit das Problem des zu weitgehenden Schutzes in DRM-Systemen nicht beseitigt. Abgesehen davon erscheint eine solche Lösung zumindest im kontinentaleuropäischen Immaterialgüterrecht auch als unrealistisch. Daneben ist zu kritisieren, daß nach *Bell* im Falle eines „exit from copyright" auch die Beschränkungen des Urheberrechts nicht mehr auf DRM-Systeme anwendbar sein sollen; *Bell*, Escape from Copyright, S. 46. Nur wenn der Inhalteanbieter die Vorteile des Urheberrechts genießen wolle, müsse er sich gefallen lassen, daß dessen Beschränkungen auch bei DRM-Systemen greifen; vgl. *Bell*, 76 N.C. L. Rev. 557, 615 f. (1998). Wie die vorliegende Untersuchung gezeigt hat, sind aber gerade bei DRM-Systemen außerhalb des urheberrechtlichen Schutzsystems Beschränkungen notwendig. In den USA haben sich auch andere Autoren mit der Frage eines „exit from copyright" – wenn auch weniger ausführlich – beschäftigt, stehen ihr aber regelmäßig

urheberrechtliche Grundsätze – insbesondere Schrankenbestimmungen – in DRM-Systemen unterlaufen werden. Im folgenden Teil wird im Überblick dargestellt, ob und inwieweit die Gesetzgeber auf europäischer, deutscher und U.S.-amerikanischer Ebene solche Beschränkungen eingeführt haben und ob diese Regelungen eine gewisse gesetzgeberische Systematik erkennen lassen. Daneben wird auch auf einschlägige Rechtsprechung eingegangen. Zu diesem Zweck werden rechtliche Beschränkungen des Urheberrechts (dazu unten A), Beschränkungen urheberrechtlicher Nutzungsverträge (dazu unten B), Beschränkungen von Technologie-Lizenzverträgen (dazu unten C) sowie von technischen Schutzmaßnahmen und dem dazugehörenden rechtlichen Umgehungsschutz (dazu unten D) dargestellt.[1975]

Es ist im Rahmen der vorliegenden Untersuchung unmöglich, eine umfassende Analyse der rechtlichen Beschränkung aller Schutzmechanismen in DRM-Systemen zu leisten. Insbesondere ist zu beachten, daß das Problem nicht gelöst wäre, wenn man einfach festlegen würde, daß jede urheberrechtliche Schrankenbestimmung auch in DRM-Systemen durschlagen muß.[1976] DRM-Systeme können dazu führen, daß manche urheberrechtlichen Schrankenbestimmungen bedeutungslos werden und daß sich die Bedeutung anderer Schrankenbestimmungen wandelt.[1977] Auch kann ein Bedarf für gänzlich neue Schrankenbestimmungen entstehen. Um festzustellen, welche Schrankenbestimmungen des Urheberrechts auch in DRM-Systemen notwendig sind, müßten die einzelnen Schrankenbestimmungen hinsichtlich ihrer Wirkung und ihres Zwecks untersucht werden. Daraus könnte abgeleitet werden, ob sie auch in DRM-Systemen noch von gleicher Bedeutung sind.[1978] Eine solche Analyse will und kann die vorliegende Arbeit nicht liefern. Der folgende Teil will vielmehr auf abstrakterer Ebene die unterschiedlichen Reaktionsmöglichkeiten der Gesetzgeber aufzeigen und im Überblick darstellen, welche dieser Möglichkeiten die Gesetzgeber in Europa, Deutschland und den USA gewählt haben. Der Überblick beschränkt sich auf urheberrechtliche Erwägungen. Beschränkungen von DRM-Systemen, die aus anderen Rechtsgebieten stammen können – unter anderem dem Kar-

ablehnend gegenüber; s. nur *Lemley*, 87 Cal. L. Rev. 111, 149 f. (1999); *Cohen*, 12 Berkeley Tech. L. J. 161, 182 f. (1997); *Heide*, 15 Berkeley Tech. L. J. 993, 1015 f. (2000).

[1975] Im Aufbau orientiert sich der vorliegende Teil damit am 2. Teil dieser Untersuchung.

[1976] *Wand*, S. 54, bezeichnet diesen Ansatz als „Durchgriffslösung".

[1977] Als Beispiel mag § 53 UrhG dienen, s. oben Fn. 1956.

[1978] Darauf weist zu Recht insbesondere *Wand*, S. 60, 125, hin. Zu weiteren Problemen im Verhältnis zwischen technischen Schutzmaßnahmen und urheberrechtlichen Schrankenbestimmungen s. *ders.*, S. 54 ff., 123 ff. *Hoeren*, MMR 2000, 3, 5, plädiert für eine grundsätzliche Neugestaltung der Schrankenbestimmungen schon im urheberrechtlichen Bereich.

tell,[1979] Datenschutz-[1980] und Verbraucherschutzrecht[1981] sowie dem Recht der freien Meinungsäußerung[1982] –, werden nicht weiter dargestellt. Eine tiefergehende Analyse der gesamten Problematik bliebe einer eigenen Untersuchung mit beträchtlichem Umfang vorbehalten.

A. Beschränkung des Urheberrechts

Das Urheberrecht wird seit jeher durch eine Vielzahl von Schrankenbestimmungen beschränkt. Art. 5 der Richtlinie zum Urheberrecht in der Informationsgesellschaft enthält eine lange Aufzählung möglicher Schrankenbestimmungen.[1983] Heute stellt sich bei vielen Schrankenbestimmungen das Problem, inwieweit sie im digitalen Umfeld anwendbar sind und ob diesbezüglich Gesetzesänderungen notwendig sind. Auf die damit zusammenhängenden Fragen wird hier nicht eingegangen. Einerseits handelt es sich um allgemeine urheberrechtliche Probleme, die nicht nur bei DRM-Systemen auftreten. Andererseits existiert zur Anwendung urheberrechtlicher Schrankenbestimmungen im digitalen Umfeld schon eine Reihe umfangreicher Untersuchungen.[1984]

B. Beschränkung von Nutzungsverträgen

In DRM-Nutzungsverträgen können Klauseln enthalten sein, durch die urheberrechtliche Schrankenbestimmungen ausgehebelt werden. Fallen diese Nutzungsverträge unter den Anwendungsbereich des Urheberrechts,[1985] können urheberrechtliche Vorschriften die Vertragsfreiheit der Parteien eines DRM-Nutzungsvertrags beschränken. In diesen Fällen

[1979] S. dazu *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 200; *Polley*, CR 1999, 345, 349 ff.; *Wand*, S. 135. 185.

[1980] *Cohen*, 28 Conn. L. Rev. 981 ff. (1996), leitet gar ein „right to read anonymously" aus dem First Amendment zur U.S.-Verfassung her.

[1981] Zur Kontrolle nach dem AGBG s. *Polley*, CR 1999, 345, 353 ff.

[1982] S. dazu oben Fn. 1957.

[1983] S. dazu *Kröger*, CR 2001, 316, 318 ff.

[1984] S. in Deutschland nur *Schricker* (Hrsg.), Urheberrecht auf dem Weg zur Informationsgesellschaft, S. 153 ff.; *Loewenheim* in: Hoeren/Sieber (Hrsg.), Teil 7.4; *Raue/Hegemann* in: Hoeren/Sieber (Hrsg.), Teil 7.5; *Bechtold*, Multimedia und das Urheberrecht, S. 11 ff., 18 ff.; *Leinemann*, S. 135 ff. Die Diskussion ist noch lange nicht abgeschlossen. S. zur neu aufgetretenen Problematik, wie P2P-Systeme (Napster, Gnutella, Freenet u. ä.) unter urheberrechtlichen Aspekten zu beurteilen sind, *Ahrens*, ZUM 2000, 1029 ff.; *Kreutzer*, GRUR 2001, 193 ff. und 307 ff.

[1985] Dies ist bei DRM-Nutzungsverträgen nicht notwendigerweise der Fall, s. dazu oben Teil 3, A II 1 b aa. Im folgenden soll jedoch auf DRM-Nutzungsverträge eingegangen werden, die auch Nutzungsverträge im urheberrechtlichen Sinn darstellen.

können urheberrechtliche Schrankenbestimmungen vertraglich nicht abbedungen werden.

I. Europäischer Rechtsrahmen

In Europa wurde das Verhältnis zwischen urheberrechtlichen Schrankenbestimmungen und Nutzungsverträgen bisher erstaunlich selten problematisiert.[1986] In europäischen Urheberrechts-Richtlinien finden sich nur vereinzelt Vorschriften zu diesem Verhältnis. So darf der Urheber eines Computerprogramms dem Nutzer vertraglich nicht untersagen, eine Sicherungskopie des Programms zu erstellen oder das Programm zu dekompilieren beziehungsweise dessen Funktionsweise zu untersuchen, Art. 9 Abs. 1 S. 2 Computerprogrammrichtlinie. Der Urheber einer Datenbank darf dem rechtmäßigen Nutzer bestimmte Nutzungshandlungen nicht vertraglich untersagen, wenn sie für den Zugang zum Inhalt der Datenbank und deren normale Benutzung erforderlich sind, Art. 15 i. V. m. Art. 6 Abs. 1 Datenbankrichtlinie. Der Inhaber des sui-generis-Datenbankrechts darf einem rechtmäßigen Nutzer nicht vertraglich untersagen, unwesentliche Teile der Datenbank zu beliebigen Zwecken zu entnehmen und/oder weiterzuverwenden, Art. 15 i. V. m. Art. 8 Abs. 1 Datenbankrichtlinie.[1987]

Die Richtlinie zum Urheberrecht in der Informationsgesellschaft[1988] hatte sich zum Ziel gesetzt, die urheberrechtlichen Schrankenbestimmungen auf europäischer Ebene zu harmonisieren.[1989] Zu diesem Zweck zählt sie in Art. 5 insgesamt 20 verschiedene Schrankenbestimmungen auf, die von den Mitgliedstaaten umgesetzt werden können.[1990] Diese Aufzählung ist abschließend.[1991] Es erstaunt daher um so mehr, daß die Richtlinie in einem Erwägungsgrund – entgegen den dargestellten Regelungen in früheren Urheberrechtsrichtlinien – ausdrücklich feststellt, daß die Schrankenbestimmungen vertraglichen Vereinbarungen nicht entgegenstehen dürfen.[1992]

[1986] Ebenso *Guibault* in: Hugenholtz (Hrsg.), S. 125, 126, 152 f.; *Vinje*, EIPR 1999, 192, 195. *Guibault* liefert eine der wenigen ausführlichen Untersuchungen zu dieser Frage aus europäischer Sicht.

[1987] S. dazu *v. Lewinski* in: Walter (Hrsg.), Datenbank-RL, Art. 6 Rdnr. 13 ff.

[1988] S. dazu allgemein oben Teil 2, D I 2 a bb 2.

[1989] Ob diese Harmonisierung geglückt ist, ist eine andere Frage; s. *Hugenholtz*, EIPR 2000, 499, 500 f.

[1990] Nur eine der Schrankenbestimmungen muß umgesetzt werden, Art. 5 Abs. 1 der Richtlinie.

[1991] Erwägungsgrund 32 der Richtlinie, ABl. EG Nr. L 167 vom 22. 6. 2001, S. 10, 12.

[1992] Erwägungsgrund 45 der Richtlinie meint: „Die in Artikel 5 Absätze 2, 3 und 4 vorgesehenen Beschränkungen sollten jedoch vertraglichen Beziehungen zur Sicherstellung eines gerechten Ausgleichs für die Rechteinhaber nicht entgegenstehen, soweit dies nach innerstaatlichem Recht zulässig ist"; ABl. EG Nr. L 167 vom 22. 6. 2001, S. 10, 14. Dieser Erwägungsgrund war in den Richtlinienentwurf während der ersten Lesung durch das Europäische Parlament eingefügt worden.

Selbst wenn das Recht eines Mitgliedstaates urheberrechtliche Schrankenbestimmungen vorsieht, kann der Urheber diese durch vertragliche Vereinbarungen umgehen. Für Inhalteanbieter in DRM-Systemen führt dies zu einer deutlichen Stärkung ihrer Position.[1993] Angesichts der lückenhaften Problematisierung des Verhältnisses zwischen Schrankenbestimmungen und Nutzungsverträgen in den europäischen Urheberrechts-Richtlinien und der fehlenden Gerichtspraxis ist die Rechtslage insgesamt unklar.[1994]

II. Deutscher Rechtsrahmen

Auch in Deutschland gibt es wenige systematische Untersuchungen zum Verhältnis zwischen Urheberrecht und Nutzungsverträgen. Im UrhG existieren nur wenige Schrankenbestimmungen, die ausdrücklich nicht abbedungen werden können. Sie beruhen auf den europäischen Richtlinien, die gerade dargestellt wurden: § 69 g Abs. 2 UrhG setzt Art. 9 Abs. 1 S. 2 der Computerprogrammrichtlinie, § 55 a S. 3 und § 87 e UrhG setzen Art. 15 der Datenbankrichtlinie um. Im Rahmen des § 69 d UrhG besteht nach nahezu einhelliger Meinung ein zwingender Kern von Befugnissen des Nutzers eines Computerprogramms, die auch durch vertragliche Abreden nicht eingeschränkt werden können.[1995]

Neben diesen ausdrücklichen Regelungen können Nutzungsverträge wegen allgemeiner urheberrechtlicher Grundsätze beschränkt werden. Grundsätzlich kann der Urheber in einem Nutzungsvertrag Nutzungsrechte räumlich, zeitlich oder inhaltlich beschränkt einräumen, § 32 UrhG. Der Zuschnitt des Nutzungsrechts ist aber nur in gewissen Grenzen möglich. Obwohl im Immaterialgüterrecht kein numerus clausus wie im Sachenrecht existiert,[1996] ist doch auf den Verkehrsschutz Rücksicht zu nehmen. Daher können Nutzungsrechte nach allgemeiner Meinung

[1993] Ebenso kritisch *Hugenholtz*, 26 Brooklyn J. Int'l L. 77, 83 (2000); *ders.*, EIPR 2000, 499, 501; *Guibault* in: Hugenholtz (Hrsg.), S. 125, 153; *Vinje*, EIPR 1999, 192, 196. *Walter* in: Walter (Hrsg.), Info-RL, Kap. IV Rdnr. 98, fragt sich dagegen, ob aus der Formulierung der „vertraglichen Beziehungen zur Sicherstellung eines *gerechten Ausgleichs*" geschlossen werden könne, daß vertragliche Vereinbarungen unzulässig seien, durch die freie Nutzungen gänzlich abbedungen würden. Dies trifft m. E. nicht zu. Der Erwägungsgrund spricht nicht von einem gerechten (Interessen-)Ausgleich zwischen den Rechteinhabern und den Nutzern, sondern von einem „gerechten Ausgleich *für die Rechteinhaber*." Die englische Fassung der Richtlinie spricht von „fair compensation for the rightholders". Es geht also um die gerechte monetäre Kompensation des Rechteinhabers.

[1994] Ebenso *Guibault* in: Hugenholtz (Hrsg.), S. 125, 155, und *Vinje*, EIPR 1999, 192, 195 f., der einen differenzierten Ansatz vorschlägt.

[1995] Darunter fällt beispielsweise das Recht, das Programm zu laden und ablaufenzulassen, es im Arbeitsspeicher des Computers zu speichern, Fehler des Programms zu beseitigen und ähnliches; s. *Loewenheim* in: Schricker (Hrsg.), UrhG-Kommentar, § 69 d Rdnr. 12 f.; *Schuhmacher*, CR 2000, 641, 645; BGH CR 2000, 656, 657 f.; *Lehmann* in: Beier/Götting/Lehmann/Moufang (Hrsg.), S. 543, 555 ff.

[1996] *Schack*, Rdnr. 541.

nur eingeschränkt werden, wenn es sich dabei nach der Verkehrsauffassung um übliche, technisch und wirtschaftlich eigenständige und damit klar abgrenzbare konkrete Nutzungsformen handelt.[1997]

Diese Grundsätze haben bei Softwareüberlassungsverträgen[1998] zu einem verästelteten Streit über die Zulässigkeit vertraglicher Nutzungsbeschränkungen geführt.[1999] Es geht um die Frage, ob der Rechteinhaber die eingeräumten Nutzungsrechte mit dinglicher Wirkung derart beschränken kann, daß die Nutzung der Software nur auf einem bestimmten Computer zulässig ist (sogenannte „CPU-Klausel"),[2000] daß die Software nicht auf einem Netzwerkserver für mehrere Rechner freigeschaltet wird (sogenannte „Netzwerkklauseln"),[2001] und daß die Weitergabe der Software untersagt oder an bestimmte Bedingungen geknüpft wird.[2002] Schließlich existieren Klauseln, die den Vertrieb der Software auf bestimmte Abnehmerkreise einschränken oder die Art und Weise des Vertriebs bestimmen wollen. Wichtigstes Beispiel solcher Klauseln sind sogenannte „OEM-Klauseln",[2003] in denen der Softwarehersteller den Lizenznehmer verpflichtet, die Software nur zusammen mit einem Computer an Endkunden zu verkaufen. Nachdem zu dieser Frage eine Vielzahl widersprüchlicher Gerichtsentscheidungen ergangen waren,[2004] entschied der Bundesgerichtshof Mitte 2000, daß solche Klauseln keine dingliche Wir-

---

[1997] BGH CR 2000, 651, 652; *Schricker* in: Schricker (Hrsg.), UrhG-Kommentar, §§ 31/32 Rdnr. 8; *Schack*, Rdnr. 541 ff.

[1998] S. dazu oben Teil 2, B II 2 a.

[1999] Die im Rahmen des § 32 UrhG entwickelten Grundsätze greifen auch im Rahmen der §§ 69 a ff., BGH CR 2000, 651, 652.

[2000] Nach überwiegender Meinung sind solche Klauseln unwirksam, da die Nutzung eines Programms auf nur einem Rechner keine abgrenzbare und anerkannte konkrete Verwendungsmöglichkeit des Programms sei; s. *Schuhmacher*, CR 2000, 641, 646 ff.; *Polley*, CR 1999, 345, 347.

[2001] Netzwerkklauseln können wirksam sein; s. dazu *Polley*, CR 1999, 345, 347; *Schuhmacher*, CR 2000, 641, 649 f.; *Lehmann*, NJW 1993, 1822, 1825; *Marly*, Softwareüberlassungsverträge, Rdnr. 983 ff., 1008 ff.

[2002] Hier kann der Erschöpfungsgrundsatz des § 69 c Nr. 3 S. 2 UrhG eingreifen, so daß derartige Klauseln jedenfalls keine dingliche Wirkung haben, *Schuhmacher*, CR 2000, 641, 648; *Polley*, CR 1999, 345, 347, 348 f.; *Marly*, Softwareüberlassungsverträge, Rdnr. 918 ff.

[2003] „OEM" ist die Abkürzung für „Original Equipment Manufacturer". Dieses Lizenzmodell wurde insbesondere von Microsoft verwendet. Microsoft schloß mit den großen Hardwareherstellern OEM-Lizenzen ab. Für den Endkunden waren OEM-Versionen der Microsoft-Software sehr viel billiger als die vergleichbare Vollversion der Software. Nach einer Grundsatzentscheidung des BGH im Jahr 2000 (s. dazu sogleich) änderte Microsoft sein Vertriebskonzept. Tatsächlich ging es in dem BGH-Fall um keine OEM-Lizenz, sondern um eine „Delivery Service Partner" (DSP)-Lizenz.

[2004] KG, CR 1998, 137; OLG München, CR 1998, 265; OLG Frankfurt, CR 1999, 7; OLG Frankfurt, CR 2000, 581; KG, CR 1996, 531. S. dazu *Witte*, CR 2000, 654; *ders.*, CR 1999, 65, 66 ff.; *Polley*, CR 1999, 345, 347 ff.

kung entfalten, da sich das Verbreitungsrecht mit der Veräußerung der Software an den Lizenznehmer erschöpft habe.[2005]

Diese Grundsätze, durch die die Ausgestaltung von Nutzungsverträgen beschränkt wird, gelten jedoch nicht, wenn dem Nutzer auf Verfügungsebene ein umfassendes Nutzungsrecht eingeräumt wird, das nur auf schuldrechtlicher Ebene eingeschränkt wird. Dies ist grundsätzlich in weiten Grenzen zulässig.[2006] Jedoch sind bei Standardverträgen die Vor-

[2005] BGH, CR 2000, 651. Die Einzelheiten der Entscheidung sind recht komplex. In dem Fall, welcher der Entscheidung des BGH zugrundelag, hatte ein Unternehmen, das unter einer Lizenz von Microsoft OEM-Versionen von Microsoft-Produkten herstellte („authorized replicator"), eine solche OEM-Version an einen ebenfalls von Microsoft lizenzierten Zwischenhändler veräußert. Dieser Zwischenhändler veräußerte die OEM-Version an einen Dritt-Händler, der sich nicht an die Bedingungen der OEM-Lizenz hielt und die Software ohne Hardware an Kunden verkaufte. Microsoft verklagte daraufhin diesen Dritt-Händler, zu dem keinerlei vertragliche Beziehungen bestanden. Entscheidend war, daß sich in dieser Vertragskette sowohl der „authorized replicator" als auch der Zwischenhändler an die Vertragsbedingungen von Microsoft gehalten hatte. Mit der Veräußerung der OEM-Version durch den „authorized replicator" an den Zwischenhändler hatte sich das Verbreitungsrecht von Microsoft eigentlich erschöpft. Fraglich war nun, ob Microsoft die Wirkung der Erschöpfung insofern begrenzen konnte, daß bei nachfolgenden Weiterveräußerungen die Bedingungen der OEM-Lizenz ebenfalls weiterhin beachtet werden mußten, wenn nicht das Verbreitungsrecht von Microsoft verletzt werden sollte. Grundsätzlich hat eine dinglich wirkende Begrenzung des Nutzungsrechts auch eine Beschränkung der Erschöpfung zur Folge, *Loewenheim* in: Schricker (Hrsg.), UrhG-Kommentar, § 17 Rdnr. 49. Danach könnte man vertreten, daß bei einer Veräußerung der OEM-Version durch den Dritt-Händler an einen Kunden ohne Hardware die Bedingungen der OEM-Lizenz nicht eingehalten seien, so daß eine Verletzung des – nur eingeschränkt eingeräumten – Verbreitungsrechts vorliege. Der BGH lehnte eine solch weitreichende Folge der Beschränkung des Verbreitungsrechts jedoch ab. Nach ihm gilt die Beschränkung der Erschöpfungswirkung nur im Verhältnis zwischen dem Urheber und dem Erstkäufer. Die Möglichkeit, ein Nutzungsrecht nach § 32 UrhG inhaltlich zu beschränken, führe nicht zu einer entsprechend eingeschränkten Erschöpfung in der Weise, daß der Urheber auf den *weiteren* Absatzweg des Werkexemplars (d. h. Verkauf durch den Erstkäufer an Dritte) Einfluß nehmen könne. Eine solche Verdinglichung schuldrechtlicher Verpflichtungen sei dem deutschen Recht fremd; s. BGH CR 2000, 651, 653. Die Relevanz der BGH-Entscheidung hängt stark von der tatsächlichen Ausgestaltung des Vertriebssystems ab; bei einem Direktvertrieb der Software an einen Händler, der sich dann an die Bedingungen der OEM-Lizenz nicht hält, würde keine Erschöpfung eintreten, und zwar auch nicht auf den nachgelagerten Vertriebsstufen, BGH, CR 2000, 651, 653. Die Frage, ob OEM-Klauseln überhaupt eine zulässige Beschränkung i. S. d. § 32 UrhG darstellen, ließ der BGH ausdrücklich offen, BGH CR 2000, 651, 653. S. zum ganzen *Chrocziel*, CR 2000, 738 ff.; *Metzger*, GRUR 2001, 210; *Jaeger*, ZUM 2000, 1070 ff.; *Witte*, CR 2000, 654 f.; *Leistner/Klein*, MMR 2000, 751 f. Im Online-Umfeld ist die Entscheidung nicht von Relevanz, da nach h. M. der Erschöpfungsgrundsatz hier nicht greift (s. oben Fn. 1619). Eine vom Sachverhalt her ähnliche U.S.-amerikanische Entscheidung ist Microsoft Corp. v. Harmony Computers & Electronics, Inc., 846 F. Supp. 208 (E.D.N.Y. 1994).

[2006] S. dazu oben Teil 2, B II 2 c.

schriften des AGB-Gesetzes zu beachten.[2007] Über § 9 Abs. 2 AGBG können Grundgedanken des Urheberrechts, die unmittelbar nur für das Verfügungsgeschäft gelten, auch für das Verpflichtungsgeschäft Wirkung entfalten.[2008]

III. U.S.-amerikanischer Rechtsrahmen

Im Gegensatz zur Lage in Europa und Deutschland ist das Verhältnis zwischen „copyright" und „contract" in den USA einer der Schwerpunkte der urheberrechtlichen Diskussion der letzten Jahre. Zwar enthält der „Copyright Act" nur wenige spezielle Regelungen zu der Frage, ob seine Vorschriften vertraglich abdingbar sind.[2009] Aus allgemeineren Grundsätzen können sich jedoch Beschränkungen von Nutzungsverträgen ergeben. Diese sollen im folgenden im Überblick dargestellt werden.

1. Federal Preemption

a) Allgemeines

Während das Urheberrecht nach U.S.-amerikanischer Verfassungslage in die Zuständigkeit des Bundes fällt, ist das Vertragsrecht einzelstaatliches Recht und bestimmt sich entweder nach dem ungeschriebenen Common Law oder nach Kodifikationen wie dem „Uniform Commercial Code".[2010] Die Wirksamkeit urheberrechtlicher Nutzungsverträge beurteilt sich daher grundsätzlich zunächst nach dem „contract law" des jeweiligen Bundesstaates. Anders als in Deutschland kann man in den USA nicht von einem eigenständigen „Urhebervertragsrecht" sprechen. Es geht vielmehr um die Schnittstelle zweier grundsätzlich getrennter Rechtsgebiete: „copyright law" und „contract law".[2011]

Aus dieser Kompetenzverteilung ergibt sich ein Konfliktpotential, das grundsätzlich durch die sogenannte „Supremacy Clause" der U.S.-Verfas-

[2007] Danach können CPU-Klauseln gegen § 9 AGBG verstoßen, *Schuhmacher*, CR 2000, 641, 646 f.; *Polley*, CR 1999, 345, 353. Gleiches gilt für Weitergabeverbote, *Schuhmacher*, a. a. O., S. 648; *Polley*, a. a. O., S. 354; *Marly*, Softwareüberlassungsverträge, Rdnr. 925 ff.

[2008] *Schuhmacher*, CR 2000, 641, 648, wendet über diese Konstruktion den Erschöpfungsgrundsatz auf schuldrechtliche Weitergabeverbote in Softwareüberlassungsverträgen an.

[2009] Dies verneint z. B. 17 U.S.C. § 203 (a) (5) und bejaht 17 U.S.C. § 113 (d). Regelmäßig fehlt eine solche Bestimmung, *Lemley*, 87 Cal. L. Rev. 111, 142 (1999).

[2010] Der „Uniform Commercial Code" ist nur ein Modellgesetz, das in den meisten Bundesstaaten der USA in einzelstaatliches Recht umgesetzt wurde. Eine Ausnahme bildet der Bundesstaat Louisiana, der über ein Zivilgesetzbuch verfügt. S. zum ganzen *Bodewig* in: Beier/Götting/Lehmann/Moufang (Hrsg.), S. 833, 836 f.

[2011] S. *Monroe*, 1 Marq. Intell. Prop. L. Rev. 143 (1997); *O'Rourke*, 12 Berkeley Tech. L. J. 53, 55 (1997); *Bodewig* in: Beier/Götting/Lehmann/Moufang (Hrsg.), S. 833, 834 f.

sung aufgelöst werden soll.[2012] Diese Bestimmung kann auch im urheberrechtlichen Bereich relevant sein.[2013] Wichtiger ist jedoch die spezialgesetzliche Regelung in 17 U.S.C. § 301. Diese „preemption doctrine" versucht, das Verhältnis zwischen Bundes- und Landesrecht im Bereich des Urheberrechts zu regeln.[2014] Im Verhältnis zwischen „contract law" und „copyright law" kann die „preemption doctrine" dazu führen, daß einzelne vertragliche Ansprüche nicht wirksam sind.[2015]

Nach der Regelung des 17 U.S.C. § 301 kommt es für den Vorrang des Bundesrechts darauf an, ob das einzelstaatliche Recht sowohl einen *Gegenstand* betrifft, der unter den Anwendungsbereich des bundesrechtlichen Urheberrechts fällt („protected subject matter"), als auch Rechte einräumt, die den ausschließlichen Rechten des Urheberrechts *gleichwertig* sind („equivalent to exclusive rights").[2016] Ein solches gleichwertiges Recht liegt nicht vor, wenn zur Verletzung dieses Rechts ein zusätzliches, über die Urheberrechtsverletzung hinausgehendes Element notwendig ist („extra element test").[2017] Wann bei Nutzungsverträgen ein solches „extra element" vorliegt, ist unter den Gerichten umstritten.[2018] Auch die Frage, was unter der „protected subject matter" des Copyright Act zu verstehen sei, ist sehr umstritten.[2019] Entscheidend ist letztlich, ob sich das einzel-

[2012] U.S. Const., Art. VI, Cl. 2: „This Constitution, and the Laws of the United States […] shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the Contrary notwithstanding."

[2013] S. beispielsweise *Lemley*, 87 Cal. L. Rev. 111, 141 Fn. 130, 147 (1999); *Goldstein*, Copyright, § 15.3, S. 15:29 ff., und im Überblick *Bodewig* in: Beier/Götting/Lehmann/Moufang (Hrsg.), S. 833, 840 f.

[2014] S. dazu in der deutschen Literatur im Überblick *Götting/Fikentscher* in: Assmann/Bungert (Hrsg.), Kap. 7, Rdnr. 202 ff.

[2015] *R. T. Nimmer*, Information Law, § 2.13, S. 2–39. Da die „preemption doctrine" nur das Verhältnis zwischen Bund und Einzelstaaten regelt, verhindert sie genau betrachtet nicht direkt die Wirksamkeit eines Vertrags. Vielmehr verhindert sie nur die Durchsetzung vertraglicher Ansprüche durch Gerichte des Einzelstaats, s. *Lemley*, 87 Cal. L. Rev. 111, 137 Fn. 108 (1999).

[2016] *Bodewig* in: Beier/Götting/Lehmann/Moufang (Hrsg.), S. 833, 842.

[2017] S. *Goldstein*, Copyright, § 15.2.1.2, S. 15:10 ff.; Baltimore Orioles v. Majore League Baseball Players Ass'n, 805 F.2d 663, 677 (7th Cir. 1986), cert. denied, 480 U.S. 941 (1987); Mayer v. Josiah Wedgwood & Sons, Ltd., 601 F.Supp. 1523, 1535 (1985); Computer Assocs. Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 716 (2d. Cir. 1992).

[2018] S. einerseits Architectronics, Inc. v. Control Systems, Inc., 935 F. Supp. 425, 439 (S.D.N.Y. 1996); Taquino v. Teledyne Monarch Rubber, 893 F.2d 1488, 1501 (5th Cir. 1990); Acorn Structures, Inc. v. Swantz, 846 F.2d 923, 926 (4th Cir. 1988); s. andererseits American Movie Classics Co. v. Turner Entertainment Co., 922 F.Supp. 926, 931f. (S.D.N.Y. 1996); Expediters International of Washington, Inc. v. Direct Line Cargo Management Services, Inc., 995 F.Supp. 468 (D.N.J. 1998); s.a. Wolff v. Institute for Elec. & Elecs. Eng'rs, Inc., 768 F. Supp. 66, 69 (S.D.N.Y. 1991) und Schrut v. News America Publishing, Inc., 123 Misc.2d 845, 846, 474 N.Y.S.2d 903, 904 (1984). Einen kurzen Überblick über den Streitstand geben *Mercer*, 30 Creighton L. Rev. 1287, 1335 (1997); *Madison*, 67 Fordham L. Rev. 1025, 1128 ff. (1998).

staatliche Recht nach Zweck und Wirkung, das heißt qualitativ von den Verwertungsrechten des Copyright Act unterscheidet.[2020]

Nach allgemeiner Meinung ist der Versuch des Gesetzgebers, durch die „preemption doctrine" das Verhältnis zwischen „copyright" und „contract" zu regeln, nur sehr unvollkommen geglückt.[2021] Im einzelnen ergeben sich viele Auslegungsprobleme. Die Gesetzgebungsgeschichte des 17 U.S.C. § 301 ist verworren und gibt für eine Auslegung nichts her.[2022] Eine allgemeine Aussage, welche Arten von Klauseln in Nutzungsverträgen wegen der „preemption doctrine" nicht wirksam sind, läßt sich daher regelmäßig nicht treffen, kommt es doch zu stark auf die Umstände des Einzelfalles – und das entscheidende Gericht – an.[2023]

[2019] Es geht um die Frage, ob unter „protected subject matter" der Anwendungs- oder der Regelungsbereich des Copyright Act zu verstehen ist. So ist umstritten, ob unter „protected subject matter" auch bloße Ideen und Fakten fallen. Wäre dies der Fall, so könnte auf einzelstaatlicher Ebene kein Schutz von Ideen oder Fakten etabliert werden. Die Frage wird von Gerichten uneinheitlich beantwortet, für eine *weite Anwendung* der „preemption doctrine" s. Financial Info., Inc. v. Moody's Investors Serv., Inc., 808 F2d 204, 208 (2d Cir. 1986); United States ex rel. Berge v. Trustees of Univ. of Alabama, 104 F.3d 1453, 1463 (4th Cir. 1997); National Basketball Ass'n v. Motorola, Inc., 105 F.3d 841, 849 (2d Cir. 1997); s. a. Baltimore Orioles, Inc. v. Major League Baseball Players Association, 805 F.2d 663, 676 (7th Cir. 1986); Alridge v. The Gap, Inc., 866 F.Supp. 312, 314 (N.D.Tex. 1994); Goldstein v. California, 412 U.S. 546, 559f., 93 S.Ct. 2303, 2311 (1973); *Mercer*, 30 Creighton L. Rev. 1287, 1332 (1997); *Grusd*, 10 Harvard J. L. & Tech. 353, 364 (1997). Für eine *enge Anwendung* s. Mayer v. Josiah Wedgwood & Sons, Ltd., 601 F.Supp. 1523, 1532 Fn. 16 (1985); Rand McNally & Co. v. Fleet Management Systems, 591 F. Supp. 726, 739 (N. D. Ill. 1983). Bromhall v. Rorvik, 478 F. Supp. 361, 367 (E.D. Pa. 1979); *McManis*, 87 Cal. L. Rev. 173, 178 f. (1999); wohl auch Smith v. Weinstein, 578 F.Supp. 1297 (1984) bezüglich Ideen. S. zum ganzen kurz *Götting/Fikentscher* in: Assmann/Bungert (Hrsg.), Kap. 7, Rdnr. 203.

[2020] Harper & Row Publishers, Inc. v. Nation Enterprises, 501 F. Supp. 848, 852 (S.D.N.Y. 1980), *aff'd in relevant part*, 723 F.2d 195 (2d Cir. 1983), *rev'd on other grounds*, 471 U.S. 539, 105 S.Ct. 2218 (1985); *Bodewig* in: Beier/Götting/Lehmann/Moufang (Hrsg.), S. 833, 842. Einen guten Überblick über das Case Law zur Frage der „preemption doctrine" im Schnittfeld von „copyright" und „contract" gibt Ballas v. Tedesco, 41 F.Supp.2d. 531, 536 Fn. 14 (1999).

[2021] *Lemley*, 87 Cal. L. Rev. 111, 115 (1999), meint plastisch: „[…] the law of preemption is a mess"; vgl. weiterhin *Bodewig* in: Beier/Götting/Lehmann/Moufang (Hrsg.), S. 833, 841.

[2022] *Abrams*, 11 Sup. Ct. Rev. 509, 545 (1983), meint: „Neither Congress nor the Copyright Office seems to have had any conception of what they were doing." Vgl. weiterhin *Lemley*, 87 Cal. L. Rev. 111, 140 Fn. 125 (1999); Architectronics, Inc. v. Control Systems, Inc. 935 F. Supp. 425, 440 f. (S.D.N.Y. 1996) m. w. N.; National Car Rental, Inc. v. Computer Associates International, Inc., 991 F.2d 426, 433 f. (8th Cir. 1993).

[2023] Vgl. Wrench LLC v. Taco Bell Corp., 51 F.Supp.2d 840, 852 (W.D.Mich. 1999); ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1455 (7th Cir. 1996).

b) ProCD, Inc. v. Zeidenberg

Das Verhältnis zwischen „copyright" und „contract" ist einer der zentralen Punkte in der ProCD-Entscheidung, die im Verlauf dieser Untersuchung schon an mehreren Stellen erwähnt wurde.[2024] Die Entscheidung ist auch für die vorliegende Frage im U.S.-amerikanischen Urheberrecht von grundlegender Bedeutung.[2025] In dem zugrundeliegenden Fall hatte ProCD die Käufer seines Produkts, das keinem urheberrechtlichen Schutz unterlag, in einem Schutzhüllenvertrag die Nutzung des Produkts nur für persönliche Zwecke erlaubt. Insbesondere wurde dem Nutzer verboten, das Produkt ganz oder teilweise in Netzwerkumgebungen anzubieten.[2026] In der Entscheidung ging es um die Frage, ob die Bedingungen des Nutzungsvertrags, der grundsätzlich dem einzelstaatlichem „contract law" unterfällt, unwirksam sind, weil die bundesrechtliche „preemption doctrine" des 17 U.S.C. § 301 eingreift.

Nach den dargestellten Voraussetzungen der „preemption doctrine"[2027] wäre dies der Fall, wenn einerseits der durch den Vertrag geschützte Gegenstand innerhalb der „protected subject matter of copyright" liegen würde, s. 17 U.S.C. § 301 (a). Dies bejahten das erst- und zweitinstanzliche Gericht.[2028] Andererseits müßten die vertraglich eingeräumten Rechte den ausschließlichen Verwertungsrechten des Urheberrechts gleichwertig sein, s. 17 U.S.C. § 301 (a). Während das erstinstanzliche Gericht diese Frage bejahte und damit den Nutzungsvertrag wegen eines Verstoßes gegen die „preemption doctrine" für unwirksam erklärte,[2029] entschied Judge *Easterbrook* in zweiter Instanz in entgegengesetzter

[2024] S. dazu oben Teil 2, B 3 a aa, Teil 3, A II 2 b bb, und Teil 3, A III 3 b aa.

[2025] *Madison*, 67 Fordham L. Rev. 1025, 1026 (1998) beginnt seine ausführliche Besprechung der Entscheidung mit der Feststellung: „ProCD, Inc. v. Zeidenberg has proved as intractable as the weather". Bezüglich der Frage der „preemption" wird die Entscheidung u. a. untersucht von *Mahajan*, 67 Fordham L. Rev. 3297 (1999); *Hill*, 31 Ind. L. Rev. 143 (1998); *Wang*, 15 J. Marshall J. Computer & Info. L. 439 (1997); *Covotta/Sergeef*, 13 Berkeley Tech.L.J. 35 (1998); *Baker*, 92 Nw. U. L. Rev. 379 (1997); *Mercer*, 30 Creighton L. Rev. 1287 (1997); *Grusd*, 10 Harv. J.L. & Tech. 353 (1997); *O'Rourke*, 12 Berkeley Tech. L.J. 53 (1997). In der deutschen Literatur findet sich Darstellungen bei *Kochinke/Günther*, CR 1997, 129, 134 f.; *Lejeune*, K&R 1999, 210, 212 f.; *Lejeune*, CR 2000, 201, 203 f. Weitere Literaturhinweise bei *Lemley*, 87 Cal. L. Rev. 111, 120 Fn. 20 (1999).

[2026] Eine ausführliche Schilderung des Sachverhalts findet sich oben Teil 3, A III 3 b aa.

[2027] Oben bei Fn. 2016 f.

[2028] ProCD, Inc. v. Zeidenberg, 908 F.Supp. 640, 656f. (W.D.Wiss. 1996); ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1453 (7th Cir. 1996).

[2029] Der Urheber wolle durch den Nutzungsvertrag genau jene Rechte vertraglich einräumen, die der „Copyright Act" dem Urheber gewähre, nämlich das Recht der Vervielfältigung und der Verbreitung; s. ProCD, Inc. v. Zeidenberg, 908 F.Supp. 640, 657 f. (W.D.Wiss. 1996).

Richtung.[2030] Vertraglich geschaffene Rechte seien mit einem urheberrechtlichen Verwertungsrecht nicht vergleichbar, da sie nur *inter partes* wirkten, während die Verwertungsrechte absolute Wirkung gegenüber jedermann entfalteten.[2031] Damit seien die vertraglich eingeräumten Rechte den urheberrechtlichen Verwertungsrechten nicht vergleichbar, die „preemption doctrine" nicht einschlägig und der Nutzungsvertrag wirksam.

In der U.S.-amerikanischen Literatur ist diese Argumentation weithin auf Ablehnung gestoßen. Dieser Kritik hat sich die vorliegende Untersuchung schon weiter oben angeschlossen:[2032] Überzieht ein Inhalteanbieter einen gesamten Markt mit einem vorformulierten, einheitlichen Nutzungsvertrag, so nähert sich dieser „relativ" wirkende Schutz durch Vertrag in seinen faktischen Auswirkungen dem absoluten Schutz durch das Urheberrecht an. Bis heute kennen die USA keinen gesetzlichen Schutz von Datenbanken. Könnte ein Inhalteanbieter diesen Datenbankschutz faktisch auf vertraglichem Wege erreichen, so würden die Wertungen mißachtet, die den Kongreß zur der Versagung des urheberrechtlichen Schutzes für Datenbanken veranlaßt haben.[2033] Durch die ProCD-Entscheidung wird die „sweat of the brow"-Doktrin, die der U.S. Supreme Court 1991 ausdrücklich aufgegeben hatte,[2034] faktisch wieder in Kraft gesetzt.[2035] Die überwiegende Literaturmeinung in den USA meint daher

[2030] Auch hinsichtlich der Frage der Wirksamkeit von „shrinkwrap licenses" hatte er die erstinstanzliche Entscheidung aufgehoben; s. oben Teil 2, B II 3 a aa.

[2031] ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1454 f. (7th Cir. 1996). *Easterbrook* meinte weiter, von diesem Grundsatz könne es zwar Ausnahmen geben, dies sei vorliegend aber nicht der Fall. Dazu kritisch *Minassian*, 45 UCLA L. Rev. 569, 601 f. (1997); *Nimmer/Brown/Frisching*, 87 Cal. L. Rev. 17, 53 ff. (1999); *Lemley*, 87 Cal. L. Rev. 111, 141 Fn. 129 (1999).

[2032] Oben Teil 3, A II 2 b bb. Es existieren aber auch Befürworter der Entscheidung, u. a. *O'Rourke*, 12 Berkeley Tech. L. J. 53 (1997); *Gomulkiewicz*, 13 Berkeley Tech. L. J. 891, 899 ff. (1998).

[2033] *Covotta/Sergeef*, 13 Berkeley Tech.L.J. 35, 41 f. (1998); *Minassian*, 45 UCLA L. Rev. 569, 592 (1997); so auch schon das erstinstanzliche Gericht in ProCD, Inc. v. Zeidenberg, 908 F.Supp. 640, 659 (W.D.Wiss. 1996).

[2034] S. oben Teil 3, A III 3 b aa.

[2035] *Karjala*, 22 U. Dayton L. Rev. 511, 539 (1997); *Minassian*, 45 UCLA L. Rev. 569, 593 ff. (1997); *Nimmer/Brown/Frischling*, 87 Cal. L. Rev. 17, 50 ff. (1999); a. A. *Wolfson*, 87 Cal. L. Rev. 79, 103, Fn. 61 (1999). Zwar mögen die Interessen der Datenbankhersteller an einem rechtlichen Investitionsschutz durchaus berechtigt sein. Es ist jedoch nicht Aufgabe eines Gerichts bei der Entscheidung eines Einzelfalles, sondern vielmehr Aufgabe des Gesetzgebers, die bestehenden Interessenkonflikte im Rahmen der politischen Willensbildung auszufechten und gegebenenfalls einen solchen Schutz gesetzlich zu verankern; ebenso *Karjala*, a. a. O., S. 541; *Grusd*, 10 Harvard J. L. & Tech. 353, 366 f. (1997); *O'Rourke*, 12 Berkeley Tech. L. J. 53, 87, 91 (1997). Siehe auch das Urteil des Supreme Court in Sachen Sony Corp. v. Universal City Studios, Inc. 464 U.S. 417, 429 (1984): „[…] it is Congress that has been assigned the task of defining the scope of the limited monopoloy that should be granted to authors or to inventors […]". A.A. *Madison*, 67 Fordham L. Rev. 1025, 1135 ff. (1998), der gerade

im vorliegenden Fall, daß die vertragliche Einräumung der Nutzungsrechte der gesetzlichen Einräumung der urheberrechtlichen Verwertungsrechte entspricht, so daß die „preemption doctrine" einschlägig und der Nutzungsvertrag unwirksam ist.[2036]

In der ProCD-Entscheidung ging es um die Frage, ob in einem Bereich, in dem der urheberrechtliche Schutz nicht greift, durch Nutzungsverträge ein urheberrechtsähnlicher Schutz geschaffen werden kann. Daneben gibt es Fälle, bei denen in einem Bereich, in dem der urheberrechtliche Schutz greift, in einem Nutzungsvertrag „nur" urheberrechtliche Schrankenbestimmungen („fair use doctrine" und ähnliches) abbedungen werden. Auch hier kann die „preemption doctrine" eingreifen und zu einer Unwirksamkeit der entsprechenden Vertragsklauseln führen.[2037] Das Verhältnis zwischen urheberrechtlichen Schrankenbestimmungen und Nutzungsverträgen wurde in den USA insbesondere in den späten 80er und frühen 90er Jahren hinsichtlich der Frage geführt, ob Schrankenbestimmungen in „shrinkwrap licenses" von Computersoftware abbedungen werden können.[2038]

c) Generelle Eignung der „Preemption Doctrine"

Insgesamt erscheint fraglich, ob die vorliegende Problematik – Verhältnis zwischen DRM-Systemen und urheberrechtlichen Grundsätzen – durch

auf die dezentrale richterliche Rechtsfindung des „common law" setzt. Dagegen jedoch *Mahajan*, 67 Fordham L. Rev. 3297, 3324 f. (1999).

[2036] Neben den dargestellten Kritikpunkten lassen sich noch weitere anführen. Zwar bezog sich die Berufungsinstanz in ProCD auf drei Entscheidungen anderer Berufungsgerichte, in denen jeweils die „preemption" von Verträgen verneint wurde. Diese Fälle sind jedoch nicht vergleichbar, da es sich dabei um Nutzungsverträge handelte, die individuell ausgehandelt worden waren. Dann stellt sich das Problem aber nicht, daß Inhalteanbieter mit standardisierten Nutzungsverträgen einen ganzen Markt abdecken können, *Karjala*, 22 U. Dayton L. Rev. 511, 537 (1997). Zu weiteren Unterschieden zwischen den Entscheidungen s. *Tolman*, 1998 BYU L.Rev. 303, 321 ff. (1998); *Karjala*, a. a. O., S. 537 f.; *Minassian*, 45 UCLA L. Rev. 569, 603 f. (1997); *Nimmer/Brown/Frischling*, 87 Cal. L. Rev. 17, 48 ff. (1999). Schließlich geht die zweitinstanzliche Entscheidung überhaupt nicht auf die Frage ein, ob der Nutzungsvertrag vielleicht wegen der erwähnten „Supremacy Clause" der Verfassung unwirksam sein könnte, s. *Nimmer/Brown/Frischling*, a. a. O., S. 46; *Lemley*, 87 Cal. L. Rev. 111, 143 (1999).

[2037] S. nur Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 269 f. (5th Cir. 1988). Tatsächlich ging es in dem Fall um die Wirksamkeit des damaligen „Louisiana Software License Enforcement Acts", der ein vertragliches Verbot des „Reverse Engineering" ausdrücklich zuließ. Auf dessen Grundlage wurde ein entsprechender Nutzungsvertrag abgeschlossen. Das Gericht erklärte die Bestimmung des Gesetzes und den darauf aufbauenden Nutzungsvertrag für unwirksam.

[2038] Dabei ging es einerseits um die Frage, ob das „Reverse Engineering" vertraglich untersagt werden kann, andererseits ging es um die Abdingbarkeit des 17 U.S.C. § 117. S. zum ganzen *Rice*, 53 U. Pitt. L. Rev. 543, 605 ff. (1992); *O'Rourke*, 45 Duke L. J. 479 ff. (1995); *Lemley*, 68 S. Cal. L. Rev. 1239, 1254 ff. (1995); *R. T. Nimmer*, § 11.12[4][b], S. 11–38 ff., § 11.16[4], S. 11–59 ff.

die „preemption doctrine“ befriedigend gelöst werden kann.[2039] Die „preemption doctrine“ ist auf Kompetenzprobleme innerhalb eines föderalen Staates zugeschnitten.[2040] Zur Lösung von Konflikten zwischen „copyright“ und „contract“ ist sie ein sehr grobes Mittel ohne jede Möglichkeit der Differenzierung im Einzelfall.[2041] Auch ist zu beachten, daß es im vorliegenden Zusammenhang um die Frage geht, ob die Vertragsfreiheit der Inhalteanbieter in DRM-Systemen wegen Interessen Dritter oder der Allgemeinheint eingeschränkt werden sollte. Auf diese Frage kann die „preemption doctrine“ keine Antwort geben. Sie bietet allenfalls eine rechtliche Konstruktion, mit der solche Interessen in Nutzungsverträgen Geltung erlangen können. Die „preemption doctrine“ setzt die normative Festlegung öffentlicher Interessen voraus, ohne selbst etwas zu deren Definition beizutragen.[2042] Im Bereich von DRM-Nutzungsverträgen ist im einzelnen unklar, welche Beschränkungen der Vertragsfreiheit notwendig und wünschenswert sind. Die „preemption doctrine“ könnte für die vorliegende Problematik nur dann wirklich weiterhelfen, wenn solche normativen Werte schon herausgarbeitet worden wären.[2043]

2. „Public Policy“-Bestimmung des UCITA

Im Rahmen des „Uniform Computer Information Transactions Act“ (UCITA)[2044] wurde ein Versuch unternommen, solche normativen Werte näher zu definieren.[2045] Das Verhältnis zwischen dem Modellgesetz UCITA, das dann in einzelstaatliches Recht transformiert wird, und dem bundesrechtlichen Urheberrecht war einer der größten Streitpunkte in der Entstehung des UCITA.[2046] Während der Entstehungsgeschichte standen sich zwei Lager gegenüber: Das eine Lager erhob die Vertragsfreiheit zur obersten Maxime. Gesetzliche Regelungen sollten so flexibel sein, daß sie

---

[2039] S. dazu *Lemley*, 87 Cal. L. Rev. 111, 144 ff. (1999); *Reichman/Franklin*, 147 U. Penn. L. Rev. 875, 920 ff. (1999).

[2040] *Reichman/Franklin*, 147 U. Penn. L. Rev. 875, 921 (1999).

[2041] *Lemley*, 87 Cal. L. Rev. 111, 145 (1999), schreibt daher: „Using preemption doctrine against contracts is something like swinging a sledgehammer at a gnat.“ *O'Rourke*, 45 Duke L. J. 479, 541 (1999), schlägt aus diesem Grund eine Anwendung des Kartellrechts vor, was *Lemley*, 87 Cal. L. Rev. 111, 145 Fn. 145 (1999) als ebenso unscharf kritisiert.

[2042] *Madison*, 67 Fordham L. Rev. 1025, 1131 f (1998); *Lemley*, 87 Cal. L. Rev. 111, 145f. (1999).

[2043] In den USA wird mitunter sogar bezweifelt, ob sich dem „Copyright Act“ solche normativen Wertentscheidungen entnehmen ließen; s. *Wolfson*, 87 Cal. L. Rev. 79, 110 (1999; *Madison*, 67 Fordham L. Rev. 1025, 1135 ff. (1998).

[2044] Allgemein dazu oben Teil 2, B II 3 a bb.

[2045] Daneben ist auch im Bereich des UCITA die „preemption doctrine“ des 17 U.S.C. § 301 (a) anwendbar, die als bundesrechtliche Regelung dem einzelstaatlichen UCITA vorgeht; s. a. § 105 (a) UCITA.

[2046] S. nur *Reichman/Franklin*, 147 U. Penn. L. Rev. 875 (1999); *Samuelson*, 13 Berkeley Tech. L. 809, 825 (1998). In der deutschen Literatur wird diese Frage von *Lejeune*, K&R 1999, 210, 212 f.; *ders.*, CR 2000, 201, 203 ff., behandelt.

den Vertragsparteien ermöglichen, durch Vertragsverhandlungen eine optimale Verteilung von Rechten zu erzielen. Das andere Lager betonte dagegen den Charakter des Urheberrechts als eines gerechten Ausgleichs zwischen den Interessen der Urheber und der Allgemeinheit, der durch Nutzungsverträge nicht unterlaufen werden dürfe.

Die ersten Entwürfe des damals unter dem Namen „Artikel 2B UCC" firmierenden Projekts aus dem Jahr 1995 verfolgten einen sehr liberalen Ansatz. Fragen der „federal preemption" wurden allenfalls am Rande behandelt. Wie in der Argumentation von Judge *Easterbrook* in der ProCD-Entscheidung[2047] sollten die Konsumenten weitgehend durch den Wettbewerb zwischen unterschiedlichen Anbietern, nicht durch rechtliche Bestimmungen geschützt werden. Ab Ende 1996 wurde von unterschiedlicher Seite gefordert, das Verhältnis des UCITA zum Immaterialgüterrecht genauer zu regeln und insbesondere die Vertragsfreiheit zu beschränken, wenn es um urheberrechtliche Grundsätze gehe. Zwei Jahre lang fanden heftige Diskussionen zu dieser Frage statt. Ende 1998 konnte man sich auf einen Kompromißtext einigen.[2048] Auch danach riß die Kritik jedoch nicht ab.[2049]

[2047] S. dazu oben Teil 3, B I 2 b aa und B I 2 b bb 1.

[2048] So sprach sich das „Policy Subcommitte" des „UCC 2B Drafting Committees" in einem Memorandum vom 4. 11. 1996 gegen eine Gesetzgebung aus, die Nutzungsverträge ermögliche, die dem Urheberrecht widersprächen, s. <http://www.2bguide.com/docs/polmem.html>. Das „American Law Institute" verabschiedete im Juni 1997 auf Vorschlag von *McManis* mit schwacher Mehrheit eine Resolution, daß Bedingungen in Massenlizenzverträgen unwirksam sein sollten, durch die urheberrechtliche Schrankenbestimmungen unterlaufen würden (sog. „*McManis* Motion" vom 9. 5. 1997, erhältlich unter <http://www.ali.org/ali/mcmanis.htm>). Die Softwareindustrie, Börsenbranche und einige Behörden reagierten auf diese Resolution mit einem Proteststurm, sollte doch das Gesetzgebungsprojekt ursprünglich die Flexibilität der Produzenten bei der Vertragsgestaltung erhöhen; s. dazu *Warlick*, 45 J. Copyright Soc'y U.S.A. 158, 165 f. (1997); *McManis*, 87 Cal. L. Rev. 173, 176 (1999); *Wolfson*, 87 Cal. L. Rev. 79, 80 f. (1999); *Lejeune*, K&R 1999, 210, 213; *Lejeune*, CR 2000, 201, 204. Die NCCUSL lehnte die „*McManis* Motion" im Juli 1997 ab und trat dafür ein, Art. 2B UCC solle bezüglich des Verhältnisses zum Urheberrecht eine neutrale Position einnehmen, s. <http://www.2bguide.com/nmtgrpt.html> und *Wolfson*, 87 Cal. L. Rev. 79, 81 (1999). Die Kritik ließ jedoch nicht nach. Bei einer großen Konferenz an der University of California at Berkeley im April 1998 wurde von akademischer Seite heftige Kritik am Verhältnis des UCC 2B zum Urheberrecht geübt; s. u. a. *Lemley*, 87 Cal. L. Rev. 111, 136 (1999); *Reichman/Franklin*, 147 U. Penn. L. Rev. 875 (1999); *Litman*, 13 Berkeley Tech. L. J. 931, 933 (1998). Auf dieser Konferenz schlugen *Reichman* und *Franklin* die Ergänzung des UCC 2B um eine Vorschrift vor, nach der Klauseln in „mass-market licenses" unwirksam sind, wenn sie bestimmten öffentlichen Interessen („education, science, research, technological innovation, freedom of speech, and the preservation of competition") entgegenlaufen; s. *Reichman/Franklin*, a. a. O., S. 930 ff.. In der Folge wurde wiederholt gefordert, das gesamte Gesetzgebungsprojekt aufzuschieben, s. u. a. den von 50 Jura-Professoren unterzeichneten Brief an die NCCUSL und das ALI vom 17. 11. 1998, erhältlich unter <http://www.2bguide.com/docs/1198ml.html>. Im Juli 1998 schlug dann *Perlman*, der „Commissioner on Uniform State Laws" des Bundesstaates Nebraska, eine Vorschrift vor, die sich eng an

Heute findet sich die entsprechende Bestimmung in § 105 (b) UCITA. Danach sind Bestimmungen in Verträgen[2050] unwirksam, wenn sie gegen eine „fundamental public policy" verstoßen. Eine Definition dieser „public policies" findet sich im UCITA nicht. Sie können sich nach U.S.-amerikanischer Rechtslage aus dem Verfassungsrecht und einzelnen Gesetzen sowohl des Bundes als auch der Bundesstaaten ergeben.[2051] Die „Official Comments" zum UCITA erwähnen als „public policies" „innovation, competition and free expression" sowie „fair comment and fair use"[2052] und erläutern diese Begriffe näher.[2053] Danach sollen beispiels-

den Vorschlag von *Reichman* und *Franklin* anlehnte (sog. „Public Policy" oder „*Perlman* Motion"); s. *Brennan*, 36 Hous. L. Rev. 61, 63 f. (1999); *McManis*, a.a.O., S. 188; abgedruckt im Anschluß an § 205 des *UCC 2B Entwurf, 1. 8. 1998*, S. 48. Der tendenziell industriefreundliche „Chair" des Gesetzgebungsprojekts, *Ring*, und der ähnlich orientierte „Reporter" *R. T. Nimmer* schlugen dagegen eine tautologische Formulierung vor („A contract term that violates a fundamental public policy is unenforceable to the extent that the term is invalid under that policy"; ebenfalls in dem erwähnten *UCC 2B Entwurf vom 1. 8. 1998* abgedruckt). Nach langwierigen Diskussionen und umfangreichem Lobbyismus entschied sich das „Drafting Committee" für einen Kompromißtext, der sich ab Dezember 1998 nur noch in kleineren Einzelheiten veränderte. Das „American Law Institute" wollte diesen Kompromißtext nicht mittragen und beschloß aus diesem und anderen Gründen, den Entwurf des UCC 2B nicht mehr weiter zu unterstützen. Daraufhin beschloß die NCCUSL, das Projekt als eigenständiges Modellgesetz unter dem Namen UCITA weiterzuverfolgen; s. dazu auch oben Teil 2, B II 3 a bb 1.

[2049] S. nur *Reichman/Franklin*, 147 U. Penn. L. Rev. 875, 963 ff. (1999). Zustimmung findet die Fassung bei *Brennan*, 36 Hous. L. Rev. 61, 64 (1999). *Gomulkiewicz*, 13 Berkeley Tech. L. J. 891, 902 Fn. 60 (1998), meint, es handele sich um ein Problem, das der Bundesgesetzgeber und nicht der Landesgesetzgeber im Rahmen des UCITA lösen müsse; s. a. *Wolfson*, 87 Cal. L. Rev. 79, 97 (1999), kritisch dazu *Nimmer/Brown/Frischling*, 87 Cal. L. Rev. 17, 74 f. (1999); *McManis*, 87 Cal. L. Rev. 173, 179 ff. (1999).

[2050] Auch „mass-market licenses", s. § 209 (a) (1) UCITA.

[2051] 16A Am. Jur. 2d Constitutional Law § 192 m.w.N.; *Brennan*, 36 Hous. L. Rev. 61, 64 ff. (1999) m.w.N. Es ist Aufgabe des Gesetzgebers und nicht der Gerichte, solche „public policies" zu definieren, s. 16A Am. Jur. 2d Constitutional Law § 192; Baker v. United States, 27 F. 2d 863, 875 (1st Cir. 1928); Muschany v. United States, 324 U.S. 49, 66 (1945), jeweils m.w.N. Die „public policies" können auch zwischen den Bundesstaaten differieren, Lane v. Sumner County, 298 S.W.2d 708, 709 (Tenn. 1957). Die könnte der Intention des UCITA – nämlich ein einheitliches Recht in allen 50 Bundesstaaten zu schaffen – zuwiderlaufen, *Brennan*, 36 Hous. L. Rev. 61, 65 f. (1999); *O'Rourke*, 14 Berkeley Tech. L. J. 635, 650 (1999); *Garon*, 17 Cardozo Arts & Ent. L. J. 491, 560 (1999).

[2052] Official Comment Nr. 1 und 3 zu § 105 UCITA, *UCITA*, S. 64 f.

[2053] Official Comment Nr. 3 zu § 105 UCITA, *UCITA*, S. 65: „Innovation policy recognizes the need for a balance between protecting property interests in information to encourage its creation and the importance of a rich public domain upon which most innovation ultimately depends. Competition policy prevents unreasonable restraints on publicly available information in order to protect competition. Rights of free expression may include the right of persons to comment, whether positively or negatively, on the character or quality of information in the marketplace. Free expression and the public interest in supporting public domain use of published information also underlie

weise Vertragsklauseln unwirksam sein, die das Zitieren kleiner Werkausschnitte, das „Reverse Engineering" von Software oder die Erstellung von Sicherungskopien untersagen.[2054]

Insgesamt ermöglicht der UCITA dem Inhalteanbieter in sehr weitem Umfang, die Bedingungen von Nutzungsverträgen in DRM-Systemen einseitig festzulegen.[2055] Manche Autoren meinen gar, der UCITA sei eine Einladung an Unternehmen, durch Verträge ihr eigenes Urheberrecht zusammenzuschustern.[2056] Der Versuch des UCITA, in der Frage des Verhältnisses zum Urheberrecht eine neutrale Position einzunehmen, war von vornherein zum Scheitern verurteilt.[2057] Derzeit ist unklar, welche Bedeutung der „public policy"-Bestimmung in der Praxis zukommen wird. Gerichtsentscheidungen liegen noch nicht vor. Das Modellgesetz wurde bisher nur zögerlich in einzelnen Bundesstaaten umgesetzt. Klar scheint jedoch, daß das Verhältnis zwischen „copyright" und „contract" auch im Rahmen des UCITA nicht abschließend und klar gelöst wurde. Man einigte sich vielmehr auf einen Formelkompromiß. Im Einzelfall ist eine umfassende Abwägung der beteiligten Interessen erforderlich, eine abstrakte Aussage ist a priori nicht möglich.[2058]

3. Sonstige Ansätze

Neben der „preemption doctrine" in 17 U.S.C. § 301 (a) und der „public policy"-Bestimmung des UCITA besteht eine Vielzahl weiterer Ansätze, durch die das Verhältnis zwischen „copyright" und „contract" geklärt oder zumindest praktikabler ausgestaltet werden soll. So wurde über eine

---

fair use as a restraint on information property rights. Fair use doctrine is established by Congress in the Copyright Act. Its application and the policy of fair use is one for consideration and determination there. However, to the extent that Congress has established policies on fair use, those can taken into consideration under this section." Zur Auslegung dieser Begriffe s. auch die ausführliche Untersuchung von *Brennan*, 36 Hous. L. Rev. 61, 75 ff. (1999).

[2054] Official Comment Nr. 3 zu § 105 UCITA, *UCITA*, S. 66. Bezüglich des „Reverse Engineering" gilt das nur unter bestimmten Voraussetzungen, *ebda.*, S. 67. In der Literatur wird als weiterer Fall einer „public policy" der Schutz der Privatsphäre genannt, s. *Brennan*, 36 Hous. L. Rev. 61, 75 (1999).

[2055] Vgl. *Reichman/Franklin*, 147 U. Penn. L. Rev. 875, 903 (1999).

[2056] S. a. *Reichman/Franklin*, 147 U. Penn. L. Rev. 875, 878, 911 ff. (1999).

[2057] Nach der ProCD-Entscheidung bedeutet eine „neutrale Position" faktisch, daß eine umfassende Vertragsfreiheit geduldet wird; s. *Warlick*, 45 J. Copyright Soc'y U.S.A. 158, 172 (1997); *Nimmer/Brown/Frischling*, 87 Cal. L. Rev. 17, 71 (1999); *Reichman/Franklin, 147* U. Penn. L. Rev. 875, 911 (1999); *Garon*, 17 Cardozo Arts & Ent. L. J. 491, 569 (1999).

[2058] Ausführlich dazu *Brennan*, 36 Hous. L. Rev. 61, 75 ff., 92 ff., 107 (1999). *Brennan* begrüßt die Regelung des § 105 (b) UCITA allerdings, da sie die notwendige Freiheit für eine Einzelfallgerechtigtkeit durch den Richter des „common law" lasse, *ebda.*, S. 107.

gesetzliche Reform der „preemption doctrine" nachgedacht.[2059] Auch wird darauf hingewiesen, daß neben der „preemption doctrine" noch andere Rechtsinstitute das Verhältnis zwischen „copyright" und „contract" beeinflussen können.[2060] So könnte die „doctrine of copyright misuse" weiterhelfen, die dem Schnittfeld zwischen Urheber- und Kartellrecht entstammt und in den letzten Jahren sowohl im Case Law als auch in der Urheberrechtsliteratur zunehmend an Bedeutung gewinnt. Danach können Vertragsbedingungen unwirksam sein, durch die der Inhaber des Urheberrechts versucht, seine Rechtsstellung in zeitlicher und/oder inhaltlicher Sicht über die gesetzlich festgelegten Grenzen des Urheberrechts hinaus auszudehnen.[2061] Auch außerhalb des UCITA können Vertragsklauseln wegen eines Verstoßes gegen die „public policy doctrine", die dem Common Law entstammt,[2062] unwirksam sein.[2063] Im unscharfen Grenzbereich zwischen „copyright" und „contract" wird diese allgemeine Inhaltskontrolle jedoch oftmals nicht weiterhelfen.[2064] Im Verhältnis zwischen „copyright" und „contract" werden mitunter auch Grundsätze

---

[2059] Eine der Gesetzesvorlagen, die zur Umsetzung der WIPO-Verträge von 1996 in den U.S.-Kongreß eingebracht wurden, wollte 17 U.S.C. § 301 (a) wie folgt ergänzen: „When a work is distributed to the public subject to non-negotiable license terms, such terms shall not be enforceable under the common law or statutes of any state to the extent that they –

1. limit the reproduction, adaptation, distribution, performance, or display, by means of transmission or otherwise, of material that is uncopyrightable under section 102 (b) or otherwise; or
2. abrogate or restrict the limitations on exclusive rights specified in sections 107 through 114 and sections 117 and 118 of this title" (Numerierung wurde vom Verfasser zur Übersichtlichkeit hinzugefügt).

Dieser sog. „Digital Era Copyright Enhancement Act" – auch bekannt als „*Campbell-Boucher* Bill", H.R. 3048, 105th Cong. (1997), erhältlich unter <http://thomas.loc.gov>; s. dazu auch *Nimmer/Brown/Frischling*, 87 Cal. L. Rev. 17, 72 ff. (1999) – konnte sich jedoch im Repräsentantenhaus nicht durchsetzen.

[2060] Siehe dazu *Lemley*, 87 Cal. L. Rev. 111, 115 f. (1999).

[2061] In der ersten Entscheidung, in der ein U.S.-amerikanisches Berufungsgericht im Bereich des Urheberrechts die „misuse doctrine" anerkannte, lizenzierte ein Softwarehersteller seine Software nur unter der Bedingung, daß der Lizenznehmer in den nächsten 99 Jahren keine ähnliche Software herstellen werde; s. Lasercomb America v. Reynolds, 911 F.2d 970 (4th Cir. 1990); s. zum ganzen *Frischmann/Moylan*, 15 Berkeley Tech. L. J. 865 ff. (2000); *Lemley*, 87 Cal. L. Rev. 111, 151 ff. (1999).

[2062] S. dazu allgemein Restatement (Second) of Contracts, Chapter 8 introductory note, § 178; *Farnsworth*, Farnsworth on Contracts, Band 2, §§ 5.1–5.9, S. 1 ff.; *Reimann*, S. 42 f.

[2063] S. dazu *Lemley*, 87 Cal. L. Rev. 111, 158 ff., 163 ff. (1999).

[2064] *Reichman/Franklin*, 147 U. Penn. L. Rev. 875, 925 ff. (1999). Auch der Versuch, die vorliegenden Probleme über das Institut der Sittenwidrigkeit („unconscionability") – einem Unterfall der „public policy doctrine" – zu lösen, wird regelmäßig nicht weiterhelfen, *Lemley*, 87 Cal. L. Rev. 111, 151 (1999); *O'Rourke*, 12 Berkeley Tech. L. J. 53, 89 (1997); *Reichman/Franklin*, a. a. O., S. 928; s. a. *Lemley*, 68 S.Cal. L. Rev. 1239, 1254 f. (1995).

des Sachenrechts herangezogen, die die Möglichkeit von dinglichen Verfügungs- und Nutzungsbeschränkungen betreffen.[2065]

IV. Zusammenfassung

Insgesamt ist das Verhältnis zwischen Urheberrecht und Nutzungsverträgen ungeklärt. Im europäischen und deutschen Recht bestehen nur vereinzelt gesetzliche Regelungen zu der Frage, ob urheberrechtliche Schrankenbestimmungen vertraglich abbedungen werden können. In den USA hat das Verhältnis zwischen „copyright" und „contract" in den letzten Jahren sehr viel mehr Aufsehen erregt. Auch dort konnten bis heute aber keine scharfen Abgrenzungskriterien aufgestellt werden. Gerichtsentscheidungen zu diesen Fragen existieren sowohl in Deutschland als auch in den USA. Eine einheitliche Entscheidungspraxis läßt sich freilich noch nicht erkennen, handelt es sich doch um recht vereinzelte Entscheidungen.

C. Beschränkung von Technologie-Lizenzverträgen

DRM-Technologie-Lizenzverträge können mittelbar Auswirkungen darauf haben, ob die Nutzer eines DRM-Systems von urheberrechtlichen Schrankenbestimmungen Gebrauch machen können.[2066] Es ist zu erwägen, ob auch die Ausgestaltung von Technologie-Lizenzverträgen unter urheberrechtlichen Gesichtspunkten zu beschränken ist. Angesichts der Tatsache, daß die Bedeutung von Technologie-Lizenzverträgen in DRM-Systemen bisher fast gar nicht beachtet wurde, ist nicht verwunderlich, daß Äußerungen und gesetzliche Regelungen zum Verhältnis von Technologie-Lizenzverträgen zu urheberrechtlichen Schrankenbestimmungen

[2065] Softwarelizenzverträge enthalten Klauseln, nach denen die Software nicht an Dritte weiterveräußert werden darf. Auch finden sich in Nutzungsverträgen Klauseln, die die Nutzungsmöglichkeit des digitalen Inhalts in inhaltlicher, zeitlicher, räumlicher oder personeller Hinsicht beschränken. Da die Beschränkungen an den digitalen Inhalt gekoppelt sind, ähneln sie Verfügungs- und Nutzungsbeschränkungen im Sachenrecht („covenants running with the land"). Grundsätzlich steht das Common Law Verfügungs- und Nutzungsbeschränkungen ablehnend gegenüber, 61 Am. Jur. 2d § 100 (Perpetuities and Restraints on Alienation); Dr. Miles Medical Co. v. John D. Park & Sons Co., 220 U.S. 373, 404 (1911); *Hemnes*, 71 Denv. U. L. Rev. 577, 579 (1994); *Merges*, 12 Berkeley Tech. L. J. 115, 121 (1997); *Reimann*, S. 142. Von diesem Grundsatz gibt es jedoch viele Ausnahmen, s. dazu 61 Am. Jur. 2d § 100 ff. (Perpetuities and Restraints on Alienation). S. zu dieser Parallele *Hemnes*, a. a. O., für Softwarelizenzverträge; *Lemley*, 87 Cal. L. Rev. 111, 121 (1999) im Bereich des UCITA; *Merges*, 12 Berkeley Tech. L. J. 115, 121 ff. (1997); *Radin/Wagner*, 73 Chi.-Kent L. Rev. 1295, 1312 f. (1998); *Fisher*, 73 Chi.-Kent L. Rev. 1203, 1211 (1998).

[2066] S. dazu oben bei Fn. 1940 ff.

fast vollständig fehlen.[2067] Einzig die Federal Communications Commission äußert sich in ihrer Beurteilung eines Technologie-Lizenzvertrags im Pay-TV-Bereich zu dieser Frage.[2068] Die FCC merkt an, durch Technologie-Lizenzverträge könnten Inhalteanbieter sicherstellen, daß DRM-Endgeräte ihre Metadaten beachten würden und damit – je nach Metadaten – unbegrenzt viele, eine oder gar keine Kopie geschützter Inhalte erstellen würden.[2069] Zwar hat sich die FCC bei der Beurteilung einzelner Bestimmungen der untersuchten Technologie-Lizenz sehr zurückgehalten. Dennoch deutete sie an, daß Technologie-Lizenzverträge nicht dazu führen dürfen, daß die Möglichkeit von Nutzern behindert oder beschränkt wird, von urheberrechtlichen Schrankenbestimmungen Gebrauch zu machen.[2070]

[2067] Dagegen finden sich durchaus Vorschriften, die die ordnungspolitischen und kartellrechtlichen Auswirkungen von DRM-Technologie-Lizenzverträge betreffen, s. Art. 4 lit. d der europäischen Fernsehsignalübertragungs-Richtlinie, in Deutschland umgesetzt durch § 9 Fernsehsignalübertragungs-Gesetz. Derzeit wird an einer Reform dieser europäischen Regelung gearbeitet, s. Anhang I Teil I lit. c des Vorschlags der Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung, KOM (2000) 384 vom 12. 7. 2000, S. 23. Der Vorschlag wurde am 1. 3. 2001 zur ersten Lesung im Europäischen Parlament behandelt. S. zu dieser Reform der europäischen Kommunikationsregelungen im Überblick *Beese/Merkt*, MMR 2000, 532 ff.; *Schulz/Leopoldt*, K&R 2000, 439 ff.

[2068] Zu diesem „POD Host Interface License Agreement" und der FCC-Untersuchung s. oben Teil 2, C II 1.

[2069] *Federal Communications Commission*, 15 FCC Rcd. 18,199 (September 18, 2000), Abs. 15: „Through the use of contractual licensing requiring consumer electronic manufacturers to install certain copy protection technology in their equipment in exchange for access to desirable digital content, copyright holders will be able to control, through the insertion of coded instructions in the digital stream, whether such equipment will allow consumers to make one copy, unlimited copies, or prohibit copying altogether of digital content received from an MVPD [multichannel video programming distributor, z. B. ein Kabelnetzbetreiber]."

[2070] Einerseits schreibt die *Federal Communications Commission*, 15 FCC Rcd. 18,199 (September 18, 2000), Abs. 29: „[…] it is suggested that the host device manufacturer could be precluded from facilitating even that degree of copying that comes within copyright law ‚fair use' copying allowances. […] At this time, we take no position on the specific terms contained in the draft DFAST license." Andererseits meint sie in Fn. 70: „We note that nothing in our decision today is intended to alter ‚fair use' unter copyright law." Noch deutlicher das „Seperate Statement" von Commissioner *Gloria Tristani*, das im Anhang zu der FCC-Entscheidung abgedruckt ist: „[…] our ruling in no way authorizes any attempt by providers of services to utilize this ruling to combine technology with copy protection in a manner that interferes with, or unreasonably restricts, a consumer's fair use of copy-protected material."

D. Beschränkung technischer DRM-Komponenten

Technische Schutzmaßnahmen bieten dem Inhalteanbieter die Möglichkeit, urheberrechtliche Grundsätze – insbesondere urheberrechtliche Schrankenbestimmungen – zu umgehen.[2071] Es besteht ein Bedürfnis, den technischen Schutz in DRM-Systemen wegen entgegenstehender Interessen Dritter oder der Allgemeinheit rechtlich zu beschränken. Im folgenden soll dargestellt werden, welche Möglichkeiten dem Gesetzgeber dafür grundsätzlich zur Verfügung stehen (dazu unten I). Danach wird untersucht, wie die Gesetzgeber und die Rechtsprechung in Europa, Deutschland und den USA tatsächlich reagiert haben (dazu unten II).

I. Grundsätzliche Reaktionsmöglichkeiten des Rechts

Will der Gesetzgeber technische Schutzmaßnahmen in ihren urheberrechtlichen Auswirkungen begrenzen, so stehen ihm dafür mehrere Regulierungsoptionen zur Verfügung. Einerseits kann er die Rahmenbedingungen von DRM-Systemen und Endgeräten beeinflussen und dadurch einen Wettbewerb zwischen unterschiedlichen DRM-Systemen fördern (dazu unten 1). Andererseits kann er versuchen, unmittelbarer die Ausgestaltung einzelner technischer Schutzmaßnahmen nach seinen Wertvorstellungen zu beeinflussen (dazu unten 2).

1. Beeinflussung von Rahmenbedingungen

Wie oben dargestellt wurde, könnte ein Wettbewerb zwischen mehreren DRM-Systemen mit unterschiedlichem Schutzniveau dazu führen, daß sich technische Schutzmaßnahmen, die einseitig nur die Interessen der Inhalteanbieter wahren, am Markt nicht durchsetzen können.[2072] Ein solcher Wettbewerb kann jedoch an Netzwerkeffekten und Lock-In-Effekten scheitern, die dazu führen, daß sich am Markt ein einziges DRM-System etabliert.[2073] Konkurrierende DRM-Systeme, die mit dem marktbeherrschenden DRM-System nicht kompatibel sind, werden gegen den Marktbeherrscher keinen Erfolg haben. In diesem Umfeld könnte der Gesetzgeber eine Kompatibilität oder zumindest Interoperabilität zwischen verschiedenen DRM-Systemen vorschreiben. Dadurch würden die Netzwerk- und Lock-In-Effekte gemindert: Sind in einem von Netzwerkeffekten geprägten Markt die Produkte der Wettbewerber untereinander kompatibel, so können die Konsumenten zwischen den angebotenen Pro-

[2071] S. dazu oben Teil 3, B II 3 a.
[2072] S. dazu oben Teil 3, B I 2 b aa.
[2073] Zu Netzwerkeffekten s. oben Teil 3, B I 2 b cc 2, zu Lock-In-Effekten s. oben Teil 3, B I 2 b cc 3.

dukten wählen. Dann erscheint auch ein Wettbewerb zwischen unterschiedlichen Anbietern möglich.[2074]

Ein solches Vorgehen des Gesetzgebers existiert zwar nicht im urheberrechtlichen Bereich. Diese Regulierungsoption wird jedoch im Pay-TV-Bereich eingesetzt, wenn auch das Regulierungsziel dort ein etwas anderes ist.[2075] So enthält die europäische Fernsehsignalübertragungs-Richtlinie[2076] in Art. 3 und 4 Vorschriften, die es erlauben sollen, daß in einer Set-Top-Box eines Fernsehers mehrere Zugangsberechtigungssysteme parallel betrieben werden können.[2077] In Deutschland finden sich entsprechende Vorschriften in §§ 5 ff. Fernsehsignalübertragungs-Gesetz[2078] sowie in § 53 Abs. 1 Rundfunk-Staatsvertrag und § 13 der dazugehörigen Satzung nach § 53 Abs. 7 Rundfunk-Staatsvertrag.[2079] Durch solche Maßnahmen kann der Gesetzgeber erreichen, daß ein DRM-Endgerät Inhalte unterschiedlicher DRM-Systeme verarbeiten kann, so daß ein Technologie-Wettbewerb zwischen den DRM-Systemen möglich wird.

[2074] *Shapiro/Varian*, S. 186; *Lemley/McGowan*, 86 Cal. L. Rev. 479, 516, 599 f. (1998); *Lemley*, 28 Conn. L. Rev. 1041, 1060 (1996). Aus Sicht eines Unternehmens, das in einem Markt mit starken Netzwerkeffekten tätig ist, kann ein offener Standard, der die Entwicklung konkurrierender Produkte für den Netzwerkmarkt erlaubt, große Nachteile haben. Dies hängt aber von den Einzelumständen ab, u. a. vom Marktanteil und der Einschätzung der Marktentwicklung durch das Unternehmen. Mitunter ist es für das Unternehmen auch erfolgversprechender, sich für offene Standards einzusetzen. S. zum ganzen *Shapiro/Varian*, S. 196 ff.; *Shy*, S. 31, 35 f., 61, 65; *Gröhn*, S. 31 ff.; *Katz/Shapiro*, 75 Am. Econ. Rev. 424, 434 ff. (1985); *dies.*, 8 (2) J. Econ. Persp. 93, 111 (1994); *Monopolkommission*, IX. Hauptgutachten, Tz. 850.

[2075] Dort ist es vorrangiges Ziel, durch eine Zugangsoffenheit auf allen Ebenen der Programmbereitstellung einen funktionsfähigen Veranstalterwettbewerb auf der Programmebene zu erreichen („Gatekeeper"-Problematik), *Monopolkommission*, XII. Hauptgutachten, Tz. 541 ff.; *dies.*, XIII. Hauptgutachten, Tz. 622; *Holznagel*, MMR 2000, 480, 483; *Thierfelder*, S. 120 f. Eine Marktspaltung in unterschiedliche inkompatible Systeme soll verhindert werden; s. dazu *Monopolkommission*, XI. Hauptgutachten, Tz. 749 ff.; *Thierfelder*, S. 121.

[2076] Richtlinie 95/47/EG des Europäischen Parlaments und des Rates vom 24. 10. 1995 über die Anwendung von Normen für die Übertragung von Fernsehsignalen, ABl. EG Nr. L 281 vom 23. 11. 1995, S. 51 ff.

[2077] Die Einzelheiten sind komplex und hängen mit der technischen Ausgestaltung der „conditional access"-Systeme zusammen; s. zu den technischen Grundlagen Teil 1, D II 2. Zur anstehenden Reform der Regelungen s. oben Fn. 2067.

[2078] Gesetz über die Anwendung von Normen für die Übertragung von Fernsehsignalen, BGBl. I vom 14. 11. 1997, S. 2710. S. dazu *Thierfelder*, S. 126 f.; *Ladeur*, ZUM 1998, 261 ff.

[2079] Satzung aller Landemedienanstalten über die Zugangsfreiheit zu digitalen Diensten gemäß § 53 Abs. 7 Rundfunkstaatsvertrag vom 26. 6. 2000, erhältlich unter <http://www.artikel5.de/gesetze/digizu.html>. Zu § 53 RfStV und der Satzung s. *Monopolkommission*, XII. Hauptgutachten, Tz. 545 f.; *dies.*, XIII. Hauptgutachten, Tz. 622; *Holznagel*, MMR 2000, 480, 483 ff.; *Thierfelder*, S. 121 ff; *Beucher/Leyendecker/von Rosenberg*, § 53 RfStV.

2. Beeinflussung technischer Schutzmaßnahmen

Neben dieser Beeinflussung von Rahmenbedingungen kann der Gesetzgeber auch versuchen, die Ausgestaltung technischer Schutzmaßnahmen in DRM-Systemen unmittelbarer nach seinen Wertvorstellungen zu beeinflussen. Dafür bieten sich vier Vorgehensweisen an, die im folgenden dargestellt werden.

a) Direkte Regulierung technischer Schutzmaßnahmen

Der Gesetzgeber könnte auf die Ausgestaltung einzelner technischer Schutzmechanismen unmittelbar regulierend einwirken. So könnte die Verwendung von technischen Schutzmaßnahmen verboten werden, die urheberrechtliche Schrankenbestimmungen nicht beachten.[2080] Durch solche Regelungen würde der Gesetzgeber faktisch vorschreiben, wie technische Schutzmaßnahmen im einzelnen auszusehen haben.

Jedoch würde eine pauschale Regelung, daß solche technische Schutzmaßnahmen verboten sind, durch die eine der urheberrechtlichen Schrankenbestimmungen unterlaufen wird, nicht genügen: Aus technischer Sicht ist es praktisch unmöglich, die diffizilen rechtlichen Einzelheiten herkömmlicher urheberrechtlicher Schrankenbestimmungen in einer technischen Schutzmaßmahme vollständig zu berücksichtigen.[2081] Daher wird es bei dieser Regulierungsoption in Einzelfällen vorkommen, daß das DRM-System die Nutzung verweigert, obwohl eine bestimmte Schrankenbestimmung eingreift.[2082] Auch wenn dieser Regulierungsoption damit faktische Grenzen gesetzt sind, kann sie hilfreich sein. So sind Zwischenstufen denkbar, in denen gesetzlich vorgeschrieben wird, daß technische Schutzmaßnahmen zumindest eine Vielzahl von Nutzungen erlauben müssen, die traditionell unter urheberrechtliche Schrankenbestimmungen fallen.[2083]

[2080] *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 198; *Koelman*, EIPR 2000, 272, 279; *Fisher*, 73 Chi.-Kent L. Rev. 1203, 1254 (1998); *Burk/Cohen*, S. 12, die diesen Ansatz „coding for fair use" nennen.

[2081] *Sander*, S. 11.

[2082] Dieses Problem stellt sich in verstärktem Maße im U.S.-amerikanischen Urheberrecht, wo die „fair use"-Doktrin reichlich konturenlos ist; s. dazu *Burk/Cohen*, S. 13: „Building the range of possible outcomes into computer code would require both a bewildering degree of complexity and an impossible level of prescience. There is currently no good algorithm that is capable of producing such an analysis, meaning that (at least for now) there is no feasible way to build rights management code that approximates the results of judicial determinations."

[2083] S. dazu *Burk/Cohen*, S. 13 ff., die in diesem Zusammenhang den „Audio Home Recording Act" erwähnen, der die Verwendung von SCMS in DAT-Geräten vorschreibt, das zumindest die Erstellung einer digitalen Kopie erlaubt. S. dazu unten Teil 4, D II 1.

b) Umfassender Schutz mit allgemeinen Gegenansprüchen der Nutzer

Ein anderer Ansatz plädiert dafür, technische Schutzmaßnahmen und deren rechtlichen Umgehungsschutz grundsätzlich nicht zu beschränken. Dies sei aus Gründen des effektiven Rechtsschutzes geboten. In vielen Fällen habe der Nutzer jedoch einen rechtlichen Anspruch auf Ausnutzung der urheberrechtlichen Schrankenbestimmungen, den er gerichtlich einklagen könne. Ein solcher Anspruch könne sich aus einem Nutzungsvertrag, aus gesetzlichen Gewährleistungsregeln oder auch den urheberrechtlichen Schrankenbestimmungen selbst ergeben.[2084] So seien vertragsfeste Schranken in Art. 5 und 6 der europäischen Computerprogrammrichtlinie stets mit einem Nutzungsvertrag verbunden. Verhindere eine technische Schutzmaßnahme die Ausübung einer Schrankenbestimmung, so liege darin ein Verstoß gegen die Bedingungen des Nutzungsvertrags. Der Nutzer müsse dann seine vertraglichen Befugnisse über den Rechtsweg einklagen.[2085] Dies gelte nicht nur für urheberrechtliche Schrankenbestimmungen, sondern auch für Beschränkungen technischer Schutzmaßnahmen aus anderen Bereichen wie dem Kartellrecht oder dem Verbraucherschutzrecht.[2086] Bei Vorliegen eines solchen Anspruches könne der Nutzer gegen zu weitgehende Schutzmaßnahmen rechtlich vorgehen. Der Nutzer werde bezüglich seiner Interessen auf den Rechtsweg verwiesen.

Auch dieser Ansatz scheint problematisch. Angesichts der rechtsökonomischen und rechtlichen Analysen der vorliegenden Arbeit erscheint schon fraglich, ob ein unbeschränkter rechtlicher Umgehungsschutz „aus Gründen des effektiven Rechtsschutzes" tatsächlich geboten erscheint.[2087] Technische Schutzmaßnahmen stellen den Rechteinhabern ein „self-executing law" mit einem ex ante wirkenden Schutz zur Verfügung.[2088] Es erscheint problematisch, den Rechteinhabern solch weitgehende Schutzmechanismen zur Verfügung zu stellen, die Nutzer und die Allgemeinheit dagegen auf den langwierigen und nur ex post wirkenden Schutz der Gerichte zu verweisen. Schließlich ist fraglich, ob bezüglich aller denkbaren Interessen der Nutzer und der Allgemeinheit ein einklagbarer Anspruch bestimmter Nutzer existiert oder sich zumindest konstru-

---

2084 So in Deutschland insbesondere *Wand*, S. 126, 148 f., 284.

2085 So *Wand* auf S. 126, 130, bezüglich der Computerprogrammrichtlinie, auf S. 133 ff. bezüglich der Datenbankrichtlinie, auf S. 148 bezüglich § 69 d UrhG, und auf S. 180 bezügl. § 87 e UrhG. *Wand* macht davon jedoch eine Ausnahme bei Schrankenbestimmungen, die die Dekompilierung von Computerprogrammen erlauben. In diesen Fällen soll die urheberrechtliche Schrankenbestimmunge zur Offenhaltung der Märkte auf den rechtlichen Umgehungsschutz „durchschlagen" und der Umgehungsschutz entsprechend rechtlich beschränkt werden („Durchgriffslösung"); zu Art. 6 Computerprogrammrichtlinie s. *Wand*, S. 131 f., zu § 69 e UrhG s. *Wand*, S. 149.

2086 *Wand*, S. 135 f.

2087 S. oben bei Fn. 1932 f.

2088 S. oben bei Fn. 1455 ff.

ieren läßt.[2089] Manche Schrankenbestimmungen dienen nicht dem Interesse einzelner bestimmter Nutzer; ihre Wirkung verteilt sich vielmehr diffus auf die gesamte Gesellschaft.[2090]

c) Indirekte Regulierung durch Beschränkung des Umgehungsschutzes

Der Gesetzgeber muß nicht unbedingt die Ausgestaltung technischer Schutzmaßnahmen direkt beeinflussen. Will er bestimmten Schrankenbestimmungen in DRM-Systemen Geltung verschaffen, so kann er auf technische Schutzmaßnahmen indirekt Einfluß nehmen, indem er den rechtlichen Umgehungsschutz entsprechend seinen Wertvorstellungen modifiziert. So kann der rechtliche Umgehungsschutz versagt werden, wenn eine technische Schutzmaßnahme einen zu weitgehenden Schutz verleiht und Interessen der Nutzer oder der Allgemeinheit außer acht läßt. Da in diesen Fällen der rechtliche Umgehungsschutz dann nicht greift, ist der Nutzer faktisch berechtigt, die technische Schutzmaßnahme zu umgehen („right to hack"). Die Beschränkung des rechtlichen Umgehungsschutzes löst das Spannungsverhältnis zwischen technischen Schutzmaßnahmen und urheberrechtlichen Schrankenbestimmungen. Diese Regulierungsoption wird mitunter als „*Cohen*-Theorem" bezeichnet.[2091] Wie sich zeigen wird, verfolgt der U.S.-amerikanische „Digital Millennium Copyright Act" diesen Ansatz.[2092]

Dabei ist zu beachten, daß viele Nutzer nicht über die technischen Kenntnisse verfügen werden, um technische Schutzmaßnahmen selbst umgehen zu können. Sie sind auf die Existenz von Umgehungsvorrichtungen oder -dienstleistungen angewiesen, die die Umgehung der technischen Schutzmaßnahme ermöglichen. Entschließt sich der Gesetzgeber, den rechtlichen Umgehungsschutz zu beschränken, so muß er bis zu einem gewissen Maß auch den Vertrieb von Umgehungsvorrichtungen oder das Angebot von Umgehungsdienstleistungen erlauben.[2093] Anderenfalls

---

[2089] Aus diesem Grund meint *Wand*, urheberrechtliche Schrankenbestimmungen für digitale Privatkopien dürften den rechtlichen Umgehungsschutz technischer Schutzmaßnahmen nicht beschränken: In diesem Fall fehle es an einem Nutzungsvertrag, aus dem ein entsprechender Anspruch des Nutzers hergeleitet werden könne. Dieses Ergebnis hält *Wand* für interessengerecht, unter anderem aufgrund einer – verkürzten und dadurch teilweise irreführenden – rechtsökonomischen Argumentation; s. *Wand*, S. 137 f. In diesem Zusammenhang stellt sich auch die Frage, inwieweit urheberrechtliche Schrankenbestimmungen als „Rechte der Nutzer" aufgefaßt werden können; s. dazu oben Fn. 1967.

[2090] S. dazu unter rechtsökonomischen Gesichtspunkten oben bei Fn. 1730 ff.

[2091] So *Lessig*, S. 139; s. dazu *Cohen*, 13 Berkeley Tech. L. J. 1089, 1141 (1998).

[2092] S. dazu unten Teil 4, D II 3 c aa.

[2093] Regelmäßig ist der Vertrieb von Umgehungsvorrichtungen und andere sog. „vorbereitende Handlungen" verboten; s. dazu oben Teil 2, D I 1. Um urheberrechtlichen Schrankenbestimmungen in DRM-Systemen Geltung zu verschaffen, wird dieses Verbot jedoch in manchen Gesetzen wieder beschränkt, so insbesondere im U.S.-amerikanischen „Digital Millennium Copyright Act", s. dazu unten Teil 4 D II 2 c aa.

ist die Beschränkung des Umgehungsschutzes faktisch wirkungslos.[2094] Wird der Vertrieb von Umgehungsvorrichtungen erlaubt, so stellt sich jedoch das Problem, daß technische Schutzmaßnahmen mit diesen Umgehungsvorrichtungen grundsätzlich zu beliebigen Zwecken umgangen werden können. Umgehungsvorrichtungen sind rechtlich „neutral": Es ist schwierig zu entscheiden, ob eine Umgehungsvorrichtung hergestellt wurde, um legitimen Zwecken zu dienen oder nicht (sogenannte „dual use"-Problematik). Dadurch wird es bei der Regulierung von Umgehungsvorrichtungen äußerst schwierig, den Umgehungsschutz den urheberrechtlichen Schrankenbestimmungen anzupassen: Wird der Einsatz von Umgehungsvorrichtungen zu stark beschränkt, so wird es Nutzern erschwert, Inhalte in einer Weise zu nutzen, die nach urheberrechtlichen Schrankenbestimmungen gesetzlich erlaubt ist. Wird der Einsatz von Umgehungsvorrichtungen zu wenig beschränkt, so wird es Nutzern erleichtert, Inhalte in einer Weise zu nutzen, für die sie unzweifelhaft die Zustimmung des Inhalteanbieters benötigen.[2095] Entscheidet sich der Gesetzgeber für diese Regulierungsoption, so muß er einen Mittelweg zwischen beiden Polen finden. Es besteht immer die Gefahr, daß am Markt Umgehungsvorrichtungen verfügbar sind, mit denen technische Schutzmaßnahmen auch in Fällen umgangen werden können, in denen keine urheberrechtlichen Schrankenbestimmungen eingreifen.

d) Indirekte Regulierung durch „Key Escrow"-System

Eine dritte Regulierungsoption versucht, diese dargestellten Schwächen zu vermeiden. Bei diesem Ansatz erlaubt der Gesetzgeber nicht den freien Vertrieb von Umgehungsvorrichtungen. Vielmehr erhält der Nutzer das Recht, in Fällen, in denen zu seinen Gunsten eine Schrankenbestimmung eingreift, von einer bestimmten Instanz die entsprechenden Mittel (Umgehungssoftware, Dechiffrier-Schlüssel und ähnliches) zu erhalten, die zur Umgehung der technischen Maßnahme notwendig sind. Eine Weitergabe dieser Mittel an Dritte ist dem Nutzer untersagt.[2096] Vielmehr können Dritte diese Mittel ebenfalls von der Instanz erhalten, wenn – und nur, wenn – sie von der Schrankenbestimmung erfaßt werden. Durch diese Regulierungsoption könnte die Gefahr gebannt werden, daß technische Schutzmaßnahmen mit Umgehungsvorrichtungen unberechtigterweise umgangen werden können, die frei am Markt erhältlich sind. Wie sich zeigen wird, verfolgt die europäische Richtlinie zum Urheberrecht in der Informationsgesellschaft diesen Ansatz.[2097]

[2094] *Koelman*, EIPR 2000, 272, 274; s. weiterhin *Samuelson*, 14 Berkeley Tech. L. J. 519, 548 (1999); *Davis*, 13 Berkeley Tech. L. J. 1144, 1147 (1998); *Benkler*, 74 N.Y.U. L. Rev. 354, 416 (1999); *Wand*, S. 56 f.; Universal City Studios, Inc. v. Reimerdes, 111 F.Supp. 2d 294, 324 (S.D.N.Y. 2000).

[2095] *Koelman*, EIPR 2000, 272, 274.

[2096] S. *Dreier*, CR 2000, 45, 47.

[2097] S. dazu unten Teil 4, D II 3 a aa.

Der Ansatz ähnelt der „Key Recovery"- oder „Key Escrow"-Problematik in der Kryptographie-Kontroverse:[2098] In beiden Fällen kann mit Hilfe eines hinterlegten Schlüssels eine verschlüsselte Kommunikation unter bestimmten Voraussetzungen dechiffriert werden.[2099] Für einen „Key Escrow" bei DRM-Systemen müßte eine Instanz („Schlüsselhinterlegungs-Instanz") existieren, bei der berechtigte Nutzer entsprechende Dechiffrier-Schlüssel und andere Umgehungsvorrichtungen erhalten könnten.

Diese Schlüsselhinterlegungs-Instanz könnte von unterschiedlichen Akteuren innerhalb eines DRM-Systems betrieben werden. Würden die Inhalteanbieter oder DRM-Systembetreiber die Schlüsselhinterlegungs-Instanz selbst betreiben, so würde sich ein Nutzer, zu dessen Gunsten eine urheberrechtliche Schrankenbestimmung eingreift, an diese Instanz wenden und eine entsprechende Umgehungssoftware, Dechiffrier-Schlüssel oder ähnliches erhalten, mit dem er den DRM-Schutz in diesem Fall umgehen und damit von der Schrankenbestimmung profitieren kann.[2100] Dieser Ansatz begegnet jedoch einigen Bedenken. Wie oben dargestellt wurde, dienen urheberrechtliche Schrankenbestimmungen oftmals den Interessen der Nutzer und der Allgemeinheit, die den Interessen der Inhalteanbieter diametral entgegenlaufen können. Könnten Inhalteanbieter kontrollieren, in welchen Fällen ein Nutzer die erforderlichen Umgehungsvorrichtungen erhält, um von Schrankenbestimmungen Gebrauch zu machen, hätten sie einen starken Anreiz, dies in möglichst vielen Fällen

[2098] Heute verfügbare Verschlüsselungsverfahren sind bei korrekter Anwendung praktisch nicht mehr zu „knacken". Verwendet ein Nutzer starke Verschlüsselungsverfahren, so kann niemand außer dem Empfänger die verschlüsselte Kommunikation entschlüsseln. Selbst für staatliche Rechtsverfolgungsorgane und Nachrichtendienste kann es unmöglich oder zumindest sehr zeitaufwendig werden, die Kommunikation zu dechiffrieren. Bei der „Key Escrow"-Problematik geht es um die Frage, ob und inwieweit der Staat vom Nutzer eines Verschlüsselungssystems verlangen darf, Zugriff auf den verwendeten Schlüssel zu erhalten, um die verschlüsselte Kommunikation in Fällen berechtigten Interesses dechiffrieren zu können. Zu diesem Zweck wird diskutiert, die verwendeten Schlüssel bei einer vertrauenswürdigen dritten Instanz („trusted third party") zu hinterlegen, von der der Staat den Schlüssel gegebenenfalls erhalten kann. In den USA wurde diese Problematik insbesondere beim „Clipper Chip" erörtert, einem Verschlüsselungs-Chip, bei dem die Möglichkeit des staatlichen Zugriffs eingebaut war; s. dazu *Anderson*, S. 466 f. Die technischen Einzelheiten dieser Verfahren sind komplex; s. zum ganzen *Kuner* in: Hoeren/Sieber (Hrsg.), Teil 17, Rdnr. 17 ff.; *Froomkin*, 1996 U. Chi. Legal F. 15 ff.; *Anderson*, S. 468 ff.; *Schneier*, S. 97 ff., 181 f.

[2099] Dennoch bestehen wichtige Unterschiede. So dient der „Key Escrow"-Ansatz im Kryptographie-Bereich staatlichen Interessen an einer Überwachung der Kommunikation seiner Bürger, während der „Key Escrow"-Ansatz im DRM-Bereich dem Interesse der Nutzer dient, in bestimmten Fällen digitale Inhalte ohne Zustimmung der Inhalteanbieter nutzen zu können. Damit sind auch die Einwände, die im Kryptographie-Bereich gegen den „Key Escrow"-Ansatz vorgebracht werden, nicht ohne weiteres auf den DRM-Bereich übertragbar.

[2100] Einen solchen Ansatz schlägt wohl *Dreier*, CR 2000, 45, 47, vor.

zu verhindern.[2101] Um diese Probleme zu vermeiden, könnte die Schlüsselhinterlegungs-Instanz auch von einer unabhängigen vertrauenswürdigen dritten Instanz („trusted third party") betrieben werden.[2102] Dadurch würden Interessenkonflikte verhindert.

Unabhängig von der Frage, ob der „key escrow" bei den Inhalteanbietern oder einer dritten Instanz angesiedelt werden sollte, ist auch dieser Ansatz insgesamt mit Problemen behaftet. Will ein Nutzer von urheberrechtlichen Schrankenbestimmungen Gebrauch machen, so muß er sich danach zunächst an eine wie auch immer geartete Instanz wenden, um die erforderlichen Umgehungsvorrichtungen zu erhalten. Zwar könnte diese Instanz mit Nutzervereinigungen (Bibliotheksverbänden, Blindenverbänden etc.) Pauschalverträge abschließen, so daß es nicht notwendig wäre, sich vor jeder einzelnen Nutzung an die Instanz zu wenden. Dennoch führt die „key escrow"-Lösung in der Tendenz zu einer „Zentralisierung der Schrankenbestimmungen": In einem DRM-System mit einer „key escrow"Lösung gibt es nur noch wenige Akteure, die darüber bestimmen, welcher Nutzer zu welchen Zwecken von Schrankenbestimmungen Gebrauch machen kann. Natürlich wird sich der Nutzer bei Fehlentscheidungen dieser Akteure auf dem Rechtsweg wehren können. Dies ist jedoch ein mühsames und langwieriges Unterfangen.

Weiterhin ist zu bedenken, daß die Transaktionskosten eines solchen Systems nicht unerheblich wären. Nutzer werden mitunter den Aufwand scheuen, sich an die Instanz zu wenden und die entsprechenden Informationen oder Umgehungsvorrichtungen zu beziehen, und erst gar nicht den Inhalt in der entsprechenden Weise nutzen.[2103] Dies gilt insbesondere, wenn die entsprechende Instanz von den Inhalteanbietern betrieben oder in sonstiger Weise von ihnen wirtschaftlich abhängig ist. Eine „key escrow"-Lösung führt zu einer deutlichen Verschlechterung der Position des Nutzers.[2104] Auch müßte ein solches System datenschutzrechtlichen Bedenken Rechnung tragen. Wird die Schlüsselhinterlegungs-Instanz von den Inhalteanbietern oder DRM-Systembetreibern unterhalten, so scheint fraglich, ob diese Akteure detaillierte Informationen über einen

---

[2101] Ebenso *Burk/Cohen*, S. 15 f.

[2102] Ein solches System wurde in Grundzügen von *Stefik*, The Internet Edge, S. 99 ff., und *ders.*, 12 Berkeley Tech. L. J. 136, 156 ff. (1997) unter dem Namen „Digital Property Trust" vorgeschlagen. Vgl. weiterhin ausführlich *Burk/Cohen*, S. 15 ff. Daneben spielen „trusted third parties" insbesondere bei asymmetrischen Verschlüsselungsverfahren als Zertifizierungsinstanzen eine Rolle.

[2103] Ebenso *Burk/Cohen*, S. 16.

[2104] *Burk/Cohen*, S. 17, merken an, daß sich durch eine „key escrow"-Lösung Schrankenbestimmungen von „liability rules" zu „property rules" wandeln könnten: Ist fraglich, ob eine Schrankenbestimmung eingreift, so läuft der Nutzer im herkömmlichen Urheberrecht allenfalls Gefahr, *ex post* Schadensersatzansprüchen ausgesetzt zu sein. In einem System des „key escrow" muß er dagegen *ex ante* die Rechtslage klären und notfalls eine Zustimmung des Inhalteanbieters einklagen.

Nutzer und dessen beabsichtigte Nutzung eines Inhalts nur aus dem Grund erhalten sollten, weil der Nutzer von einer Schrankenbestimmung Gebrauch machen will.[2105] Schließlich wäre der Aufbau von „key escrow"-Infrastrukturen, die auch im internationalen Kontext funktionieren müssen, mit entsprechenden Kosten verbunden.

Trotz aller Einwände hat diese recht anbieterfreundliche Regulierungsoption ihre Vorteile. Viele Probleme würden zudem gelindert, wenn der „key escrow" nicht im Umfeld der – durch eigene Interessen vorbelasteten – Inhalteanbieter, sondern bei einer unabhängigen dritten Instanz angesiedelt würde.[2106]

e) Kombination der Regulierungsmöglichkeiten

Alle Regulierungsmöglichkeiten, durch die technische Schutzmaßnahmen in Einklang mit urheberrechtlichen Schrankenbestimmungen gebracht werden sollen, haben ihre Schwächen. Sie lassen sich aber auch untereinander kombinieren. So schlagen *Burk* und *Cohen* vor,[2107] auf einer ersten Ebene technische Schutzmaßnahmen direkt gesetzlich zu regulieren (dazu oben a). Danach müßten technische Schutzmaßnahmen in DRM-Systemen einen bestimmten Ausschnitt der Schrankenbestimmungen direkt auf der technischen Ebene beachten.[2108] Bezüglich darüber hinausgehender und komplizierterer Fälle, in denen urheberrechtliche Schrankenbestimmungen eingreifen, könnte auf einer zweiten Ebene der „key escrow"-Ansatz unter Einschaltung einer vertrauenswürdigen dritten Instanz verfolgt werden (dazu oben d).[2109]

Trotzalledem wird man sich wohl damit abfinden müssen, daß es keine Patentlösung gibt, um technische Schutzmaßnahmen mit allen denkbaren

---

[2105] Ebenso *Burk/Cohen*, S. 16. Dabei können technische Ansätze helfen. Auch mag die Verortung des „key escrows" bei einer unabhängigen vertrauenswürdigen dritten Instanz das Problem lindern; s. dazu *Burk/Cohen*, S. 19 f.; *Stefik*, The Internet Edge, S. 101. Dabei sind aber auch berechtigte Interessen der Inhalteanbieter zu berücksichtigen. Sie müssen Möglichkeiten haben, einen Nutzer zu identifizieren, der sich unter einem Vorwand entsprechende Umgehungsvorrichtungen besorgt hat und diese zu anderen Zwecken mißbraucht. Dabei handelt es sich um das allgemeine Spannungsverhältnis zwischen Anonymität und Identifizierung, das auch in anderen Bereichen auftritt (beispielsweise digitales Geld).

[2106] Ebenso *Burk/Cohen*, S. 19, die ihre Lösung selbst als „second-best"-Lösung bezeichnen, *Burk/Cohen*, S. 27. Dabei sind auch berechtigte Sicherheitsinteressen der Inhalteanbieter zu beachten. Sie haben kein Interesse daran, einer dritten Instanz Informationen über die Umgehung ihrer technischen Schutzmaßnahmen zur Verfügung zu stellen, wenn dadurch die Sicherheit des DRM-Systems insgesamt beeinträchtigt wird.

[2107] *Burk/Cohen*, S. 20 ff.

[2108] So könnte der Gesetzgeber beispielsweise vorsehen, daß ein DRM-System die Erstellung einer einzelnen digitalen Privatkopie erlauben muß. Dies ist in den USA bei DAT-Geräten mit dem „Audio Home Recording Act" faktisch geschehen; s. dazu oben Teil 2, D II 1 b.

[2109] S. zu den Einzelheiten *Burk/Cohen*, S. 21. Sie schlagen vor, diese Instanz beim U.S. Copyright Office der Library of Congress anzusiedeln.

Beschränkungen des Urheberrechts und anderer Rechtsgebiete in Einklang zu bringen.[2110]

II. Tatsächliche Reaktionen des Rechts

Nachdem die unterschiedlichen Regulierungsoptionen aufgezeigt wurden, die den Gesetzgebern zur Verfügung stehen, um technische Schutzmaßnahmen in Einklang mit urheberrechtlichen Schrankenbestimmungen zu bringen, soll im Überblick[2111] dargestellt werden, welche Optionen die Gesetzgeber tatsächlich gewählt haben. Dabei wird auch auf die einschlägige Rechtsprechung eingegangen. Teilweise werden technische Schutzmaßnahmen durch gesetzliche Regelungen unmittelbar beschränkt (dazu unten 1). Teilweise stehen dem Nutzer auch nur allgemeine Ansprüche gegen umfassend ausgestaltete Schutzmaßnahmen zur Verfügung (dazu unten 2). Häufiger wird mittelbar auf technische Schutzmaßnahmen Einfluß genommen, indem der rechtliche Umgehungsschutz beschränkt oder ein „key escrow"-System etabliert wird (dazu unten 3).

1. Direkte Regulierung technischer Schutzmaßnahmen

a) U.S.-amerikanischer Rechtsrahmen

Der U.S.-amerikanische „Audio Home Recording Act" schreibt vor, daß digitale Aufnahmegeräte, die für den privaten Konsumenten bestimmt sind, mit dem „Serial Copy Management System" ausgestattet sein müssen.[2112] Das bedeutet implizit, daß diese Geräte mindestens eine digitale Kopie eines Originals erstellen können.[2113] Digitale Aufnahmegeräte, die überhaupt keine digitale Privatkopie zulassen, sind damit am Markt nicht erhältlich. Durch solche Regelungen kann mittelbar urheberrechtlichen Schrankenbestimmungen zum Durchbruch verholfen werden.

Weiterhin bestehen in den USA gesetzliche Beschränkungen von Pay-TV-Schutzmaßnahmen zum Schutz des Free-TV. Die analogen Kopierschutzverfahren von Macrovision, die nach 17 U.S.C. § 1201 (k) (1) in analoge Videorekorder und -kameras integriert werden müssen,[2114] dürfen nach der Regelung des 17 U.S.C. § 1201 (k) (2) von den Geräteherstellern und den Rechteinhabern nicht in beliebiger Weise eingesetzt werden. Sie dürfen das Kopieren von Videoinhalten durch die Konsumenten nur verhindern, wenn es um Pay-Per-View-, Video-on-Demand- und normalen Pay-TV-Sendungen[2115] oder um das Kopieren von einem physikalischer Speicher-

[2110] Ebenso *Koelman*, The Protection of Technological Measures, S. 1.

[2111] Im folgenden werden nicht alle Vorschriften untersucht, in denen technische Schutzmaßnahmen geschützt oder sonstwie reguliert werden. Vielmehr werden nur die wichtigsten Vorschriften exemplarisch herausgegriffen.

[2112] S. dazu oben Teil 2, D II 1b.

[2113] Zu den technischen Grundlagen von SCMS s. oben Teil 1, D II 1.

[2114] S. dazu oben Teil 2, D II 1 b.

[2115] 17 U.S.C. § 1201 (k) (2) (A) und (B).

medium[2116] geht. In anderen Fällen – insbesondere bei Sendungen im Free-TV – dürfen die Kopierschutzverfahren nicht eingesetzt werden.[2117] Auch wenn die Vorschrift kein unmittelbar urheberrechtliches Regelungsziel hat, zeigt sie doch die Möglichkeit des Gesetzgebers, durch eine direkte Regulierung technischer Schutzmaßnahmen negative Auswirkungen von DRM-Systemen mit einem zu hohen Schutzniveau zu vermeiden.

b) Deutscher und europäischer Rechtsrahmen

In Deutschland und Europa existieren ähnliche Regelungen. Durch den 4. Rundfunkänderungsstaatsvertrag, der am 1. 4. 2000 in Kraft getreten ist,[2118] wurde mit § 5 a RfStV eine neue Vorschrift eingefügt, nach der die Fernsehausstrahlung bestimmter „Ereignisse von erheblicher gesellschaftlicher Bedeutung" in verschlüsselter Form und gegen besonderes Entgelt nicht zulässig ist. Solche Sendungen müssen im Free-TV ausgestrahlt werden.[2119] Darunter fallen sportliche Großereignisse, unter anderem Olympische Spiele und bestimmte Fußballspiele, § 5 a Abs. 2 RfStV.[2120] Die Regelung beruht auf Art. 3 a der novellierten Fernsehrichtlinie der EG aus

---

[2116] Bespielte Videokassetten oder DVDs, 17 U.S.C. § 1201 (k) (2) (C).

[2117] S. dazu auch *U.S. House of Representatives*, H.R. Rep. No. 105–796, S. 70; *Pollack*, 17 Cardozo Arts & Ent. L. J. 47, 104 (1999).

[2118] Gesetz zum Vierten Rundfunkänderungsstaatsvertrag und zur Änderung des Landesmediengesetzes vom 20. 12. 1999, Gesetzblatt Baden-Württemberg Nr. 22 vom 30. 12. 1999, S. 665–683.

[2119] § 5 a RfStV lautet auszugsweise:

„(1) Die Ausstrahlung im Fernsehen von Ereignissen von erheblicher gesellschaftlicher Bedeutung (Großereignisse) in der Bundesrepublik Deutschland verschlüsselt und gegen besonderes Entgelt ist nur zulässig, wenn der Fernsehveranstalter selbst oder ein Dritter zu angemessenen Bedingungen ermöglicht, dass das Ereignis zumindest in einem frei empfangbaren und allgemein zugänglichen Fernsehprogramm in der Bundesrepublik Deutschland zeitgleich oder, sofern wegen parallel laufender Einzelereignisse nicht möglich, geringfügig zeitversetzt ausgestrahlt werden kann. […] Als allgemein zugängliches Fernsehprogramm gilt nur ein Programm, das in mehr als zwei Drittel der Haushalte tatsächlich empfangbar ist.

(2) Großereignisse im Sinne dieser Bestimmung sind:

1. Olympische Sommer- und Winterspiele,
2. bei Fußball-Europa- und -Weltmeisterschaften alle Spiele mit deutscher Beteiligung sowie unabhängig von einer deutschen Beteiligung
3. das Eröffnungsspiel, die Halbfinalspiele und das Endspiel,
4. die Halbfinalspiele und das Endspiel um den Vereinspokal des Deutschen Fußball-Bundes,
5. Heim- und Auswärtsspiele der deutschen Fußballnationalmannschaft,
6. Endspiele der europäischen Vereinsmeisterschaften im Fußball (Champions League, UEFA-Cup) bei deutscher Beteiligung. […]"

Zwar schreibt die Regelung nur vor, daß die Großereignisse bei einer Übertragung in einem verschlüsselten Pay-TV-Sender daneben in einem unverschlüsselten, allgemein zugänglichen Fernsehprogramm empfangbar sein müssen. Da eine solche Parallelausstrahlung regelmäßig nicht wirtschaftlich sinnvoll ist, hat die Regelung zur Folge, daß die Großereignis de facto dem Free-TV vorbehalten bleiben.

[2120] S. zu der ganzen Regelung *Bröcker/Neun*, ZUM 1998, 766 ff.

dem Jahr 1997.[2121] Unabhängig davon, wie man zu dieser Regelung aus ordnungspolitischen Gesichtspunkten stehen mag,[2122] sind sie – wie die U.S.-amerikanischen Regelungen – ein Beispiel für die Bemühung des Gesetzgebers, aus seiner Sicht nachteilige Folgen von DRM-Systemen mit hohem Schutzniveau zu begrenzen. Mitunter wird vorgeschlagen, den Regelungsansatz des § 5 a RfStV beziehungsweise der Fernsehrichtlinie auch auf die urheberrechtliche Problematik von DRM-Systemen anzuwenden.[2123]

2. Umfassender Schutz mit allgemeinen Gegenansprüchen der Nutzer

Mitunter stehen dem Nutzer gegen umfassende technische Schutzmaßnahmen rechtliche Gegenansprüche zur Verfügung, die sich aus unterschiedlichen allgemeinen Vorschriften ergeben können.

a) Deutscher Rechtsrahmen

In einem Fall, der dem Bundesgerichtshof 1999 zur Entscheidung vorlag, hatte ein Softwarehersteller in sein Programm eine verborgene Programmsperre eingebaut. Die Programmsperre verhinderte, daß der Erwerber der Software das Programm an einen Dritten weiterveräußern konnte.[2124] Bei einer Weiterveräußerung erklärte sich der Softwarehersteller nur gegen die Zahlung einer erneuten Vergütung bereit, die Programmsperre aufzuheben.[2125] Mit Hilfe der Programmsperre konnte der Softwarehersteller faktisch die Wirkungen des urheberrechtlichen Erschöpfungsgrundsatzes aushebeln. Unter dem Blickwinkel der vorliegenden Untersuchung geht es in diesem Fall um die Frage, ob durch technische Schutzmaßnahmen die Beschränkung des § 17 Abs. 2 UrhG[2126]

[2121] Richtlinie 97/36/EG des Europäischen Parlaments und des Rates vom 30. 6. 1997 zur Änderung der Richtlinie 89/552/EWG des Rates zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Ausübung der Fernsehtätigkeit, ABl. EG Nr. L 202 vom 30. 7. 1997, S. 60–71.

[2122] Solche Regelungen führen zu einer Wettbewerbsverzerrung zwischen dem Pay- und dem Free-TV und zu einer Erhöhung der Markteintrittsbarrieren im Pay-TV-Bereich; s. *Monopolkommission*, XIII. Hauptgutachten, Tz. 620.

[2123] *Hugenholtz*, 26 Brooklyn J. Int'l L. 77, 89 (2000); *ders.*, 6 Maastricht Journal of European and Comparative Law 308, 318 (1999); s. a. *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 199 f.

[2124] Dies war jedenfalls der Effekt der Programmsperre. Tatsächlich enthielt das Programm eine jährlich auftretende Programmsperre („expiration date"), die nur durch die Eingabe eines Codeworts, das der Erwerber vom Softwarehersteller erfragen mußte, deaktiviert werden konnte. Veräußerte der Erwerber der Software das Programm an einen Dritten, so konnte der Softwarehersteller den Verkauf faktisch vereiteln, wenn er dem Dritten das entsprechende Codewort nicht mitteilte; s. OLG Bremen, WRP 1997, 573.

[2125] Zusätzlich teilte der Softwarehersteller dem Erwerber die Existenz der Programmsperre nicht mit, OLG Bremen, WRP 1997, 573.

[2126] Im vorliegenden Fall ging es um die Vorschrift des § 69 c Nr. 3 S. 2 UrhG, der eine Ausgestaltung des Erschöpfungsgrundsatzes im Bereich der computerrechtlichen Vorschriften des UrhG ist.

umgangen werden kann.[2127] Die Vorinstanz zum BGH[2128] hatte entschieden, das Verbreitungsrecht des Softwareherstellers habe sich durch die Veräußerung des Exemplars an den Ersterwerber erschöpft.[2129] Durch die Programmsperre setze der Softwarehersteller faktisch den Erschöpfungsgrundsatz außer Kraft. Dieses Verhalten sei sittenwidrig und berechtige zu Schadensersatzansprüchen nach § 826 BGB.[2130] Der Bundesgerichtshof wies die Klage aus anderen Gründen ab[2131] und ging auf die Frage des Verhältnisses zwischen dem Erschöpfungsgrundsatz und technischen Schutzmaßnahmen nicht ein.[2132]

Neben urheberrechtlichen Grundsätzen können auch andere Vorschriften die Ausgestaltung technischer Schutzmaßnahmen beeinflussen. So können Fehlfunktionen technischer Schutzmaßnahmen zu kaufrechtlichen Mängelgewährleistungsansprüchen führen.[2133] Auch kann ein Verstoß gegen §§ 1, 3 UWG vorliegen.[2134]

[2127] Bei Online-DRM-Systemen wird sich das Problem nicht stellen, da nach h. M. der Erschöpfungsgrundsatz im Online-Umfeld nicht greift, s. oben Fn. 1619. Die Entscheidung wird hier dennoch angeführt, da sie einerseits für Offline-DRM-Systeme relevant ist. Andererseits ist es eine der wenigen Entscheidungen, deren Sachverhalt explizit das Verhältnis von urheberrechtlichen Grundsätzen zu technischen Schutzmaßnahmen betrifft.

[2128] OLG Bremen, WRP 1997, 573.

[2129] Zwar sei eine schuldrechtliche Verpflichtung, das Exemplar nicht weiterzuveräußern, wirksam. Dingliche Wirkung entfalte diese aber nicht, weil der Erschöpfungsgrundsatz zwingenden Charakter habe, OLG Bremen, WRP 1997, 573, 575.

[2130] OLG Bremen, WRP 1997, 573, 575 ff. In dem zugrundeliegenden Fall hatte der Softwarehersteller das Programm an einen Ersterwerber veräußert, der das Programm an einen Zweiterwerber weiterveräußerte. Als dieser die Software an einen Dritterwerber weiterveräußern wollte, bemerkte der Zweiterwerber die Programmsperre, was die Weiterveräußerung unmöglich machte. Der Rechtsstreit betsand daher zwischen dem Zweiterwerber und dem Softwarehersteller.

[2131] Der BGH verneinte, daß der Softwarehersteller über den notwendigen Vorsatz verfügt habe, der sich bei § 826 BGB auch auf den Schaden selbst beziehen müsse; s. BGH CR 2000, 94, 95 f. – Programmsperre III.

[2132] Die einzigen Ausführungen des BGH zu dieser Frage lauten: „[…] die Frage der generellen Zulässigkeit des Einbaus einer Programmsperre, insbesondere im Verhältnis zu Zweit- und Dritterwerbern, ist bislang – soweit ersichtlich – höchstrichterlich noch nicht abschließend entschieden"; BGH CR 2000, 94, 96 – Programmsperre III.

[2133] S. dazu ausführlich *Marly*, Softwareüberlassungsverträge, Rdnr. 795 ff.; BGH NJW 1987, 2004 – Programmsperre II; OLG Celle, CR 1994, 217; OLG Köln, CR 2000, 354, 355; *Loewenheim* in: Schricker (Hrsg.), UrhG-Kommentar, § 69 d Rdnr. 10. Zur Frage, ob Programmsperren ein Kündigungsrecht geben, s. BGH NJW 1981, 2684 – Programmsperre I; OLG Köln, NJW 1996, 733.

[2134] Der durch eine technische Schutzmaßnahme auferlegte Zwang, ein Computerprogramm nach 25-maliger Nutzung beim Hersteller zu registrieren, kann, wenn der Nutzer darauf im Nutzungsvertrag nicht hingewiesen wurde, gegen §§ 1, 3 UWG verstoßen, OLG München, CR 2001, 11 ff. – Omnipage.

b) U.S.-amerikanischer Rechtsrahmen

In den USA wird seit längerer Zeit diskutiert, ob ein Rechteinhaber seine Interessen gegenüber Vertragspartnern durch technische Schutzmaßnahmen in unbeschränktem Umfang durchsetzen kann. Die Problematik wird unter dem Stichwort „electronic self-help" behandelt.[2135] Auch wenn sich die Diskussion nicht auf DRM-Systeme beschränkt, können gesetzliche Regelungen, die die Möglichkeiten einer „electronic self-help" einschränken, auch Auswirkungen auf die Ausgestaltung technischer Schutzmaßnahmen in DRM-Systemen haben.

Die rechtliche Zulässigkeit der „electronic self-help" ist von den Einzelumständen abhängig und insgesamt im U.S.-amerikanischen Recht unklar.[2136] So existieren Gerichtsentscheidungen, nach denen die Fern-Deaktivierung („remote deactivation") von Computersoftware durch den Softwarehersteller rechtlich zulässig ist, wenn der Käufer gegen Nutzungsbestimmungen verstoßen oder die Lizenzgebühren nicht gezahlt hat.[2137] Im Rahmen des „Uniform Computer Information Transactions Act" (UCITA)[2138] wurde versucht, Rechtsklarheit bezüglich der Zulässigkeit der „electronic self-help" zu schaffen. Das Modellgesetz unterscheidet dabei zwischen zwei Fällen:[2139] Im ersten Fall (§ 816 UCITA) geht es um technische Schutzmaßnahmen, die eingreifen, nachdem der Lizenznehmer gegen Vertragsbedingungen verstoßen und der Lizenzgeber daraufhin den Vertrag gekündigt hat. Die technischen Schutzmaßnahmen sollen in diesem Fall verhindern, daß der Lizenznehmer den lizenzierten Gegenstand – unter anderem Software und andere digitale Inhalte[2140] –

[2135] *Dolly*, 33 J. Marshall L. Rev. 663 (2000); *Cohen*, 13 Berkeley Tech. L. J. 1089 ff. (1998); *Roditti*, 21 Rutgers Computer & Tech. L. J. 431 ff. (1995); *Heaton*, 6 B.U. J. Sci. & Tech. L. 8 (2000).

[2136] *Heaton*, 6 B.U. J. Sci. & Tech. L. 8 (2000), Abs. 9; *Cohen*, 13 Berkeley Tech. L. J. 1089, 1112 f. (1998); *Dolly*, 33 J. Marshall L. Rev. 663, 674 (2000).

[2137] American Computer Trust Leasing v. Jack Farrell Implement Co., 763 F. Supp. 1473, 1492 ff. (D. Minn. 1991), *aff'd*, American Computer Trust Leasing v. Boerboom, 967 F.2d 1208 (8th Cir. 1992); s. dazu *R. T. Nimmer*, § 11.28[4], S. 11–111 f.; *Heaton*, 6 B.U. J. Sci. & Tech. L. 8 (2000), Abs. 5; vgl. weiterhin North Texas Preventive Imaging, LLC v. Eisenberg, 1996 U.S. Dist. Lexis 19990, 1996 WL 1359212, (C.D.Cal. 1996). Es sind aber auch Entscheidungen mit dem entgegengesetzten Ergebnis ergangen, z. B. Clayton X-Ray Co. v. Professional Systems Corp., 812 S.W. 2d 565 (Mo. App. 1991). S. zu weiteren Fällen *Edwards*, 58 U. Pitt. L. Rev. 763, 774 ff. (1997); *Roditti*, 21 Rutgers Computer & Tech. L. 431, 435 ff. (1995); *R. T. Nimmer*, § 11.28[4], S. 11–111 m. w. N.; *Cohen*, 13 Berkeley Tech. L. J. 1089, 1112 Fn. 81 (1998); *Lejeune*, CR 2000, 265, 270 Fn. 42. Die einzelnen Fälle unterscheiden sich im Sachverhalt erheblich.

[2138] S. dazu allgemein oben Teil 2, B II 3 a bb.

[2139] S. zur Abgrenzung § 605 (f) UCITA sowie die Official Comments Nr. 1 und 6 zu § 605 UCITA, *UCITA*, S. 238. S. zum ganzen in der deutschen Literatur *Lejeune*, CR 2000, 265, 270 f.

[2140] S. zum lizenzierten Gegenstand im Rahmen des UCITA § 102 (a) (35), (38) und (41) UCITA.

nach Vertragskündigung weiter nutzen kann. Im zweiten Fall (§ 605 UCITA) geht es um technische Schutzmaßnahmen, die schon im Vorfeld verhindern sollen, daß der Lizenznehmer überhaupt gegen Vertragsbedingungen verstößt.

Gemäß § 816 i. V. m. § 815 UCITA hat der Lizenzgeber grundsätzlich das Recht, nach einer Beendigung der Lizenz[2141] die weitere Nutzung des lizenzierten Gegenstandes durch technische Schutzmaßnahmen zu verhindern („remote deactivation").[2142] Dies ist jedoch nur unter den engen Voraussetzungen des § 816 Abs. (c) ff. UCITA zulässig.[2143] Die Vorschriften zur „electronic self-help" waren während der Entstehungsgeschichte des UCITA äußerst umstritten.[2144] Als Reaktion auf die anhaltende Kritik wurden einerseits die Voraussetzungen des § 816 UCITA strenger gefaßt.[2145] Andererseits beschloß die NCCUSL im August 2000, daß der Lizenzgeber bei „mass-market licenses" keine „electronic self-help" verwenden dürfe. Diese bedeutende Einschränkung findet sich nun in § 816 (b) S. 2 UCITA. Für Nutzungsverträge in DRM-Systemen bedeutet das, daß ein Inhalteanbieter, der nach Vertragskündigung den Nutzer von der weiteren Nutzung des geschützten Inhalts beziehungsweise der geschützten Software ausschließen will, in bestimmten Fällen keine technischen Schutzmaßnahmen verwenden kann, um dieses Ziel zu erreichen.

Gemäß § 605 UCITA ist der Lizenzgeber unter bestimmten Voraussetzungen berechtigt, technische Schutzmaßnahmen einzusetzen, die ge-

---

2141 Der Lizenzgeber kann bei Vertragsverstößen des Lizenznehmers den Lizenzvertrag unter bestimmten Voraussetzungen kündigen und die Lizenz beenden, s. § 802 i. V. m. § 701 UCITA. Danach können grundsätzlich auch Verstöße eines Nutzers gegen einen DRM-Nutzungsvertrag den Inhalteanbieter bzw. DRM-Systembetreiber zu einer Kündigung des Nutzungsvertrags berechtigen.

2142 Dies kann für den Lizenznehmer sehr nachteilhaft sein: Ist der Lizenzgeber eines Computerprogramms berechtigt, nach ausbleibenden Zahlungen des Lizenznehmers den Vertrag zu kündigen und das Programm aus der Ferne abzuschalten („remote deactivation"), so kann dies zu erheblichen Umsatzeinbußen des Lizenznehmers führen, wenn es sich beispielsweise um Auftragsbearbeitungs- oder Maschinensteuerungssoftware handelt. Daher ist es Ziel von Vorschriften wie § 816 UCITA, die Stellung des Lizenznehmers nicht über Gebühr zu schwächen; s. *R. T. Nimmer*, § 11.28[4], S. 11–110; *Heaton*, 6 B.U. J. Sci. & Tech. L. 8 (2000), Abs. 12 f.

2143 So muß der Lizenznehmer der Verwendung der „electronic self-help" zugestimmt haben, § 816 (c) UCITA. Der Lizenzgeber muß den Lizenznehmer 15 Tage vor Ausübung der „electronic self-help" darauf hinweisen, § 816 (d) UCITA. Der Lizenzgeber darf sie nicht ausüben, wenn dadurch öffentliche Interessen beeinträchtigt werden, § 816 (f) UCITA. Bei einer unberechtigten Ausübung der „electronic self-help" stehen dem Lizenznehmer Schadensersatzansprüche zu, § 816 (e) UCITA.

2144 Zwischenzeitlich wurden die entsprechenden Vorschriften sogar aus dem Entwurf entfernt, da man sich nicht auf eine einheitliche Fassung einigen konnte. S. zum ganzen *Cohen*, 13 Berkeley Tech. L. J. 1089 ff. (1998); *Edwards*, 58 U. Pitt. L. Rev. 763 ff. (1997); *Heaton*, 6 B.U. J. Sci. & Tech. L. 8 (2000), Abs. 11 f.; *Dolly*, 33 J. Marshall L. Rev. 663, 678 ff. (2000); *Lejeune*, CR 2000, 265, 270 f.

2145 S. dazu *Heaton*, 6 B.U. J. Sci. & Tech. L. 8 (2000), Abs. 18 ff.

währleisten, daß digitale Inhalte nur in den Grenzen des Nutzungsvertrags genutzt werden können. Als Beispiel wird eine Schutzmaßnahme genannt, die sicherstellt, daß ein Nutzer einen Inhalt nur 30 Minuten nutzen kann, wenn er nur zu dieser Nutzungszeit berechtigt ist.[2146] Auch ist es zulässig, technisch zu verhindern, daß der Nutzer mehr als eine Kopie eines digitalen Inhalts erstellt.[2147] Ein weiteres Beispiel ist eine Schutzmaßnahme, die ein Computerspiel, das der Nutzer nach dem Nutzungsvertrag nur einmal benutzen darf, nach dieser Nutzung löscht.[2148] Solange der Nutzungsvertrag wirksam ist, kann es zulässig sein, durch technische Schutzmaßnahmen Nutzungen zu verhindern, die nach urheberrechtlichen Grundsätzen erlaubt wären.[2149] Es ist nicht unbedingt erforderlich, daß der Nutzer vorher über die Verwendung dieser Schutzmaßnahmen unterrichtet wurde.[2150] Eine dem § 816 (b) S. 2 UCITA entsprechende Regelung, wonach solche Maßnahmen bei „mass-market licenses" nicht erlaubt sind, fehlt.[2151] § 605 UCITA kann auch bei DRM-Systemen eingreifen.[2152]

Insgesamt sind Maßnahmen der „electronic self-help" im Rahmen des UCITA in recht weitem Umfang möglich. Der Einsatz technischer Schutzmaßnahmen in DRM-Systemen wird durch den UCITA nur in Randbereichen beschränkt.

3. Indirekte Regulierung technischer Schutzmaßnahmen

Daneben existiert eine Vielzahl von Regelungen, die nur indirekt beschränkende Auswirkungen auf den technischen Schutz in DRM-Syste-

---

[2146] Official Comment Nr. 2 zu § 605 UCITA, *UCITA*, S. 239.

[2147] Official Comment Nr. 3 b zu § 605 UCITA, *UCITA*, S. 239.

[2148] Official Comment Nr. 3 d zu § 605 UCITA, *UCITA*, S. 240.

[2149] Da die technischen Schutzmaßnahmen nur zur Durchsetzung wirksamer Vertragsbedingungen eingesetzt werden dürfen, hängt die Zulässigkeit der technischen Schutzmaßnahmen aber letztlich von der Wirksamkeit der Nutzungsverträge ab. Hier stellen sich Fragen „preemption doctrine" und der „public policy"-Bestimmung des UCITA; s. dazu oben Teil 3, B III 1, S. 304 ff., und B III 2, S. 308. Zu dieser Abhängigkeit kritisch *Cohen*, 13 Berkeley Tech. L. J. 1089, 1097 f. (1998).

[2150] Die Aufzählung in § 605 (b) UCITA ist alternativ, nicht kumulativ zu verstehen, s. Official Comment Nr. 3 zu § 605 UCITA, *UCITA*, S. 239.

[2151] Zwar verabschiedete das NCCUSL Executive Committee im Januar 2001 eine Änderung des § 605 UCITA, die im August 2001 von der Vollversammlung der NCCUSL angenommen werden soll. Danach soll in § 605 (f) UCITA das Verhältnis zu § 816 UCITA klargestellt werden, wobei auch auf „mass-market licenses" eingegangen wird. Dabei handelt es sich allerdings nur um einen speziellen Fall im Schnittfeld zwischen § 605 und § 816 UCITA, der die grundsätzliche Anwendbarkeit des § 605 UCITA auf „mass-market licenses" nicht beseitigt. Der Text des Änderungsvorschlags ist unter <http://www.ucitaonline.com/docs/0101a.htm> abrufbar. Aktuelle Informationen zum Stand des UCITA finden sich unter <http://www.ucitaonline.com>.

[2152] Der Official Comment Nr.2 zu § 605 UCITA, *UCITA*, S. 238 f., stellt selbst die Parallele zum rechtlichen Umgehungsschutz nach 17 U.S.C. § 1201 (Digital Millennium Copyright Act) her.

men haben. Diese Regelungen setzen regelmäßig am rechtlichen Umgehungsschutz technischer Schutzmaßnahmen an.[2153]

a) Europäischer Rechtsrahmen

aa) Art. 6 Abs. 4 Richtlinie zum Urheberrecht in der Informationsgesellschaft

Das Verhältnis zwischen urheberrechtlichen Schrankenbestimmungen und dem rechtlichen Umgehungsschutz war einer der umstrittensten Punkte in der Entstehungsgeschichte der Richtlinie zum Urheberrecht in der Informationsgesellschaft.[2154] Die diesbezüglichen Regelungen unterscheiden sich in den einzelnen Entwurfsfassungen erheblich. Erst im Frühsommer 2000 konnte man sich bei den Verhandlungen auf eine grobe Linie einigen, von der in der Folgezeit nur noch in Einzelheiten abgewichen wurde. In der Endfassung der Richtlinie findet sich in Art. 6 Abs. 4 eine ausführliche und schwer durchschaubare Regelung zum Verhältnis zwischen urheberrechtlichen Schrankenbestimmungen und rechtlichem Umgehungsschutz.[2155] Die folgenden Ausführungen beschränken sich auf die Darstellung der Regelung in ihrer Endfassung.[2156]

(1) **Ausgangspunkt: Gesetzliche Verpflichtung zum „Key Escrow".** Grundsätzlich sind die Mitgliedstaaten nach Art. 6 Abs. 4 der Richtlinie unter engen Voraussetzungen berechtigt, „geeignete Maßnahmen" zu ergreifen, um dem Begünstigten einer urheberrechtlichen Schrankenbestimmung die Nutzung eines Werks zu ermöglichen, ohne davon durch eine technische Schutzmaßnahme abgehalten zu werden.[2157] Der Begriff der „geeigneten Maßnahme" des Mitgliedstaats ist nicht näher definiert. Durch diese Maßnahme soll aber sichergestellt werden, daß die Rechteinhaber dem Begünstigten die Mittel zur Verfügung stellen, die der Begünstigte zur Umgehung der technischen Schutzmaßnahme benötigt. Damit verfolgt die europäische Richtlinie grundsätzlich einen „key escrow"-Ansatz, wie er

---

[2153] Auch hier wird nur exemplarisch auf einige Regelungskomplexe eingegangen. Zur Problematik bei den WIPO-Verträgen s. *Wand*, S. 43 f.

[2154] S. zur Richtlinie allgemein oben Teil 2, D I 2 a bb 1.

[2155] Im folgenden kann nur ein grober Überblick über die gesamte Regelung gegeben werden. Zusätzlich findet sich in Erwägungsgrund 48 die Aussage, daß durch den rechtlichen Umgehungsschutz die „Forschungsarbeiten im Bereich der Verschlüsselungstechniken" nicht behindert werden dürften, ABl. EG Nr. L 167 vom 22. 6. 2001, S. 10, 14. Was das im einzelnen bedeutet, wird nicht gesagt.

[2156] Frühere Entwurfsfassungen werden hinsichtlich des Verhältnisses von Schrankenbestimmungen und rechtlichem Umgehungsschutz untersucht von *Bechtold* in: Hoeren/Sieber (Hrsg.), Kap. 7.11, Rdnr. 40; *Wand*, S. 105 f.; *Koelman*, EIPR 2000, 272, 273 ff.; *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 192 ff. S. a. Begründung des Rates zum Gemeinsamen Standpunkt Nr. 43, *Rat der Europäischen Union*, ABl. EG Nr. C 344 vom 1. 12. 2000, S. 19.

[2157] Zusätzliche Voraussetzung ist, daß der betreffende Begünstigte rechtmäßigen Zugang zu dem geschützten Werk hat, also beispielsweise der berechtigte Inhaber einer Werkkopie ist.

oben dargestellt wurde.[2158] Allerdings scheint auch eine direkte gesetzliche Regulierung technischer Schutzmaßnahmen[2159] zulässig zu sein.[2160] Dagegen ist wohl keine gesetzliche Beschränkung des rechtlichen Umgehungsschutzes („right to hack") möglich, wie dies im U.S.-amerikanischen „Digital Millennium Copyright Act" der Fall ist.[2161]

(2) **Einschränkungen.** Der Handlungsspielraum der Mitgliedstaaten, ein „key escrow"-System zu etablieren, wird jedoch in dreifacher Hinsicht bedeutend eingeschränkt.

(a) **Vorrang „freiwilliger Maßnahmen".** Art. 6 Abs. 4 der Richtlinie setzt zunächst auf „freiwillige Maßnahmen" der Rechteinhaber, „einschließlich Vereinbarungen zwischen den Rechteinhabern und anderen betroffenen Parteien". Danach könnten sich die Rechteinhaber beispielsweise in einem Vertrag mit Bibliotheksverbänden und ähnlichen Institutionen verpflichten, den Verbandsmitgliedern in berechtigten Fällen Umgehungsvorrichtungen zur Verfügung zu stellen, damit diese von urheberrechtlichen Schrankenbestimmungen profitieren können. Nur wenn die Rechteinhaber nicht auf freiwilliger Basis Maßnahmen ergreifen, um den Begünstigten urheberrechtlicher Schrankenbestimmungen die Nutzung der Werke zu ermöglichen, können die Mitgliedstaaten tätig werden und solche Maßnahmen erzwingen.[2162]

[2158] S. oben Teil 4, D I 2 d.

[2159] S. dazu allgemein oben Teil 4, D I 2 a.

[2160] Dies ist wohl gemeint, wenn es in Erwägungsgrund 51 der Richtlinie heißt: „Werden innerhalb einer angemessenen Frist keine derartigen freiwilligen Maßnahmen oder Vereinbarungen getroffen, sollten die Mitgliedstaaten angemessene Maßnahmen ergreifen, um zu gewährleisten, daß die Rechteinhaber *durch Änderung einer schon angewandten technischen Maßnahme* oder durch andere Mittel den von derartigen Ausnahmen oder Beschränkungen Begünstigten geeignete Mittel für die Inanspruchnahme dieser Ausnahmen oder Beschränkungen an die Hand geben", ABl. EG Nr. L 167 vom 22. 6. 2001, S. 10, 14; s. a. *Vinje*, EIPR 2000, 551, 556. Enger dagegen *v. Lewinski/Walter* in: Walter (Hrsg.), Info-RL, Kap. VII, Rdnr. 157.

[2161] Insoweit noch anders *Bechtold* in: Hoeren/Sieber (Hrsg.), Kap. 7.11, Rdnr. 43. S. zu dieser Regulierungsoption oben Teil 4, D I 2 c. Zum DMCA s. unten Teil 4, D II 3 c aa.

[2162] Dabei genießen diese Maßnahmen selbst wiederum den Rechtsschutz des Art. 6 Abs. 1, s. Art. 6 Abs. 4 Unterabs. 3 der Richtlinie. Die Richtlinie schweigt darüber, ab wann die Mitgliedstaaten zu „angemessenen Maßnahmen" berechtigt sind; in Erwägungsgrund 51 wird lediglich eine „angemessene Frist" gefordert, s. ABl. EG Nr. L 167 vom 22. 6. 2001, S. 10, 14; s. dazu *v. Lewinski/Walter* in: Walter (Hrsg.), Info-RL, Kap. VII, Rdnr. 159; *Vinje*, EIPR 2000, 551, 557. Die Verständlichkeit der Vorschrift wird unnötigerweise erschwert, da die Richtlinie den Begriff der „Maßnahme" nebeneinander in unterschiedlichen Bedeutungszusammenhängen verwendet; so ist einerseits von „freiwilligen Maßnahmen der Rechtsinhaber", andererseits von „geeigneten Maßnahmen der Mitgliedstaaten" die Rede. Zu allem Überfluß spricht Art. 6 Abs. 4 Unterabs. 2 dann noch von „geeigneten Maßnahmen", worunter weder „geeignete Maßnahmen der Mitgliedstaten" noch „freiwillige Maßnahmen der Rechtsinhaber", sondern vielmehr normale technische Schutzmaßnahmen i. S. d. Art. 6 Abs. 1 der Richtlinie zu verstehen sind.

(b) **Abstufung hinsichtlich unterschiedlicher Schrankenbestimmungen.** Bei bestimmten Schrankenbestimmungen – unter anderem Vervielfältigungen durch öffentliche Bibliotheken, vorübergehende Aufzeichnungen durch Sendeunternehmen und Nutzung zur wissenschaftlichen Forschung – sind die Mitgliedstaaten *verpflichtet*, „geeignete Maßnahmen" zu ergreifen, falls die Rechteinhaber nicht selbst „freiwillige Maßnahmen" treffen, Art. 6 Abs. 4 Unterabs. 1 der Richtlinie. Bei anderen Schrankenbestimmungen – nämlich jener bezüglich der Vervielfältigung zum privaten Gebrauch[2163] – sind die Mitgliedstaaten dazu nur unter bestimmten Voraussetzungen *berechtigt*, Art. 6 Abs. 4 Unterabs. 2 der Richtlinie.[2164] Bei wiederum anderen Schrankenbestimmungen sind die Mitgliedstaaten *nicht einmal berechtigt*, solche „geeigneten Maßnahmen" zu ergreifen. Diese letzte Gruppe von Schrankenbestimmungen erfaßt unter anderem das Zitatrecht und die Verwendung geschützter Werke zu Zwecken der Kritik oder Parodie. Die tiefere Logik einer Regelung, die unter gewissen Umständen die Umgehung technischer Schutzmaßnahmen erlaubt, wenn dadurch Werke zu Forschungszwecken genutzt werden können,[2165] die aber die Umgehung verbietet, wenn es um die Kritik oder Parodie von Werken geht,[2166] bleibt unklar.[2167]

(c) **Abhängigkeit vom gewählten Geschäftsmodell.** Schließlich ist es den Mitgliedstaaten versagt, bezüglich irgendeiner der Schrankenbestimmungen geeignete Maßnahmen[2168] zu treffen, wenn die technisch geschützten Werke der Öffentlichkeit „aufgrund einer vertraglichen Vereinbarung in

[2163] Es handelt sich um Art. 5 Abs. 2 lit. b der Richtlinie. Zwar enthält Art. 5 Abs. 2 lit. a eine ähnliche Ausnahme, die unter Art. 6 Abs. 4 Unterabs. 1 fällt. Sie bezieht sich jedoch nur auf fotomechanische Vervielfältigungen analoger Art; s. dazu *Walter* in: Walter (Hrsg.), Info-RL, Kap. IV, Rdnr. 117 ff. Darum geht es bei bei DRM-Systemen jedoch nicht.

[2164] Selbst wenn der Mitgliedstaat in diesem Fall „geeignete Maßnahmen" ergreift, ist der Inhalteanbieter nicht gehindert, seinerseits mittels technischer Schutzmaßnahmen die Anzahl der Kopien, die erstellt werden können, zu kontrollieren, s. Art. 6 Abs. 4 Unterabs. 2 a. E. der Richtlinie.

[2165] Art. 6 Abs. 4 Unterabs. 1 i. V. m. Art. 5 Abs. 3 lit. a der Richtlinie.

[2166] Die Schrankenbestimmungen der Art. 5 Abs. 3 lit. d und lit. k finden sich – neben vielen anderen Schrankenbestimmungen – in der Aufzählung des Art. 6 Abs. 4 nicht wieder. Natürlich kann ein Schriftwerk auch kritisiert werden, indem man dieses nur beschreibt, so daß man in einem DRM-System keine technischen Schutzmaßnahmen des Werks manipulieren müßte. Bei Art. 5 Abs. 3 lit. d geht es aber um die Fälle, in denen zu Zwecken der Kritik aus einem Werk zitiert wird. Verhindert ein DRM-System das Kopieren von Ausschnitten des digitalen Inhalts – dies können nicht nur Text, sondern auch Musikstücke oder Videofilme sein –, so sieht Art. 6 Abs. 4 keine Möglichkeit vor, diesen technischen Schutz entsprechend der Schrankenbestimmung des Art. 5 Abs. 3 lit. d zu begrenzen. Zwar könnte man einwenden, es bliebe immer noch die analoge Kopie möglich (Abschreiben, neu Aufnehmen, Abfilmen). Wie oben dargelegt wurde, ist eine solche „Schrankenbestimmung minderwertiger Qualität" jedoch abzulehnen; s. dazu oben bei Fn. 1959 ff.

[2167] Ebenfalls kritisch *Kröger*, CR 2001, 316, 323 f.

[2168] S. zu diesem Begriff immer bei Fn. 2157.

einer Weise zugänglich gemacht werden, daß sie Mitgliedern der Öffentlichkeit von Orten und zu Zeiten ihrer Wahl zugänglich sind", Art. 6 Abs. 4 Unterabs. 4 der Richtlinie. Mit dieser Formulierung ist das „right of communication to the public" im Sinne des Art. 3 Abs. 2 der Richtlinie gemeint. Unter dieses neu eingeführte Verwertungsrecht kann eine Vielzahl von Online-DRM-Diensten subsumiert werden, ist doch nur erforderlich, daß der Nutzer den einzelnen digitalen Inhalt zu einer beliebigen Zeit individuell auswählen und nutzen kann, s. Art. 3 Abs. 2 der Richtlinie.[2169] Bietet ein Inhalteanbieter in einem DRM-System digitale Inhalte derart zum Abruf an,[2170] daß die Nutzer vor der Nutzung einen Nutzungsvertrag abschließen müssen,[2171] so sind die Mitgliedstaaten überhaupt nicht berechtigt, den Inhalteanbieter zu verpflichten, durch die Bereitstellung entsprechender Umgehungsvorrichtungen die Ausnutzung urheberrechtlicher Schrankenbestimmungen zu ermöglichen. In diesem Fall ist der Inhalteanbieter damit faktisch *an keinerlei Schrankenbestimmungen gebunden*.[2172] Dies bedeutet faktisch, daß sich der Inhalteanbieter durch die Wahl eines bestimmten Geschäftsmodells urheberrechtlicher Schrankenbestimmungen entledigen kann.[2173]

[2169] Zur Reichweite dieses Verwertungsrechts s. a. *Walter* in: Walter (Hrsg.), Info-RL, Kap. III, Rdnr. 81 ff.; Erwägungsgrund 25 der Richtlinie, ABl. EG Nr. L 167 vom 22. 6. 2001, S. 10, 12.

[2170] Dies wird in einem Online-DRM-System regelmäßig der Fall sein. Auch ein Abonnementdienst, in dem der Nutzer eine monatliche Pauschalgebühr zahlt, dann aber individuellen Zugriff auf ein großes Musikarchiv hat, fällt darunter. Anderes gilt nur, wenn es sich beispielsweise um einen radioähnlichen Dienst handelt, der ständig vorausgewählte Inhalte überträgt.

[2171] Dabei genügt auch der Abschluß eines Formularvertrags. Die deutsche Fassung der Richtlinie spricht nur von einer „vertraglichen Vereinbarung", während die englische Fassung genauer von „agreed contractual terms" (im Gegensatz zu „negotiated contractual terms") spricht.

[2172] Bietet der Inhalteanbieter dagegen seine Inhalte in einem radioähnlichen Dienst an, in dem der Nutzer die einzelnen Inhalte nicht individuell auswählen kann, greift Art. 6 Abs. 4 Unterabs. 4 nicht ein.

[2173] Das Europäische Parlament versuchte die weitreichenden Folgen des Art. 6 Abs. 4 Unterabs. 4 der Richtlinie augenscheinlich abzumildern, indem es in zweiter Lesung einen neuen Erwägungsgrund einfügte, wonach die Ausnahme des Art.6 Abs. 4 Unterabs. 4 nur für die „Erbringung interaktiver Dienste auf Abruf auf der Grundlage von vertraglichen Vereinbarungen", nicht aber für „sonstige Formen nicht-interaktiver Online-Nutzungen" gelte; diese Formulierung findet sich nun in Erwägungsgrund 53 der Richtlinie, ABl. EG Nr. L 167 vom 22. 6. 2001, S. 10, 14. Inhaltlich ändert dies freilich nichts. Eine klare Definition des Begriffs „interaktive Online-Nutzung" existiert nicht. Nahezu jede Online-Nutzung kann als „interaktiv" aufgefaßt werden. Außerdem ändert der Erwägungsgrund nichts an der Formulierung der eigentlichen Richtlinienvorschrift. Auch gibt es informelle Verlautbarungen aus den Reihen der Kommission, die Vorschrift beziehe sich nur auf „Video-on-Demand"-Dienstleistungen und ähnliches, s. *Vinje*, EIPR 2000, 551, 557. Einerseits erscheint fraglich, ob durch eine solche Auslegung eine wirkliche Beschränkung des Art. 6 Abs. 4 Unterabs. 4 erreicht werden kann. Andererseits handelt es sich eben auch nur um informelle Verlautbarungen, die sich nicht im Wortlaut der Richtlinie niedergeschlagen haben.

(3) **Beurteilung.** Bedenkt man, daß das Anbieten digitaler Inhalte zum individuellen Abruf in Online-DRM-Systemen das am weitesten verbreitete Geschäftsmodell ist[2174] und auf absehbare Zeit bleiben wird, so zeigt sich, daß die Vorschrift des Art. 6 Abs. 4 Unterabs. 4 der Richtlinie in aller Regel für Online-DRM-Systeme einschlägig ist. Die Richtlinie billigt damit, daß technische Schutzmaßnahmen alle urheberrechtlichen Schrankenbestimmungen umgehen können. Wie oben dargelegt wurde, ist es nach der Richtlinie auch zulässig, Schrankenbestimmungen durch vertragliche Vereinbarungen auszuhebeln.[2175] Zusammengenommen ergibt dies, daß sich Inhalteanbieter in Online-DRM-Systemen unter der Geltung der Richtlinie problemlos lästiger urheberrechtlicher Schrankenbestimmungen entledigen könen. Die Richtlinie unterstützt in hohem Maße die oben dargestellte „Privatisierung des Rechtsschutzes".[2176] Vergleicht man die europäische Richtlinie mit der Rechtslage in den USA, handelt es sich faktisch um die legislative Ausprägung der Grundgedanken der U.S.-amerikanischen ProCD-Entscheidung in potenzierter Form.[2177]

Selbst wenn man Art. 6 Abs. 4 Unterabs. 4 der Richtlinie außer Betracht läßt, muß sich der restliche Art. 6 Abs. 4 einiges an Kritik gefallen lassen. Wichtige Schlüsselbegriffe[2178] werden nicht definiert, ja nicht einmal erläutert.[2179] Es zeigt sich, daß die Richtlinie bezüglich der Interessen der Allgemeinheit primär auf freiwillige Vereinbarungen mit den Rechteinhabern ohne staatliche Intervention setzt. Ob das Ergebnis dieses komplexen Ineinandergreifens privater und staatlicher Akteure ein gerechter Interessenausgleich sein wird, ist angesichts der erfolgten rechtlichen und rechtsökonomischen Analyse zumindest eine offene Frage.[2180]

[2174] Darunter fallen auch viele Abonnementdienste, s. dazu oben Fn. 2170.

[2175] S. dazu oben bei Fn. 1992.

[2176] S. a. *Vinje*, EIPR 2000, 551, 557.

[2177] Diese Ausführungen gelten aber nur im Online-Bereich. Geht es um DRM-Systeme, bei denen Inhalte offline vertrieben werden (DVDs u. ä.), greift diese Kritik nicht, da Art. 6 Abs. 4 Unterabs. 4 der Richtlinie nicht einschlägig ist.

[2178] Es seien nur „geeignete Maßnahmen", „freiwillige Maßnahmen", „Vereinbarungen zwischen den Rechteinhabern und anderen betroffenen Parteien" und „betroffene Parteien" erwähnt. Zu der verwirrenden Verwendung des Begriffs der „Maßnahme" s. oben Fn. 2162.

[2179] Ebenso kritisch *Hugenholtz*, EIPR 2000, 499, 500, der meint: „The only legal security this type of lawmaking creates is the certainty of another round of lobbying and infighting at the national level. Eventually […], the European Court of Justice, already overworked, will have to finish the job left largely undone by the European legislature". Aus diesen und aus anderen Gründen fragt sich *Hugenholtz*, ob die Richtlinie überhaupt eine harmonisierende Wirkung habe. Er bezweifelt dies stark und zieht damit gleichzeitig die Kompetenz der Europäischen Union zum Erlaß der Richtlinie in Frage; s. dazu *ebda.*, 501 f.; vgl. weiterhin *Vinje*, EIPR 2000, 551 ff.

[2180] S. a. *Kröger*, CR 2001, 316, 322, sowie *Vinje*, EIPR 2000, 551, 556 ff., der in seiner Kritik allerdings nicht ganz so weit geht.

Bei Art. 6 Abs. 4 der Richtlinie, der eigentlich die Interessen der Allgemeinheit schützen soll, handelt es sich um einen zahnlosen Tiger.

bb) Sonstige Richtlinien

In anderen europäischen Urheberrechtsrichtlinien finden sich keine ausdrücklichen Regelungen, die das Verhältnis technischer Schutzmaßnahmen zu urheberrechtlichen Schrankenbestimmungen regeln. So ist das Verhältnis des rechtlichen Umgehungsschutzes in Art. 7 Abs. 1 lit. c der Computerprogrammrichtlinie[2181] zu den Schrankenbestimmungen der Art. 5 und 6 Computerprogrammrichtlinie unklar. Die Computerprogrammrichtlinie statuiert keine ausdrücklichen Ausnahmen vom rechtlichen Umgehungsschutz. Ob die Schrankenbestimmungen der Art. 5 und 6 den rechtlichen Umgehungsschutz des Art. 7 Abs. 1 lit. c begrenzen, ist umstritten.[2182]

Die Zugangskontrollrichtlinie[2183] kennt keinerlei Beschränkungen des rechtlichen Umgehungsschutzes. Dies erscheint besonders problematisch, da sich der Regelungsbereich dieser Richtlinie mit dem Regelungsbereich des Umgehungsschutzes nach der Richtlinie zum Urheberrecht in der Informationsgesellschaft überschneidet.[2184] Der Zugang zu digitalen Inhalten und deren Nutzung lassen sich bei wirtschaftlicher Betrachtungsweise oftmals nicht trennen. Enthält der rechtliche Umgehungsschutz von Nutzungskontrollmaßnahmen[2185] Beschränkungen, während der rechtliche Umgehungsschutz von Zugangskontrollmaßnahmen keinen Beschränkungen unterliegt, so können die bestehenden Beschränkungen ins Leere laufen: Durch ein vorgeschaltetes Zugangskontrollrecht können Beschränkungen von Nutzungskontrollmaßnahmen und urheberrechtliche Schrankenbestimmungen unterlaufen werden, da der Rechteinhaber durch eine umfangreiche Zugangskontrolle mittelbar auch die Nutzung des Werks kontrollieren kann.[2186]

[2181] S. dazu oben Teil 2, D I 2 b b 2.

[2182] Vgl. *Wand*, S. 72 f., 126 ff., einerseits und *Walter* in: Walter (Hrsg.), Software-RL, Art. 7 Rdnr. 15, andererseits; s. weiterhin *Marly*, K&R 1999, 106, 107. In der vorliegenden Untersuchung wird darauf noch im Rahmen des deutschen Rechts eingegangen, da Art. 7 Abs. 1 lit. c der Computerprogrammrichtlinie in § 69 f Abs. 2 UrhG umsetzt; s. unten Teil 4, D II 3 b bb.

[2183] S. dazu allgemein oben Teil 3, D I 2 b bb 3.

[2184] S. dazu oben Teil 3, D I 2 b bb 3 bb.

[2185] Damit ist Art. 6 der Richtlinie zum Urheberrecht in der Informationsgesellschaft gemeint. Auf die Unschärfe des Begriffs der „Nutzungskontrolle" wurde schon in Fn. 1121 hingewiesen.

[2186] S. dazu ausführlich *Heide*, 15 Berkeley Tech. L. J. 993, 1026 ff. (2000). Ähnlich wie *Heide* plädiert *Ginsburg*, From Having Copies to Experiencing Works, S. 3, im Bereich des U.S.-amerikanischen Rechts dafür, das „access right" als integralen Bestandteil des Urheberrechts aufzufassen und vergleichbaren Schrankenbestimmungen zu unterwerfen wie die herkömmlichen Verwertungsrechte. Ebenso *Goldstein*, Copyright, § 5.17.1, S. 5:248.

b) Deutscher Rechtsrahmen

aa) Entwurf eines 5. Urheberrechts-Änderungsgesetzes

Der Entwurf eines 5. Urheberrechts-Änderungsgesetzes[2187] stammt aus dem Jahr 1998. Seine Regelungen zum rechtlichen Umgehungsschutz müssen den starken Änderungen angepaßt werden, denen die europäische Richtlinie zum Urheberrecht in der Informationsgesellschaft seit 1998 bis zu ihrer Verabschiedung 2001 unterworfen war. Dennoch sollen die Regelungen des deutschen Gesetzesentwurfs zum Verhältnis des rechtlichen Umgehungsschutzes zu urheberrechtlichen Schrankenbestimmungen kurz dargestellt werden, da sie eine recht erstaunliche Grundhaltung zeigen. In dem Gesetzesentwurf findet sich keinerlei Beschränkung des rechtlichen Umgehungsschutzes.[2188] Die Begründung stellt ausdrücklich klar, daß die Umgehung einer technischen Schutzmaßnahme „auch dann verboten ist, wenn sie zum Zweck einer nach den §§ 45 ff. zulässigen Verwertungshandlung erfolgt."[2189] Es liege in der Natur technischer Schutzmaßnahmen, daß deren Wirkungsweise vom Vorliegen oder Nichtvorliegen bestimmter, die Zulässigkeit einer Verwertungshandlung begründender Umstände unabhängig sei. Werde die Umgehung technischer Schutzmaßnahmen in bestimmten Fällen erlaubt, so verliere der Rechteinhaber zugleich auch den (technischen) Schutz gegen eventuelle künftige rechtsverletzende Handlungen. Daher sei es geboten, daß der rechtliche Umgehungsschutz an die abstrakte Eignung der technischen Schutzmaßnahmen zum Schutz vor Rechtsverletzungen anknüpfe.[2190] Eine Beschränkung des rechtlichen Umgehungsschutzes komme daher nicht in Betracht. Die einzige Beschränkung, die der Entwurf anerkennen will, ist die Regelung der urheberrechtlichen Schutzfrist in § 64 UrhG. Nach dem Entwurf dient eine technische Schutzmaßnahme nach Ablauf der urheberrechtlichen Schutzfrist nicht mehr dem Schutz vor einer „Rechtsverletzung", so daß der rechtliche Umgehungsschutz nicht mehr eingreife.[2191] Außer der zeitlichen Beschränkung sieht der Gesetzesentwurf damit keinerlei Beschränkung des rechtlichen Umgehungsschutzes vor. Wäre der Entwurf geltendes Recht, würde er das Gleichgewicht zwischen den Interessen der Rechteinhaber und der Allgemeinheit, den das

[2187] S. dazu allgemein Teil 2, D I 2 a cc 1.

[2188] Nach § 96 a UrhG-E dürfen „technische Vorrichtungen […] ohne *Erlaubnis des Rechtsinhabers* nicht umgangen […] werden." Eine Formulierung, daß sich eine solche Erlaubnis auch aus gesetzlichen Vorschriften ergeben könnte, fehlt. Diesen Weg hatten frühe Entwürfe der Richtlinie zum Urheberrecht in der Informationsgesellschaft gewählt. S. a. *Wand*, S. 169, 175 ff.; *Marly*, K&R 1999, 106, 109.

[2189] *Bundesministerium der Justiz*, Begründung zum 5. UrhGÄndG-Entwurf, S. 23.

[2190] *Bundesministerium der Justiz*, Begründung zum 5. UrhGÄndG-Entwurf, S. 23 f.

[2191] *Bundesministerium der Justiz*, Begründung zum 5. UrhGÄndG-Entwurf, S. 24.

Urheberrecht zu schaffen versucht, gleichsam durch die Hintertür zerstören.[2192]

bb) Sonstige Vorschriften

Beim rechtlichen Umgehungsschutz des § 69 f Abs. 2 UrhG ist das Verhältnis zu urheberrechtlichen Schrankenbestimmungen umstritten. Der Gesetzgeber hat das Problem gesehen, aber nicht gelöst.[2193] Vornehmlich geht es um das Verhältnis zu § 69 d und § 69 e UrhG. Das UrhG statuiert selbst keine ausdrücklichen Ausnahmen zum Umgehungsschutz des § 69 f Abs. 2 UrhG. Die §§ 69 d und 69 e sind nach ihrem Wortlaut lediglich Schrankenbestimmungen zu den in § 69 c UrhG geregelten Verwertungsrechten.[2194] Auslegungstechnisch knüpft der Meinungsstreit an die Formulierung des § 69 f Abs. 2 UrhG an, wonach Umgehungsvorrichtungen verboten sind, die die *unerlaubte* Beseitigung oder Umgehung technischer Schutzmaßnahmen erleichtern. Unklar ist, ob unter einer solchen „Erlaubnis" auch eine gesetzliche Erlaubnis zu verstehen ist. Dann könnten die Vorschriften der §§ 69 d und 69 e als Fälle einer solchen gesetzlichen Erlaubnis angesehen werden. Daher ist streitig, ob trotz § 69 f Abs. 2 UrhG Umgehungsvorrichtungen angeboten werden dürfen, die zur Fehlerberichtigung des Computerprogramms verwendet werden können, s. § 69 d Abs. 1 UrhG.[2195] Umstritten ist auch, ob Umgehungsvorrichtungen angeboten werden dürfen, die die Erstellung von Sicherungskopien ermöglichen, s. § 69 d Abs. 2 UrhG.[2196] Schließlich ist fraglich, ob Umgehungsvorrichtungen angeboten werden dürfen, die eine Dekompilierung von Computersoftware erlauben, s. § 69 e UrhG.[2197]

[2192] Ebenfalls kritisch *Marly*, K&R 1999, 106, 109; *Dreier*, CR 2000, 45, 47. Für eine vollständige Analyse dieser These müßten aber die Auswirkungen eines unbeschränkten Umgehungsschutzes auf die Ziele der einzelnen Schrankenbestimmungen des UrhG untersucht werden; s. dazu *Wand*, S. 175 ff., der grundsätzlich keine Beschränkungen des rechtlichen Umgehungsschutzes befürwortet, jedoch Ausnahmen bezüglich einzelner urheberrechtlicher Schrankenbestimmungen macht.

[2193] „Nicht geklärt hat die Richtlinie das Verhältnis zwischen dem Recht auf Sicherungskopie (Art. 5 Abs. 1 und 2) und dem Schutz von Kopierschutzmechanismen (Art. 7 Abs. 1 c)"; *Bundesregierung*, BT-Drs. 10/4022 vom 18. 12. 1992, S. 12. Die deutsche Gesetzesbegründung klärt das Verhältnis freilich ebenfalls nicht.

[2194] *Wand*, S. 147.

[2195] S. dazu *Raubenheimer*, CR 1996, 69, 72 ff.; *König*, NJW 1995, 3293, 3294 f.; ablehnend *Wand*, S. 148; vgl. weiterhin OLG München, CR 1996, 11, 16 f.

[2196] Bejahend *Raubenheimer*, CR 1994, 129, 131; *König*, NJW 1995, 3293, 3295; *Nordemann/Vinck* in: Fromm/Nordemannn (Hrsg.), § 69 f Rdnr. 3; ablehnend *Wand*, S. 148; *Loewenheim* in: Schricker (Hrsg.), UrhG-Kommentar, § 69 f Rdnr. 11.

[2197] Bejahend *Wand*, S. 149. *Wand* meint, grundsätzlich werde § 69 f Abs. 2 UrhG durch urheberrechtliche Schrankenbestimmungen nicht begrenzt. Nur so sei ein effektiver Rechtsschutz möglich. Ansonsten würde Schutzbehauptungen Tür und Tor geöffnet. Er macht jedoch für § 69 e UrhG eine Ausnahme von diesem Grundsatz. S. *Wand*, S. 147 ff. Weiterhin besteht Streit zu der Frage, ob die tatsächliche Umgehung einer technischen Schutzmaßnahme, die regelmäßig zu einer Umarbeitung und Vervielfältigung i. S. d. § 69 c Nr. 1 und 2 UrhG führt, aufgrund der §§ 69 d oder 69 e gerechtfer-

c) U.S.-amerikanischer Rechtsrahmen

Der „Digital Millennium Copyright Act" (DMCA) enthält in 17 U.S.C. § 1201 einen umfassenden rechtlichen Umgehungsschutz technischer Schutzmaßnahmen, die den Zugang zu digitalen Inhalten oder deren Nutzung kontrollieren.[2198] Dieser Umgehungsschutz wird durch mehrere spezifische Schrankenbestimmungen beschränkt (dazu unten aa). Auch wird diskutiert, ob zusätzlich allgemeine Schrankenbestimmungen des Urheberrechts auf den rechtlichen Umgehungsschutz anwendbar sind (dazu unten bb).[2199]

aa) Ausdrückliche Schrankenbestimmungen des DMCA

17 U.S.C. § 1201 enthält in den Absätzen (d) – (j) ausführliche Bestimmungen, die den rechtlichen Umgehungsschutz beschränken.[2200] In diesen Fällen wird den technischen Schutzmaßnahmen ein rechtlicher Schutz versagt. Dem Nutzer steht also ein „right to hack" zu.[2201] So findet sich in 17 U.S.C. § 1201 (d) eine Schrankenbestimmung für Bibliotheken, Archive und Bildungseinrichtungen und in Absatz (e) eine Schrankenbestimmungen für staatliche Ermittlungs- und Nachrichtenbehörden. Unter den Voraussetzungen des Absatzes (f) darf ein Nutzer die technischen Schutzmaßnahmen eines Computerprogramms umgehen, wenn dies zum „Reverse Engineering" des Programms notwendig ist. Nach Absatz (g) können technische Schutzmaßnahmen umgangen werden, wenn dies zu Forschungszwecken im Bereich der Kryptographie-Forschung notwendig ist. Absatz (i) erlaubt die Umgehung technischer Schutzmaßnahmen, wenn diese Schutzmaßnahmen ohne Wissen der Nutzer Nutzungsprofile erstellen und durch die Umgehung das Sammeln personenbezogener Daten verhindert werden soll. Damit soll datenschutzrechtlichen Bedenken Rechnung getragen werden.[2202] Schließlich können Schutzmaßnahmen

tigt sein kann. Dies ist keine Problematik des § 69 f Abs. 2 UrhG, erfaßt dieser rechtliche Umgehungsschutz doch nur vorbereitende Handlungen und nicht die tatsächlich Umgehungshandlung. Auf jenen Streit wird hier nicht näher eingegangen; s. dazu OLG Düsseldorf, CR 1997, 337, 338 f.; OLG Karlsruhe, CR 1996, 341, 342 m. Anm. *Raubenheimer*; LG Mannheim, NJW 1995, 3322; *Loewenheim* in: Schricker (Hrsg.), UrhG-Kommentar, § 69 d Rdnr. 10; *Bechtold* in: Hoeren/Sieber (Hrsg.), Teil 7.11, Rdnr. 55.

[2198] S. dazu ausführlich oben Teil 2, D I 2 a dd und D I 2 b dd.

[2199] Daneben existieren auch Schrankenbestimmungen für den rechtlichen Schutz von Metadaten in 17 U.S.C. § 1202; s. dazu *Wand*, S. 250 f.; *N. B. Nimmer/D. Nimmer*, § 12A.10, S. 12A-108 ff. Die Vorschrift und ihre Schrankenbestimmungen sind für die vorliegende Frage der Beschränkung des rechtlichen Umgehungsschutzes aber nicht relevant.

[2200] S. dazu im Überblick *Wand*, S. 236 ff.; *N. B. Nimmer/D. Nimmer*, § 12A.04 f., S. 12A-34 ff.; *Ginsburg*, 23 Colum.-VLA J. L. & Arts 137, 148 ff. (1999).

[2201] Zu dieser Regulierungsmöglichkeit im allgemeinen s. oben Teil 4, D I 2 c.

[2202] S. zu dieser Frage auch 17 U.S.C. § 1205.

umgangen werden, wenn dies notwendig ist, um Sicherheitsschwächen eines Computersystems oder -netzwerks zu beiseitigen, Absatz (j).

Die kurze Übersicht erschließt die Komplexität der sieben Schrankenbestimmungen,[2203] die im vollen Gesetzestext fünf Druckseiten lang sind, nicht einmal annährungsweise. *Erstens* unterscheidet der DMCA zwischen technischen Schutzmaßnahmen, die den Zugang zu Inhalten kontrollieren (17 U.S.C. § 1201 (a)), und technischen Schutzmaßnahmen, die die Nutzung der Inhalte kontrollieren (17 U.S.C. § 1201 (b)). Während einige Schrankenbestimmungen nur bei Zugangskontrollmaßnahmen greifen,[2204] gelten andere Schrankenbestimmungen zusätzlich auch bei Nutzungskontrollmaßnahmen.[2205] *Zweitens* unterscheidet der DMCA zwischen tatsächlichen Umgehungshandlungen und vorbereitenden Handlungen. Während einige Schrankenbestimmungen nur bezüglich der tatsächlichen Umgehungshandlung greifen,[2206] erfassen andere Schrankenbestimmungen zusätzlich auch vorbereitende Handlungen.[2207] Von den Schrankenbestimmungen, die sowohl tatsächliche Umgehungshandlungen als auch vorbereitende Handlungen betreffen, beziehen sich manche allerdings nur vorbereitende Handlungen in bezug auf Zugangskontrollmaßnahmen,[2208] während andere auch vorbereitende Handlungen in bezug auf Nutzungskontrollmaßnahmen vom rechtlichen Umgehungsschutz ausnehmen.[2209]

[2203] Auf die siebte Schrankenbestimmung bezüglich des Jugendschutz in Abs. (h), wird hier nicht näher eingegangen, s. dazu *D. Nimmer*, 46 J. Copyright Soc'y U.S.A. 401, 409 ff. (1999); *Ginsburg*, 23 Colum.-VLA J. L. & Arts 137, 150 f. (1999).

[2204] So die Schrankenbestimmung für Bibliotheken, Abs. (d) – s. dazu Abs. (d) (4) –, die Schrankenbestimmung für die Kryptographie-Forschung, Abs. (g), jene für den Datenschutz, Abs. (i), sowie jene für Sicherheitsüberprüfungen, Abs. (j).

[2205] So die Schrankenbestimmung für staatliche Ermittlungs- und Nachrichtendienste, Abs. (e), sowie die Schrankenbestimmung bezüglich des „Reverse Engineering" in Abs. (f).

[2206] So die Schrankenbestimmung für Bibliotheken, Abs. (d) – s. dazu Abs. (d) (4) –, sowie jene für den Datenschutz, Abs. (i).

[2207] So die Schrankenbestimmung für staatliche Ermittlungs- und Nachrichtendienste, Abs. (e), die Schrankenbestimmung bezüglich des „Reverse Engineering", Abs. (f), die Schrankenbestimmung für die Kryptographie-Forschung, Abs. (g), und für Sicherheitsüberprüfungen in Abs. (j). S. dazu auch *Samuelson*, 14 Berkeley Tech. L. J. 519, 535 (1999).

[2208] So die Schrankenbestimmung für die Kryptographie-Forschung, s. Abs. (g) (4), und die Schrankenbestimmung für Sicherheitsüberprüfungen, s. Abs. (j) (4). Beide Vorschriften zitieren bezüglich der vorbereitenden Handlungen nur Abs. (a) (2) – Zugangskontrollmaßnahmen –, nicht aber Abs. (b) – Nutzungskontrollmaßnahmen.

[2209] So wohl die Schrankenbestimmung für staatliche Ermittlungs- und Nachrichtendienste, Abs. (e), und die Schrankenbestimmung bezüglich des „Reverse Engineering", s. Abs. (f) (2). Hier zeigen sich Unstimmigkeiten des Gesetzes. Die Schrankenbestimmungen der Abs. (f) (2), (g) (4) und (j) (4) nehmen jeweils Vorrichtungen vom Umgehungsverbot aus, die den Zugangskontrollschutz nach Abs. (a) (2) verletzen würden. Im Falle der Schrankenbestimmung des Abs. (f) ist der Hersteller einer solchen Vorrichtung aber zugleich auch vom Nutzungskontrollschutz nach Abs. (b) freigestellt, wäh-

Schrankenbestimmungen, die nur die tatsächliche Umgehung technischer Schutzmaßnahmen vom rechtlichen Umgehungsschutz ausnehmen, sind sehr problematisch. Wie schon dargelegt wurde, sind viele Nutzer, die nach dieser Schrankenbestimmung berechtigt wären, eine technische Schutzmaßnahme zu umgehen, aufgrund fehlender eigener technischer Kenntnisse darauf angewiesen, daß am Markt Vorrichtungen oder Dienstleistungen erhältlich sind, mit denen die Schutzmaßnahme umgangen werden kann.[2210] Erfaßt die Schrankenbestimmung die Herstellung und Verbreitung dieser Vorrichtungen – also vorbereitende Handlungen – nicht, so werden Umgehungsvorrichtungen legalerweise nicht zu beschaffen sein. Damit läuft aber die gesamte Schrankenbestimmunge ins Leere. Nach Abs. (i) darf der Nutzer eines DRM-Systems Zugangskontrollmaßnahmen umgehen, um die Erstellung von personenbezogenen Nutzerprofilen zu vermeiden. Nach dem Wortlaut der Vorschrift ist allerdings niemand berechtigt, Umgehungsvorrichtungen herzustellen, mit denen der durchschnittliche Nutzer die Zugangskontrollmaßnahme umgehen kann. Theoretisch müßte der Nutzer die Umgehungsvorrichtung selbst entwickeln und dürfte sie an niemanden weitergeben – eine unrealistische Aussicht.[2211]

Drittens ist zu beachten, daß das Verbot der tatsächlichen Umgehung von Zugangskontrollmechanismen nach 17 U.S.C. § 1201 (a) (1) erst mit zweijähriger Verspätung am 28. 10. 2000 in Kraft trat.[2212] Der Kongreß hatte das „U.S. Copyright Office" der „Library of Congress" ermächtigt, während dieser Zeit eine Ausnahmeliste von Werkkategorien zu erstellen, bei denen das Verbot der tatsächlichen Umgehung nach 17 U.S.C. § 1201 (a) (1) nicht greifen soll.[2213] Nach einem umfangreichen Konsultations- und Anhörungsprozeß, in dem teilweise sehr weitgehende Ausnahmeregelungen gefordert wurden,[2214] bestimmte das „Copyright Office" zwei

rend das bei Abs. (g) (4) und (j) (4) nicht der Fall ist. S. dazu auch *Samuelson*, 14 Berkeley Tech. L. J. 519, 548 (1999).

[2210] S. dazu oben Teil 3, D I 2 bS. 316.

[2211] Vgl. *Samuelson*, 14 Berkeley Tech. L. J. 519, 554 (1999); *N. B. Nimmer/D. Nimmer*, § 12A.05[B][1], S. 12A-56; *Wand*, S. 243 f. Weitere Beispiele finden sich bei *D. Nimmer*, 148 U. Penn. L. Rev. 673, 727 ff. (2000).

[2212] S. schon oben Teil 2, D I 2 a dd 1 b.

[2213] Vgl. *Cohen*, EIPR 1999, 236, 237 ff.; *D. Nimmer*, 148 U. Penn. L. Rev. 673, 694 ff., 723 ff. (2000). Die Verfassungsmäßigkeit dieses Verfahrens zweifelt *Jiles*, 52 Admin. L. Rev. 443 (2000), unter dem Gesichtspunkt der Gewaltenteilung an.

[2214] So wurden Ausnahmen für DVDs, für Werke, die ausschließlich in einem DRM-geschützten Format erhältlich sind, für Videospiele, für Werke mit schwachem urheberrechtlichen Schutz, für das „Reverse Engineering" von Computerprogrammen, für die Kryptographie-Forschung sowie umfassend für alle Arten des „fair use" gefordert. Der Auftrag des Gesetzgebers an das „Copyright Office" ist unglücklich formuliert. So fordert 17 U.S.C. § 1201 (a) (1) (B) die Festlegung von „classes of works", die vom Umgehungsverbot ausgenommen werden sollen. Was unter einer „class of work" zu verstehen ist, und inwieweit dies mit der Tatsache zu vereinen ist, daß die meisten

Werkkategorien, bei denen der rechtliche Schutz gegen die tatsächlich Umgehung von Zugangskontrollmaßnahmen nicht greift.[2215] In beiden Werkkategorien geht es um Fälle, in denen technische Zugangskontrollmaßnahmen fehlerhaft funktionieren.[2216] Diese Ausnahmen gelten aber nur hinsichtlich des Verbots der tatsächlichen Umgehung von Zugangskontrollmaßnahmen, nicht hinsichtlich vorbereitender Handlungen.[2217] Damit stellt sich auch hier das oben beschriebene Problem, inwiefern durchschnittliche Nutzer von den Ausnahmen überhaupt profitieren können. Die beiden Ausnahmen gelten zunächst bis zum Jahr 2003. Dann hat das „Copyright Office" eine neue Liste von Werkkategorien zu erstellen.

Die differenzierte Regelung der Schrankenbestimmungen des rechtlichen Umgehungsschutzes im DMCA ist in sich unschlüssig und läßt ein gesetzgeberisches Konzept vermissen.[2218] Im Gegensatz zur weiten Fassung der urheberrechtlichen „fair use doctrine" hat der U.S.-Gesetzgeber im DMCA versucht, die Beschränkungen technischer Schutzmaßnahmen im einzelnen und abschließend aufzuzählen. Es gibt jedoch eine Vielzahl

urheberrechtlichen Schrankenbestimmungen nicht an eine Werkkategorie, sondern an eine bestimmte Nutzungsart oder allenfalls eine bestimmte Nutzerkategorie anknüpfen, blieb letztlich unklar; s. dazu *D. Nimmer*, 148 U. Penn. L. Rev. 673, 694 f. (2000). S. insgesamt <http://www.loc.gov/copyright/1201/anticirc.html>.

[2215] 37 C.F.R. § 201.40 (2000). Der vollständige Bericht des „Copyright Office" ist in *Library of Congress*, 65 Fed. Reg. 64555 ff. (2000), abgedruckt.

[2216] Dabei geht es einerseits um Listen von Webseiten, die von Filterprogrammen eingesetzt werden, um Nutzern den Zugang zu bestimmten Webseiten (z. B. pornographischen Inhalts) zu verweigern. Es ist schon öfters vorgekommen, daß diese Filterprogramme zusätzlich auch Webseiten filtern, die überhaupt nicht anstößigen Inhalts sind; s. dazu unten bei Fn. 2264 f. Dem Nutzer wird jedoch in aller Regel nicht mitgeteilt, welche Webseiten das Filterprogramm filtert. Um Fehlfunktionen des Programms herauszubekommen, muß der Nutzer daher die technischen Schutzmaßnahmen des Programms umgehen und die – regelmäßig durch Verschlüsselung gesicherte – Liste der gefilterten Webseiten extrahieren; s. dazu *Library of Congress*, 65 Fed. Reg. 64555, 64564 (2000). Andererseits geht es um Computerprogramme, Datenbanken und andere geschützte Inhalten, in denen eine technische Schutzmaßnahme den Zugang zu den Inhalten nur aus dem Grund verhindert, weil sie fehlerhaft funktioniert. Solche Probleme traten früher insbesondere bei fehlerhaft funktionierenden Dongles auf; s. dazu *Library of Congress*, 65 Fed. Reg. 64555, 64564 ff. (2000).

[2217] Der Auftrag an die Library of Congress in 17 U.S.C. § 1201 (a) (1) (B) ff. bezieht sich nur auf das Umgehungsverbot des Abs. (a) (1), nicht auch auf das Umgehungsverbot des Abs. (a) (2). S. a. *Koelman/Herberger* in: Hugenholtz (Hrsg.), S. 165, 195.

[2218] *Samuelson*, 14 Berkeley Tech. L. J. 519, 548 (1999), die auf S. 562 meint: „The anti-circumvention provisions of the DMCA […] are unpredictable, overbroad, inconsistent, and complex. The many flaws in this legislation are likely to be harmful to innovation and competition in the digital economy sector, and harmful to the public's broader interests in being able to make fair and other noninfringing uses of copyrightes works."; *Bechtold* in: Hoeren/Sieber (Hrsg.),Teil 7.11, Rdnr. 73; *Ginsburg*, 23 Colum.-VLA J. L. & Arts 137, 151 (1999); *D. Nimmer*, 148 U. Penn. L. Rev. 673, 701 f., 739 f. (2000); *N. B. Nimmer/D. Nimmer*, § 12A.07[A], S. 12A-79.

von Handlungen, die legitim erscheinen, sich aber nicht unter eine der bestehenden Beschränkungen subsumieren lassen.[2219] Die Tatsache, daß für bestimmte Bereiche Schrankenbestimmungen geschaffen wurden, für andere Bereiche dagegen nicht, zeigt den starken Einfluß von Lobbyisten auf das Gesetzgebungsverfahren.[2220] Aus diesen Gründen wird inzwischen mitunter eine Gesetzesänderung gefordert.[2221]

bb) Anwendbarkeit allgemeiner urheberrechtlicher Schrankenbestimmungen

Sehr umstritten ist derzeit die Frage, ob neben diesen spezifischen Schrankenbestimmungen auch allgemeine urheberrechtliche Schrankenbestimmungen den rechtlichen Umgehungsschutz beschränken können. Dabei geht es insbesondere um die „fair use doctrine" des 17 U.S.C. § 107. Für eine solche Argumentation gibt es mehrere Ansatzpunkte. Nach dem *ersten Ansatzpunkt* ist zu beachten, daß bei Nutzungskontrollmaßnahmen der Umgehungsschutz nach dem Wortlaut des 17 U.S.C. 1201 (b) (A) auf Schutzmaßnahmen beschränkt ist, die ein „right of a copyright owner under this title in a work" schützen. Man kann diese Formulierung abstrakt oder konkret verstehen. Nach der konkreten Betrachtungsweise steht dem Urheberrechtsinhaber beim Eingreifen der „fair use doctrine" gar kein „right of a copyright owner" mehr zu, das durch die technische Schutzmaßnahme geschützt werden könnte. Damit wären die urheberrechtlichen Schrankenbestimmungen der 17 U.S.C. §§ 107-121 bei Nutzungskontrollmaßnahmen in vollem Umfang auch auf den rechtlichen Umgehungsschutz anwendbar.[2222] Nach der abstrakten Betrachtungsweise ist mit der Formulierung „right of a copyright owner" nur gemeint, ob die technische Schutzmaßnahme ein Recht schützt, das dem Urheberrechtsinhaber abstrakt-generell durch den Copyright Act zugewiesen wird. Betrachtet man den Wortlaut der Vorschrift, erscheint diese abstrakte Betrachtungsweise überzeugender.

Nach dem *zweiten Ansatzpunkt* ist 17 U.S.C. § 1201 (c) (1) zu beachten: „Nothing in this section shall affect rights, remedies, limitations or *defenses to copyright infringement, including fair use*, under this title."[2223] Dies könnte als ein Einfalltor für urheberrechtliche Schrankenbestimmungen verstanden werden.[2224] Dabei ist aber zu beachten, daß es

[2219] *Samuelson*, 14 Berkeley Tech. L. J. 519, 543 ff. (1999), und *Band*, EIPR 1999, 92, nennen dafür u. a. Fehlerkorrektur, Virenkontrolle, Schutz von Geschäftsgeheimnissen sowie die Meinungs- und Pressefreiheit. S. weiterhin *D. Nimmer*, 148 U. Penn. L. Rev. 673, 727 ff. (2000).

[2220] Ebenso *Samuelson*, 14 Berkeley Tech. L. J. 519, 534 ff., 538 (1999).

[2221] So *Samuelson*, 14 Berkeley Tech. L. J. 519, 538, 546 (1999).

[2222] S. dazu *Wand*, S. 244 m. w. N.

[2223] Hervorhebung durch den Verfasser.

[2224] So *Marly*, K&R 1999, 106, 109 f.; s. a. *Samuelson*, 14 Berkeley Tech. L. J. 519, 539 f. (1999).

bei einer Umgehung technischer Schutzmaßnahmen um eine Verletzung des 17 U.S.C. § 1201 geht, der nicht zum „copyright" im engeren Sinne gezählt wird. Die zitierte Vorschrift spricht dagegen nur von „defenses to *copyright infringement*". Sie betrifft einen anderen Fall: Vorliegend geht es um die Frage, ob sich ein Inhalteanbieter, der gegen einen Nutzer *aus dem rechtlichen Umgehungsschutz* vorgeht, entgegenhalten lassen muß, daß zu Gunsten des Nutzers eine allgemeine urheberrechtliche Schrankenbestimmung eingreift. Die zitierte Vorschrift regelt dagegen den Fall, daß der Inhalteanbieter gegen den Nutzer *aus dem Urheberrecht* vorgeht, der Nutzer sich dann auf eine allgemeine urheberrechtliche Schrankenbestimmung beruft, der Inhalteanbieter aber entgegnen will, diese Schrankenbestimmung greife nicht, weil sie durch die engeren Schrankenbestimmungen des rechtlichen Umgehungsschutzes in 17 U.S.C. § 1201 (d) ff. verdrängt werde. Die zitierte Vorschrift regelt damit gerade den umgekehrten Fall. Urheberrecht und rechtlicher Umgehungsschutz sind getrennt voneinander zu behandeln, 17 U.S.C. § 1201 (c) (1) gibt für die vorliegende Problematik nichts her.[2225]

Eine umfassende Schrankenbestimmung für den rechtlichen Umgehungsschutz – ähnlich der „fair use defense" im herkömmlichen Urheberrecht – im Gesetzgebungsverfahren des DMCA zwar erwogen, aber letztlich verworfen.[2226] Sie ist im Gesetz nicht vorgesehen, ansonsten wäre die ausdifferenzierte Schrankenregelung der 17 U.S.C. § 1201 (d) – (j) auch unnötig.[2227]

III. Zwischenergebnis

Es zeigt sich, daß die Gesetzgeber in Europa, Deutschland und den USA das Spannungsverhältnis zwischen technischen Schutzmaßnahmen in DRM-Systemen und urheberrechtlichen Schrankenbestimmungen sehr wohl gesehen haben. In bestimmten Bereichen existieren zwar erst vereinzelt Regelungen. Durch den „Digital Millennium Copyright Act" und die europäische Richtlinie zum Urheberrecht in der Informationsgesellschaft wurde jedoch sowohl in den USA als auch in Europa der Versuch unter-

[2225] Ebenso *Dusollier*, EIPR 1999, 285, 293; Universal City Studios, Inc. v. Reimerdes, 111 F.Supp. 2d 294, 322 (S.D.N.Y. 2000); wohl auch *D. Nimmer*, 148 U. Penn. L. Rev. 673, 723 Fn. 264 (2000); zweifelnd *Ginsburg*, 23 Colum.-VLA J. L. & Arts 137, 151 f. (1999); *dies.*, 24 Colum.-VLA J. L. & Arts 1, 8 f. (2000); mit anderer Begründung, aber gleichem Ergebnis, *Wand*, S. 245 f. Unrichtig daher *Marly*, K&R 1999, 106, 109 f.

[2226] *U.S. House of Representatives*, H.R. Rep. No. 105–551, Part 2, S. 86; Universal City Studios, Inc. v. Reimerdes, 111 F.Supp. 2d 294, 322 ff. (S.D.N.Y. 2000). Ausführlich zur Gesetzgebungsgeschichte in dieser Beziehung *D. Nimmer*, 148 U. Penn. L. Rev. 673, 716 ff. (2000).

[2227] Vgl. Universal City Studios, Inc. v. Reimerdes, 111 F.Supp. 2d 294, 323 (S.D.N.Y. 2000); *D. Nimmer*, 148 U. Penn. L. Rev. 673, 723 (2000).

nommen, eine umfassende und abschließende Regelung dieses Spannungsverhältnisses zu schaffen. Zwar unterscheiden sich beide Regelungskomplexe in ihren Einzelheiten deutlich. Sie ähneln sich jedoch in ihrer Komplexität, Unübersichtlichkeit und ihren logischen Unstimmigkeiten.

E. Ergebnis

Der vorangegangene Teil der Untersuchung zeigt im Überblick, daß den Gesetzgebern vielfältige Möglichkeiten zur Verfügung stehen, um Schutzmechanismen in DRM-Systemen – Urheberrecht, Nutzungsverträge, Technologie-Lizenzverträge, technische Schutzmaßnahmen und rechtlicher Umgehungsschutz – in ihren Schutzwirkungen zu beschränken. Teilweise existieren umfangreiche gesetzliche Regelungen zu dieser Frage. Sie zeichnen sich oftmals durch einen hohen Komplexitätsgrad und logische Brüche aus. Teilweise bestehen nur vereinzelte Regelungen, während in anderen Bereichen Regelungen völlig fehlen.[2228] In Europa wurden bisher manche Bereiche des Problemkomplexes – insbesondere das Verhältnis urheberrechtlicher Grundsätze zu Nutzungsverträgen und zu Technologie-Lizenzverträgen – fast überhaupt nicht problematisiert. Ein stimmiges Konzept, wie DRM-Systeme mit urheberrechtlichen Schrankenbestimmungen in Einklang zu bringen sind, existiert heute nicht.

[2228] Auf diese Bereiche wurde hier gar nicht eingegangen. So sieht beispielsweise der Umgehungsschutz nach 47 U.S.C. § 605 und § 553 (s. dazu oben Teil 2, D I 2 b dd 4) keinerlei Beschränkungen vor.

Teil 5: Ausblick

> *Ultimately, the reality of sophisticated DRM technology is about far more than Napster, online entertainment and copyright law. […] It is about constructing a civil digital society in the Internet Age, where rules created for and by its citizens can be implemented and respected wherever and whenever legitimate interests are in play.*[2229]
>
> *Das Internet wirft keine spezifischen, nur auf das Netz selbst beschränkten Rechtsprobleme auf. Vielmehr steht das Internet selbst nur als Spitze des Eisbergs für die allgemeine Frage nach einer Wissensordnung und den Spezifika einer Informationsgesellschaft. Hinter dem Internet wölbt sich der Zenit des Informationsrechts.*[2230]

Inhalteanbieter setzen in DRM-Systemen zunehmend auf Schutzmechanismen außerhalb des Urheberrechts. Der Schutz durch Technik, Nutzungsverträge und Technologie-Lizenzverträge ist flexibler und individueller als das notwendigerweise pauschalierende Urheberrecht. Weiterhin bieten diese ineinandergreifenden Schutzmechanismen – insbesondere der Schutz durch Technik – ein gleichbleibend hohes Schutzniveau. Inhalteanbieter können den Schutzumfang eines DRM-Systems selbst festlegen. Es läßt sich eine *Privatisierung des Rechtsschutzes* beobachten.[2231] Die Gesetzgeber unterstützen diese Entwicklung, indem sie neue Regelungen zum rechtlichen Umgehungsschutz technischer Schutzmaßnahmen schaffen und Nutzungsverträge zunehmend als wirksam anerkennen.

Fraglich scheint, ob diese Privatisierungstendenz nicht zu weit geht. Es geht darum, ob die Privatisierung des Rechtsschutzes wegen entgegenstehender öffentlicher Interessen zu begrenzen ist. Die Gesetzgeber auf internationaler wie nationaler Ebene haben dieses Problem erkannt und gehen zunehmend – auf unterschiedlichen Wegen und mit unterschiedlichem Erfolg – dazu über, die unterschiedlichen Schutzmechanismen in DRM-Systemen gesetzlich zu beschränken. Dabei wird mitunter nicht direkt die Ausgestaltung der Schutzmechanismen beeinflußt. Bei technischen Schutzmaßnahmen wird also nicht vorgeschrieben, wie solche Schutzmaßnahmen im einzelnen auszusehen haben. Vielmehr wird der rechtliche Umgehungsschutz beschränkt, der die technischen Schutzmaßnahmen begleitet. Öffentliche Interessen werden nicht durch eine direkte Regulierung implementiert, vielmehr werden Parameter reguliert,

---

[2229] *Shear*, S. 9 f.
[2230] *Hoeren*, NJW 1998, 2849, 2854.
[2231] S. zum ganzen ausführlicher oben Teil 3, B II 1.

die auf indirektem Wege das Regulierungsziel – die Wahrung öffentlicher Interessen – zu wahren versprechen.

Diese Charakteristika von DRM-Systemen – ein zunehmender Schutz durch Technik und Vertrag, eine zunehmende Privatisierung des Rechtsschutzes mit grundsätzlicher Unterstützung durch den Gesetzgeber, eine Beschränkung dieser Privatisierungstendenz durch gesetzliche Regelungen zur Wahrung öffentlicher Interessen und der zunehmende Übergang zur indirekten Regulierung durch den Gesetzgeber – sind kein Spezifikum von DRM-Systemen. Vielmehr handelt es sich um Tendenzen, die sich allgemein im Internet-Recht beobachten lassen.[2232]

Im Bereich des Datenschutzes sind diese Tendenzen seit längerer Zeit zu beobachten.[2233] Im Internet sammeln Unternehmen durch Cookies und andere Identifizierungstechnologien große Datenmengen, die Auskunft über einzelne Nutzer und ihre Gewohnheiten geben, mithin ein vollständiges Nutzungs- und Bewegungsprofil erstellen können. Um dieser Gefahr zu begegnen, besteht in Europa und Deutschland ein Komplex rechtlicher Regelungen, der vom Bundesdatenschutzgesetz über das Teledienstedatenschutzgesetz, den Mediendienste-Staatsvertrag bis zu speziellen telekommunikationsrechtlichen Vorschriften reicht.[2234] Zunehmend

---

[2232] S. dazu nur *Lessig*. Zu Privatisierungstendenzen s. *Holitscher*, Schweizerische Zeitschrift für Politikwissenschaft 5 (2), S. 134 ff. (Sommer 1999). Zur zunehmenden indirekten Regulierung durch den Gesetzeger im Internet s. *Lessig*, 14 Berkeley Tech. L. J. 759, 762 f. (1999). Zur Selbstregulierung im Internet ausführlich *Mayer*, S. 58 ff., 239 ff.; *ders*., K&R 2000, 13 ff.; vgl. weiterhin *Perritt*, MMR-Beilage zu Heft 7/2000, S. 1 ff.; *Werle* in: Hoffmann-Riem (Hrsg.), S. 141 ff.; zur Selbstregulierung im Datenschutzrecht s. *Heil*, DuD 2001, 129 ff.

[2233] Da sich das Datenschutzrecht schon seit langer Zeit intensiv mit dem Verhältnis zwischen rechtlicher und technischer Regulierung auseinandersetzt, könnte das Urheberrecht vom Datenschutzrecht nach Auffassung des Verfassers einiges lernen. Eine interessante Parallele zwischen den Problemen des Datenschutzes und den Lösungsansätzen in DRM-Systemen stellt *Zittrain*, 52 Stan. L. Rev. 1201 (2000), her. Gerade zwischen dem Datenschutzrecht und DRM-Systemen lassen sich deutliche Parallelen erkennen. Wie bei DRM-Systemen könnten auch im Datenschutzbereich technische Schutzsysteme („Privacy-Enhancing Technologies") den rechtlichen Schutz bis zu einem gewissen Maß ersetzen. Ebenfalls parallel zur Bedeutung des Urheberrechts in DRM-Systemen könnte dem herkömmlichen Datenschutzrecht in diesem Umfeld eine Auffangfunktion zukommen. Daneben käme dem Datenschutzrecht – wie dem Urheberrecht in DRM-Systemen – eine neue Aufgabe zu, nämlich Rahmenbedingungen für einen effektiven Selbstschutz zu setzen. Unter Umständen könnte die „Privatisierung des Rechtsschutzes" durch „Privacy-Enhancing Technologies" zu weit gehen. Erfolgt der Selbstschutz durch Verschlüsselung, so macht der Staat mitunter ein Interesse geltend, die verschlüsselte Kommunikation wegen öffentlicher Interessen abhören zu können; s. *Trute*, JZ 1998, 822, 829. Dies ist Streitpunkt der sogenannten „Krypto-Kontroverse", s. dazu oben Fn. 2098. Wie bei DRM-Systemen stellt sich also die Frage, ob die „Privatisierung des Rechtsschutzes" wegen öffentlicher Interessen beschränkt werden sollte.

[2234] Einen Überblick über die für das Internet relevanten Vorschriften geben die Kapitel 16.1 bis 16.4 in *Hoeren/Sieber* (Hrsg.), Handbuch Multimedia-Recht.

könnten jedoch technische Schutzmechanismen den Schutz personenbezogener Daten gewährleisten. Mit Hilfe sogenannter „Privacy-Enhancing Technologies" (PET) können Nutzer im Internet ihre persönlichen Daten selbst schützen beziehungsweise eine Kontrolle über die Verwendung dieser Daten behalten (*Schutz durch Technik*).[2235] Der Gesetzgeber unterstützt diese *Privatisierung des Rechtsschutzes*, gestaltet sie aber auch gleichzeitig mit, wenn er Regelungen des Systemdatenschutzes[2236] und des Selbstdatenschutzes[2237] in Gesetzen verankert.[2238] In den Vereinigten Staaten, die über eine völlig andere Tradition im Datenschutzrecht verfügen,[2239] wird in letzter Zeit vorgeschlagen, die Nutzer sollten ihre Datenschutzinteressen durch entsprechende vertragliche Beziehungen zu Unternehmen, die personenbezogene Daten erheben, schützen (*vertraglicher Schutz*).[2240] Auch wird vorgeschlagen, der Gesetzgeber solle ein „property right" für personenbezogene Daten schaffen, das als Grundlage für Transaktionen und „Rechtseinräumungen" dienen könnte, die durch „Privacy-Enhancing Technologies" wie insbesondere P3P[2241] ermöglicht würden (*kombinierter Schutz durch Recht und Technik*).[2242] Schließlich spielt die *Selbstregulierung* im U.S.-amerikanischen Datenschutzrecht seit langem eine außerordentlich wichtige Rolle.[2243]

[2235] Es gibt eine Vielzahl unterschiedlicher „Privacy-Enhancing Technologies", von denen einige in Teil 1, E V, dargestellt wurden. Auf das Vollzugsdefizit klassischer datenschutzrechtlicher Normen im Internet weist *Roßnagel* in: Kubicek/Braczk/Klumpp/Roßnagel (Hrsg.), S. 385, hin.

[2236] Durch Systemdatenschutz sollen Infrastrukturen derart ausgestaltet werden, daß datenschutzrechtliche Probleme und Risiken erst gar nicht entstehen. Dazu gehört die Einräumung von Wahlmöglichkeiten für Anonymisierung oder Pseudonymisierung, die organisatorische Abschottung und dateneinsparende Ausgestaltung von Datenverarbeitungsbereichen wie auch die Vermeidung von Funktionsbündelungen, s. *Hoffmann-Riem*, AöR 32 (1998), 513, 535; *Roßnagel*, ZRP 1997, 26, 29.

[2237] Der Nutzer wird insbesondere über „Privacy-Enhancing Technologies" zum Selbstschutz befähigt.

[2238] Zur Bedeutung des Systemdatenschutzes und des Selbstdatenschutzes im Datenschutzrecht s. *Hoffmann-Riem*, AöR 32 (1998), 513, 534 ff.; *Roßnagel*, ZRP 1997, 26, 29. Gesetzliche Regelungen, die den Systemdatenschutz betreffen, finden sich in Deutschland z. B. in § 3 Abs. 4 Teledienstedatenschutz-Gesetz und § 12 Abs. 5 Mediendienstestaatsvertrag; s. weiterhin § 4 Abs. 1 Teledienstedatenschutz-Gesetz und § 13 Abs. 1 Mediendienstestaatsvertrag.

[2239] S. dazu nur *Roßnagel* in: Kubicek et al. (Hrsg.), S. 385, 386 ff.; ausführlich *Schwartz/Reidenberg*.

[2240] *Samuelson*, 52 Stan. L. Rev. 1125 (2000); *Basho*, 88 Cal. L. Rev. 1507 (2000).

[2241] S. dazu oben bei Fn. 719 ff.

[2242] So *Lessig*, S. 160; s. a. *N.N.*, 112 Harv. L. Rev. 1574, 1646 f. (1999); kritisch *Schwartz*, 2000 Wis. L. Rev. 743; kritisch zur Einführung eines „property right" für personenbezogene Daten *Litman*, 52 Stan. L. Rev. 1283 (2000); *Lemley*, 52 Stan. L. Rev. 1545 (2000). Zu P3P aus der Sicht der deutschen bzw. europäischen Datenschutzrechts s. *Lohse/Janetzko*, CR 2001, 55, 59 ff.; *Enzmann*, DuD 2000, 535 ff.

[2243] S. dazu nur *Roßnagel* in: Kubicek et al. (Hrsg.), S. 385, 387 ff.

Die „Internet Corporation for Assigned Names and Numbers“ (ICANN)[2244] ist unter anderem für die Verwaltung des „Domain Name System“ (DNS) zuständig.[2245] Neben einer 32 Bit langen IP-Adresse (beispielsweise 134.2.34.92) verfügt jeder Rechner im Internet über einen sogenannten „Domain Namen“ (beispielsweise www.jura.uni-tuebingen.de). Das Domain Name System garantiert, daß Domain Namen den zugrundeliegenden IP-Adressen eindeutig zugeordnet werden. Es stellt damit eines der grundlegenden Funktionspfeiler des Internet dar. Herkömmlicherweise wäre die Verwaltung einer solchen Infrastruktur von staatlichen oder supranationalen Institutionen wahrgenommen worden.[2246] Dagegen ist ICANN eine private „non-profit corporation“ nach kalifornischem Recht (*Privatisierung von Kontroll- und Organisationsinstanzen*). Dies hat in den letzten Jahren im Internet-Recht zu einer breiten Diskussion geführt, ob Aufgaben, die früher vom Staat aufgenommen wurden, „privatisiert“ werden können, und ob das Recht dieser Entwicklung Schranken entgegensetzt beziehungsweise entgegensetzen sollte (*Beschränkung der Privatisierung wegen öffentlicher Interessen*).[2247]

Bei der Registrierung von Domain Namen ergibt sich oftmals ein Konflikt mit Marken- und anderen Kennzeichenrechten. Ist ein U.S.-amerikanischer Journalist berechtigt, für sich den Domain Namen „mcdonalds.com“ zu registrieren?[2248] Kann ein Dritter den Domain Namen „juliaroberts.com“ für sich registrieren?[2249] In den letzten Jahren sind zu diesen und ähnlichen Fragen, die das Verhältnis zwischen Domain Namen und Kennzeichenrechten betreffen, in vielen Ländern der Welt eine Unzahl von Konfliktfällen aufgetreten. Um eine möglichst schnelle und reibungslose Möglichkeit der Streitschlichtung zu bieten, wurde im Rahmen der ICANN die „Uniform Dispute Resolution Policy“ (UDRP)[2250] entwickelt, die den Inhabern von Marken- und anderen Kennzeichenrechten erlaubt, die Registrierung eines Domain Namens anzugreifen

---

[2244] <http://www.icann.org>.

[2245] Die letztendliche Kontrolle über das DNS liegt aber immer noch beim U.S. Departement of Commerce, das den „Root Zone File“ kontrolliert; s. *Froomkin*, 50 Duke L. J. 17, 44 (2000). Zur ICANN allgemein s. *Kleinwächter*, MMR 1999, 452; *Mayer*, K&R 2000, 13, 16 f.

[2246] Tatsächlich wurde vorgeschlagen, die Verwaltung des DNS bei der „International Telecommuncation Union“ oder der „World Intellectual Property Organization“ anzusiedeln. Vor Gründung der ICANN wurde das DNS lange Jahre faktisch von einem Mann, *Jonathan Postel*, verwaltet.

[2247] S. aus der U.S.-amerikanischen Literatur *Froomkin*, 50 Duke L. J. 27 (2000); *Weinberg*, 50 Duke L. J. 187 (2000); *Zittrain*, 14 Berkeley Tech. L. J 1071 (1999); s. a. *Perritt*, MMR-Beilage zu Heft 7/2000, S. 1 ff.; vgl. weiterhin umfassend *Kesan/Shah*.

[2248] So 1994 geschehen durch den Wired-Reporter *Joshua Quittner*, s. *Bechtold*, ZUM 1997, 427, 440.

[2249] So geschehen 1998, s. <http://arbiter.wipo.int/domains/decisions/html/2000/d2000–0210.html>.

[2250] <http://www.icann.org/udrp/udrp-policy-24oct99.htm>.

und, wenn das außergerichtliche Konfliktlösungsverfahren für den Markeninhaber positiv verläuft, die Kontrolle über den Domain Namen zu erhalten.[2251] Inhaber von Domain Namen haben keine Wahl, ob sie sich den Regelungen der UDRP unterwerfen wollen. Vielmehr verpflichtet ICANN durch eine Vertragskette jeden Inhaber eines Domain Namens, sich an die Bedingungen des UDRP zu halten und im Streitfall an einem Konfliktlösungsverfahren teilzunehmen.[2252] ICANN, ein privates Unternehmen, schafft faktisch durch eine Vertragspyramide ein neues, international geltendes „Markenrecht" für Domain Namen (*Schutz durch Vertrag*).[2253] Dieser *Privatisierung des Rechtsschutzes* wird mitunter vorgeworfen, sie schütze einseitig die Interessen von Markeninhabern und vernachlässige die Nutzung von Domain Namen für nichtkommerzielle Zwecke wie Parodie, Kritik oder Kunst.[2254] Eine statistische Analyse von bisher entschiedenen UDRP-Fällen zeigt, daß Markeninhaber in 80% aller Fälle Erfolg haben.[2255] Wichtiger ist aber, daß die Ergebnisse stark davon abhängen, bei welchem der vier existierenden „Dispute Resolution Service Provider" das Konfliktlösungsverfahren anhängig ge-

[2251] S. dazu allgemein *Bettinger*, CR 2000, 234; *Strömer*, K&R 2000, 587. Die UDRP wurde maßgeblich von einem Bericht der WIPO aus dem Jahr 1999 zu immaterialgüterrechtlichen Fragen von Domain Namen beeinflußt. Derzeit findet bei der WIPO ein „Second WIPO Internet Domain Name Process" statt, der 2001 in einem weiteren Bericht enden soll und zu einer Erweiterung des Anwendungsbereichs und/oder einer inhaltlichen Überarbeitung der UDRP führen könnte; s. dazu <http://wipo2.wipo.int/process2>.

[2252] ICANN verpflichtet die Registrare von Domain Namen, die Bedindungen der UDRP in Verträge zu integrieren, mit denen Dritte bei ihnen Domain Namen registrieren können, s. *Internet Corporation for Assigned Names and Numbers*, Registrar Accreditation Agreement, § II.K. Damit reicht ICANN die vertragliche Verpflichtung, an einem UDRP-Verfahren teilzunehmen, über die Registrare an jeden Registranten weiter; s. a. *Bettinger*, CR 2000, 234, 235; *Halpern/Mehrotra*, 21 U. Pa. J. Int'l Econ. L. 523, 554 f. (2000). Derzeit bezieht sich die UDRP nur auf Domain Namen in den Top-Level-Domains .com, .net und .org.

[2253] S. dazu auch *Halpern/Mehrotra*, 21 U. Pa. J. Int'l Econ. L. 523 ff. (2000). Diese Ausführungen sind notwendigerweise verkürzt. Insbesondere bezieht sich die UDRP derzeit nur auf das Problem des sog. „cybersquatting", also die mißbräuchliche und bösgläubige Registrierung eines Domain Namens, an dem ein Dritter Kennzeichenrechte besitzt, s. *Internet Corporation for Assigned Names and Numbers*, Uniform Dispute Resolution Policy, § 4 (a). Von einem umfassenden „Markenrecht" ist die UDRP damit noch weit entfernt. Jedoch werden zur Zeit Ausweitungen der UDRP erwogen, s. oben Fn. 2251.

[2254] S. dazu *Mueller*, S. 23 f.; *Halpern/Mehrotra*, 21 U. Pa. J. Int'l Econ. L. 523, 558 (2000). Zu anderen Schwächen der UDRP s. *Walker*, 15 Berkeley Tech. L. J. 289, 308 ff. (2000).

[2255] *Mueller*, S. 10. Dabei ist jedoch zu beachten, daß die UDRP nur Fälle erfaßt, in denen der Kennzeicheninhaber dem Inhaber des Domain Namens eine mißbräuchliche und bösgläubige Registrierung vorwirft, und daß das Konfliktlösungsverfahren nur von den Kennzeicheninhabern initiiert werden kann. Dies trägt zu dem kennzeichenfreundlichen Ergebnis der Statistik bei; s. a. *Halpern/Mehrotra*, 21 U. Pa. J. Int'l Econ. L. 523, 558 (2000).

macht wird:[2256] Nach einer im November 2000 veröffentlichten Untersuchung gewannen die Kennzeicheninhaber bei Konfliktlösungsverfahren, die beim WIPO „Dispute Resolution Service Provider" anhängig gemacht wurden, 67,5% der Fälle, während sie beim Konkurrenten eResolution nur 44,2 % aller Fälle gewannen.[2257] Da der Markeninhaber als Kläger berechtigt ist, den „Dispute Resolution Service Provider" auszuwählen,[2258] kann er durch ein „Forum Shopping" das Ergebnis des Konfliktlösungsverfahrens beeinflussen.[2259] Bedenkt man den Vorwurf, daß in dem UDRP-System Interessen der Allgemeinheit zu wenig berücksichtigt werden und daß Inhaber von Domain Namen weltweit von einer privatrechtlich organisierten Institution in Kalifornien gezwungen werden, sich diesem System zu unterwerfen, stellt sich auch hier ein Konflikt zwischen einer Privatisierung des Rechtsschutzes und *öffentlichen Interessen* (Förderung von Parodie, Kritik oder Kunst).[2260]

Ein weiteres Problem des Internet-Rechts ist der Jugendschutz. Um Kinder und Jugendliche vor jugendgefährdenden Inhalten in herkömmlichen Medien zu schützen, sieht das Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte vor, daß bestimmte jugendgefährdende Schriften Kindern oder Jugendlichen nicht zugänglich gemacht werden dürfen. Zu diesem Zweck erstellt eine Bundesprüfstelle eine Liste jugendgefährdender Schriften. Die personelle Zusammensetzung und das Verfahren dieser Bundesprüfstelle ist gesetzlich im einzelnen geregelt, §§ 8 ff. GjSM.[2261] Im Internet stößt dieser Regulierungsansatz[2262] an seine Grenzen: Jugengefährdende Inhalte sind aus dem Ausland erhältlich, Anbieter können problemlos den Server wechseln, das Angebot ändert sich beinahe täglich. Aus diesem Grund haben mehrere private Unternehmen sogenannte „Filterprogramme" entwickelt. Diese Softwareprogramme, die regelmäßig auf dem Rechner des Nutzers installiert werden, verhindern, daß von diesem Rechner aus jugendgefährdende Web-Seiten

[2256] Insgesamt existieren vier akkreditierte „Dispute Resolution Service Provider", von denen der Bekannteste bei der „World Intellectual Property Organization" in Genf angesiedelt ist; s. <http://www.icann.org/udrp/approved-providers.htm>. Die eigentlichen Entscheidungen werden nicht von dem „Dispute Resolution Service Provider" selbst, sondern von einem Streitschlichter oder einem aus drei Personen besetzten Gremium des „Dispute Resolution Service Providers" entschieden.

[2257] *Mueller*, S. 11, 22.

[2258] *Internet Corporation for Assigned Names and Numbers*, Uniform Dispute Resolution Policy, § 4 (d).

[2259] Die Untersuchung zeigt auch, daß ein „Forum Shopping" tatsächlich stattfindet, s. *Mueller*, S. 18 f.

[2260] Diese These ist notwendigerweise vereinfacht; auf den eingeschränkten Anwendungsbereich der UDRP wurde u. a. in den Fn. 2252 und 2253 hingewiesen.

[2261] Zu weiteren Ansätzen, den Jugenschutz zu gewährleisten (Freiwillige Selbstkontrolle der Filmwirtschaft, rundfunkrechtliche Regelungen), s. im Überblick *Hoffmann-Riem* in: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), S. 261, 281 f.

[2262] Grundsätzlich greift das GjSM auch im Internet, s. nur § 3 Abs. 1 Nr. 4 GjSM.

aufgerufen werden können (*Schutz durch Technik*). Dabei legen die Hersteller der Filterprogramme regelmäßig selbst fest, welche Web-Seiten gefiltert werden und welche nicht. Die Aufgaben, die nach herkömmlichem Verständnis der Bundesprüfstelle zufallen könnte, wird im Internet faktisch von privaten Unternehmen durchgeführt (*Privatisierung des Rechtsschutzes*). In den USA sind viele Schulen und Bibliotheken durch ein im Dezember 2000 erlassenes Gesetz letztlich gezwungen, solche Filterprogramme zu installieren.[2263] In diesem Fall schützt der Staat Kinder und Jugendliche nicht mehr selbst, sondern gewährleistet nur noch, daß Dritte diesen Schutz bieten (Trend zur *indirekten Regulierung*). Diese Entwicklung ist nicht unproblematisch. In der Vergangenheit kam es öfters vor, daß die Filterprogramme nicht nur jugendgefährdende Inhalte, sondern darüber hinaus auch weitere, völlig ungefährliche Inhalte gefiltert haben. Dies geschieht teilweise absichtlich, teilweise unabsichtlich.[2264] Bei Filterprogrammen entscheiden also private Unternehmen, welche Web-Seiten auf – teilweise öffentlich zugänglichen – Computern betrachtet werden können. Dies hat zum Vorwurf der „privaten Zensur" geführt.[2265] Auch hier geht es darum, ob die Privatisierung des Rechtsschutzes wegen *öffentlicher Interessen* beschränkt werden sollte.[2266]

Es ließen sich noch weitere Beispiele für solche Parallelentwicklungen zu DRM-Systemen finden.[2267] Es zeigt sich, daß unterschiedliche Bereiche

---

[2263] Zwar besteht keine direkte Verpflichtung. Jedoch wird die Vergabe von Haushaltsmitteln und Zuschüssen an die Bildungseinrichtungen davon abhängig gemacht, daß auf ihren Computern Filterprogramme installiert werden. Die Einzelheiten des Gesetzes, dessen Wortlaut fast 20 Seiten lang ist, sind komplex; s. Children's Internet Protection Act, Pub. L. No. 106–554, §§ 1701 ff., 114 Stat. 2763A, S. 335–352 (2000); s. dazu auch *Nadel*, First Amendment's Limitations, S. 1149 f.

[2264] Beispiele finden sich bei <http://sethf.com/anticensorware/smartfilter/gotalist.php> und <http://www.peacefire.org>; *Electronic Privacy Information Center*, S. 29 ff. Mitunter wird den Filterprogrammen eine Fehlerrate von 76% vorgeworfen, s. *Library of Congress*, 65 Fed. Reg. 64555, 64564 (Oct. 27, 2000).

[2265] S. dazu *Lessig*, S. 176 ff.; *ders.*, 38 Jurimetrics J. 629, 665 ff. (1998); *Benkler*, 71 U. Colo. L. Rev. 1203, 1250 (2000); s. a. *Bohorquez*, 43 N.Y.L. Sch. L. Rev. 523 (1999); *Nadel*, First Amendment's Limitations, S. 1150 ff.

[2266] Ein erster Ansatz ist in den USA die Ausnahme von Filterprogrammen aus dem rechtlichen Umgehungsschutz nach 17 U.S.C. § 1201 (a) (1) durch das U.S. Copyright Office im Oktober 2000; s. dazu oben bei Fn. 2216.

[2267] In den USA wird beispielsweise der Zugang zu Breitbandkabelnetzen unter dem Aspekt der Privatisierung essentieller Infrastrukturen diskutiert, s. dazu *Lemley/Lessig*, 48 UCLA L. Rev. 925 (2001); *Ku*, 75 Tul. L. Rev. 87 (2000). Gleiches gilt für die Frage, wer die Kontrolle über Chatforen und Mailinglisten im Internet hat, die als „privatisierte öffentliche Plätze" angesehen werden können; s. dazu *Lessig*, S. 66; *N.N.*, 112 Harv. L. Rev. 1574, 1604 (1999); *Goldstone*, 69 U. Colo. L. Rev. 1 (1998). Bei der umstrittenen Zulässigkeit unverlangter Werbe-E-Mails („Spamming") und von Hyperlinks bestehen sowohl technische als auch rechtliche Lösungsansätze, s. *Sorkin*, 35 U.S.F. L. Rev. 325 (2001) bzw. *Bechtold*, The Link Controversy Page. Schließlich kann das von der IFPI Deutschland propagierte Filtersystem „Rights Protection System"

des Internet-Rechts durch gleiche Problemkonstellationen gekennzeichnet sind. Dies soll nicht heißen, daß keine Unterschiede zwischen den Bereichen bestehen. Auch treten die beschriebenen Phänomene nicht nur im Internet auf. Es ist beispielsweise ein allgemeines Phänomen, daß Aufgaben, die traditionell vom Staat wahrgenommen wurden, zunehmend von privaten Akteuren wahrgenommen werden.[2268] Hybride Governance-Formen werden immer wichtiger. Dabei stellt sich die Frage, welche Aufgaben dem Staat und dem Gesetzgeber noch zukommen.[2269] Auch in Bereichen außerhalb des Internet-Rechts wird auf vertragliche und technische Schutzmaßnahmen gesetzt.[2270] Dennoch scheinen die Parallelen

(RPS) unter diesem Aspekt betrachtet werden. RPS filtert raubkopierte MP3-Dateien, die ein Nutzer in Deutschland von einem ausländischen Server abruft, an den Verbindungen der deutschen Internet Service Provider ins Ausland und verweigert damit dem Nutzer in Deutschland den Abruf der ausländischen MP3-Datei; zur Funktionsweise s. oben Fn. 462. Von der IFPI Deutschland wird dieses Verfahren mit dem Argument propagiert, im Grundsatz ändere sich gegenüber der bisherigen Lage gar nichts, da auch schon bisher raubkopierte CDs bei der Einfuhr nach Deutschland von der Zollbehörde beschlagnahmt werden können, s. § 111 a UrhG. RPS sei nichts anderes als eine „virtuelle Grenzbeschlagnahme". Dabei wird jedoch ein wichtiger Unterschied unterschlagen. Die Grenzbeschlagnahme nach § 111 a UrhG ist nur zulässig, wenn die Rechtsverletzung offensichtlich ist. Sie wird durch die Zollbehörde durchgeführt. Widerspricht der Verfügungsberechtigte der Beschlagnahme, so knüpft sich daran ein gesetzlich geregeltes Verfahren nach § 111 a Abs. 4 UrhG an. Bei RPS entscheidet dagegen nicht die Zollbehörde, sondern IFPI bzw. deren Mitglieder – also letztlich die Schallplattenindustrie, mithin *private Unternehmen* – darüber, welche Dateien gefiltert werden und welche nicht. Die Erfahrung mit Filterprogrammen zum Jugendschutz zeigen, daß solche Filtersysteme oftmals mehr Inhalte filtern, als sie eigentlich filtern dürften. Wie bei Filterprogrammen zum Jugendschutz stellt sich damit bei RPS das Problem einer zu weitgehenden *Privatisierung des Rechtsschutzes*.

[2268] S. zu der internationalen Dimension dieses Phänomens *Ronit/Schneider*, 12 Governance 243 ff. (1999). Zur Privatisierungstendenz bei Standardisierungen s. *Salter* in: Cutler/Haufler/Porter (Hrsg.), S. 97 ff.

[2269] S. dazu nur *Engel*, A Constitutional Framework.

[2270] Eine interessante Parallele zeigt sich beim wettbewerbsrechtlichen Schutz von Vertriebsbindungssystemen. Der BGH hatte 1999 seine langjährige Rechtsprechung aufgegeben, wonach der Hersteller, der seine Produkte ausschließlich über ein gedanklich und praktisch lückenloses Vertriebssystem absetzt, einen Anspruch aus § 1 UWG gegen Außenseiter hat, die nur durch Ausnutzen des Vertragsbruchs eines gebundenen Händlers in den Besitz des vertriebenen Produkts gelangen konnten, BGH, DB 2000, 1323 m. Anm. *Kapp*. Vor der Entscheidung hatte der Hersteller gegen die Außenseiter, die einen fremden Vertragsbruch ausnutzten und mit denen der Hersteller in keinerlei vertraglicher Beziehung standen, faktisch ein absolut wirkendes Ausschließlichkeitsrecht. In der Entscheidung von 1999 änderte der BGH seine Rechtsprechung und verneinte einen solchen Anspruch. Aber auch nach der Entscheidung ist der Hersteller nicht schutzlos gestellt. Vielmehr wies der BGH selbst darauf hin, daß es dem Hersteller freistehe, die Einhaltung der vertraglichen Verpflichtungen der gebundenen Händler durch ein Nummernsystem zu kontrollieren, BGH, DB 2000, 1323, 1326. In der Terminologie dieser Arbeit handelt es sich dabei um einen *technischen Schutz* eines *vertraglichen Schutzsystems*. Wieterhin führte der BGH aus, daß dem Hersteller gegen einen Außenseiter, der diese Kontrollnummer entferne, ein Unterlassungsanspruch nach § 1 UWG zustehe, BGH, DB 2000, 1323, 1326; BGH, GRUR 1999, 1109 –

zwischen unterschiedlichen Bereichen des Internet-Rechts stark genug, um sie unter einem einheitlichen Analyseansatz zu betrachten. Es geht um den Zugang zu und die Nutzung von Information. Es geht um die Frage, wer Zugang und Nutzung kontrollieren darf und wie weit diese Kontrolle geht. Die Zwecke der Kontrolle sind vielfältig: Bei DRM-Systemen wollen Inhalteanbieter Zugang und Nutzung kontrollieren, um ihre Investitionen refinanzieren zu können. Bei Filtersystemen im Jugendschutzbereich wollen Eltern kontrollieren, welche Informationen ihre Kinder betrachten können. Bei „Privacy-Enhancing Technologies" wollen Nutzer kontrollieren, wie Informationen über sie von Dritten gesammelt und verarbeitet werden. Auch die Gründe für Beschränkungen, denen solche Schutzsysteme unterliegen müssen, sind vielfältig. Sie können dem Urheberrecht, dem Datenschutzrecht, dem Kartellrecht, dem AGB-Gesetz oder den Grundrechten entstammen. Die Definition von Rahmenbedingungen des Informationszugangs und der Informationsnutzung könnte die Aufgabe eines zukünftigen Informationsrechts werden. Fragen der Regulierung von DRM-Systemen und des Urheberrechts gehen in diesem umfassenderen Rechtsgebiet auf.

Eines der zentralen Charakteristika eines entstehenden Informationsrechts ist damit die Regelung der Kontrolle über Information. Oftmals geht es um das Verhältnis zwischen privater Regulierung und öffentlichen Interessen. In DRM-Systemen ist die Aufgabe des Rechts weniger, selbst einen ausreichenden Schutz zu bieten, als Rahmenbedingungen für technische Verfahren zu setzen, eventuelle Lücken im technischen und vertraglichen Schutz von digitalen Inhalten zu schließen und zu weit gehende Schutzmechanismen zu beschränken. In einem so dynamischen Umfeld wie dem Internet und anderen digitalen Medien kann der Gesetzgeber alleine die anstehenden Aufgaben nicht mehr erfüllen.[2271] Vielmehr werden andere Schutzmechanismen – Technik und Vertrag – zunehmend an Bedeutung erlangen. Unternehmen wie Nutzer werden nicht mehr nur durch das Recht geschützt. Sie sollen vielmehr aufgrund einer rechtlichen Technikgestaltung zum Selbstschutz befähigt werden.[2272] Zentrale Infra-

Entfernung der Herstellungsnummer I; s. a. BGH, GRUR 2001, 841 – Entfernung der Herstellungsnummer II. Nach der Terminologie dieser Arbeit ist dies ein *rechtlicher Umgehungsschutz* des technischen Schutzes. Hinsichtlich des Schutzes von Vertriebsbindungssystemen deutet sich damit ein Trend von einem Schutz durch ein „property right" zu einem Schutz durch Vertrag, Technik und rechtlichen Umgehungsschutz an. Dieses Schutzsystem ähnelt dem Ineinandergreifen unterschiedlicher Schutzmechanismen in DRM-Systemen, wie sie in der mittleren Säule der Abbildung 7, S. 263, dargestellt wurden.

[2271] *Roßnagel*, ZRP 1997, 26, 27, meint: „In der Netzwelt wird sich der demokratische Rechtsstaat an Ohnmachtserfahrungen gewöhnen müssen."

[2272] S. dazu *Bechtold*, ZUM 1997, 449 f.; *Roßnagel*, ZRP 1997, 26, 29. Zur rechtlichen und verletzlichkeitsreduzierenden Technikgestaltung in der IT-Sicherheit s. ausführlich *Hammer*, S. 337 ff., 359 ff.; *ders.*, DuD 200, 137 ff.

strukturen werden zunehmend von privaten Akteuren zur Verfügung gestellt. Die Aufgabe des Staates reduziert sich von einer Erfüllungs- zu einer Struktur-, Gewährleistungs- und Auffangverantwortung.[2273] Es geht um Fragen einer rechtlichen Technikgestaltung[2274] und einer staatlich regulierten Selbstregulierung.[2275]

Angesichts dieses Problembergs scheinen die Lösungen, die die unterschiedlichen wissenschaftlichen Disziplinen im Bereich von DRM-Systemen heute anzubieten haben, ernüchternd. Die *Techniker* arbeiten an immer neuen technischen Systemen zum Schutz digitaler Inhalte. In vielen Bereichen ist die Forschung noch nicht abgeschlossen. Kein Techniker weiß, wo die Reise wirklich hingehen wird. Die *Ökonomen* wissen noch zu wenig über die Zusammenhänge in Märkten für Informationsgüter, um verläßliche Aussagen machen zu können. Und daß die *Juristen* – sei es die Wissenschaft, seien es die Gerichte, seien es die Gesetzgeber – der gesamten technisch-ökonomischen Entwicklung hinterherhinken, ist wahrlich kein Novum.

Noch undurchsichtiger wird dieses Dickicht einer entstehenden Informationsgesellschaft,[2276] wenn man versucht, die Lösungsansätze der unterschiedlichen Disziplinen in Bezug zueinander zu setzen und miteinander zu vereinen. Wenn es dieser Arbeit gelungen ist, im Bereich von DRM-Systemen auch nur ein wenig Licht in das Dickicht zwischen Recht, Technik und Ökonomie zu bringen, wäre schon viel erreicht.

[2273] Vgl. *Roßnagel*, ZRP 1997, 26, 30; *Hoffmann-Riem*, S. 15 ff.

[2274] S. dazu *Roßnagel*, ZRP 1997, 26, 28 f.; *Hoffmann-Riem*, AöR 32 (1998), 513, 537. Zur damit zusammenhängenden Technikfolgenabschätzung s. *Roßnagel* in: Schulte (Hrsg.), S. 139 ff.; umfassend und interdisziplinär dazu *Bröchler/Simonis/Sundermann* (Hrsg.).

[2275] S. dazu ausführlich *Hoffmann-Riem* in: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), S. 261 ff.; vgl. weiterhin *Hoffmann-Riem/Schulz/Held*, S. 50: „Der Staat beschränkt sich darauf, die Strukturen zu schaffen, die eine Selbstregulierung ermöglichen, und gegebenfalls in den Selbstregulierungsprozeß einzugreifen, wenn und insoweit die Regulierungsziele durch Selbstregulierung nicht erreicht werden oder unerwünschte (Neben)-Effekte eintreten"; *Hoffmann-Riem*, AöR 32 (1998), 513, 537 f.; *Hoffmann-Riem* in: Schulte (Hrsg.), S. 3, 18 ff. Zur staatlich regulierten Selbstregulierung im Telekommunikationssektor s. *Hoffmann-Riem/Eifert* in: Hoffmann-Riem (Hrsg.), S. 9 ff.; zur staatlich regulierten Selbstregulierung im Datenschutzrecht s. *Roßnagel* in: Kubicek et al. (Hrsg.), S. 385, 390 f.; zur staatlich regulierten Selbstregulierung und indirekten Regulierung im Umweltrecht s. *Volkmann*, JuS 2001, 521 ff.

[2276] Zur Entwicklung der Informationsgesellschaft s. das bahnbrechende Werk von *Castells*.

Sachverzeichnis

(Die Zahlen beziehen sich auf die jeweiligen Seiten)