Kartellrechtlicher Schutz vor technischen Schutzmassnahmen?

Weiterführende Gedanken zum Aufsatz von Rolf Auf der Maur/Claudia Keller, Privatkopie: Ein wohlerworbenes Recht, sic! 2/2004, 79

JACQUELINE SCHWERZMANN *

Mit Umsetzung der WIPO-Verträge und der EU-Informationsrichtlinie wird der Privatgebrauch durch technische Schutzmassnahmen (von Kopiersperren bis Digital-Rights-Management-Systemen) weitgehend abgeschafft. Der Privatgebrauch kann damit traditionell zugangserhaltende Funktionen, welche sich mit der Digitalisierung von Inhalten noch ausgeweitet haben, nicht mehr wahrnehmen. Dies hat eine Privatisierung, Monopolisierung und Technifizierung im Urheberrecht zur Folge und erhöht die Kollisionsgefahr mit kartellrechtlichen Bestimmungen, vor allem Art. 7 KG. Potentielle Konfliktsituationen ergeben sich im Bereich des Zugangs zu nichtsubstituierbaren, gesellschafts-relevanten Inhalten bei Industrieweiten de facto-Standards und im Zusammenhang mit Koppelungs-geschäften oder unangemessenen Geschäftsbedingungen. Fraglich erscheint, ob das Kartellrecht genügend griffig ist. Aus diesem Grund sind entweder eine Stärkung der Nutzerstellung oder eine Beschränkung des Rechtsschutzes für technische Schutzmassnahmen angebracht.

Les conventions de l'OMPI et la directive de l'UE sur la société de l'information ont considérablement réduit l'usage privé face aux mesures techniques de protection (allant du blocage des copies jusqu'aux systèmes de «digital rights management»). L'usage privé ne peut plus garantir ainsi l'accès à l'information, fonction qui était traditionnellement la sienne et qui s'est encore développée avec la digitalisation des contenus. Cela entraîne une privatisation, une monopolisation et une technicisation du droit d'auteur ainsi que l'augmentation du risque de collision avec les dispositions du droit des cartels, en particulier avec l'art. 7 LCart. Ce problème se pose avec les restrictions à l'accès à des contenus non substituables mais qui sont socialement importants, avec les standards de fait que l'industrie doit appliquer, ou encore avec des transactions couplées ou des conditions générales inéquitables. Il est donc nécessaire de renforcer l'aménagement des conditions d'utilisation ou alors de restreindre la protection juridique des mesures techniques de protection.

I. Der Privatgebrauch (Art. 19 URG) und seine Funktionen

Der Privatgebrauch (Art. 19 Abs. 1 URG) ist in seinem jeweiligen sozial-wirtschaftlichen Umfeld und technischen Fortschritt eingebettet und erfüllte im Laufe der Zeit unterschiedliche Funktionen. So werden dem Privatgebrauch traditionell Funktionen zugeordnet, welche sich auf das Prinzip der «Sozial-

bindung» des Urheberrechts stützen[1]. Hinzu kommen praktische Überlegungen, welche sich vor allem aus dem Stand der Technik ergeben. Das Institut des Privatgebrauchs war immer Ausdruck der gesetzgeberischen Interessenabwägung zwischen den Interessen der Allgemeinheit und denen der Urheberrechtsinhaber.

1. Analoger Privatgebrauch

Bis zum Aufkommen digitaler Datenverarbeitung und damit auch digitaler Werke hatte der Privatgebrauch vor allem folgende Funktionen[2]:

– Allgemeine Zugänglichkeit von Werken für Gesellschaft: Weil das Urheberrecht den Rechtsinhaber mit einem beschränkten Monopol über sein Werk ausstattet, um ihm die wirtschaftliche und ideelle Ausschöpfung seines Werks zu sichern und damit Anreiz für weitere kulturelle Schöpfungen zu legen, werden im Gegenzug gewisse Minimalzugangsregeln für die Allgemeinheit erlassen. Die Allgemeinheit hat ein legitimes Interesse am ungehinderten und möglichst breiten Zugang zu den Kulturgütern, einerseits zu Bildungszwecken andererseits als Grundlage für weiteres geistiges Schaffen, da geistiges Schaffen immer auf Bestehendem aufbaut.

– Individuelle kulturelle Auseinandersetzung: Durch die Möglichkeit, Werke im persönlichen Freundeskreis auszutauschen und gemeinsam zu diskutieren, und durch die Freistellung der persönlichen Auseinandersetzung, etwa in Form von privaten Bearbeitungen, vom urheberrechtlichen Verbotsrecht, wird dem einzelnen Gesellschaftsmitglied die kulturelle Auseinandersetzung mit geschützten Werken ermöglicht.

– Schutz der Privatsphäre vor Kontrollhandlungen: Die Durchsetzung der absoluten Urheberrechte im Privatbereich wäre mit zu starken Eingriffen in die Privatsphäre des Nutzers verbunden, soweit sie praktisch überhaupt durchführbar wäre.

2. Digitaler Privatgebrauch

Mit Ausnahme von Punkt 3 – die Digitaltechnik erlaubt relativ einfach eine Kontrolle des Privatgebrauchs – sind diese Funktionen des Privatgebrauchs auch im digitalen Umfeld noch zutreffend, auch wenn auf Grund der (technisch bedingt) gewachsenen Verfügungsmacht des Privatnutzers das Potential zur kommerziellen Nutzung gestiegen ist. Zusätzlich haben jedoch (ebenfalls technisch bedingt) zusätzliche Funktionen des Privatgebrauchs an Bedeutung gewonnen:

– Garantie der freien individuellen Werknutzung: Mit dieser Funktion ist die Freiheit des Nutzers abgesichert, ein rechtmässig erworbenes Werk nach eigener Wahl der Mittel und Modalitäten zu geniessen (Ort, Zeit, Art)[3]. Diese Funktion wird vor allem durch das Privatvervielfältigungsrecht sichergestellt. Dieses ermöglicht die Portabilität von Werken im privaten Haushalt (etwa die Übertragbarkeit von Werken auf unterschiedliche Nutzungsgeräte, wie für Musik: CD-Player, Computer, Autoradio, Handy oder portabler Player) sowie die Interoperabilität (das Abspielen auf Geräten und mit Software nach Wahl)[4].

---

[1] Vergleiche zum Begriff der Sozialbindung: E. Pahud, Die Sozialbindung des Urheberrechts, Bern 2000. Das Schweizer Recht anerkennt im Gegensatz zum deutschen Recht (Art. 14 Abs. 2 GG) nicht explizit die Sozialgebundenheit des Eigentums. Dennoch ist auch in der Schweiz anerkannt, dass Schutzwürdigkeit und Schutzumfang des Eigentums, mithin auch des Immaterialgüterrechts, an dessen personalen und sozialen Bezug gemessen wird: R. Weber, Eigentum als Rechtsinstitut, ZSR 1997, 166; J. P. Müller, Grundrechte in der Schweiz, 3. Aufl., Bern 1999; Pahud, 87.

[2] Vgl. auch C. Gasser, Der Eigengebrauch im Urheberrecht, Bern 1997.

[3] http://digitalconsumer.org/bill.html: Die US-Konsumentenorganisation DigitalConsumer.org fordert folgende Nutzerrechte: 1. right to time-shift 2. right to space-shift 3. right to make back up copies 4. right to choose platform 5. right to use different formats.

[4] Nach einer Umfrage des Gartner-Instituts vom September 2002 gehen beispielsweise 82% resp. 77% der US-Amerikaner davon aus, dass es legal ist, Musik zu Back-up-Zwecken oder zwecks Abspielung in einem anderen Gerät zu kopieren (Berkman Center for Internet & Society, Copyright and Digital Media in a Post-Napster World, Research Publication No. 2003-05 8/2003)

– Back-up-Kopien: Da digitale Inhalte flüchtiger sind als analoge, und digitale Datenträger auf Grund der technischen Weiterentwicklung der Formate schnell nicht mehr abspielbar, dienen Back-up-Kopien dem Werkerhalt[5].

II. Technische Schutzmassnahmen

1. Definition

Art. 6 Abs. 3 der EU-Urheberrechtsrichtlinie 2001/29/EG[6] definiert technische Schutzmassnahmen in urheberrechtlichem Kontext als «Technologien, Vorrichtungen oder Bestandteile, die im normalen Betrieb dazu bestimmt sind, Werke oder sonstige Schutzgegenstände betreffende Handlungen zu verhindern oder einzuschränken, die nicht von der Person genehmigt worden sind, die Inhaber der Urheberrechte oder der dem Urheberrecht verwandten gesetzlich geschützten Schutzrechte oder des in Kapitel III der Richtlinie 96/9/EG verankerten Sui-generis-Rechts ist». Unter dem Stichwort der «Wirksamkeit» werden die technischen Schutzmassnahmen weiter präzisiert: «Technische Massnahmen sind als ‹wirksam› anzusehen, soweit die Nutzung eines geschützten Werks oder eines sonstigen Schutzgegenstandes von den Rechtsinhabern durch eine Zugangskontrolle oder einen Schutzmechanismus wie Verschlüsselung, Verzerrung oder sonstige Umwandlung des Werks oder sonstigen Schutzgegenstandes oder einen Mechanismus zur Kontrolle der Vervielfältigung, die die Erreichung des Schutzziels sicherstellen, unter Kontrolle gehalten wird.»

2. Arten technischer Schutzmassnahmen

Als rechtlich geschützte Arten von technischen Schutzmassnahmen gelten damit:

– Zugangskontrollen (Passwörter, Biometrie, elektronische Zertifikate)

– Werkschutzmechanismen (Verschlüsselung, Verzerrung)

– Kopierkontrollen (Copyflags)

Technische Schutzmassnahmen können in ihrer Funktion unterschieden werden in nutzungsver-hindernde oder zugangsverhindernde Massnahmen, d.h. solche, welche gewisse Nutzungshand-lungen beeinträchtigen oder solche, welche den Zugang kontrollieren. Oftmals lassen sich allerdings diese beiden Funktionen von technischen Schutzmassnahmen nicht klar auseinander halten, da manche technischen Massnahmen beide Funktionen gleichzeitig erfüllen[7].

3. Anwendungen

a) Kopiergeschützte Tonträger

Der Zugangsschutz besteht bei kopiergeschützten Audio-Tonträgern darin, dass die Musikträger entweder nicht von CD-Laufwerken eines Computers oder nicht mit frei wählbaren Softwareplayern abgespielt werden können. Die Nutzungskontrolle stellt sicher, dass die gespeicherte Musik nicht, in begrenzter Anzahl, oder in nicht frei wählbare Formate kopiert werden kann. Die Tonträger nur als kopiergeschützt zu bezeichnen, greift demnach zu kurz.

Ältere technische Schutzmassnahmen reichen von im Tonträger eingebauten Datenfehlern oder Datenmanipulationen bis hin zu undokumentierten Abweichungen vom CD-Audio-Standard. Neuere technische Massnahmen basieren auf der sogenannten «Multisession»-Technologie. Auf einer Un-CD

[5] Bei Computerprogrammen sind Back-up-Kopien teilweise durch Spezialnormen gesetzlich erlaubt: Gemäss Art. 24 Abs. 2 URG ist es gestattet, eine Sicherungskopie herzustellen. Auch im analogen Umfeld ist es erlaubt, eine Kopie zur Sicherung des Werks zu erstellen (Art. 24 Abs. 1 URG).

[6] Deckungsgleich das deutsche Urheberrechtsgesetz in § 95a UrhG.

[7] Der amerikanische «Digital Millennium Copyright Act» beispielsweise baut auf dieser Unterscheidung auf und erlaubt in §1201 die Umgehung von Nutzungskontroll-Massnahmen zu Zwecken des «Fair use», nicht aber die Umgehung von Zugangskontroll-Massnahmen. Für den Privatnutzer bleibt diese Lücke aber nutzlos, da der Handel mit Umgehungstechnologie trotzdem verboten bleibt, er sich also nicht mit Umgehungswerkzeugen versorgen kann, welche ihm eine Umgehung ermöglichen würden. Eine private Herstellung von Umgehungstechnologie ist meistens zu aufwändig.

befinden sich sowohl normale Audio-Dateien, welche herkömmliche CD-Player abspielen, sowie weitere Dateien, welche dieselbe Musik in komprimierter und verschlüsselter Form enthalten. Nur die letzteren Dateien können vom CD-Laufwerk des Computers gelesen werden. Auf diese Musikdaten kann auf einem Computer nur mit Playern zugegriffen werden, welche in der Regel mit DRM-Funktionen angereichert sind[8].

b) DVDs

Im Bereich der DVDs garantiert der «Region Code», welcher auf der DVD angebracht ist, regional eingeschränkten Zugang. Insgesamt gibt es 8 Region-Codes für DVDs[9]. DVDs können jeweils nur in Geräten abgespielt werden, welche denselben Region-Code aufweisen wie die abzuspielende DVD[10], um den Rechtsinhabern eine zum Voraus bestimmte Verwertungskaskade abzusichern.

Eine weitere Zugangs-, gleichzeitig aber auch Nutzerkontrolle besteht im so genannten CSS (Content Scrambling System). CSS ist eine Verschlüsselung- und Authentisierungsmethode für Daten. Nur zertifizierte Abspielgeräte ermöglichen die Entschlüsselung. Die «DVD Copy Control Association» vergibt so genannte «Player Keys» aus einem Sortiment von 400 Master-Schlüsseln, welche die Abspielgeräte als authorisiert qualifizieren[11]. Ab 2000 müssen DVD-Drives in Computern das «Region Coding» zusätzlich zu CSS unterstützen.

c) Umfassende Digital Rights Management Systeme

Ab wann genau eine Kombination von technischen Schutzmassnahmen als «Digital Rights Management» (DRM) System gilt, ist uneinheitlich beschrieben[12]. So können – je nach Definition auch Schutzmassnahmen bei Tonträgern oder DVDs – unter den Begriff DRM fallen. Allerdings werden DRM-Systeme meistens nicht nur als Kontrollösungen für Inhalte verstanden, vielmehr bestehen sie in der Regel aus einer Kombination verschiedener technischer Massnahmen zur Zugangs-, Kopier- und Nutzungskontrolle[13]. Als Basis dazu dienen Informationen zur Erfassung der Identität von Nutzenden sowie zur Beschreibung von gehandelten Inhalten und Nutzungsbestimmungen. Schliesslich ist oftmals auch ein Lizenzierungs-[14], Abrechnungs- und Zahlungssystem systemimmanent, sodass sie umfassende Vertriebssysteme für digitale Inhalte, insbesondere einschliesslich der Lizenzierung, ermöglichen.

---

[8] Zur technischen Funktionsweise von Abspielsperren für Audio-CDs: J.H. Haldermann, Evaluating New Copy-Prevention Techniques for Audio CDs, www.cs.princeton.edu/~jhalderm/papers/drm2002.pdf. (Dez. 2003); F.P. Volpe/D. Bär, Die Un-CDs, c't 2003, 144 ff. Aus wettbewerblicher Sicht sei hier erwähnt, dass solche Audioträger nicht CDs genannt werden dürfen, da sie dem CD-Standard nicht entsprechen. Allfällige CD-Vortäuschungen könnten als unlauter gelten (Art. 3 Ziff. i UWG), bzw. Gewährleistungsansprüche auslösen (vgl. dazu B. Goldmann/A. Liepe, Vertrieb von kopiergeschützten Audio-CDs in Deutschland, ZUM 2002, 362 ff.; N. Wiegand, Technische Schutzmassnahmen in Musik-CDs, MMR 2002, 722–730).

[9] 1: USA und Kanada, 2: Europa und Japan, 3: Südost-Asien, 4: Lateinamerika und Australien, 5: Russland, Rest von Asien, Afrika, 6: China. Genau genommen kommen noch zwei Codes dazu: 7: Reserve, 8: Internationale Verbreitung, für Flugzeuge und Kreuzfahrtschiffe. Vgl. http://dvddemystified.com/dvdfaq.html.

[10] Bei DVD-Laufwerken in Computern kann der Region-Code fünfmal geändert werden, bis er fix auf der letzten Region stehen bleibt.

[11] Vgl. zur genauen Funktionsweise J. Taylor, DVD Demystified, New York 2000, 484; http://dvddemystified.com/dvdfaq.html; S. Bechtold, Vom Urheber- zum Informationsrecht, München 2002, 108. Mittlerweile sind auch DVDs im Handel, welche «aktiv» nach einer Region-Code-Abfrage des Gerätes Ausschau halten und dementsprechend in Code-Free-Playern nicht abspielbar sind (Regional Coding Enhancement, RCE, www.dvdtalk.com/rce.html.)

[12] Technisch betrachtet hat sich noch keine einheitliche Definition durchgesetzt, woraus Digital Rights Management genau zu bestehen hat, um dieser Bezeichnung gerecht zu werden. T. Pack, Digital Rights Management: Can technology provide long-term solutions, EContent 2001 (www.onlineinc.com/articles/econtent/pack5a_01.html) zitiert einen Media-Analysten von Forrester Research: «The term 'digital rights management' means something different to almost everyone you ask». Oft bestehen umfassende DRM-Systeme aus kombinierten Hard- und Software-Mechanismen, die dem Distributor Einflussmöglichkeiten über seinen Inhalt sichern: «Software and hardware that enable a publisher to specify terms and conditions for digital works and to control how they can be used» (STEFIK). Der US-Experte Bill Rosenblatt (www.giantsteps.com) umschreibt DRM-Systeme kurz und bündig: «Technology that describes, identifies, and protects digital content».

[13] Vgl. Commission Staff Working Paper; Digital Rights. Background, Systems, Assessment. SEC (2002)197, www.europa.eu.int/information_society/newsroom/docu-ments/drm. Bechtold (Fn. 11), 20.

[14] Näheres zur Gültigkeit der Onlinelizenzen vergleiche L. Bühler, Schweizerisches und internationales Urheberrecht im Internet, Freiburg 1999, 302.

DRM-Systeme sind oft proprietär, das heisst von einem Hersteller nach eigenen Standards entwickelt. Daher hängt die konkrete Ausgestaltung vom jeweiligen Anbieter ab – es gibt nicht ein einziges DRM-Modell. Ein DRM-System besteht aus mehreren Komponenten, wobei jede der begriffsnotwendigen Komponenten durch mehrere technische Massnahmen sichergestellt wird:

– Beschreibung des Inhalts: genaue Angaben zur Herkunft und Autorenschaft des Inhalts (z.B. ISBN-Nummer für Bücher).

– Identifikation der Nutzung: Angaben, welche Rechte vergeben werden (eine maschinenlesbare Rechtesprache, beispielsweise XrML) und Angaben, wie der Nutzer authentisiert wird (Authentisierungsmechanismen, beispielsweise Zertikfikate oder Passwörter).

– Schutz des Inhalts: Verschlüsselung oder anderes technisches Verfahren, mit dem die beabsichtigte Verwendung des gelieferten Inhalts sichergestellt wird.

– Evtl. Mechanismus zur Abrechnung und Zahlungsabwicklung: Rückmeldung der Verwendung und Zahlungssystem (oftmals Kreditkarte).

Der Rechteinhaber betreibt gleichzeitig einen Inhalts- und einen Lizenzserver. Auf Ersterem lagern die Inhalte, auf dem zweiten die Lizenzen, die zum Gebrauch der Inhalte gewährt werden[15]. Bezieht ein Nutzer ein Stück Inhalt, wird dieses in der Regel mitsamt den so genannten Metadaten (Daten über die Daten, z.B. Identifikationsangaben) in verschlüsselter Form geliefert. In älteren Systemen enthalten die Metadaten auch die Definition der zulässigen Nutzung, in neueren Systemen werden die Nutzungsrechte, die ebenfalls in maschinenlesbarer Form vorhanden sein müssen, separat in so genannten digitalen Lizenzen geliefert. Solche Lizenz liefert der Lizenzserver des Urhebers. Gegen Speicherung der Identität des Nutzers (Passwort, Biometrie etc.) liefert er den Key zur Entschlüsselung des Inhalts sowie die Rechteinformationen zur Nutzung des Inhalts. Spezifische Applikationen, die der Nutzer auf seinem Wiedergabegerät installiert haben muss, spielen den Inhalt ab oder stellen ihn dar (z.B. Windows Media Player). Zum Teil werden auch generell verbreitete Leseprogramme (wie etwa Acrobat Reader) mittels Plugins zu DRM-tauglicher Abspielsoftware umfunktioniert[16].

Der Zugang zu Inhalten wird bei Digital Rights Management erst nach Akzept vordefinierter, nicht-verhandelbarer Lizenzbedingungen eingeräumt. Bei Tonträgern oder DVDs ist der Zugang insoweit eingeschränkt, als nur mittels gewissen Geräten auf die Inhalte zugegriffen werden kann. Für die Nutzung zu verwendende Formate (Software) und Abspielgeräte (Hardware) sind vom Rechtsinhaber vorgegeben. Die freie Produktewahl für Abspielgeräte und Abspielsoftware ist somit zu Gunsten der Sicherheit des Inhalts eingeschränkt[17]. Verarbeitung und Transformation in andere Formate sind eingeschränkt bis verboten, da die Kontrolle oft über die Abstimmung der Formate sichergestellt wird.

5. Trusted Computing

Das so genannte Trusted Computing basiert darauf, dass Programme und/oder Daten auf ihre Integrität getestet werden[18]. Damit wird aus Sicht des Rechteinhabers eine weitere Sicherheitsebene erreicht. Die Idee des Trusted Computing beruht darauf, dass schon auf der Hardwareebene mittels digitalen Signaturen sichergestellt wird, dass nur Programme zur Ausführung gelangen, die signiert und damit vertrauenswürdig sind. Trusted Computing stellt damit eine Erweiterung der DRM-Idee dar, in der DRM-Technologien nicht mehr nur auf Daten, sondern auch auf ganze Programme angewendet

[15] Der Lizenzserver könnte auch ausgelagert sein und einem spezialisierten Lizenzvertreiber übertragen werden.

[16] InterTrust war eines der ersten Unternehmen, das DRM-Lösungen anbot und ist heute zur Mehrheit im Besitz von Sony und Phillips. Das Haupt-DRM-Produkt ist «RightsSystem». Als Beispiel für die Funktionsweise von DRM-Systemen, vgl. www.intertrust.com/main/technology/ index.html.

[17] Denkbar wären auch produkt-neutra-le Hardware- / Softwarelösungen, welche nicht auf proprietären Produkte-Standards, sondern auf offenen Standards beruhen. Mangels Standardisierung sind Kontrollösungen oft proprietär und basieren oftmals auf dem Prinzip von «security through obscurity» (Sicherheit durch Geheimhaltung der genauen Programmabläufe, d.h. keine kryptologisch einwandfreien Lösungen). Dies bedingt, dass genau die vorgeschriebene Software verwendet werden muss, um eine Abschottung des Inhalts gegen aussen und somit eine Wirksamkeit der technischen Schutzmassnahmen zu gewährleisten.

[18] Dies ist deshalb möglich, weil alle modernen Computer nach der Von-Neumann-Architektur (J. Neumann et al., Preliminary Discussion of the Logical design of an Electronic Computing Instrument. U.S. Army Ordonance Dept. Report. Princeton 1946) aufgebaut sind, also Programme und Daten gleich behandeln und auch im gleichen Speicher ablegen und verarbeiten. Die Idee des Trusted Computing wurde zuerst von Arbaugh et al. (W. Arbaugh et al., A Secure and Reliable Bootstrap Architecture, www. computer.org/proceedings/sp/7828/78280065abs.htm) vorgeschlagen.

werden. Ein Trusted Computing System beruht auf Hardware, die im Kern der Rechnerarchitektur verankert ist[19]. Diese Kernkomponenten sind dafür verantwortlich, den Zugriff auf Programme und auf Daten zu kontrollieren und nur dann zu gestatten, wenn Sicherheitsüberprüfungen erfolgreich ausgeführt werden konnten. Im Prinzip lassen sich in einer solchen Architektur zwei Bereiche betrachten:

– Programmausführung: Eine Trusted Computing Architektur könnte sich darauf beschränken, Sicherheitsüberprüfungen bei Programmen vorzunehmen. Dies hätte den Effekt, dass nur signierte Programme zur Ausführung gelangen, diese dann aber freien und ungehinderten Zugang auf Daten hätten. Eine solche Architektur könnte die Problematik von bösartigen Programmen (Viren, Würmern, usw.) weitgehend lösen, würde aber in Bezug auf die Kontrolle über Inhalte keine Einschränkungen ermöglichen. Je nach Signierungspraxis könnten jedoch Programme ausgeschlossen werden.

– Datenzugriff: In einem weitergehenden Schritt kann eine Trusted Computing Architektur auch den Zugriff auf Daten regeln und auch bei diesen Sicherheitsüberprüfungen vornehmen, und jedem Programm nur dann den Zugriff auf Daten gestatten, falls diese Daten gemäss der Sicherheitskriterien als unbedenklich eingestuft wurden. Eine solche Architektur kann je nach Implementierung auch eine Verbindung zwischen Sicherheitsüberprüfungen für Programme und Sicherheitsüberprüfungen für Daten herstellen, sodass Bestandteil der sicherheitsrelevanten Aspekte eines Programmes auch ist, auf welche Daten dieses Programm zugreifen darf.

Die Konsequenzen einer breit angewendeten Trusted Computing Architektur mit ihren effizienten Kontrollmöglichkeiten können momentan erst abgeschätzt werden[20]. Sollte ein populäres Betriebssystem wie Windows zu einem Trusted Computing System werden und alle Möglichkeiten der darunterliegenden Trusted Computing Architektur ausnutzen, würde das bedeuten, dass den Benutzern digitaler Inhalte

nicht die Wahl bliebe, auf eine andere und weniger vollständig kontrollierte und gesteuerte Anwendung umzusteigen. Des Weiteren hätten Open Source Produkte[21] kaum mehr eine Chance, Weiter am Markt zu bestehen, da diese in einer Trusted Computing Plattform kaum als vertrauenswürdig lizenziert werden dürften.

III. Rechtslage bezüglich Privatgebrauch vs. technische Schutzmassnahmen

Das Missbrauchspotential bei digitalen Werken hat zugenommen[22], was die Rechteinhaber veranlasst, den Gebrauch ihrer Werke mittels technischen Schutzmassnahmen stärker zu kontrollieren. Damit wird in Kauf genommen, dass nicht nur potentiell illegale Privatnutzer-Handlungen (denen im Übrigen bereits mit bestehendem Urheberrecht zu begegnen gewesen wäre) verunmöglicht werden, sondern auch legale. Anders als das Recht bietet die Technik als faktische Massnahme die Möglichkeit zur direkten Durchsetzung[23]. Technik funktioniert aber auch undifferenzierter als Recht nach dem Alles-oder-Nichts-Prinzip: so stellte sich schnell einmal das Problem, dass Verfügungsfreiräume, wie etwa der Privatgebrauch, mit dem absoluten Durchsetzungsanspruch der Technik kollidieren.

Die neuen internationalen rechtlichen Regelwerke[24], die den Schutz technischer Massnahmen verlangen, lassen den umsetzenden Ländern Spielraum bei der Bewertung des Vorranges zwischen urheberrechtlichen Schranken und technischen Schutzmassnahmen. Sowohl im deutschen als auch

[19] Intels Initiative beruht z.B. auf der Einbettung der sicherheitsrelevanten Hardware in den Prozessorkern.

[20] Die in der Mitte April in der Trusted Computing Group vetretenen Firmen (ursprünglich 1999 als «Trusted Computing Platform Alliance» gegründet von Compaq, HP, IBM, Intel und Microsoft, mittlerweile ca. 200 Mitglieder, das Ziel dieses Zusammenschlusses ist es, gemeinsame Standards zu schaffen) beschreiben das Konzept eines Trusted Computing System als etwas, das nicht unmittelbar mit DRM zu tun hat und als eigentliches Ziel die Vertrauenwürdigkeit einer Plattform hat, die ein Benutzer verwendet. Allerdings liegt der Schluss nahe, Trusted Computing auch zur Absicherung von urheberrechtlichen Machtstellungen zu benutzen.

[21] Open Source Produkte sind Programme, deren Quellcode offen gelegt ist und die in der Regel mit öffentlichen Lizenzen kostenfrei verfügbar gemacht wird (Weitere Angaben bei www.opensource.org).

[22] Gewöhnlich wird auf das Tauschen von – vorwiegend Konsumgütern – in P2P-Netzwerken verwiesen.

[23] Vgl. dazu J.R. Reidenberg, Lex informatica, Texas Law Review, (76) 1998, Vol. 3.

[24] Art. 11WCT (WIPO Copyright Treaty) / Art. 18 WPPT (WIPO Performances and Phonograms Treaty): die Schweiz hat die beiden WIPO-Verträge noch nicht ratifiziert; Art. 6 Abs. 4 EU-Urheberrechtsrichtlinie 2001/29/EG. Diese ergänzt bestehende Spezial-Richtlinien (Computerprogramm-Richtlinie; Zugangskontrolldienste-Richtlinie) und weitet den Rechtsschutz für technische Schutzmassnahmen auf alle urheberrechtlichen Inhalte aus. Allerdings gelten für technische Schutzmassnahmen an Computerprogrammen weiterhin die spezialgesetzlichen Regeln (Erw. 50 EU-Urheberrechtsrichtlinie).

im amerikanischen Recht (als zwei Beispiele der Umsetzung) ist der Privatgebrauch jedoch weit-gehend eingeschränkt worden, diese Rechtsumsetzungen favorisieren technische Schutzmass-nahmen gegenüber den klassischen Privatgebrauchs-Ausnahmen.

– Deutschland (§ 95b UrhG[25]): Die Rechteinhaber werden verpflichtet, dem Privatnutzer, der rechtmässig Zugang zum Werk hat, die Vervielfältigung ganzer Werke auf Papier (oder einem ähnlichen Träger) mittels photomechanischem Verfahren (oder einem Verfahren mit ähnlicher Wirkung) zu ermöglichen. Wie genau die Zugänglichmachung durch die Rechtsinhaber erfolgen soll, darüber schweigt das Gesetz. Der Private kann den Anspruch klageweise zivilrechtlich durchsetzen, allerdings wurde ein Verbandsklagerecht abgelehnt. Bei interaktiven Onlinediensten ist die Privatkopie vollständig ausgeschlossen.

– USA (§ 1201 Digital Millennium Copyright Act; DMCA): Im DMCA wird nicht explizit festgelegt, wie «Fair use» und technische Schutzmassnahmen zueinander stehen. In Entscheid Universal City Inc. v. Reimerdes[26] hat der Court of Appeals des Second Circuit im November 2001 entschieden, dass die Fair-use-Ausnahmen bei technischen Schutzmassnahmen nicht anwendbar sind, sondern ausschliesslich die in § 1201 (d)-(j) speziell genannten Ausnahmen[27].

Der umfassende Schutz vor Änderungen technischer Massnahmen und die Tendenz, den Privatgebrauch weitgehend auszuschliessen, haben eine Monopolisierung (Kombination von technischem, vertraglichem und gesetzlichem Schutz), Privatisierung (individuelle Lizenzierung) und Technifizierung des Urheberrechts zur Folge. Diese Entwicklungen erhöhen das Missbrauchspotential für Rechteinhaber bezüglich der von ihnen kontrollierten Inhalte. Daher ist – ebenso – stärker als bisher das Wettbewerbsrecht zur Korrektur gefragt[28].

IV. Technische Schutzmassnahmen und Wettbewerbsrecht

1. Immaterialgüterrecht und Wettbewerbsrecht

Art. 3 Abs. 2 KG sieht vor, dass Wettbewerbsbeschränkungen, welche sich ausschliesslich aus der Gesetzgebung über das geistige Eigentum ergeben, nicht kartellrechtlich beurteilt werden können. Diese Norm wird nach herrschender Meinung nicht als absolute Nicht-Anwendbarkeit des Kartellrechts auf das Urheberrecht verstanden; auf Missbräuche des geistigen Eigentums ist das Kartellrecht anwendbar. Über die genaue Tragweite der Norm herrscht jedoch kein Konsens[29].

Vom EuGH wird nach wie vor die Unterscheidung in Bestand der Schutzrechte und in der Ausübung getroffen, bzw. auf den spezifischen Gegenstand der Immaterialgüterrechte abgestellt: Das Kartellrecht lässt den Bestand der spezifischen Schutzrechte unberührt, beschränkt aber unter Umständen deren Ausübung[30]. Generell geht die Tendenz in Richtung zunehmend breiterer Anwendung des Kartellrechts auch auf urheberrechtliche Sachverhalte.

2. Kartellrechtliche Problemfelder von technischen Schutzmassnahmen

[25] Gemäss § 69a Abs. 5 UrhG finden diese Bestimmungen keine Anwendung auf Computerprogramme, da hier spezialgesetzliche Regelungen greifen, welche allerdings ähnlich ausgestaltet sind.
[26] http://laws.findlaw.com/2nd/009185. html.
[27] Ausnahmen zugunsten von öffentlichen Bibliotheken, Archiven und Schulen zum Zweck der Eruierung der Anschaffung eines Werkexemplars, zu Gunsten von staatlichen Behörden, im Falle von «Reverse Engineering» zum Zwecke der Herstellung von Interoperabilität bei Computerprogrammen, für die Erforschung von Verschlüsselungstechnologien, um den Schutz von Minderjährigen sicherzustellen, um das Sammeln von personenbezogenen Daten zu verhindern, für Sicherheitstests.
[28] Vgl. dazu auch Bühler (Fn. 14), 20.
[29] Eine Übersicht zu den Lehrmeinungen bei R. M. Hilty, Vom Janusgesicht des Immaterialgüterrechts – Versuch einer europatauglichen Interpretation von Art. 3 Abs. 2 KG, in: P. Forstmoser (Hg.), Zürich 1999, 328. Zur Revision des Kartellgesetzes: P. Krauskopf / D. Senn, Die Teilrevision des Kartellrechts – Wettbewerbspolitische Quantensprünge, sic! 2003, 22 ff.
[30] Kritik an dieser allzu groben Unterscheidung bei A. Heinemann, Immaterialgüterschutz in der Wettbewerbsordnung, Tübingen 2002, 288 ff.

Im Vordergrund stehen Kollisionen mit dem Missbrauchsverbot von Art. 7 KG[31], womit Marktbe-herrschung vorausgesetzt wird. Grundsätzlich herrschen auf dem Medienmarkt wie auch auf dem Softwaremarkt bereits jetzt starke Konzentrationstendenzen[32]. Mit der Ausschlusswirkung von technischen Schutzmassnahmen können diese zunehmen und die Innovation in der Produkteent-wicklung bremsen, bzw. den Zugang zu Inhalten erschweren. Ob eine Marktbeherrschung (Art. 4 Abs. 2 KG) vorliegt, bleibt im konkreten Einzelfall abzuklären. Entscheidend ist, dass der relevante Markt für urheberrechtliche Werke in der Regel eng zu ziehen ist, da urheberrechtliche Inhalte einen – im Bewusstsein des Verbrauchers – hohen Individualitätsgrad aufweisen und daher selten substituierbar sind, weshalb Marktbeherrschung öfters gegeben sein kann[33].

Im Zusammenhang mit Zugangs- und Nutzungskontrollen stehen folgende Problemfelder im Vordergrund:

– Problematik der Zugangsverweigerung zu nicht-substituierbaren, gesellschaftsrelevanten Inhalten.

– Problematik der Monopolisierung von de facto-Standards bei technischen Schutzmassnahmen.

– Problematik der Ausdehnung der Marktdominanz der urheberrechtlichen Rechtsinhaber auf den nachgelagerten Markt für Rezeptionsmitteln für digitale Inhalte (Lesesoftware, Abspielgeräte).

– Problematik von missbräuchlichen Nutzungsbedingungen und Preisen.

3. Die «essential facility»-Doktrin (Art. 7 Abs. 1 i.V.m. Art. 7 Abs. 2 a/e KG)

a) Die «essential facility»-Doktrin

Im Zusammenhang mit einem kartellrechtlich zu schaffenden Zugang zu Monopolbereichen wird oft mittels der «essential facility»-Doktrin (EF-Doktrin) argumentiert. Die Doktrin stammt aus dem US-amerikanischen Antitrustrecht und wurde ursprünglich für strategisch wichtige Einrichtungen körperlicher Natur, etwa Bahnhöfe, entwickelt. Sie gewann an Bedeutung im Zusammenhang mit der Öffnung von Netzwerk-Infrastrukturen wie Elektrizität oder Telefon. Die Aufgabe der EF-Doktrin besteht darin, die missbräuchliche Ausnützung der marktbeherrschenden Stellung von Eigentümern wesentlicher Infrastruktureinrichtungen zu unterbinden[34]. Die Doktrin fand vor allem auf die Verweigerung von Geschäftsbeziehungen Anwendung. Die Voraussetzungen zur Anwendbarkeit der EF-Doktrin sind:

– Marktbeherrschende Stellung.

– Wesentliches Zugangsobjekt: vernünftigerweise nicht duplizierbar und fehlende Substituierbarkeit.

– Zugangsverweigerung bei eigener Tätigkeit auf dem abgeleiteten Markt[35].

– Fehlen von Rechtfertigungsgründen.

Die zentrale Frage ist, ob urheberrechtlichen Inhalten die Qualität von «wesentlichen Einrichtungen» zukommen kann. Dass Immaterialgüterrechte dafür grundsätzlich in Frage kommen, hat der Magill-

[31] Auf rein horizontale Absprachen wird nicht näher eingegangen, da sich diese Problemfelder unabhängig vom Privatgebrauchsthema stellen.

[32] So teilen sich den Musikmarkt nach der Fusion von Sony und BMG noch vier Player (Universal: 25%, Sony / BMG 25%, EMI 12%, Warner 12%), vgl. Süddeutsche Zeitung vom 7. November 2003.

[33] B. Schmidhauser, Kommentar zum schweizerischen Kartellgesetz, Zürich 1997, KG 4 N 58.

[34] Die EU-Kommission hat die EF-Doktrin erstmals in den so genannten Hafen-Entscheidungen in den Jahren 1992 und 1993 (Entscheid der Kommission vom 11. Juni 1992, CMLR 1992, «B&I-Holyhead / Sealink». Entscheid der Kommission vom 21. Dezember 1993, ABl 1994 L 15/8 vom 18. Januar 1994, «Sea Containers / Stena Sealink») ausdrücklich erwähnt, der Magill-Entscheid gilt häufig als Übernahme der Doktrin (als Anwendung von Art. 82 EGV) durch den Europäischen Gerichtshof (EuGH, Urteil vom 06. April 1995, Rs. C-241/91, Slg. 1995, I-743, «Magill TV Guide/ITP, BBC und RTE»). In der Schweiz wird die Doktrin nicht explizit angewendet, gilt jedoch in Art. 7 Abs. 2 lit. a KG als mitenthalten (B. Hübscher / P. Rieder, Die Anwendung der «Essential facility»-Doktrin für das schweizerische Wettbewerbsrecht, sic! 1997, 439 ff.)

[35] Im IMS-NDC-Verfahren hat die EU-Kommission die EF-Doktrin auch auf einen Sachverhalt angewendet, bei dem nicht die Entwicklung eines neuen Produkts auf einem nachgelagerten Markt verunmöglicht wurde, sondern auf demselben Markt, für den die «essential facility», eine geschützte Methode zur Erhebung von Daten über den deutschen Pharmamarkt, entwickelt wurde. Dieses Verfahren war im Zeitpunkt des Abschlusses des Manuskripts noch pendent. www.imshealth.com/ims/portal/front/articleC/ 0,2777,6599_3665_43811705,00.html (Oktober 2003).

Entscheid gezeigt, in welchem Programminformationen von Fernsehsendern als urheberrechtliche Inhalte grundsätzlich als wesentliche Einrichtung akzeptiert wurden. Bei Missbrauch kann der Rechteinhaber in ein Lizenzverhältnis gezwungen werden [36].

b) Urheberrechtliche Inhalte per se als «essential facility»

Technische Schutzmassnahmen können den Zugang zu Werken gänzlich unterbinden. Da zudem die urheberrechtlichen Schrankenregelungen nicht mehr anwendbar sind, nebst dem Privatgebrauch etwa das Zitatrecht oder das Recht der Berichterstattung über aktuelle Ereignisse, kann der Zugang zu Inhalten stärker ausgeschlossen werden als früher. Falls Inhalte jedoch eine wichtige Infrastruktur für nachfolgende Märkte darstellen, ihnen die Qualität der Nicht-Substituierbarkeit und der Nicht-Duplizierbarkeit zukommt, kann eine Lizenzierung kartellrechtlich erzwungen werden.

Bei Konsumgütern dürfte diese Konstellation kaum je auftreten. Eher denkbar ist sie bei schwierig zu generierender Information, weil deren Erstellung beispielsweise hohe Infrastrukturkosten bedingt und vor einer Liberalisierung etwa von Staatsseite bereitgestellt wurde, wie Wetterdaten oder andere statistische Daten (soweit ihnen Werkqualität zukommt – was allerdings nur dann eine Rolle spielen darf, wenn die Anwendbarkeit von technischen Schutzmassnahmen ebenfalls auf urheberrechtliche Werke beschränkt bleibt).

Auch wenn im Bereich des Zugangserhalts zu Information die Auswirkung technischer Schutz-massnahmen besonders unbefriedigend sind, bleibt doch festzustellen, dass hier das Kartellrecht an seine Grenzen stösst. Dieses hat im Bereich der «essental facility» primär die Aufrechterhaltung des Wettbewerbs im Angebotsmarkt im Visier, weniger den Schutz der Konsumenten und ihrer Informa-tionsbedürfnisse.

c) Schnittstelleninformationen als «essential facility»

Schnittstellen (Interfaces) sind Übergänge zwischen verschiedenen Hardwareteilen, zwischen Hardware und Software, zwischen verschiedenen Softwareprodukten und zwischen Computer-systemen und Mensch[37]. Die Kenntnis von Schnittstellen-Informationen ist die Voraussetzung für Kompatibilität im Bereich der Computertechnologie.

Werden Standards offiziellen Standard Development Organizations entwickelt, sind diese in der Regel öffentlich oder werden diskriminierungsfrei lizenziert. Verwendet ein Unternehmen aber einen nur ihm bekannten, proprietären Standard, ist ein Unternehmen, das ergänzende Produkte anbieten will, auf Schnittstellen-Informationen angewiesen. Speziell wenn der proprietäre Standard auf Grund der Marktmacht des Unternehmens zum industrieweiten De facto-Standard wird, führt kein Weg mehr an den Schnittstellen-Informationen vorbei, will ein zweites Unternehmen auf einem nachgelagerten Markt ein Produkt erfolgreich anbieten.

Das Urheberrecht stellt die Dekompilierung für Computerprogramme frei, d.h. gemäss Gesetz dürfen in Selbsthilfe die nötigen Schnittstellen-Informationen erforscht werden, sofern das Unternehmen, das an den Schnittstellen-Informationen interessiert ist, für das Computerprogramm eine Lizenz erworben hat, zudem darf die Information bloss zur Herstellung von Interoperabilität verwendet werden[38]. Dieser Grundsatz gilt unbeschadet allfälliger technischer Schutzmassnahmen, mit welchen das Computerprogramm geschützt ist. Das heisst, dass das Dekompilierungsrecht einem allfälligen Recht auf Integrität der Schutzmassnahmen vorgeht[39].

Die vorgenannte Regel gilt nur für Computerprogramme, darüber hinaus sowie allenfalls, wenn Informationen über Programme nicht durch Dekompilierung gewonnen werden können, greift unter Umständen die «essential-Facility»-Theorie ein. Informationen über eine Schnittstelle können durch-aus

[36] R. M. Hilty, Lizenzvertragsrecht, Bern 2001, 413.
[37] Vgl. die Definition in der EU-Computerprogramm-Richtlinie 91/250/EWG, Erwägungsgründe 10-12.
[38] Art. 21 URG i.V.m. Art. 17 URV.
[39] Vgl. dazu S. Lewinsky, Die Diplomatische Konferenz der WIPO 1996 zum Urheberrecht und zu verwandten Schutzrechten, ZUM 1997, 638.

eine «essential facility» darstellen, da ohne Zugang zu den Informationen ein Tätigwerden auf vor- oder nachgelagerten Märkten nicht möglich ist, falls das Unternehmen, welche die Schnittstellen-Informationen monopolisiert, eine marktbeherrschende Stellung inne hat. Das Verweigern des Zu-gangs zu den Schnittstellen-Informationen kann missbräuchlich sein, wenn das Unternehmen selber auf dem vor- oder nachgelagerten Markt tätig ist und keine so genannten legitimate business reasons das Verhalten rechtfertigen. In Betracht fällt die Verpflichtung, Schnittstellen-Informationen weiter-zugeben, allenfalls gegen angemessene Lizenzgebühr (Art. 13b KG)[40].

Als Beispiel können genannt werden: Schnittstellen-Informationen bei marktbeherrschender Betriebssystem-Software (wie Microsoft-Windows)[41] oder bei allfällig sich durchsetzender marktbeherrschender DRM- oder Playersoftware. So versucht Microsoft mit seiner DRM-Software (Media Data Session Toolkit) wie auch mit dem Windows Media Player Marktanteile zu gewinnen, indem diese an das Betriebssystem gekoppelt werden[42].

4. Unangemessene Preise oder Geschäftsbedingungen (Art. 7 Abs. 2 lit. c KG)

Art. 7 Abs. 2 lit. c KG könnte zur Anwendung kommen, falls über die Kontrolle des Zugangs oder der Nutzung von Inhalten der Abschluss von automatisierten Standardverträgen und ihre allfällige Ab-sicherung mittels technischer Mittel unangemessene Preise oder Konditionen durchgesetzt werden: Beispielsweise wenn zuerst günstigere Einstiegskonditionen geboten werden und bei ausreichend generierten Netzwerkeffekten, welche ein Umsteigen auf andere Produkte nur noch mit hohem Aufwand zulassen, die Preis- oder Konditionenschraube angezogen wird[43].

5. Koppelungsgeschäfte (Art. 7 Abs. 2 lit. f KG)

Falls der Kauf von spezifischer Software oder Hardware zur Bedingung gemacht wird beim Kauf von Inhalten, etwa spezifische Playersoftware oder Abspielgeräte, die erst den Zugang zu den Inhalten ermöglicht, kann darin ein Koppelungsgeschäfte gegenüber den Verbrauchern liegen, welches gemäss Art. 7 Abs. 2 lit. f KG unzulässig ist. Mangels Standardisierung sind DRM-Kontrollösungen oft proprietär. In manchen Fällen gäbe es offene Standards, die Portabilität und Interoperabilität gewährleisten würden, diese erscheinen aber, wohl aufgrund der stärkeren Kontrollierbarkeit und damit Kontrollmöglichkeiten eines proprietären Systems, für Anbieter unattraktiv.

Nebst dem Musikmarkt versuchen Anbieter, auch den Markt für Abspiel-Soft- und Hardware zu dominieren. Sony vertreibt etwa seine Musik mit eingebauten proprietären Sony-DRM-Lösungen von Intertrust und lässt sie meist nur zur Abspielung auf Sony-Geräten zu[44] .

V. Konsequenzen

Der Nachteil der Anwendung des Kartellrechts auf die oben dargelegter Problemfelder liegt in der einzelfallbezogenen sowie gleichermassen zeit- und kostenintensiven Durchsetzung solcher Rechtsansprüche. Mangels einer abstrakten Regel können bis zur Durchsetzung der kartellrechtlichen Ansprüche, welche immer auch den Nachweis der marktbeherrschenden Stellung des Anbieters voraussetzen, die Informationen für den Nachfrager bereits wertlos geworden sein. Das Erzwingen von Lizenzen dürfte nur in Ausnahmefällen möglich sein.

---

[40] Vgl. dazu etwa den Fall IBM aus dem Jahre 1984, bei Heinemann (Fn. 30, dort Fn. 1274), 517, mit weiteren Verweisen.

[41] Gegen Microsoft wurden auch schon zahlreiche Verfahren geführt, basierend auf der herausragenden Stellung ihres Betriebssystems von rund 90% Marktanteil.

[42] Microsoft verfolgt die Strategie, basierend auf der herausragenden Stellung ihres Betriebssystems Windows Nachfolge-Produkte daran zu koppeln, was die Marktbeherrschung auf weitere Märkte ausweiten könnte. Vgl. dazu den neuesten Kartellfall, den RealNetworks als Hersteller des Real-Player in San Jose (CA) gegen Microsoft angestrengt hat (NYtimes vom 19. Dezember 2003: RealNetworks Accuses Microsoft of Restricting Competition) wegen der Koppelung des Windows Media Player an das Windows-Betriebssystem.

[43] Dies ist Praxis im Softwaremarkt, etwa bei Microsoft-Produkten. Vgl. dazu auch Hilty (Fn. 36), 440.

[44] So brachte Sony im November 2003 eine CD der Gruppe «Naturally Seven» auf den Markt, deren digitale Files nur mit von Sony hergestellten oder lizenzierten Musik-Abspielgeräten abgespielt werden können. http://news.zdnet.co.uk/business/legal/0,39020651,39117759,00.htm, NZZ vom 21. November 2003, 65: Sony kündigt neues Kopierschutzverfahren an.

Diese Erkenntnis spricht dagegen, sich alleine auf das Kartellrecht zu verlassen, um eine Lösung für die voraussehbaren, negativen Folgen der technischen Abschottung von urheberrechtlichen Inhalten zu finden. Vielmehr sollte den Bedenken bereits auf Stufe des Urheberrechts, bei der Ausgestaltung der Unabänderbarkeit der technischen Schutzmassnahmen oder mittels zwingenden Schrankenbestimmungen im Sinne von Nutzerrechten Rechnung getragen werden. Nach dem Vorbild von Art. 6 der EU-Computerprogramm-Richtlinie 91/ 250/EWG und der entsprechenden Lösung von Art. 21 URG über die Dekompilierung von Computerprogrammen soll den relevanten Schrankenbestim-mungen zwingend der Vortritt vor technischen Schutzmassnahmen gelassen werden. Nur auf diese Weise kann demokratisch, kulturell oder anderen gesellschaftlich motivierten Zwecken des Privatge-brauchs angemessen Rechnung getragen werden. Bedenken der Rechtsinhaber nach einer Aushöhlung ihrer Stellung könnte dann mit neuen Geschäftsmodellen von Industrieseite und unter Umständen mit neuen Abgabemodellen Rechnung[45] getragen werden.

* lic. iur., Zürich.

[45] Vgl. etwa das Modell des ISP als Vergütungsmanager, bei L. Sobel, DRM as an Enabler of Business Models: ISPs as Digital Retailers, Berkeley Technology Law Journal, 2003.