UNIVERSITÄTSLEHRGANG
FÜR INFORMATIONSRECHT UND RECHTSINFORMATION
AN DER RECHTSWISSENSCHAFTLICHEN FAKULTÄT DER UNIVERSITÄT WIEN

Art. 6 Abs. 4 Info-RL
Tod der Privatkopie ?

MASTER THESIS

zur Erlangung des akademischen Grades

MASTER OF LAWS (LL.M.)

INFORMATIONSRECHT UND RECHTSINFORMATION

an der Universität Wien

(Universitätslehrgang für Informationsrecht und Rechtsinformation)

vorgelegt von

Dr. Gregor König

begutachtet von

MMag. Dr. Albrecht Haller

im September 2003

Hinweise

Dieses Layout basiert auf der Typoskriptvorlage der Reihe „Österreichische Rechtswissenschaftlichen Studien“ (ÖRSt). Die Verwendung, Bearbeitung und allfällige Veröffentlichung der Bearbeitung erfolgt mit freundlicher Bewilligung des Manz-Verlages. Ansonsten wird auf das UrhG verwiesen.

Als UrhG wird in den jeweiligen Kapiteln das österreichische bzw deutsche Urheberrechtsgesetz bezeichnet.

Vorliegende Arbeit orientiert sich im Wesentlichen an den AZR (*Friedl/H. Loebenstein* (Hrsg), Abkürzungs- und Zitierregeln der österreichischen Rechtssprache und europarechtlicher Rechtsquellen[5] (2001)). Zeitschriftenartikel werden mit der Anfangsseitenzahl zitiert, um eine leichtere Auffindbarkeit in der RDB zu ermöglichen. Wo es möglich ist, wird auch die genaue Seitenzahl des Zitats angegeben.

Die URLs wurden zuletzt am 1. September 2003 überprüft. Literatur und Judikatur wurden ebenfalls bis zu diesem Datum berücksichtigt.

Inhaltsverzeichnis

Abkürzungsverzeichnis

aA	=	anderer Ansicht
aaO	=	am angeführten Ort
AB	=	Ausschussbericht
ABGB	=	Allgemeines bürgerliches Gesetzbuch, JGS 946/1811
abl	=	ablehnend
ABl	=	Amtsblatt der Europäischen Gemeinschaften
Abs	=	Absatz
abw	=	abweichend
aE	=	am Ende
amtl	=	amtlich, -e, -er, -es
Anm	=	Anmerkung
AnwBl	=	Österreichisches Anwaltsblatt (ab 1951)
arg	=	argumento
Art	=	Artikel
Aufl	=	Auflage
Begr	=	Begründung
BG	=	Bundesgesetz
BGB	=	(deutsches) Bürgerliches Gesetzbuch
BGBl	=	Bundesgesetzblatt
BGH	=	(deutscher) Bundesgerichtshof
BlgNR	=	Beilage(-n) zu den stenografischen Protokollen des Nationalrates
BMBWK	=	Bundesministerium für Bildung, Wissenschaft und Kultur
BMG	=	Bundesministeriengesetz idF von 2001
BMJ	=	Bundesministerium für Justiz
Bsp	=	Beispiel/e
bspw	=	beispielweise
BT	=	(deutscher) Bundestag
B-VG	=	Bundesverfassungsgesetz 1920 idF v 1929
bzgl	=	bezüglich
bzw	=	beziehungsweise
C	=	Amtsblatt der Europäischen Gemeinschaften, Reihe Communication (Mitteilungen und Ausschreibungen)
CD-ROM	=	Compact Disc-Read Only Memory
Celex	=	Rechtsdatenbank der Europäischen Gemeinschaft (Communitatis Europeae Lex)
CR	=	Computer und Recht (ab 1985)
DatenbankRL	=	Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken, ABl Nr L 77 v 27. März 1996, 20.
DatenschutzRL	=	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl Nr L 281 v 23. November 1995, 31.
dh	=	das heißt
DMCA	=	Digital Millennium Copyright Act vom 28. Oktober 1998
DPRA	=	Digital Performance Right in Sound Recordings Act of 1995
Dr	=	Drucksache

DRM	=	Digital Rights Management
dt	=	deutsch, -e, -er, -es
dUrhG	=	deutsches Urheberrechtsgesetz vom 9. September 1965 idgF
E	=	Entscheidung
EB	=	Erläuternde Bemerkungen zur Regierungsvorlage
ECG	=	Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz), BGBl I 152/2001
ECMS	=	Electronic Copyright Management System
E-CommerceRL	=	Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), ABl Nr L 178 v 17. Juli 2000, 1
ecolex	=	Fachzeitschrift für Wirtschaftsrecht (ab 1990)
EFTA	=	European Free Trade Association (Europäische Freihandelsassoziation)
EG	=	Europäische Gemeinschaft
EGV	=	Vertrag zur Gründung der Europäischen Gemeinschaft idF von 1997
EMRK	=	Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950 („Europäische Menschenrechtskonvention")
endg	=	endgültig
engl	=	englisch, -e, -er, -es
EP	=	Europäisches Parlament
Erl	=	Erläuterung
Erläut	=	Erläuterungen zur Regierungsvorlage
Erw	=	Erwägungsgrund
EU	=	Europäische Union
EuGH	=	Gerichtshof der Europäischen Gemeinschaften
EuGI	=	Gericht der Europäischen Gemeinschaften I. Instanz
EvBl	=	Evidenzblatt der Rechtsmittelentscheidungen in Österreichische Juristen-Zeitung (1934-1938, ab 1946)
EV	=	Einführungsverordnung
EWG	=	Europäische Wirtschaftsgemeinschaft
EWR	=	Europäischer Wirtschaftsraum
f, ff	=	folgende
FN	=	Fußnote
FolgerechtsRL	=	Richtlinie 2001/84/EG des Europäischen Parlaments und des Rates vom 27. September 2001 über das Folgerecht des Urhebers des Originals eines Kunstwerks, ABl Nr L 272 v 13. Oktober 2001, 32.
ftp	=	file transfer protocol
G	=	Gesetz
GATT	=	General Agreement on Tariffs and Trade (Allgemeines Zoll- und Handelsabkommen) BGBl 1962/233
GP	=	Gesetzgebungsperiode
GRUR	=	Gewerblicher Rechtsschutz und Urheberrecht (1896-1944, ab 1948)
GRURInt	=	Gewerblicher Rechtsschutz und Urheberrecht – Internationaler Teil (ab 1967)

hA	=	herrschende Ansicht
HGB	=	Handelsgesetzbuch
hL	=	herrschende Lehre
Hrsg	=	Herausgeber
HS	=	Halbsatz
http	=	hyper text transfer protocol
idF	=	in der Fassung
idR	=	in der Regel
idS	=	in diesem Sinne
ieS	=	im engeren Sinn
IFPI	=	International Federation of the Phonographic Industry
IMA	=	Interessengemeinschaft Österreichischer Museen und Ausstellungshäuser
InfoSoc-RL	=	Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (ABl L 167 v 22. Juni 2001, 10, berichtigt durch ABl L 6 v 10. Jänner 2002, 71).
Info-RL	=	siehe InfoSoc-RL
inkl	=	inklusive
insbes	=	insbesondere
iS	=	im Sinne
ISBN	=	International Standard Book Number
ISP	=	Internet Service Provider
ISRC	=	International Standard Recording Code
iVm	=	in Verbindung mit
iwS	=	im weiteren Sinn
JBl	=	Juristische Blätter (1872-1938, ab 1946)
jew	=	jeweils; jeweilig, -e, -er, -es
Jud	=	Judikatur
JurPC	=	JurPC, Internet-Zeitschrift für Rechtsinformatik
K&R	=	Kommunikation und Recht (ab 1998)
KabelSatRL	=	Richtlinie 93/83/EWG des Rates vom 27. September 1993 zur Koordinierung bestimmter urheber- und leistungsschutzrechtlicher Vorschriften betreffend Satellitenrundfunk und Kabelweiterverbreitung, ABl Nr L 248 v 6. Oktober 1993, 15.
Kap	=	Kapitel
KG	=	Kammergericht
KOM	=	Kommission
L	=	Amtsblatt der Europäischen Gemeinschaften, Reihe Legislation (Rechtsvorschriften)
LAN	=	Local Area Network
leg cit	=	legis citatae (der zitierten Vorschrift)
Lfg	=	Lieferung
Lit	=	Literatur
lit	=	litera (Buchstabe)
Ls	=	Leitsatz
lt	=	laut
LVG	=	Literarische Verwertungsgesellschaft

mA	=	meiner Ansicht
MarkenRL	=	Erste Richtlinie 89/104/EWG des Rates vom 21. Dezember 1988 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die Marken, ABl Nr L 40 v 11. Februar 1989, 1.
mE	=	meines Erachtens
MMR	=	MultiMedia und Recht (ab 1998)
MP3	=	MPEG-1 Audio Layer 3
MP4	=	MPEG-1 Audio Layer 4
MPEG	=	Moving Picture Experts Group
MR	=	Zeitschrift für Medien und Recht (ab 1983)
mwH	=	mit weiteren Hinweisen
mwN	=	mit weiteren Nachweisen
NJW	=	Neue Juristische Wochenschrift (ab 1947)
Nov	=	Novelle
Nr	=	Nummer
NR	=	Nationalrat
Ob	=	Oberster Gerichtshof in Zivilsachen
OGH	=	Oberster Gerichtshof
OLG	=	Oberlandesgericht
ÖBl	=	Österreichische Blätter für gewerblichen Rechtsschutz und Urheberrecht (ab 1952)
ÖJZ	=	Österreichische Juristen-Zeitung (1934-1938, ab 1946)
ÖSGRUM	=	Österreichische Schriftenreihe zum Gewerblichen Rechtsschutz, Urheber- und Medienrecht (ab 1985)
österr	=	österreichisch, -e, -er, -es
PDA	=	Personal Digital Assistant
PDF	=	Portable Document Format
Pkt	=	Punkt
PPV	=	Produktpiraterie-VO, VO Nr 3295/94 des Rates vom 22. Dezember 1994 über Maßnahmen zum Verbot der Überführung nachgeahmter Waren und unerlaubt hergestellter Vervielfältigungsstücke oder Nachbildungen in den zollrechtlich freien Verkehr oder in ein Nichterhebungsverfahren sowie zum Verbot ihrer Ausfuhr und Wiederausfuhr, durchgeführt durch die VO Nr 1367/95 der Kommission vom 16. Juni 1995 und geändert durch die VO Nr 241/99 des Rates vom 25. Jänner 1999
RBÜ	=	Revidierte Berner Übereinkunft zum Schutze von Werken der Literatur und der Kunst, Pariser Fassung BGBl 1982/319
RDB	=	Rechtsdatenbank
RdW	=	Österreichisches Recht der Wirtschaft (ab 1983)
RfR	=	Zeitschrift für Rundfunkrecht (ab 1977), Beilage zu ÖBl
RGBl	=	(deutsches) Reichsgesetzblatt
RiAA	=	Recording Industry Association of America
RIS	=	Rechtsinformationssystem des Bundes
RL	=	Richtlinie der Europäischen Gemeinschaften
Rn	=	Randnummer
Rs	=	Rechtsache
RSpr	=	Rechtsprechung
RV	=	Regierungsvorlage
Rz	=	Randzahl

S	=	Satz, Seite
SchutzdauerRL	=	Richtlinie 93/98/EWG des Rates vom 29. Oktober 1993 zur Harmonisierung der Schutzdauer des Urheberrechts und bestimmter verwandter Schutzrechte, ABl Nr L 290 v 24. November 1993, 9.
Sec	=	Section
Slg	=	Sammlung
SoftwareRL	=	Richtlinie 91/250/EWG des Rates vom 14. Mai 1991 über den Rechtsschutz von Computerprogrammen, ABl Nr L 122 vom 17. Mai 1991, 42.
sog	=	sogenannt, -e, -er, -es
SSt	=	Entscheidungen des österreichischen Obersten Gerichtshofes in Strafsachen und Disziplinarangelegenheiten, veröffentlicht von seinen Mitgliedern unter Mitwirkung der Generalprokuratur (1921-1938, ab 1946)
st	=	ständig(e)
StGB	=	Strafgesetzbuch, BGBl 1974/60
StPO	=	Strafprozessordnung 1975, BGBl 631/1975
SWK	=	Österreichische Steuer- und Wirtschaftskartei (ab 1925)
SZ	=	Entscheidungen des österreichischen Obersten Gerichtshofes in Zivil- (und Justizverwaltungs-) sachen, veröffentlicht von seinen Mitgliedern (1919-1938, ab 1946)
techn	=	technisch, -e, -er, -es
TKG	=	Telekommunikationsgesetz, BGBl I 1997/100 idgF
TRIPS	=	Trade-Related Aspects of Intellectual Property Rights Abkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums vom 15.4.1994
ua	=	unter anderem
UFITA	=	Archiv für Urheber-, Film-, Funk- und Theaterrecht (1928-1944, ab 1954)
UNESCO	=	United Nations Education, Scientific and Cultural Organisation (Organisation der Vereinten Nationen für Erziehung, Wissenschaft und Kultur)
UNO	=	United Nations Organization (Organisation der Vereinten Nationen)
UrhG	=	Urheberrechtsgesetz BGBl 1936/111 über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte idgF
UrhG-Nov	=	Urheberrechtsgesetz-Novelle
URL	=	Uniform Ressource Locator
U.S.C.	=	United States Code
usw	=	und so weiter
UWG	=	Bundesgesetz gegen den unlauteren Wettbewerb BGBl 1984/448 idgF
v	=	vom, von
va	=	vor allem
Vermiet- und VerleihRL	=	Richtlinie 92/100/EWG des Rates vom 19. November 1992 zum Vermietrecht und Verleihrecht sowie zu bestimmten dem Urheberrecht verwandten Schutzrechten im Bereich des geistigen Eigentums, ABl Nr L 346 v 27. November 1992, 61.
vgl	=	vergleiche
VO	=	Verordnung der EG

VÖB	=	Vereinigung Österreichischer Bibliothekarinnen und Bibliothekare
VÖZ	=	Verband österreichischer Zeitungsherausgeber und -verleger
vs	=	versus (gegen)
VwGH	=	Verwaltungsgerichtshof
WBl	=	Wirtschaftsrechtliche Blätter, Beilage zu Juristische Blätter (ab 1987)
WCT	=	WIPO Copyright Treaty
WIPO	=	World Intellectual Property Organization
WK	=	Wirtschaftskammer Österreichs
WPPT	=	WIPO Performances and Phonograms Treaty
WTO	=	World Trade Organisation (Welthandelsorganisation)
WUA	=	Welturheberrechtsabkommen BGBl 1957/108
WWW	=	World Wide Web
Z	=	Zahl, Ziffer
zB	=	zum Beispiel
ZfRV	=	Zeitschrift für Rechtsvergleichung (1960-1990) Zeitschrift für Rechtsvergleichung, Internationales Privatrecht und Europarecht (ab 1991)
ZKDSG	=	(deutsches) Gesetz zum Schutz von Zugangskontrolldiensten vom 19. März 2002 idgF
ZRS	=	Zivilrechtssache
ZugangskontrollRL	=	Richtlinie 98/84/EG des Europäischen Parlaments und des Rates vom 20. November 1998 über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten ABl Nr L 320 vom 28. November 1998, 54
ZuKG	=	Zugangskontrollgesetz BGBl I 2000/60 über den Schutz zugangskontrollierter Dienste
zum	=	zumindest
ZUM	=	Zeitschrift für Urheber- und Medienrecht (ab 1957; bis 1983 Film und Recht)
zT	=	zum Teil

Literaturverzeichnis

Bayreuther, Beschränkungen des Urheberrechts nach der neuen EU-Urheberrechtsrichtlinie, ZUM 2001, 828.

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

Biehl/Thielscher, Copyright-Schutz digitaler Daten durch kryptographische Fingerprint-Schemata und kognitive Robotik – Perspektiven und Grenzen der KI-Forschung (1999)

Brenn, Richtlinie über Informations- und Kommunikationsdienste mit Zugangskontrolle und Überlegungen zur innerstaatlichen Umsetzung, ÖJZ 1999, 81.

Brenn, Zugangskontrollgesetz, Kurzkommentar (2001).

Buchinger/Zivny, Kampf den Raubkopien – Gesetzesnovelle schränkt Vervielfältigung geschützter Werke ein, in Die Presse, Rechtspanorama vom 7. April 2003.

Ciresa, Österreichisches Urheberrecht, 2. Lfg (2000).

Dreier, Die Umsetzung der Urheberrechtsrichtlinie 2001/29/EG in deutsches Recht, ZUM 2002, 28.

Dreier, Urheberrecht an der Schwelle des 3. Jahrtausends. Einige Gedanken zur Zukunft des Urheberrechts, CR 2001, 45.

Fallenböck/Haberler, Technische Schutzmaßnahmen und Urheberrecht in der Informationsgesellschaft, ecolex 2002, 262.

Flechsig, Grundlagen des Europäischen Urheberrechts – Die Richtlinie zur Harmonisierung des Urheberrechtsschutzes in Europa und die Anforderungen an ihre Umsetzung in deutsches Recht, ZUM 2002, 1.

Freytag, Digital Millenium Copyright Act und europäisches Urheberrecht für die Informationsgesellschaft, MMR 1999, 207.

Fromm/Nordemann (Hrsg), Urheberrecht: Kommentar zum Urheberrechtsgesetz und zum Urheberrechtswahrnehmungsgesetz, 9. Aufl (1998)

Gaster, Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft, ZUM 1995, 740.

Haller, Music on Demand – Internet, Abrufdienste und Urheberrecht (2001).

Haller, Österr. Justizministerium: Entwurf für Zugangskontrollgesetz, MMR 5/2000, XI.

Haller, Zum EG-Richtlinienvorschlag betreffend Urheberrecht in der Informationsgesellschaft, MR 1998, 61.

Heide, Copyright in the EU and U.S.: What 'Access-Right'?, Journal of the Copyright Society of the USA, Vol. 48, No. 3, Spring 2001 und http://papers.ssrn.com/sol3/papers. cfm?abstract_id=270861

Heide, Access Control and Innovation under the Emerging EU Electronic Commerce Framework, B.T.L.J. (2000), Vol.15, No.3 und http://www.law.berkeley.edu/journals/btlj/articles/vol15/heide/heide.html

Helberger, Hacken von Premiere bald verboten ?, ZUM 1999, 295.

Hoeren, Entwurf einer EU-Richtlinie zum Urheberrecht in der Informationsgesellschaft – Überlegungen zum Zwischenstand der Diskussion, MMR 2000, 515.

Hoeren, Internetrecht (Februar 2003).

Jaeger, Auswirkungen der EU-Urheberrechtsrichtlinie auf die Regelungen des Urheberrechtsgesetzes für Software, CR 2002, 309.

König, Die Informationsrichtlinie und ihre geplante Umsetzung in Österreich (2003).

Kröger, Die Urheberrechtsrichtlinie für die Informationsgesellschaft – Bestandsaufnahme und kritische Bewertung, CR 2001, 316.

Linnenborn, Update: Europäisches Urheberrecht in der Informationsgesellschaft, K&R 2001, 394.

Marly, Rechtsschutz für technische Schutzmechanismen geistiger Leistungen, K&R 1999, 106.

Metzger/Kreutzer, Richtlinie zum Urheberrecht in der „Informationsgesellschaft – Privatkopie trotz technischer Schutzmaßnahmen ?, MMR 2002, 139.

Mogel, EU-Richtlinienvorschlag: Urheberrecht in der Informationsgesellschaft, ecolex 2001, 241.

Mogel, Europäisches Urheberrecht (2001).

Pohler, Urheberrecht und Multimedia – ein unauflöslicher Konflikt ? Aktuelle Rechtsfragen (1998).

Raubenheimer, Vernichtungsanspruch gemäß § 69f UrhG, CR 1994, 129.

Reinbothe, Die EG-Richtlinie zum Urheberrecht in der Informationsgesellschaft, GRURInt 2001, 733.

Reinbothe, Die Umsetzung der EU-Urheberrechtsrichtlinie in deutsches Recht, ZUM 2002, 43.

Reinbothe, Neue Medien und Urheberrecht – Strategien der Europäischen Union im Europäischen Umfeld, ÖBl 1998, 155.

Schippan, Urheberrecht goes digital - Das Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft, ZUM 2003, 378.

Spindler, Europäisches Urheberrecht in der Informationsgesellschaft, GRUR 2002, 105.

v. Lewinski/Gaster, Die diplomatische Konferenz der WIPO 1996 zum Urheberrecht und zu verwandten Schutzrechten – Ergebnisse und Folgen, ZUM 1997, 607.

Wand, Technische Schutzmaßnahmen und Urheberrecht (2001).

Walter (Hrsg), Europäisches Urheberrecht (2001).

Wildpaner, Behindert die Anti-Pirateriegesetzgebung des DMCA den „Fair Use“?, MR 2002, 383.

Wittmann, Die EU-Urheberrechts-Richtlinie – ein Überblick, MR 2001, 143.

Zecher, Die Umsetzung der EU-Urheberrechtsrichtlinie in deutsches Recht, ZUM 2002, 52.

Sonstige Quellen und online Datenbanken

http://bundesrecht.juris.de

„Deutsches RIS“, beschränkt auf das Bundesrecht (nicht vollständig!).

http://europa.eu.int

Datenbank des Europaservers.

http://europa.eu.int/comm/commissioners/liikanen/profile/interest/digitalrights.pdf

Europäische Kommission, Commission Staff Working Paper Digital Rights, Brüssel 2002.

http://www.ivir.nl

Instituut voor Informatierecht, Amsterdam.

http://www.uni-muenster.de/Jura.itm/hoeren/

Institut für Informations-, Telekommunikations- und Medienrecht – Zivilrechtliche Abteilung, Münster (Hoeren-Skript).

http://www.urheberrecht.org

Institut für Urheber- und Medienrecht, München.

I. Einleitung

Die Informationsrichtlinie sieht als erste Richtlinie (im folgenden RL) im Urheberrechtsbereich in ihrem Art 6 erstmals einen Schutz von techn Maßnahmen zum Urheberrechtschutz für alle Werkkategorien vor (der Softwarebereich ist allerdings weiterhin in Art 7 Abs 1 lit c SoftwareRL geregelt). Da die RL diesen Schutz in die Hände der Mitgliedstaaten legt, entstehen dem Einzelnen keine konkreten Rechte und Pflichten. Was nun ist aber mit jenem Kreis von aus den Schrankenbestimmungen des Art 5 Info-RL oder aus den freien Werknutzungen, die auf gesetzlichen Lizenzen basieren, Begünstigten? Die Schutzmechanismen, die durch Art 6 Info-RL geschützt werden, werden ja auch in den Ausnahmefällen keinen Zugang erlauben. Diesen Interessenkonflikt zwischen Rechteinhabern und Werknutzungsberechtigten versucht Art 6 Abs 4 Info-RL zu lösen, der allerdings mehr Probleme und Fragen aufwirft. Diese sollen im Rahmen der vorliegenden Arbeit behandelt und – wenn möglich – gelöst bzw beantwortet werden.

Die Arbeit beschäftigt sich zunächst mit Digital Rights Management (DRM) Systemen, welche (zumindest auch) eingesetzt werden können, um die Ziele des Art 6 Info-RL zu verwirklichen. Es werden die grundsätzlichen techn Lösungsansätze präsentiert und einige DRM-Systeme der Praxis vorgestellt.

Anschließend erfolgt ein kurzer geschichtlicher Abriss der Info-RL. Bevor näher auf Art 6 Abs 4 Info-RL eingegangen wird, werden die anderen Absätze der Bestimmung und deren Problematik besprochen.

Das folgende Kapitel beschreibt nach einer Übersicht der verschiedenen Lösungsmöglichkeiten einer Umsetzung von Art 6 Abs 4 Info-RL, wozu sich der österr bzw dt Gesetzgeber entschlossen haben.

Schließlich erläutert die Arbeit auch das Verhältnis von ZugangskontrollRL und Info-RL bzw deren Umsetzungen in österr und dt Recht. Zu diesem Zweck werden die Regelungen näher vorgestellt, bevor auf etwaige Überschneidungen eingegangen wird.

Im Anhang finden sich der Volltext von Art 6 Info-RL und der der Umsetzung entsprechenden Bestimmungen des österr und dt UrhG.

II. Digital Rights Management Systems

A. Begriff

Vor allem durch das Internet aufgekommene Missbrauchsmöglichkeiten können oft besser durch techn Einrichtungen verhindert werden als dies durch rechtliche Sanktionen möglich wäre. Dieser techn Schutz wird daher als wesentliches Element der „digitalen Agenda“ auch in den Verträgen der WIPO[1] sowie der Info-RL vorgesehen. Jene techn Schutzmöglichkeiten werden zusammengefasst als Digital Rights Management (DRM) Systems oder Electronic Copyright Management Systems (ECMS) bezeichnet und können verschiedene Komponenten beinhalten, mit denen Rechte im digitalen Umfeld techn identifiziert, organisiert, beschränkt und durchgesetzt werden sollen.[2] Interessanter Nebennutzen wäre darüber hinaus die Ermöglichung nutzungsabhängiger Individualabrechnungen.[3]

Einige DRM-Systeme beruhen auf der Verpackung verschlüsselter digitaler Werke in einer Software-Schicht, welche die Copyright- und Nutzungsinformationen oder Verweise auf selbige enthält, andere wiederum schützen den Inhalt über die Hardware. Trefflich bezeichnet man DRM-Systeme als „Wächter“ über die im Inneren enthaltenen Informationen. Sie verfolgen verschiedene Ziele:

- Legitimation (Legitimation): Gewährleistung, dass nur bezahlte Inhalte konsumiert werden; Informationen sollen nur berechtigten Personen zur Verfügung stehen. Dies wird erreicht durch verschiedene Hardware- oder Software-Lösungen.
- Vertraulichkeit (Confidentiality): Schutz von sensibler Information in ungesicherten Netzen, erzielt durch Verschlüsselungsverfahren.
- Integrität der Daten (Data Integrity): Schutz vor unautorisierter Änderung der Daten, ermöglicht durch Digitale Fingerabdrücke.
- Authentizität der Daten (Data Authenticity): Identifizierbarkeit urheberrechtlich geschützter Werke und deren Urheber, verwirklicht über Digitale Wasserzeichen.

B. Technische Lösungsansätze

DRM-Systeme können verschiedene Eigenschaften haben. Sie können die Kopierfähigkeit eines geschützten Objekts beeinflussen und werden deshalb auch anti-copying-devices genannt[4], andere beschränken lediglich den Zugang

---

1 Siehe dazu unten III.A.
2 Working Paper Digital Rights, 3.
3 *Bechtold*, GRUR 1998, 18 (19).
4 Vgl *Hoeren*, MMR 2000, 515 (520).

oder den Nutzungsumfang[5], wieder andere ermöglichen die Überwachung von Werknutzungen, indem Werke, geschützte Leistungen, Rechteinhaber und Nutzungsumfang automatisch oder individuell identifiziert und beschrieben werden. Schon oben angesprochen wurde die Funktion der individuellen Abrechnung auf dem Weg des Werkes vom Anbieter zum Nutzer. Dabei kann die Abrechnungsfunktion in das Werk selbst oder in die Werkumgebung (Software oder Hardware) eingebunden sein, wobei die Realisierung über vertrauenswürdige Dritte, den sog Clearing-Stellen[6] bzw Trust-Centern, erfolgen soll.

Folgende Grundprinzipien werden technikseitig angewandt:

1. Digitale Wasserzeichen (Watermarks)

Bei digitalen Wasserzeichen handelt es sich um im Inhalt des Werkes selbst für den Nutzer nicht wahrnehmbare (also versteckte) und den Gebrauch des Werkes nicht beeinträchtigende und im Idealfall auch nicht veränder- oder entfernbare Informationen.[7] Nur der Rechtsinhaber kann durch Vergleich mit dem Original diese Markierungen erkennen. Es existieren allerdings auch Verfahren, die bewusst sichtbare Markierungen an dem zu schützenden Objekt anbringen (Tattooing) und ebenfalls als Wasserzeichen bezeichnet werden.

Mittels digitaler Wasserzeichen ist nicht nur das Auffinden derart markierter Objekte mit automatisierten Suchmaschinen, die Darlegung der Urheberschaft[8] und die Identifikation illegaler Kopien möglich, sondern auch bei nutzerseitig installierten Software- oder Hardwarelösungen die Durchsetzung von Nutzungsbeschränkungen zB durch Einfügen eines auf das Abspielgerät abgestimmten Codes in das Werkexemplar, der die Nutzung verhindern oder kanalisieren soll.[9]

In der Theorie müssen Wasserzeichentechniken bestimmten Anforderungen gerecht werden. Die in das Datenmaterial eingebrachte Wasserzeicheninformation muss gegenüber zufälligen Veränderungen des Datenmaterials oder Medienverarbeitungen widerstandsfähig sein (Robustheit). Es darf nicht möglich sein, die eingebaute Information aufzuspüren, zu verfälschen oder zu zerstören, selbst unter den Bedingungen, dass einem möglichen Angreifer zwar das Verfahren der Implementierung bekannt ist und ihm mindestens ein markiertes Datenmaterial zur Verfügung steht, der geheime Schlüssel jedoch unbekannt ist (Sicherheit).

2. Kryptografieverfahren

Die Verschlüsselung bzw Passwort-Sicherung kodiert die Daten mithilfe mathematischer Algorithmen so, dass auf das Werk oder Teile desselben ohne

---

[5] Working Paper Digital Rights, 10.

[6] ZB die Clearingstelle Multimedia für Verwertungsgesellschaften (CMMV), siehe http://www.cmmv.de.

[7] Genauer dazu *Biehl/Thielscher*, Copyright-Schutz digitaler Daten durch kryptographische Fingerprint-Schemata und kognitive Robotik, 9f.

[8] *Linnenborn*, K&R 2001, 394 (399).

[9] Working Paper Digital Rights, 3 u 19.

entsprechenden Entschlüsselungscode nicht zugegriffen werden kann.[10] Diese Verfahren finden auch schon außerhalb des Urheberrechts einen großen Anwendungsbereich (Pay-TV).[11] Problematisch erweist sich bei symmetrischen Verfahren mit nur einem Schlüssel zur Ver- und Entschlüsselung die leichte Entschlüsselbarkeit und die notwendige Passwortweitergabe, was bei asymmetrischen Verfahren vermieden wird. Hier wird das Werk mittels eines öffentlichen Schlüssels des Adressaten vom Rechteinhaber verschlüsselt, sodass nur der Adressat mittels seines privaten Schlüssels eine Entschlüsselung vornehmen kann. Diese Verfahren gelten wegen der Vermeidung des Problems des Schlüsselaustausches als besonders sicher.[12]

3. Hardwareseitiger Schutz

Die Hardwarelösung besteht in Benutzung von Hardwaresteckern, sog Dongles, die an eine Schnittstelle des Computers angesteckt werden und einen Chip mit Informationen oder Programmteilen beinhalten. Während Ausführung des Programms wird laufend auf den Dongle zugegriffen, wird er abgesteckt, funktioniert das Programm nicht mehr ordentlich oder gar nicht. Auch eine Vervielfältigung ist entgegen einer Software-Schutzlösung schwer bis gar nicht möglich.[13] Da allerdings der Hardwareschutz relativ teuer ist, eignet er sich besser für kostenintensive Inhalte wie aufwendig programmierte Software und ist für die Vielzahl von Inhalten und Zugriffen im Internet eher schlecht einsetzbar.

Eine weitere Möglichkeit, Inhalte hardwareseitig zu schützen, besteht in der physischen Zerstörung eines Teilstücks des Originaldatenträgers, etwa dem Sektor einer CD. Bei Vervielfältigung dieser CD versucht das Kopierprogramm den gesamten Inhalt auszulesen, was fehlschlägt und zu einem Abbruch führt. Das Originalprogramm selbst umgeht allerdings bewusst den kaputten Sektor. Seit einiger Zeit ist dieser Schutz nicht mehr effektiv, da moderne Kopierprogramme in der Lage sind, den kaputten Sektor der CD zu erkennen und zu ignorieren.

---

[10] *Bechtold*, GRUR 1998, 18 (20); *Wand*, Technische Schutzmaßnahmen und Urheberrecht, 11.

[11] *Wand*, Technische Schutzmaßnahmen und Urheberrecht, 12f.

[12] Folgende Probleme stellen sich aber auch bei asymmetrischer Verschlüsselung: Privatheit des privaten Schlüssels garantieren (Lösung: Chipcard, PIN-Code); Zuordnung des Schlüsselpaars zu einer Person (Lösung: Trusted Third Party; zB Pretty Good Privacy PGP, siehe http://www.pgpi.org); Rechtssicherheit neben techn Sicherheit. Lösung zu letztem Pkt die RL 1999/93/EG des europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen sowie deren Umsetzung in Österreich, das Bundesgesetz über elektronische Signaturen (Signaturgesetz), BGBl I 1999/190 idgF, bzw in Deutschland, das Gesetz über Rahmenbedingungen für elektronische Signaturen, online unter http://www.iid.de/iukdg/gesetz/SigAendG2.pdf.

[13] *Wand*, Technische Schutzmaßnahmen und Urheberrecht, 17.

4. Digitale Fingerabdrücke (Fingerprints)

Digitale Fingerabdrücke sollen die Integrität der Daten sicherstellen und sind das Ergebnis der Anwendung von Hash-Funktionen. Eine Hash-Funktion stellt eine Abbildung von Nachrichten beliebiger Länge auf Wörter fester Länge dar. Damit eine Hash-Funktion als sicher gilt, muss sie zwei Anforderungen erfüllen. Einerseits darf es nicht möglich sein, aus einem einmal erzeugten Hashwert (mit vernünftigem Aufwand) die ursprüngliche Byte-Folge zu rekonstruieren (Unumkehrbarkeit), andrerseits darf es ebenso nicht möglich sein, zwei unterschiedliche Bytefolgen zu konstruieren, die den gleichen Hashwert haben. Die kleinste Veränderung in einer Bytefolge muss also zwingend zu einem anderen Hashwert führen (Kollisionsfreiheit).

Zu beachten ist hier, dass sich bei digitalen Daten die Datei verändern kann, ohne dass dadurch der Inhalt beeinflusst wird, zB durch Kompression. Hier wäre es daher sinnvoll, zusätzlich zu einem Fingerabdruck auf Basis der Datei (also der Syntax) auch eine Art Fingerabdruck des Inhalts (also der Semantik) anzufertigen. Die praktische Umsetzung dieses Ansatzes findet man zB im AudioID-System[14], welches vom Fraunhofer Institut für Integrierte Schaltungen[15] entwickelt wird. Mittels AudioID wird einem Musikstück eine Art inhaltsbasierter Fingerabdruck entnommen. Damit soll dann das einfache Auffinden von va illegalen Audio- und Videodaten im Internet ermöglicht werden.

C. DRM-Systeme im Überblick

Beispielhaft sollen im folgenden einige kommerzielle DRM-Systeme vorgestellt werden:[16]

1. Content Guard

Content Guard[17] als Gemeinschaftsprojekt von Xerox und Microsoft ermöglicht Rechteinhabern, ihre Werke mit einer Schutzhülle zu umgeben, um auf diese Art Rechte und Modalitäten der Nutzung festzulegen.[18] Dies erfolgt für Rechteinhaber einfach über XrML (eXtensible rights Mark-up Language), einer eigenen Sprache zur Festlegung der Parameter.

2. DAS

Digital Asset Server[19] von Microsoft dient dem elektronischen Publizieren sog e-Books, indem es als Schnittstelle zwischen Autor bzw

---

[14] http://www.iis.fraunhofer.de/amm/download/audioid_d.pdf.

[15] http://www.iis.fraunhofer.de.

[16] Weitere hier nicht behandelte Systeme sind etwa Macrovisions (http://www.macrovision.com) MacroSAFE für Videos und ADo^{2}RA^{sm} (http://www.dwsco.com/ps_adora.html) von Digital World Service (http://www.dwsco.com).

[17] http://www.contentguard.com.

[18] Working Paper Digital Rights, 21.

[19] http://www.microsoft.com/reader/default.asp.

Distributor und Nutzer fungiert. Der Rechteinhaber vergibt individuell Beschränkungen in Bezug auf die Verwertungshandlungen, der Nutzer bekommt seine Version über die Schnittstelle ausgeliefert[20], die er mit entsprechender Lesesoftware von Microsoft im vorgegebenen Rahmen gebrauchen kann.

3. EMBASSY Trust System

Das EMBASSY Trust System[21] von WaveSystems[22] ist ein Client-Server-Modell, wo eine kleine Verbindung aus Hardware-Chip und Betriebssystemsoftware (EMBASSY Trusted Client) in das System des Nutzers implementiert wird. In diesem System werden dann die Nutzerinformationen gespeichert, alle erforderlichen Transaktionen abgewickelt und Sicherheitsbestimmungen überwacht. Diese Clients sind über das Internet an spezielle Server angeschlossen (EMBASSY Trust Assurance Network). Vorteile dieses Systems sind für den Nutzer die sichere Datenverwahrung und für den Anbieter die sichere Abwicklung des Geschäfts sowie die Rechteeinhaltung. Das System eignet sich aufgrund seiner geringen Größe für viele Anwendungsbereiche (PC, PDA, einfache Verbraucherelektronik), angefangen von allgemeinen E-Commerce-Anwendungen bis hin zur gezielten Content-Verwaltung urheberrechtlich geschützter Objekte.[23]

4. EMMS

Das Electronic Media Management System[24] von IBM[25] ist eine praktisch bewährte E-Commerce-Softwarelösung, die mit ihren fünf Softwareprodukten eine techn Plattform für den Handel und die Auslieferung von audiovisuellen digitalen Inhalten über verschiedene digitale Übertragungssysteme ermöglicht. Firmen wie Liquid Audio, Reciprocal, RealNetworks, BMG Entertainment und Sony Music Entertainment Japan vertrauen auf diese Technik. Sie beinhaltet bspw eine Software zum Watermarking, also dem Versehen von Bildern mit digitalen Wasserzeichen.[26]

5. FileOpen

FileOpen[27] stellt (zusätzliche) umfangreiche Sicherheitsfunktionen für Dateien im PDF-Format zur Verfügung und ist demnach als Plug-In für Adobe Acrobat[28] erhältlich. An zusätzlichen Sicherheitsbeschränkungen ermöglicht FileOpen eine Verschlüsselung nicht über Passwort, sondern verpackt die

---

[20] Working Paper Digital Rights, 20.
[21] http://www.wave.com/technology/ets.html.
[22] http://www.wave.com.
[23] http://www.wave.com/technology/trust_client.html.
[24] http://www.ibm.com/software/is/emms/.
[25] http://www.ibm.com.
[26] Working Paper Digital Rights, 20. Siehe oben II.B.1.
[27] http://www.fileopen.com.
[28] http://www.adobe.de.

geschützten Inhalte zusammen mit dem Client-Programm in einer Datei. Beim Starten der Datei installiert sich die Zugriffserlaubnis unbemerkt in der Registry des PC-Systems, sodass eine Weitergabe der Datei nicht mehr möglich ist. Als zusätzliche Maßnahmen lassen sich auch eine Selbstzerstörungsfunktion oder ein Ablaufdatum für die Nutzung einbauen.[29] Für diese Einschränkungen gibt es im Gegensatz zu den Acrobat-eigenen Sicherheitsfunktionen auch noch keine Software zur Umgehung.

6. Info2Clear

Info2Clear[30] soll den interaktiven Abruf von digitalen Zeitungsartikeln ermöglichen und richtet sich demnach an die Zeitungsindustrie. Hier werden die Inhalte mit einem nicht entfernbaren verschlüsselten Siegel versehen, das den Gebrauch kontrolliert und die Suche und Identifizierung bei unerlaubter Verwendung im Internet erleichtert.[31]

7. InterTrust

InterTrust[32] ist ein universelles DRM-System für Anbieter von digitaler Information, Technik und kommerzieller Services. Zentrales Element ist eine Sicherheitsdatenbank, ein sog InterRight Point auf dem PC oder einem sonstigen Abspielgerät, welche die Identität, die Zugriffsrechte, die Transaktionen und das Budget des Nutzers verwaltet. Die Rechteinhaber bieten ihre Inhalte verschlüsselt in sog Digiboxes an. Wenn der Status des auf dem Gerät des Nutzers vorhandenen InterRight Point mit jenem der Digibox übereinstimmt oder besser ist, wird der Zugriff auf den Inhalt ermöglicht. Die Rechteinhaber können Regelungen betreffend Öffnen, Abspielen, Kopieren und Ausdrucken sowie Abrechnung treffen.[33]

8. Liquid Audio

Liquid Audio[34] für den Musik- und Audiobereich besteht aus einer Player- und einer Serversoftware. Audiodateien werden mit einem nicht hörbaren digitalen Wasserzeichen versehen, um diese im Internet auffinden oder auf eine bestimmte Abspielsoftware eines bestimmten Nutzers kodieren zu können. Nutzungsrechte, wie Abspielen, Kopieren, Speichern auf CD-ROM können vom Rechteinhaber individuell und umfassend festgelegt werden. Liquid Audio arbeitet im Musikbereich mit ca 66 Verlagen zusammen.[35]

---

[29] http://www.fileopen.com/faqpage.html.
[30] http://www.info2clear.com.
[31] Working Paper Digital Rights, 22.
[32] http://www.intertrust.com.
[33] Working Paper Digital Rights, 20.
[34] http://www.liquidaudio.com.
[35] Working Paper Digital Rights, 21.

9. Mediaforce

Bei Mediaforce Anti-Piracy Services[36] handelt es sich nicht um DRM-Systeme ieS, allerdings lassen sich mit Dateinamenvergleich und sich automatisch verändernder und anpassender intelligenter Suchalgorithmen, die 25 peer-to-peer Systeme, Internetseiten und Newsgroups auf urheberrechtlich bedenkliche Kopien durchsuchen und diese mit den Datenbanken der Rechteinhaber vergleichen, gleiche Ziele verfolgen.

10. RPS

Das Rights Protection System[37] der IFPI[38] ist ein System zur Sperrung des Zugriffs auf Urheberrechte verletzende Websites. Es unterbindet gezielt den Zugriff auf einzelne URLs, also zB auf einzelne MP3-Songs mit unerlaubt angebotenen oder gesetzwidrigen Inhalten.

Hierfür wird eine Caching-Technik eines großen Software-Anbieters eingesetzt. Als Hardware-Komponenten können Geräte verschiedener Hersteller eingesetzt werden, da das System den ISP-Systemstandards entspricht und vollkommen kompatibel ist. Die entwickelte Technik ist in der Lage, die Datenanfragen an die Border-Gateway-Router der einzelnen ISP zu analysieren und gezielt den Zugriff auf die URLs mit illegalen oder gesetzeswidrigen Inhalten zu verhindern. Damit man den grenzüberschreitenden Datenverkehr analysieren kann, müssen die RPS-Server bei allen ISP mit einer eigenen Auslandsleitung zusätzlich zu der normalen techn Ausstattung aufgestellt werden. Da alle Systemkomponenten den Standards der ISP entsprechen, ist eine Implementierung in deren Systeme kurzfristig, schnell und ohne hohen Kostenaufwand möglich. Das laufende System bedarf keiner extra Wartung.

Damit das RPS den Zugriff auf illegale Webseiten verhindern kann, muss der Server mit den entsprechenden URLs versorgt werden. Das könnte dadurch geschehen, dass die bei den einzelnen ISP aufgestellten RPS Server über eine gesicherte Datenleitung von einem zentralen Punkt aus versorgt werden. Dies kann mehrmals täglich erfolgen (zB im Stundentakt), damit die URL-Liste immer auf dem neuesten Stand bleibt. Die „URL-Negativliste“ würde natürlich einer ständigen Datenpflege durch die Rechteinhaber bedürfen. Um Missbräuchen und fahrlässigen Antragstellungen vorzubeugen, böte sich eine Freistellung der mit RPS ausgerüsteten ISP an, etwa verbunden mit der aus dem Grenzbeschlagnahmeverfahren bekannten Sicherheitsleistung.

11. SDMI – Einheitlicher Schutzstandard ?

Secure Digital Music Initiative (SDMI)[39] ist ein Zusammenschluss von mehr als 180 Unternehmen und Organisationen aus den Bereichen

---

[36] http://www.mediaforce.com/about/technology.asp.
[37] http://www.ifpi.de/index.htm?jumpUrl=/recht/re22.html.
[38] http://www.ifpi.at bzw http://www.ifpi.de.
[39] http://www.sdmi.org.

Informationstechnologie, Sicherheitssysteme, ISP, Musikproduktion und Consumer Electronic.

Ziel ist, einen gemeinsamen offenen Technologiestandard zu entwickeln, der sich mit dem Schutz vor Piraterie bei der Sicherung der Urheberrechte beim Abspielen, Speichern und Handeln von digitalen Musikstücken befasst.[40] Das System setzt verschiedene Techniken wie Watermarking ein, um das Abspielen von Musikstücken nur auf SDMI-kompatiblen Geräten zu ermöglichen und die MP3-Piraterie zu verhindern. Mit ihrem Brief „An Open Letter to the Digital Community" werden Nutzer eingeladen, Technologien, die sie auf ihren Systemen einzusetzen gedenken, zu hacken. Ergebnisse sowie die eingesetzten Tools sollten an SDMI gesendet werden[41], um daraus Schlüsse auf die Schutztauglichkeit zu ziehen.

12. TCPA

Die Trusted Computing Platform Alliance[42], eine von Compaq, HP, IBM, Intel und Microsoft gegründete Initiative, hat sich zum Ziel gesetzt, zukünftige Rechnergenerationen mit einem speziellen Sicherheits-Chip auszustatten, um eine sichere Plattform zu schaffen. Zentraler Baustein dieses Hardware-gestützten Konzepts ist der sog „Fritz-Chip", verantwortlich für Benutzerauthentifizierung, Identifikation und Verschlüsselung. Das Konzept geht von der Annahme aus, dass der Rechner grundsätzlich eine unsichere Umgebung darstellt. Geschützte Inhalte lassen sich daher auf dem System erst dann wiedergeben, wenn der Chip die erfolgreiche Überprüfung der Umgebung ausgeführt hat. Diese Überprüfung beinhaltet den Test der Hardwarekomponenten, des BIOS, des Betriebssystems, der Treiber und Anwendungen. Wenn eine kritische Komponente kein gültiges Zertifikat vorweisen kann, verweigert der Chip den Zugriff auf geschützte Inhalte. Microsofts Schutzsystem Palladium[43] als Bestandteil der nächsten Windows-Version soll als Software-Schnittstelle für die von der Hardware vorbereitete sichere Umgebung eingesetzt werden. Unter Palladium werden sich DRM-geschützte Inhalte ohne ausdrückliche Erlaubnis des Rechteinhabers nicht mehr kopieren lassen, da das Betriebssystem schon den Versuch blockiert. Die Umgehung wird dadurch verhindert, dass nur ausdrücklich zugelassene Anwendungen auf die Inhalte zugreifen dürfen.

---

[40] Working Paper Digital Rights, 19.

[41] Working Paper Digital Rights, 19.

[42] http://www.trustedcomputing.org.

[43] Siehe http://www.jmd-software.de/html/tcpa.htm: Palladium arbeitet im Grunde genau wie der Fritzchip - nur wird hier sämtliche Software auf gültige Seriennummern überprüft. Programme oder Dokumente mit ungültigen Signaturen können dann entweder nicht gestartet werden oder werden gleich gelöscht. Palladium ist unter Windows also für die Überprüfung sämtlicher Daten zuständig und somit das Gewissen des PCs. Es bestimmt, was „*vertrauenswürdig*" ist und was nicht. So sollen zB Viren nicht an ihm vorbeikommen, da sie nicht verifiziert bzw nicht vertrauenswürdig sind. Ähnliches gilt auch für andere Programme, die für den PC gefährlich oder auch illegal sind.

Problematisch ist, dass das System techn vollkommen sicher gegen Angriffe sein müsste, es werden sich außerdem immer Hersteller finden, die Anwendungen ohne integrierte DRM-Mechanismen anbieten. Aus wirtschaftlicher Sicht stellt sich die Frage, warum sich jemand ein System kaufen sollte, dass ihn derart in seiner Freiheit einschränkt.

D. Probleme

Alle oben vorgestellten techn Maßnahmen bieten zwar einen großen Fortschritt im Hinblick auf die Reduzierung der Risiken des Raubkopierens, neue Geschäftsmodelle und Verbesserungen der Verwertungsbeteiligung der Berechtigten[44], haben aber mit den Schwierigkeiten der für professionelle Hacker leichten Umgehbarkeit der Sicherungen und auf Seiten der Nutzer der Ausspähung privater Daten zu kämpfen.[45] Aufgrund eines fehlenden einheitlichen Schutzstandards sowie der für den durchschnittlichen Nutzer abschreckend komplizierten und einschränkenden Handhabung haben diese Systeme (noch) keine breite Akzeptanz gefunden.

Solange keine interessengerechte Abwägung zwischen einem ausreichend vor Piraterie bewahrenden techn Schutz und einem solchen, der für den Verbraucher aufgrund von Benutzungshindernissen noch akzeptabel ist, gefunden wird, werden es DRM-Systeme nicht leicht haben und nur schwer zum Durchbruch gelangen. Weniger umfassende Werke wie Grafiken können per Screenshot abgespeichert und anschließend beliebig vervielfältigt werden, sodass der techn Schutz dort endet, wo die Bildschirmdarstellung zulässigerweise erfolgt. Ebenso stellt sich dieses Problem bei analog vorliegenden Musikwerken, die analog oder digital mitgeschnitten werden können.

---

[44] Working Paper Digital Rights, 4.

[45] Working Paper Digital Rights, 3 und 14. Beachte zum Datenschutz auch Art 9 Info-RL.

III. Geschichte der Info-RL

A. Die Urheberrechtsverträge der WIPO

Ausgangspunkt der in der Info-RL behandelten Themen sind der WIPO Copyright Treaty (im folgenden WCT) und der WIPO Performances und Phonograms Treaty (im folgenden WPPT). Beide bereits in Kraft stehenden Verträge wurden am 20. Dezember 1996 im Rahmen der Diplomatischen Konferenz beschlossen.[46] Der WCT bezieht sich dabei auf die Rechte der Urheber, der WPPT auf jene der ausübenden Künstler sowie die Tonaufzeichnungen der Darbietungen. In beiden Verträgen finden sich die Grundprinzipien der Inländerbehandlung, der Mindestrechte und des Formalitätenverbots.[47]

B. Europäische Rechtsgrundlagen

Rechtsgrundlage der Info-RL ist Art 249 EG-Vertrag 1997 (im folgenden EGV). Die RL stützt sich erklärtermaßen[48] insbes auf die Niederlassungsfreiheit (Art 55), die Dienstleistungsfreiheit (Art 47 Abs 2) und die Notwendigkeit zur Errichtung und des Funktionierens eines gemeinsamen Binnenmarktes (Art 95). Der Beschluss über die angestrebte Harmonisierung hat entsprechend dem Verfahren nach Art 251 EGV zu erfolgen.[49]

C. Grünbuch 1995

Konkrete Maßnahmen der Gesetzgebung im Zusammenhang mit der technologischen Entwicklung wurden zunächst im Grünbuch von 1988 zum Urheberrecht[50] vorgeschlagen. Dieses behandelte fünf Themen, bei denen primärer Handlungsbedarf gesehen wurde: Schutz von Computerprogrammen, Piraterie, Vermiet- und Verleihrechte, Rechtsschutz von Datenbanken und private Vervielfältigung. Bis auf letzteres wurden diese Gebiete durch die sog

---

[46] Weiterführend *König*, Die Informationsrichtlinie und ihre geplante Umsetzung in Österreich, 4f und FN 15.

[47] Siehe dazu auch *König*, Die Informationsrichtlinie und ihre geplante Umsetzung in Österreich, FN 24.

[48] Beachte 2. Vorerw zur RL 2001/29/EG.

[49] Zu den europäischen Grundlagen siehe genauer *König*, Die Informationsrichtlinie und ihre geplante Umsetzung in Österreich, 9ff.

[50] „*Grünbuch über Urheberrecht und die technologische Herausforderung. Urheberrechtsfragen, die sofortiges Handeln erfordern*“, KOM(1988) 172 endg vom 23. August 1988. Diesem folgend veröffentlichte die Kommission im Jänner 1991 die „*Initiativen zum Grünbuch. Arbeitsprogramm der Kommission auf dem Gebiet des Urheberrechts und der verwandten Schutzrechte*“ (KOM(1990) 584 endg vom 17. Jänner 1991).

Rechtsangleichungsinitiativen der ersten Generation geregelt.[51] Jener gesetzgeberische Rahmen im Bereich des Urheberrechts nennt sich „*acquis communautaire*“, der auch einen Ausgleich zwischen Rechten und Interessen der Beteiligten auf einem hohen Schutzniveau für geistiges Eigentum darstellt.[52]

Das Konzept „*Informationsgesellschaft*“ wurde erstmals im Dezember 1993 im Weißbuch der Kommission zum Thema „*Wachstum, Wettbewerbsfähigkeit, Beschäftigung – Herausforderungen der Gegenwart und Wege ins 21. Jahrhundert*“[53] verwendet. Dieses Weißbuch gilt als Wegweiser und Reflexionsgrundlage für die Gemeinschaft und die Mitgliedstaaten und bildet den Hintergrund für eine Reihe weiterer Grundsatzpapiere.[54]

Grundlage sowie Ausgangspunkt der Info-RL war das Grünbuch der Kommission „*Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft*“ (im folgenden Grünbuch)[55] vom 19. Juli 1995. Ausgehend von einem Konsultationsprozess wurde es der Kommission ermöglicht, mit diesem Grünbuch ein Arbeitsprogramm für den Bereich des Urheberrechts und der Leistungsschutzrechte festzulegen.[56]

In seinem IX. Abschnitt geht das Grünbuch näher auf techn Identifizierungs- und Schutzsysteme ein, wobei neben dem gewaltigen Risiko einer Digitalisierung geschützter Werke und Leistungen auch deren Chancen durch verbesserte Möglichkeiten einer Identifizierung von Werken und Leistungen sowie der betreffenden Rechtsinhaber erkannt werden. Ähnlich wie bei Büchern (International Standard of Book Numbering, im folgenden ISBN) oder bei Tonträgern (International Standard Recording Code, im folgenden ISRC) soll es möglich sein, für alle Werke und Leistungen eine solche Kennung einzuführen. Diese Identifizierungssysteme könnten auch die Erhebung und Verteilung der den Rechtsinhabern zustehenden Vergütung wirksam erleichtern. Auch außerhalb des gesetzgeberischen Rahmens hat die Kommission im Rahmen des ESPRIT-Programms Projekte wie CITED[57] durchgeführt, welche in Pilotprojekten wie COPYCAT[58] getestet wurden.

---

[51] Dazu zählen die SoftwareRL, die Vermiet- und VerleihRL, die Kabel- und SatellitenRL, die SchutzdauerRL und die DatenbankRL. Siehe auch *König*, Die Informationsrichtlinie und ihre geplante Umsetzung in Österreich, 37ff. Weiters dazu zählen lässt sich auch die Richtlinie 2001/84/EG des Rates vom 27. September 2001 zum Folgerecht des Urhebers des Originals eines Kunstwerkes (FolgerechtsRL).

[52] Siehe zum Konzept des „*acquis communautaire*“ auch *Reinbothe*, ÖBl 1998, 155 (156).

[53] ISBN 92 826 74 24-X-1994.

[54] Siehe dazu wiederum *König*, Die Informationsrichtlinie und ihre geplante Umsetzung in Österreich, 19.

[55] KOM (95) 382 endg vom 19. Juli 1995 - ABl C 97 vom 1. April 1996.

[56] Zu Inhalt und Aufbau sowie zu den für die Info-RL entscheidenden Kapiteln des Grünbuchs siehe *König*, Die Informationsrichtlinie und ihre geplante Umsetzung in Österreich, 20ff.

[57] Copyright in Transmitted Electronic Documents.

[58] Copyright Ownership Protection in Computer Assisted Training. Vgl auch die Projekte „Copearms” und „Occapi”. Dazu *Pohler*, Urheberrecht und Multimedia – ein unauflöslicher Konflikt ?, 51ff.

Ein weiteres Element besteht darin, in der Hardware Schutzsysteme zu installieren, mit denen oben genannte Kodierungen voll genutzt werden können. Von Bedeutung in diesem Bereich sind Systeme wie das SCMS[59]. Auch hier ist eine Harmonisierung erforderlich, denn *„die unkoordinierte Einführung von Maßnahmen der Mitgliedstaaten, mit denen die Vermarktung von bestimmten Schutznormen nicht entsprechenden „Waren" untersagt würde, würde der Schaffung technischer Handelshemmnisse gleichkommen und müsste eine Intervention der Gemeinschaft auslösen.*"[60]

Als drittes Element schließlich sollen auch Fragen zum Schutz der Privatsphäre des Benutzers geklärt werden. Jene stellen sich insofern, als die Netzbetreiber über jeden einzelnen Teilnehmer genaue Daten zur Nutzung von Information erheben und zusammenstellen könnten.

Am 20. November 1996 hat die Kommission der Europäischen Gemeinschaften eine Mitteilung namens *„Initiativen zum Grünbuch über Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft"*[61] beschlossen und versucht, die Schlussfolgerungen aus der insgesamt rund zweijährigen Konsultation nach dem Grünbuch zu ziehen.[62] Hier wurde ua das Thema des rechtlichen Schutzes der Integrität von techn Identifikations- und Schutzsystemen[63] als vorrangig eingestuft. Dabei sollten insbes die Merkmale der Schutzvorrichtung, die Art der verbotenen Handlungen und die angemessenen Sanktionen festgelegt werden.[64]

D. Vom Vorschlag zum Gemeinsamen Standpunkt

Der Info-RL-Vorschlag wurde von der Kommission am 10. Dezember 1997 angenommen und schließt einerseits unmittelbar an das Grünbuch an und deckt andrerseits die wesentlichen binnenmarktrelevanten Bestimmungen der WIPO-Verträge ab. Art 6 sieht hier einen angemessenen Rechtsschutz in Bezug auf technologische Maßnahmen[65] vor. Danach sollen alle Handlungen, die neben der Umgehung solcher techn Vorrichtungen nur einen begrenzt wirtschaftlich bedeutsamen Zweck oder Nutzen haben, durch Maßnahmen der Mitgliedstaaten im Bereich des Rechtsschutzes hintan gehalten werden. Dies soll aber nur gelten, wenn der handelnden Person den Umständen nach bekannt ist, dass diese Handlungen die unerlaubte Umgehung wirksamer techn Maßnahmen ermöglichen oder erleichtern. Diese Formulierung des Vorschlages muss als gänzlich missglückt betrachtet werden. Denn wenn der

---

[59] Serial Copyright Management System.

[60] *Gaster*, ZUM 1995, 740 [752].

[61] KOM (96) 568 endg.

[62] Die Kommission sammelte in dieser Zeit ca 350 Meinungsäußerungen aus interessierten Kreisen in Reaktion auf das Grünbuch. Daneben wurden bei einer Anhörung in Brüssel am 8. und 9. Jänner 1996 Fragen des Erwerbs und der Wahrnehmung von Rechten sowie der techn Identifizierungs- und Schutzsysteme diskutiert.

[63] Diese Systeme sollen zumindest eine der folgenden Funktionen erfüllen: Zugangskontrolle, Identifikation des Werks oder des Rechtsinhabers und Kopierschutz.

[64] KOM (96) 568 endg, 16f.

[65] Gemeint wohl: techn Maßnahmen.

Umgeher im Bewusstsein der Unerlaubtheit der Umgehungshandlung diese selbst verwirklicht, handelt er legal, da sich die Kenntnis auf die Unerlaubtheit der eigenen Handlungen, nicht aber auf das Ermöglichen oder Erleichtern einer Umgehungshandlung bezieht, wie sie Art 6 verlangt. Ist die handelnde Person lediglich ein Beitragstäter, so ist diese fremde Hilfeleistung illegal, während die eigene Umgehung dies nicht ist. Dieses groteske Ergebnis kann vom RL-Gesetzgeber nicht beabsichtigt gewesen sein.

Der Wirtschafts- und Sozialausschuss verabschiedete auf seiner 357. Plenartagung am 9. September 1998 eine Stellungnahme zum vorliegenden RL-Entwurf[66] und betonte dabei, dass das Verbot des Art 6 die Balance zwischen dem Wunsch der Rechteinhaber, jede Vorrichtung, die dazu dient, techn Hürden zu umgehen, oder eine solche Umgehung als Nebeneffekt gestattet, genau zu kontrollieren, und dem Recht des Verbrauchers, solche Vorrichtungen für rechtmäßige Zwecke zu nutzen, wahren soll und das Verbot auch auf solche Vorrichtungen erstrecken, bei denen „*Verkaufsförderung, Werbung und Vermarktung ausdrücklich auf eine solche Umgehung abgestellt sind*“.[67]

Das EP beschloss am 10. Februar 1999 insgesamt 56 Abänderungsvorschläge.[68] Es findet eine Aufteilung in die Umgehung techn Schutzvorrichtungen selbst (Abs 1) und in Vorbereitungshandlungen (Abs 2) statt, wobei für letztere zusätzliche Voraussetzungen in lit a-c geschaffen werden. Neu ist dabei, dass die Vorbereitungshandlungen Gegenstand einer Verkaufsförderung, einer Werbung oder einer Vermarktung mit dem Ziel der Umgehung des Schutzes sind oder hauptsächlich zur Umgehung des Schutzes entworfen, produziert, angepasst oder geliefert worden sind. Die bisher in Abs 2 enthaltenen Definitionen der techn Maßnahme und jener von deren Wirksamkeit befinden sich nunmehr im neuen Abs 2a (Abänderungsvorschläge Nr 49 bis 54). Außerdem begegnet das EP der oben geäußerten Kritik an der Formulierung „*obwohl der betreffenden Person bekannt ist oder den Umständen nach bekannt sein muss, dass diese Handlungen die unerlaubte Umgehung wirksamer technologischer Maßnahmen ermöglichen oder erleichtern*“ und sieht überhaupt kein subjektives Element mehr vor (Abänderungsvorschlag Nr 49). Der Rat hielt es im Abgeänderten Vorschlag vom 25. Juni 1999[69] für notwendig, wiederum ein subjektives Element hinzuzufügen. Mit der Wendung „*obwohl der betreffenden Person bekannt ist oder den Umständen nach bekannt sein muss, dass sie eine unerlaubte Handlung vornimmt.*“ wird aber nicht mehr der Fehler wie im ursprünglichen RL-Vorschlag gemacht, sodass nun sowohl unmittelbare wie auch Beitragstäterschaft erfasst sind. Außerdem wird hier in der dt Fassung erstmals richtig von techn statt technologischen Maßnahmen gesprochen.

Am 8. Juni 2000 konnte schließlich in der Rat-Arbeitsgruppe eine politische Einigung erzielt werden, die zum Text des Gemeinsamen

---

66 ABl C 407 vom 28. Dezember 1998, 30.
67 ABl C 407 vom 28. Dezember 1998, Pkt 3.8.2.
68 ABl C 150 vom 10. Februar 1999, 171.
69 KOM (1999) 250 endg; ABl C 180 vom 25. Juni 1999, 6.

Standpunktes, vom Rat genehmigt am 28. September 2000, geführt hat.[70] In Art 6 wird in Abs 1 die Formulierung *„…,dass sie eine unerlaubte Handlung vornimmt.“* durch *„…,dass sie dieses Ziel verfolgt.“* ersetzt, die Liste der Tätigkeiten in Abs 2 erschöpfend aufgezählt und das Verhältnis zwischen den Schranken in Art 5 und dem Schutz der techn Maßnahmen nunmehr so geregelt: die Definition der schutzfähigen techn Maßnahme (umfassender als im geänderten Kommissionsvorschlag oder in Abänderungsvorschlag Nr 54 des EP) macht deutlich, dass Art 6 vor Umgehung jeglicher techn Maßnahme schützen will, die dazu bestimmt ist, vom Rechtsinhaber nicht genehmigte Handlungen zu verhindern oder einzuschränken unabhängig davon, ob die Person, die für die Umgehung verantwortlich ist, ein Begünstigter einer der Ausnahmen iS des Art 5 ist.[71] Dafür sieht der Rat in Abs 4 Maßnahmen zum Schutz der legitimen Interessen der von Ausnahmen Begünstigten vor: danach sind die Mitgliedstaaten angehalten, sofern die Rechtsinhaber dies nicht freiwillig tun, geeignete Maßnahmen zu treffen, um sicherzustellen, dass die Rechtsinhaber den Begünstigten die Hilfsmittel zur Nutzung der betreffenden Ausnahmen oder Beschränkungen zur Verfügung stellen (Unterabsätze 1 und 2); vertragliche Vereinbarungen sollen aber vorgehen (Unterabsatz 4). Dazu wird der Rechtsschutz des Art 6 auf solche techn Maßnahmen ausgeweitet, mit denen sichergestellt werden soll, dass die Hilfsmittel zur Nutzung der Ausnahmen/Beschränkungen verfügbar sind (Unterabsatz 3).[72]

E. Erlass und Veröffentlichung

Der Gemeinsame Standpunkt wurde dem EP am 26. Oktober 2000 übermittelt, nachdem sich die Kommission diesem am 20. Oktober 2000 uneingeschränkt angeschlossen hat. Der Ausschuss für Recht und Binnenmarkt, in der Angelegenheit federführend, sah sich zufolge des bis dahin noch nie da gewesenen Lobbyings[73] mit 230 Änderungsanträgen zum Berichtsentwurf des Mitglieds des EP *Enrico Boselli* konfrontiert. In den Sitzungen vom 30. Jänner und 5. Februar 2001 wurde schließlich der endgültige Berichtsentwurf beschlossen. Dieser umfasste 15 Änderungsanträge zum Gemeinsamen Standpunkt des Rates. Dem Plenum in Straßburg lagen darüber hinaus noch weitere Abänderungsanträge vor. Nach einer ausführlichen Debatte nahm das EP schließlich die RL in zweiter Lesung am 14. Februar 2001[74] mit neun der fünfzehn vom Rechtsausschuss eingebrachten Änderungsanträge an, in einer Stellungnahme vom 29. März 2001 stimmte die Kommission allen Änderungen des EP zu.[75] Der Rat nahm die Änderungen des

---

[70] Gemeinsamer Standpunkt (EG) Nr 48/2000; ABl C 344 vom 1. Dezember 2000, 1-22.

[71] ABl C 344 vom 1. Dezember 2000, Begr Pkt 43.

[72] ABl C 344 vom 1. Dezember 2000, Begr Pkt 44.

[73] Von Seiten der Urheberverbände, der Geräteindustrie, der Verbraucherschutzverbände, der Fernsehanstalten und Internetanbieter, der Telefongesellschaften, der Museen und Bibliotheken sowie von Einzelfirmen.

[74] ABl C 276 vom 14. Februar 2001, 121.

[75] KOM (2001) 170 endg.

EP am 9. April 2001 an, die Unterzeichnung durch das EP und den Rat erfolgte am 22. Mai 2001. Am 22. Juni 2001 schließlich wurde die „*RICHTLINIE 2001/29/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft*“, die das Datum der Unterschrift durch die Präsidentin des EP trägt, im Amtsblatt der Europäischen Gemeinschaften L 167 auf den Seiten 10ff veröffentlicht.

Zur RL selbst fallen drei Punkte auf, wie schon *Haller*[76] festgestellt hat:

- Die erhebliche Verzögerung des Gesetzgebungsvorgangs der RL: Dabei hieß es schon in dem Begleitbrief zu den Initiativen 1996 der zuständigen Dienststelle der Kommission, dass die Kommission „*zu den … vier vorrangigen Themen voraussichtlich in der ersten Hälfte 1997 Gesetzgebungsvorschläge vorlegen*“ werde. Schon die Vorlage des ursprünglichen RL-Vorschlags hat sich um mehrere Monate verzögert. Dafür dürfte einerseits die durch den Abschluss der WIPO-Verträge notwendige Verlängerung des Ausarbeitungszeitraums des Vorschlags verantwortlich sein, andrerseits ist auch dem während des gesamten Konsultationsprozesses in stärkster Form auftretenden Lobbyismus Teilschuld für die Verzögerung zuzuschreiben.
- Was ursprünglich in separaten Gesetzen hätte geregelt werden sollen, ist nunmehr in einen einzigen Richtlinienvorschlag gepackt worden.
- Schließlich hat sich in der langen Entstehungsgeschichte der RL der Charakter des Projekts grundlegend geändert: Ging es ursprünglich um vier von der EG autonom zu regelnde Problemkreise (ausgehend vom Grünbuch 1995), stellt die RL jetzt zum größten Teil eine Umsetzung der WIPO-Verträge im Lichte des „*acquis communautaire*“ dar.

[76] In MR 1998, 61 und in Music on Demand, 78.

IV. Art 6 – Pflichten in Bezug auf technische Maßnahmen

A. Historischer Hintergrund

Erste Überlegungen zu den techn Entwicklungen wurden schon im „*Grünbuch über Urheberrecht und die technologische Herausforderung – Urheberrechtsfragen, die sofortiges Handeln erfordern*“[77] angestellt. Schon damals war das Ziel der EG-Kommission, das Eigentum als Ergebnis der Kreativität und umfangreicher Investitionen gegenüber unrechtmäßiger Übernahme durch andere zu schützen.[78] Neben rechtlichen Instrumentarien kommen eben auch techn Schutzmaßnahmen zur Erreichung dieses Ziels in Betracht. Letztere wurden von der Kommission im Grünbuch allerdings nur für audiovisuelle Werke (Tonaufnahmen, Video- oder Fernsehprogramme) problematisiert[79], insbes fehlt eine Auseinandersetzung mit dem Schutz von Computerprogrammen und Datenbanken.

Für Computerprogramme folgte die erste (nicht abschließende) Regelung bereits in Art 7 Abs 1 lit c SoftwareRL: Danach müssen die Mitgliedstaaten geeignete Maßnahmen gegen Personen vorsehen, die sich des Inverkehrbringens oder des Erwerbszwecken dienenden Besitzes von Mitteln schuldig machen, die allein dazu bestimmt sind, die unerlaubte Beseitigung oder Umgehung techn Programmschutzmechanismen zu erleichtern.[80] Diese Mittel können auch beschlagnahmt werden (Abs 3 leg cit). Nicht definiert wird allerdings, wann eine „*unerlaubte Beseitigung oder Umgehung*“ von Schutzmechanismen vorliegt. Angesprochen ist durch das Merkmal „*Inverkehrbringen und den Erwerbszwecken dienenden Besitz*“ nur der Kreis

---

[77] KOM (88), 172 endg vom 23. August 1988.

[78] KOM (88), 172 endg, 4.

[79] KOM (88), 172 endg, 118 f und 139 ff.

[80] Dieser Schutz wird durch die Info-RL nicht erweitert; vgl Erw 50: „*Ein solcher harmonisierter Rechtsschutz lässt die speziellen Schutzbestimmungen gemäß der Richtlinie 91/250/EWG unberührt. Er sollte insbesondere nicht auf den Schutz der in Verbindung mit Computerprogrammen verwendeten technischen Maßnahmen Anwendung finden, der ausschließlich in jener Richtlinie behandelt wird.*“ Darüber hinaus stellt Satz 3 des Erw 50 klar, dass techn Maßnahmen umgangen werden dürfen, um die Wahrnehmung der Schranken (Sicherungskopie, Dekompilierung) zu ermöglichen: „*Er sollte die Entwicklung oder Verwendung anderer Mittel zur Umgehung technischer Maßnahmen, die erforderlich sind, um Handlungen nach Artikel 5 Absatz 3 oder Artikel 6 der Richtlinie 91/250/EWG zu ermöglichen, nicht aufhalten oder verhindern. Artikel 5 und 6 jener Richtlinie sehen ausschließlich Ausnahmen von den auf Computerprogramme anwendbaren ausschließlichen Rechten vor.*“ „*Any means*“ in der engl und „*tout moyen*“ in der franz Fassung besagen, dass unter „*anderen Mitteln*“ in der dt Fassung jegliche Mittel zur Umgehung von techn Maßnahmen zu den genannten Zwecken erlaubt sein sollen. Hier geht der Schutz techn Maßnahmen in der Info-RL ganz beträchtlich über jenen in der SoftwareRL hinaus (dazu auch *Jaeger*, CR 2002, 309 (310 aE)).

der kommerziell arbeitenden Personen, privat ist der Besitz solcher Hilfsmittel und die Umgehung bzw Beseitigung der Schutzmechanismen nicht verboten.

Vgl weiters die Regelungen im Grünbuch 1995 (oben Kap III.C).

B. Definitionen (Abs. 3)

1. Technische Maßnahme

Art 6 Abs 3 Info-RL enthält Legaldefinitionen. Unter „*technischer Maßnahme*" werden alle 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 Urheberrechte verwandten gesetzlich geschützten Schutzrechte oder des Sui-generis-Rechtes für Datenbanken ist, verstanden. Erfasst sind also Software-Kopierschutzmechanismen sowie Dongles, Zugangskontrollen bei Datenbanken (etwa Registrierungen bei Bild- oder Tonsammlungen), verschlüsselte Fernsehprogramme der Pay-TV-Anbieter sowie sämtliche zugangskontrollierte Dienste gegenüber der unbefugten Verwertung eines geschützten Werkes oder sonstigen Schutzgegenstands. Die Bandbreite des Art 6 ist dementsprechend groß.

2. Wirksamkeit

Der Rechtsschutz gegen solche Maßnahmen greift jedoch nur ein, wenn diese wirksam sind. „*Wirksam*" ist eine solche techn Maßnahme dann, soweit die Nutzung eines geschützten Werkes oder eines sonstigen Schutzgegenstandes von den Rechtsinhabern durch eine Zugangskontrolle oder einen Schutzmechanismus wie Verschlüsselung, Verzerrung oder sonstige Umwandlung des Werkes oder sonstigen Schutzgegenstandes oder einen Mechanismus zur Kontrolle der Vervielfältigung (Kopierschutz), die die Erreichung des Schutzzieles sicherstellen, unter Kontrolle gehalten wird. Es muss sich daher um tatsächlich greifende Sperren handeln und nicht bloß um leicht auszuschaltende Vorrichtungen, die einfach auf ein Verbot des Rechtsinhabers hinausliefen.[81] Für die Wirksamkeit der Maßnahme trägt dabei der Rechteinhaber die Beweislast.[82] In diesem Zusammenhang stellt Erw 48 auch klar, dass techn Schutzvorrichtungen den normalen Betrieb elektronischer Geräte und deren Entwicklung nicht behindern dürfen und dass aus dem Rechtsschutz keine Verpflichtung der Gerätehersteller oder Dienstleistungsanbieter abgeleitet werden darf, ihre Geräte oder Dienstleistungen so zu konzipieren, dass sie den techn Maßnahmen entsprechen. Diese Klarstellung stammt auch aus der US-amerikanischen

[81] *Walter* in Europäisches Urheberrecht, Info-RL, Rz 155.
[82] Vgl *Fallenböck/Haberler*, ecolex 2002, 262 (263).

Gesetzgebung, wo sie üblicherweise mit den Begriffen „*playability clause*“ und „*no-mandate clause*“ umschrieben werden.[83]

3. Probleme in der Formulierung

Übersehen wird dabei, dass die gewählte Formulierung die Regelung ad absurdum führt: Der Schutz soll nach Abs 1 nur gegen die Umgehung „*wirksamer technischer Maßnahmen*“ greifen. „*Wirksam*“ ist eine techn Maßnahme nach Abs 3 allerdings nur, wenn „*die Nutzung ... unter Kontrolle gehalten wird*“ (beachte auch den engl Text: „*achieves the protection objective*“). Wenn aber ein Sicherungsmechanismus umgangen werden kann, erfüllt er seinen Zweck der Kontrollhaltung nicht mehr und ist somit nicht mehr wirksam, sodass der Schutz nicht greift. Nach *Hoeren* wäre zwischen einer ex-ante- und einer ex-post-Betrachtung zu unterscheiden. Es ist nämlich nicht auszuschließen, dass ein Schutzsystem ex-ante wirksam war, wenn es ex-post gehackt worden ist. Ein Schutzmechanismus wäre wohl schon dann „*wirksam*“, wenn er den Durchschnittsbenutzer davon abhält, unerwünschte Nutzungsvorgänge vorzunehmen.[84]

Weiters wird durch die gewählte Formulierung „*soweit die Nutzung eines geschützten Werkes … von den Rechtsinhabern durch eine Zugangskontrolle … unter Kontrolle gehalten wird*“ ermöglicht, dass der Urheber nicht nur die Nutzung seines Werkes, sondern auch den Zugang zu diesem kontrollieren kann. Denn wer den Zugang zur Nutzung kontrolliert, verfügt über ein Kontrollsystem zur Überwachung des Systems als solches. *Linnenborn* stellt daher zutreffend fest, dass ein Werk durch das Urheberrecht und techn Maßnahmen geschützt wird, wobei letztere selbst durch das Gesetz geschützt werden und „*damit quasi unter Hinzuziehung des Umgehungsverbots ein Zugangskontrollrecht geschaffen*“ wird.[85] Dies war wohl vom EU-Gesetzgeber nicht beabsichtigt[86], es wäre besser gewesen, die Zugangskontrolle gänzlich auszunehmen.[87]

---

[83] Vgl Title 17 U.S.C. Sec 1201 (c) (3) DMCA.

[84] *Hoeren*, MMR 2000, 515 (520). Vgl auch *Fallenböck/Haberler*, ecolex 2002, 262 (263).

[85] *Linnenborn*, K&R 2001, 394 (398).

[86] Siehe die Begründung des Rates zum gemeinsamen Standpunkt, der ausdrücklich den Zugang zu Werken als eigenständigen Kontrollmechanismus streichen wollte; Gemeinsamer Standpunkt (EG) Nr 48/2000; ABl C 344 vom 1. Dezember 2000, 1-22.

[87] Diese wird außerdem in der ZugangskontrollRL geregelt, siehe VII.A.

C. Rechtsschutz gegen Umgehung (Abs 1)

Art 6 behandelt nun die Pflichten in Bezug auf techn Maßnahmen horizontal für alle Werke und Schutzgegenstände mit Ausnahme von Software. Dabei legt Abs 1 fest, dass es Aufgabe der Mitgliedstaaten ist, einen angemessenen Rechtsschutz gegen die Umgehung wirksamer techn Maßnahmen durch eine Person, der bekannt ist oder den Umständen nach bekannt sein muss[88], dass sie dieses Ziel verfolgt, vorzusehen. Art 6 richtet sich also an die Mitgliedstaaten, die Art der Sanktionen (verwaltungsrechtlich, zivilrechtlich oder strafrechtlich) zu bestimmen. Unmittelbar entstehen hierdurch keine konkreten Rechte und Pflichten der Rechtsunterworfenen. Sollte ein Mitgliedstaat aber die RL in diesem Pkt nicht ordnungsgemäß umsetzen, können Schadenersatzansprüche Einzelner gegenüber dem Staat entstehen. Schutzgut des Art 6 Abs 1 ist die Integrität der techn Schutzmaßnahmen.[89]

Die Bestimmung lehnt sich an den Wortlaut der entsprechenden Regelungen im WCT und WPPT[90] an. Demnach muss der Rechtsschutz zwei Erfordernissen entsprechen: er soll angemessen sein, also weder die Interessen der Hersteller noch der Benützer noch der Allgemeinheit über Gebühr berücksichtigen und es sollen solche Handlungen nicht betroffen sein, die der Urheber gestattet hat oder die gesetzlich erlaubt sind.

Zunächst stellt sich die Frage (im WCT und WPPT wie auch in der Info-RL), welcher Rechtsschutz im konkreten Fall angemessen ist. Eine Lösung kann nur in der RSpr gefunden werden. Wegen dieses auslegungsbedürftigen Begriffs der Angemessenheit ist keine wirkliche Harmonisierung europäischen Rechts zu erwarten, obwohl dies ja gerade angestrebt wird.

Abs 1 ist lediglich gegen die Umgehung techn Maßnahmen selbst gerichtet, der sogleich zu behandelnde Abs 2 erfasst die Vorbereitungshandlungen, die die Umgehung dieser Schutzmaßnahmen erleichtern oder erst ermöglichen. Dies ist ein wesentliches Element, da die eigentliche Gefahr für die Rechte des geistigen Eigentums nicht die einzelnen Umgehungshandlungen durch Privatpersonen, sondern die vorbereitenden

---

[88] Damit nimmt die RL einen Fahrlässigkeitstatbestand auf, um vorab etwaigen Beweisschwierigkeiten vorzubeugen, wobei die Formulierung, wie *Spindler* in GRUR 2002, 105 (116), betont, eher auf grobe denn leichte Fahrlässigkeit schließen lässt.

[89] *Flechsig*, ZUM 2002, 1 (14).

[90] Art 11 WCT und Art 18 WPPT. Dabei bestand unter den Konferenzteilnehmern weitgehend Einigkeit, dass ein entsprechender Rechtsschutz notwendig ist, „*man stritt allerdings über die Eigenschaften der zu erfassenden Systeme, der maßgeblichen Zweckbestimmung eines zur Schutzumgehung geeigneten Mechanismus, das zu sanktionierende Tun des „infringers", die vorzusehenden Rechtsbehelfe sowie das erforderliche Ausmaß an Kenntnis des Rechtsbrechers. Hinsichtlich der Zweckbestimmung der „device" reichte die Palette der Vorschläge von „Mechanismen, deren Hauptzweck oder -effekt in der Umgehung liegt" bis zu solchen, die nur auf den „einzig verfolgten Zweck der Umgehung" abstellen wollten.*" (aus *v.Lewinski/Gaster*, ZUM 1997, 607 (619)).

Handlungen darstellen werden, die von Handelsunternehmen vorgenommen werden, die Vorrichtungen zur Umgehung herstellen, zum Verkauf anbieten, vermieten oder in der Öffentlichkeit bewerben könnten.[91] Die RL richtet sich damit nicht gegen den „*kleinen Umgeher*", sondern va gegen den (gewerblichen) Piraten und die Hacking-Industrie.[92] Der Ausdruck „*obwohl bekannt ist oder den Umständen nach bekannt sein muss*" wird auch schon in den Bestimmungen über die Durchsetzung in der WTO/TRIP's-Vereinbarung verwendet (vgl Art 45 über Schadenersatz). Damit wird ein subjektives Element eingeführt, welches jene Handlungen vom Schutz ausnimmt, die ohne das Bewusstsein vorgenommen werden, dass sie die Umgehung techn Schutzvorrichtungen bedeuten. Die umgehende Person muss also schuldhaft handeln, wobei Fahrlässigkeit ausreicht. Es sollte hervorgehoben werden, dass ein solcher Rechtsschutz die Initiative ergänzt, die von der Kommission im Bereich des rechtlichen Schutzes von Diensten, die einer Zugangskontrolle unterliegen[93], vorgeschlagen worden ist. Diese betrifft den harmonisierten Schutz vor dem unbefugten Empfang von zugangskontrollierten Diensten, die geistiges Eigentum enthalten können oder auf geistigem Eigentum beruhen, während sich die Info-RL auf die unbefugte Verwertung eines geschützten Werks oder sonstigen Schutzgegenstands, wie die unbefugte Vervielfältigung, Zugänglichmachung oder Sendung bezieht.[94]

Der Rechtsschutz des Abs 1 gilt für techn Maßnahmen, die wirksam Handlungen beschränken, die von den Inhabern von Urheberrechten oder verwandten Schutzrechten oder des Sui-generis-Rechts an Datenbanken[95] nicht genehmigt worden sind.[96] Zu beachten ist weiters, dass der Rechtsschutz nicht dazu verpflichtet, Vorrichtungen, Komponenten, Produkte oder Dienstleistungen zu entwerfen, die den techn Maßnahmen entsprechen, solange jene nicht in anderer Weise unter das Verbot des Art 6 fallen.

Der Rechtsschutz techn Maßnahmen lässt einzelstaatliche Rechtsvorschriften, die den privaten Besitz von Vorrichtungen, Erzeugnissen oder Bestandteilen zur Umgehung techn Maßnahmen untersagen, unberührt.[97]

---

[91] KOM(1997) 628 endg, Erl 1 zu Art 6.

[92] Vgl *Haller*, MR 1998, 61 (62); ebenso *Mogel*, ecolex 2001, 241 (244) und in Europäisches Urheberrecht, 291.

[93] Vgl den Vorschlag der Kommission für eine Richtlinie des Europäischen Parlaments und des Rates zum Rechtsschutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten, KOM(97) 356 endg vom 9. Juli 1997. Die ZugangskontrollRL wurde am 20. November 1998 erlassen.

[94] KOM(1997) 628 endg Erl 4 zu Art 6. Siehe dazu näher Kap VII.

[95] Vorgesehen in Kap III der DatenbankRL: Datenbanken als Unterfall der Sammelwerke genießen dann urheberrechtlichen Schutz, wenn sie die für diesen Schutz erforderliche Werkhöhe (Originalität) erreichen. Daneben sieht die DatenbankRL einen Sonderschutz gegen wesentliche Entnahmen aus Datenbanken, die die geforderte Werkhöhe nicht erreichen, vor, wenn für die Beschaffung, Überprüfung oder Darstellung ihres Inhalts eine nach Art oder Umfang wesentliche Investition erforderlich war. Da dies eine dem bisherigen System des UrhG fremde Schutzart darstellt, spricht man in diesem Zusammenhang vom Sui-generis-Schutz von Datenbanken.

[96] RL 2001/29/EG Erw 48.

[97] RL 2001/29/EG Erw 49.

Weiters ist zu beachten, dass der Rechtsschutz in Abs 1 nicht mit dem Rechtsschutz der in Verbindung mit Computerprogrammen verwendeten techn Maßnahmen, der ausschließlich in der SoftwareRL[98] behandelt wird, verwechselt werden darf.[99]

Inhaltlich folgt die RL mit Abs 1 den Vorgaben des amerikanischen Rechts in Form der durch den DMCA[100] neu formulierten Sec 1201 des Copyright Act[101]: Demnach darf niemand wirksame techn Maßnahmen umgehen, wobei aber ein großer Katalog von Ausnahmen vorliegt. Von Bedeutung ist insbes das das ganze amerikanische Recht durchziehende Fair-Use-Prinzip. Demnach darf der Urheber seine Ausschließlichkeitsrechte nicht unfair ausüben. Dieser Grundsatz ist im Kern von Billigkeitserwägungen getragen, weshalb die Prüfung nicht bei den ausdrücklich im Gesetz aufgezählten Merkmalen stehen bleiben darf, sondern gegebenenfalls weitere Aspekte in die Betrachtung mit einbezogen werden müssen. Das österr Recht kennt diesen Fair-Use-Grundsatz nicht.

Voraussetzung für den Schutz des Urheberrechts vor Umgehung techn Maßnahmen durch Herstellung und Vertrieb hierfür geeigneter Geräte ist, dass diese Geräte primär zur Umgehung hergestellt werden oder neben der

---

98 RL 91/250/EWG in Art 7 Abs 1 lit c.

99 RL 2001/29/EG Erw 50.

100 Dieser wurde am 28. Oktober 1998 vom amerikanischen Präsidenten unterzeichnet und passt das US-Copyright Law an die digitale Informationsgesellschaft an. Er ist deshalb auch für das europäische Urheberrecht so wichtig, da das Medium Internet *„einen globalen Grundkonsens zumindest über die wichtigsten durch dieses Phänomen neu aufgeworfenen Rechtsfragen erfordert“* (*Freytag*, MMR 1999, 207 (207)). Er besteht aus fünf Teilen, wobei Titel I (*„WIPO Copyright Performances and Phonograms Treaties Implementation Act of 1998*“) den WCT und den WPPT umsetzt, Titel II (*„Online Copyright Infringement Liability Limitation Act*“) die Mitverantwortlichkeit der Diensteanbieter für Urheberrechtsverletzungen der Nutzer regelt (vgl Art 13 bis 15 E-CommerceRL), Titel III (*„Computer Maintenance Competition Assurance Act*“) eine Schrankenregelung für die Software-Vervielfältigung bei der Computerreparatur und -wartung einführt, Titel IV (*„Miscellaneous Provisions*“) einen Katalog von Schrankenregelungen (ua zugunsten von Bibliotheken, ephemere Aufnahmen von Rundfunkveranstaltern, Fernausbildung, Webcasting usw) enthält und Titel V (*„Vessel Hull Design Protection Act*“) ein neues Designschutzrecht für Schiffsrümpfe schafft. Vgl dazu auch „THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998, U.S. Copyright Office Summary“, http://www.loc.gov/copyright/legislation/dmca.pdf und *Freytag*, Digital Millennium Copyright Act und europäisches Urheberrecht für die Informationsgesellschaft, MMR 1999, 207.

Der erste Titel des DMCA erstreckt den Schutz des US-Rechts auf alle nach den WIPO-Verträgen zu schützenden ausländischen Werke und andere Schutzgegenstände oder stellt den bereits erloschenen Schutz wieder her. Die USA ging allerdings davon aus, dass bezüglich der Online-Zugänglichmachung keine Gesetzesänderung erforderlich ist.

101 Genau: 17 U.S.C. § 1201 (a) (1) (A)

Title 17 United States Code; Chapter 12 – Copyright Protection and Management Systems; § 1201. Circumvention of Copyright Protection Systems *“(a) Violations regarding Circumvention of Technological Measures – (1) (A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title.*”

Umgehung nur einen beschränkt bedeutsamen wirtschaftlichen Zweck oder Nutzen haben oder gerade zum Zweck der Umgehung angeboten werden.

Problematisch ist va der Nachweis des Herstellungszweckes. Es ist nahezu unmöglich, einem Programmierer nachzuweisen, dass er ein Programm zur Umgehung techn Schutzmöglichkeiten und nicht für die legitime Systemwartung entwickelt hat. Ebenso wird es sich mit Passwort-Entschlüsselungs-Programmen verhalten, die auch eingesetzt werden können, wenn der Berechtigte sein eigenes Kennwort vergessen hat.[102] Mit dieser Regelung wollte die EU-Kommission das Verhältnismäßigkeitsprinzip wahren[103], in der Praxis kann sich die Umsetzung allerdings als schwierig erweisen. So könnte man auf das bei Computerprogrammen bewährte Prinzip[104] zurückgreifen und sowohl auf die Geeignetheit zur Umgehung[105] als auch auf den Hauptzweck des Mittels nach der allgemeinen Lebenserfahrung[106] abstellen.

Grundsätzlich unterscheidet man zwei Kategorien von Umgehungsmaßnahmen: Einerseits solche, die den unerlaubten Zugang zum Werk verhindern, und andrerseits Maßnahmen, die die unerlaubte Verwertungshandlung selbst verhindern. Was die Herstellung bzw den Vertrieb von Geräten betrifft, ist die Umgehung beider Arten von Schutzvorrichtungen verboten. Die Ausführung der Umgehungshandlung selbst (sei es auch mit Hilfe solcher Geräte) ist dagegen nur bei der Umgehung des Schutzes gegen unberechtigten Zugang eine eigenständige Rechtsverletzung. Denn während es bis dahin urheberrechtlich keine Verletzungshandlung war, wenn man sich gegen den Willen des Urhebers Zugang zum Werk verschafft, waren Verwertungshandlungen, gegen die die zweite Kategorie von Schutzvorrichtungen schützen soll, schon bisher verboten, sodass es in diesem Bereich keines urheberrechtlichen Schutzes bedarf. Solche Verwertungshandlungen waren in bestimmten Fällen sogar vom Ausschließlichkeitsrecht des Urhebers ausgenommen (vgl das Prinzip des fair use). Weiters enthält Sec 1201 Copyright Act eine Reihe von Schrankenbestimmungen für diese neuen Verbote, die im Rahmen dieser Arbeit nicht behandelt werden können.

---

[102] Vgl bspw das Programm Advanced Password Recovery (http://www.elcomsoft.com/apdfpr.html) zur Entschlüsselung passwortgeschützter PDF-Dateien.

[103] *Wand*, Technische Schutzmaßnahmen und Urheberrecht, 112.

[104] *Fromm/Nordemann*, Urheberrecht, § 69f, Rn 3.

[105] *Spindler*, GRUR 2002, 105 (116).

[106] *Raubenheimer*, CR 1994, 129 (132).

D. Rechtsschutz gegen Vorbereitungshandlungen (Abs 2)

Abs 2 verpflichtet die Mitgliedstaaten, einen angemessenen Rechtsschutz gegen die Herstellung, die Einfuhr, die Verbreitung, den Verkauf, die Vermietung, die Werbung im Hinblick auf Verkauf oder Vermietung und den Besitz zu kommerziellen Zwecken von Vorrichtungen, Erzeugnissen oder Bestandteilen sowie die Erbringung von Dienstleistungen vorzusehen.[107] Dieser Schutz besteht allerdings nur gegen solche Vorrichtungen, Erzeugnisse oder Bestandteile, die entweder Gegenstand einer Verkaufsförderung, Werbung oder Vermarktung mit dem Ziel (!) der Umgehung wirksamer techn Maßnahmen sind *oder* die abgesehen von der Umgehung wirksamer techn Maßnahmen nur einen begrenzten wirtschaftlichen Zweck oder Nutzen haben[108] *oder* die hauptsächlich entworfen, hergestellt, angepasst oder erbracht werden, um die Umgehung wirksamer techn Maßnahmen zu ermöglichen oder zu erleichtern. Dabei wird nur die unerlaubte Umgehung inkriminiert, aus dem Zweck der Regelung folgt, dass schon eine gesetzliche Lizenz genügt, damit eine Umgehung legal ist.[109] Aus Erw 49 ergibt sich, dass sich der Schutz der RL in diesem Pkt nicht auf kommerzielle Zwecke beschränkt; dies gilt lediglich für den Besitz von Gegenständen, die der Umgehung dienen können. Es blieb also den Mitgliedstaaten überlassen, den privaten Besitz von Anti-Kopier-Einrichtungen zu untersagen.

Mit der Formulierung „*begrenzten wirtschaftlichen Zweck oder Nutzen*" wird der Schutz außerordentlich weit gezogen, da es nicht mehr wie in Abs 1 auf Vorsatz oder grobe Fahrlässigkeit, sondern nur auf die Geeignetheit des Produkts oder der Leistung bei wirtschaftlich geringem Wert ankommt.[110] Bei der Umsetzung hätten daher im Wesentlichen bei fehlender Zwecksetzung des Produkts zur Umgehung nur Unterlassungs- bzw Vernichtungsansprüche in Betracht kommen können, um den Schutz angesichts der Multifunktionalität verschiedenster Produkte nicht ausufern zu lassen.[111]

Obwohl Erw 48 betont, dass techn Maßnahmen nicht dazu führen dürfen, den „*normalen Betrieb*" elektronischer Geräte und ihre techn Entwicklung zu behindern sowie „*Vorrichtungen oder Handlungen (…) untersagt werden, deren wirtschaftlicher Zweck und Nutzen nicht in der Umgehung technischer Schutzvorkehrungen besteht*", ergeben sich in der Praxis Abgrenzungsprobleme zwischen noch erlaubten Geräten oder Software, die

---

[107] In diesem Pkt folgt die Info-RL damit dem Vorbild des DMCA (17 U.S.C. Sec 1201 (a) (2) (A) – (C)) und geht deutlich über die Vorgaben des WCT hinaus. Die Aufzählung ist taxativ.

[108] Damit wird sichergestellt, dass gesetzlich nicht verbotene elektronische Geräte (in der Literatur werden immer wieder Feuermelder als Bsp erwähnt; vgl zB *Walter* in Europäisches Urheberrecht, Info-RL, Rz 154) nicht nur deshalb den Sanktionen unterfallen, weil sie auch, aber nicht vornehmlich zur Überwindung von techn Schutzsystemen genutzt werden können. Ein begrenzter Nebennutzen solcher Programme reicht allerdings für deren Legalisierung nicht mehr aus.

[109] *Haller*, MR 1998, 61 (65).

[110] *Marly*, K&R 1999, 106 (110). AA *Hoeren*, MMR 2000, 515 (520).

[111] *Spindler*, GRUR 2002, 105 (116).

das Umgehen von Kopierschutzmechanismen mittelbar erleichtern soll, und solchen, die primär dazu dienen, zu prognostizieren.[112] Jede Brennersoftware für CDs, die bspw als Kopierschutz eingesetzte Lesefehler auf CDs korrigieren kann, könnte demnach bereits als Umgehungsmechanismus qualifiziert werden, auch wenn sie nur auftretende Fehler beim Auslesen von Daten beheben soll. Andrerseits kann dieser Vorfeldschutz nicht effektiv genug sein, da er sich nur auf Produkte und Dienstleistungen, nicht aber auf reine Information von Privaten, die eine Anleitung zur Umgehung darstellt, bezieht. Derjenige, der die Information zur Verfügung stellt, fällt wohl unter Abs 1, jene, die sie verbreiten, allerdings nicht unter Abs 2. Wird daher zB auf einer Website auf eine anderweitig erhältliche Information zur Entfernung eines Kopierschutzes hingewiesen, liefe Art 6 Abs 2 ins Leere.

Zu beachten ist weiters, dass die RL einen Umgehungsschutz nur in Bezug auf urheberrechtlich geschützte Werke oder Leistungen vorsieht, nicht aber in Bezug auf gemeinfreie Werke oder sonst urheberrechtlich nicht geschütztes Material, da letzteres von der RL gar nicht erfasst ist. Es besteht daher auch keine Notwendigkeit, den Rechtsschutz auch auf diese Fälle auszudehnen. Während dies praktisch Auswirkungen auf Umgehungshandlungen nach Art 6 Abs 1 Info-RL hat, wird sich hinsichtlich der Vorrichtungen nach Art 6 Abs 2 Info-RL kaum etwas ändern, da die einmal einem urheberrechtlich geschützten Werk vom Rechtsinhaber beigegebene techn Schutzmaßnahme erhalten bleibt, auch wenn der urheberrechtliche Schutz abgelaufen ist. Das bedeutet aber auch, dass ein Mechanismus, der geeignet ist, den Schutz eines gemeinfrei gewordenen Werkes zu überwinden, häufig auch zur Umgehung wirksamer Maßnahmen zum Schutz geschützter Werke und Leistungen dient und untersagt werden kann, da in der Praxis (noch) nicht zwischen einem Zugriff auf gemeinfreies und geschütztes Material unterschieden werden kann, und schon gar nicht, ob von einem geschützten Werk auf eine durch die Schrankenbestimmungen gedeckte oder aber auf eine dem Urheber vorbehaltene Art und Weise Gebrauch gemacht werden soll. Damit hat der RL-Gesetzgeber die Mitgliedstaaten vor die Wahl gestellt, entweder einen zu weitgehenden Schutz vorzusehen, oder aber eine Durchbrechung von Schutzmechanismen zuzulassen, die in der Praxis nicht nur legitime Interessen verfolgt, sondern regelmäßig auch zu illegitimen Zwecken missbraucht werden kann.

[112] Dazu *Hoeren*, MMR 2000, 515 (520).

V. Art 6 Abs 4

1. Grundsätzliche Regelung

Mit Art 6 wird Urhebern und Leistungsschutzberechtigten eine rechtliche Handhabe gegen Personen, die techn Schutzmechanismen umgehen, gewährt. Dies könnte sich für die dort Begünstigten dann als problematisch erweisen, wenn damit auch die Schrankenbestimmungen des Art 5 obsolet werden, weil diese Schutzmechanismen auch in den Ausnahmefällen keinen Zugang erlauben und dieser nur unter unzulässiger Umgehung erlangt werden könnte. Die unbeschränkte Anwendung der Schutzmaßnahmen könnte nämlich dazu führen, dass sie den Gebrauch der freien Werknutzungen wie etwa das Recht der privaten Kopie praktisch verdrängen würden, wenn auch solche freien Nutzungen unter den Kopierschutz fallen.[113] Wenn die techn Schutzeinrichtungen auch den gesetzlich zulässigen Gebrauch ausschließen, entwickelt sich der „Code as Code".[114] Ein eigenes verabsolutiertes techn Urheberrechtsgesetz entstünde, von dem die demokratisch legitimierte Legislative ausgeschlossen wäre.[115]

Bis zum Gemeinsamen Standpunkt war dieses Problem auf jene Weise gelöst, dass Art 6 Abs 1 iVm Abs 3 die Umgehung von techn Schutzmaßnahmen durch *rechtsverletzende* Handlungen inkriminiert.[116] Dabei sah Art 5 Abs 2 lit ba Abgeänderter RL-Vorschlag die gesetzliche Lizenz zur privaten Vervielfältigung auf digitalen Trägern vor und betonte der damalige Erw 27, dass Ausnahmen betreffend Privatkopien weder den Einsatz techn Maßnahmen noch deren Durchsetzung im Falle einer unerlaubten Umgehung dieser Maßnahmen behindern sollten.[117]

Die RL stellt jetzt folgende Regelung auf, die die Interessen aller Beteiligten berücksichtigen soll und das Verhältnis des Schutzes vor Umgehung von wirksamen techn Maßnahmen in Art 6 zu den Ausnahmen in

---

[113] *Wittmann*, MR 2001, 144 (146).

[114] *Kröger*, CR 2001, 316 (321).

[115] *Spindler*, GRUR 2002, 105 (115); *Hoeren*, MMR 2000, 515 (520).

[116] Art 6 Abs 3 Abgeänderter RL-Vorschlag definiert die „*technische Maßnahme*" als „*alle Technologien, Vorrichtungen oder Komponenten, die bei normalem Funktionieren dazu bestimmt sind, einer Verletzung der Urheberrechte oder verwandten Schutzrechte, die gesetzlich oder nach dem in Kapitel III der Richtlinie 96/9/EG verankerten Recht sui generis vorgesehen sind, vorzubeugen oder eine solche Verletzung zu verhindern.*"

[117] Für einen Vorrang von Art 6 sprach auch, dass die Kommission Abänderungsvorschlag 47 des EP, der eine klarstellende Regelung beinhaltete, aus unerfindlichen Gründen nicht übernommen hat. Dem Art 5 Abs 4 wäre folgender 2. Satz angefügt worden: „*Diese Ausnahmen und Schranken dürfen den Einsatz technischer Mittel zum Schutz der Werke im Hinblick auf die Wahrung der Interessen der Rechtsinhaber nicht behindern und den Schutz dieser Maßnahmen gemäß Artikel 6 nicht beeinträchtigen.*"

Art 5 klarstellen soll. Prinzipiell wird über die Definition der techn Maßnahme in Abs 3 den Rechtsinhabern die vollständige Kontrolle überlassen („*…Handlungen zu verhindern oder einzuschränken, die nicht von der Person genehmigt worden sind, die Inhaber der Urheberrechte…ist.*"), die RL setzt hierbei auf freiwillige Maßnahmen der Rechtsinhaber (aufgrund von Eigeninitiative oder gegenseitigen Vereinbarungen, wobei die Mitgliedstaaten fördernd eingreifen sollen[118]). Dies wurde im Hinblick auf die unterschiedlichen Verhandlungspositionen der Rechtsinhaber und der Nutzer vielfach kritisiert. Da auch die DatenbankRL (in Art 8 Abs 1) und die SoftwareRL (in Art 7 Abs 1 lit c) hinsichtlich des bestimmungsgemäßen Gebrauchs jew zwingende Regelungen vorsehen, wäre auch für die Info-RL wünschenswert gewesen, klare Ziele vorzugeben, welcher Zugang dem Nutzer trotz techn Schutzmaßnahmen in jedem Fall gewährt werden muss.

Mit der gegenüber dem RL-Vorschlag ausgeweiteten Regelung, den rechtlichen Schutz vor Umgehung schon dann eingreifen zu lassen, wenn die techn Maßnahme eine Handlung einschränkt, die vom Rechteinhaber *nicht genehmigt* wurde, ist es dem reinen Wortlaut nach für den Rechteinhaber möglich, jede Nutzungshandlung wirksam und rechtlich zulässig techn zu unterbinden. So ist es ihm im digitalen Kontext, wo eine Nutzungshandlung immer auch zumindest eine Vervielfältigung mit sich bringt, erlaubt, techn Schutzmaßnahmen auch dort zu ergreifen, wo er eine Nutzung nicht untersagen dürfte. Damit können auch Inhalte der Allgemeinheit entzogen werden, die gar keinen urheberrechtlichen Schutz genießen oder deren Schutz durch Zeitablauf erloschen ist.[119]

Nur wenn es nicht zu freiwilligen Maßnahmen der Rechtsinhaber kommt, regelt Abs 4, dass es Aufgabe des nationalen Gesetzgebers ist, sicherzustellen, dass die Rechtsinhaber den Begünstigten Mittel zur Nutzung der betreffenden Ausnahme/Beschränkung in dem für die Nutzung erforderlichen Maße innerhalb einer angemessenen Frist[120] zur Verfügung stellen. So können sie die Rechtsinhaber verpflichten, bspw ihre Schutzvorrichtungen zu modifizieren oder zu beschränken, sodass sich der Begünstigte selbst Zutritt verschaffen kann. Voraussetzung ist eben, dass der betreffende Begünstigte rechtmäßig Zugang zu dem geschützten Werk oder Schutzgegenstand hat. Zu beachten ist, dass sich Abs 4 nur auf Art 6 Abs 1 bezieht und der Rechtsschutz gegen Vorbereitungshandlungen gemäß Art 6 Abs 2 nicht berührt wird.[121]

---

118 RL 2001/29/EG Erw 51.

119 *Dreier*, ZUM 2002, 28 (36).

120 RL 2001/29/EG Erw 51.

121 Andere Lösungsmöglichkeiten in der Literatur: Einführung einer Sicherungsklausel, wonach das System der Schranken und Ausnahmen von den techn Schutzmaßnahmen und ihrem gesetzlichen Schutz unberührt bleiben soll (*Heide*, Access Control and Innovation under the Emerging EU Electronic Commerce Framework (FN 41) aE; *Heide*, Copyright in the EU and U.S.: What 'Access-Right' ? (FN 36), 17); Normierung spezifischer Schranken in Bezug auf die techn Schutzmaßnahmen statt einer Durchgriffslösung (*Wand*, Technische Schutzmaßnahmen und Urheberrecht, FN 37, 124ff); gesetzliche Verpflichtung des Verwenders von techn Schutzmaßnahmen, die schrankenmäßig erlaubten Nutzungen zu ermöglichen (*Dreier*, CR 2001, 45).

2. Fallgruppen

Bzgl der Einschränkung des Abs 4 ist die Regelung allerdings auf ausdrücklich angeführte Ausnahmetatbestände beschränkt. Es können drei Gruppen unterschieden werden:

1. In den in Unterabsatz 1 aufgezählten Fällen sind die Mitgliedstaaten verpflichtet (arg „*…treffen die Mitgliedstaaten…*"), Einschränkungen anzuordnen. Es gilt dies für reprografische Vervielfältigungen (Art 5 Abs 2 lit a), Vervielfältigungen durch öffentliche Bibliotheken (Art 5 Abs 2 lit c), Sendeunternehmen (Art 5 Abs 2 lit d) und soziale Einrichtungen (Art 5 Abs 2 lit e) sowie Nutzungen für Zwecke des Unterrichts und der Wissenschaft (Art 5 Abs 3 lit a), zugunsten behinderter Personen (Art 5 Abs 3 lit b) und für Gerichts- und Verwaltungsverfahren (Art 5 Abs 3 lit e). In diesen Fällen sind die Rechtsinhaber zwar nicht angehalten, den durch diese Vorschriften Begünstigten Mittel in die Hand zu geben, um techn Schutzmaßnahmen im Rahmen der freien Werknutzung auszuschalten. Setzen sie solche freiwilligen Maßnahmen aber nicht, dann haben die Mitgliedstaaten die Pflicht, geeignete Schritte zu ergreifen, um den Begünstigten die freien Werknutzungen im Rahmen der im nationalen Recht bestimmten Grenzen zu ermöglichen. In der Wahl solcher Maßnahmen sind die Mitgliedstaaten frei, die näheren Bedingungen und das Verfahren werden gesetzlich zu regeln sein.
   Problematisch erscheint, dass in der Aufzählung des Unterabsatz 1 die absolute Schranke des Art 5 Abs 1 Info-RL fehlt. Setzt hier ein Mitgliedstaat keine Maßnahmen und wirkt ein Kopierschutz derart, dass auch die in Art 5 Abs 1 freigestellten Vervielfältigungen betroffen wären, kann ein Nutzer die Schranke nicht durchsetzen.
2. Unterabsatz 2 streicht die Ausnahme des Art 5 Abs 2 lit b (Privatkopien) besonders heraus: hier ist der Mitgliedstaat berechtigt, aber nicht verpflichtet (arg „*Ein Mitgliedstaat kann…*"), Maßnahmen zu setzen, den Rechtsinhaber anzuhalten, Vervielfältigungen zum privaten Gebrauch im erforderlichen Maße (festgelegt durch Art 5 Abs 2 lit b und Abs 5) durch den Begünstigten zu ermöglichen, sofern dies nicht durch den Rechtsinhaber (innerhalb einer angemessenen Frist[122]) bereits ermöglicht wurde. Mit der fehlenden Verpflichtung wird ein wesentliches Harmonisierungsziel aufgegeben. Dies wurde damit begründet, dass durch die digitale Kopie kein Qualitätsverlust eintritt und eine Verpflichtung des Rechtsinhabers, „Entschlüsselungsmittel" zur Verfügung zu stellen, techn Schutzmaßnahmen weitgehend wirkungslos machen würde. Daneben ist der Kreis der denkbaren Situationen, in denen die Vervielfältigung zum privaten Gebrauch zum Tragen kommt, so groß, dass eine feinsinnige Abwägung notwendig sein wird, mit der bestimmt wird, in welchen Fällen und auf welche Arten die Mitgliedstaaten die Rechtsinhaber dazu verpflichten wollen, den Begünstigten

[122] RL 2001/29/EG Erw 52.

entsprechende Entschlüsselungsmittel zur Verfügung zu stellen.[123] Die EU hat damit ein klares Zeichen zugunsten der Absicherung techn Schutzmaßnahmen[124] in Richtung Schutzwürdigkeit des Rechteinhabers und zu Lasten der Nutzungsberechtigten, somit auch gegen den freien Fluss von Informationen und Kulturgütern[125], gesetzt. Rechteinhaber können auch dort techn und faktisch eine Nutzung untersagen, wo sie vertraglich dazu nicht in der Lage wären.[126] Hiermit wird auch bedenklich stark in das Grundrecht auf Informationsfreiheit des Art 10 Abs 1 EMRK als wesentliche Grundlage der Meinungs- und Informationsfreiheit eingegriffen.[127]
Dem Rechtsinhaber ist es aber freigestellt, geeignete Maßnahmen zur Kontrolle der Zahl der Vervielfältigungen zu ergreifen, also eine Mengenbeschränkung einzuführen. Leider trifft die RL bzgl der Anzahl der möglichen Kopien keine Regelung, angesichts des Art 5 (insbes des Drei-Stufen-Tests) wird diese eher gering zu bemessen sein.[128] Weiters können die Rechtsinhaber auch zwischen verschiedenen Anwendungsbereichen differenzieren, indem sie bspw private Kopien von Neuerscheinungen eher beschränken als Kopien von älterem Material.[129]

3. Für die dritte Gruppe, bestehend aus den restlichen Ausnahmen des Art 5 Abs 3, besteht keine Eingriffsbefugnis der Mitgliedstaaten. Diese sind daher durch die Anwendung techn Maßnahmen absolut geschützt und können somit ausgehebelt werden.

3. Vorrang vertraglicher Vereinbarungen im Online-Bereich

Unterabsatz 4 schränkt den Handlungsspielraum der Mitgliedstaaten erheblich ein, indem er jene Werke und sonstigen Schutzgegenstände, welche durch eine vertragliche Vereinbarung der Öffentlichkeit interaktiv (online) zugänglich gemacht werden, von der Regelung des Unterabsatz 1 und 2 ausnimmt, sodass sich der Rechtsinhaber für interaktive Dienste auf Abruf (ua das Internet) der urheberrechtlichen Schranken entledigen kann. Anbieter von Inhalten können sich somit Schrankenbestimmungen entziehen, indem sie dem Abruf aus dem Internet eine vertragliche Vereinbarung, etwa durch Bestätigen einer Nutzungsvereinbarung beim erstmaligen Aufruf der Site, voranstellen.[130]

---

123 *Walter* in Europäisches Urheberrecht, Info-RL, Rz 158.

124 *Spindler*, GRUR 2002, 105 (115).

125 *Metzger/Kreutzer*, MMR 2002, 139 (142).

126 *Wand*, Technische Schutzmaßnahmen und Urheberrecht, 125.

127 *Wand*, Technische Schutzmaßnahmen und Urheberrecht, 90f.

128 *Spindler* in GRUR 2002, 105 (118) plädiert in diesem Zusammenhang für nicht weniger als drei Kopien. Darüber hinaus sieht die Kommission in einer Erklärung zu Erw 52 die Vervielfältigung zu Zwecken der zeitversetzten Wiedergabe wohl als klassischen Fall der privaten Vervielfältigung, mitgeteilt bei *Reinbothe*, GRURInt 2001, 733 (742).

129 Siehe *Reinbothe*, GRURInt 2001, 733 (742).

130 *Bayreuther*, ZUM 2001, 828 (838).

Vertragliche Vereinbarungen haben demnach faktischen Vorrang vor den Schrankenbestimmungen.[131]

Aus rein zivil- bzw vertragsrechtlicher Sicht ist die Unterscheidung zwischen interaktiven Diensten auf Abruf und nicht interaktiven Formen der Online-Nutzung zunächst nur schwer verständlich, da es einem Vertragspartner selbstverständlich offen steht, sich strengeren als den gesetzlichen Bestimmungen zu unterwerfen, an denen er dann auch festhalten muss. Art 6 Abs 5 Unterabsatz 4 legt aber den fatalen Umkehrschluss nahe, dass der Nutzer in anderen Fällen trotz entgegenstehender vertraglicher Vereinbarungen jederzeit die gesetzlichen Schranken heranziehen könnte, diese sohin zwingender Natur seien. Das kann vom RL-Gesetzgeber nicht gemeint sein, da die Info-RL auch dem Grundsatz unterliegt, dass zunächst freiwillige Vereinbarungen gefördert werden sollen. Bedeutung erlangt die Betonung der vertraglichen Vorkehrungen für jene Mitgliedstaaten, welche keine ausgeprägte Unterscheidung zwischen sachenrechtlich geprägtem Immaterialgüterrecht und schuldrechtlich geprägter Nutzung wie die österr oder dt Rechtsordnung kennen.[132]

Die Regelung ist wohl deshalb so getroffen worden, weil schon durch den Vertrag sichergestellt wird, dass der Rechtsinhaber geeignete Maßnahmen treffen muss, um den Mitgliedern der Öffentlichkeit die Nutzung im erforderlichen Maße zu ermöglichen. Nicht interaktive Formen der Online-Nutzung, wie Pay-per-view oder Webcasting, sollen allerdings im Anwendungsbereich dieser Vorschriften verbleiben.[133] Nach *Reinbothe* will die Kommission mit dieser Bestimmung klarstellen, dass sich derjenige, der im interaktiven elektronischen Rechtsverkehr einer Vereinbarung zugestimmt hat, später nicht mehr entgegen dem Vereinbarten auf Ausnahmen berufen kann.[134] Mit einer solchen Regelung ist aber auch verbunden, dass durch vertragliche Vereinbarungen im Bereich der Internetdienste jegliche Privatkopie ausgeschlossen werden darf, wodurch eben die Regelung des Art 6 Abs 4 Unterabsatz 2 weitgehend ausgeschaltet wird.[135] Ein Konsument wäre im E-Commerce-Handel damit gegenüber herkömmlichen Handelsformen stark benachteiligt[136], was im Hinblick auf die Zunahme des Online- im Vergleich zum klassischen Handel doch sehr bedenklich erscheint.

Metzger/Kreuter[137] und *Linnenborn*[138] vertreten deshalb eine einschränkende Interpretation und wollen Unterabsatz 4 nur auf das Original, welches auf dem Server liegt und nicht auf die dem Nutzer in den Speicher

---

131 *Flechsig*, ZUM 2002, 1 (16); *Reinbothe*, GRURInt 2001, 733 (742).

132 *Spindler*, GRUR 2002, 105 (118).

133 RL 2001/29/EG Erw 53. Bei Online-Rundfunk von sog Broadcast-Servern (Webradios) fehlt es auch regelmäßig an entsprechenden urhebervertragsrechtlichen Vereinbarungen.

134 *Reinbothe*, GRURInt 2001, 733 (742).

135 Daneben wären auch die Privilegierungen für Bibliotheken (Art 5 Abs 2 lit c) und für Behinderte (Art 5 Abs 3 lit b) besonders betroffen.

136 So *Metzger/Kreuter*, MMR 2002, 139 (141) und *Bayreuther*, ZUM 2001, 828 (838).

137 In MMR 2002, 139 (141f).

138 In K&R 2001, 394 (400f).

gelieferte Kopie anwenden. Diese im Speicher entstehende Vervielfältigung eines Werkes wäre demnach wie alle anderen Werke zu behandeln, wodurch auch Art 6 Abs 4 Unterabsatz 1 und 2 wiederum uneingeschränkt zur Anwendung gelangen würden. Eine Deckung im Wortlaut des Unterabsatzes 4 findet diese Auslegung freilich nicht, da an das Werk und nicht an die Abrufhandlung angeknüpft wird. Außerdem bezieht sich Unterabsatz 4 auch auf die Regelung des Unterabsatz 2, der wiederum auf die Schranke des Art 5 Abs 2 lit b Info-RL verweist. Diese Schranke zum privaten Gebrauch bezieht sich allerdings nur auf das Vervielfältigungsrecht, sodass sich auch aus diesem Grund ein ausschließlicher Bezug zur Zugänglichmachung verbietet.

Somit wird im Bereich der interaktiven Nutzung das Recht auf Privatkopie faktisch ausgehebelt, da der Anbieter interessanter Inhalte in der Regel eine Nutzungsvereinbarung treffen wird.[139] Der Anwendungsbereich des Gesetzgebers, in jenem Gebiet gegen techn Maßnahmen vorgehen zu können, wird daher gering sein, da Rechteinhaber, die ihre Inhalte sowieso freiwillig anbieten, nicht daran interessiert sein werden, aufwendige techn Maßnahmen zu treffen.

Schließlich ist in diesem Zusammenhang von Interesse, dass die Info-RL an keiner Stelle definiert, was als „*interaktiv*“ zu bestimmen ist. Aus Art 3 Abs 1 und Erw 28 kann gefolgert werden, dass die RL darunter offenbar alle netzvermittelten Übertragungen, die einen Abruf erfordern, versteht. Pay-per-View, Webcasting oder Near-On-Demand-Dienste sind daher auch von dieser Regelung ausgenommen[140]; zweifelhaft wäre hier die Einordnung von Push-Diensten.

4. Weiterer Regelungsinhalt

Unterabsatz 3 regelt, dass alle techn Maßnahmen (sowohl die von den Rechtsinhabern freiwillig angewandten, als auch die zur Umsetzung der von den Mitgliedstaaten getroffenen Maßnahmen) den Rechtsschutz nach Abs 1 genießen. Dies bedeutet, dass neben techn Maßnahmen, die den Schutz von Werken oder sonstigen Schutzgegenständen bewirken, auch jene, die die Nutzung im Rahmen der genannten Ausnahmen ermöglichen sollen („*Entschlüsselungsvorrichtungen*“), gegen eine Umgehung dasselbe Schutzniveau aufweisen.

Unterabsatz 5 dehnt die Anwendung des Abs 4 auf die Vermiet- und VerleihRL und die DatenbankRL (somit den sui-generis-Schutz von Datenbanken) aus, sodass etwa Art 6 und 9 DatenbankRL bei der Anwendung techn Maßnahmen beschränkt werden. Damit wird etwa die Möglichkeit der digitalen Privatkopie weiter eingeschränkt, denn die Bereitstellung als Datenbank ist wohl eine der häufigsten Formen eines Online-Dienstes.

Technik nimmt keine Rücksicht auf die Sozialpflichtigkeit des geschützten Gutes, sie nimmt auch keine Rücksicht auf den Schutz der Privatsphäre und den Datenschutz. Technik dient immer nur den Interessen

---

[139] *Spindler*, GRUR 2002, 105 (119); *Dreier*, ZUM 2002, 28 (37).
[140] *Reinbothe*, GRURInt 2001, 733 (742); *Linnenborn*, K&R 2001, 394 (400).

desjenigen, der sich ihrer bedient. Ist dieser dabei frei, kann er Reglementierung herbeiführen, wo Freiheit geboten ist; kann er denjenigen ausschließen, der partizipieren soll; kann er schließlich Geld verlangen, wofür schon bezahlt wurde. Es ist ausgehend von der Regelung der Info-RL nun Aufgabe des nationalen Gesetzgebers, dafür zu sorgen, dass er die Realisierung wichtiger Allgemeininteressen nicht vom „good will“ der Industrie abhängig macht.

VI. Nationale Umsetzungen

A. Lösungsmöglichkeiten

Für eine Umsetzung der Bestimmung in nationales Recht kämen folgende Lösungen in Betracht[141]:

1. Anspruchslösung

Man stellt dem Begünstigten einen gerichtlichen Anspruch auf Bereitstellung der Mittel zur Erstellung einer Privatkopie zur Verfügung. Nachteil: aus Zeit- und Kostengründen würden viele potentielle Kläger auf eine Klage verzichten (so auch *Linnenborn*, K&R 2001, 394 (401)). Auch lässt die lange Dauer von Gerichtsverfahren eine solche Waffe wirkungslos erscheinen. Was würde es nützen, nach zwei Jahren sein Recht durchzusetzen, eine private Kopie von einer CD anfertigen zu dürfen?

In den USA geht man in diesem Zusammenhang den Weg der Sammelklage gegen die Verhinderung von Privatkopien durch techn Maßnahmen, was nach österr und dt Recht das Problem nach sich ziehen würde, dass jeder Anspruch auf Erstellung einer Privatkopie im Einzelfall erneut geltend zu machen wäre. Hier würde eine Verbandsklagebefugnis helfen (siehe unten 4.).

2. Selbsthilfelösung

Danach soll die Umgehung techn Schutzmaßnahmen erlaubt sein, wenn der Begünstigte innerhalb der Schrankenregelung zur Privatkopie handelt. Eigentlich untersagte Handlungen wären in besonderen Fällen ausnahmsweise gerechtfertigt. Das hierdurch erweckte Interesse der Industrie, eigenmächtiges Vorgehen bei den Konsumenten zu verhindern, hätte im Zweifel auch faktisch zur Folge, dass entsprechende Mittel zur Ermöglichung der Kopie trotz Schutzmaßnahme bereitgestellt würden.

Gegen diese Lösung spricht die RL selbst: es handelt sich dann nicht mehr um ein „*zur Verfügung stellen der Mittel durch die Rechtsinhaber*". Außerdem wäre nur der techn versierte Verbraucher begünstigt, eine Gleichbehandlung aller potentiellen Nutzer daher ausgeschlossen. Andernfalls wäre die techn Maßnahme auch gar nicht wirksam iS des Art 6 Abs 3 Info-RL.[142] Weiters hätte der Rechtsinhaber das Problem, bei Zugriffen auf das geschützte Material nicht erkennen zu können, ob es sich dabei um einen

---

[141] Nach *Metzger/Kreutzer*, MMR 2002, 139 (140f).

[142] Siehe oben IV.B.2.

legalen oder nicht gerechtfertigten Zugriff handelt. Jedes Umgehungstool könnte damit seine Berechtigung finden.[143]

3. Pönalisierungslösung

Danach sollen Rechtsinhaber, die keine geeigneten Mittel zur Umgehung der techn Schutzmaßnahmen bereit stellen, um Privatkopien zu ermöglichen, in die Pflicht genommen werden und ein Bußgeld zahlen. Vorbild für diese Lösung bildet das Kartellrecht, wo der Verstoß gegen die Pflicht, die für die Einhaltung der Schranken erforderlichen Mittel bereitzustellen, bestraft wird.[144]

Mit dem Wortlaut der RL in Einklang zu bringen ist diese Lösung aber nur (entgegen *Metzger/Kreutzer*, MMR 2002, 139 (140)), wenn das Bußgeld erst nach mehrmaligem Verstoß des Rechtsinhabers gegen das Gebot der Bereitstellung von Mittel zur Umgehung techn Schutzmaßnahmen angedroht wird. Denn zunächst soll ja der Rechtsinhaber freiwillig eine Maßnahme setzen. Dagegen darf noch kein Bußgeld verhängt werden. Erst dann soll der Mitgliedstaat sicherstellen, dass die Rechtsinhaber die Mittel bereitstellen. Hier wäre eine geeignete Sanktion ein Bußgeld, aber erst nach neuerlichem Verstoß gegen diese Bestimmung. Eine solche Regelung hätte auch eine nicht unerhebliche Abschreckungswirkung (finanzielle Belastung, negative Publicity).

4. Verbandsklagenlösung

Sollte der Rechtsinhaber keine geeigneten Mittel zur Verfügung stellen, um techn Schutzmaßnahmen zu umgehen, sollen die Verbraucherschutzverbände Verbandsklage (Unterlassungsverpflichtung des Rechtsinhabers) erheben können. Hier ergeben sich aber ähnliche Bedenken hinsichtlich der Vereinbarkeit mit dem Wortlaut wie bei der Pönalisierungslösung. Vorteil einer solchen Lösung ist ihre Effektivität aufgrund der Abschreckungswirkung: wäre bspw eine Musik-CD oder eine CD-ROM derart kopiergeschützt, dass nicht einmal eine private Kopie möglich wäre, müsste die gesamte Auflage vom Markt genommen werden. Einem solchen wirtschaftlichen Risiko wird sich wohl kaum ein Anbieter bewusst aussetzen.

5. Behördenlösung

Alternativ könnte man auch daran denken, eine eigene Behörde mit der Überwachung und Geltendmachung der Rechte nach Art 6 Abs 4 zu betrauen. Wie aber *Dreier*[145] betont, erscheint eine allgemeine Behörde, bei der sämtliche Schlüssel zur Überwindung von Schutzmechanismen im Vorhinein zu hinterlegen wären, als allzu aufwendig und letztlich wohl nicht praktikabel.

---

[143] *Wand*, Technische Schutzmaßnahmen und Urheberrecht, 124. Siehe auch *Reinbothe*, GRURInt 2001, 733 (742).

[144] *Metzger/Kreutzer*, MMR 2002, 139 (140).

[145] In ZUM 2002, 28 (39).

B. Österreichische Umsetzung

1. Geschichte

Mit der Veröffentlichung der Info-RL im ABl am 22. Juni 2001 wurde Österreich gemäß Art 13 Abs 1 verpflichtet, die RL bis zum 22. Dezember 2002 in österr Recht umzusetzen.[146] Dies sollte in Form einer UrhG-Nov 2002 durch den Bund[147] erfolgen. Das Bundesministerium für Justiz (im folgenden BMJ)[148] hat dabei am 5. Dezember 2001 eine Besprechung mit Vertretern der beteiligten Kreise abgehalten[149] und dabei den Diskussionsentwurf[150] einer UrhG-Nov 2002 (noch ohne Erläuterungen) vorgestellt. Dieser Entwurf enthält einerseits die Umsetzung der Info-RL und die Anpassung des österr Urheberrechts an den WCT und den WPPT, andrerseits wird die RL-Umsetzung auch für eine moderate Modernisierung des österr Urhebervertragsrechts[151] und für eine Verbesserung der Rechtsstellung der ausübenden Künstler, die an der gewerbsmäßigen Herstellung von Filmen mitwirken[152], zum Anlass genommen. Auf diese beiden letzten Bereiche kann im Rahmen dieser Arbeit nicht eingegangen werden, sie wurden im Hinblick auf die vorzeitige Beendigung der XXI. Legislaturperiode und die Mahnung Österreichs durch die Europäische Kommission aufgrund der dadurch bedingten Überschreitung der Umsetzungsfrist im Gesetzgebungsvorhaben auch nicht weiter verfolgt.

---

146 Aufgrund der Problematik des Themas und des weitreichenden Lobbyismus haben zu diesem Stichtag nur zwei der 15 Mitgliedstaaten eine Umsetzung vorgenommen (Dänemark und Griechenland).

147 Gemäß Art 10 Abs 1 Z 6 B-VG ist die Gesetzgebung und Vollziehung in Urheberrechtsangelegenheiten Bundessache.

148 Anlage zu § 2 BMG, F Z 1.

149 Die dabei erwünschten Stellungnahmen durften auch legislative Wünsche über die RL-Umsetzung hinaus enthalten, welche in bisherigen UrhG-Nov wegen Zeitmangels nicht berücksichtigt werden konnten.

150 GZ 8.117/11-I.4/2001.

151 Übernahme der Zweckübertragungstheorie (§ 31 Abs 5 dUrhG) in § 33 Abs 1a UrhG, des Grundsatzes der Nichtigkeit von Verfügungen über Rechte hinsichtlich noch nicht bekannter Nutzungsarten (§ 31 Abs 4 dUrhG) in § 24 Abs 1 UrhG und des sog Bestsellerparagraphen (§ 32a dUrhG) in § 37a UrhG aus den Bestimmungen des dUrhG. Mit § 33 Abs 1a UrhG sollte die Zweckübertragungstheorie gegenüber dem dt Vorbild dadurch erweitert werden, dass die gegenständliche Beschränkung auf den Vertragszweck immer dann gilt, wenn die Nutzungsarten im Vertrag nicht ausdrücklich einzeln bezeichnet sind (freilich haben die Deutschen mit ihrer UrhG-Nov 2002 die Bestimmung derart geändert). Beim sog Bestsellerparagraphen handelt es sich um einen Anspruch des Urhebers auf Vertragsanpassung, der eine Korrektur des vereinbarten Entgelts im Fall des besonderen Erfolgs des Werkes auf dem Markt ermöglichen soll.

152 Deren Rechtsstellung soll an jene der Filmurheber seit der UrhG-Nov 1996 angepasst werden. Danach sieht das Gesetz eine Vermutung vor, dass die gesetzlichen Vergütungsansprüche der ausübenden Künstler auf diese und die Produzenten je zur Hälfte aufzuteilen sind.

Nach Einlangen der Stellungnahmen zum Diskussionsentwurf hat das BMJ am 25. Juli 2002 den Ministerialentwurf[153] einer UrhG-Nov 2002 präsentiert. Die Begutachtungsfrist, innerhalb der wiederum zahlreiche Stellungnahmen eingegangen sind, endete mit 20. September 2002. Die rechtzeitige Umsetzung der Info-RL mit Jahresende scheiterte an der politischen Situation aufgrund vorgezogener Neuwahlen.[154]

Am 8. April 2003 stand die geplante Umsetzung auf der Tagesordnung des Justizausschusses[155] und wurde am 29. April im NR[156] und am 15. Mai im Bundesrat[157] behandelt. Die nunmehrige UrhG-Nov 2003 wurde am 6. Juni im BGBl I 2003/32 veröffentlicht und trat am 1. Juli 2003 in Kraft.[158] Darüber hinaus wurde bzgl Art 6 Info-RL und dessen Umsetzung eine Berichtspflicht des BMJ bis zum 1. Juli 2004 dem NR gegenüber festgelegt.[159]

2. Regelung

Der Umgehungsschutz für techn Maßnahmen iS der Info-RL ist in Österreich bisher nicht geregelt worden. In Umsetzung des Art 7 Abs 1 lit c SoftwareRL, der die Mitgliedstaaten zu geeigneten Maßnahmen gegen die Verbreitung sowie den zu Erwerbszwecken dienenden Besitz von Umgehungsvorrichtungen verpflichtete, wurde mit der UrhG-Nov 1993 § 91

---

153 GZ 8.117/25-I.4/2002. Im Internet: http://www.parlament.gv.at/archiv/XXI.pdf/ME/00/03/000363.pdf und http://www.bmj.gv.at/gesetzes/download/urheberrecht2002.pdf.

154 Zu den Rechtsfolgen der Nichtumsetzung von RLn vgl *v. Lewinski* in Europäisches Urheberrecht, Allgemeiner Teil, 1. Kap, Rz 43-56. Hier nur soviel: Der EGV sieht, um Verzögerungen bei der Umsetzung zu vermeiden, ein Verletzungsverfahren in den Art 226ff (ex-Art 169ff) EGV 1997 vor. Daneben hat der EuGH in seiner RSpr die Möglichkeit der unmittelbaren Anwendbarkeit von RLn und eines Staatshaftungsanspruches aufgezeigt.

155 Bericht unter http://www.parlament.gv.at/pd/pm/XXII/I/his/000/I00051_.html.

156 Die stenografischen Protokolle zur Sitzung des Nationalrates können unter http://www.parlament.gv.at/pd/pm/XXII/NRSP/NRSP_012/012_158.html abgerufen werden.

157 Die stenografischen Protokolle zur Sitzung des Bundesrates können unter http://www.parlament.gv.at/pd/pm/BR/BRSP/BRSP_696/696_056.html abgerufen werden.

158 Folgende Übergangsbestimmung gilt: *„Die Gesetzmäßigkeit von Vervielfältigungsstücken eines Werks, der Aufzeichnung eines Vortrags oder einer Aufführung, eines Lichtbildes, eines Schallträgers oder der Aufzeichnung einer Rundfunksendung, die vor dem Inkraft-Treten dieses Gesetzes hergestellt worden sind, ist nach der bisher geltenden Rechtslage zu beurteilen. Soweit die Verbreitung von Vervielfältigungsstücken nach der bisher geltenden Rechtslage zulässig, dürfen sie auch weiterhin frei verbreitet werden.*"

159 Diese beinhaltet die Beantwortung der Fragen, ob und inwieweit techn Schutzmaßnahmen von Rechteinhabern in Anspruch genommen werden, ob und inwieweit von deren Seite freiwillige Maßnahmen zur Sicherstellung der freien Werknutzungen getroffen worden sind und für den Fall, dass diese nicht ausreichen würden, welche gesetzlichen Maßnahmen vorgeschlagen werden, um die freien Werknutzungen zu ermöglichen (Entschließungstext des Justizausschusses vom 4. April 2003; http://www.parlament.gv.at/pd/pm/XXII/I/images/000/I00051__3098.pdf).

Abs 1a UrhG eingeführt und § 92 UrhG ergänzt. Diese Vorschriften beziehen sich allerdings nur auf Schutzmechanismen von Computerprogrammen.[160]

Der Umsetzung von Art 6, der ein breites Anwendungsgebiet besitzt, wird nunmehr mit § 90c UrhG nachgekommen. Dabei wird gegenüber der Info-RL eine etwas andere Gliederung verwendet, die Formulierungen aber soweit als möglich unverändert übernommen. Die zivil- und strafrechtlichen Sanktionen wurden dabei weitgehend an jene bei Urheberrechtsverletzungen angepasst, der Anspruch auf angemessenes Entgelt ist aber seiner Art nach nicht möglich, da es bei der Umgehung techn Schutzmaßnahmen nicht um die Nutzung eines Werks geht (somit fehlt auch der Verweis auf § 86 in Abs 4). § 90c UrhG gilt nicht für Computerprogramme.[161]

Problematisch ist, dass § 90c UrhG insoweit von der Diktion des Art 6 Info-RL abweicht, als er auf Schutzmaßnahmen gegen Rechtsverletzungen abstellt[162], während die Info-RL techn Maßnahmen gegen unerlaubte Handlungen schützt. Da die Nov insoweit enger als die Info-RL ist, bleibt die österr Regelung in diesem Punkt hinter der europäischen zurück.

Anspruchsberechtigter ist nur der Inhaber eines auf das UrhG gegründeten Ausschließungsrechts, da es sich beim Schutz techn Maßnahmen um einen Hilfsanspruch jener Rechte handelt.[163]

---

[160] Daneben könnte gegen die Herstellung und Verbreitung von Umgehungsvorrichtungen auch § 1 UWG Schutz bieten. Dabei geht die RSpr in Zusammenhang mit Pay-TV- oder Computerprogrammen davon aus, dass der unberechtigte Vertrieb von Decodern oder das Anbieten von Programmen zur Beseitigung des Kopierschutzes als sittenwidrige Ausbeutung fremder Leistung wettbewerbswidrig iS des § 1 UWG ist (OLG Wien 20. Dezember 1990 – Decoder; OGH 25. Oktober 1988 – MBS-Familie). Rein private Handlungen ohne Geschäftszweck, wie sie praktisch im Internet sehr häufig vorkommen (man denke etwa an digitale Kopien und deren Verbreitung im Internet – vgl MP3- und MP4-Files), werden von dieser Regelung allerdings nicht erfasst.

[161] Einschlägig ist § 90b, der inhaltlich den durch die UrhG-Nov 1993 eingeführten § 91 Abs 1a übernimmt (in Umsetzung von Art 7 Abs 1 lit c SoftwareRL) und die Sanktionen an § 90c UrhG, mit dem Art 6 Info-RL umgesetzt wird, anpasst. Dem steht Art 7 SoftwareRL, der ja durch die Info-RL nicht berührt wird, nicht entgegen, da diese Bestimmung keine bestimmten Sanktionen vorschreibt.

[162] § 90c Abs 2 lautet: „*Unter wirksamen technischen Maßnahmen sind alle Technologien, Vorrichtungen und Bestandteile zu verstehen, die im normalen Betrieb dazu bestimmt sind, die in Abs 1 bezeichneten Rechtsverletzungen zu verhindern oder einzuschränken, und die dieses Schutzziel auch tatsächlich erreichen. …*“.

[163] Dies wird insofern von der IFPI (im Internet abrufbar unter http://www.parlinkom.gv.at/pd/pm/XXI/ME/his/003/ME0036319.html, 13f) zu Recht kritisiert, als jene, die kein Ausschließungsrecht haben (wie bei Nutzungshandlungen, die bloße Vergütungsansprüche nach sich ziehen), die Umgehung techn Schutzmaßnahmen nicht verhindern können. Außerdem bestehe der Schutz techn Maßnahmen nur, wenn dadurch eine Rechtsverletzung verhindert oder eingeschränkt werde. Bei jeder freien Werknutzung dürften techn Schutzmaßnahmen umgangen werden, Hacking-Equipment angeboten und beworben werden, womit auch Art 6 Abs 4 Info-RL obsolet werden würde. Es wird daher folgende Formulierung für Abs 2 Satz 1 vorgeschlagen: „*Unter technischen Maßnahmen sind alle Technologien, Vorrichtungen und Bestandteile zu verstehen, die im normalen Betrieb dazu bestimmt sind, Handlungen zu verhindern oder einzuschränken, die nicht vom Inhaber des Urheberrechts oder verwandten Schutzrechts genehmigt worden sind.*“

Zum Schutz techn Maßnahmen durch § 90c wird kritisiert[164], dass der dadurch etablierte Kopierschutz dem Konsumenten vom Gesetzgeber schlicht aufgezwungen wird. Dies führe zu Kompatibilitätseinschränkungen und zu Wettbewerbsverzerrungen. Durch das Zusammenspiel faktischer techn Kontrolle, deren Legalisierung sowie restriktiven Lizenzen entstünde ein neues absolutes Recht, das auch nach dauerhafter Veräußerung eine Kontrolle über eine Sache stärker als das Eigentumsrecht ermöglicht.

Für das in Art 6 Abs 4 Info-RL geregelte Verhältnis von techn Schutzmaßnahmen und den Ausnahmen des Art 5 Info-RL *„ist zu erwarten, dass diese Bestimmung in der Praxis so umgesetzt werden wird, dass die technischen Maßnahmen von vornherein so ausgestaltet werden, dass sie die Nutzung der angeführten Ausnahmen in dem durch Art 6 Abs 4 Info-RL gesteckten Rahmen ermöglichen.*“[165] Nun ist Art 6 Abs 4 so weit formuliert, dass der nationale Gesetzgeber grundsätzlich zwei Möglichkeiten hat: Er kann entweder für den Fall fehlender freiwilliger Maßnahmen der Rechtsinhaber sofort eine Regelung zur Sicherung der Ansprüche der durch Art 5 Info-RL Begünstigten treffen oder aber zunächst die weitere nationale Entwicklung beobachten und erst gesetzlich eingreifen, wenn sich dafür ein praktisches Bedürfnis zeigt.[166] Im Hinblick auf die Unsicherheiten der künftigen techn Entwicklung und der sich herausbildenden Usancen im elektronischen Bereich wurde in der Nov iS der zweiten Wahlmöglichkeit entschieden und derzeit von einer gesetzlichen Regelung abgesehen.[167]

---

164 *Georg Jakob*, Universität Salzburg, Abteilung Rechtsinformatik, im Internet abrufbar unter http://www.parlinkom.gv.at/pd/pm/XXI/ME/his/003/ME0036313.html, 5f.

165 Begr des Ministerialentwurf, S 25.

166 *v. Lewinski* in Europäisches Urheberrecht, Info-RL, Rz 159.

167 *v. Lewinski*, aaO Begr des Ministerialentwurf, 26. Vgl dazu die Bedenken von *Fallenböck/Haberler* in ecolex 2002, 262 (265f), die eine ausdrückliche Regelung bevorzugen würden, die auf das Recht der durch die freien Werknutzungen Begünstigten hinweisen und das techn geschützte Werk im erforderlichen Maß „*freigeben*“ soll, sofern diese dazu rechtmäßig Zugang haben. Dazu auch die Kritik der Bundeskammer für Arbeiter und Angestellte (im Internet abrufbar unter http://www.parlinkom.gv.at/pd/pm/XXI/ME/his/003/ME0036331.html, 5ff), die es als nicht zielführend ansieht, die weitere Marktentwicklung abzuwarten. Diesfalls *„wäre das Verhältnis zwischen technischen Schutzmaßnahmen und den Ausnahmebestimmungen derart unbestimmt, dass der Rechtsanwender Rechte und Pflichten aus diesen Bestimmungen widerstreitenden Inhalts nicht annähernd erschließen kann.*“ Die AK fordert daher eine Zielbestimmung, die ein ausgewogenes Verhältnis der einander ausschließenden Rechte der Urheber und Nutzungsberechtigten bringen soll und die Förderung freiwilliger Selbstregulierung der Branche, deren Verletzung mit Regelungen im Verordnungsweg sanktioniert werden sollen. Keine Sanktionen sollte es aber gegenüber Verbrauchern geben, die Umgehungshandlungen ausschließlich zur Ausübung freier Werknutzungsrechte ergreifen.

Diese Vorgehensweise des Gesetzgebers wurde mit folgendem Argument von mehreren Seiten[168] kritisiert: nur auf freiwillige Maßnahmen der Rechtsinhaber zu hoffen, stellt die Möglichkeit, freie Werknutzungen zuzulassen oder zu untersagen, völlig in die Disposition der Rechtsinhaber. *Jakob*[169] schlägt daher vor, folgende Bestimmung einzufügen: „*Technische Schutzmaßnahmen sind dann unzulässig, bzw. ihre Umgehung jedermann gestattet, wenn durch diese Maßnahmen Rechte der freien Werknutzung faktisch verhindert oder eingeschränkt werden.*" Dies findet im RL-Text freilich keine Stütze.

C. Deutsche Umsetzung

1. Geschichte

Das Bundesministerium für Justiz hat am 18. März 2002 einen Referentenentwurf[170] zur Änderung des UrhG vorgelegt, der die Info-RL umsetzen und gleichzeitig der Vorbereitung der Ratifikation der beiden WIPO-Verträge dienen soll. Eine erste Anhörung zur Umsetzung der Info-RL fand am 22. April 2002 in Berlin statt.[171] Die Bundesregierung legte schließlich am 6. November 2002 den Gesetzentwurf[172] vor. Am 11. April 2003 hat der Bundestag mit großer Mehrheit das „*Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft*" verabschiedet.

Schon bei der Zieldefinition wird klargestellt, dass das Gesetz nicht den Anspruch erhebt, das Urheberrecht umfassend zu reformieren, sondern „*im Wesentlichen zunächst nur die zwingenden, fristgebundenen Vorgaben der Richtlinie sowie die verbindlichen Vorgaben der beiden WIPO-Verträge umgesetzt werden*"[173] sollen. Somit hält die jetzt verabschiedete Neufassung des UrhG nur für einen Teil der praxisrelevanten Probleme Regelungen bereit,

---

168 Siehe *Georg Jakob*, Universität Salzburg, Abteilung Rechtsinformatik, im Internet abrufbar unter http://www.parlinkom.gv.at/pd/pm/XXI/ME/his/003/ME0036313.html, 6 und die Stellungnahme der VÖB, im Internet abrufbar unter http://www.parlinkom.gv.at/pd/pm/XXI/ME/his/003/ME0036308.html, 3 sowie inhaltlich gleich lautend des Bücherverbands Österreichs, im Internet abrufbar unter http://www.parlinkom.gv.at/ pd/pm/XXI/ME/his/003/ME0036322.html, 3.

169 AaO 6.

170 Zu finden unter http://www.urheberrecht.org/topic/Info-RiLi/ent/RefEntw_Infoges_18_3_02.pdf.

171 Zur näheren Information siehe http://www.urheberrecht.org/topic/Info-RiLi/anhoerung.php3. Am 15. Oktober 2002 erfolgte eine weitere Anhörung zu § 52a des Regierungsentwurfes, näheres unter http://www.urheberrecht.org/topic/Info-RiLi/anhoerung52a.php.

172 Siehe http://www.urheberrecht.org/topic/Info-RiLi/ent/1500038.pdf. Dies erfolgte nach Stellungnahme des Bundesrates vom 27. September 2002 (http://www.urheberrecht.org/topic/Info-RiLi/ent/stellungnahme_br.rtf) und Gegenäußerung der Bundesregierung (http://www.urheberrecht.org/topic/Info-RiLi/ent/11523.pdf) zum Regierungsentwurf vom 16. August 2002 (http://www.urheberrecht.org/topic/Info-RiLi/ent/RegE_UrhR_InfoG.pdf).

173 Begründung, BT-Dr 15/38, S 1

andere Sachverhalte, wie etwa die Behandlung elektronischer Pressespiegel, folgen erst in einer weiteren UrhG-Nov. Dies ist auch durch die relativ kurze Umsetzungsfrist der Info-RL bedingt.[174]

Das Gesetz konzentriert sich auf die vier Kernpunkte Einführung des Rechts auf öffentliche Zugänglichmachung, Anpassung der Schrankenregelungen an die Vorgaben der RL, Einführung ergänzender Schutzbestimmungen (darunter auch die Umsetzung des Art 6 Info-RL; dazu sogleich) und Stärkung der Rechtsstellung der ausübenden Künstler.

2. Regelung

Der Gesetzgeber gewährt im neuen § 95b UrhG den Schrankenbegünstigten das „*Recht zur Durchsetzung der Schranke*", indem er dem Verwender von techn Maßnahmen dazu verpflichtet, den durch eine Vielzahl von nachfolgend aufgezählten Schrankenbestimmungen (§§ 45, 45a, 46, 47, 52a, 53, 55) Begünstigten, soweit sie rechtmäßig Zugang zu dem Werk oder Schutzgegenstand haben, die notwendigen Mittel zur Verfügung zu stellen, um von den Schrankenbestimmungen in dem erforderlichen Maße Gebrauch machen zu können. So wird beispielsweise ein Zeitungsverleger, wenn er ein durch Zugangscode geschütztes elektronisches Archiv betreibt, einer Universität den Zugangscode zur Verfügung stellen müssen. Weigert er sich aber und verstößt er somit gegen das Gebot des § 95a Abs 1 UrhG[175], so kann er von dem durch die Schrankenbestimmung Begünstigten darauf in Anspruch genommen werden, die zur Verwirklichung der jew Befugnis benötigten Mittel zur Verfügung zu stellen (Abs 2 leg cit). Nach Satz 2 des 2. Abs soll dies nur dann nicht gelten, wenn das vom Verwender von Schutzmaßnahmen „*angebotene Mittel*" einer Vereinbarung zwischen Vereinigungen der Rechtsinhaber und der durch die Schranken Begünstigten entspricht, da dann vermutet wird, „*dass das Mittel ausreicht*". Diese Passage wurde erst relativ spät eingefügt und soll für Verbände einen Anreiz schaffen, techn Schutzstandards zu etablieren.

Aufgrund der zahlreichen Schrankenbestimmungen werden es sich Rechteinhaber bei dieser Regelung überlegen, ob sie ihre Werke mit techn Schutzmaßnahmen versehen, da sie sich einem Herausgabeanspruch des Begünstigten (Abs 2) und einer Verbandsklage (§ 2a Unterlassungsklagengesetz) gegenüber sehen können. Neben den Kosten für die Verschlüsselungssoftware kommen auch diejenigen Kosten für die Rechtsinhaber hinzu, die ihnen durch die Zurverfügungstellung der Zugangscodes an die Begünstigten entstehen sowie jene durch

---

174 Siehe dazu auch näher *Schippan*, ZUM 2003, 378f.

175 Mit § 95a UrhG wird in sehr enger, teils wortgleicher Anlehnung Art 6 Abs 1 bis 3 Info-RL umgesetzt. Abs 1 bestimmt dabei, dass wirksame techn Schutzmaßnahmen zum Schutz eines nach dem UrhG geschützten Werkes oder Schutzgegenstandes ohne Zustimmung des Rechtsinhabers nicht umgangen werden dürfen, soweit dem Handelnden bekannt ist oder den Umständen nach bekannt sein muss, dass die Umgehung erfolgt, um den Zugang zu einem solchen Werk oder Schutzgegenstand oder deren Nutzung zu ermöglichen.

Kennzeichnungspflichten gemäß § 95d UrhG[176]. Ob diese abschreckende Wirkung für Rechteinhaber im digitalen Zeitalter das richtige Signal des Gesetzgebers darstellt, ist zu bezweifeln. Er hat den ihm durch die Richtlinie eingeräumten Gestaltungsspielraum somit einseitig zu Lasten der Rechteinhaber ausgenutzt. So kritisiert etwa *Schippan*[177], dass der Gesetzgeber nicht zunächst das „*mildere Mittel*" der freiwilligen – auch einseitigen – Maßnahmen von Seiten der Rechteinhaber eingesetzt hat, obwohl freiwillige Selbstkontrollorgane auch in anderen Medienbereichen erfolgreich zur Lösung von Interessengegensätzen beitragen (etwa der Deutsche Werberat oder die Freiwilligen Selbstkontrollmedien im Rundfunk- und Multimediabereich). Er plädiert damit iS der österr Lösung.

Auf Freiwilligkeit der Rechtsinhaber zu setzen eröffnet zwar eine gewisse Flexibilität (in der Begründung des Entwurfes werden als Umsetzungsalternativen genannt: Weitergabe von Schlüsselinformationen an Begünstigte zum ein- oder mehrmaligen Überwinden der techn Maßnahmen; Überlassung von Informationen an Verbände zur Verteilung an Begünstigte; Internetabruf[178]) und Zukunftsorientiertheit, *Schippan* übersieht in seinem Vorschlag aber, dass solche Alternativen nur dann Erfolgsaussicht haben können, wenn zumindest im Falle eines Scheiterns die staatliche Anordnung droht.

Die Nichtumsetzung der Kann-Vorschrift zur Durchsetzung der Privatkopieschranke bei der Anwendung techn Schutzmaßnahmen wird damit begründet, dass diese Frage weiterer Prüfungen bedarf und gesondert mit allen Betroffenen, Vertretern der Länder, der Rechtswissenschaft sowie der Rechtspraxis intensiv und *ohne Zeitdruck* erörtert werden soll. Sie wird unter anderem ebenfalls Gegenstand eines weiteren Gesetzentwurfes werden.[179]

---

[176] § 95d Kennzeichnungspflichten lautet:

„(1) Werke und andere Schutzgegenstände, die mit technischen Maßnahmen geschützt werden, sind deutlich sichtbar mit Angaben über die Eigenschaften der technischen Maßnahmen zu kennzeichnen.

(2) Wer Werke und andere Schutzgegenstände mit technischen Maßnahmen schützt, hat diese zur Ermöglichung der Geltendmachung von Ansprüchen nach § 95 b Abs. 2 mit seinem Namen oder seiner Firma und der zustellungsfähigen Anschrift zu kennzeichnen. Satz 1 findet in den Fällen des § 95 b Abs. 3 keine Anwendung."

[177] In ZUM 2003, 387.

[178] Begründung, BT-Dr 15/38, S 27.

[179] Begründung, BT-Dr 15/38, S 15.

VII. Zugangskontrolle

A. Zugangskontrollrichtlinie

Die ZugangskontrollRL, zeitlich vor der Info-RL angesiedelt, verpflichtet die Mitgliedstaaten, zum Schutz der Anbieter von zugangskontrollierten Diensten zivilrechtliche Rechtsbehelfe und strafrechtliche Sanktionen vorzusehen. Sie war von den Mitgliedstaaten bis 28. Mai 2000 umzusetzen.

Geschützt werden Fernseh- und Radiosendungen (Rundfunkdienste) und Dienste der Informationsgesellschaft, die den Interessenten gegen Entgelt angeboten werden und einer Zugangskontrolle unterliegen.[180] Gemeint sind techn Maßnahmen, die die Inanspruchnahme und den Empfang eines geschützten Dienstes von der individuellen Erlaubnis des Diensteanbieters abhängig machen. Damit wird sichergestellt, dass der Nutzer einen Bezugsvertrag mit dem Diensteanbieter abschließt und für den jew Abruf das dafür vorgesehene Entgelt entrichtet.[181]

Mit der RL wird den Diensteanbietern eine Handhabe gegen die gewerbliche Herstellung und den Vertrieb nicht autorisierter Umgehungsvorrichtungen, also gegen die Piraterie, gegeben. Dazu zählen sowohl Dekoder, Smartcards (Hardware) als auch spezielle Programme (Software) zum Knacken von Passwörtern. Mit dem Begriff „*Zugang*" ist nur der Zugriff auf das Werk, also das „*Ob*", nicht das „*Wie*" zu verstehen. Nutzungseinschränkungen und diese regelnde Bestimmungen sind daher nicht erfasst.

Geschützt sind nur entgeltliche Dienste, wobei der Begriff „*Entgelt*" autonom nach Gemeinschaftsrecht auszulegen ist (vgl Art 50 EGV – „*in der Regel gegen Entgelt*").[182] Nach der RSpr des EuGH[183] besteht das Wesensmerkmal des Entgelts darin, dass es die wirtschaftliche Gegenleistung

---

[180] Erfasst sind somit Pay-TV, Video-on-Demand, passwortgeschützte Internetdienste. Techn kann die Zugangskontrolle durch Verschlüsselung der Übertragungssignale, durch elektronische Sperren oder den Einsatz von Passwörtern erreicht werden (*Brenn*, Zugangskontrollgesetz, 2). Die Einschränkung auf den Schutz entgeltlich angebotener Dienste erklärt sich daraus, dass die RL die Vergütung der Diensteanbieter sichern will. Entscheidend dabei ist die konkrete Gegenleistung wie sie etwa auch bei Gebühren vorliegt, eine werbefinanzierte Website, die vom Nutzer unentgeltlich abgerufen werden kann, ist dagegen nicht mehr erfasst.

[181] *Brenn*, Zugangskontrollgesetz, 2.

[182] Bei der Sicherung der Zahlung des Entgelts blieben frühere Fassungen der RL aber nicht stehen. So fielen zB auch der Jugendschutz, der Schutz des Urheberrechts, der Datenschutz oder die Exklusivität eines Angebots unter ihren Anwendungsbereich. Eine Verschlüsselung eines Filmes für Zuschauer ab 18 Jahren, die ausschließlich dem Jugendschutz und nicht der Sicherung der Zahlung eines Entgeltes diente, war also erfasst (*Helberger*, ZUM 1999, 295).

[183] EuGH 7. Dezember 1993, Rs C-109/92 – Wirth vs Landeshauptstadt Hannover.

für die betreffende Leistung darstellt. Erforderlich ist also eine unternehmerische Tätigkeit, die mit Gewinnerzielungsabsicht bzw Erwerbsabsicht in Zusammenhang steht[184]; reine Kostendeckung ist nicht ausreichend. Das Entgelt muss allerdings nicht für jede einzelne Inanspruchnahme bzw jeden einzelnen Abruf geleistet werden, erfasst sind auch Dauerschuldverhältnisse, wo die Gegenleistung bspw in der monatlichen Rundfunkgebühr besteht.[185]

Zur Bedeutung der RL siehe die (mittlerweile etwas überholten) Zahlen zum Pay-TV bei *Brenn*, Zugangskontrolle, 3ff.

B. Umsetzung in Österreich

1. Regelungsinhalt

In Umsetzung der RL verabschiedete der österr Gesetzgeber im Juni 2000 im NR einstimmig das vom BMJ ausgearbeitete ZuKG, das am Tag nach seiner Verlautbarung im BGBl (ausgegeben am 11. Juli 2000) in Kraft getreten ist. Mit diesem Gesetz werden die Herstellung und der Vertrieb von Geräten und Programmen für den nichtautorisierten Abruf geschützter Dienste bekämpft. Es werden Unterlassungs-, Beseitigungs- und Schadenersatzansprüche (nach Vorbild der §§ 81 bis 90 UrhG[186]) zugunsten des Diensteanbieters geschaffen (§ 5ff ZuKG).[187] Strafrechtliche Sanktionen (angelehnt an §§ 91 bis 93 UrhG) werden gegen gewerbliche Piraten vorgesehen (§ 10 ZuKG). Die Sanktionsmaßnahmen beziehen sich daher nicht auf private Nutzer, die Umgehungsvorrichtungen verwenden. Im Rahmen des Strafverfahrens soll es auch möglich sein, Umgehungsvorrichtungen dem gewerblichen Verkehr zu entziehen (§ 11f ZuKG).

---

184 Diese Voraussetzung fehlt bspw bei Tätigkeiten, die ein Staat ohne wirtschaftliche Gegenleistung im Rahmen seiner Aufgaben, insbes in den Bereichen Soziales, Kultur, Bildung und Justiz ausübt. Gleich zu behandeln sind Fälle, in denen staatliche Tätigkeiten von Selbstverwaltungskörpern (zB Notariatskammer oder Sozialversicherungsträger) ausgeübt werden. Gebühren oder Abgaben für staatliche Leistungen stellen daher kein Entgelt idS dar.

185 *Brenn*, Zugangskontrollgesetz, 12.

186 Siehe dazu *Haller*, MMR 5/2000, XI.

187 Mit der verschuldensunabhängigen Unterlassungsklage wird ein für die Zukunft wirksames gerichtliches Verbot künftiger unerlaubter Handlungen erreicht. Bei Wiederholungsgefahr kann eine vorbeugende Unterlassungsklage erhoben werden. Rechtfertigungsgründe, die sich aus gesetzlichen Bestimmungen, aber auch aus einer umfassenden Interessenabwägung aus Geboten oder Verboten der gesamten Rechtsordnung ergeben können, sind zu beachten. Der Beseitigungsanspruch ist verschuldensunabhängig und steht unter dem Verhältnismäßigkeitsprinzip (§ 6 Abs 1 letzter HS), wonach der Anspruch nur so weit gehen soll, wie dies im Einzelfall notwendig ist, um die Rechtsposition des Diensteanbieters ausreichend und effektiv zu schützen. Der Schadenersatzanspruch deckt auch den entgangenen Gewinn ab (§ 7 Abs 2), nicht aber den immateriellen Schaden. § 7 Abs 3 sieht, um Beweisschwierigkeiten vorzubeugen, einen pauschalierten Anspruch vor (doppeltes angemessenes Entgelt für die Inanspruchnahme eines Dienstes).

Wegen des geringeren Unrechtsgehaltes werden Werbemaßnahmen, die sich auf Umgehungsvorrichtungen beziehen, sowie Serviceleistungen an solchen Vorrichtungen nur unter Verwaltungsstrafdrohung gestellt (§ 13 ZuKG). Ziel des Gesetzes ist es, dem Recht auf Zugangskontrolle ähnlich dem Urheberrecht als absolut geschütztem Rechtsgut Anerkennung zu verschaffen (§ 3 ZuKG).

2. Begriffe

Der Begriff *„Dienste der Informationsgesellschaft"*, wie ihn die ZugangskontrollRL und das ZuKG verwendet, wird in § 2 Z 5 leg cit definiert:[188]

„5. Dienst der Informationsgesellschaft: ein in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachter Dienst, wobei als

a) im Fernabsatz erbrachter Dienst ein Dienst, der ohne gleichzeitige körperliche Anwesenheit der Parteien erbracht wird, als

b) elektronisch erbrachter Dienst ein Dienst, der mittels Geräten für die elektronische Verarbeitung, einschließlich digitaler Kompression, und Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen sowie vollständig über Draht, über Funk, auf optischem oder anderem elektromagnetischen Weg gesendet, weitergeleitet und empfangen wird, und als

c) auf individuellen Abruf eines Empfängers erbrachter Dienst ein Dienst, der durch die Übertragung von Daten auf individuelle Anforderung erbracht wird, verstanden werden;"

Gemeint sind elektronische Dienste, die im Fernabsatz auf individuellen Abruf des Empfängers in der Regel gegen Entgelt[189] erbracht werden.

Fernabsatz (lit a) liegt dabei vor, wenn Anbieter und Empfänger nicht gleichzeitig anwesend sind. Erfasst sind damit neben Geschäften über das Internet auch Bestellungen aus dem Katalog per Telefon oder elektronische Buchungen eines Flugtickets, nicht aber die Buchung über ein Computernetz, wenn der Kunde im Reisebüro anwesend ist.

Elektronisch (lit b) heißt, dass der Dienst über ein elektronisches System erbracht wird, in dem die Daten sowohl beim Sender (am Ausgangspunkt) als auch beim Empfänger (am Endpunkt) elektronisch verarbeitet und gespeichert

---

[188] Die ZugangskontrollRL verweist zur Definition auf die sog Transparenzrichtlinie (98/34/EG, ABl L 204 vom 21. Juni 1998, 37, geändert durch 98/48/EG, ABl L 217 vom 5. August 1998, 18), die das Notifikationsverfahren regelt (das ist das Verfahren zur Mitteilung von Vorschriften eines Mitgliedstaates an die Kommission und die anderen Mitgliedstaaten), in Österreich umgesetzt durch das Notifikationsgesetz 1999 (BGBl I 1999/183). Die dort benutzten Begriffsbestimmungen verwendet – sprachlich und redaktionell leicht verändert – auch das ZuKG.

[189] Siehe dazu oben Kap VII.A.

werden.[190] Dies trifft daher nicht für Post- und Telefondienste zu, entgegen *Brenn*[191] aber schon für Internet-Telefonie, sofern die Signalübertragung digital erfolgt. Gemeint sind Übertragungen von Punkt-zu-Punkt (Online-Dienste, Video/Audio-On-Demand), nicht aber Übertragungen Punkt-zu-Multipunkt (Broadcasting, Teletext, Streaming).

Auf individuellen Abruf des Empfängers (lit c) bedeutet, dass der Inhalt vom Empfänger gesondert angefordert wird.[192] Daher fallen zwar E-Mail-Dienste darunter, nicht aber jene Dienste, die gleichzeitig für eine unbegrenzte Anzahl von Empfängern erbracht werden, wie bspw Near-Video/Audio-On-Demand-Anwendungen, bei denen es nicht im Belieben des Nutzers steht, wann er den Dienst in Anspruch nimmt. Entscheidend ist somit die Interaktivität eines Dienstes unter Beachtung einer zeitlichen Komponente. Der Output muss in unmittelbaren zeitlichen Zusammenhang mit dem Input des Nutzers stehen.

Problematisch sind sog „*konvergente Phänomene*", die aufgrund des Verschmelzens von Telekommunikationsdiensten, Rundfunkdiensten und Diensten der Informationsgesellschaft entstehen und von der EU in ihrem Grünbuch von 1997 zur Konvergenz[193] behandelt werden. Bei Abgrenzungsschwierigkeiten ist wohl entscheidend, ob die interaktiven Elemente überwiegen. Reines Internet-Radio oder -TV ist aber sicher kein Dienst der Informationsgesellschaft.

Anhang V der Transparenzrichtlinie enthält eine Beispielsliste von Diensten, die nicht Dienste der Informationsgesellschaft sind. Auch Offline-Dienste, wie der Vertrieb von CD-ROM oder Software auf Disketten, sind dort aufgezählt. Da dieser Anhang bei der aufgrund der techn Gegebenheiten schwierigen Auslegung des § 2 Z 5 heranzuziehen sein wird[194], ist davon auszugehen, dass eben genannter Bereich vom Anwendungsbereich der ZugangskontrollRL und des ZuKG nicht erfasst ist, sehr wohl aber von der Info-RL und ihrer Umsetzung, da letztgenannte Regelungen keinen Unterschied zwischen Offline- und Online-Nutzung machen.

Z 6 definiert die Zugangskontrolle:

„*6. Zugangskontrolle: eine technische Maßnahme oder Vorrichtung, die den Zugang zu einem geschützten Dienst in verständlicher Form von einer vorherigen individuellen Erlaubnis abhängig macht;*"

Mit einer Zugangskontrolle wird der erlaubte Zugang zum jeweils geschützten Dienst, dh der Empfang in verständlicher Form, von einer

---

190 *Brenn*, Zugangskontrollgesetz, 19. Die Sendung kann dabei drahtlos (über Funk), drahtgebunden, auf optischem oder anderem elektromagnetischen Wege erfolgen.

191 In Zugangskontrollgesetz, 23.

192 *Brenn*, Zugangskontrollgesetz, 19.

193 „*Grünbuch zur Konvergenz der Branchen Telekommunikation, Medien und Informationstechnologie und ihren ordnungspolitischen Auswirkungen*", KOM(1997) 623 vom 3. Dezember 1997.

194 *Brenn*, Zugangskontrollgesetz, 20.

vorherigen Genehmigung des Diensteanbieters abhängig gemacht.[195] Dies kann techn durch eine Verschlüsselung der Übertragungssignale, elektronische Sperren oder den Einsatz von Passwörtern bewerkstelligt werden. Das Recht auf Zugangskontrolle kann immer schon dann in Anspruch genommen werden, wenn nur ein Teil des Dienstes geschützt ist.

Als Umgehungsvorrichtung (Z 8) kommt jede Hardware oder Software oder jede Kombination aus beiden in Betracht, die den nicht autorisierten Zugang zu einem geschützten Dienst, also die Umgehung einer techn Schutzmaßnahme ermöglicht. Beispiele für Umgehungsvorrichtungen sind inoffizielle Smartcards (zB SECA Non Active Card = SNAC), welche digitale Fernsehprogramme, die nach einem bestimmten Verfahren verschlüsselt sind (zB SECA/Mediaguard[196]), entschlüsseln können und verkaufte Leerkarten (zB Wafer Gold Cards), wobei die notwendige Software von bestimmten Servern herunter geladen werden kann, um damit die gewünschten Pay-TV-Kanäle zu entschlüsseln. Nicht entscheidend ist, ob die Umgehungsvorrichtung entgeltlich oder unentgeltlich in Verkehr gelangt, vielmehr muss eine Erwerbsabsicht mit dem Vertrieb einhergehen. Auch das Aktualisieren der Karte ist verboten, weil dadurch die Umgehungskarte oder die Software angepasst wird und eine neue Umgehungsvorrichtung entsteht.

Wird hingegen der Kopierschutz einer DVD geknackt, liegt ebenso ein rein urheberrechtliches Problem vor wie wenn die so frei geschalteten Videos oder dazugehörigen Musikstücke auf die Festplatte geladen und in weiterer Folge über Internet verbreitet werden. Sind die Daten (in einem bestimmten Format) aber nur gegen Entgelt zugänglich und wird der Zugangscode geknackt, so wird eine Umgehungseinrichtung zur Verfügung gestellt. Gleiches gilt, wenn der DVD-Ländercode durch eine bestimmte Tastenkombination bei der Sony Playstation, einem DVD-Player oder einem DVD-Laufwerk eines PCs umgangen wird.[197]

3. Recht auf Zugangskontrolle

§ 3 ZuKG definiert das Recht auf Zugangskontrolle als absolutes Recht, welches dem Anbieter eines geschützten Dienstes eine ähnliche Rechtsposition verschafft, wie das Urheberrecht dem Rechteinhaber oder die Rechtsansprüche des Wettbewerbsrechts dem Unternehmer. Da ein absolut geschütztes Rechtsgut dem Geschädigten einen Schadenersatzanspruch nach zivilrechtlichen Vorschriften verschafft, kann sich auch der private Nutzer einem solchen Anspruch gegenüber sehen. Neu ist, dass das ZuKG einen besonderen Rechtsschutz für Diensteanbieter vor Signalpiraterie schafft und

---

[195] *Brenn*, Zugangskontrollgesetz, 20. Der Zugang muss also durch eine individuelle Erlaubnis des Diensteanbieters im Vorfeld ermöglicht worden sein.

[196] Digitales Verschlüsselungssystem, entwickelt von der Societe Europeenne de Controle d' Access (SECA), welches in mehreren europäischen Staaten eingesetzt wird. Nutzer der als sicher geltenden Codierung sind beispielsweise CANAL+ Frankreich, CANAL+ Spanien, Canal Digitaal Niederlande und D+ (Telepiu) Italien.

[197] Ähnlich wie der DVD-Ländercode funktionieren auch die Regional Encoding Enhancements, eine territorial-bezogenen Beschränkung der Nutzungsmöglichkeiten einer CD.

den Vergütungsanspruch des Diensteanbieters sichern soll. Von Bedeutung ist daher Erw 21 der ZugangskontrollRL, nach dem die RL andere innerstaatliche Rechtsvorschriften, insbesondere solche, die den Schutz des geistigen Eigentums oder den gewerblichen Rechtsschutz betreffen, unberührt lässt. Dies gilt daher va für Urheberrechte und verwandte Schutzrechte.

Nach *Brenn*[198] weist die Rechtsposition der Diensteanbieter eine Nahebeziehung zum Rechtsinstitut der Beeinträchtigung fremder Forderungsrechte auf. Eine direkte Anwendung ist nicht möglich, da in den gegebenen Fallkonstellationen der Nutzer mit dem Diensteanbieter tatsächlich keinen Bezugsvertrag abgeschlossen hat und daher von einem bereits entstandenen fremden Forderungsrecht nicht die Rede sein kann.

Mangels Warenverwandtschaft (Substituierbarkeit) zwischen einem geschützten Dienst (als wettbewerbsrechtlich geschützte Hauptleistung) einerseits und einer Umgehungsvorrichtung (Dekoder, Software) andrerseits steht dem betroffenen Diensteanbieter ein Unterlassungsanspruch nach § 14 UWG nicht zur Verfügung. Das Recht auf Zugangskontrolle schließt die Schutzlücke und ist rechtsgeschäftlich übertragbar (zB auf den Anbieter der Inhalte, wie den Musik- oder Filmhersteller).

4. Unerlaubte Handlungen

An unerlaubten Handlungen verbietet § 4 ZuKG in Übereinstimmung mit Art 4 der RL in Abs 1 die Herstellung, die Einfuhr, den Vertrieb, den Verkauf, die Vermietung oder Verpachtung und die Innehabung[199] von Umgehungsvorrichtungen sowie deren Installierung, Wartung, Instandsetzung oder Austausch (Serviceleistungen).[200] Die Verbotsnormen beziehen sich nur auf gewerbliche Tätigkeiten, da die ZugangskontrollRL die Vergütung der Diensteanbieter sicherstellen will.[201]

Nach Abs 2 sollen auch Werbe- und andere Marketingmaßnahmen zu gewerblichen Zwecken im Zusammenhang mit Umgehungsvorrichtungen verboten sein.[202] Damit werden die Handlungen der kommerziellen Kommunikation angesprochen[203], aber auch die Förderung des Erscheinungsbildes eines Unternehmens.

---

198 In Zugangskontrollgesetz, 30.

199 Es gilt der handelsrechtliche Besitzbegriff (vgl Art 5 der 4. EVHGB, dRGBl I S 1999/1938), Besitzwille ist nicht erforderlich.

200 Näher *Brenn*, Zugangskontrollgesetz, 35.

201 Siehe auch *Brenn*, Zugangskontrollgesetz, 32.

202 Die Verbotsnormen der Abs 1 und 2 sollen sich im Sinn der ZugangskontrollRL zunächst auf alle Handlungen erstrecken, die im Inland begangen werden (Handlungs- bzw Erfolgsort). Im Zusammenhang mit Serviceleistungen müssen aber auch Fernwartungen oder Ersatzteilsendungen aus dem Ausland erfasst werden, die im Inland verwirklicht werden (§ 4 Abs 3). Mit der Regelung in Abs 3 wird eine Ausnahme zu dem in der E-CommerceRL (Art 3 Abs 2) normierten Herkunftslandprinzip aufgestellt.

203 Diesen liegen die Überlegungen der Kommission im „*Grünbuch über kommerzielle Kommunikation im Binnenmarkt*“, KOM (1996) 192 endg vom April 1996 zugrunde. Vgl dazu auch Erw 14 ZugangskontrollRL.

C. Umsetzung in Deutschland

Die RL ist in Deutschland durch das Zugangskontrolldiensteschutzgesetz (ZKDSG) umgesetzt worden,[204] welches am 23. März 2002 in Kraft getreten ist. Verboten ist hiernach die gewerbsmäßige Verbreitung von Vorrichtungen, die dazu bestimmt sind, den geschützten Zugang von Fernseh- und Radiosendungen sowie von Tele- und Mediendiensten zu überwinden (§ 1 ZKDSG).

Die von der RL geforderten Sanktionen sind im ZKDSG hauptsächlich durch strafrechtliche und ordnungsrechtliche Normen (§§ 5ff ZKDSG) umgesetzt. Zivilrechtlich bedeutet das ZKDSG ein Schutzgesetz, sodass eine verschuldete Verletzungshandlung nach den allgemeinen Schadenersatz- und bereicherungsrechtlichen Regelungen des BGB geahndet werden kann. Nur der Anspruch auf Gewinnherausgabe hat in § 4 ZKDSG ausdrücklich Einzug gefunden. Die Tathandlungen unterscheiden sich nicht von denen des ZuKG.

D. Überschneidende Regelungen ?

Wie oben gezeigt, bezieht sich die ZugangskontrollRL neben Rundfunk- und Fernsehdiensten auch auf die Dienste der Informationsgesellschaft[205], wie sie in der Richtlinie über die techn Normung definiert sind[206] und für die eine Zugangskontrolle vorgesehen ist.

Die RL richtet sich, wie oben schon erwähnt, nur gegen Dienste, die gegen Entgelt angeboten werden. Auch kostenlos zugängliche Signale können aber durchaus ihren Wert haben. Um die Piraterie in diesem Bereich näher betrachten zu können, enthält die RL in ihrem Art 7 eine Revisionsklausel, nach der die Kommission zunächst drei Jahre nach ihrem Inkrafttreten und in Folge alle zwei Jahre den in den gemeinschaftsrechtlichen Gesetzgebungsprozeß eingebundenen Institutionen einen Bericht über die Anwendung der RL und gegebenenfalls Vorschläge zur Anpassung zu unterbreiten hat. Dabei hat die Kommission schon 1999 eine Studie[207] in Auftrag gegeben, ob auch für kostenlose Dienste ein sachlicher Schutzbedarf besteht.[208] Vorerst wird aber nicht auf den Wert des zu schützenden Signals, sondern ausschließlich auf das zu entrichtende Entgelt bzw die Vergütung des Diensteanbieters abgestellt.

Da sich auch das österr ZuKG nur gegen gewerbliche Tätigkeiten, die durch eine Erwerbsabsicht bzw Gewinnerzielungsabsicht charakterisiert sind,

---

[204] Behandelt werden nur wesentliche Unterschiede zur österr Umsetzung.

[205] Art 1 und 2 lit a ZugangskontrollRL.

[206] Zwar ist dort Entgeltlichkeit Voraussetzung, doch wird dies in der Praxis kaum eine Rolle spielen. Es kann der Zugangskontrolle zum einzelnen Werk auch eine Zugangskontrolle zum Dienst, in dem das Werk angeboten wird, vorgeschaltet sein.

[207] „*Study on the use of conditional access systems for reasons other than the protection of renumeration, to examine the legal and the economic implications within the Internal Market and the need of introducing specific legal protection*" des Instituut voor Informatierecht (http://www.ivir.nl) der Universiteit van Amsterdam, publiziert am 6. August 2001, online unter http://www.ivir.nl/publications/other/ca-report.html.

[208] *Brenn*, Zugangskontrollgesetz, 11.

richtet, werden Hacker, die Zugangskontrolleinrichtungen nur überwinden, um ihre Fähigkeiten unter Beweis zu stellen, nicht erfasst. Solche Handlungen können jedoch allgemein zivilrechtlichen, datenschutzrechtlichen (vorsätzliches Verschaffen widerrechtlichen Zugangs zu einer Datenanwendung nach § 52 Abs 1 Z 1 Datenschutzgesetz), strafrechtlichen (Datenbeschädigung nach § 126a StGB, betrügerischer Datenverarbeitungsmissbrauch nach § 148a StGB bzw Geheimnisverletzungen nach §§ 118, 119 StGB oder §§ 102, 103 TKG iVm § 88 TKG) oder eben urheberrechtlichen Bestimmungen („*Technical Measures*“ nach Art 6 Info-RL und § 90c UrhG oder Computerprogramme nach § 90 UrhG) unterliegen.

Darüber hinaus sind nach den Zugangskontrolldienstschutzgesetzen nur Diensteanbieter, nicht aber Rechtsinhaber aktivlegitimiert.[209] Die Sicherheit des zu schützenden Systems liegt nur indirekt in ihrem Interesse, dh ihr Interesse liegt zB nur in der Zugangskontrolle, nicht aber in dem zu schützenden Dienst selbst.[210] Nichtsdestoweniger bleibt es Diensteanbietern aber unbenommen, das Recht der Zugangskontrolle vertraglich auf andere Personen zu übertragen, wodurch auch die Aktivlegitimation zur Durchsetzung der entsprechenden Ansprüche übergeht.[211]

Die nationalen Umsetzungen bieten daher keinen Schutz vor nicht entgeltlichen (iS von gewerbsmäßigen) Handlungen; keinen Schutz bei geschützten, aber unentgeltlichen Angeboten; keine Regelungswirkung bzgl Nutzungseinschränkungen, die über die Frage des Zugangs als solchen hinausgehen und regelmäßig keine rechtlichen Möglichkeiten für den Urheber als Rechteinhaber, soweit dieser nicht auch Diensteanbieter ist. Nur in diesem kleinen Regelungsbereich überschneiden sich Info-RL und ZugangskontrollRL[212] sowie deren nationale Umsetzungen, der Schutzzweck bleibt aber jeweils ein anderer. Insofern nicht verständlich ist die Begründung des Entwurfes einer dt Umsetzung, die ihr keine Überschneidung mit dem Regelungsbereich der Info-RL und dem UrhG attestiert.[213]

---

209 *Haller*, Music On Demand, 75.
210 *Helberger*, ZUM 1999, 295.
211 *Haller*, MMR 5/2000, XI.
212 *Dreier*, ZUM 2002, 28 (36), der von einer gewissen Überschneidung spricht.
213 BT-Dr. 14/7229, S 7.

VIII. Fazit

Mit Art 6 Info-RL wird abgesehen von § 91 Abs 1a österr UrhG zum Schutz von Computerprogrammen bzw § 69f Abs 2 dUrhG erstmals im Urheberrecht ein rechtlicher Schutz für techn Maßnahmen statuiert.

Zu Art 6 Abs 1 Info-RL ist zu bemerken, dass die in dieser Bestimmung gewählte Formulierung die Regelung ad absurdum führt, da der Schutz nur gegen Umgehung „*wirksamer technischer Maßnahmen*" greifen soll. Kann ein Sicherungsmechanismus, wie vorausgesetzt, aber umgangen werden, erfüllt er seinen Zweck der Kontrollhaltung nicht mehr und ist somit nicht wirksam, sodass der Schutz nicht greift. Diesem Dilemma entgeht man nur, wenn man wie *Hoeren* zwischen einer ex-ante- und einer ex-post-Betrachtung unterscheidet.

Von Bedeutung ist Art 6 Abs 2 Info-RL, der die die Umgehung der Schutzmaßnahmen erleichternden oder erst ermöglichenden Vorbereitungshandlungen verhindern will. Die eigentliche Gefahr für die Rechte des geistigen Eigentums geht ja nicht von den einzelnen Umgehungshandlungen durch Privatpersonen aus, sondern von Vorrichtungen zur Umgehung, die im Handel zum Verkauf angeboten, vermietet oder in der Öffentlichkeit beworben werden.

Zum Verhältnis zwischen den techn Schutzmaßnahmen und dem Ausnahmenkatalog des Art 5, welches in Art 6 Abs 4 Info-RL in der Weise geregelt wird, dass auf freiwillige Maßnahmen der Rechtsinhaber gesetzt wird (Abs 3; Erlaubnis) und erst in zweiter Linie die Mitgliedstaaten Regelungen zur Sicherung der Nutzung im erforderlichen Maß treffen sollen (Abs 4; keine Verpflichtung aber in Bezug auf die Privatkopie), ist zu betonen: Die Möglichkeit, die Regelung durch vertragliche Vereinbarungen im Online-Bereich außer Kraft zu setzen, ist aus Sicht des Schutzzwecks schwer verständlich und benachteiligt den Konsumenten des E-Commerce-Handels stark gegenüber demjenigen des herkömmlichen Handels.

Auch in Österreich ist abgesehen von dem bereits erwähnten § 91 Abs 1a der Schutz techn Maßnahmen neu. Man hat sich mit § 90c bis auf die Gliederung zwar weitgehend an der Regelung des Art 6 Info-RL orientiert, problematisch ist aber, dass § 90c UrhG insoweit von der Diktion des Art 6 Info-RL abweicht, als er auf Schutzmaßnahmen gegen Rechtsverletzungen abstellt, während die Info-RL techn Maßnahmen gegen unerlaubte Handlungen schützt. Die Nov ist also insoweit enger als die Info-RL und die österr bleibt in diesem Punkt hinter der europäischen Regelung zurück. Zu kritisieren ist auch, dass der dadurch etablierte Kopierschutz dem Konsumenten vom Gesetzgeber schlichtweg aufgedrängt wird, was zu Kompatibilitätseinschränkungen und Wettbewerbsverzerrungen führen kann.

Für das Verhältnis von Art 5 zu Art 6 Info-RL hat sich der österr Gesetzgeber im Hinblick auf die Unsicherheiten der künftigen techn

Entwicklung (?) dafür entschieden, freiwillige Maßnahmen der Rechtsinhaber abzuwarten und erst dann eine gesetzliche Regelung zu treffen, wenn sich ein praktisches Bedürfnis dafür zeige. Er hat es sich damit sehr einfach gemacht und keine der in dieser Arbeit genannten Lösungsmöglichkeiten einer Umsetzung verwirklicht.

Die deutsche Umsetzung von Art 6 Abs 1 bis 3 Info-RL erfolgt in sehr enger, teils wortgleicher Anlehnung. § 95b UrhG gewährt den Schrankenbegünstigten das *„Recht zur Durchsetzung der Schranke"*, indem ihnen zum erforderlichen Gebrauch der Schranke notwendige Mittel zur Verfügung zu stellen sind. Dies wird durch einen Herausgabeanspruch des Begünstigten (Abs 2) und eine Verbandsklage (§ 2a Unterlassungsklagengesetz) abgesichert.

Die ZugangskontrollRL und deren nationale Umsetzung unterscheidet sich von der Info-RL und den Urheberrechtsgesetzen insoweit, als sie keinen Schutz vor nicht entgeltlichen (iS von gewerbsmäßigen) Handlungen; keinen Schutz bei geschützten, aber unentgeltlichen Angeboten; keine Regelung bzgl Nutzungseinschränkungen, die über die Frage des Zugangs als solchen hinausgehen und regelmäßig keine rechtlichen Möglichkeiten für den Urheber als Rechteinhaber, soweit dieser nicht auch Diensteanbieter ist, vorsehen. Nur im letztgenannten kleinen Regelungsbereich überschneiden sich Info-RL und ZugangskontrollRL sowie deren nationale Umsetzungen. Dabei darf aber der jew Schutzzweck nicht außer acht gelassen werden, der Schutz der Info-RL ist auf die Rechtsstellung der Urheber und Leistungsschutzberechtigten, der Schutz der ZugangskontrollRL aber auf den Vergütungsanspruch des Diensteanbieters gerichtet.

Schließlich soll noch die Titelfrage beantwortet werden: wird der den Mitgliedstaaten durch Art 6 Info-RL gewährte Spielraum zur Gänze ausgenutzt, so kann die Frage nach dem Tod der Privatkopie faktisch wohl nur mit Ja beantwortet werden. Sieht man die dt Umsetzung, dann mit Nein – einem Umgeher kann in zulässigen Fällen einer Privatkopie ja nichts geschehen. Geschickterweise hat der österr Gesetzgeber die Beantwortung dieser Frage den Rechtsinhabern überlassen, indem er auf deren freiwillige Maßnahmen setzt, sich zurücklehnt und die weitere Entwicklung beobachten will. Für Österreich kann die Antwort zum jetzigen Zeitpunkt daher nur lauten: Man (Ich) weiß es nicht.

Judikaturverzeichnis

OGH 25. Oktober 1988 – MBS-Familie, 4 Ob 94/88, WBl 1989, 56.
OLG Wien 20. Dezember 1990 – Decoder, 1 R 199/90, ecolex 1996, 612.

EuGH 7. Dezember 1993 – Wirth vs Landeshauptstadt Hannover, Rs C-109/92 (Celex-Nr 61992J0109), Slg 1993, I-6447.

Anhang[214]

Art 6 Info-RL (Volltext)

KAPITEL III
SCHUTZ VON TECHNISCHEN MASSNAHMEN UND VON INFORMATIONEN FÜR DIE WAHRNEHMUNG DER RECHTE

Artikel 6
Pflichten in Bezug auf technische Maßnahmen

(1) Die Mitgliedstaaten sehen einen angemessenen Rechtsschutz gegen die Umgehung wirksamer technischer Maßnahmen durch eine Person vor, der bekannt ist oder den Umständen nach bekannt sein muss, dass sie dieses Ziel verfolgt.

(2) Die Mitgliedstaaten sehen einen angemessenen Rechtsschutz gegen die Herstellung, die Einfuhr, die Verbreitung, den Verkauf, die Vermietung, die Werbung im Hinblick auf Verkauf oder Vermietung und den Besitz zu kommerziellen Zwecken von Vorrichtungen, Erzeugnissen oder Bestandteilen sowie die Erbringung von Dienstleistungen vor,

a) die Gegenstand einer Verkaufsförderung, Werbung oder Vermarktung mit dem Ziel der Umgehung wirksamer technischer Maßnahmen sind oder

b) die, abgesehen von der Umgehung wirksamer technischer Maßnahmen, nur einen begrenzten wirtschaftlichen Zweck oder Nutzen haben oder

c) die hauptsächlich entworfen, hergestellt, angepasst oder erbracht werden, um die Umgehung wirksamer technischer Maßnahmen zu ermöglichen oder zu erleichtern.

(3) Im Sinne dieser Richtlinie bezeichnet der Ausdruck "technische Maßnamen" alle 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 Urheberrechte verwandten gesetzlich geschützten Schutzrechte oder des in Kapitel III der Richtlinie 96/9/EG verankerten Sui-generis-Rechts ist. Technische Maßnahmen sind als "wirksam" anzusehen, soweit die Nutzung eines geschützten Werks oder eines sonstigen Schutzgegenstands von den Rechtsinhabern durch eine Zugangskontrolle oder einen Schutzmechanismus wie Verschlüsselung, Verzerrung oder sonstige Umwandlung des Werks oder sonstigen Schutzgegenstands oder einen Mechanismus zur Kontrolle der

[214] Hervorhebungen vom Autor.

Vervielfältigung, die die Erreichung des Schutzziels sicherstellen, unter Kontrolle gehalten wird.

(4) Werden von Seiten der Rechtsinhaber freiwillige Maßnahmen, einschließlich Vereinbarungen zwischen den Rechtsinhabern und anderen betroffenen Parteien, nicht ergriffen, so treffen die Mitgliedstaaten ungeachtet des Rechtsschutzes nach Absatz 1 geeignete Maßnahmen, um sicherzustellen, dass die Rechtsinhaber dem Begünstigten einer im nationalen Recht gemäß Artikel 5 Absatz 2 Buchstaben a), c), d) oder e) oder Absatz 3 Buchstaben a), b) oder e) vorgesehenen Ausnahme oder Beschränkung die Mittel zur Nutzung der betreffenden Ausnahme oder Beschränkung in dem für die Nutzung der betreffenden Ausnahme oder Beschränkung erforderlichen Maße zur Verfügung stellen, soweit der betreffende Begünstigte rechtmäßig Zugang zu dem geschützten Werk oder Schutzgegenstand hat.

Ein Mitgliedstaat kann derartige Maßnahmen auch in Bezug auf den Begünstigten einer Ausnahme oder Beschränkung gemäß Artikel 5 Absatz 2 Buchstabe b) treffen, sofern die Vervielfältigung zum privaten Gebrauch nicht bereits durch die Rechtsinhaber in dem für die Nutzung der betreffenden Ausnahme oder Beschränkung erforderlichen Maße gemäß Artikel 5 Absatz 2 Buchstabe b) und Absatz 5 ermöglicht worden ist; der Rechtsinhaber kann dadurch nicht gehindert werden, geeignete Maßnahmen in Bezug auf die Zahl der Vervielfältigungen gemäß diesen Bestimmungen zu ergreifen.

Die von den Rechtsinhabern freiwillig angewandten technischen Maßnahmen, einschließlich der zur Umsetzung freiwilliger Vereinbarungen angewandten Maßnahmen, und die technischen Maßnahmen, die zur Umsetzung der von der Mitgliedstaaten getroffenen Maßnahmen angewandt werden, genießen den Rechtsschutz nach Absatz 1.

Die Unterabsätze 1 und 2 gelten nicht für Werke und sonstige Schutzgegenstände, die der Öffentlichkeit aufgrund einer vertraglichen Vereinbarung in einer Weise zugänglich gemacht werden, dass sie Mitgliedern der Öffentlichkeit von Orten und zu Zeiten ihrer Wahl zugänglich sind.

Wenn dieser Artikel im Zusammenhang mit der Richtlinie 92/100/EWG und 96/9/EG angewandt wird, so findet dieser Absatz entsprechende Anwendung.

§ 90c öUrhG (Volltext)

Schutz technischer Maßnahmen

§ 90c

(1) Der Inhaber eines auf dieses Gesetz gegründeten Ausschließungsrechts, der sich wirksamer technischer Maßnahmen bedient, um eine Verletzung dieses Rechts zu verhindern oder einzuschränken, kann auf Unterlassung und Beseitigung des dem Gesetz widerstreitenden Zustandes klagen,

1. wenn diese Maßnahmen durch eine Person umgangen werden, der bekannt ist oder den Umständen nach bekannt sein muss, dass sie dieses Ziel verfolgt,

2. wenn Umgehungsmittel hergestellt, eingeführt, verbreitet, verkauft, vermietet und zu kommerziellen Zwecken besessen werden,

3. wenn für den Verkauf oder die Vermietung von Umgehungsmitteln geworben wird oder

4. wenn Umgehungsdienstleistungen erbracht werden.

(2) Unter wirksamen technischen Maßnahmen sind alle Technologien, Vorrichtungen und Bestandteile zu verstehen, die im normalen Betrieb dazu bestimmt sind, die in Abs. 1 bezeichneten Rechtsverletzungen zu verhindern oder einzuschränken, und die die Erreichung dieses Schutzziels sicherstellen. Diese Voraussetzungen sind nur erfüllt, soweit die Nutzung eines Werks oder sonstigen Schutzgegenstandes kontrolliert wird

1. durch eine Zugangskontrolle,

2. einen Schutzmechanismus wie Verschlüsselung, Verzerrung oder sonstige Umwandlung des Werks oder sonstigen Schutzgegenstands oder

3. durch einen Mechanismus zur Kontrolle der Vervielfältigung.

(3) Unter Umgehungsmitteln beziehungsweise Umgehungsdienstleistungen sind Vorrichtungen, Erzeugnisse oder Bestandteile beziehungsweise Dienstleistungen zu verstehen,

1. die Gegenstand einer Verkaufsförderung, Werbung oder Vermarktung mit dem Ziel der Umgehung wirksamer technischer Maßnahmen sind,

2. die, abgesehen von der Umgehung wirksamer technischer Maßnahmen, nur einen begrenzten wirtschaftlichen Zweck oder Nutzen haben oder

3. die hauptsächlich entworfen, hergestellt, angepasst oder erbracht werden, um die Umgehung wirksamer technischer Maßnahmen zu ermöglichen oder zu erleichtern.

(4) Die §§ 81, 82 Abs. 2 bis 6, §§ 85, 87 Abs. 1 und 2, § 87a Abs. 1, § 88 Abs. 2, §§ 89 und 90 gelten entsprechend.

(5) Die Abs. 1 bis 4 gelten nicht mit Beziehung auf Rechte an Computerprogrammen.

§ 95a und § 95b dUrhG (Volltext)

§ 95a
Schutz technischer Maßnahmen

(1) Wirksame technische Maßnahmen zum Schutz eines nach diesem Gesetz geschützten Werkes oder eines anderen nach diesem Gesetz geschützten Schutzgegenstandes dürfen ohne Zustimmung des Rechtsinhabers nicht umgangen werden, soweit dem Handelnden bekannt ist oder den Umständen nach bekannt sein muss, dass die Umgehung erfolgt, um den Zugang zu einem solchen Werk oder Schutzgegenstand oder deren Nutzung zu ermöglichen.

(2) Technische Maßnahmen im Sinne dieses Gesetzes sind Technologien, Vorrichtungen und Bestandteile, die im normalen Betrieb dazu bestimmt sind, geschützte Werke oder andere nach diesem Gesetz geschützte Schutzgegenstände betreffende Handlungen, die vom Rechtsinhaber nicht genehmigt sind, zu verhindern oder einzuschränken. Technische Maßnahmen sind wirksam, soweit durch sie die Nutzung eines geschützten Werkes oder eines anderen nach diesem Gesetz geschützten Schutzgegenstandes von dem Rechtsinhaber durch eine Zugangskontrolle, einen Schutzmechanismus wie Verschlüsselung, Verzerrung oder sonstige Umwandlung oder einen Mechanismus zur Kontrolle der Vervielfältigung, die die Erreichung des Schutzziels sicherstellen, unter Kontrolle gehalten wird.

(3) Verboten sind die Herstellung, die Einfuhr, die Verbreitung, der Verkauf, die Vermietung, die Werbung im Hinblick auf Verkauf oder Vermietung und der gewerblichen Zwecken dienende Besitz von Vorrichtungen, Erzeugnissen oder Bestandteilen sowie die Erbringung von Dienstleistungen, die

1. Gegenstand einer Verkaufsförderung, Werbung oder Vermarktung mit dem Ziel der Umgehung wirksamer technischer Maßnahmen sind oder

2. abgesehen von der Umgehung wirksamer technischer Maßnahmen nur einen begrenzten wirtschaftlichen Zweck oder Nutzen haben oder

3. hauptsächlich entworfen, hergestellt, angepasst oder erbracht werden, um die Umgehung wirksamer technischer Maßnahmen zu ermöglichen oder zu erleichtern.

(4) Von den Verboten der Absätze 1 und 3 unberührt bleiben Aufgaben und Befugnisse öffentlicher Stellen zum Zwecke des Schutzes der öffentlichen Sicherheit oder der Strafrechtspflege.

§ 95b
Durchsetzung von Schrankenbestimmungen

(1) Soweit ein Rechtsinhaber technische Maßnahmen nach Maßgabe dieses Gesetzes anwendet, ist er verpflichtet, den durch eine der nachfolgend genannten Bestimmungen Begünstigten, soweit sie rechtmäßig Zugang zu dem Werk oder Schutzgegenstand haben, die notwendigen Mittel zur Verfügung zu stellen, um von diesen Bestimmungen in dem erforderlichen Maße Gebrauch machen zu können:

1. § 45 (Rechtspflege und öffentliche Sicherheit),
2. § 45a (Behinderte Menschen),
3. § 46 (Sammlungen für Kirchen-, Schul- oder Unterrichtsgebrauch), mit Ausnahme des Kirchengebrauchs,
4. § 47 (Schulfunksendungen),
5. § 52a (Öffentliche Zugänglichmachung für Unterricht und Forschung),
6. § 53 (Vervielfältigungen zum privaten und sonstigen eigenen Gebrauch)
a) Absatz 1, soweit es sich um Vervielfältigungen auf Papier oder einen ähnlichen Träger mittels beliebiger photomechanischer Verfahren oder anderer Verfahren mit ähnlicher Wirkung handelt,
b) Absatz 2 Satz 1 Nr. 1,
c) Absatz 2 Satz 1 Nr. 2 in Verbindung mit Satz 2 Nr. 1 oder 3,
d) Absatz 2 Satz 1 Nr. 3 und 4 jeweils in Verbindung mit Satz 2 Nr. 1 und Satz 3,
e) Absatz 3,
7. § 55 (Vervielfältigung durch Sendeunternehmen).

Vereinbarungen zum Ausschluss der Verpflichtungen nach Satz 1 sind unwirksam.

(2) Wer gegen das Gebot nach Absatz 1 verstößt, kann von dem Begünstigen einer der genannten Bestimmungen darauf in Anspruch genommen werden, die zur Verwirklichung der jeweiligen Befugnis benötigten Mittel zur Verfügung zu stellen.

(3) Die Absätze 1 und 2 gelten nicht, soweit Werke und sonstige Schutzgegenstände der Öffentlichkeit auf Grund einer vertraglichen Vereinbarung in einer Weise zugänglich gemacht werden, dass sie Mitgliedern der Öffentlichkeit von Orten und zu Zeiten ihrer Wahl zugänglich sind.

(4) Zur Erfüllung der Verpflichtungen aus Absatz 1 angewandte technische Maßnahmen, einschließlich der zur Umsetzung freiwilliger Vereinbarungen angewandten Maßnahmen, genießen Rechtsschutz nach § 95a.