Dirk Günnewig (Dortmund)

Architecture is Policy!

Politische Steuerung durch Technik in digitalen Informations- und Kommunikationsnetzwerken am Beispiel des Einsatzes von *Digital Rights Management*-Systemen

Gemäß einem umfassenden Verständnis bestehen Digital Rights Management-*Systeme aus drei interdependenten Komponenten: technologische, rechtliche und wirtschaftliche Bestandteile. Aus ihrer Integration in eine soziale Umgebung resultieren vielfältige Interessenkonflikte, die die Steuerung der DRM-Systeme durch das Recht begleiten. Dieser Artikel untersucht aus* policy-*analytischer Perspektive eine neue Steuerungsstrategie für DRM-Systeme und damit auch für digitale Inhalte. Die konkreten Interessenkonflikte um den Einsatz von DRM-Systemen werden nicht adressiert, um den Rahmen dieses Artikels nicht zu sprengen. Der Artikel befasst sich jedoch mit den Effekten der vorgestellten Steuerungsstrategie auf politische Entscheidungsfindungsprozesse und der Implementation der Strategie in die politische Realität. Das zentrale Ziel dieses Artikels ist es, dem/der LeserIn einen Überblick über diese neue Form politischer Steuerung von digitalen Inhalten zu geben.*

Keywords: Code is Law, politische Steuerung, Regulierung, Politikfeldanalyse
Code is Law, regulation, governance, government, policy analysis

1. Einleitung

Das Urheberrecht ist nicht nur ein ökonomisches Schutzrecht. Der effektive Schutz des geistigen Eigentums durch Urheber- und ökonomische Verwertungsrechte ist nur ein Teil der im deutschen Urheberrechtsgesetz (UrhG) ausgedrückten staatlichen Ziele. Zugleich verfolgt der Staat damit das Ziel, die optimale Nutzbarkeit geistiger Güter durch die Allgemeinheit sicherzustellen. Es existiert eine urheberrechtliche Interessenbalance, die zwischen den InhaberInnen von Urheberrechten sowie den Werknutzern besteht. Dem liegt das Ziel zugrunde, Wissen und Innovationen in der Gesellschaft zu fördern. Einerseits will der Gesetzgeber einen (finanziellen) Anreiz zur Produktion geistiger Güter geben. Das UrhG sieht daher den Schutz der Werke als ein privates und vermögenswertes Gut vor. Dem Rechteinhaber wird die exklusive Auswertbarkeit des Werkes eingeräumt.

Im Gegenzug wird die freie Nutzbarkeit und der Zugang zu Wissen unter bestimmten Bedingungen vor dem Hintergrund für die Werknutzer eingefordert, dass Innovationen aus Innovationen hervorgehen. Diese Interessen der Allgemeinheit werden in klar definierten Schrankenbestimmungen ausgedrückt. Diese Interessenbalance droht im Internet aus dem Gleichgewicht zu geraten: Zunächst verschob sie sich zu Ungunsten der Rechteinhaber, denn geistige Güter sind massenhaft kostenlos in illegalen Distributionsplattformen erhältlich. *Digital Rights Management*-Systeme (DRM-Systeme) sollen dem einen Riegel vorschieben, indem sie die vom Rechteinhaber vorgesehenen Nutzungsregeln effektiv durchsetzen und illegale Nutzungen unterbinden.

Gesetzliche Bestimmungen zum Schutz vor Umgehung technischer Schutzmaßnahmen sorgen für eine Strafbewährung unerlaubter Handlungen. Nutzungsverträge werden seitens der Rechteinhaber eingesetzt, um NutzerInnen an bestimmte Nutzungsregeln zu binden. Sie werden mittels DRM-Technologien effektiv durchgesetzt.

In Folge der Kombination dieser drei Schutzmechanismen können gemäß dem UrhG einige Schrankenbestimmungen ausgehebelt werden, wie beispielsweise die Erlaubnis der Privatkopie. Die Verträge können durch die Rechteinhaber diktiert und dank DRM-Technologien effektiv durchgesetzt werden. Hier ist eine gesetzlich abgesicherte Privatisierung des Rechts erkennbar, die die Interessen der Allgemeinheit desavouiert. Ein unreguliertes DRM-System hat das Potential, ein *Digital Restriction Management*-System zu sein.

Die häufig am Gesetzgeber kritisierte Inflexibilität, auf solche komplexe Herausforderungen angemessen zu reagieren, trifft insbesondere hier zu, wie auch das so genannte Staatsversagen im Allgemeinen.

Nach einem kurzen Überblick über die technischen und rechtlichen Grundlagen von DRM-Systemen und die Herausforderungen der digitalen Distribution geistigen Eigentums wird eine Steuerungsstrategie herausgearbeitet, die den Herausforderungen der Diversifikation und Kontextabhängigkeit geistigen Eigentums und der technologischen Entwicklung Rechnung tragen soll. Kern des Artikels ist es, aus der Perspektive der politikwissenschaftlichen Steuerungsdebatte einen neuen Steuerungsansatz zu diskutieren,[1] der sich mit dem Konzept der Steuerung durch den Software-Code beschäftigt. Es sollen Überlegungen angestellt werden, wie die Steuerungskompetenz von der Privatwirtschaft zurück zum Staat verschoben werden könnte.

2. Begriffsbestimmung: DRM-Systeme = technische und rechtliche Bestandteile

Der Begriff *Digital Rights Management* sorgt immer wieder für Missverständnisse. Präziser wäre es, von *Rights Management for Digital Goods* zu sprechen. *Digital Goods* können verschiedene digitale Daten sein. In der öffentlichen Diskussion wird vor allem eine Untergruppe in den Vordergrund gestellt, nämlich die urheberrechtlich geschützten digitalen Medien, wie Musikstücke, Texte und Filme (*eContent*), auf die sich auch dieser Artikel bezieht.

DRM-Systeme zielen darauf ab, Nutzungsregeln an *eContent* effektiv durchzusetzen und ihn gegen unrechtmäßige bzw. unzulässige Nutzungen zu schützen (Garnett 2001). Sie bestehen aus technischen, rechtlichen und wirtschaftlichen Schutzmechanismen (Davis Jr. 2001; Bechtold 2002, 8; Günnewig/Hauser 2002; Guth 2002; Intel Corp. 2002, 3).

2.1. DRM-Technologien

DRM-Technologien sind aus verschiedenen technischen Komponenten modular aufgebaut. Ihr Ziel ist das Management von *eContent* und darauf bezogener Nutzungsregeln, die effektiv durchgesetzt werden. Anders ausgedrückt regeln DRM-Technologien, *wer welchen* eContent *wann* und *wo wie* nutzen kann. Sie sollen die grundsätzlich unkontrollierte Umgebung der Online-Distribution in eine kontrollierte umwandeln.

Eine Vielzahl optionaler Komponenten kommen zum Einsatz. Ihr Kern sind typischerweise Zugangskontrollverfahren, Identifizierungssysteme für NutzerInnen und Content, Verschlüsselungs- und Kopierschutzverfahren, Metadaten und *Rights Expression Languages*.[2]

Der/die KonsumentIn bestellt die digitalen Medien z.B. über eine eCommerce-Plattform beim Content-Provider. Dabei laufen mehrere Prozesse ab, die hier vereinfacht dargestellt werden. Im Mittelpunkt der DRM-Technologie steht der *eContent*, der in einem verschlüsselten digitalen Container (*secure container*) enthalten ist (Spenger 2003). Nur autorisierte NutzerInnen erhalten über einen speziellen Schlüssel Zugang.

Ein Problem der Verschlüsselung ist, dass der/die NutzerIn und die Clientsoftware nicht erfahren können, was sich in dem Container

befindet und welche Nutzungsregeln und -kosten sich auf den *eContent* beziehen. Diese Informationen stehen als Metadaten unverschlüsselt auf der Außenhülle des Containers. Sie enthalten Informationen zum *eContent*, u.a. zu den Urheberrechten (Herre 2003, 93; Paskin 2003). Ein wesentlicher Bestandteil sind die Nutzungsregeln. Sie regeln z.B. ob und wie oft der *eContent* kopiert, ob er anderen BenutzerInnen zur Verfügung gestellt werden darf, und ob die Nutzungserlaubnis zu einem bestimmten Termin ausläuft. Sie werden in Metadaten und *Rights Expression Languages* (REL) ausgedrückt. Mit dem Design von REL werden mehrere Ziele verbunden (Günnewig 2004, 239ff.): ein flexibler und ausbaufähiger Mechanismus für die Definition von Nutzungsregeln und Autorisierungen von NutzerInnen, die Interoperabilität zwischen verschiedenen technischen Systemen, die REL nutzen, sowie die einfache Definition von Nutzungsregeln beispielsweise durch die Content-Provider. In den REL kann etwa ausgedrückt werden, ob der/die BenutzerIn einen Inhalt abspielen, ausdrucken, kopieren, weitergeben oder kommentieren darf.

Oftmals werden menschlich nicht wahrnehmbare digitale Wasserzeichen in den Content integriert. Sie sind robust, d.h. weitestgehend sicher gegen Angriffe. Die Wasserzeichen beinhalten Informationen zum Rechteinhaber oder über den/die NutzerIn.

Der so vorbereitete *eContent* wird an das Medienabspielgerät übermittelt, das die Metadaten und REL richtig interpretieren kann und die Entschlüsselung entsprechend der darin festgelegten Nutzungsregeln vornimmt. Es ist von entscheidender Bedeutung für die Gesamtsicherheit des Systems, dass es sich um ein (vor Angriffen) sicheres Endgerät (*secure player*) handelt.

Nach seiner Identifizierung kann der/die KonsumentIn den *eContent* entsprechend der Nutzungsregeln nutzen. Zur Identifizierung werden in der Regel passwortbasierte Zugangsschutzverfahren genutzt. Hash-Wert basierte Verfahren, die aus der spezifischen Hardwarekonfiguration des Endgerätes einen bestimmten Wert ermitteln, der in die Identifikation einfließt, sind heute entgegen früherer Ansätze nicht mehr gebräuchlich. Eine Veränderung der Hardwarekonfiguration erforderte bei früheren DRM-Systemen eine erneute Übertragung des DRM-geschützten Contents.

DRM-Technologien bieten keinen hundertprozentigen Schutz des *eContent* gegen Angriffe (Shapiro/Vingralek 2001, 3f.; Bechtold 2002, 6, 89; Pfitzmann et al. 2002; Schneier 2002; Biddle et al. 2003, 345; Cheng/Rambhia 2003, 177; Felten 2003, 57; Gooch 2003, 22; Hauser/Wenz 2003). Ein Sicherheitsproblem beim Einsatz von DRM-Technologien ist, dass der digitale Content in die Ohren und Augen der KonsumentInnen gelangen muss. Selbst eine noch so raffinierte DRM-Technologie, die den Übertragungsweg bis hin zum Ausgabegerät wie dem Lautsprecher gegen Angriffe sichert, muss passen, wenn der *eContent* ausgegeben wird („*analog hole*“, Haber et al. 2003, 227). So kann z.B. ein Mikrophon vor den Lautsprecher gestellt werden. Oftmals können die Daten bereits innerhalb des Verarbeitungsgeräts, beispielsweise des Computers, abgegriffen werden.

2.2. Rechtliche Aspekte

Die rechtlichen Herausforderungen des Einsatzes von DRM-Systemen können aus zwei Perspektiven betrachtet werden (Bechtold 2004):

1. Schutz von technischen Maßnahmen
2. Schutz vor technischen Maßnahmen

Der Schutz von technischen Maßnahmen ist erforderlich, da die DRM-Technologie keinen hundertprozentigen Schutz vor Angriffen bietet. Kommt es zum Bruch des Schutzverfahrens, greift der urheberrechtliche Schutz. Zum Schutz dienen in DRM-Systemen drei rechtliche Komponenten (Günnewig 2003a):

1. Schutz durch Nutzungsverträge
2. Schutz durch Technologielizenzverträge
3. Schutz vor Umgehung technischer Maßnahmen durch straf- und zivilrechtliche Bestimmungen

Ihr Ziel ist es, rechtmäßige Nutzungen zu definieren und unrechtmäßige zu unterbinden. Die drei rechtlichen Mechanismen sind in urheberrechtliche Bestimmungen eingefasst.

Die Hoffnungen in Verträge sind groß, „… (to) become the instrument par excellence to fill the legal vacuum of the internet“ (Hugenholtz 1999, 308). Viele Computernutzer kennen Nutzungsverträge von der Softwareinstallation, wobei ein Vertrag durch Anklicken eines entsprechenden Buttons zu akzeptieren ist, ansonsten wird die Software nicht installiert.

Zwei Typen von Nutzungsverträgen sind zu unterscheiden:

1. DRM-Technologie-Nutzungsvertrag
   → vor der Installation der DRM-Software vom/von der NutzerIn zu akzeptieren
2. Content-Nutzungsvertrag
   → vor Nutzung des *eContents* vom/von der NutzerIn zu akzeptieren

In diesen Verträgen werden die Nutzungsregeln für die Software und vor allem für den *eContent* definiert. Der/die NutzerIn verpflichtet sich dabei darauf, die Schutzmechanismen nicht zu umgehen und die Nutzungsregeln einzuhalten.

Technologielizenzverträge werden zwischen den HerstellerInnen von Komponenten von DRM-Systemen abgeschlossen. Sie enthalten technische Implementationsvorschriften.

DRM-Technologien stellen sicher, dass die Bestimmungen des Vertrages eingehalten werden. Wird der technische Schutz jedoch umgangen, greifen urheberrechtliche Bestimmungen zum Schutz vor Umgehung technischer Maßnahmen. Das Umgehungsverbot wird durch straf- und/oder zivilrechtliche Sanktionen flankiert.

Das Verhältnis zwischen dem Einsatz technischer Schutzmaßnahmen in Verbindung mit Nutzungsverträgen und gesetzlichen Bestimmungen zum Schutz vor ihrer Umgehung auf der einen Seite und den urheberrechtlichen Schrankenbestimmungen auf der anderen Seite ist sowohl interessenpolitisch als auch juristisch umstritten und problematisch.

Um der Gefahr vorzubeugen, dass sich die Rechteinhaber durch Nutzungsverträge und den Einsatz technischer Schutzmaßnahmen ein eigenes Urheberrecht schaffen, wurden diese beiden Komponenten rechtlich eingeschränkt (Schutz vor technischen Maßnahmen). Urheberrechtliche Bestimmungen zur Wahrung der Interessen der Allgemeinheit – wie Schrankenbestimmungen – sollen einem allzu weitführenden Rechtsschutz der Rechteinhaber vorbeugen.

Der deutsche Gesetzgeber greift den Konflikt zwischen dem rechtlichen Schutz technischer Schutzmechanismen und der Garantie urheberrechtlicher Schranken auf (Günnewig et al. 2002). Werden technische Maßnahmen eingesetzt und ergreifen die Rechteinhaber keine freiwilligen Maßnahmen zur Ermöglichung der Privatkopie, können Privatkopien nicht erstellt werden, selbst wenn §53 UrhG dies erlaubt (Dreier/Nolte 2003, 499; Krüger 2004, 204). Ein *right to hack*, also eine Selbsthilfemaßnahme, die die Umgehung des Schutzmechanismus ermöglicht, beinhaltet das UrhG nicht (Reinbothe 2002; Reinbothe 2002a, 2).

Die Rechteinhaber sind gemäß §95b dazu verpflichtet, „… die notwendigen Mittel zur Verfügung zu stellen, um von diesen Bestimmungen in dem erforderlichen Maße Gebrauch machen zu können …“ (Art. 95b Abs. 1 UrhG). Hierbei setzt der Gesetzgeber auf die Mitwirkung der Rechteinhaber und zunächst auf deren freiwillige Maßnahmen.

Die entsprechenden Mittel kann der Schrankenbegünstigte vom Rechteinhaber einklagen. Der Gesetzgeber setzt dabei auf eine Selbstregulierung zwischen Vereinigungen von Rechteinhabern und Begünstigten, damit nicht jede/r Begünstigte die Rechteinhaber verklagen muss (Bechtold 2004, 34f.). Hierzu können sie beispielsweise untereinander Verträge schließen.

2.3. Wirtschaftliche Aspekte

Wie in den vorangegangenen Ausführungen gezeigt wurde, bieten die technischen und die rechtlichen Bestandteile von DRM keinen umfassenden Schutz gegen unrechtmäßige Nutzungen durch KonsumentInnen. Vor diesem Hintergrund lautet die Quintessenz: „Legale Angebote müssen gegen illegale Angebote konkurrieren!“ (Fetscherin 2003, 301).

DRM-Systeme können zwar die illegalen Quellen (*darknet*) urheberrechtlich geschützten *eContents* nicht austrocknen, allerdings wird an sie von der Inhalteindustrie die Hoffnung ge-

knüpft, einige der negativen Folgen und Probleme zu lindern und neue Geschäftsmodelle für *eContent* zu ermöglichen (Sobel 2003, 669). DRM-Systeme zielen darauf ab, die Bereitschaft der KonsumentInnen zu erhöhen, für den Content zu bezahlen (Sander 2002, 68). Attraktive Geschäftsmodelle und Medienangebote sind hierbei von zentraler Bedeutung.

3. Privatisierung des Rechtsschutzes

Mit der Privatisierung des Urheberrechts ist im Zusammenhang der Anwendung von DRM-Systemen gemeint, dass die Rechteinhaber den Werknutzern nahezu perfekt die Zugangs- und Nutzungsregeln für urheberrechtlich geschützte Werke vorschreiben können. Diese Entwicklung wird durch das gesetzliche Verbot der Umgehung technischer Maßnahmen unterstützt (Günnewig 2003).

Durch die Technik wird der/die NutzerIn auf die Einhaltung des Nutzungsvertrags verpflichtet. Die Folge ist, dass die DRM-Systeme aufgrund ihrer Charakteristika einen besseren und umfassenderen Schutz für die Interessen der Rechteinhaber bieten, als die *Real Space Architecture* – nämlich das UrhG – jemals zuvor.

Der Inhalteanbieter kann durch die Kombination der Schutzmechanismen in weiten Grenzen selbst den Schutzumfang und das -niveau festlegen, ohne auf eine gesetzliche Ausgestaltung der Schutzmechanismen zurückgreifen zu müssen (Koelman 2000, 279; Bechtold 2002, 370). Dabei besteht die Gefahr, dass die Schrankenbestimmungen durch eine Kombination des Einsatzes von technischen Maßnahmen wie DRM-Systemen, vertraglichen und gesetzlichen Bestimmungen zum Schutz vor Umgehung technischer Maßnahmen zu Ungunsten der Werknutzer durch die Rechteinhaber ausgehebelt werden (Samuelson 1999, 548f.; Koelman/Helberger 2000, 189ff.; Grassmuck 2003, 1016f.). Eine derartige Situation bezeichnet Shapiro (1999, xv) mit dem Begriff der „*control revolution*". Damit ist gemeint, dass die Möglichkeit zur Kontrolle von Institutionen zu den Individuen überwechselt. Dies lässt sich auf kollektive AkteurInnen ausweiten. Damit kommt es zu einer neuen Situation: Schutzumfang und -intensität, die bislang durch das Urheberrecht definiert wurden, werden durch gesellschaftliche AkteurInnen vorgegeben (Bechtold 2002, 370).

Diese Entwicklung hin zur Privatisierung des Rechtsschutzes wird gesetzlich gestützt, indem Nutzungsverträge als wirksam anerkannt werden und die Umgehung technischer Schutzmaßnahmen verboten wird (Bechtold 2002, 370, 439): „Rightsholders can effectively write their own intellectual property statute in computer code" (Burk/Cohen 2001, 51).

Damit gehen Beobachtungen einher, dass am Markt befindliche DRM-Systeme vor allem die Interessen der Rechteinhaber berücksichtigen, die diese Systeme einsetzen (Stefik 2000, 96; Lessig 2001, 110, 200; Fox 2002; Fox/LaMacchia 2003, 61).

4. Steuerungskonzept: *„Code is Law"*

„*The answer to the machine is in the machine.*"
(Clark 1996, 139)

Die Regulierung des Internets und darüber realisierter Anwendungen und Kommunikationsprozesse findet großes Interesse in politikwissenschaftlichen Steuerungsdebatten. Die Zeit ist vorüber, in der pauschal angenommen wurde, dass es resistent gegenüber Steuerungsinterventionen sei und der Nationalstaat seine Souveränität im so genannten Cyberspace verloren habe (Goldsmith 1998; Berman 2000, 1263, 1281; Weinstock Netanel 2000, 401).

Obwohl einige AkteurInnen fordern, dass das Internet frei von staatlichen Interventionen bleiben soll, beanspruchen die Nationalstaaten für sich, steuernd einzugreifen. Die Suche nach effektiven und technologieadäquaten Steuerungskonzepten kennzeichnet die gegenwärtige Steuerungsdebatte.

Die Steuerung des Akteursverhaltens in IuK-Netzen kann durch andere Steuerungsinstrumente als durch das Recht bzw. durch Gesetze erfolgen, so der Tenor der jüngeren Diskussionen der *Code is Law*-Debatte.

Bezogen auf geistiges Eigentum können demnach zwei Strategien verfolgt werden, um Eigentumsinteressen der Rechteinhaber wirksam zu schützen und gleichzeitig Ausnahmen davon zugunsten der Allgemeinheit zu realisieren:

1. Traditioneller Schutz des Urheberrechts – Basierend auf politischen Entscheidungen definieren Gesetze einen Raum und die Bedingungen, unter denen Dritte in ihn eindringen dürfen. In Fällen unrechtmäßigen Eindringens greifen zivil- oder strafrechtliche Sanktionen.
2. Schutz durch technische Vorrichtungen – Auch hier wird ein solcher Raum definiert, um den jedoch kein rechtlicher, sondern ein code-basierter, programmierter „Zaun" gezogen wird, der unerwünschtes Eindringen verhindert (Lessig 1999, 122; Lessig 2001a, 219).

Das Konzept des *Code is Law* setzt sich mit Fragen der Steuerbarkeit des Cyberspace und mit den Auswirkungen staatlicher Interventionen auf das Akteursverhalten auseinander.

4.1. Kernthese und Begriffsverständnis

Im *Real Space* sind Gesetze, die Bankraub kriminalisieren, hilfreich, doch dicke Mauern, schusssicheres Glas und bewaffnete Wächter sind die besseren und effektiveren Mittel gegen Bankraub (Greenleaf 1998, 604). Im Cyberspace sind Gesetze, die die unrechtmäßige Nutzung von *eContent* verbieten auch hilfreich, um illegale Handlungen zu sanktionieren. Doch technische Schutzmaßnahmen, die unrechtmäßige Handlungen unterbinden, sind ungleich effektiver, nicht zuletzt aufgrund der mangelhaften Möglichkeit der Strafverfolgung in IuK-Netzen. Der Software-Code und die Hardware-Architektur sollen im Cyberspace Mauern um geistiges Eigentum ziehen.

Die Kernthese der Steuerungsstrategie Code ist, dass die technische Architektur der Hard- und Software in ihren regulativen Auswirkungen einer rechtlichen Regulierung gleichkommen kann. Bestimmte Steuerungsaufgaben, die bislang in rechtlichen Bestimmungen ausgedrückt wurden, werden an die technologische Architektur übertragen. Nicht mehr das Recht, sondern die Technik (Code) steuert das Verhalten der AkteurInnen und deren Handlungsoptionen, indem sie bestimmt, wie sich ein Computersystem und damit dessen NutzerInnen verhalten können (Reidenberg 1998, 568; Lessig 1999a, 410; Lutterbeck 2000, 52; Weinstock Netanel 2000, 400; Shah/Kesan 2002; Zoellick 2002, xvii).

> The code of cyberspace – its architecture and the software and hardware that implemented that architecture – regulates life in cyberspace generally. Its code is its law (Lessig 2001, 35).

Damit wird der Hauptunterscheidungspunkt zum Recht deutlich. Das Recht ist ein ex-post-Schutz, es wird nach einer erfolgten Straftat durch Strafverfolgungsbehörden und Gerichte durchgesetzt. Hingegen kommt es bei der Steuerung durch den Code nicht so weit, denn er unterbindet Straftaten von vornherein auf technischem Wege: Der/die NutzerIn hat keine Alternative zur Befolgung der durch den Code durchgesetzten Nutzungsregeln. Die Steuerung durch den Code ist somit ein ex-ante-Schutz (Reidenberg 1998, 572; Hugenholtz 1999, 315).

Allerdings ist anzumerken, dass durch den Code nicht nur festgelegt wird, wie sich ein IuK-System verhält und wie NutzerInnen dieses nutzen können. Zudem legt er fest, wie mit grundsätzlichen Werten der Gesellschaft wie Privatsphäre, Redefreiheit und ähnlichem umgegangen wird (Shah/Kesan 2002, 5).

Eine der Kernannahmen des *Code is Law*-Konzeptes ist, dass Code die Definition und Durchsetzung von Nutzungs- und Verhaltensregeln weitreichend ermöglicht (Lessig 1999a, 410). Der Code wird, wie auch Gesetze, von Menschenhand geschrieben und ist effektiv steuerbar (Lessig 1996, 1408). Die Technologie gibt dem Gesetzgeber und anderen steuerungskompetenten Akteuren ein neues Instrument in die Hand, um Adressatenverhalten wirksam und zuverlässig zu steuern. Dazu wird die Konfiguration des technischen Systems beeinflusst (Reidenberg 1998, 568).

Auf den ersten Blick erscheint es, als ob der Code aufgrund seiner Ausschließlichkeit anders

als das schlecht in internationalen IuK-Netzen durchsetzbare (nationale) Recht nicht durchbrochen werden könnte. Die Hoffnung einiger Autoren und Autorinnen, dass der Code nahezu perfekt die Nutzung geistiger Güter im Internet steuern kann, können DRM-Technologien allerdings aufgrund ihrer geschilderten Sicherheitsprobleme nicht erfüllen. Die Steuerung durch den Code kann somit illegal umgangen werden. Code unterscheidet sich damit nur bedingt vom Recht. Recht und Code sind beide im Cyberspace keine hundertprozentig effektiven Steuerungsinstrumente.

Trotz der Sicherheitsprobleme ist die Steuerung durch den Code im Vergleich zu rechtlichen Steuerungsmethoden jedoch deutlich effektiver, denn seine Durchsetzbarkeit ist im Cyberspace wesentlich höher als die von Gesetzen. Die Kombination der Steuerung durch Gesetze und Code erreicht ein merklich höheres Schutzniveau als einer der beiden Schutzmechanismen für sich genommen.

Zusammenfassend wurde deutlich, dass der Code eine neue Methode der Verhaltenssteuerung in Bezug auf die Nutzung einer IuK-Technologie ist, die im Cyberspace im Vergleich zum Recht um einiges effektiver Handlungsrestriktionen und -spielräume definieren kann. Code entspricht eher den Anforderungen und den Spezifika der IuK-Systeme weitreichender als das Recht.

4.2. Verhältnis zwischen Code und Recht: Steuerung des Codes von DRM-Systemen entsprechend gesetzlicher Vorgaben

Bezogen auf das Steuerungskonzept ist die Betrachtung des Verhältnisses zwischen der technologischen Architektur der Hard- und Software (Code) und den rechtlichen Bestimmungen wesentlich:

> Politics and technology are linked. The linkages occur when program administrators translate political forces into design parameters, accomodating interests by modifying the system under development (Klein 2000, 316).

TechnikerInnen schreiben Code und legen damit die Handlungsoptionen der Systemnutzer fest. Sie sind dabei in soziale Kontexte eingebunden, wie z.B. in Standardisierungsgremien. Zudem werden sie durch Gesetze beeinflusst (Eichener/Voelzkow 1995, 253; Reidenberg 1998, 571). In der wissenschaftlichen Diskussion über DRM-Technologien setzt sich zunehmend folgendes Verständnis durch:

> Instead of taking DRM systems as given constants that are exogenous to the policy process, this article joins an emerging scholarship which asks how DRM systems could be altered in a value-centered design process so that important policy and legal values are preserved (Bechtold 2003, 599).[3]

In Deutschland erfolgt die Techniksteuerung gemäß Eichener und Voelzkow im Wesentlichen durch die technische Normung und nur in Ausnahmefällen durch Gesetze. Erst am Ende der Technikentwicklung und -gestaltung bestehe die Möglichkeit zur interessenpolitischen und gesetzlichen Beeinflussung, um mit der Absicht der Verwirklichung gemeinwohlorientierter Ziele Korrekturen am Code vorzunehmen. Sie weisen darauf hin, dass insbesondere in innovativen Technikfeldern eine entwicklungsbegleitende Normung stattfände, in „… der die sachliche und institutionelle Trennung von Forschung, Entwicklung und Normung überwunden wird“ (Eichener/Voelzkow 1995, 253).

Demnach kann in solchen Bereichen schon zu einem früheren Zeitpunkt die Technikentwicklung beeinflusst werden. Regulative technische Standards werden oftmals zwischen privaten AkteurInnen getroffen. Sie definieren Restriktionen hinsichtlich der konkreten Ausgestaltung der Technologie und der wirtschaftlichen Möglichkeiten ihrer Anwendung (Voelzkow 1994, 134; Davidson et al. 2002, 2).

Eichener und Voelzkow kommen zu dem Ergebnis, dass die technische Standardisierung auch hinsichtlich außertechnischer Folgen des Technologieeinsatzes eine entscheidende Rolle spielt. Sie definieren den Handlungsrahmen, den Technologien für soziales Verhalten vorgeben. Daher ist es für staatliche Regulatoren wichtig, Einfluss auf die Standardisierungsgremien auszuüben.[4]

Die Standardisierung hat in Bezug auf DRM-Systeme nicht den Stellenwert, den Ei-

chener und Voelzkow ihnen in ihren allgemeineren Betrachtungen zuschreiben. Dafür sprechen mehrere Gründe: modularer Aufbau, Flexibilität hinsichtlich der Nutzungsregeln für *eContent* und damit weitreichende Neutralität gegenüber außertechnischen Folgen und Relevanz nationalstaatlicher urheberrechtlicher Regeln. DRM-Technologien sind hinsichtlich der Nutzungsregeln für *eContent* flexibel. Aufgrund dessen besteht eine weitreichende Neutralität bezüglich der außertechnischen Folgen.

Die Technologie-Hersteller besitzen ein enormes Interesse an der Flexibilität der Systeme hinsichtlich der Nutzungsregeln für *eContent*. Dadurch sollen die Content-Provider je nach Geschäftsmodell äußerst differenzierte Nutzungsregeln durchsetzen können. Zudem sollen damit die Anforderungen verschiedener nationalstaatlicher Urheberrechtsgesetze berücksichtigt werden können, damit die Systeme auf möglichst vielen Märkten durch die Technology-Provider angeboten werden können. Andernfalls könnte es dazu kommen, dass Content-Provider die Systeme nicht nutzen, weil sie keine legalen Angebote damit realisieren können. Dies widerspräche dem Geschäftsinteresse der Technology-Provider.

Voelzkow (1994, 134) führt zudem zur technischen Standardisierung aus, dass technische Normen auch außertechnische Kriterien und Wertbezüge reflektieren. Dies ist bei Standards bezüglich der DRM-Technologiekomponenten nicht gegeben, solange das eben beschriebene Ziel der Flexibilität von den Technology-Providern verfolgt wird.

Die DRM-Technologie verursacht in Folge ihrer Flexibilität hinsichtlich der Nutzungsregeln und ihrer Modulierbarkeit aufgrund verschiedener alternativer Technologiekomponenten prinzipiell keine negativen sozialen, politischen und wirtschaftlichen Externalitäten, sollte das System keine signifikante Barriere zur rechtmäßigen Nutzung von *eContent* für die Konsumentinnen und Konsumenten darstellen. Ein restriktives System, das die Nutzung entsprechend der urheberrechtlichen Vorgaben erschwert, wenn beispielsweise zum Hören eines Musikalbums nach jedem Musikstück erneut das Passwort abgefragt werden würde, könnte KonsumentInnen vom Kauf abhalten und somit wirtschaftliche Externalitäten verursachen. Negative wirtschaftliche Folgen können auch dadurch entstehen, dass ein DRM-System im Gegensatz zu den illegalen Downloadangeboten unrechtmäßige Nutzungen unterbindet, die das Urheberrechtsgesetz verursacht.

Die Externalitäten resultieren vor allem aus der Konfiguration der DRM-Systeme. Je nachdem, welche Komponenten von den DRM-Service- oder -Technology-Providern wie zusammengestellt werden und vor allem welche Nutzungsregeln definiert werden, resultieren aus dem Technologieeinsatz unterschiedliche negative Externalitäten für die beteiligten AkteurInnen und die beschriebene Balance im Urheberrecht. Steuerungskonzepte sollten sich daher auf die Steuerung der Systemkonfiguration konzentrieren. Zur Verwirklichung des Steuerungsziels sollen technische und organisatorische Strukturen entwickelt werden.

Nationalstaatliche urheberrechtliche Regeln sind im Bereich von DRM-Technologien relevant. Dafür sprechen mehrere Gründe. DRM-Technologien verarbeiten urheberrechtlich geschützten *eContent*. Die Designanforderungen an die Konfiguration und Anwendung der DRM-Technologie-Komponenten werden basierend auf urheberrechtlichen Bestimmungen definiert. Damit ist der regulative Zugriff basierend auf dem UrhG sehr gut möglich, sofern der diese Systeme einsetzende Content-Provider nationalstaatlichen urheberrechtlichen Regeln unterworfen werden kann.

Die DRM-Technologien setzen lediglich die Bestimmungen um, die das UrhG für die Nutzung von urheberrechtlich geschütztem *eContent* vorsieht. Wie angesprochen wurde, ist nicht die DRM-Technologie selbst, sondern ihre konkrete Konfiguration in Anwendungskontexten der Gegenstand gesetzlicher Bestimmungen bzw. Steuerungsversuche.

Auch die Konfiguration wird nicht direkt gesteuert, sondern die Art und Weise, wie die Beteiligten mit urheberrechtlich geschützten Werken umgehen dürfen. Dadurch sollen die mit dem Urheberrecht verbundenen politischen Ziele realisiert werden.

Vor diesem Hintergrund bietet sich die Techniksteuerung durch Normung nicht an, um nationalstaatliche, im Urheberrecht ausgedrückte politische Ziele zu realisieren. Die Anforderungen an DRM-Technologien werden in gesetzlichen Bestimmungen ausgedrückt, die berücksichtigt werden müssen, damit Content-Provider die DRM-Systeme legal einsetzen können, ohne rechtliche Sanktionen befürchten zu müssen. Angesichts der Variabilität der DRM-Systeme hinsichtlich der Nutzungsmöglichkeiten von *eContent* kann der Gesetzgeber grundsätzlich direkt (hierarchisch) gesetzlich die DRM-Systeme steuern.

Dies gilt sofern er Einfluss auf die DRM-Technology-, -Service- oder Content-Provider üben kann. Der Staat könnte den Inhalteanbietern die Verwendung solcher technischer Schutzmaßnahmen verbieten, die die urheberrechtlichen Schranken nicht beachten. Eine andere Möglichkeit wäre, derartigen Schutzmaßnahmen den rechtlichen Umgehungsschutz zu entziehen (*right to hack*) (Bechtold 2002, 409). Auf diese Weise könnte der Staat auch auf solche Inhalteanbieter signifikanten Einfluss hinsichtlich der Verhinderung eines zu weitreichenden Rechtsschutzes ausüben, die ihren *eContent* aus einem dritten Staat anbieten. Dass sich die Medienunternehmen aufgrund dessen aus dem lukrativen deutschen Markt zurückziehen, ist unwahrscheinlich.

Diese direkte Steuerung durch die gesetzliche Beschränkung der technischen Schutzmechanismen ist in vielen Urheberrechtsgesetzgebungen weltweit zu erkennen (Bechtold 2002, 416). Der rechtliche Umgehungsschutz ist ein Beispiel für gesetzliche Bestimmungen bezogen auf DRM-Technologien. Allerdings regulieren sie nicht die DRM-Technologien selbst, sondern lediglich ihr Umfeld, indem sie den Schutz durch eine straf- und zivilrechtliche Absicherung verbessern.

Code und Gesetz können demnach eng miteinander zusammenhängen: Code implementiert Gesetze effektiv und Gesetze definieren die durch den Code realisierten Verhaltensrestriktionen der Systemnutzer.

Lessig (1999, 122f.; 2001a, 226) weist darauf hin, dass die Steuerung durch den Code nicht die Steuerung durch das Recht gänzlich ablöst, sondern ergänzt. So existiere ein Mischungsverhältnis zwischen den beiden Ansätzen.

Code ist das Gesetz, doch das Verständnis ist ein anderes, als wenn von Gesetzen gesprochen wird, die die Parlamente verabschieden. Code bestimmt die Funktionsweise des technischen Systems, er setzt Handlungen Restriktionen und eröffnet Spielräume. So gesehen ist Code das Gesetz des Computers. Wird jedoch – wie bei Lessig – davon gesprochen, dass Code Funktionen des Gesetzes übernehmen soll, so kann vor dem Hintergrund des Selbstverständnisses und der Anforderungen eines demokratisch parlamentarischen Systems nicht mehr von *Code is Law* gesprochen werden. Code ist dann Gegenstand von Gesetzen. Code ist das Gesetz des Computers, aber gesetzliche Bestimmungen sind die Gesetze des Code. Demnach ist Code ein mögliches Steuerungsinstrument, dessen sich der Gesetzgeber oder andere steuerungskompetente AkteurInnen bedienen, um politische Ziele möglichst effektiv in der gesellschaftlichen Realität durchzusetzen. Er ist so etwas wie die straf- oder zivilrechtlichen Bestimmungen, die ein Gesetz durch die Androhung von Strafen als Steuerungsinstrument absichern. Dies wird durch die Beeinflussung der Systemkonfiguration realisiert.

Code kann somit Gegenstand der politischen Steuerung sein. Code wird derart gesteuert, dass er hilft, bestimmte Steuerungsziele zu verwirklichen. Durch die Steuerung des Code wird erreicht, dass er das Verhalten seiner NutzerInnen steuert. Es handelt sich um eine indirekte Form der Verhaltenssteuerung. Konkreter: Code sollte gesteuert werden, um Steuerungsziele des Urheberrechts effektiv durchzusetzen. Code ist somit ein Instrument politischer Steuerung, dessen Ziel es ist, menschliches Verhalten zu steuern.

> In answer to those who say that the net can not be regulated, I've argued that whether it can be regulated depends on its architecture. Some architectures would be regulable, others would not (Lessig 1999, 107).

Code erweitert die Möglichkeiten des Rechts (bzw. von Gesetzen), während Gesetze den

Code absichern. Code und Recht (bzw. Gesetze) stehen somit in einem engen Zusammenhang und überlappen (Reidenberg 1998, 583, 586). Dem liegt das Verständnis zugrunde, dass DRM-Technologien flexibel sind und weitreichend an politische Vorgaben angepasst werden können. Sie müssen nicht notwendigerweise nur die Interessen der Rechteinhaber wahren, wie ihnen oftmals vorgeworfen wird.

Vor dem Hintergrund der Ausführungen zur Steuerung durch den Code und zum deutschen Urheberrecht sind mehrere Forderungen an den Code von DRM-Technologien zu stellen:

1. Garantie einer neutralen und vertrauenswürdigen technischen Architektur, in der die politisch (durch den Staat und/oder gesellschaftliche AkteurInnen) definierten Ziele und Handlungsbedingungen umgesetzt werden können. Mit neutral ist gemeint, dass sie auch nicht durch versteckte technische Funktionen versteckten Interessen dienen darf.
2. Das System muss sicher gegen Angriffe sein.

5. Fazit: Vor- und Nachteile der Steuerung durch den Code von DRM-Systemen

Die Vorteile der Steuerung durch den Code sind bezogen auf DRM-Systeme im Vergleich zu Gesetzen:

1. Code reagiert schnell, Gesetze langsam – Technische Innovationen und neue Nutzungsmöglichkeiten von *eContent* schaffen in kurzen Zyklen politische und rechtliche Herausforderungen. Gesetzliche Bestimmungen verlieren oftmals den Wettlauf mit der Technologie, denn Gesetzgebungsprozesse sind in der Regel langwierig. Die Abänderung des Codes und damit der durch ihn durchgesetzten Nutzungsregeln ist hingegen über IuK-Netze innerhalb von Sekunden per Tastendruck möglich (Shapiro 1999, 14; Zoellick 2002, xvii).
2. Code steuert Verhalten ex-ante, Gesetze ex-post.
3. *Customization of rules* – Urheberrechtliche Regeln können aufgrund der hohen Flexibilität von DRM-Technologien weitreichend an unterschiedliche Anforderungen angepasst werden (Reidenberg 1998, 577, 579f.).
4. Code ist global, Gesetze national – Code ist im Internet international durchsetzbar, (nationale) Gesetze sind im Internet nicht international durchsetzbar.
5. Code ist effektiv, Gesetze sind ineffektiv – Nationale Gesetze sind angesichts der Globalität des Internets oftmals nicht in der Lage, Verhalten effektiv zu steuern. Ein Problem ist die grenzüberschreitende Strafverfolgung. Hingegen erlaubt es der Code, nationale Grenzen im Internet wieder zu errichten, indem z.B. durch DRM-Technologien nationalstaatliche urheberrechtliche Regeln durchgesetzt werden. Diese Regeln können auch die Grenzen des Nationalstaates überschreiten, so dass Content-Provider aus dritten Staaten diese gesetzlichen Anforderungen befolgen müssen, um *eContent* KonsumentInnen im betreffenden Staat offerieren zu können. Berücksichtigen sie diese nicht, so könnte ihnen etwa der rechtliche Schutz vor Umgehung technischer Maßnahmen verwehrt werden. Technische Nutzungsregeln sind somit international eher durchsetzbar als rechtliche (Berman 2000, 1265).
6. Transparenz der Nutzungsbedingungen beim Code – Vor der Nutzung ist für den/die NutzerIn transparent, ob eine spezifische Nutzung unter die Schrankenbestimmung fällt. Aufgrund von fehlendem juristischen Fachwissen wusste er/sie dies im analogen Bereich oftmals nicht.

Zwei wesentliche Nachteile können gegenüber dem Ansatz der Steuerung durch den Code vorgebracht werden, die eng miteinander verbunden sind: So sind die urheberrechtlichen Schranken nicht eindeutig in Code ausdrückbar, und eine einseitige Steuerung ist nicht möglich.

Mehrere AutorInnen (Burk/Cohen 2001, 55, 65, 79; Bechtold 2002, 409; Lohmann 2002; Felten 2003, 58; Lohmann 2003, 6; Uzuner et al. 2003, 5) halten es für unwahrscheinlich, dass im Code das gesamte Spektrum von Schranken ausgedrückt werden kann, die die urheber-

rechtlichen Schrankenbestimmungen und ihre Auslegung durch die Gerichte den NutzerInnen einräumen:

> It seems fairly certain that no one can mathematically model fair use, as it is understood today, because the legal definition of fair use is fuzzy and imprecise (Fox/LaMaccia 2003, 63).[5]

Die *Fair Use*-Bestimmungen des amerikanischen Copyrights sind den Schrankenbestimmungen des deutschen UrhG ähnlich. Auch sie sehen Ausnahmen vom exklusiven Verwertungsrecht der Rechteinhaber vor.

Das Problem für die Entwicklung von DRM-Technologien ist, dass nicht klar mitgeteilt werden kann, in welchen Fällen Nutzungen gemäß der *Fair Use*-Bestimmungen ermöglicht werden müssen. *Fair Use* ist in vielen Fällen hochgradig situationsspezifisch bestimmt. Die Auslegung des *Fair Use* erfolgt daher oftmals erst durch die Gerichte. Der jeweilige Nutzungskontext entscheidet, ob eine Nutzung gemäß der Bestimmungen des *Fair Use* bzw. der urheberrechtlichen Schranken erlaubt ist.

Die erforderliche Fall-zu-Fall-Entscheidung über den Bedarf des Zugangs in einem spezifischen Nutzungskontext erfordert ein (menschliches) Entscheidungsvermögen, das nicht durch technische Vor-Einstellungen nachgeahmt werden kann (Felten 2003, 58).

Das deutsche Urheberrecht unterscheidet sich hinsichtlich des Umfangs situationsspezifisch zu entscheidender Fälle vom US-amerikanischen. Die fallbezogene Entscheidung nehmen in den USA Gerichte vor. Im deutschen UrhG wird sie bereits weitreichend durch den Gesetzgeber vorweggenommen. Deutsche Schrankenbestimmungen sind präziser formuliert und erfassen nur bestimmte, einzeln festgelegte Einzelfälle. Es ist daher im deutschen Urheberrecht in einer geringeren Anzahl von Fällen eine situationsspezifische Festlegung erforderlich, ob es sich um eine Schrankennutzung handelt. Das heißt, dass es in Deutschland tendenziell weitaus einfacher sein sollte, zahlreiche Schrankennutzungen in DRM-Technologien zu kodieren.

Zusammenfassend kann nicht davon ausgegangen werden, dass der Gesetzgeber lediglich die DRM-Systeme gesetzlich steuern muss, um Schranken und andere Ziele des Urheberrechts durchzusetzen. Bei diesem Steuerungsmechanismus wird es laut Bechtold (2002, 409) in Einzelfällen dazu kommen, dass eine DRM-Technologie die Nutzung verweigert, obwohl eine Schrankenbestimmung greift. Damit sind diesem Steuerungsmechanismus Grenzen gesetzt. Sie deuten darauf hin, dass weitere Steuerungsmechanismen erforderlich sind, um die gesamte Bandbreite urheberrechtlicher Schranken zu garantieren.

Für bestimmte Systeme trifft es also zu, dass ein einzelner steuernder Akteur effektiv das Verhalten der Systembenutzer steuern kann. Für andere Systeme gilt dies jedoch nicht – nicht zuletzt angesichts der Internationalität des Internets. So kann ein Staat oftmals keinen Einfluss auf den Code bestimmter Technologien – wie z.B. DRM-Technologien – ausüben, wenn der/die AnbieterIn des Contents und der DRM-Technologien seine/ihre Dienstleistungen aus einem anderen Staat mit einem ihm/ihr genehmeren Rechtssystem anbieten kann (Barlow 1998). Eine einseitige Steuerung ist somit häufig nicht möglich.

Die Beeinflussung ist oftmals unmöglich, denn Nationalstaaten können im derzeitigen Internet in der Regel keine Informationspakete an den territorialen Grenzen stoppen, die via IuK-Netze transferiert werden (Burk 1998, 960f.). Goldsmith (1998, 1123) merkt hierzu an, dass der Nationalstaat auch im physischen Bereich meist nicht die Möglichkeit habe, sämtliche Postpakete zu kontrollieren, die über die Staatsgrenzen in den Staat hineingelangen. Mit Stichproben reagieren Nationalstaaten auf solche schwer kontrollierbaren Importe. Stichproben sind auch im digitalen Bereich mit einem gewissen Aufwand möglich. Ist die zu erwartende Strafe ausreichend hoch und die Stichprobe umfassend genug, schreckt sie potentielle TäterInnen ab.

Zusammenfassend kann dennoch davon ausgegangenen werden, dass durch den Code gesellschaftliches Handeln grundsätzlich effektiv gesteuert werden kann. Er sorgt dafür, dass insbesondere einfache NutzerInnen von illegalen Handlungen abgehalten werden. Jedoch ist

anzumerken, dass ExpertInnen oft rasch Umgehungswerkzeuge entwickeln, mit denen die codierten Handlungsrestriktionen der DRM-Systeme umgangen werden können. Oftmals integrieren sie dieses Fachwissen wenig später in leicht bedienbare Softwaretools und erlauben es so auch dem/der einfachen NutzerIn, Restriktionen zu umlaufen (Haber et al. 2003, 230).

Daher wird die nachträgliche Klagemöglichkeit von Rechteinhabern gegen Rechtsverletzungen durch NutzerInnen immer ein wichtiger Bestandteil sein, die Steuerung durch Code rechtlich abzusichern. Code dient in DRM-Technologien dazu, die folgende Maxime zu erfüllen: „Keep honest people honest."

ANMERKUNGEN

1 Dieser Ansatz wird ausführlicher dargestellt in Günnewig (2004).
2 Ausführlicher bei Becker et al. 2003. Eine umfassende Darstellung folgt in Günnewig 2004, 211ff.
3 Vgl. auch Burk/Cohen 2001; Mulligan/Burstein 2002; Cohen 2003; Erickson 2003; Fox/LaMacchia 2003.
4 Vgl. auch Reidenberg 1998, 589f.
5 Vgl. auch Bechtold 2001; Felten 2003, 58.

LITERATUR

Barlow, John Perry (1998). Wein ohne Flaschen. Globale Computernetze, Ideen-Ökonomie und Urheberrecht, in: Stefan *Bollmann* (Hg.): Kursbuch Internet, Hamburg, 83–112.

Bechtold, Stefan (2001). Fair Use by Design or by Law? Internet: http://www.jura.uni-tuebingen.de/~s-bes1/drm/fair_use_by_design.pdf.

Bechtold, Stefan (2002). Vom Urheber- zum Informationsrecht – Implikationen des Digital Rights Management, München.

Bechtold, Stefan (2003). The Present and Future of Digital Rights Management – Musings on Emerging Legal Problems, in: Eberhard *Becker*/Willms *Buhse*/Dirk *Günnewig*/Niels *Rump* (Hg.): Digital Rights Management. Technological, Economic, Legal and Political Aspects, Heidelberg/Berlin, 597–654.

Bechtold, Stefan (2004). Schutz und Identifizierung durch technische Maßnahmen, in: Thomas *Hoeren*/Ulrich *Sieber* (Hg.): Handbuch Multimedia-Recht, Teil 7.11 in der 9. Ergänzungslieferung (i. E., vorab vom Autor zugeschickte Fassung. Die Seitenzahlen stimmen nicht denen mit der veröffentlichten Fassung überein).

Becker, Eberhard/Willms *Buhse*/Dirk *Günnewig*/Niels *Rump* (Hg.) (2003). Digital Rights Management. Technological, Economic, Legal and Political Aspects, Heidelberg/Berlin.

Berman, Paul Schiff (2000). Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to „Private" Regulation, in: University of Colorado Law Review, 71, 1263–1310.

Biddle, Peter/Paul *England*/Marcus *Peinado*/Bryan *Willman* (2003). The Darknet and the Future of Content Protection, in: Eberhard *Becker*/Willms *Buhse*/Dirk *Günnewig*/Niels *Rump* (Hg.): Digital Rights Management. Technological, Economic, Legal and Political Aspects, Heidelberg/Berlin, 344–365.

Burk, Dan L. (1998). Virtual Exit in the Global Information Economy, in: Chicago-Kent Law Review, 73, 943–995.

Burk, Dan L./Julie E. *Cohen* (2001). Fair Use Infrastructure for Rights Management Systems, in: Harvard Journal of Law and Technology, 15(1), 41–84.

Cheng, Spencer/Avni *Rambhia* (2003). DRM and Standardization – Can DRM be Standardized?, in: Eberhard *Becker*/Willms *Buhse*/Dirk *Günnewig*/Niels *Rump* (Hg.): Digital Rights Management. Technological, Economic, Legal and Political Aspects, Heidelberg/Berlin, 162–177.

Clark, Charles (1996). The Answer to the Machine is in the Machine, in: P. Bernt *Hugenholtz* (Hg.): The Future of Copyright in a Digital Environment – Proceedings of the Royal Academy Colloquium organized by the Royal Netherland Academy of Science (KNAW) and the Institute for Information Law (Amsterdam, 6–7 July 1995), The Hague/London/Boston, 139–145.

Cohen, Julie (2003). DRM and Privacy, in: Communications of the ACM. Special Issue: Digital rights management and fair use by design, 46(4), 47–49.

Davidson, Alan/John *Morris*/Robert *Courtney* (2002). Strangers in a Strange Land: Public Interest Advocacy and Internet Standards, Center for Democracy and Technology. Internet: http://www.intel.si.umich.edu/tprc/papers/2002/97/Strangers_CDT_to_TPRC.pdf.

Davis Jr., David D. (2001). What Digital Rights Management Means Today, in: Computers in Libraries, 21(6). Internet: http://www.copyright.com/PDFs/ComputerLibraries.pdf.pdf.

Dreier, Thomas/Georg *Nolte* (2003). The German Copyright – Yesterday, Today, Tomorrow, in: Eberhard *Becker*/Willms *Buhse*/Dirk *Günnewig*/Niels *Rump* (Hg.): Digital Rights Management. Technological, Economic, Legal and Political Aspects, Heidelberg/Berlin, 479–501.

Eichener, Volker/Helmut *Voelzkow* (1995). Die entwicklungsbegleitende Normung als Schnittstel-

le zwischen Forschung und Entwicklung, Technikfolgenabschätzung und technischer Regulierung, in: Renate *Martinsen*/Georg *Simonis* (Hg.): Paradigmenwechsel in der Technologiepolitik?, Opladen, 253–280.

Erickson, John S. (2003). Fair use, DRM, and trusted computing, in: Communications of the ACM. Special Issue: Digital rights management and fair use by design, 46(4), 34–39.

Felten, Edward W. (2003). A Skeptical View of DRM and Fair Use, in: Communications of the ACM. Special Issue: Digital rights management and fair use by design, 46(4), 57–59.

Fetscherin, Marc (2003). Evaluating Consumer Acceptance for Protected Digital Content, in: Eberhard *Becker*/Willms *Buhse*/Dirk *Günnewig*/Niels *Rump* (Hg.): Digital Rights Management. Technological, Economic, Legal and Political Aspects, Heidelberg/Berlin, 301–320.

Fox, Barbara L. (2002). Fair Use Friendly DRM? Paper zum Vortrag beim „Fair Use by Design?" Workshop, Computer, Freedom and Privacy Conference 2002, San Francisco. Draft only. Internet: http://www.cfp2002.org/fairuse/fox.pdf.

Fox, Barbara L./Brian A. *LaMacchia* (2003). Encouraging recognition of fair uses in DRM systems, in: Communications of the ACM. Special Issue: Digital rights management and fair use by design, 46(4), 61–63.

Garnett, Nic (2001). Digital Rights Management, Copyright, and Napster. Internet: http://www.acm.org/sigs/sigecom/exchanges /issue-2.2/SEE2.2-Garnett.pdf.

Goldsmith, Jack (1998). Regulation of the Internet: Three Persistent Fallacies, in: Chicago-Kent Law Review, 73, 1119–1131.

Gooch, Richard (2003). Requirements for DRM Systems, in: Eberhard *Becker*/Willms *Buhse*/Dirk *Günnewig*/Niels *Rump* (Hg.): Digital Rights Management. Technological, Economic, Legal and Political Aspects, Heidelberg/Berlin, 16–25.

Grassmuck, Volker (2003). Der zweite Korb dient der Allgemeinheit!, in: ZUM Sonderheft/2003, 1014–1017.

Greenleaf, Graham (1998). An Endnote on Regulating Cyberspace: Architecture vs. Law?, in: University of New South Wales Law Review, 21(2), 593–622.

Günnewig, Dirk (2003). New Copyright for the Digital Age: Political Conflicts in Germany, in: Eberhard *Becker*/Willms *Buhse*/Dirk *Günnewig*/Niels *Rump* (Hg.): Digital Rights Management, Technological, Economic, Legal and Political Aspects, Heidelberg/Berlin, 528–583.

Günnewig, Dirk (2003a). Das Recht soll's richten. Streit um Gesetze gegen das Hacken von DRM-Systemen. Internet: http://www.digital-rights-management.de/guennewig/texte/2003 03.html.

Günnewig, Dirk (2004): Architecture is Policy – Politikwissenschaftliche Herleitung und Analyse eines Steuerungskonzeptes für digitale Informations- und Kommunikationstechnologien am Fallbeispiel von Digital Rights Management Systemen. Inauguraldissertation, Ruhr-Universität Bochum (i. E.).

Günnewig, Dirk/Tobias *Hauser* (2002). Musik im Hochsicherheitstrakt. Digital Rights Management – Stand der Dinge, in: c't 2002/Heft 16, 182–185.

Günnewig, Dirk/Tobias *Hauser*/Gerald *Himmelein* (2002). Digitale Rechte am Scheideweg, in: c't 2002/Heft 17, 18–19.

Guth, Susanne (2002). Perspectives of DRM. Diplomarbeit an der Wirtschafts-Universität Wien.

Haber, Stuart/Bill *Horne*/Joe *Pato*/Tomas *Sander*/Robert Endre *Tarjan* (2003). If Piracy is the Problem, is DRM the Answer?, in: Eberhard *Becker*/Willms *Buhse*/Dirk *Günnewig*/Niels *Rump* (Hg.): Digital Rights Management. Technological, Economic, Legal and Political Aspects, Heidelberg/Berlin, 224–233.

Hauser, Tobias/Christian *Wenz* (2003). DRM Under Attack: Weaknesses in Existing Systems, in: Eberhard *Becker*/Willms *Buhse*/Dirk *Günnewig*/Niels *Rump* (Hg.): Digital Rights Management. Technological, Economic, Legal and Political Aspects, Heidelberg/Berlin, 206–223.

Herre, Jürgen (2003). Content Based Identification (Fingerprinting), in: Eberhard *Becker*/Willms *Buhse*/Dirk *Günnewig*/Niels *Rump* (Hg.): Digital Rights Management. Technological, Economic, Legal and Political Aspects, Heidelberg/Berlin, 93–100.

Hugenholtz, P. Bernt (1999). Code as code, or the end of intellectual property as we know it, in: Maastricht Journal of European and Comparative Law, 6(3), 308–318.

Intel Corp. (2002). Protecting Content in the Digital Age. Balancing Creative Use with Creator Rights, Intel Literature Center, o.O.

Klein, Hans A. (2000). System Development in the Federal Government: How Technology Influences Outcomes, in: Policy Studies Journal, 28(2), 313–328.

Koelman, Kamiel J. (2000). A Hard Nut to Crack: The Protection of Technological Measures, in: European Intellectual Property Review, 22(6), 272–288.

Koelman, Kamiel J./Natali *Helberger* (2000): Protection of Technological Measures, in: P. Bernt *Hugenholtz* (Hg.): Copyright and Electronic Commerce, The Hague/London/New York, 165–227.

Krüger, Christof (2004). Die digitale Privatkopie im „zweiten Korb", in: GRUR (Gewerblicher Rechtsschutz und Urheberrecht), 3, 204–207.

Lessig, Lawrence (1996). The Zones of Cyberspace, in: Stanford Law Review, 48, 1403–1411.

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

Lessig, Lawrence (1999a). Keynote Address: Commons and Code, in: Fordham Intellectual Property Media & Entertainment Law Review, 9, 405–419.

Lessig, Lawrence (2001). The Future of Ideas. The Fate of the Commons in a Connected World, New York.

Lessig, Lawrence (2001a). Code und andere Gesetze des Cyberspace, Berlin.

Lohmann, Fred von (2002). Vortrag beim „Fair Use by Design?" Workshop. Computer, Freedom and

Privacy Conference 2002, San Francisco, eigene Mitschrift.

Lohmann, Fred von (2003). Fair Use and Digital Rights Management: Preliminary Thoughts on the (Irreconcilable?) Tension between Them. Internet: http://www.eff.org/IP/DRM/cfp_fair_use_and_ drm.pdf.

Lutterbeck, Bernd (2000). Globalisierung des Rechts – am Beginn einer neuen Rechtskultur?, in: Computer und Recht, 1, 52–60.

Mulligan, Deirdre/Aaron *Burstein* (2002). Implementing Copyright Limitations in Rights Expression Languages, in: Conference Proceeding verteilt beim 2002 ACM Workshop on Digital Rights Management, The Wyndham City Center, Washington DC, 113–127.

Paskin, Norman (2003). Identification and Metadata, in: Eberhard *Becker*/Willms *Buhse*/Dirk *Günnewig*/Niels *Rump* (Hg.): Digital Rights Management. Technological, Economic, Legal and Political Aspects, Heidelberg/Berlin, 26–61.

Pfitzmann, Andreas/Hannes *Federrath*/Markus *Kuhn* (2002). Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität technischer Schutzmechanismen. Studie im Auftrag des Deutschen Multimediaverbandes(dmmv) e.V. und des Verbandes Privater Rundfunk & Telekommunikation (VPRT) e.V. Finale Version vom 13.3.2002, Dresden, Berlin, Cambridge. Internet: http://page.inf.fu-berlin.de/~feder/publ/2002/copyright-studie/PfFK2002 Final2002-03-13.pdf.

Reidenberg, Joel (1998). Lex Informatica: The Formulation of Information Policy Rules Through Technology, in: Texas Law Review, 76(3), 553–593.

Reinbothe, Jörg (2002). A Review of the Last Ten Years and A Look at What Lies Ahead: Copyright and Related Rights in the European Union. Conference European Copyright Revisited, Santiago de Compostela, 16-18 June 2002. Internet: http://europa.eu.int/comm/internalmarket/en/intprop/news/ reinbothe04-04-02.htm.

Reinbothe, Jörg (2002a): The Legal Framework for Digital Rights Management. Paper präsentiert beim Digital Rights Management Workshop der Europäischen Kommission am 28. Februar 2002, Brüssel.

Samuelson, Pamela (1999). Challenges for the World Intellectual Property Organization and the Trade-related Aspects of Intellectual Property Rights Council in Regulating Intellectual Property Rights in the Information Age, in: European Intellectual Property Review, 21(11), 578–591.

Sander, Tomas (2002). Golden Times for Digital Rights Management, in: Paul *Syverson* (Hg.): Fincancial Cryptography Conference 2001, LNCS, Vol. 2339, Berlin/Heidelberg, 64–74.

Schneier, Bruce (2002). Palladium and the TCPA, in: Crypto-Gram Newsletter. Internet: http://www.schneier.com/crypto -gram-0208.html"#1.

Shah, Rajiv/Jay P. *Kesan* (2002). Governance Characteristics of „Code"? The Role of Transparency, Defaults, and Standards, Paper präsentiert bei der Telecommunications Policy Research Conference, 28.-30. September 2002, Alexandria, Virginia. Internet: http://www.intel.si.umich.edu/tprc/papers/2002/97/Strangers_CDT_to_TPRC.pdf.

Shapiro, Andrew L. (1999). The Control Revolution. How the Internet is Putting Individuals in Charge and Changing the World We Know, New York.

Shapiro, William/Radek *Vingralek* (2001). How to Manage Persistent State in DRM Systems, InterTrust Star Lab, Santa Clara.

Sobel, Lionel S. (2003). DRM as Enabler of Business Models: ISPs as Digital Retailers. Symposium The Law & Technology of Digital Rights Management, in: Berkeley Technology Law Journal, 18(2), 667–696.

Spenger, Gabriele (2003). Authentication, Identification Techniques and Secure Containers. Baseline Technologies, in: Eberhard *Becker*/Willms *Buhse*/Dirk *Günnewig*/Niels *Rump* (Hg.): Digital Rights Management. Technological, Economic, Legal and Political Aspects, Heidelberg/Berlin, 62–80.

Stefik, Mark (2000). The Internet Edge. Social, Technical, and Legal Challenges for a Networked World, Cambridge/Massachusetts.

Uzuner, Ozlem/Frank III *Field*/Lee W. *McKnight* (2003). Policy Implications of Copyright Infringement Detection Systems. Submitted to 7th International Conference on Technology Policy and Innovation, Monterrey 2003, Internet: http://www.ai.mit.edu/ozlem/Uzuner-Monterey-Abstract.pdf.

Voelzkow, Helmut (1994). Verhandlungssysteme zwischen organisierten Interessen und Staat. Eine steuerungs- und demokratietheoretische Analyse der Teilhabe organisierter Interessen an öffentlicher Politik – dargestellt am Beispiel der technischen Regelsetzung. Habilitationsschrift, Bochum.

Weinstock Netanel, Neil (2000). Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory, in: California Law Review, 88, 395–498.

Zoellick, Bill (2002). CyberRegs. A Business Guide to Web Property, Privacy, and Patents, Boston et al.

AUTOR

Dirk GÜNNEWIG. Persönlicher Referent des Rektors der Universität Dortmund; Mitarbeit in einem interdisziplinären Forschungsprojekt zum Thema Digital Rights Management; Beratungstätigkeit. Forschungsschwerpunkte: politische Interessen, Lobbying und Strategien zur politischen Steuerung im Bereich der Informations- und Kommunikationstechnologien.

Kontakt: Universität Dortmund, D-44221 Dortmund.

E-mail: guennewig@digital-rights-management.org