DeCSS – oder: Spiel mir das Lied vom Code

von Bernhard Knies[*]

Einleitung

In Deutschland wird heute viel über die Einführung von Kopierschutzsystemen durch die Musikindustrie zum Schutz Ihrer CDs vor den immer beliebteren selbstgebrannten Privatkopien diskutiert.[1] Kaum im Blickpunkt der Öffentlichkeit stehen dagegen die Erfahrungen mit einem bereits etablierten Kopierschutzsystem, das sich die Filmindustrie zum Schutz ihrer auf DVD verbreiteten Filme hat einfallen lassen und das heute in den Vereinigten Staaten für interessante Rechtsstreitigkeiten sorgt.

Dort wird schon seit längerem über den Umgang mit Kopierschutzsystemen von DVDs gestritten. Es mußte entschieden werden, wie das „Recht des Verbrauchers" auf seine Privatkopie, sowie sein Recht zur freien Meinungsäußerung einerseits mit dem Recht der Industrie in Einklang gebracht werden kann ihre Produkte vor dem digitalen Datenklau zu schützen. Dabei geht es insbesondere um den Kopierschutz von DVDs, der mit dem Softwaretool DeCSS umgangen werden kann.

1. Umfassender Kopierschutz von DVDs

Die Filmindustrie hat schon bei der Entwicklung der DVD, also der digitalen Nachfolgerin der VHS-Kassette, über einen wirksamen technologischen Schutz ihres Produktes nachgedacht. Das erklärte Ziel war es, dem Verbraucher nach Wahl des Rechteinhabers sowohl die analoge, wie auch die digitale Privatkopie zu verwehren, die DVD also vor jeglicher Privatkopie zu schützen.

a. Analoger Kopierschutz

Der Schutz von VHS-Kauf- oder Leihkassetten vor einer Privatkopie durch den Verbraucher ist ein „alter Hut", den die Industrie nahtlos auch auf den digitalen Inhalt ihrer DVDs übertragen konnte. Der hierfür verwandte Schutzstandard stammt von der Firma Macrovision und ist nun schon fast zehn Jahre alt.[2] Das System gibt am analogen Bildausgang einer damit geschützten VHS-Kassette oder auch der DVD ein Störsignal aus, das einen VHS-Videorecorder[3] über die Bilddaten täuscht und ihn dazu veranlaßt, das analoge Ausgangssignal falsch zu interpretieren. Das „dürftige" Ergebnis der Privatkopie sieht der frustrierte Nutzer in Form von „laufenden Bildern", Rauschen und anderen Störsignalen auf seiner Privatkopie, die damit ungenießbar wird. Da der Schutz der Kaufkassetten durch Macrovision in Verbraucherkreisen wenig bekannt ist, dürfte der ein oder andere verhinderte „Privatkopierer" an einen

---

[*] Dr. iur, Rechtsanwalt in München, www.new-media-law.net.

[1] Vgl. hierzu zusammenfassend *Goldmann/Lippe*, ZUM 2002, 362 ff. und *Knies,* ZUM 2002, 793 ff.

[2] Vgl. hierzu *Bögeholz,* c´t 20/1999, S. 132 ff., mit einer ausführlichen technischen Beschreibung der Funktionsweise, sowie die Produktbeschreibung von Macrovision bei http://www.macrovision.com/solutions/video/copyprotect.

[3] Andere Videosysteme wie Beta oder andere Standards scheinen hingegen auf das Störsignal von Macrovision regelmäßig nicht hereinzufallen, vgl. *Bögeholz*, a.a.O.

Defekt seines geliebten Videorecorders geglaubt und womöglich vergebliche Reparaturversuche gestartet haben.

Die Industrie hat bei der Einführung der DVD dieses sogenannte APS-Verfahren (Analog Copy Protection System) übernommen, so daß bei DVDs, die mit dem Schutz von Macrovision ausgestattet sind,[4] ebenfalls keine analogen Privatkopien hergestellt werden können. Ohne spezielle Filterhardware (im Fachjargon „Macrovision-Killer") ist die analoge Kopie auf die VHS-Kassette also nicht mehr möglich.[5]

Das neueste offenbar aber noch nicht ganz praxistaugliche analoge Kopierschutzsystem ebenfalls aus dem Hause Macrovision arbeitet mit sogenannten „Wasserschutzzeichen", diese sollen auch auf analogen Privatkopien, die etwa mittels Filterhardware hergestellt wurden, versteckt erhalten bleiben und weitere Kopien verhindern.[6] Die Industrie möchte mit diesem Verfahren nach Meinung der Kritiker das „analoge Loch" stopfen.[7]

Offenbar mißtraut die Industrie aber den analogen Kopierschutzsystemen zusehends mehr. So gibt es Überlegungen innerhalb der Konzerne, die analogen Schnittstellen an Hifi-Anlagen und DVD-Playern gänzlich abzuschaffen und nur noch auf besser kontrollierbare digitale Ausgänge zu setzen.[8]

b. Digitaler Kopierschutz durch CSS

Dies erstaunt um so mehr, als der von der Industrie erdachte digitale Kopierschutz heute die herbste Niederlage seitens der „Privatkopiererfront" einstecken mußte. Noch 1996 glaubte die Unterhaltungsindustrie einen wasserdichten Schutz ihrer digitalen Inhalte entwickelt zu haben. Man hat mit großem Aufwand die CSS-Codierungssoftware („Content Scramble System") entwickelt, die den Inhalt einer DVD verschlüsselt.[9] Nur mit Hilfe dieses Quellcodes kann der digitale Inhalt der DVD später wieder sichtbar gemacht werden. Der Quellcode von CSS ist, technisch gut geschützt, in allen heimischen DVD-Playern und auch in Computerprogrammen wie etwa WIN-DVD installiert, mit denen man DVDs zusammen mit einem tauglichen Laufwerk auf dem Laptop oder PC betrachten kann.[10] Die von CSS verwendeten Schlüssel sind 40 Bit lang, sie galten aber schon bei der Einführung des Standards

---

[4] Nicht jeder Hersteller schützt heute allerdings seine DVD durch Macrovision, da die Firma für die Lizenz seines Schutzsystems offenbar doch recht erhebliche Beträge von den Filmherstellern fordert und sich der Schutz insofern nur bei „teuren" Streifen lohnt.

[5] Zum APS-Schutzsystem von Macrovision und den technischen Umgehungsmöglichkeiten vgl. ausführlich *Laue/Zota*, c´t 2/2002, S. 86 ff., die Autoren beschreiben insbesondere eine Möglichkeit den Schutz über den Umweg von PC-Graphikkarten zu umgehen, die sich offenbar von Macrovision nicht täuschen lassen. Weiter gibt es auch im Handel Geräte, die das Macrovision Störsignal ausblenden, vgl. etwa die Darstellung bei http://www.dvdboard.de/FAQ/new/index.html?kb/macrovision.htm.

[6] Vgl. hierzu die technische Beschreibung bei http://www.macrovision.com/solutions/video/copyprotect, sowie *Himmelein,* c´t2/2002, S. 80 ff.

[7] Vgl. www.heise.de/newsticker/data/vza-27.05.02-000/.

[8] Vgl. *Laue/Zota*, a.a.O.

[9] Vgl. zu der historischen Entwicklung von CSS ausführlich 111 F.Supp. 2d 294 (S.D.N.Y. 2000), S. 15, mit dem Hinweis, daß CSS ursprünglich von Matsushita Electric und Toshiba entwickelt wurde, die später eine kostenlose Lizenz an DVD CCA vergaben.

[10] Vgl. etwa die technische Beschreibung auf der Homepage der DVD CCA, www.dvdcca.org/faq.html.

als minderwertiger Schutz, dessen „Entschlüsselung“ in absehbarer Zeit erwartet wurde.[11]

Lizenzgeber des CSS-Systems ist die amerikanische DVD CCA („DVD Copy Control Association“).[12] Die DVD CCA lizenziert das zweistufige CSS-System einerseits an Hersteller von DVDs (also in der Regel die Filmindustrie) sowie andererseits an die Hersteller von DVD-Abspielgeräten und von Abspiel-Software. Das System setzt voraus, daß sowohl die DVD, als auch das Abspielgerät mit CSS ausgerüstet sind, um das Abspielen des codierten Filmes zu ermöglichen. Die Information auf der DVD selbst ist mit Hilfe von CSS verschlüsselt, das Abspielgerät entschlüsselt sie wieder. Eine digitale (Privat)-Kopie kann von der DVD somit ohne entsprechende Software nicht hergestellt werden.

Das System gibt der Industrie weiterhin auch die Möglichkeit mit den sogenannten Ländercodes die Abspielbarkeit von DVDs regional zu beschränken.[13] Damit soll der Filmindustrie die Möglichkeit erhalten bleiben, Filme in unterschiedlichen Ländern zu verschiedenen Zeitpunkten auszuwerten. Die Veröffentlichung der DVDs in Amerika liegt oft vor dem offiziellen Kinostart der Filme in Europa und man möchte vermeiden, daß das europäische Publikum schon vor dem Kinostart etwa über das Internet die amerikanische DVD bestellt.[14] Auch die Ausnutzung von unterschiedlichen Preisniveaus dürfte wohl eine unausgesprochene Rolle spielen. So sind beispielsweise amerikanische DVDs trotz des hohen Dollarkurses regelmäßig erheblich günstiger als europäische.

Sowohl Ländercode wie auch Kopierschutz sind somit abhängig von dem CSS-System. Die Industrie war der Meinung, diesen CSS-Code so sicher in der Hard- und Software versteckt zu haben, daß keiner an ihn herankäme, um etwa unverschlüsselte Kopien von DVDs herstellen zu können.[15]

c. Entschlüsselung des Schutzes durch das Hacker-DeCSS-Programm

Hackergruppierungen sahen jedoch in dem Versteck des Codes eine willkommene Aufgabe. Sie machten sich auf die Suche nach dem Code. Ihnen mißfiel offenbar insbesondere, daß die CSS-Software das Betrachten von DVDs auf dem von ihnen favorisierten Linux-System nicht zuließ.[16] Also begann man, an einer Möglichkeit zu arbeiten, die DVD auf der Festplatte zu speichern, um sie von dort aus auch auf dem Linux-Rechner abspielen zu können. Hierfür war man allerdings auf den geheimen Quellcode der CSS-Software angewiesen.

---

[11] Vgl. *Bögeholz*, c´t 20/1999, S. 132 sehr ausführlich auch zum Aufbau des technischen Schutzes durch CSS; eine gute technische Beschreibung findet sich auch bei *Bogk,* c´t 8/200, S. 220.

[12] Vgl. www.dvdcca.org.

[13] Vgl. hierzu die Erläuterung der DVDCCA, www.dvdcca.org/faq.html. Viele DVD sind mit diesem sogenannten „Ländercode“ beschränkt, das bedeutet, daß sie nur auf einem Abspielgerät mit dem entsprechenden Ländercode abgespielt werden können. So benötigt man in Europa etwa DVD und Abspielgerät mit dem Ländercode 2.

[14] Dies kann der Kunde freilich umgehen, wenn er ein DVD-Abspielgerät mit amerikanischem Ländercode erwirbt.

[15] Auch die Lizenzverträge, die die DVD CCA mit ihren Lizenznehmern schließt, sehen strenge Sicherheits- und Geheimhaltungsvorschriften vor.

[16] Vgl. hierzu etwa Andy Patrizio auf www.wired.com/news/politics/0,1283,35394,00.html. Dagegen verweist die DVD CCA in ihrer Homepage darauf, daß man gerade eben an den Hersteller sigma designs einen DVD-Player für Linux lizenziert habe, www.dvdcca.org/faq.html.

Einer norwegischen Gruppe von Hackern, die sich MoRE („Masters of Reverse Engineering“) nennt, gelang unter Ägide des damals 15 Jahre alten Norwegers Jon Johansen schließlich im September 1999 dank eines Lapsus eines Lizenznehmers der CSS-Software, die „Entdeckung“ dieses Codes.[17] Die Firma Xing Technology Corporation hatte den Code nicht gut genug in ihrem Programm versteckt, so daß er den feindlichen Hackern in die Hände fiel.[18] Die erfolgreiche Entwicklung des DVD-Players für Linux-Systeme wurde schnell zur Nebensache, man entdeckte die wundervollen Möglichkeiten freier Kopierbarkeit der einmal entschlüsselten DVD, die nun auch in (qualitativ schlechteren) MPEG-Files abgespeichert oder sogar auf CDR gebrannt werden konnte.[19] In der Folge verbreiteten die Hacker den CSS-Code „kollegialerweise“ gleich über das gesamte Internet. Dort kann der geneigte Surfer ihn nun auf vielen Seiten unter dem neuen sinnigen Namen DeCSS als kleinen Programmfile von 30.000 Bit Größe herunterladen. Das Programm begrüßt den Nutzer als Version DeCSS 1.b („by MoRE“) und gibt damit einen dezenten Hinweis auf seine norwegischen Entdecker. Der Schutz von DVDs durch CSS war mit dieser Entdeckung mehr oder weniger am Ende.

Mit Hilfe des DeCSS-Programms kann man nun geschützte DVDs kopieren oder auch auf solchen Geräten abspielen, die nicht die von der CCA lizenzierte CSS-Technologie benutzen. Verständlich, daß die Veröffentlichung des Quellcodes die Industrie stark verärgert, glaubt die mächtige MPAA („The Motion Picture Association of America“) doch, daß der kleine Wurm einen jährlichen Schaden in Höhe von etwa $ 2,5 Milliarden pro Jahr verursache.[20] In der Tat dürfte der durch die Veröffentlichung des Quellcodes von CSS angerichtete Schaden für die Industrie wohl kaum mehr zu beheben sein, denn einmal veröffentlicht, wird sich die Sequenz nie mehr geheimhalten lassen und die Entwicklung eines komplett neuen Systems wäre mit einem gigantischen Aufwand verbunden, da ganze Generationen von DVD-Abspielgeräten umgerüstet werden müßten.[21] Die Umgehung des Kopierschutzes wird indes immer populärer, im Internet werden inzwischen Bücher mit Anleitungen zum Knacken des Kopierschutzes von DVDs angeboten.[22] Zudem soll es möglich sein, mit Hilfe neuer Kompressionstechniken wie etwa DivX den Inhalt ganzer DVDs auf eine CD-ROM zu brennen.

Die Filmindustrie fühlte sich verständlicherweise herausgefordert. Mit schnellen juristischen Schritten mußten die Hacker deshalb rechnen. Doch zuvor ließ man sich noch einiges amüsantes Beiwerk zur Erheiterung der Konzerne einfallen. So wurde etwa der Quellcode auf T-Shirts gedruckt und von dem Musiker Josef Wecker gefühlvoll zu dem „Lied vom Code“ vertont, das man sich passenderweise bei MP3.com herunterladen konnte.[23] Ein Sympathisant rief gar zu einem Wettbewerb zu künstlerischer Verarbeitung des Codes auf,[24] dessen Juror bezeichnenderweise der Norweger Jon Johansen ist, der als eigentlicher „Entdecker“ des Codes gilt, und

---

[17] Vgl. 111 F.Supp. 2d 294 (S.D.N.Y. 2000), S. 17.
[18] Vgl. hierzu die Darstellung bei www.decss.com; *Thomas*, „DVD Encryption – DeCSS“, 2000 Ent.L.R., 135; *Bogk,* c´t 8/2000, S. 220 ff.
[19] Vgl. die technische Darstellung bei www.decss.com.
[20] Vgl. hierzu etwa Andy Patrizio auf www.wired.com/news/politics/0,1283,35394,00.html.
[21] Auf diesen Aspekt weist auch 111 F.Supp. 2d 294 (S.D.N.Y. 2000), S. 27 hin.
[22] Etwa das Buch „Expert Guide to Copying DVDs“ auf http://www.expert-guides.com/library/dvd_ripping.asp.
[23] Vgl. Heise Newsticker vom 8.9.2000, www.heise.de/newsticker/data/ghi-08.09.00-000/.
[24] Siehe DeArt, www.lemuria.org.

heute über ärgerliche Hausdurchsuchungen der norwegischen Polizei klagt.[25] Johansen, mittlerweile volljährig, mußte sich auf eine Anzeige der MPA hin in Oslo vor einem Strafgericht verantworten.[26] In erster Instanz kann er sich zwischenzeitlich über einen Freispruch freuen,[27] allerdings ist offenbar die Staatsanwaltschaft in die Berufung gegangen,[28] so daß Johansen weiter um seine Freiheit bangen muß.

2. Die amerikanischen Entscheidungen zu DeCSS

Die oben geschilderten „Raubzüge“ der norwegischen Hacker ließen, wie bereits erwähnt, nicht lange auf juristische Fehden warten. Die Industrie wehrte sich mit Klagen gegen die Betreiber von Websites, auf denen die Umgehungssoftware DeCSS zum Download angeboten wurde.

Der heute vor amerikanischen Gerichten ausgetragene Streit über die Rechtmäßigkeit der Veröffentlichung des Quellcodes CSS durch die Hacker bewegt sich im Spannungsfeld zwischen dem Schutz der technologischen Maßnahmen (wie etwa durch den Digital Millenium Copyright Act) einerseits und dem Recht auf freie Meinungsäußerung (dem „free speech“) und der Kunstfreiheit andererseits.

In Kalifornien wurde ein Student, Mitbetreiber einer Website, auf der das Hacker-Tool zum Download angeboten wurde, von der DVD CCA (DVD Copy Control Association) mittels einer einstweiligen Verfügung auf Unterlassung in Anspruch genommen. Die DVD CCA konnte allerdings die örtliche Zuständigkeit des Kalifornischen Gerichtes nicht belegen, so daß der Rechtsstreit von dem Studenten Pavlovich letztlich aus formalen Gründen gewonnen wurde.[29] Das oberste Bundesgericht der Vereinigten Staaten lehnte eine Befassung mit der Sache ab.[30] Eine peinliche Schlappe für die Filmstudios.

Erfolgreicher war man hingegen in New York. Hier wurde in einer Art Musterrechtsstreit die Hackerseite www.2600.com (betrieben von den Herausgebern des Magazins „Hacker Quarterly“)[31] vor dem United States Distric Court of New York auf Unterlassung verklagt, die ebenfalls DeCSS zum Download bereit hielt.[32]

Das Gericht untersagte im Ergebnis den Betreibern der Seite, den Code zu veröffentlichen und mit Links auf andere Seiten im Web zu verweisen, auf denen das streitige Tool DeCSS ebenfalls heruntergeladen werden kann.[33] Das Urteil wurde als erster entscheidender Sieg der Filmindustrie bewertet.[34]

---

[25] Vgl. Florian Rötzer in Heise Newsticker vom 25.1.01, www.heise.de/tp/deutsch/inhalt/te/5716/1.html.
[26] http://www.heise.de/newsticker/data/anw-09.12.02-000/.
[27] http://www.heise.de/newsticker/data/anw-07.01.03-001/.
[28] http://www.heise.de/newsticker/data/anw-20.01.03-006/.
[29] http://www.heise.de/bin/nt.print/newsticker/data/nij-02.01.03-000/?id=30881803&todo=print.
[30] http://www.heise.de/bin/nt.print/newsticker/data/cp-04.01.03-001/?id=39a7f591&todo=print.
[31] Darunter dem Beklagten „Meisterhacker“ Eric Corley, der unter dem Pseudonym Emanuel Goldstein fingierte, einem Charakter aus George Orwells 1984, vgl. 111 F.Supp. 2d 294 (S.D.N.Y. 2000), S. 11 f. Bezeichnenderweise wurde das Magazin Hacker Quarterly auch 1984 von Corley gegründet, es gilt als Bibel der Hacker-Community.
[32] 111 F.Supp. 2d 294 (S.D.N.Y. 2000), 00 Civ. 00277.
[33] 111 F.Supp. 2d 294 (S.D.N.Y. 2000), 00 Civ. 00277.
[34] Vgl. http://www.heise.de/newsticker/data/fr-18.08.00-000/.

a. Das „Recht“ auf die Privatkopie

Die Beklagten hatten sich zuvor mit dem interessanten Argument verteidigt, daß es DeCSS dem Nutzer erst ermögliche, seinen Anspruch auf „fair use“, also die vom Gesetzgeber vorgesehenen Schranken des Urheberrechts zu nutzen. Die Kopie werde nicht zu urheberrechtsverletzenden Zwecken, sondern zum gesetzgeberisch erlaubten Gebrauch im Rahmen der Schranken des Urheberrechts gemacht.[35] In diesem Zusammenhang kann man sich auch im Hinblick auf die Richtlinie zur Informationsgesellschaft die Frage stellen, ob denn die vom Gesetzgeber vorgesehenen Schranken des Urheberrechts wie insbesondere die Privatkopie dem Nutzer quasi kraft Gesetzes zustehen, oder ob sie der Rechteinhaber eben durch technische Maßnahmen vereiteln darf.[36] Das New Yorker Gericht war der Meinung, daß die Ausnutzung der Schranken des Urheberrechts dem Verbraucher nicht zwingend gestattet werden müsse.

b. Die freie Meinungsäußerung

Weiter verteidigten sich die Beklagten damit, daß die Bekanntgabe des Computer Codes auf Websites unabhängig von seinem Inhalt vom Grundrecht der freien Meinungsäußerung erfaßt werde. Die Veröffentlichung des Codes könne gesetzlich somit nicht beschränkt werden. Das Gericht gestand in diesem Punkt zwar zu, daß es sich bei dem Veröffentlichen des Computer Codes[37] grundsätzlich um eine Meinungsäußerung handeln könne. Diese könne aber nicht schrankenlos gewährleistet werden, wie auch andere Formen der Meinungsäußerung wie die Veröffentlichung von Computer Viren aus Gründen der nationalen Sicherheit unterbunden werden müßten.[38]

c. Verstoß gegen das Verbot der Umgehung von technischen Schutzmaßnahmen

Das New Yorker Gericht hatte schließlich darüber zu entscheiden, ob die CSS eine technische Schutzmaßnahme im Sinne des 17 U.S.C. § 1201 (a) (1) sei und ob DeCSS rechtsverletzend wirke.

Die Vereinigten Staaten waren den Europäern in Bezug auf den Schutz digitaler Rechte in der Informationsgesellschaft zeitlich um einige Nasenlängen voraus. Ihr Digital Millenium Copyright Act (DCMA)[39] konnte schon am 28. Oktober 1998 von Präsident Clinton unterzeichnet werden.

---

[35] Vgl. hierzu 111 F.Supp. 2d 294 (S.D.N.Y. 2000), S. 2. Dieses Spannungsverhältnis zwischen „fair use“ und der starken Zugangskontrolle wurde auch schon bei den Anhörungen im amerikanischen Kongreß zum Erlaß des DCMA gesehen und erörtert, vgl. hierzu 111 F.Supp. 2d 294 (S.D.N.Y. 2000), S. 2 und 29, sowie *Nimmer,* A Riff on Fair Use in the Digital Millenium Copyright Act, 148 U. Pa. L. Rev. 673, 739 – 741 (2000

[36] Vgl. hierzu *Knies,* ZUM 2002, 793 ff.

[37] Dabei wird der Computer Code als die Abfolge von 0 (für „aus“) und 1 (für „an“) definiert, 111 F.Supp. 2d 294 (S.D.N.Y. 2000), S. 5.

[38] 111 F.Supp. 2d 294 (S.D.N.Y. 2000), S. 3, mit dem Hinweis, daß die Verfassung keinen „Selbstmord Pakt“ darstelle.

[39] The Digital Millenium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998).

Ebenso wie die Richtlinie der Gemeinschaft zur Informationsgesellschaft[40] schützt auch der Digital Millenium Copyright Act technische Maßnahmen von Herstellern, die diese sich haben einfallen lassen, um ihre Urheberrechte im digitalen Umfeld zu schützen. Damit wurde ein eher wettbewerbsrechtliches Nebengebiet in das Urheberrecht eingearbeitet. Ausgangspunkt der Überlegungen war, daß der Gesetzgeber von einer erhöhten Verletzlichkeit der Urheberrechte im digitalen Umfeld ausging. Wenn man sich schon nicht auf ein generelles Verbot der digitalen Privatkopie einigen konnte, so wollte man doch wenigstens den Herstellern und Rechteinhabern die Möglichkeit eröffnen, die digitale Kopie und die Verbreitung ihrer Inhalte mit technischen Schutzmaßnahmen zu verhindern.

Diese Schutzmaßnahmen selber genießen nun ihrerseits grundsätzlich den Schutz des amerikanischen, wie auch des europäischen Gesetzgebers. Sie haben ihren Ursprung in den beiden Verträgen der WIPO zum Schutz des Urheberrechtes in der Informationsgesellschaft, dem WIPO Tonträgervertrag WPPT[41] und dem Artikel 11 des WIPO-Urheberrechtsvertrages WCT von 1997.[42]

Der amerikanische Gesetzgeber hat in der Folge der beiden WIPO-Verträge zwei hier relevante Vorschriften zu den technischen Schutzmaßnahmen eingeführt, nämlich 17 U.S.C. § 1201 (a) (1), der den aktiven Vorgang des Umgehens der Schutzmaßnahme verhindern soll,[43] sowie den 17 U.S.C. § 1201 (a) (2), der schon die Bereitstellung von Technik zur Umgehung von Schutzmaßnahmen verhindern will. Die beiden Vorschriften ähneln von Aufbau und Systematik den europäischen Vorschriften aus der Richtlinie zur Informationsgesellschaft.[44]

Das New Yorker Gericht bejaht im Ergebnis das Vorliegen der gesetzlichen Voraussetzungen, daß nämlich zum einen CSS einen effektiven Schutz von urheberrechtlich geschütztem Material darstellt und zum anderen DeCSS nur dazu entwickelt wurde, um diesen Schutz zu umgehen.[45] Zutreffend stellt es fest, daß die Motivation der Schöpfer der DeCSS Software (nämlich einen auf Linux laufenden DVD-Player zu schaffen) für die Frage der rechtswidrigen Umgehung belanglos sei.[46] Mit dem Bereitstellen der DeCSS Software auf ihrem Server hätten die Beklagten also die Bestimmung des 17 U.S.C. 1201 (a)(2) verletzt.

---

[40] Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl. EG Nr. L 167 vom 22.6.2001.

[41] WIPO Performances and Phonogram Treaty vom 20. Dezember 1996, WIPO doc. CRNR/DC/95 vom 23.12.1996.

[42] WIPO Copyright Treaty vom 20.12.1996, WIPO Doc. CRNR/DC/94 vom 23.12.1996. Der Text des WCT findet sich auf der Webseite der WIPO unter http://clea.wipo.int/PDFFILES/English/WO/WO033EN.PDF. Zu diesen beiden Verträgen vgl. auch ausführlich *Knies,* Tonträgerherstellerrechte, S. 58 ff.

[43] Der Text der Vorschrift ist auf die aktive Umgehung der Schutzmaßnahme zugeschnitten.

[44] Vgl. hierzu unten 4. (a).

[45] 111 F.Supp. 2d 294 (S.D.N.Y. 2000), S. 30 ff.

[46] 111 F.Supp. 2d 294 (S.D.N.Y. 2000), S. 35, hierfür spricht auch, daß sich die Beklagten ja sehr einfach bei der Lizenzgeberin, der DVD CCA um eine (im übrigen nahezu kostenlose) Lizenz hätten bemühen können.

Auch die Ausnahmevorschriften sieht das Gericht als nicht einschlägig an,[47] wobei vorliegend insbesondere die fair-use-Ausnahme von Interesse ist. Fraglich war hier insbesondere die bereits oben aufgeworfene Frage, ob und inwieweit es den Rechteinhabern möglich sein solle, die gesetzlich vorgesehenen Schranken des Urheberrechts mit den Mitteln der Verschlüsselungstechnologie für den Verbraucher quasi nutzlos zu machen. Denn in der Tat kann dieser ja von der durch CSS geschützten DVD keine Privatkopie mehr herstellen. Das Gericht weist aber darauf hin, daß die fair-use-Ausnahme des 17 U.S.C. § 107 grundsätzlich nur für die Einschränkung von *Urheberrechten* gelte. Sie greife aber nicht als Ausnahme vom Schutz der spezialgesetzlich kodifizierten und geschützten „technischen Schutzmaßnahmen“, obwohl der Kongreß diese Problematik durchaus gesehen habe.[48]

Der amerikanische Gesetzgeber hat sich nämlich mit 17 U.S.C. § 1201(a)(1) dafür entschieden den „fair use“ nur dann zuzulassen, wenn der Rechteinhaber dem Nutzer einmal den Zugang zu dem geschützten Werk gestattet hat. In diesem Fall soll der Nutzer, wenn dies technisch möglich ist, auch die Ausnahmevorschriften nutzen können.[49] Schützt er den Inhalt aber einmal über die (ihrerseits gesetzlich geschützte) technische Maßnahme (wie etwa CSS), dann soll der Inhalt eben auch nicht über den „fair use“ zugänglich oder gar privat kopierbar sein.

d. Verstoß gegen das Umgehungsverbot durch das Verlinken auf andere Sites

Die zweite Frage, die das Gericht zu entscheiden hatte war diejenige, ob die Beklagten durch die auf www.2600.com gelegten Links auf andere Websites, die die DeCSS-Software ebenfalls zum Download anbieten, auch gegen die oben genannten Vorschriften verstoßen, ob man also in diesen Links ein Anbieten der verletzenden DeCSS-Software an die Öffentlichkeit im Sinne der Vorschrift des 17 U.S.C. § 1201 (a) sehen könne oder nicht. Das Gericht bejaht diese Frage grundsätzlich, wobei es aber einen Unterschied mache, welchen Inhalt die Seiten hätten, auf die mit dem Link hingewiesen werde.[50] Das Gericht unterscheidet zwischen Links auf Websites, die automatisch mit dem Download der DeCSS-Software beginnen, solchen, die noch einen Klick des Users anfordern und jenen, die neben der DeCSS-Software auch noch anderen Inhalt bieten. Diese Unterscheidung dürfte allerdings im Ergebnis wenig tragfähig sein, da dann die Verantwortlichkeit dessen, der den Link legt, stark davon abhängt, was sich aktuell auf der Website befindet, auf die dieser Link zeigt.

Die Entscheidung des United State District Court hat auch in der Berufungsinstanz gehalten. Sie wurde am 28. November 2001 vom United States Court of Appeal Second Circiut bestätigt.[51] Damit ist die weitere Verbreitung der DeCSS-Software in Amerika illegal, die Filmindustrie hat einen wichtigen Sieg zum Schutz ihres verletzlichen Inhaltes erzielt.

---

[47] Die Beklagten hatten sich neben der fair-use-Ausnahme auf die Ausnahmevorschrift des „reverse engeneering“ des 17 U.S.C. § 1201 (f) berufen, die Umgehungsmaßnahmen dann gestattet, wenn sie lediglich Interoperabilität zwischen verschiedenen Systemen schaffen wollen.

[48] 111 F.Supp. 2d 294 (S.D.N.Y. 2000), S. 42 f. Man habe die Aushöhlung der „fair use“-Vorschriften bewußt in Kauf genommen.

[49] Vgl. hierzu die Darstellung bei 111 F.Supp. 2d 294 (S.D.N.Y. 2000), S. 43.

[50] 111 F.Supp. 2d 294 (S.D.N.Y. 2000), S. 48 f.

[51] 2001 WL 1505495 (2nd Cir.(N.Y.).

3. Rechtsbehelfe in Deutschland gegen die Verbreitung von DeCSS

Auch auf deutschen und europäischen Servern kann man heute recht schnell die streitige DeCSS-Software finden. Die MPAA hat auch schon damit begonnen, Abmahnschreiben an die Betreiber dieser Websites zu versenden, wobei man sich allerdings nur auf das amerikanische Recht bezieht, und damit in Deutschland wohl kaum echte Erfolgsaussichten haben wird.[52]

Im folgenden soll deshalb untersucht werden, ob das Bereitstellen der DeCSS-Software auf deutschen Servern nach deutschem Recht unterbunden werden könnte.

a. Die Regelungen der Richtlinie zur Informationsgesellschaft

Vorschriften, die einen eigenständigen gesetzlichen Rechtsschutz von technischen Schutzsystemen wie CSS bieten, finden sich in der Richtlinie der Gemeinschaft zur Informationsgesellschaft.[53] Ebenso wie das amerikanische Pendant haben diese zunächst wenig beachteten Vorschriften ihren Ursprung in den beiden WIPO-Verträgen. Die Richtlinie baut (wie das amerikanische Recht) einen zweistufigen Schutz des Schutzsysteme auf. Zum einen soll nach Art. 6 Abs. 1 der Richtlinie die aktive Umgehung des technischen Schutzes unterbunden werden. Art. 6 Abs. 2 der Richtlinie hingegen soll Vorbereitungshandlungen verhindern, wie etwa das Angebot von Technik oder Systemen mit denen die geschützte technische Maßnahme umgangen werden kann. Diese Vorschriften der Richtlinie sollen nach dem Gesetzentwurf der Bundesregierung vom 6.11.2002[54] in einen neuen § 95 a des UrhG einfließen. Nach dem RegE § 95 a Abs. 1 dürfen technische Maßnahmen nicht umgangen werden, nach Abs. 2 sind auch die Verbreitung, Einfuhr und Herstellung solcher primär auf die Umgehung abzielender Systeme rechtswidrig.[55]

Ein System wie CSS, das den Zugriff auf den Inhalt der DVD durch Verschlüsselung sperrt und gleichzeitig Vervielfältigung und digitale Verbreitung steuert, fällt klar unter die vom RegE gewählte Definition. Die Verbreitung des Codes oder des DeCSS-Programms ließe sich über den § 95a Abs. 2 RegE unterbinden.

Der Verstoß gegen die Vorschriften kann nach § 95b RegE mit zivilrechtlicher Unterlassungsklage und nach § 108b RegE auch mit strafrechtlicher Sanktion verfolgt werden.

---

[52] Vgl. etwa Heise Newsticker vom 31.8.2000, www.heise.de/newsticker/data/ghi-31.08.00-000/.

[53] Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl. EG Nr. L 167 vom 22.6.2001.

[54] Gesetzentwurf der Bundesregierung BT DRs. 15/38, vgl. http://www.urheberrecht.org/topic/Info-RiLi/ent/1500038.pdf.

[55] § 95a Abs. 2 RegE definiert den Schutz der technischen Maßnahme sehr breit wie folgt: „Technologien, Vorrichtungen und Bestandteile, die im normalen Betrieb dazu bestimmt sind, Werke oder andere Schutzgegenstände betreffende Handlungen zu verhindern oder einzuschränken, die nicht vom Rechtsinhaber genehmigt sind (technische Schutzmaßnahmen), dürfen ohne Zustimmung des Rechtsinhabers nicht umgangen werden, soweit durch sie die Nutzung eines geschützten Werkes oder eines sonstigen Schutzgegenstandes von dem Rechtsinhaber durch eine Zugangskontrolle, einen Schutzmechanismus wie Verschlüsselung, Verzerrung oder sonstige Umwandlung oder einen Mechanismus zur Kontrolle der Vervielfältigung, die das Erreichen des Schutzziels sicherstellt, unter Kontrolle gehalten wird."

Die Frage, ob innerhalb dieses Schutzsystems dem Verbraucher zwingend die Möglichkeit gewährt werden muß, sein „Recht“ auf die Privatkopie einzufordern, wird von der deutschen Umsetzungsgesetzgebung nicht thematisiert. Diese Frage wird in der komplizierten Regelung des Art. 6 Abs. 4 der Richtlinie behandelt, wobei aber ein Anspruch des Verbrauchers auf die Privatkopie derzeit wohl letztlich verneint werden muß.[56]

b. Ergebnis

Das (künftige) deutsche Recht wird also im Ergebnis, ebenso wie das amerikanische Recht, die Verbreitung der DeCSS-Software nicht gestatten. Auch im deutschen Recht würde ein „Anspruch“ des Verbrauchers auf die Privatkopie gegenüber dem vorrangigen Schutz dessen zurücktreten, der seine Inhalte mit technischen Schutzmaßnahmen, wie dem CSS-Programm oder analogen Kopierschutzmechanismen wie denen von Macrovision schützt. Die Debatte über die Tragweite des technischen Schutzes im Verhältnis zu den Ansprüchen der Öffentlichkeit auf freien Informationszugang steckt aber gewiß noch in den Kinderschuhen. Mit dem technischen Schutzniveau selbst mag die Industrie den „Normalverbraucher“ von der Privatkopie abhalten, den Hacker und den technischen Freak wird jedes neue Schutzsystem aber eher anspornen. Die Problematik wird uns also gewiß erhalten bleiben, gleich ob digital oder analog.

[56] Vgl. hierzu die detaillierte Darstellung bei *Knies,* ZUM 2002, 793 ff.