Lars Rau

Phänomenologie und Bekämpfung von ‘Cyberpiraterie’

Eine kriminologische und kriminalpolitische Analyse

Cuvillier Verlag Göttingen

Illegale Beschaffung und Distribution von Schutzgegenständen geistigen Eigentums über das Internet haben sich spätestens seit dem Siegeszug der sogenannten Online-Tauschbörsen (P2P-Filesharing-Systeme) zu einem regelrechten Massenphänomen entwickelt.

Die vorliegende Arbeit untersucht die vielfältigen Tatbegehungsmodalitäten, die Täterstruktur und -motivation, die Auswirkungen von Cyberpiraterie sowie Bekämpfungs- und Überwachungsstrategien bezüglich des Problems. Neben einer kritischen Beurteilung der strafrechtlichen Situation enthält die Arbeit auch eigene Lösungsvorschläge.

Angesichts der starken Dynamik des Themenkreises ist bei der Wahl der Bekämpfungsstrategien stets die aktuelle digitale Realität zu berücksichtigen. Der Wahlspruch der Verwertungsgesellschaften, wonach „das Schützbare zu schützen und das Nicht-Schützbare zu vergüten" ist, scheidet in diesem Zusammenhang die Geister. Während die Vertreter der Unterhaltungsindustrie sämtliche digitalen Werke für schützbar erklären, zeigt die vorliegende Arbeit exemplarisch auf, dass ein umfassender Schutz digitaler Inhalte im Internet zur Zeit weder rechtlich noch technisch durchsetzbar ist.

Nicht nur aus diesem Grund sondern auch aus rechtspolitischen und kriminologischen Erwägungen ist es dringend geboten, zivilrechtliche Alternativen zu dem derzeit eingeschlagenen, strafrechtlichen Weg zu etablieren.

ISBN 3-86537-246-5

Lars Rau

Phänomenologie und Bekämpfung von ‘Cyberpiraterie’

Eine kriminologische und kriminalpolitische Analyse

Inauguraldissertation zur Erlangung des Doktorgrades
am Fachbereich Rechtswissenschaften der *Justus-Liebig-Universität* Gießen

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

1. Aufl. – Göttingen : Cuvillier, 2004
Zugl.: Gießen, Univ., Diss., 2004
ISBN 3-86537-246-5

Nonnenstieg 8, 37075 Göttingen
Telefon: 0551-54724-0
Telefax: 0551-54724-21
www.cuvillier.de

1. Auflage, 2004

ISBN 3-86537-246-5

Vorwort

Die Bearbeitung eines Themas mit Internetbezug bringt es mit sich, dass häufig technische Details zur Sprache kommen, die nicht jedem Leser bekannt sein können. Daher habe ich mich entschieden, der Arbeit einen einführenden Teil voranzustellen, der die wichtigsten technischen Zusammenhänge erläutert. IT-bewanderte Leser können diesen Teil getrost überspringen und die Lektüre auf Seite 26 beginnen. Leser mit normalen IT-Kenntnissen erhalten mit dem ersten Teil eine Möglichkeit zum Nachschlagen.

Mein herzlicher Dank gilt Herrn *Prof. Dr. Edwin Kube*, *BKA*-Abteilungspräsident a.D., für die freundliche Betreuung des Promotionsvorhabens, die Möglichkeit der freien Themenwahl und die Erstellung des Erstgutachtens.
Besonderen Dank schulde ich Herrn *Prof. Dr. Arthur Kreuzer*, Direktor des *Instituts für Kriminologie an der Justus-Liebig-Universität Gießen e.V.*, sowie Herrn *Prof. Dr. Bernhard Jestaedt*, Richter am *Bundesgerichtshof*, für die Übernahme der Koreferate und ihre wertvollen Anregungen.

Schließlich danke ich Herrn *Ing. Roland Rau* und Frau *Margrit Rau* für Ihre stetige Unterstützung.
Ihnen ist diese Arbeit gewidmet.

Weilburg, im September 2004

Lars Rau
(lr@rau-online.de)

Inhaltsverzeichnis

Seitenzahl

Literaturverzeichnis

Ahlf, Ernst-Heinrich / u.a. (Hrsg.)
Bundeskriminalamtgesetz - BKAG,
Stuttgart, München, Hannover, Berlin, Weimar, Dresden 2000.
(zitiert: Ahlf-*Bearbeiter*)

Bager, Jo
Orientierungslose Infosammler – Warum die Suche im Internet oft mühsam geht und was die Suchmaschinen dagegen tun,
c't 23/1999, S. 158-161.

Bager, Jo / Kossel, Axel
Die Software-Vermieter – Application Service Provider: Anwendungen, Technik, Risiken,
c't 7/2001, S. 190-194.

Bager, Jo / Mansmann, Urs
Nachrichten-Dienst – Das Usenet in der Praxis,
c't 18/2002, S. 102-107.

Barlow, John Perry
The Economy of Ideas - A framework for patents and copyrights in the Digital Age (Everything you know about intellectual property is wrong),
Wired Magazine, 2.03 – März 1994,
http://www.wired.com/wired/archive/2.03/economy.ideas.html.

Baumbach, Adolf / Hefermehl, Wolfgang
Wettbewerbsrecht: Gesetz gegen den unlauteren Wettbewerb, Zugabeverordnung, Rabattgesetz und Nebengesetze,
22. Auflage, München 2001.

Bayreuther, Frank
Beschränkungen des Urheberrechts nach der neuen EU-Urheberrechtsrichtlinie,
ZUM 2001, S. 828-839.

Becker, Jürgen
Neue Übertragungstechniken und Urheberschutz,
ZUM 1995, S. 231-249.

Berger-Zehnpfund, Petra
Kinderpornographie im Internet – Rechtliche Aspekte der Bekämpfung des Kindesmissbrauchs in internationalen Datennetzen,
Kriminalistik 1996, S. 635-639.

Beucher, Klaus / Engels, Stefan
Harmonisierung des Rechtsschutzes verschlüsselter Pay-TV-Dienste gegen Piraterieakte,
CR 1998, S. 101-110.

Bleich, Holger
Schlüsselfreigabe – Krypto-Export aus den USA soll erleichtert werden,
c't 3 /2000, S. 41.
(zitiert: *Bleich*, Schlüsselfreigabe)

ders.
Selbstverdunkelung – Anonymes Mailen in der Praxis,
c't 16/2000, S. 156-159.
(zitiert: *Bleich*, Selbstverdunkelung)

Blittkowsky, Ralf
Gefilterte Informationen – China und die Menschenrechte im Internet,
c't 9/1999, S. 74-79.

Blümel, Markus / Soldo, Erwin — Internet für Juristen - Online-Einstieg leicht gemacht, Köln, Berlin, Bonn, München, 1998.

Bögeholz, Harald — Datentresor – Hardware-Kopierschutz für Festplatten, **c't** 2/2001, S. 24-25.

Bortloff, Nils — Erfahrungen mit der Bekämpfung elektronischer Musikpiraterie im Internet, **GRUR Int.** 2000, S. 665-672.

Bosak, Jan Michael — Urheberrechtliche Zulässigkeit privaten Downloadings von Musikdateien, **CR** 2001, S. 176-181.

Boutin, Paul — The RIAA's Low Watermark – The SDMI Challenge produced scientific evidence that encryption can't stop piracy. So the industry tried a new tool to secure digital music: censorship, **Wired Magazine**, 9.07 - Juli 2001, http://www.wired.com/wired/archive/9.07/mustread.html.

Brauch, Patrick — „IRC wird irgendwie fortbestehen" – Ein Interview mit Volker Paulsen, gewählter IRCnet-Koordinator für Deutschland, über die Zukunft des IRC, **c't** 11/2000, S. 112-113. (zitiert: *Brauch*, „IRC wird irgendwie fortbestehen")

ders. — Kaputt gespielt – Angriffe gegen Chat-Server bedrohen Fortbestand des freien Kommunikationsdienstes IRC, **c't** 11/2000, S. 110-112. (zitiert: *Brauch*, Kaputt gespielt)

ders. — Schutz vor Schmutz? – Was Internet-Filtersoftware in der Praxis taugt, **c't** 23/2000, S. 230-238. (zitiert: *Brauch*, Schutz vor Schmutz?)

Bremer, Lars — XP-Aktivierung entschlüsselt – Welche Daten die Windows-Produkt-ID enthält, **c't** 15/2001, S. 17.

Brors, Dieter — Zwangsmaßnahmen – Registrierungspflicht für Standardsoftware, **c't** 26/1998, S. 17.

Busse, Rudolf — Patentgesetz, 5. Auflage, Berlin, New York 1999.

Carstens, Matthias — Musik kompakt – Audio-Kompression mit MPEG Layer-3, **c't** 21/1998, S. 242-250.

Creifelds, Carl / Weber, Claus (Hrsg.) — Creifelds Rechtswörterbuch, 17. Auflage, München 2002.

Dallinger, Wilhelm — Aus der Rechtsprechung des Bundesgerichtshofs in Strafsachen, **MDR** 1975, S. 722-726.

Dambeck, Holger — Tausch-Angst – Filmbranche nimmt File-Sharing-Nutzer ins Visier, **c't** 4/2002, S. 42. (zitiert: *Dambeck*, Tausch-Angst – Filmbranche nimmt File-Sharing-Nutzer ins Visier)

ders. — Teurer Spaß – Homepage und Urheberrecht, **c't** 25/2001, S. 236-238. (zitiert: *Dambeck*, Teurer Spaß – Homepage und Urheberrecht)

Dannecker, Gerhard — Neuere Entwicklungen im Bereich der Computerkriminalität: Aktuelle Erscheinungsformen und Anforderungen an eine effektive Bekämpfung, **BB** 1996, S. 1285-1294.

Decius, Marc / Panzieri, Ralf — Kinderpornographie im Internet Relay Chat – Nutzung des Chat-mediums IRC (Internet Relay Chat) für die illegale Verbreitung kinderpornographischer Bild- und Videodateien, Studie im Auftrag des Deutschen Kinderschutzbundes e.V. - in der Fassung vom 01.04.1998, anzufordern unter http://www.dksb.de.

Decker, Ute — Haftung für Urheberrechtsverletzungen im Internet – Anforderungen an die Kenntnis des Host Providers, **MMR** 1999, S. 7-14.

Demuth, Thomas — Unerkannt surfen – Privatsphäre im World Wide Web, **c't** 6/2000, S. 196-201.

Diedrich, Oliver — Die Halloween-Dokumente – Microsoft-Analysen zu Linux und Open-Source-Software, **c't** 24/1999, S. 52-53.

Diesler, Peter — Razzia im Sündenpfuhl – Sex im Netz, **CHIP** 11/1995, S. 51-55.

Dreier, Thomas — Rechtsschutz von Computerprogrammen – Die Richtlinie des Rates der EG vom 14. Mai 1991, **CR** 1991, S. 577-584. (zitiert: *Dreier*, Rechtsschutz von Computerprogrammen)

ders. — Urheberrecht an der Schwelle des 3. Jahrtausends – einige Gedanken zur Zukunft des Urheberrechts, **CR** 2000, S. 45-49. (zitiert: *Dreier*, Urheberrecht an der Schwelle des 3. Jahrtausends)

ders. — Verletzung urheberrechtlich geschützter Software nach der Umsetzung der EG-Richtlinie, **GRUR** 1993, S. 781-792. (zitiert: *Dreier*, Verletzung urheberrechtlich geschützter Software nach der Umsetzung der EG-Richtlinie)

Eichenberg, Christiane / Ott, Ralf — Suchtmaschine – Internetabhängigkeit: Massenphänomen oder Erfindung der Medien?
c't 19/1999, S. 106-111.

Eisenberg, Ulrich — Kriminologie,
5. Auflage, München 2000.

Ekey, Friedrich L. / Klippel, Diethelm /Kotthoff, Jost / Meckel, Astrid /Plaß, Gunda — Heidelberger Kommentar zum Wettbewerbsrecht,
Heidelberg 2000.
(zitiert: HK Wettbewerbsrecht-*Bearbeiter*)

Elschner, Günter / Schuhmacher, Dirk — Checkliste für Rechenzentren (fortgeführt von *Eppe, Mark / Lehnhardt, Joachim*),
Veröffentlicht auf der Homepage des Deutschen Forschungsnetzes,
http://www.dfn.de/content/beratung-weiterbildung/rechtimdfn/checkliste.

Engel, Christoph — Inhaltskontrolle im Internet,
AfP 1996, 220-227.

Ermert, Monika — Antiautoritäres Filtersystem – ICRASafe soll „Selbstregulierung im Internet" sichern,
c't 20/2000, S. 28-29.
(zitiert: *Ermert*, Antiautoritäres Filtersystem)

dies. — „Das Kopieren von digitalen Inhalten lässt sich nicht verhindern",
Gespräch mit Ross Anderson,
c't 12/2001, S. 54.
(zitiert: *Ermert*, „Das Kopieren von digitalen Inhalten lässt sich nicht verhindern")

dies. — IPv6 auf allen Kanälen – Die Einführung des neuen IP-Standards drängt,
c't 1/2000, S. 32-34.
(zitiert: *Ermert*, IPv6 auf allen Kanälen)

dies. — Web-Taufpaten – Das Rennen um neue Top Level Domains ist eröffnet,
c't 16/2000, S. 42.
(zitiert: *Ermert*, Web-Taufpaten)

Erne, Markus — Lean Listening – Datenreduktion – die Technik von MPEG-Audio,
KEYS 2/1999, S. 34-38.

Federrath, Hannes / Berthold, Oliver / Köhntopp, Marit / Köpsell, Stefan — Tarnkappen fürs Internet – Verfahren zur anonymen und unbeobachteten Kommunikation,
c't 16/2000, S. 148-155.

Feuerbach, Heinrich T. / Schmitz, Peter — Freiheitskämpfer – Entwickler freier Software gegen Patentierung,
c't 16/1999, S. 79-81.

Fezer, Karl-Heinz — Markenrecht - Kommentar zum Markengesetz, zur Pariser Verbandsüber-einkunft und zum Madrider Markenabkommen,
3. Auflage, München 2001.

Flechsig, Norbert P./ Gabel, Detlev Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks,
CR 1998, S. 351-358.

Flechsig, Norbert P. Rechtmäßige private Vervielfältigung und gesetzliche Nutzungsgrenzen - Zur Frage, in welchem Umfang privat hergestellte Vervielfältigungsstücke einer außerprivaten Nutzung zugeführt werden dürfen und zur Beweislast im Urheberverletzungsprozess,
GRUR 1993, S. 532-538.

Franzheim, Horst Strafrechtliche Konsequenzen der Urheberrechtsnovelle,
NJW-CoR 1994, S. 160-164.
(zitiert: *Franzheim*, Strafrechtliche Konsequenzen der Urheberrechtsnovelle)

ders. Überkriminalisierung durch Urheberrechtsnovelle
CR 1993, S. 101-103.
(zitiert: *Franzheim*, Überkriminalisierung durch Urheberrechtsnovelle)

Fremerey, Frank Gefahren und Chancen – Hackerkongress zwischen Kreativität und Paranoia,
c't 2/1999, S. 28.
(zitiert: *Fremerey*, Gefahren und Chancen)

ders. Rauben und Kopieren – Softwarepiraten in den Netzen ihrer Verfolger,
c't 8/2000, S. 98-103.
(zitiert: *Fremerey*, Rauben und Kopieren)

Fromm, Friedrich Karl / Nordemann, Wilhelm Kommentar zum Urheberrechtsgesetz und zum Urheberrechtswahrnehmungsgesetz,
9. Auflage, Stuttgart, Berlin, Köln 1998.
(zitiert: Fromm/Nordemann-*Bearbeiter*)

Fryer, Bronwyn The Software Police,
Wired Magazine 3.05 – Mai 1995,
http://www.wired.com/wired/archive/3.05/police.html.

Garfinkel, Simson L. Good Clean PICS - The most effective censorship technology the Net has ever seen may already be installed on your desktop,
Hotwired Network, Mai 1997,
http://www.hotwired.com/packet/garfinkel/97/05/index2a.html.
(zitiert: *Garfinkel*, Good Clean PICS)

ders. Is Stallman Stalled?,
Wired Magazine 1.01 – März/April 1993,
http://www.wired.com/wired/archive/1.01/stallman.html.
(zitiert: *Garfinkel*, Is Stallman Stalled?)

ders. Wer regiert das Internet?
konr@d April/Mai 1999, S. 54-61, in der Übersetzung von *Philipp Oehmke*.
(zitiert: *Garfinkel*, Wer regiert das Internet?)

Glaser, Peter — E-Mail und die Detektive,
konr@d August/September 1999, S. 106-109.
(zitiert: *Glaser*, E-Mail und die Detektive)

ders. — So hat der Sex das Netz gemacht,
konr@d Oktober/November 1999, S. 26-29.
(zitiert: *Glaser*, So hat der Sex das Netz gemacht)

Gleich, Clemens — Entfesselte Musik – Microsofts neues Digital Rights Management ausgehebelt,
c't 23/2001, S. 62.

Godwin, Mike — Coming Soon: Hollywood Versus the Internet,
veröffentlicht auf der Homepage von *Cryptome*,
http://www.cryptome.org/mpaa-v-net-mg.htm

Goltzsch, Patrick — Nationales Internet,
Telepolis vom 24.02.2000,
http://www.heise.de/tp/deutsch/inhalt/te/5833/1.html.

Goos, Hauke — Die Zukunft des Verbrechens,
SPIEGEL Online vom 29.02.2000,
http://www.spiegel.de/reporter/0,1518,65892,00.html.

Gorman, Greg / Lober, Andreas — Gewalt im Spiel – Indizierung und Beschlagnahme von Software,
c't 11/1999, S. 82-89.

Gounalakis, Georgios / Rhode, Lars — Haftung des Host-Providers: Ein neues Fehlurteil aus München?
- Besprechung des Grundurteils des LG München I vom 30.03.2000 (Az. 7 O 3625/98 - abgedruckt in **NJW** 2000, S. 2214),
NJW 2000, S. 2168-2171.

Gravenreuth, Günter Freiherr von — Anmerkung zum Urteil des AG München vom 28.05.1998 (Az. 8340 Ds 465 Js 173158/95 - abgedruckt in **CR** 1998, S. 500-505),
CR 1998, S. 628-629.
(zitiert: *Gravenreuth*, Anmerkung zum Urteil des AG München vom 28.05.1998)

ders. — Computerviren, Hacker, Datenspione, Crasher und Cracker,
NStZ 1989, S. 201-207.
(zitiert: *Gravenreuth*, Computerviren, Hacker, Datenspione, Crasher und Cracker)

ders. — Juristisch relevante technische Fragen zur Beurteilung von Computer-Programmen,
GRUR 1986, S. 720-727.
(zitiert: *Gravenreuth*, Juristisch relevante technische Fragen zur Beurteilung von Computer-Programmen)

ders. — Neue Formen der Softwarepiraterie,
CR 1995, 309-310.
(zitiert: *Gravenreuth*, Neue Formen der Softwarepiraterie)

Green, Dave
Demo or Die! – You're a teen hacker, you want to impress, you demo code,
Wired Magazine 3.07 – Juli 1995,
http://www.wired.com/wired/archive/3.07/democoders.html.

Gruhler, Andreas
PICS – eine moderne Version der Zensur? – Das technische Konzept eines umstrittenen Kontrollinstruments und seine Auswirkungen auf die Netzwelt,
Telepolis vom 07.05.1998,
http://www.heise.de/tp/deutsch/inhalt/te/1464/1.html.

Grzeszik, Bernd
Freie Software: Eine Widerlegung der Urheberrechtstheorie?
MMR 2000, S. 412-417.

Günther, Andreas
Anmerkung zum Urteil des OLG Karlsruhe vom 13.06.1994 (Az. 6 U 52/94 – abgedruckt in **CR** 1994, S. 607-611),
CR 1994, S. 611-616.

Gunther, Bernhard
Piraten - Vom Gold der Inkas bis zum geistigen Eigentum. Die Geschichte einer verwegenen Metapher,
Telepolis vom 24.09.2001,
http://www.heise.de/tp/deutsch/inhalt/te/9608/1.html.

Günnewig, Dirk / Hauser, Tobias
Musik im Hochsicherheitstrakt – Digital Rights Management – Stand der Dinge,
c't 16/2002, S. 182-185.

Günnewig, Dirk / Hauser, Tobias / Himmelein, Gerald
Digitale Rechte am Scheideweg – Rechtsschutz für DRM-Systeme in den Bundestag eingebracht,
c't 17/2002, S. 18-20.

Gwennap, Linley
Pentium III Serial Number Is Just a Tool – But Is It a Can Opener or a Gun?,
Microprocessor Report, Editorial vom 15.02.1999,
http://www.mdronline.com.

Haberstumpf, Helmut
Zur urheberrechtlichen Beurteilung von Programmen für Datenverarbeitungsanlagen,
GRUR 1982, S. 142-151.

Hahn, André / Jerusalem, Matthias
Internetsucht: Jugendliche gefangen im Netz,
Berlin 2001,
veröffentlicht auf der Homepage des Vereins *mediarisk international*,
http://www.onlinesucht.de/internetsucht_preprint.pdf.

Hansen, Sven
Musik mit weißer Weste – Kommerzielle Musikangebote im Netz,
c't 16/2002, S. 70-73.

Harbonn, Jacques
Kopierschutztechniken für Audio-CDs,
ZDNet.de – Produkte & Tests,
http://produkte.zdnet.de/test/76/1/1365.html.

Harbort, Stephan — Verbrechen im Cyberspace – Neue Erscheinungsformen zeitspezifischer Computerkriminalität,
Kriminalistik 1996, S. 194-198.

Harke, Dietrich — Musikkopien – illegal? – Zum Download von MP3-Dateien und zum Kopieren von Musik-CDs,
c't 5/2000, S. 112-114.

Heghmanns, Michael — Strafrechtliche Verantwortlichkeit für illegale Inhalte im Internet,
JA 2001, S. 71-78.

Heib, Andreas — 98 die Zweite – Was die zweite Ausgabe von Windows98 bringt,
c't 15/1999, S. 86-91.

Heinzmann, Peter L. / Ochsenbein, Andreas — Strafrechtliche Aspekte des Internet – Technische und rechtliche Grundlagen – Teil 1,
Kriminalistik 1998, S. 513-520.
(zitiert: *Heinzmann/Ochsenbein,* Strafrechtliche Aspekte des Internet – Teil 1)

dieselben — Strafrechtliche Aspekte des Internet – Technische und rechtliche Grundlagen – Teil 2,
Kriminalistik 1998, S. 599-606.
(zitiert: *Heinzmann/Ochsenbein,* Strafrechtliche Aspekte des Internet – Teil 2)

Hellmich, Foelke — Von Raubkopien und GEMA-Gebühren,
c't 21/1998, S. 136.

Herberger, Scania — Wirksamkeit von Sanktionsdrohungen gegenüber Kindern, Jugendlichen und Heranwachsenden im Hinblick auf Normbekräftigung und normkonformes Verhalten – Analyse des möglichen Beitrags des Strafrechts zur Normbekräftigung unter Berücksichtigung von Aspekten der moralischen Entwicklung,
München 2000.

Heymann, Thomas — Bundles, Bytes und Paragrafen – Rechtsfragen der Softwarenutzung,
c't 8/2000, S. 104-109.

Himmelein, Gerald / Schmitz, Peter — Fast alles ist verboten – Der Rechtsstatus von Privatkopien vor der Umsetzung der EU-Richtlinie,
c't 2/2002, S. 82-85.

Himmelein, Gerald / Vahldiek, Axel — CDs auf die Platte – Zehn CD-Emulatoren für Windows,
c't 17/2002, S. 122-127.

Himmelein, Gerald — Der digitale Knebel – Intel und Microsoft wollen Daten vor dem Anwender schützen,
c't 15/2002, S. 18-20.
(zitiert: *Himmelein*, Der digitale Knebel)

ders. — Geschenk mit Pferdefuß – Rights Management im Online-Fanclub, **c't** 13/2001, S. 39. (zitiert: *Himmelein*, Geschenk mit Pferdefuß)

ders. — Sind wir alle kriminell? – Gesetzesänderungen und Kopiersperren sollen Raubkopien vereiteln, **c't** 2/2002, S. 80-81. (zitiert: *Himmelein,* Sind wir alle kriminell?)

ders. — Volle Kontrolle, Editorial **c't** 14/2001, S. 3. (zitiert: *Himmelein*, Volle Kontrolle)

Hoeren, Thomas / Sieber, Ulrich (Hrsg.) — Handbuch Multimedia-Recht, 4. Auflage, München 2003 (Stand: November 2002) (zitiert: Hoeren/Sieber-*Bearbeiter*)

Hoeren, Thomas — Anmerkung zum Urteil des OLG München vom 08.03.2001 (Az. 29 U 3282/00), **MMR** 2001, S. 379-381. (zitiert: *Hoeren*, Anm. zum Urteil des OLG München)

ders. — Das Internet für Juristen – eine Einführung, **NJW** 1995, S. 3295-3298. (zitiert: *Hoeren,* Das Internet für Juristen)

Horvath, John — Die Gleichmacher - In Osteuropa ist Software-Piraterie ein Lebensstil (aus dem Englischen übersetzt von *Florian Rötzer*), **Telepolis** vom 18.12.1997, http://www.heise.de/tp/deutsch/inhalt/te/1356/1.html.

Howard-Spink, Sam — Labels focusing attention on CD copy-protection, **Music Business International**, October 2001, S. 53-55.

Jaeger, Stefan — Gesetze und Lücken, Rechtliche Schritte gegen Angriffe im Netz, **c't** 4/1999, S. 232-238. (zitiert: *S. Jaeger*, Gesetze und Lücken)

ders. — Grund zur Sorge? – Computerkriminalität erneut gestiegen, **c't** 17/1998, S. 176. (zitiert: *S. Jaeger*, Computerkriminalität erneut gestiegen)

ders. — Kleingedrucktes – Über den Umgang der Internet-Diensteanbieter mit Vertragsklauseln, **c't** 19/1999, S. 262-264. (zitiert: *S. Jaeger*, Kleingedrucktes)

Jaeger, Til — Zwang zur Freiheit – Freie Software als Ausweg aus dem Lizenzterror, **c't** 8/2000, S. 120-122. (zitiert: *T. Jaeger*, Zwang zur Freiheit)

Janovsky, Thomas — Internet und Verbrechen – Die virtuelle Komponente der Kriminalität, **Kriminalistik** 1998, S. 500-504.

Janssen, Dirk — Die Regulierung abweichenden Verhaltens im Internet – Eine Untersuchung verschiedener Regulierungsansätze unter Berücksichtigung der deutschen Rechtsordnung, Baden-Baden 2003.

Jestaedt, Bernhard — Die erfinderische Tätigkeit in der neueren Rechtsprechung des Bundesgerichtshofs, **GRUR** 2001, S. 939-944.

Kindermann, M. — Vertrieb und Nutzung von Computersoftware aus urheberrechtlicher Sicht, **GRUR** 1983, S. 150-161.

Koch, Alexander — Grundrecht auf Verschlüsselung? **CR** 1997, S. 106-110, auch veröffentlicht auf laWWW.de, http://lawww.de/Library/Krypto/index.shtml (zitiert: *A. Koch,* Grundrecht auf Verschlüsselung?)

Koch, Frank A. — Das neue Softwarerecht und die praktischen Konsequenzen, **NJW-CoR** 1994, S. 293-300. (zitiert: *F. A. Koch*, Das neue Softwarerecht und die praktischen Konsequenzen)

ders. — Urheber- und kartellrechtliche Aspekte der Nutzung von Open-Source-Software (Teil 1), **CR** 2000, S. 273-281. (zitiert: *F. A. Koch*, Urheber- und kartellrechtliche Aspekte der Nutzung von Open-Source-Software - Teil 1)

Köhn, Rüdiger / Theurer, Marcus — Sind CDs in Deutschland zu teuer? – Handel beklagt Preissteigerungen / Musikindustrie hält dagegen, **FAZ** vom 20.11.2001, S. 30.

Köhntopp, Marit / Köhntopp, Kristian — Datenspuren im Internet, **CR** 2000, S. 248-257.

König, M. Michael — Anmerkung zum Urteil des LG Mannheim vom 20.01.1995 (Az. 7 O 197/94), **NJW-CoR** 1995, S. 191. (zitiert: *M. M. König*, Anmerkung zum Urteil des LG Mannheim vom 20.01.1995)

ders. — Schuss nach hinten – Über das Vermieten von Software, **c't** 16/1999, S. 162-163. (zitiert: *M. M. König*, Schuss nach hinten)

ders. — Zur Zulässigkeit der Umgehung von Software-Schutzmechanismen, **NJW** 1995, S. 3293-3295. (zitiert: *M. M. König*, Zur Zulässigkeit der Umgehung von Software-Schutzmechanismen)

König, Volker — Im Netz verfangen - Stiften Softwarefahnder zu Straftaten an? **c't** 1/1994. S. 46-47.

Kohler, Josef — Urheberrecht an Schriftwerken und Verlagsrecht, Stuttgart 1907.

Kornmeier, Udo — Nutzungsrechte bei Multimedia-Auswertungen, in: *Moser, Rolf / Scheuermann, Andreas* (Hrsg.), Handbuch der Musikwirtschaft, 5. Auflage, Starnberg 1999.

Kossel, Axel — Ein waches Auge – Kalkuliertes Risiko beim Internet-Zugang, **c't** 3/1999, S. 142-145.

Krempl, Stefan — Content an der Kette – Die schöne neue Welt digitaler Rechte, **c't** 4/2002, S. 32-33. (zitiert: *Krempl*, Content an der Kette)

ders. — Die große Filteroffensive – Großindustrie und Politik wollen mit unliebsamen Inhalten im Internet aufräumen, **Telepolis** vom 10.09.1999, http://www.heise.de/tp/deutsch/inhalt/te/5277/1.html. (zitiert: *Krempl*, Die große Filteroffensive)

ders. — Generalüberholung für das Internet – Virtuelles Roundtable-Gespräch zum Status von IPv6, **c't** 20/1999, S. 212-214. (zitiert: *Krempl*, Generalüberholung für das Internet)

ders. — Kampf um die Ohrmuscheln – Music-Selling übers Netz: Ein neuer Vorstoß zum Schutz des Copyright, **Telepolis** vom 17.12.1998, http://www.heise.de/tp/deutsch/inhalt/te/2567/1.html. (zitiert: *Krempl*, Kampf um die Ohrmuscheln)

ders. — Konzerne im Visier, **c't** 4/1999, S. 182-184. (zitiert: *Krempl*, Konzerne im Visier)

Kreutzer, Till — Napster, Gnutella & Co.: Rechtsfragen zu Filesharing-Netzen aus der Sicht des deutschen Urheberrechts de lege lata und de lege ferenda – Teil 1, **GRUR** 2001, S. 193-204. (zitiert: *Kreutzer*, Napster, Gnutella & Co. – Teil 1)

ders. — Napster, Gnutella & Co.: Rechtsfragen zu Filesharing-Netzen aus der Sicht des deutschen Urheberrechts de lege lata und de lege ferenda – Teil 2, **GRUR** 2001, S. 307-312. (zitiert: *Kreutzer*, Napster, Gnutella & Co. – Teil 2)

Kreuzer, Arthur (Hrsg.) — Gießener Delinquenzbefragungen I – Grundsätzliche Fragen der Dunkelfeldforschung, in: Ehrengabe für Anne-Eva Brauneck, S. 101-115, Mönchengladbach 1999.

Kube, Edwin / Bach, Wolfgang / Erhardt, Elmar / Glaser, Ulrich — Technologische Entwicklung und Kriminalitätsvorbeugung, **ZRP** 1990, S. 301-305.

Kube, Edwin / Störzer, Hans Udo / Timm, Klaus Jürgen (Hrsg.) — Kriminalistik - Handbuch für Praxis und Wissenschaft (Band 1), Stuttgart, München, Hannover, Berlin, Weimar, 1992. (zitiert: Kube/Störzer/Timm-*Bearbeiter*)

Kube, Edwin — Technische Entwicklung und neue Kriminalitätsformen – Was geschieht, was droht?, **Kriminalistik** 1996, S. 618-625.

Kühne, Hans-Heiner — Nochmals: Die Strafbarkeit der Zugangsvermittlung von pornographischen Informationen im Internet – Besprechung des Urteils des LG München I vom 17.11.1999 – 20 Ns 465 Js 173158/95 (abgedruckt in **NJW** 2000, S. 1051), **NJW** 2000, S. 1003-1004.

Kürten, Oliver — Cyber-Klau – Raubkopien und Passwort-Deal im Internet, **PC-Intern** 8/1998, S. 33-39.

Kuhn, Markus — In die Röhre geguckt – Unerwünschte Abstrahlung erlaubt Lauschangriff, **c't** 24/1998, S. 90-97.

Kuri, Jürgen — Canned Heat – Die neue Internet-Verwaltung nimmt Gestalt an, **c't** 5/1999, S. 32.

Lackner, Karl / Kühl, Kristian — Strafgesetzbuch - mit Erläuterungen, 24, Auflage, München 2001. (zitiert: Lackner/Kühl-*Bearbeiter*)

Laue, Christoph / Zota, Volker — Kopieren auf Umwegen – Audio und Video analog duplizieren, **c't** 2/2002, S. 86-89.

Learmonth, Michael — The Enforcer - David Powell's Copyright Control Services chases software pirates around the world. And if his deals with 2 leading record labels go through, his digital dragnet may put an end to free music downloads, **The Industry Standard Europe** vom 16.02.2001, http://www.thestandard.com/article/display/0,1151,22315,00.html.

Lehmann, Michael / Tucher, Tobias von — Urheberrechtlicher Schutz von multimedialen Webseiten, **CR** 1999, S. 700-706.

Leitner, Felix von — Das nächste Netz – IPv6 wird zum Protokoll-Unterbau des Internet, **c't** 16/2001, S. 202-207.

Lehmann, Michael — Unvereinbarkeit des § 5 Teledienstegesetz mit Völkerrecht und Europarecht,
CR 1998, S. 232-234.

Lehmkuhl, Frank — „Musikdienste drohen zu floppen" – Interview mit Medienforscher Karsten Weber,
FOCUS 34/2001, S. 132.

Loewenheim, Ulrich — Urheberrechtliche Probleme bei Multimediaanwendungen,
GRUR 1996, S. 830-836.

Luckhardt, Norbert — Kennzeichen DE – Rechtsfragen zur privaten Homepage,
c't 18/1999, S. 122-123.
(zitiert: *Luckhardt*, Kennzeichen DE)

ders. — Pretty Good Privacy – Teil 1: Einstieg in das Web of Trust,
c't 12/1999, S. 212-214.
(zitiert: *Luckhardt*, Pretty Good Privacy – Teil 1)

ders. — Pretty Good Privacy – Teil 2: Schlüsselfragen und –antworten,
c't 13/1999, S. 208-210.
(zitiert: *Luckhardt*, Pretty Good Privacy – Teil 2)

ders. — Pretty Good Privacy – Teil 3: Dateibearbeitung und geteilte Schlüssel,
c't 16/1999, S. 172-175.
(zitiert: *Luckhardt*, Pretty Good Privacy – Teil 3)

Machill, Marcel / Waltermann, Jens (V.i.S.d.P.) — Memorandum der Bertelsmann-Stiftung zur Verantwortlichkeit im Internet,
Gütersloh 1999, ursprünglich veröffentlicht auf der Homepage der Bertelsmann-Stiftung (http://bertelsmann-stiftung.de). Mittlerweile zu finden in *Waltermann, Jens / Machill, Marcel* (Hrsg.), Verantwortung im Internet - Selbstregulierung und Jugendschutz,
Gütersloh 2000.

Mäger, Stefan — Der urheberrechtliche Erschöpfungsgrundsatz bei der Veräußerung von Software,
CR 1996, S. 522-526.

Malpricht, Marc M. — Über die rechtlichen Probleme beim Kopieren von Musik-CDs und beim Download von MP3-Dateien aus dem Internet,
NJW-CoR 2000, S. 233-234.

Marly, Jochen — Softwareüberlassungsverträge,
3. Auflage, München 2000.

Mayer, Franz — Recht und Cyberspace,
NJW 1999, S. 1782-1791.

McCandless, David — Warez Wars,
Wired Magazine 5.04 – April 1997,
http://www.wired.com/wired/archive/5.04/ff_warez.html.

McClure, Stuart / Scambray, Joel — How hackers cover their tracks, **CNN interactive**, 25.01.1999, http://www.cnn.com/tech/computing/9901/25/hacktracts.idg.

Meier, Bernd-Dieter — Softwarepiraterie – eine Straftat? – Überlegungen zum Strafrechtsschutz für Computerprogramme, **JZ** 1992, S. 657-665.

Menge, Rainald — Mit rotem Hut – Interview mit Red-Hat-Chef Bob Young, **c't** 22/1999, S. 46-47.

Mes, Peter — Patentgesetz – Gebrauchsmustergesetz, München 1997.

Meseke, Bodo — Ermittlung und Fahndung im Internet, in: Festschrift für Horst Herold – Das Bundeskriminalamt am Ausgang des 20. Jahrhunderts, Wiesbaden 1998.

Metzger, Axel / Kreutzer, Till — Richtlinie zum Urheberrecht in der „Informationsgesellschaft" – Privatkopie trotz technischer Schutzmaßnahmen? **MMR** 2002, S. 139-142.

Meyer, Carsten — Kreuzverhörtest – Der c't-Leser-Hörtest: MP3 gegen CD, **c't** 6/2000, S. 92-94.

Minar, Nelson — Distributed Systems Topologies: Part 1, **O'Reilly Network** (OpenP2P.com), 14.12.2001, http://www.openp2p.com/pub/a/p2p/2001/12/14/topologies_one.html.

Möller, Erik — Kopieren ohne Grenzen – Dateien tauschen in Peer-to-Peer-Netzen, **c't** 6/2001, S. 150-155. (zitiert: *Möller*, Kopieren ohne Grenzen)

ders. — Sicherheit in Peer-to-Peer-Netzen - Beim Tauschen und Suchen sollte man die Risiken kennen, **Telepolis** vom 29.06.2001, http://www.heise.de/tp/deutsch/inhalt/te/7972/1.html (zitiert: *Möller*, Sicherheit in Peer-to-Peer-Netzen)

Mönkemöller, Lutz — Moderne Freibeuter unter uns? – Internet, MP3 und CD-R als GAU für die Musikbranche!, **GRUR** 2000, S. 663-669.

Münker, Reiner — Urheberrechtliche Zustimmungserfordernisse beim Digital Sampling, Frankfurt am Main, Berlin, Bern, New York, Paris, Wien 1995

Negroponte, Nicholas — Being Digital, London 1995.

Neumann, A. Lin — Information Wants To Be Free – But This Is Ridiculous, **Wired Magazine** 3.10 – Oktober 1995, http://www.wired.com/wired/archive/3.10/piracy.html.

Ochsenbein, Andreas — Strafrechtliche Aspekte des Internet – Lösungen und Möglichkeiten, **Kriminalistik** 1998, S. 685-688.

Patalong, Frank — RIAA-Viren im FastTrack-Netzwerk? Die auf eine Verunsicherung der P2P-Nutzer abzielenden Aktionen der Entertainment-Industrie scheinen Früchte zu tragen. Es gerüchtelt im Netz - über Hackaktionen, Viren, Account-Streichungen und Abmahnungen, **SPIEGEL Online** vom 26.07.2002, http://www.spiegel.de/netzwelt/netzkultur/0,1518,206714,00.html.

Paul, Werner — Die Computerkriminalität in der Statistik, **NJW-CoR** 1995, S. 42-45.

Peeck, Klaus — Musik hinter Gittern – Kopierschutz für Audio-CDs, **c't** 15/2001, S. 16.

Persson, Christian — Pentium-III-Seriennummer doch „weich" einschaltbar – Intels Datenschutz-Konzept noch mal geändert, **c't** 5/1999, S. 16.

Persson, Christian / Siering, Peter — Big Brother Bill – Microsofts heimliche ID-Nummern – angeblich eine Panne, **c't** 6/1999, S. 16-20.

Pitscheneder, Robert — Ethik-TÜV im Netz – Ein Schablonensystem soll das WWW nach moralischen Kriterien bewerten und für die Zukunft rüsten, **FOCUS** 39/1999, S. 228-230. (zitiert: *Pitscheneder*, Ethik-TÜV im Netz)

ders. — Streit um das Namensschild, **FOCUS** 18/1999, S. 250. (zitiert: *Pitscheneder*, Streit um das Namensschild)

Pogue, David — Some Warez over the Rainbow, **Macworld Magazine** 10/1997, http://www.macworld.com/1997/10/opinion/3919.html; auch zu beziehen über die Homepage des Autors (http://www.pogueman.com).

Poll, Günter /Brauneck, Anja — Rechtliche Aspekte des Gaming-Markts, **GRUR** 2001, S. 389-396.

Puscher, Frank — Internet im Untergrund, **internet world** 1/1999, S. 34-36.

Radcliffe, Deborah — Handling crime in the 21st century, **CNN interactive**, 15.12.1998, http://www.cnn.com/TECH/computing/9812/15/cybersleuth.idg/index.html.

Raubenheimer, Andreas — Anmerkung zum Urteil des LG Düsseldorf vom 20.03.1996 (Az. 12 O 849/93),
CR 1996, S. 740-741.
(zitiert: *Raubenheimer*, Anmerkung zum Urteil des LG Düsseldorf vom 20.03.1996)

ders. — Anmerkung zum Urteil des OLG Karlsruhe vom 10.01.1996 (Az. 6 U 40/95 - abgedruckt in **CR** 1996, S. 341),
CR 1996, S. 342-343.
(zitiert: *Raubenheimer*, Anmerkung zum Urteil des OLG Karlsruhe vom 10.01.1996)

ders. — Die jüngste Rechtsprechung zur Umgehung/Beseitigung eines Dongles,
NJW-CoR 1996, S. 174-182
(zitiert: *Raubenheimer*, Die jüngste Rechtsprechung zur Umgehung / Beseitigung eines Dongles)

ders. — Zunehmende Bedeutung des Hardware Locks (Dongle, Key) in der jüngsten deutschen Rechtsprechung,
veröffentlicht auf der Homepage der *WIBU-Systems AG*, 1997,
http://www.wibu.de/de/presse_rechtslage.php.
(zitiert: *Raubenheimer,* Zunehmende Bedeutung des Hardware Locks in der jüngsten deutschen Rechtsprechung)

Redeker, Helmut — Der EDV-Prozess – Zivilrechtliche Probleme von Software und Internet,
2. Auflage, München 2000.

Reiser, Veit — Bericht über Softwarepiraten, eine Pressekonferenz, über zivilrechtliche Ambitionen und die strafrechtliche Keule – oder viel Lärm um wenig,
NJW-CoR 1995, S. 51-54.

Rink, Jürgen — Die Geister, die ich rief – Chancen und Risiken elektronischer Bücher,
c't 6/1999, S. 192-202.

Roehrl, Armin / Schmiedl. Stefan — Vogelfrei – Die wichtigsten Open-Source-Lizenzen,
c't 1/2002, S. 170-173.

Röttgers, Janko — Die Fake-Fluter - Overpeer Inc. versucht, Tauschbörsen mit einer zum Patent angemeldeten "Methode zur Verhinderung sinkender Platten-verkäufe" zu unterwandern
Telepolis vom 12.07.2002,
http://www.heise.de/tp/deutsch/inhalt/musik/12897/1.html.
(zitiert: *Röttgers*, Die Fake-Fluter)

ders. — Piraten hinter Gittern - Bis zu fünf Jahre Haft für Kopf der Warez-Gruppe DrinkOrDie,
Telepolis vom 28.02.2002,
http://www.heise.de/tp/deutsch/inhalt/te/11964/1.html.
(zitiert: *Röttgers*, Piraten hinter Gittern)

Rötzer, Florian — Europäische Musiker überreichen Petition an das EU-Parlament – Angeblich schützen nur schärfere Urheberrechtsgesetze die "Kreativität",
Telepolis vom 14.07.2000,
http://www.heise.de/tp/deutsch/inhalt/musik/8380/1.html.
(zitiert: *Rötzer*, Europäische Musiker überreichen Petition an das EU-Parlament)

ders. — FBI CIA NSA IRS ATF BATF DOD WACO – Hacktivisten gegen Echelon,
Telepolis vom 07.10.1999,
http://www.heise.de/tp/deutsch/inhalt/te/5358/1.html .
(zitiert: *Rötzer*, FBI)

ders. — Mit dem Niedergang von Napster sinken auch die CD-Verkäufe - Diese Koinzidenz mag geradezu symbolisch anmuten, zumal die Zahl der CD-Verkäufe während der Boomzeit von Napster am höchsten waren,
Telepolis vom 14.08.2001,
http://www.heise.de/tp/deutsch/inhalt/musik/9313/1.html.
(zitiert: *Rötzer*, Mit dem Niedergang von Napster sinken auch die CD-Verkäufe)

Runte, Christian — Produktaktivierung – Zivilrechtliche Fragen der „Aktivierung“ von Software,
CR 2001, S. 657-664.

Schack, Haimo — Urheber- und Urhebervertragsrecht,
2. Auflage, München 2001.

Schaefer, Martin / Rasch, Clemens / Braun, Thorsten — Zur Verantwortlichkeit von Online-Diensten und Zugangsvermittlern für fremde urheberrechtsverletzende Inhalte,
ZUM 1998, S. 451-457.

Scheja, Katharina — Per Mausklick in die Haft(ung) – Rechtliche Grundlagen zum Up- und Download im Internet,
c't 6/2002, S. 170-174.

Schipprack, Annette / Wegner, Jochen — Alles Gute, Web! – Vor zehn Jahren legte Tim Berners-Lee den Grundstein des WWW – nichts hat die Informationstechnik seit Gutenberg so revolutioniert,
FOCUS 11/1999, S. 174.

Schmidt, Jürgen — Heimliche Sammler – Multimedia-Player übermitteln ID-Nummern,
c't 23/1999, S. 20-21.

Schmidt, Susanne / Hüttermann, Christian — Zauberer der Informationsgesellschaft – Erste Open-Source-Konferenz „Wizards of OS“ in Berlin,
c't 16/1999, S. 112-115.

Schmitz, Peter / Preiß, Bernd — Streit ums Byte – Raubkopie – Nutzerselbsthilfe oder Diebstahl?
c't 8/2000, S. 112-113.

Schneider, Iris — Horchposten im Netz – Abhörpläne der EU stoßen bei Online-Nutzern und Providern auf zunehmende Ablehnung, **FOCUS** 13/1999, S. 264. (zitiert: *I. Schneider*, Horchposten im Netz)

Schneider, Jürgen — Urheberrechtsverletzungen im Internet bei Anwendung des § 5 TDG, **GRUR** 2000, S. 969-973 (zitiert: *J. Schneider*, Urheberrechtsverletzungen im Internet bei Anwendung des § 5 TDG)

Schönke, Adolf / Schröder, Horst — Strafgesetzbuch (Kommentar), 26. Auflage, München 2001. (zitiert: Schönke/Schröder-*Bearbeiter*)

Schricker, Gerhard (Hrsg.) — Kommentar zum Urheberrechtsgesetz, 2. Auflage, München 1999. (zitiert: Schricker-*Bearbeiter*)

ders. (Hrsg.) — Kommentar zum Urheberrechtsgesetz, München 1987. (zitiert: Schricker-*Bearbeiter* (1987))

ders. (Hrsg.) — Urheberrecht auf dem Weg in die Informationsgesellschaft, Baden-Baden 1997. (zitiert: *Autor* in *Schricker*, Urheberrecht auf dem Weg in die Informationsgesellschaft)

Schuhmacher, Dirk — Sperrungsverpflichtungen für Access-Provider bezüglich des Zugangs zu Webseiten mit rechtswidrigen Inhalten, veröffentlicht auf der Homepage des Deutschen Forschungsnetzes, http://www.dfn.de/content/beratung-weiterbildung/rechtimdfn/archiv/sperrungsverpflichtungen

Schult,Thomas J. — Der Klick zum Hit – Music on Demand: Die neue Napster-Liga, **c't** 14/2001, S. 106.

Schultz, Hartmut C. — Computerkriminalität – Die neue Dimension des Verbrechens und wie man sich davor schützt, München 1992.

Schulz, Hajo — Winquisition – Wieder blaue Briefe von Microsoft, **c't** 25/2001, S. 54. (zitiert: *H. Schulz*, Winquisition)

Schulz, Werner — US-Datenschützer: „Big-Brother inside", **VDI nachrichten** vom 05.02.1999, S. 15. (zitiert: *W. Schulz*, US-Datenschützer: „Big-Brother inside")

Schulzki-Haddouti, Christiane — Das Ende der Schweigsamkeit – EU-Parlament verabschiedet Echelon-Untersuchungsbericht, **c't** 19/2001, S. 44. (zitiert: *Schulzki-Haddouti*, Das Ende der Schweigsamkeit)

dies. Das Prinzip Anonymität,
c't 9/1999, S. 45-46.
(zitiert: *Schulzki-Haddouti*, Das Prinzip Anonymität)

dies. Gemäßigtes Krötenschlucken – Gesetzesauswertung stellt Weichen für Online-Recht,
c't 18/1999, S. 80-82.
(zitiert: *Schulzki-Haddouti*, Gemäßigtes Krötenschlucken)

dies. Grünes Licht für Kryptographie – Bundeskabinett verabschiedet liberale Eckwerte,
c't 13/1999, S. 46.
(zitiert: *Schulzki-Haddouti*, Grünes Licht für Kryptographie)

dies. Internet-Hilfssheriffs – BKA will Provider zur Inhaltskontrolle verpflichten,
c't 1/1999, S. 16.
(zitiert: *Schulzki-Haddouti*, Internet-Hilfssheriffs)

dies. Kein MP3 für deutsche Surfer?
Spiegel Online vom 24.02.2000,
http://www.spiegel.de/netzwelt/politik/0,1518,66046,00.html
(zitiert: *Schulzki-Haddouti*, Kein MP3 für deutsche Surfer?)

dies. Polizei im Netz – Das BKA jagt Kriminelle im Internet,
c't 13/1999, S. 16.
(zitiert: *Schulzki-Haddouti*, Polizei im Netz)

dies. Sichere Häfen – Sonderbotschafter Aaron zum Datenschutz,
c't 4/1999, S. 42.
(zitiert: *Schulzki-Haddouti*, Sichere Häfen)

dies. Trümpfe für den E-Commerce – EU-Parlament regelt Provider-Haftung und Spam,
c't 11/2000, S. 46
(zitiert: *Schulzki-Haddouti*, Trümpfe für den E-Commerce)

dies. World Wide Fahndung – Scott Charney, Chefermittler im US-Justizministerium, zur Strafverfolgung im Internet,
c't 15/1999, S. 74-75.
(zitiert: *Schulzki-Haddouti*, World Wide Fahndung)

Schuster, Andreas Hacker's Dream – Risikofaktor ICQ,
PC-Intern 8/1998, S. 45-47.

Schweickhardt, Dieter / Henke, Ruth Jukebox im Internet – Musik aus dem Datennetz kann die klassische CD und Kassette ersetzen. Schon verbreiten Internet-Piraten und Künstler Tausende Songs,
FOCUS, 37/1998, S. 148-153.

Schwerdtfeger Armin / Evertz, Stephan / Kreuzer, Philpp Amadeus / Peschel-Mehner, Andreas / Poeck, Torsten
Cyberlaw – Grundlagen, Checklisten und Fallbeispiele zum Online-Recht,
Wiesbaden 1999
(zitiert: Schwerdtfeger-*Bearbeiter*)

Sieber, Ulrich
Die rechtliche Verantwortlichkeit im Internet – Grundlagen, Ziele und Auslegung von § 5 TDG und § 5 MDStV,
MMR-Beilage zu Heft 2/1999, auch veröffentlicht auf der Homepage des Fachbereichs Jura der Universität München,
http://www.jura.uni-muenchen.de/einrichtungen/ls/sieber/article/mmr/5mmrbei_dt.htm.
(zitiert: *Sieber*, Die rechtliche Verantwortlichkeit im Internet)

ders.
Die Verantwortlichkeit von Providern im Rechtsvergleich,
ZUM 1999, S. 196-213, auch veröffentlicht auf der Homepage des Fachbereichs Jura der Universität München,
http://www.jura.uni-muenchen.de/einrichtungen/ls/sieber/article/rechtsvergleich/sie_prov_deutsch.pdf.
(zitiert: *Sieber*, Die Verantwortlichkeit von Providern im Rechtsvergleich)

ders.
Internationales Strafrecht im Internet – Das Territorialitätsprinzip der §§ 3, 9 StGB im globalen Cyberspace,
NJW 1999, S. 2065-2073, auch veröffentlicht auf der Homepage des Fachbereichs Jura der Universität München,
http://www.jura.uni-muenchen.de/einrichtungen/ls/sieber/article/InternationalesStrafrecht/9StGB.pdf.
(zitiert: *Sieber*, Internationales Strafrecht im Internet)

ders.
Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen – Zur Umsetzung von § 5 TDG am Beispiel der Newsgroups des Internet – Teil 1,
CR 1997, S. 581-598.
(zitiert: *Sieber*, Kontrollmöglichkeiten – Teil 1)

ders.
Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen – Zur Umsetzung von § 5 TDG am Beispiel der Newsgroups des Internet – Teil 2,
CR 1997, S. 653-669.
(zitiert: *Sieber*, Kontrollmöglichkeiten – Teil 2)

ders.
Kriminalitätsbekämpfung und freie Datenkommunikation im Internet,
MMR-Editorial 7/1998, auch veröffentlicht auf der Homepage des Fachbereichs Jura der Universität München,
http://www.jura.uni-muenchen.de/einrichtungen/ls/sieber/article/mmr/mmr_dt.htm.
(zitiert: *Sieber*, Kriminalitätsbekämpfung)

ders.
Missbrauch der Informationstechnik und Informationsstrafrecht – Entwicklungstendenzen in der internationalen Informations- und Risikogesellschaft – Teile 1-3,
veröffentlicht auf der Homepage des Fachbereichs Jura der Universität München,

http://www.jura.uni-muenchen.de/einrichtungen/ls/sieber/article/mitis/com_tu31.htm.
Bei der Veröffentlichung handelt es sich um eine aktualisierte und erweiterte Fassung des Aufsatzes „Computerkriminalität und Informationsstrafrecht – Entwicklungen in der internationalen Informations- und Risikogesellschaft“, der in **CR** 1995, S. 100-113 veröffentlicht wurde.
(zitiert: *Sieber*, Missbrauch der Informationstechnik)

Siering, Peter — Des Käufers Pflichten - Praxis der Zwangsaktivierung bei Office XP,
c't 13/2001, S. 46-47
(zitiert: *Siering*, Des Käufers Pflichten)

ders. — Kaufen verbindet – Microsofts Rechtsgebaren – zwischen Piraterieschutz und Monopolgehabe,
c't 9/2001, S. 130-135
(zitiert: *Siering*, Kaufen verbindet)

ders. — Lizenz-Kontrolle – Microsoft befragt seine Firmenkunden,
c't 14/2001, S. 30.
(zitiert: *Siering*, Lizenz-Kontrolle)

ders. — XPionage – Windows XP nährt Schnüffelvorwürfe,
c't 2/2002, S. 48.
(zitiert: *Siering*, XPionage – Windows XP nährt Schnüffelvorwürfe)

Sietmann, Richard — „Das Internet ist ein Mittel, Aufmerksamkeit zu erlangen“ – Michael Goldhaber über sein Modell der „Attention Economy“,
c't 13/2000, S. 52-53.
(zitiert: *Sietmann*, Goldhaber-Interview)

ders. — Nummernspiele – Ressourcenkonflikte um Namen und Adressen bleiben ein Politikum,
c't 9/1999, S. 180-191.
(zitiert: *Sietmann*, Nummernspiele)

Slatalla, Michelle / Quittner, Joshua — Gang War In Cyberspace,
Wired Magazine 2.12 – Dezember 1994,
http://www.wired.com/wired/archive/2.12/hacker.html.

Stallman, Richard — GNU Manifest,
veröffentlicht auf der Homepage der **FSF,**
http://www.gnu.org/gnu/manifesto.html; eine Übersetzung ins Deutsche von *Peter Gerwinski* findet sich unter
http://www.gnu.de/mani-ger.html.
(zitiert: *Stallman*, GNU Manifest)

ders. — Why Software Should Not Have Owners,
veröffentlicht auf der Homepage der **FSF**,
http://www.fsf.org/philosophy/why-free.html.
(zitiert: *Stallman*, Why Software Should Not Have Owners).

Steinberg, Don — Digital Underground, **Wired Magazine** 5.01 – Januar 1997, http://www.wired.com/wired/archive/5.01/esgrayzone.html.

Suler, John — Do Boys (and Girls) Just Wanna Have Fun? Gender-Switching in Cyberspace, Veröffentlicht auf der Homepage der Rider-University, Lawrenceville (USA), http://www.rider.edu/~suler/psycyber/genderswap.html.

Theurer, Marcus — Das Unternehmergespräch mit Christa Mikulski, geschäftsführende Gesellschafterin der Plattenfirma ZYX Music, **FAZ** vom 22.10.2001, S. 20.

Tröndle, Herbert / Fischer, Thomas — Strafgesetzbuch und Nebengesetze, 51. Auflage, München 2003.

Ullmann, Eike — Urheberrechtlicher und patentrechtlicher Schutz von Computerprogrammen – Aufgaben der Rechtsprechung, **CR** 1992, S. 641-648.

Ulmer, Eugen /Kolle, Gert — Der Rechtsschutz von Computerprogrammen, **GRUR Int.** 1982, S. 489-500.

Vassilaki, Irini E. — Multimediale Kriminalität – Entstehung, Formen und rechtspolitische Fragen der „Post-Computerkriminalität“, **CR** 1997, S. 297-302. (zitiert: *Vassilaki*, Multimediale Kriminalität)

ders. — Was ich nicht weiß ... – Provider-Haftung nach dem erweiterten Teledienstegesetz, **c't** 7/2002, S. 210. (zitiert: *Vassilaki*, Was ich nicht weiß)

Waldenberger, Arthur — Anmerkung zum Urteil des OLG München vom 08.03.2001 (Az. 29 U 3282/00), **MMR** 2001, S. 378-379. (zitiert: *Waldenberger*, Anm. zum Urteil des OLG München)

ders. — Teledienste, Mediendienste und die „Verantwortlichkeit“ der Anbieter, **MMR** 1998, S. 124-129. (zitiert: *Waldenberger*, Teledienste, Mediendienste und die „Verantwortlichkeit“ der Anbieter)

ders. — Zur zivilrechtlichen Verantwortlichkeit für Urheberrechtsverletzungen im Internet, **ZUM** 1997, S. 176-188. (zitiert: *Waldenberger,* Zur zivilrechtlichen Verantwortlichkeit für Urheberrechtsverletzungen im Internet)

Wandtke, Artur-Axel / Bullinger, Winfried (Hrsg.) — Praxiskommentar zur Urheberrecht, München 2002. (zitiert: Wandtke/Bullinger-*Bearbeiter*)

Weber, Karsten / Haug, Sonja — Kaufen oder Tauschen – Deutsche MP3-Konsumenten durchleuchtet, **c't** 17/2001, S. 36-37.

Weisse, Andreas — Der Kupferkessel – Abstrahlsicherer Raum als Stasi-Hinterlassenschaft, **c't** 3/2000, S. 115.

Wiebe, Andreas — Rechtsschutz für Software in den neunziger Jahren, **BB** 1993, S. 1094-1103.

Wiedenhoff, Chris — Abgeschmettert – Die einstweilige Verfügung gegen Diamond ist vom Tisch, **c't** 23/1998, S. 20.

Wiedmann, Klaus-Peter / Frenzel, Tobias / Walsh, Gianfranco — Musik im Internet – Ansätze der digitalen Distribution aus der Kundenperspektive (Teil 2), **musikmarkt** 50/2001, S. 18-19. (zitiert: *Wiedmann/Frenzel/Walsh*, Musik im Internet - Teil 2)

Wilkens, Andreas / Zota, Volker — Streitpauschale – Branchenverband und Verwerter brechen Gespräche ab, **c't** 6/2002, S. 17.

Wittich, Uta / Görgen, Thomas / Kreuzer, Arthur — Wenn zwei das gleiche berichten …: Beitrag zur kriminologischen Dunkelfeldforschung durch vergleichende Delinquenzbefragungen bei Studenten und Strafgefangenen, Mönchengladbach 1998.

Wrede, Klaus — Sind Sie ein Internet-Junkie? **FirstSurf** vom 15.09.1997, http://www.firstsurf.de/wrede5.htm.

Wuermeling, Joachim — Copyright-Richtlinien, Pressemitteilung auf der Homepage des *CSU*-Europaabgeordneten *Joachim Wuermeling* vom 06.02.2001, http://www.wuermeling.net/pdf/presseberichte/copyright_richtlinien_060201.pdf.

Ye, Sang — Computer Insect, **Wired Magazine** 4.07 – Juli 1996 (in der Übersetzung von *Geremie R. Barme*), http://www.wired.com/wired/archive/4.07/es.sinobug.html.

Ziebarth, Mark — Der wilde Westen – Piraterie oder ordnungsgemäße Nutzung?, **KEYS** 2/1999, S. 42-45.

Zimmerl, Hans — Internetsucht – Die Fakten, veröffentlicht im Österreichischen Gesundheitsinformationsnetz (GIN), http://gin.uibk.ac.at/thema/internetsucht/internetsucht.html.

Zimmermann, Christian — Der Hacker – Computerkriminalität: Die neue Dimension des Verbrechens, München 1996.

Zota, Volker / Buschmann, Andree — Konkurrierende Klangkonserven – Verlustbehaftete Audioformate im Vergleich, **c't** 23/2000, S. 152-161.

Zota, Volker / Hansen, Sven / Himmelein, Gerald — Frustscheiben – Abspielschutz für Audio-CDs verärgert Kunden, **c't** 22/2001, S. 52-53.

Zota, Volker — Klonverbot – Kopierschutz als Rettung vor Gelegenheitskopierern, **c't** 2/2002, S. 90-93. (zitiert: *Zota*, Klonverbot - Kopierschutz als Rettung vor Gelegenheitskopierern)

ders. — Moviez in Hülle und Fülle – Der Filmtausch im Internet erreicht ungeahnte Ausmaße, **c't** 6/2002, S. 158-167 (zitiert: *Zota*, Moviez in Hülle und Fülle)

ders. — Tauschangriff – Die Fronten zwischen Musikbranche und P2P-Börsen verhärten sich, **c't** 16/2002, S. 66-69. (zitiert: *Zota*, Tauschangriff)

ders. — Wasserzeichen-Blamage – Die Folgen des SDMI-Hack, **c't** 10/2001, S. 54. (zitiert: *Zota*, Wasserzeichen-Blamage)

Abkürzungsverzeichnis

€	Euro
3D	three-dimensional / dreidimensional
a.A.	anderer Ansicht
a.a.O.	am angegebenen Ort
a.E.	am Ende
a.F.	alte Fassung
A/D	Analog/Digital
AAC	Advanced Audio Coding (Dateiformat)
ABl. EG	Amtsblatt der Europäischen Gemeinschaft
Abs.	Absatz
ACE	Dateiformat der Software WinAce
ADSL	Asymmetric Digital Subscriber Line
AfP	Zeitschrift für Medien- und Kommunikationsrecht
AG	Aktiengesellschaft
AG (Stadt)	Amtsgericht (Stadt)
AGB	Allgemeine Geschäftsbedingungen
AHRA	Audio Home Recording Act
AI	Artificial Intelligence
ALE WG	Address Lifetime Expectation Working Group
Allg.	Allgemein(e Grundlagen)
amtl.	amtlich(e)
Anm.	Anmerkung(en)
AOL	America Online
ARPA	Advanced Research Projects Agency
Art.	Artikel
ASIC	Application Specific Integrated Circuit
ASCII	American Standard Code for Information Interchange
ASM	Assembler
ASP	Application Service Providing
AT&T	American Telephone & Telegraph Company
ATA	Advanced Technology Attachment Interface
ATAPI	Advanced Technology Attachment Packet Interface
ATRAC	Adaptive Transform Acoustic Coding
AVI	Audio Video Interleave (Dateiformat)
Az.	Aktenzeichen
BB	Betriebs-Berater
BBS	Bulletin Board System
Begr.	Begründung
BGB	Bürgerliches Gesetzbuch

BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt.	Sammlung der Entscheidungen des Bundesgerichtshofs in Strafsachen
BGHZ	Sammlung der Entscheidungen des Bundesgerichtshofs in Zivilsachen
BIN	Binary (Dateiformat)
BIOS	Basic Input Output System
BKA	Bundeskriminalamt
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten / Bundeskriminalamtgesetz
BMG	Bertelsmann Music Group
BPI	British Phonographic Industry
BR-Drucks.	Drucksache(n) des Deutschen Bundesrates
BSA	Business Software Alliance
BSD	Berkeley Software Design
BT-Drucks.	Drucksache(n) des Deutschen Bundestages
BV	Besloten Vennootschap (met beperkte aansprakelijkheid)
BVerfG	Bundesverfassungsgericht
BVerfGE	Sammlung der Entscheidungen des Bundesverfassungsgerichts
bzw.	beziehungsweise
c't	Magazin für Computertechnik
ca.	circa
CBR	Constant Bitrate
CCC	Chaos Computer Club
CCS	Copyright Control Service
CD	Compact Disc
CD-R	Compact Disc - Recordable
CD-ROM	Compact Disc - Read Only Memory
CD-RW	Compact Disc - Rewritable
CDS	Cactus Data Shield
CNN	Cable News Network
COM	Command (Dateiformat)
CORE	Internet Council of Registrars
CPRM	Content Protection for Recordable Media
CPU	Central Processing Unit
CR	Computer und Recht
CSU	Christlich Soziale Union
D.C.	District of Columbia
DADC	Digital Audio Disc Corporation
DARPA	Defense Advanced Research Projects Agency
DAT	Digital Audio Tape

DCC	Direct Client-to-Client
d.h.	das heißt
DDR	Deutsche Demokratische Republik
DENIC	Deutsche Network Information Center e.G.
ders.	derselbe
DFN	Deutsches Forschungsnetz
DH	Diffie/Hellmann
dies.	dieselbe
DIHK	Deutscher Industrie- und Handelskammertag
DiMA	Digital Media Association
DivX	Digital Video X (Dateiformat)
DIZ	Distribution (Dateiformat)
DKSB	Deutscher Kinderschutzbund
DM	Deutsche Mark
DMCA	Digital Millennium Copyright Act
DNS	Domain Name System
DOC	Document (Dateiformat)
DOD	Department Of Defense
DPMA	Deutsches Patent- und Markenamt
DRM	Digital Rights Management
DSS	Digital Signature Standard
DVD	Digital Versatile Disc
DVD-R	Digital Versatile Disc - Recordable
DVD-ROM	Digital Versatile Disc - Read Only Memory
DYNIP	Dynamically Allocated IP Address
e.G.	eingetragene Genossenschaft
e.V.	eingetragener Verein
EA	Electronic Arts
EDV	elektronische Datenverarbeitung
EFF	Electronic Frontier Foundation
EG	Europäische Gemeinschaft
Einl.	Einleitung
EMACS	Editing Macros
entg.	endgültig
EPIC	Electronic Privacy Information Center
EPÜ	Übereinkommen über die Erteilung europäischer Patente (Europäisches Patentübereinkommen)
etc.	et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof

EuGH Slg.	Amtliche Sammlung der Entscheidungen des (Europäischen) Gerichtshofs
EXE	Executable (Dateiformat)
f.	folgende (Seite)
ff.	fortfolgende (Seiten)
F-Serve	Full-Serve
FBI	Federal Bureau of Investigation
FITUG	Förderverein Informationstechnik und Gesellschaft
Fn.	Fußnote
FNC	Federal Network Council
FSF	Free Software Foundation
FTC	Federal Trade Commission
FTP	File Transfer Protocol
FXP	File Exchange Protocol
G8	Gruppe der Acht (Staaten): USA, Frankreich, Großbritannien, Japan, Italien, Kanada, Russland und Deutschland
GA	Goltdammer's Archiv für Strafrecht
GATT	General Agreement on Tariffs and Trade
GEMA	Gesellschaft für Musikalische Aufführungs- und Vervielfältigungsrechte
GfK	Gesellschaft für Konsumforschung
GFU	Gesellschaft für Unterhaltungs- und Kommunikationselektronik
GG	Grundgesetz für die Bundesrepublik Deutschland
GMX	Global Message Exchange
GNU	Gnu's Not UNIX
GPG	GNU Privacy Guard
GPL	GNU General Public Licence
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GRUR Int.	Gewerblicher Rechtsschutz und Urheberrecht - Internationale Ausgabe
GUI	Graphical User Interface
GUID	Globally Unique Identifier
GVU	Gesellschaft zur Verfolgung von Urheberrechtsverletzungen
h.M.	herrschende Meinung
HDTV	High Definition Television
HiFi	High Fidelity
Hrsg.	Herausgeber
HTML	Hypertext Markup Language
i.d.R.	in der Regel
i.S.d.	im Sinne des / der
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
IAPC	Internet Anti-Piracy Campaign

IBM	International Business Machines Corporation
ICANN	Internet Corporation for Assigned Names and Numbers
ICMP	Internet Control Message Protocol
ICQ	I Seek You
ID	Identifier
ID3	Identifier 3
IDA	Internet Addiction Disorder
IDC	International Data Corporation
IDE	Intelligent Drive Electronics / Integrated Drive Electronics
IDSA	Interactive Digital Software Association
IETF	Internet Engineering Task Force
IFPI	International Federation of the Phonographic Industry
IGMP	Internet Group Management Protocol
IIA	Information Industry Association
IIS-A	Fraunhofer-Institut für Integrierte Schaltungen
IMP	Internet Message Processor
Inc.	Incorporated / Incorporation
Int.	International
IP	Internet Protocol
IPR	International Planning and Research Corporation
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IPnG	Internet Protocol next Generation
IRC	Internet Relay Chat
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISRC	International Standard Recording Code
IT	Informationstechnologie
IuKDG	Informations- und Kommunikationsdienstegesetz
JA	Juristische Arbeitsblätter
JP(E)G	Joint Photographic Experts Group (auch Dateiformat)
JZ	Juristenzeitung
KBit/s	Kilobit pro Sekunde
KG	Kammergericht
kHz	Kilohertz
LAN	Local Area Network
LG	Landgericht
LLC	Limited Liability Company
m.w.N.	mit weiteren Nachweisen

M3U	MPEG-1 Layer-3 Playlist (Dateiformat)
MAC	Media Access Control
MAN	Metropolitan Area Network
MBit/s	Megabit pro Sekunde
MCPS	Mechanical Copyright Protection Society
MDR	Monatsschrift für Deutsches Recht
MDStV	Staatsvertrag über Mediendienste
MFTP	Multisource File Transfer Protokoll
MP3	MPEG-1 Layer-3 (Dateiformat)
MID	MIDI = Musical Instrument Digital Interface
MIT	Massachusetts Institute Of Technology
MOD	Music On Demand
Mod	Modification
MPAA	Motion Picture Association of America
MP(E)G	Motion Picture Experts Group (auch Dateiformat)
MMR	MultiMedia und Recht
MSN	Microsoft Network
NASA	National Aeronautics and Space Administration
NCP	Network Control Protocol
NCSA	National Center for Supercomputing Applications
NEC	Nippon Electric Company
NFO	Information (Dateiformat)
NIC	Network Information Center
NJW	Neue Juristische Wochenschrift
NJW-CoR	Computerreport der Neuen Juristischen Wochenschrift
Nr.	Nummer
NSI	Network Solutions, Incorporated
NStZ	Neue Zeitschrift für Strafrecht
NYPD	New York Police Departement
o.g.	oben genannte(n)/(r)
OECD	Organization for Economic Co-operation and Development
OEM	Original Equipment Manufacturer
OLG	Oberlandesgericht
Op	Operator
OS	Open Source / Open Software
P2P	Peer-to-Peer
PC	Personal Computer
PC-CY	Committee of Experts on Crime in Cyber-Space
PDA	Personal Digital Assistant
PDF	Portable Document Format (Dateiformat)

PERMIP	Permanently Allocated IP Address
PDA	Personal Digital Assistant
PGP	Pretty Good Privacy
PICS	Platform for Internet Content Selection
PIU	Pathological Internet Use
PKS	Polizeiliche Kriminalstatistik
PSN	Processor Serial Number
PWA	Pirates With Attitudes
QoS	Quality of Service
RAR	Dateiformat der Software WinRAR
Rdnr(n).	Randnummer(n)
RAM	Random Access Memory
RegTP	Regulierungsbehörde für Telekommunikation und Post
RFC	Requests For Comments
RG	Reichsgericht
RGSt.	Sammlung der Entscheidungen des Reichsgerichts in Strafsachen
RIAA	Recording Industry Association of America
ROM	Read Only Memory
RPS	Rights Protection System
Rs.	Rechtssache(n)
RSACi	Recreational Software Advisory Council
S.	Seite(n)
SACD	Super Audio CD
SAF	Secure Audio Format (Dateiformat)
SCMS	Serial Copy Management System
SCSI	Small Computer System Interface
SDMI	Secure Digital Music Initiative
SFV	Simple File Validator (Dateiformat)
SigG	Signaturgesetz
SIIA	Software and Information Industry Association
SLD	Second Level Domain
Slg.	Sammlung
SNES	Super Nintendo Entertainment System
SPA	Software Publishers Association
SPD	Sozialdemokratische Partei Deutschlands
StGB	Strafgesetzbuch
T-DSL	Telekom-Digital Subscriber Line
T-Online	Telekom-Online
TCP	Transfer Control Protocol
TCP/IP	Transfer Control Protocol/Internet Protocol

TDG	Gesetz über die Nutzung von Telediensten / Teledienstegesetz
TDDSG	Gesetz über den Datenschutz bei Telediensten / Teledienstedatenschutzgesetz
TEMPEST	Temporary Emanation and Spurious Transmission / Transient Electromagnetic Pulse Emanations Standard
TKG	Telekommunikationsgesetz
TLD	Top Level Domain
TOC	Table Of Contents
TPM	Trusted Platform Module
TTF	True Type Font (Dateiformat)
TTL	Time to Live
TV	Television
TXT	Text (Dateiformat)
u.a.	unter anderem
UdSSR	Union der Sozialistischen Sowjetrepubliken
ugs.	umgangssprachlich
UIN	Universal Identification Number
UrhG	Gesetz über das Urheberrecht und verwandte Schutzrechte
URL	Uniform Resource Locator
US(A)	United States (of America)
UWG	Gesetz gegen den unlauteren Wettbewerb
V.i.S.d.P.	Verantwortlich(er) im Sinne des Presserechts
VBR	Variable Bitrate
VDI	Verein Deutscher Ingenieure
VDSL	Very-High-Bit-Rate Digital Subscriber Line
verb.	verbunden(e)
vgl.	vergleiche
VQF	Vector Quantization Format (Dateiformat)
VUD	Verband der Unterhaltungssoftware Deutschland
W3	World Wide Web
W3C	World Wide Web Consortium
WAN	Wide Area Network
WAV	(Pulse Code Modulated) Wave Audio File (Dateiformat)
WCT	WIPO Copyright Treaty
WIPO	World Intellectual Property Organization
WMA	Windows Media Audio
WPPT	WIPO Performances and Phonograms Treaty
WWW	World Wide Web
WYSIWYG	What You See Is What You Get
XLS	Excel Spreadsheet File (Dateiformat)
z.B.	zum Beispiel

ZaRD	Zentralstelle für anlassunabhängige Recherche in Datennetzen
ZDNet	Ziff Davis Net
ZIP	Dateiformat der Software WinZip
ZPÜ	Zentralstelle für private Überspielungsrechte
ZUM	Zeitschrift für Urheber- und Medienrecht
ZRP	Zeitschrift für Rechtspolitik

Stand des Literaturverzeichnisses: 26.05.2003
Stand der Online-Verweise: 22.08.2004

Teil 1 – Einführung

A. Bedeutung und Einordnung des Forschungsgegenstands

Das Internet ist allgegenwärtig. Es vergeht kaum ein Tag, an dem man nicht in den Medien auf World Wide Web- (WWW bzw. W3) oder E-Mail-Adressen aufmerksam gemacht wird. Ein großer Teil der deutschen Bevölkerung ist bereits über die „elektronische Post" zu erreichen, und beinahe jedes deutsche Unternehmen verfügt über eine eigene Online-Präsenz. Das Internet hat sich als ein Medium etabliert, in dem sich Individual- und Massenkommunikation vereinen.

Unternimmt man den Versuch einer Definition des Begriffes Internet, könnte man zu folgendem Ergebnis kommen: „Das Internet umfasst die Gesamtheit der menschlichen Kommunikation, gleich in welcher medialen Form – schriftlich, gesprochen, als bewegtes Bild oder in Kombination daraus, die nach einem bestimmten technischen Verfahren über eine beliebige Distanz erfolgt".[1] Sofern man den Begriff der Kommunikation eng auslegt, muss ergänzend die Möglichkeit des gegenseitigen Datenaustausches erwähnt werden.

Die große Bedeutung des Internet für Gegenwart und Zukunft ist unbestritten. Verfolgt man die Bemühungen von Informationstechnologie-Konzernen wie *Microsoft* oder *America Online (AOL),* die darauf ausgerichtet sind, die Vorherrschaft im „Netz der Netze" zu erlangen, wird deutlich, welch hohen Wert die Ware Information mittlerweile erlangt hat.

Als Computernetz vereinfacht das Internet nicht nur die Informationsbeschaffung und ermöglicht dem Handel völlig neue Vermarktungsmöglichkeiten, sondern es dient – vor allem bei der gemeinsamen Nutzung von Ressourcen – auch der Kostenersparnis[2].

Die positiven Einflüsse des Internet auf Gesellschaft und Wirtschaft sind unverkennbar. Von dem Grundsatz jedoch, dass neue technische Strukturen und Systeme quasi Magnetpole und Kristallisationspunkte für neue Formen der Kriminalität sind[3], bleibt auch das Internet nicht ausgenommen. Bei praktisch allen Straftaten mit Kommunikationsbedarf kann das Netz eingesetzt werden. Von der länderübergreifenden Koordination mafioser Unternehmungen bis hin zur Anstiftung zum Mord per E-Mail – alles ist denkbar und wird früher oder später Realität. Bereits 1996 beschrieb *Edwin Kube*, ehemaliger Abteilungspräsident im *Bundeskriminalamt (BKA),* die Möglichkeit des Online-Mordes: Der Täter dringt in das Computernetz einer Großklinik ein und verändert die Medikation für einen Schwerkranken auf der Intensivstation. Es habe den Anschein, so *Kube*, "dass das perfekte Verbrechen näher gerückt ist, als manche dies anzunehmen glauben".[4]

Vor allem im Bereich des Urheberrechts stellt das Internet ein weltweites Betätigungsfeld für Kriminelle dar. Es ist bereits heute möglich, von jedem Ort der Welt aus mit einem handelsüblichen Computer und einem Telefonanschluss beinahe jedes erhältliche Computerprogramm oder

---

[1] *Blümel/Soldo*, S. 8; eine offizielle Definition des Begriffs Internet wurde vom *Federal Network Council (FNC)* am 24.10.1995 in einer einstimmigen Resolution festgelegt und ist vor allem für die Rechtssicherheit bei Vertragsverhandlungen von Bedeutung. Der Wortlaut findet sich unter http://www.itrd.gov/fnc/Internet_res.html.
[2] Vgl. *Sieber*, Kontrollmöglichkeiten – Teil 1, **CR** 1997, S. 588.
[3] *Kube/Bach/Erhardt/Glaser*, **ZRP** 1990, S. 301 f.
[4] *Goos*, **SPIEGEL Online** vom 29.02.2000.

Musikstück als Raubkopie[5] direkt über das Internet zu beziehen; es entstehen lediglich Kosten für den Zugang zum Internet und die Telefongebühren. Die Urheber der Werke erhalten in diesen Fällen keine Vergütung.

Die vorliegende Arbeit enthält zunächst eine allgemeine Einführung in die Materie Internet, widmet sich im zweiten Teil dem Problem der Internet-Softwarepiraterie und untersucht im dritten Teil das recht junge Phänomen der Online-Musikpiraterie. Innerhalb der beiden Piraterieteile werden zuerst die Strukturen und Mechanismen beschrieben, die hinter der Verbreitung von Raubkopien über das Internet stehen. Schließlich werden die Bekämpfungsstrategien analysiert, die derzeit verfolgt werden. Am Ende jedes Teils werden die erfolgversprechendsten Strategien zusammengefasst und mit eigenen Ansätzen ergänzt.

B. Die Geschichte des Internet

Ende der 60er Jahre entstand im Auftrag des US-Verteidigungsministeriums *(Department Of Defense – DOD)* der Vorläufer des heutigen Internet – das *ARPA-Net*. Benannt wurde es nach der *Advanced Research Projects Agency*, einer staatlichen Organisation, die vorwiegend für das *DOD* Forschungsaufträge an Universitäten und Forschungsinstitute vergab. Die *ARPA* wurde 1957 als Reaktion auf den Start des *Sputniks* durch die UdSSR gegründet. Da von der *ARPA* zunehmend Projekte koordiniert wurden, die militärischen Zwecken dienten, wurde sie bald in *DARPA (Defense Advanced Research Projects Agency)* umbenannt. Ziel des ursprünglichen *ARPA*-Projektes war es, ein Kommunikationsmedium für das Militär zu schaffen, das selbst nach einem Atomschlag noch funktionsfähig wäre. Um dies zu erreichen, entschieden sich die Entwickler für eine Netzstruktur zur Verknüpfung einzelner Militärcomputer. Wie das damalige *ARPA-Net* beruht auch das heutige Internet auf einem System mehrerer gleichberechtigter Netzknoten (Internet Message Processors – IMPs), die Nachrichten senden, empfangen oder weiterleiten können. Die Netzstruktur gewährleistet, dass die Nachrichten auf vielen unterschiedlichen Wegen vom Absender zum Empfänger gelangen können, weshalb die Kommunikation zwischen zwei Computern auch noch bei Ausfall eines oder mehrerer Teilnetze stattfinden kann.

Ursprünglich – Ende 1969 – bildeten 4 Knotenrechner das Herzstück des *ARPA-Net*. Dieses erste experimentelle Netz wurde von den kalifornischen Universitäten in Los Angeles und Santa Barbara sowie dem *Stanford Research Institute* und der Universität von Utah in Betrieb genommen. 1971 waren es bereits 15 Knotenrechner, die 23 Militärcomputer miteinander vernetzten[6], und noch im selben Jahr wurde die erste E-Mail versandt[7].

---

[5] Obwohl es sich beim Wort „Raubkopie" nicht um einen zutreffenden juristischen Terminus handelt (Raub setzt eine Wegnahme einer fremden Sache mit Gewalt oder unter Anwendung von Drohungen voraus, vgl. § 249 StGB) wird es in der vorliegenden Arbeit verwendet, da es Teil des allgemeinen Sprachgebrauchs ist. Zu verstehen ist hierunter stets ein nichtlizenziertes Vervielfältigungsstück eines urheberrechtlich geschützten Werkes.
Verwendet wird auch der Begriff der Piraterie; dieser gehört ebenfalls zum allgemeinen Sprachgebrauch, darüber hinaus kennt die Rechtssprache den Begriff der Produktpiraterie. Nach der Definition in *Creifeld's Rechtswörterbuch* ist hierunter die „gezielte Verletzung von Urheberrechten und gewerblichen Schutzrechten, das gewerbsmäßige Aneignen fremden geistigen Eigentums durch Nachahmung und Kopie" zu verstehen.

[6] *Hoeren*, Das Internet für Juristen, **NJW** 1995, S. 3295.

[7] *Meseke*, S. 506.

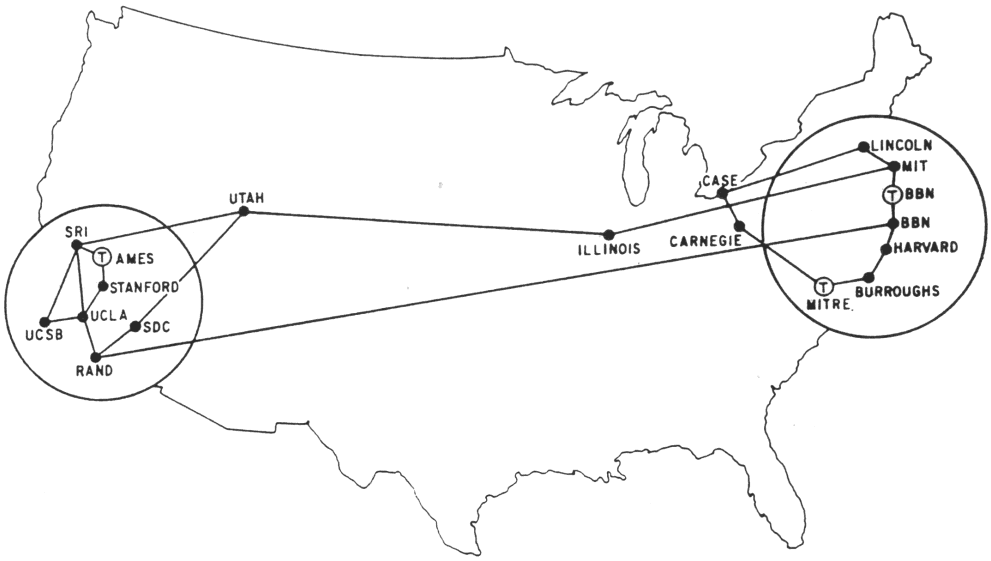


Abbildung 1 – das *ARPA-Net* im September 1971

1972 erhöhte sich die Zahl der Knotenrechner auf 37, und bis 1977 waren ganze 111 Knotenrechner in das Netz eingewoben[8]. Ursprüngliches Kommunikationsprotokoll[9] war das Network Control Protocol (NCP). Von 1969 bis 1976 verblieb die Federführung des Projektes beim *DOD*, erst Mitte der 70er Jahre beteiligten sich zunehmend auch Universitäten, die nicht in das *ARPA*-Projekt involviert waren, sowie andere Bildungseinrichtungen an der Weiterentwicklung des Netzes, das mit zunehmender ziviler Nutzung als Internet bezeichnet wurde.

1976 wurde ein neues, erweitertes Übertragungsprotokoll namens Transfer Control Protocol/ Internet Protocol (TCP/IP) vorgestellt, welches das rudimentäre NCP ablöste. Die spätere Entscheidung, das TCP/IP freizugeben und auch im Betriebssystem *UNIX* zu integrieren (1980), hat deutlich zur Verbreitung der Internet-Technologie beigetragen. Der eigentliche Durchbruch des Internet erfolgte jedoch mit der Erfindung des WWW, welches die Nutzung des Internet durch eine Art grafische Bedienoberfläche wesentlich vereinfachte.[10]

Im März des Jahres 1989 schlug der US-Forscher *Tim Berners-Lee* das sogenannte Hypertextsystem zur Datenverwaltung im Internet vor, welches eine einheitliche grafische Darstellung von Informationen ermöglichte. *Berners-Lee* gilt als einer der wichtigsten Entwickler des WWW und ist derzeit Vorsitzender des *World Wide Web Consortium (W3C)*[11], einer Organisation, die es sich seit 1994 zur Aufgabe gemacht hat, neue WWW-Standards zu entwickeln. 1990 wurde das erste Programm vorgestellt, mit dem man das WWW per Hypertextsystem nutzen konnte – der Begriff des Browsers

---

[8] *Blümel/Soldo*, S. 13.
[9] Unter einem Protokoll versteht man einen Regelsatz für die Datenübertragung. Hält sich ein Partner der Kommunikation nicht an diese Regeln, wird die Kommunikation erheblich gestört oder kommt gar nicht erst zustande.
[10] *Heinzmann/Ochsenbein*, Strafrechtliche Aspekte des Internet – Teil 1, **Kriminalistik** 1998, S. 514.
[11] Zur Tätigkeit des *W3C* – siehe unten Teil 2, C. II. 1.

war geboren. *Marc Andreessen*, Student am *National Center for Supercomputing Applications (NCSA)*, veröffentlichte 1993 den populären Browser *Mosaic*, aus dem später der beliebte und weit verbreitete Browser *Netscape* hervorging[12].

Nach Schätzungen umfasste das Internet 1996 mehr als 61.000 intra- und internationale Netze, die aus ca. 30 Millionen Rechnern bestanden.[13] Die Teilnehmerzahl wurde weltweit auf 35 Millionen geschätzt.[14] Nur drei Jahre später gingen Experten davon aus, dass über 160 Millionen Menschen einen Anschluss ans globale Datennetz hatten.[15]

Nach einer Studie der *Gesellschaft für Konsumforschung (GfK)* nutzten Anfang 2000 30% der Bundesbürger zwischen 14 und 69 Jahren das WWW.[16] Eine neuere Studie des Meinungsforschungsinstituts *Forsa* vom Januar 2002 kommt zu dem Ergebnis, dass mittlerweile sogar 27,8 Millionen Deutsche (ca. 43%) über 14 Jahre „online" sind[17].

Experten rechnen für Deutschland mittelfristig mit einem Nutzungsgrad von deutlich über 50% der Bevölkerung.[18] In den USA sind bereits 92 Millionen Menschen „online", was einem Bevölkerungsanteil von ca. 40% entspricht.[19]

C. Die technischen und organisatorischen Grundlagen des Internet

I. Die Datenübertragung im Internet

1. Die Netzstruktur

Das Internet besteht aus zahlreichen, lose miteinander verbundenen Teilnetzen.[20] Die in den Netzwerken befindlichen Computer können grob in zwei Kategorien unterteilt werden: Server und Clients. Beim Server handelt es sich um einen Rechner, der einen Dienst anbietet, wohingegen der Client ein Rechner ist, der den angebotenen Dienst nutzt. Benötigt beispielsweise der Sachbearbeiter eines großen Unternehmens bestimmte Kundendaten, wird er diese im Regelfall von seinem Arbeitsplatzrechner (Client) aus über das Netzwerk bei einem Server anfordern, der eine Datenbank als Dienst für alle Mitarbeiter bereithält.

---

[12] http://www.w3history.org.
[13] *Harbort*, **Kriminalistik** 1996, S. 195.
[14] *Hoeren*, Das Internet für Juristen, **NJW** 1995, S. 3295.
[15] *Schippracke/Wegner*, **FOCUS** 11/1999, S. 174.
[16] **Heise Online News** vom 22.02.2000, http://www.heise.de/newsticker/meldung/8144.
[17] **Heise Online News** vom 14.01.2002, http://www.heise.de/newsticker/meldung/24006.
[18] Gemäß einer *Infratest*-Studie, siehe **Heise Online News** vom 20.09.2000, http//www.heise.de/newsticker/meldung/6173.
[19] Nach einer Studie des Marktforschungsinstituts *Nielsen*, http://www.nielsenmedia.com und von *CommerceNet*, http://www.commerce.net.
[20] Diese unterscheiden sich in erster Linie anhand ihrer Größe: Die Wide Area Networks (WANs) bestehen aus Verbindungen, die sich über einen weiten Weg (z.B. von Europa nach Amerika) erstrecken. Ein Metropolitan Area Network (MAN) ist deutlich kleiner als ein WAN und wird beispielsweise zur Vernetzung mehrerer Bürogebäude eines Unternehmens eingesetzt, die sich in unterschiedlichen Stadtteilen befinden. Als Local Area Network (LAN) wird z.B. die Vernetzung der Rechner innerhalb eines Unternehmens bezeichnet. Schon die Verbindung zweier einzelner Computer ist ein LAN - vgl. die Darstellung bei *Sieber*, Kontrollmöglichkeiten – Teil 1, **CR** 1997, S. 588 f.

Zwischen den Teilnetzen bestehen Hauptdatenleitungen (sogenannte Backbones), die mit ihren großen Bandbreiten und schnellen Routern[21] tatsächlich das Rückgrat des Internet bilden. Während bei einem ISDN[22]-Kanal nur eine Übertragungsrate von 64 KBit/s möglich ist, kann mit einem 155 MBit/s Backbone (z.B. die Leitung des Wissenschaftsnetzes zwischen München und Nürnberg) die 2.400-fache Menge an Daten in der gleichen Zeit übertragen werden[23].

Die Verantwortlichkeit für den Bereich der Teilnetze liegt bei unzähligen, nur lose zusammengeschlossenen Organisationen, weshalb das Netz eine eher anarchische Struktur hat, in der es an Verantwortlichen fehlt, die den gesamten Netzbetrieb steuern könnten.[24] Neben Universitäten und Forschungseinrichtungen kümmern sich hauptsächlich privatwirtschaftliche Unternehmungen um den Betrieb und die Unterhaltung der Infrastruktur der Teilnetze. So handelt es sich bei den sogenannten Carriern (Network-Provider), die die technischen Grundlagen für eine weitläufige Vernetzung liefern, meist um Telekommunikationsunternehmen wie die *Deutsche Telekom.* Als Backbone-Provider bezeichnet man Organisationen, die sich in erster Linie auf den Anschluss großer Unternehmen oder Internet Service Provider (ISPs) an das Internet konzentrieren. Hierzu mieten sie in der Regel von den Carriern Leitungen an. ISPs wiederum sind Unternehmen wie *Arcor* oder *Freenet,* und ihre hauptsächliche Tätigkeit ist die Zugangsvermittlung (Access-Providing), d.h. sie verschaffen dem Privatkunden gegen Gebühr einen Zugang zum Internet. Zu den Serviceleistungen, die sie ihren Kunden zusätzlich zum Access-Providing bieten, zählt im Regelfall der Betrieb eines Webservers, eines E-Mail-Servers und eines Proxyservers[25]. Auch Universitäten können für ihre Studenten und Mitarbeiter als ISP fungieren.

Von den ISPs zu unterscheiden sind die Online Service Provider (auch „Online-Dienste"). Letztere erweitern das Internet Service Providing um ein eigenes Angebot an Diensten, die den Kunden einen zusätzlichen Vertragsanreiz bieten sollen. Diese Dienstleistungen – meist Zugang zu eigens geschaffenen Informationsquellen, Gesprächsforen etc. – können nur von registrierten Kunden des jeweiligen Online-Dienstes in Anspruch genommen werden. Bekannte Online-Dienste sind z.B. *T-Online* oder *AOL.*

2. Die Regeln der Datenübertragung – TCP/IP als wichtigstes Protokoll[26]

Bei einer Datenübertragung wird die zu versendende Datei in mehrere kleinere Datenpakete zerlegt, von denen jedes mit den Adressen des gewünschten Empfängers und des aktuellen Absenders versehen wird. Das für die Übertragung verwendete Protokoll enthält die Regeln für den Datentransfer, es legt beispielsweise die Größe der zu versendenden Datenpakete fest und übernimmt die Fehlerkontrolle innerhalb der Datenkommunikationsverbindung. Der im Internet hauptsächlich zum Einsatz kommende Protokoll-Stack, also die Liste aller innerhalb einer

---

[21] Router sind Verbindungsrechner, die sich an den Netzknotenpunkten befinden und für die Vermittlung der Daten im Netzsystem zuständig sind.
[22] Integrated Services Digital Network – siehe auch Fn. 45.
[23] *Sieber,* Kontrollmöglichkeiten – Teil 1, **CR** 1997, S. 590.
[24] *Heinzmann/Ochsenbein*, Strafrechtliche Aspekte des Internet – Teil 1, **Kriminalistik** 1998, S. 514.
[25] Zur Funktionsweise eines Proxy-Servers siehe unten Teil 2, C. III. 8. a) (2) (b).
[26] Einige Internet-Dienste verwenden spezielle Protokolle, die in ihrer Funktionsweise jedoch grundsätzlich mit dem TCP/IP vergleichbar sind. WWW, E-Mail, File Transfer, News und Instant Messaging werden im Anschluss genauer dargestellt.

Kommunikationsverbindung verwendeten Protokolle, ist der TCP/IP-Stack[27]. Die Adressen, mit denen die zu versendenden Datenpakete versehen werden, bezeichnet man als IP-Adressen. Sie werden typischerweise durch vier Zahlenblöcke (Bytes) dargestellt, die mit Punkten verbunden werden (z.B. 195.65.124.23).

Jeder dauerhaft in das Internet eingebundene Rechner (Host) und Router hat eine eigene, 32 Bit lange IP-Adresse. Auch Rechner, die nur vorübergehend an das Internet angeschlossen werden – z.B. bei der Einwahl von zu Hause aus – bekommen für die Dauer der Verbindung eine individuelle IP-Adresse zugeteilt, anhand derer sie zu identifizieren sind. IP-Adressen sind eindeutig und unverwechselbar. Um Adresskonflikte zu vermeiden, werden die Netzwerkadressen von dazu berufenen Organisationen vergeben.

Die Funktionsweise des Internet-Protokolls kann mit der eines Briefumschlags verglichen werden, der eine Absender- und Empfängeradresse trägt, und in dessen Innern sich das Datenpaket befindet. Die Spezifika des Datenpaketes ergeben sich aus dem Transmission Control Protocol (TCP). Das TCP zerlegt die zu versendende Datei in viele kleine Datenpakete und nummeriert diese fortlaufend. Bildlich gesprochen versieht das TCP die Datenpakete mit nummerierten Umschlägen. Diese werden dann in den Umschlägen des IP dem angegebenen Empfänger zugestellt. Das TCP bildet dabei zusätzlich eine Prüfsumme der zu sendenden Daten und vergleicht diese mit der aus den empfangenen Daten errechneten Prüfsumme. Stimmen die beiden Prüfsummen nicht überein, so werden die Daten – soweit erforderlich – noch einmal übermittelt. Auch wenn empfangene Datenpakete nicht quittiert werden, erfolgt automatisch eine erneute Übersendung. Das TCP übernimmt somit eine Fehler- und Flusskontrolle.[28]

Eine weitere wichtige Aufgabe des TCP ist die Vergabe von Portnummern an die einzelnen Pakete: Je nachdem, für welchen Internet-Dienst (E-Mail, WWW, News etc.) eine Datei bestimmt ist, muss sie mit einer entsprechenden Portnummer versehen werden. Die Portnummer ist ein Zusatz zur IP-Adresse, der innerhalb der verschiedenen Dienste eine verlässliche Zuordnung ermöglicht. Die Portnummern sind entweder standardisiert oder müssen bei einem speziellen Server abgefragt werden. Bei den standardisierten Portnummern repräsentiert jede Nummer einen unterschiedlichen Dienst (z.B. Port 119 für den News-Dienst; Port 80 für das WWW). Erhält der Empfänger also ein Datenpaket mit der Portnummer 119, wird dieses dem News-Dienst zugeordnet und mit der entsprechenden News-Software verarbeitet. Die Portnummern von Sender und Empfänger müssen stets gleich sein, bei manchen Diensten (z.B. beim FTP-Dienst) sind sie sogar frei wählbar.[29]

Der Weg der einzelnen Datenpakete durch das Netz über die verschiedenen Router bis zum Empfänger wird regelmäßig nicht vom Versender, sondern vom Internet-Protokoll bestimmt. Zwar sieht das Protokoll die Möglichkeit vor, den Datenpaketen ein bestimmtes Routing vorzuschreiben, aber hiervon wird nur in seltenen Fällen Gebrauch gemacht. Über die im Header veränderbaren Optionen „strict source routing“ und „loose source routing“ kann der Sender beispielsweise

---

[27] Die aktuelle Version des IP-Protokolls wird auch als „IPv4“ bezeichnet und soll längerfristig von Version 6 („IPv6“) abgelöst werden – siehe dazu unten Teil 2, C. III. 3.
[28] *Sieber*, Kontrollmöglichkeiten – Teil 1, **CR** 1997, S. 594.
[29] *Sieber*, Kontrollmöglichkeiten – Teil 1, **CR** 1997, S. 595.

verhindern, dass seine Datenpakete über die Verbindungs-rechner eines bestimmten Staates geleitet werden. Im Normalfall berechnet das Internet-Protokoll – vor allem unter Berücksichtigung freier Leitungen – immer nur den Weg des Datenpaketes zum nächstgelegenen Router im Hinblick auf die Erreichung des Endzieles. Das Datenpaket wird so durch jede Übermittlung seinem Ziel ein Stück näher gebracht, wobei die einzelnen Übertragungsschritte auch als Sprünge oder Hops bezeichnet werden. Die verschiedenen Datenpakete einer einzelnen Nachricht (z.B. einer E-Mail) können dabei auf unterschiedlichen Wegen – und auch in unterschiedlicher Reihenfolge – ihr Ziel erreichen, da sie dort vom TCP wieder in der richtigen Reihenfolge zusammengesetzt werden[30].

3. Das Domain Name System (DNS)

Da Menschen in der Regel besser mit Namen als mit Zahlen umgehen können, werden den aus Dezimalzahlen bestehenden IP-Adressen bestimmte Namen (auch „Domains“) fest zugeordnet. So ist z.B. dem Teilnetz der Universität Gießen mit der IP-Adresse 134.176.xxx.xxx der Domain-Name „uni-giessen.de“ zugeordnet.

Die Verknüpfung von IP und Domain ermöglicht es, dass man als Zieladresse für eine Datei „ftp.uni-giessen.de“ anstelle der zugeordneten IP-Adresse „134.176.2.11“ angeben kann. Allerdings muss der Name erst wieder in die Zahlenform übersetzt werden, bevor der Datentransfer erfolgen kann. Hierfür gibt es eigene Server, die in großen Datenbanken die Zuordnungen beinahe aller vergebenen IP-Nummern zu den entsprechenden Hostnamen bereithalten, sogenannte Nameserver oder DNS-Server. Der Übersetzungs-vorgang wird auch als „DNS-Lookup“ bezeichnet.

Der Domain-Name (im Beispiel „uni-giessen.de“) muss bei dafür vorgesehenen Organisationen gegen eine fortlaufende Gebühr registriert werden. Bei den Domains unterscheidet man grob zwischen Top Level Domains (TLDs) und Second Level Domains (SLDs) bzw. Subdomains. Seit einigen Jahren werden die nachfolgenden Top Level Domains vergeben:

Domain-Endung	***Einsatzbereich***	***Beispiel***
.edu	US-Universitäten	http://www.virginia.edu
.mil	US-Militäreinrichtungen	http://www.navy.mil
.gov	US Regierungseinrichtungen	http://www.fbi.gov
.int	Internationale Organisationen	http://www.wipo.int
.net	Netzbetreiber	http://www.tiscali.net
.org	Non-Profit-Organisationen	http://www.icann.org
.com	Kommerzielle Organisationen	http://www.microsoft.com

Abbildung 2 – die sieben ursprünglichen Top Level Domains

Von 1993 bis 1999 oblag die Vergabe der Top Level Domains .com, .net und .org exklusiv dem US-Unternehmen *Network Solutions, Inc. (NSI*[31]*)*, welches seinerzeit von der US-Regierung dazu beauftragt wurde. Unter dem Namen *International Network Information Center (InterNIC*[32]*)* hatte *NSI*

[30] *Sieber,* Kontrollmöglichkeiten – Teil 1, **CR** 1997, S. 594.
[31] http://www.networksolutions.com.
[32] *InterNIC* war ein gemeinsames Projekt der US-Regierung und von *NSI*.

schätzungsweise über 5 Millionen „virtuelle Adressschilder“ registriert, bis im April 1999 das Registrierungsmonopol der *NSI* zugunsten fünf weiterer Unternehmen bzw. Organisationen[33] aufgehoben wurde. Koordiniert wird der laufende Liberalisierungsprozess von einer eigens ins Leben gerufenen Organisation: Die *Internet Corporation for Assigned Names and Numbers (ICANN*[34]*)* wurde von der US-Regierung als eine Art „Aufsichtsrat des Internet“ gegründet, um das Funktionieren des DNS zu gewährleisten.[35]

Da sich die „Namensvorräte“ vor allem in der .com-Domain rapide verknappen – bereits Mitte 1999 standen nur noch ca. 1.760 Wörterbuchbegriffe zur Verfügung[36] – beschloss die *ICANN* im Juli 2000 die Einführung von neuen TLDs[37]. Im November 2000 wurde erstmals bekannt gegeben, wie die neuen Domains aussehen, und für welche Einsatzbereiche sie vorgesehen sind.[38]

Domain-Endung	***Einsatzbereich***
.biz	Unternehmen / Business (allgemein)
.info	Informationsseiten aller Art (frei zugänglich)
.pro / .prof	Berufsgruppen
.museum	Museen
.aero	Luftverkehr / Fluggesellschaften
.coop	Genossenschaftliche Unternehmen
.name	Einzelpersonen (frei zugänglich)

Abbildung 3 – die neuen Top Level Domains

Zu den TLDs gehören streng genommen auch die Country Domains (z.B. .de für Deutschland, .fr für Frankreich oder .nl für die Niederlande), die eine geographische Strukturierung von Domain-Namen ermöglichen[39]. Deren Vergabe obliegt jedoch nicht *NSI* oder den neuen Mitbewerbern, sondern Registrierungsstellen in den entsprechenden Ländern.[40]

Hierzulande war bis zum Mai 1996 ausschließlich das *Deutsche Network Information Center e.G. (DENIC*[41]*)* für die Vergabe von Domains mit der Endung .de zuständig und hat in dieser Eigenschaft eine Vielzahl von IP-Adressen registriert. Durch das starke Wachstum des Internet und den damit verbundenen technischen Aufwand hat sich das *DENIC* jedoch von der Registrierung getrennt und diese an diverse deutsche ISPs übergeben, die allerdings Mitglieder in der *DENIC*-Genossenschaft sein müssen.

---

[33] Zunächst erhielten nur *AOL*, das *Internet Council of Registrars* (*CORE*), die *France Telecom/Oléane*, *Melbourne IT* und *register.com* die Erlaubnis, die Top Level Domains .COM, .NET und .ORG zu vergeben.
[34] http://www.icann.org.
[35] Vgl. *Kuri*, **c't** 5/1999, S. 32.
[36] *Pitscheneder*, Streit um das Namensschild, **FOCUS** 18/1999, S. 250.
[37] *Ermert*, Web-Taufpaten, **c't** 16/2000, S. 42.
[38] Die Domain .info ist mittlerweile verfügbar, die anderen Domains werden nach und nach zur Vergabe freigegeben.
[39] Eine umfangreiche Liste von Country Domains findet sich unter http://www.iana.org/cctld/cctld-whois.htm.
[40] In naher Zukunft wird es auch die Länder-Domain .eu für europäische Internetangebote geben, doch zuerst muss die EU-Kommission eine entsprechende Infrastruktur für die Vergabe der Domains schaffen.
[41] http://www.denic.de.

Das *DENIC* verwaltet weiterhin Internet-Adressen, insbesondere die Country Domain .de und führt alle dazugehörigen Tätigkeiten für Mitglieder und Nichtmitglieder aus – z.B. Inkasso, technische und betriebliche Betreuung der Anlagen und Geräte, Wahrnehmung der Interessen der Genossenschaft, Herstellung und Unterhaltung der notwendigen eigenen Konnektivität. Die sicherlich wichtigste Aufgabe, die das *DENIC* erfüllt, ist der Betrieb des Primary Nameservers für die Domain .de und die damit verbundenen Registrierungsvorgänge. Der Primary Nameserver muss, da er über sämtliche relevanten Daten für den deutschen Teil des Internets verfügt, ohne Ausfälle 24 Stunden am Tag verfügbar sein.[42]

Unter Second Level Domains oder Subdomains versteht man Domains, die innerhalb einer Top Level bzw. Country Domain vergeben werden. Subdomains der Country Domain .de sind z.B. „uni-giessen", „dresdner-bank" oder „focus". Subdomains der Top Level Domain .com sind unter anderem „microsoft" und „coca-cola".

Je nachdem, wofür ein Rechner innerhalb eines Teilnetzes eingesetzt wird, erhält er ein eigenes Kürzel vor den Domain-Namen. Getrennt nach den verschiedenen Diensten gibt es bei der Universität Gießen Rechner mit den folgenden Adressen:

www.uni-giessen.de (für den WWW-Dienst)
ftp.uni-giessen.de (für den File Transfer Dienst)
news.uni-giessen.de (für den News-Dienst)

II. Zugang des privaten Nutzers zum Internet

Den Zugang zum Internet erhält der private Nutzer im Normalfall über einen ISP oder einen Online-Dienst[43]. Mit diesem schließt er zunächst einen Vertrag über die Bereitstellung eines Internet-Zugangs. Mit seinem Modem[44] oder einem ISDN-Adapter[45] stellt er eine Telefonverbindung zum ISP her. In den meisten Fällen unterhalten ISPs flächendeckend Einwahlknoten oder haben eine bundesweit einheitliche Service-Nummer eingerichtet, so dass dem Nutzer für die Telefonverbindung mit dem Rechner des ISP nur die Kosten für den Ortsbereich oder sogar geringere Kosten entstehen. Hinzu kommt schließlich ein monatlicher Betrag für die Bereitstellung des Zuganges, den der Nutzer an den ISP zu entrichten hat. Neben diesem klassischen Vertragsmodell gibt es außerdem Internet-By-Call und die sogenannten Flatrates. Internet-By-Call bezeichnet einen Service, bei dem sich der Kunde unter einer kostenpflichtigen Telefonnummer ins Internet einwählen kann, wobei die Kosten für den Dienst per Telefonrechnung abgerechnet werden. Bei

---

[42] Weitere Nameserver (Secondary Nameserver), die dafür Sorge tragen sollen, dass Informationen über registrierte .de-Domains bestmöglich im Internet verbreitet werden, befinden sich momentan in Deutschland (xlink1.xlink.net, ns.germany.eu.net), innerhalb Europas (ns.ripe.net, sunic.sunet.se) und an zentralen Standorten in den USA (ns.uu.net, admii.arl.army.mil, dns-west.nersc.gov).

[43] Bei Studenten übernehmen die Rechenzentren der jeweiligen Universitäten diese Funktion.

[44] Modulator / Demodulator – ein Modem wandelt die digitalen Informationen eines PC in analoge Signale um, die dann über analoge Telefonleitungen versendet werden können. Das Modem der Gegenstelle wandelt diese dann wieder zurück in digitale Informationen. Mittlerweile ist ein Modem Bestandteil der meisten PC-Komplettsysteme, die in Deutschland verkauft werden.

[45] Bei ISDN (Integrated Services Digital Network) handelt es sich um eine weit verbreitete Variante der digitalen Telefontechnik. Ein ISDN-Adapter – meist in Form einer Steckkarte – erweitert den heimischen PC um einen ISDN-Telefonanschluss.

einer Flatrate hingegen zahlt der Nutzer einen festen monatlichen Betrag an den ISP und kann sich dafür rund um die Uhr über eine Freecall-Nummer, d.h. ohne Telefonkosten, mit dem Internet verbinden. Zu einigen ISPs kann der Nutzer anstelle einer Modem- oder ISDN-Verbindung auch eine ADSL[46]-Verbindung herstellen. Diese ist um ein Vielfaches schneller als die beiden herkömmlichen Verbindungsmethoden, erfordert jedoch zusätzliche Hardwarekomponenten und ist derzeit noch nicht für jeden Haushalt erhältlich.

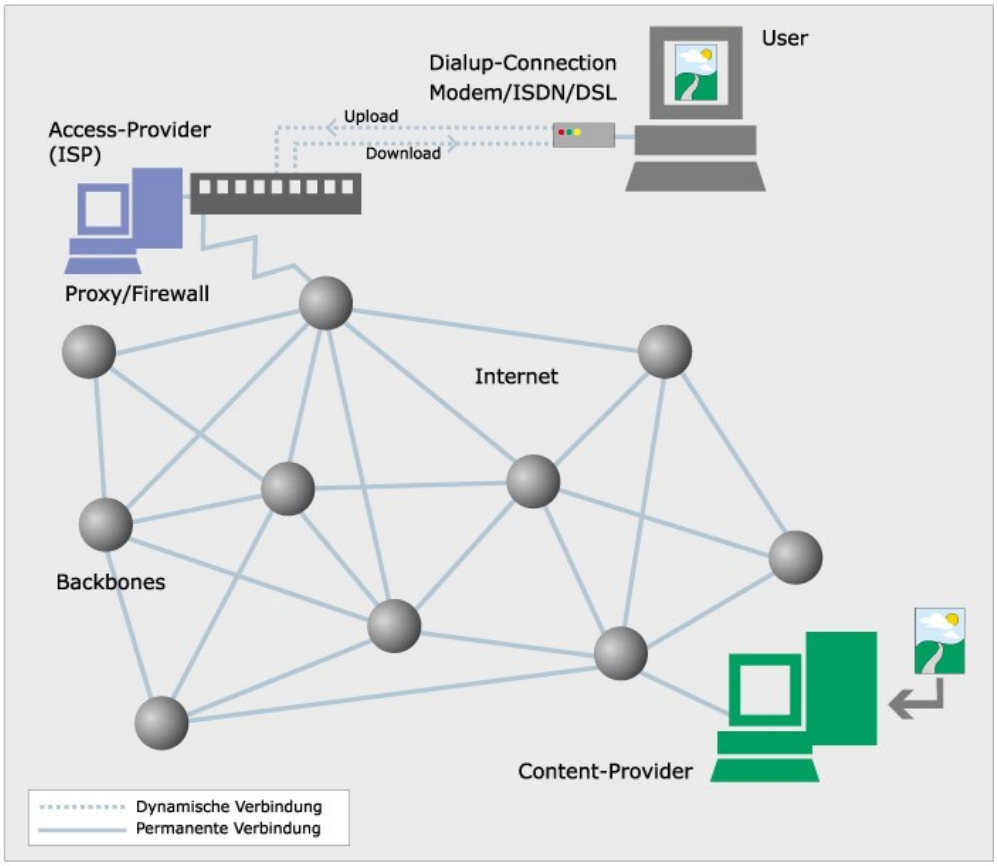


Abbildung 4 – die Verbindung des privaten Nutzers mit dem Internet

Die Rechner des ISP sind dauerhaft durch schnelle Datenleitungen („Standleitungen“ oder „Permanent Lines“) mit dem Internet verbunden. Über den zwischengeschalteten Einwahlknoten wird der private Nutzer somit Teil des Internet – allerdings nur für die Dauer des „Gesprächs“ mit seinem ISP. Da sich an einem Einwahlknoten eines ISP oftmals viele Kunden gleichzeitig einwählen, befinden sich dort mehrere Modems bzw. ISDN- oder ADSL-Gegenstellen. Wählt sich ein Nutzer ein, wird er mit einer freien Gegenstelle verbunden, sofern nicht alle „Andockmöglichkeiten“ belegt sind. So erhält der Rechner des Einwählenden für die Dauer der Verbindung immer die IP-Adresse der Gegenstelle, über die er mit dem Internet verbunden ist. Da sich die IP-Adresse mit jeder neuen

---

[46] Asymmetric Digital Subscriber Line – im Vergleich zum analogen Modem, wo bestenfalls 56 KBit/s Sekunde übertragen werden können, können bei ADSL bis zu 8 MBit/s transportiert werden. Das entspricht einem Text von ca. vier Seiten Länge im Verhältnis zu einem Text von ca. 570 Seiten Länge, der innerhalb einer Sekunde zwischen zwei Rechnern übertragen werden kann. Größter deutscher Anbieter für ADSL-Anschlüsse ist die *Deutsche Telekom* mit ihrem Produkt *T-DSL*.

Einwahl beim Provider ändern kann, bezeichnet man die auf diese Weise vergebenen Adressen auch als dynamische IP-Adressen („dynamically allocated IP addresses“ oder kurz „DYNIPs“). Anhand der ersten Bytes der IP-Adresse kann man jedoch immer noch das (Teil-)Netz des ISP erkennen. Lediglich das hintere Byte oder die beiden hinteren Bytes variieren.

Neben den dynamischen Verbindungen zum ISP sind auch permanente Verbindungen möglich. In diesem Fall spricht man ebenfalls von Standleitungen, welche derzeit hauptsächlich von Unternehmen angemietet werden. In Deutschland ist die Miete von Standleitungen noch sehr kostenintensiv, wohingegen sie z.B. in den USA auch für den Privatkunden erschwinglich ist. Besitzer einer Standleitung bekommen von ihrem Provider eine permanente IP-Adresse („PERMIP“) zugeteilt.

D. Die wichtigsten Bereiche / Dienste des Internet[47]

I. World Wide Web (WWW)

Beim WWW handelt es sich wohl um den bekanntesten Bereich des Internet. Das „virtuelle Schaufenster“ wird in erster Linie dazu genutzt, Informationen in multimedialer Form zu verbreiten und zu beziehen. Auf sogenannten Homepages bzw. Webseiten präsentieren sich Unternehmen, Organisationen, Privatpersonen und sonstige Einrichtungen. Das WWW ermöglicht einen Internet-Auftritt in Schrift, Bild (auch Video), Ton und sonstigen Formen der Animation. Neben der reinen Präsentation bieten kommerzielle Anbieter zunehmend auch Waren und Dienstleistungen über das WWW an. Unter den Begriff des E-Commerce fallen vor allem Online-Shopping, Online-Banking oder Online-Brokerage. Allerdings werden diese neuen Möglichkeiten in Deutschland vom Verbraucher nur zögerlich in Anspruch genommen. Für die nächsten Jahre wird jedoch mit einer deutlichen Steigerung der Inanspruchnahme dieser Leistungen gerechnet.

Ein weiterer wichtiger Nutzen des WWW liegt in seiner Eigenschaft als riesiger Informationspool. Es gibt kaum eine erdenkliche Information, die nicht über das WWW bezogen werden kann. Dies ist unter anderem dadurch bedingt, dass alle großen Medienunternehmen, Universitäten und Forschungseinrichtungen im Web präsent sind. Auch im Bereich der Service-Dienstleistungen – z.B. Support Hotlines für technische Fragen – hat das WWW eine nicht zu unterschätzende Bedeutung erlangt.

Derjenige, der eine Webseite ins Netz stellt und somit Informationen bereitstellt oder Meinungen verbreitet, gilt als Content Provider. Diese sind von den reinen Informationsvermittlern (z.B. *Yahoo.com*) zu unterscheiden, die Listen von Webseiten zusammenstellen, sich jedoch den Inhalt der aufgeführten Seiten nicht zu eigen machen.

Beinahe alles, was man auf Webseiten betrachten kann (z.B. Texte oder Bilder), lässt sich per Mausklick in digitaler Form auf die eigene Festplatte abspeichern (neudeutsch „herunterladen“ oder „downloaden“), um es dort auch ohne Verbindung zum Internet („offline“) zu reproduzieren. Auch Dateien, die sich nicht in eine visuelle Form fassen lassen (z.B. Softwareaktualisierungen – sogenannte Updates), kann man über das WWW herunterladen.

---

[47] Ausgewählt wurden nur solche Dienste, die für die weitere Arbeit von Bedeutung sind. Dienste wie Gopher, Telnet, Archie etc. spielen für den Bereich der Cyberpiraterie keine nennenswerte Rolle.

Die Programme, mit denen man sich im WWW bewegt, werden als (Web-)Browser bezeichnet[48]. Charakteristisch für einen Browser ist seine Bedienung: In ein Eingabefeld können per Tastatur WWW-Adressen eingegeben und somit gezielt angesteuert werden. Mit den sogenannten Back- und Forward-Buttons[49] können – ähnlich den Navigationstasten eines CD-Spielers – die bereits vollzogenen Sprünge von Webseite zu Webseite rückgängig gemacht bzw. wiederholt werden. Das Fortbewegen von Webseite zu Webseite wird allgemein als „Surfen“ oder „Websurfen“ bezeichnet.

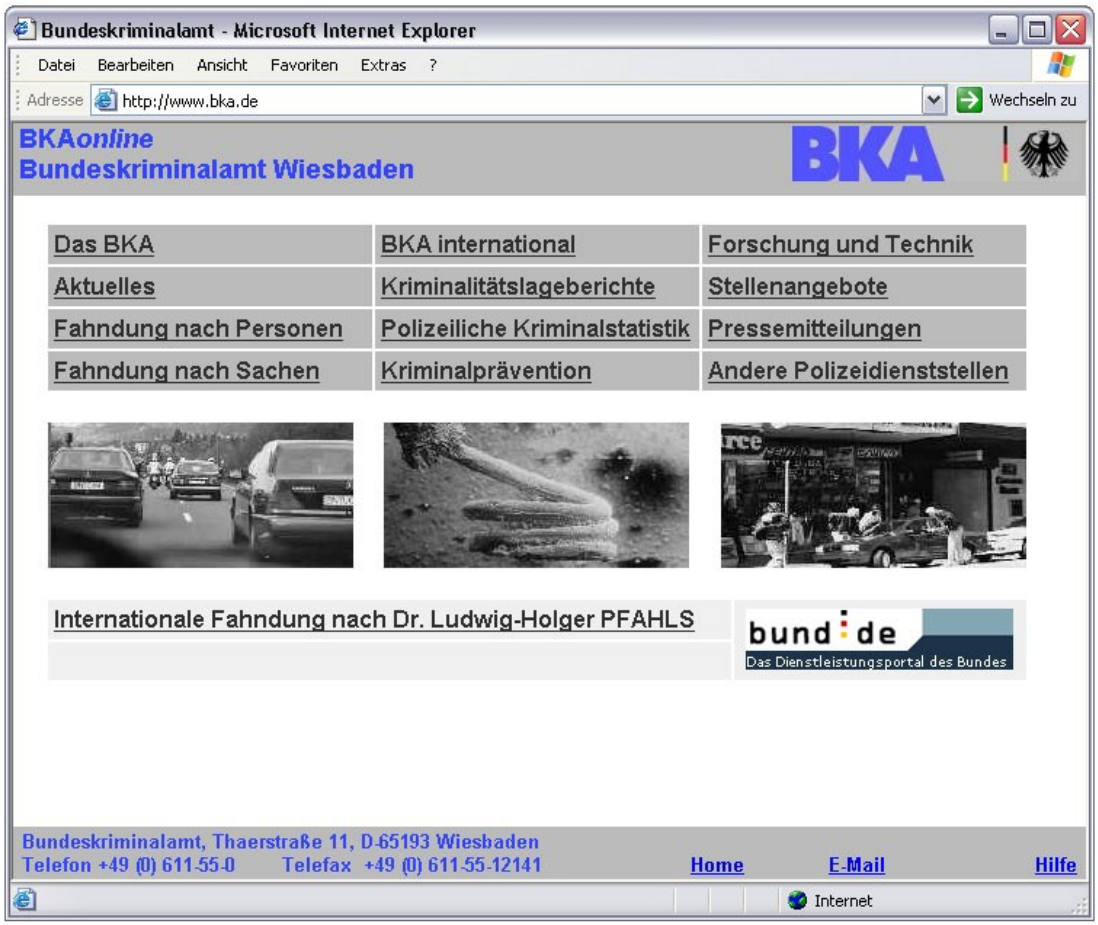


Abbildung 5 – die Homepage des *BKA* im WWW

Im sogenannten Cache der Browser-Software – vergleichbar mit dem menschlichen Kurzzeitgedächtnis – sind die vollzogenen Sprünge als Informationen abgelegt. Je nach Größe des Cache können beliebig viele Sprünge rekonstruiert werden. Im Cache werden außerdem Bilder und andere Informationen der geladenen Webseiten abgelegt, damit diese bei einem Wiederaufrufen der zugehörigen Seiten nicht erneut aus dem WWW heruntergeladen werden müssen, sondern sofort auf dem heimischen PC zur Verfügung stehen.

---

[48] Werden im Verlauf der Arbeit beispielhaft Computerprogramme oder Dateiformate erwähnt, handelt es sich in der Regel um *Windows*-kompatible Software und Dateiformate, da diese am weitesten verbreitet sind. Nach einer Untersuchung des Marktforschungsunternehmens *International Data Corporation (IDC)* hatten *Microsoft Windows* Betriebssysteme 2002 im Bereich der Desktop-Systeme einen weltweiten Marktanteil von 93,85%, http://www.idc.com.

[49] Unter Buttons versteht man in der Computersprache virtuelle Knöpfe, die man mit der Maus betätigen kann.

Um eine höchstmögliche Interaktionsfähigkeit der Browser zu erreichen, werden hauptsächlich von Drittanbietern modulare Programmerweiterungen (sogenannte Plug-Ins) angeboten, mit denen sich die Browser modifizieren lassen. Zu erwähnen sind in diesem Zusammenhang vor allem das Unternehmen *Macromedia*, das mit *Shockwave* bzw. *Flash* weit verbreitete Plug-Ins geschaffen hat, mit denen aufwändige grafische Animationen auf Webseiten ermöglicht werden, sowie *RealNetworks*, die mit der Entwicklung von *RealVideo* und *RealAudio* einen Quasi-Standard für die Verbreitung von Video- und Klang-Daten im WWW gesetzt haben.

Die Dateien, aus denen sich Webseiten zusammensetzen, befinden sich auf sogenannten Webservern. Diese müssen permanent mit dem Internet verbunden sein, damit die Informationen einer Homepage rund um die Uhr abrufbar sind. Meist werden sie von ISPs betrieben, die dort für jeden ihrer Kunden einen bestimmten Speicherplatz zur Erstellung einer Homepage („Webspace") bereithalten. Allerdings gibt es auch Betreiber von Webservern, die jedermann werbefinanzierten Webspace kostenlos zur Verfügung stellen (z.B. *XOOM, Geocities* oder *Tripod*). Die Vergabe geschieht meist ohne Überprüfung der wahren Identität des Webseitenbesitzers (Content Providers), so dass in diesem Zusam-menhang auch von anonymem Webspace gesprochen werden kann. Der Speicherplatz, der pro Homepage zur Verfügung steht, ist im Schnitt auf ca. 10 Megabyte begrenzt, weshalb sich anonymer Webspace nur bedingt zur Verbreitung großer Datenmengen eignet.

Die grundlegende Programmiersprache, in der Homepages programmiert werden, ist die Hypertext Markup Language (HTML). Um eine einfache Homepage in HTML zu erstellen, bedarf es mittlerweile keiner tiefgreifenden Programmierkenntnisse mehr. Durch die weite Verbreitung sogenannter WYSIWYG[50]-HTML-Editoren ist das Programmieren von Webseiten schnell erlernbar und beinahe jedermann möglich. Die fertig programmierte Homepage wird schließlich auf den Rechner transferiert (neudeutsch: „hochgeladen" oder „upgeloadet"), auf dem sich der Webspace befindet.

Die Orientierung im WWW kann auf verschiedene Arten erfolgen: Zunächst besteht die Möglichkeit, durch das Eingabefeld eines Browsers gezielt eine bekannte WWW-Adresse anzusteuern. WWW-Adressen werden gemeinhin als URLs (Uniform Resource Locators) bezeichnet. Jede Seite hat einen individuellen URL, der fast immer mit dem Kürzel „www" beginnt und mit der entsprechenden Domain endet (z.B. „www.uni-giessen.de"). Aufgrund der logischen Struktur der Adressen ist es auch möglich, eine gesuchte Seite durch Ausprobieren zu finden.[51]

An die Domain-Endung einer Adresse sind häufig Ketten von Begriffen und Zeichenfolgen angehängt, die durch sogenannte Slashes (rechtsgeneigte Schrägstriche) miteinander verbunden sind. Die Zeichen, die jeweils zwischen zwei Slashes eines URL stehen, bilden die Ordnernamen der Verzeichnisstruktur der Homepage. Ganz am Ende der URL – also hinter dem letzten Slash – steht der Name der Datei, die man mit der URL aufruft:

http://www.domain.de/ordner/unterordner/unterordner2/datei.html

http://www.domain.com/o53425/neu/briefe/brief_1.doc

---

[50] WYSIWYG steht für „what you see is what you get".

[51] Interessiert man sich beispielsweise für die Produkte des Automobilherstellers Ford, wird man die internationale Präsentation unter „www.ford.com" und die deutsche Webseite unter „www.ford.de" finden.

Sucht man nach einer Information, weiß jedoch nicht, unter welchem URL man diese finden kann, bieten sich kostenfreie Suchdienste bzw. Suchmaschinen (z.B. *Google, AllTheWeb, Altavista, Metacrawler, HotBot, Lycos* oder *Yahoo*) an.[52] Suchdienste unterhalten in den meisten Fällen eigene Datenbanken gigantischen Ausmaßes, die Informationen über Webseiten aus aller Welt enthalten. Um diese Datenbanken auf dem aktuellsten Stand zu halten, durchforsten spezielle Programme („Spiders" oder „Bots") das Web rund um die Uhr.[53] Sie „hangeln" sich dabei von URL zu URL, sammeln Informationen in Form von Schlüsselworten auf den durchsuchten Seiten und übertragen diese in die Datenbank der Suchmaschine. Auf diese Weise wird versucht, jede bestehende Seite des WWW anhand von Schlüsselworten zu katalogisieren.

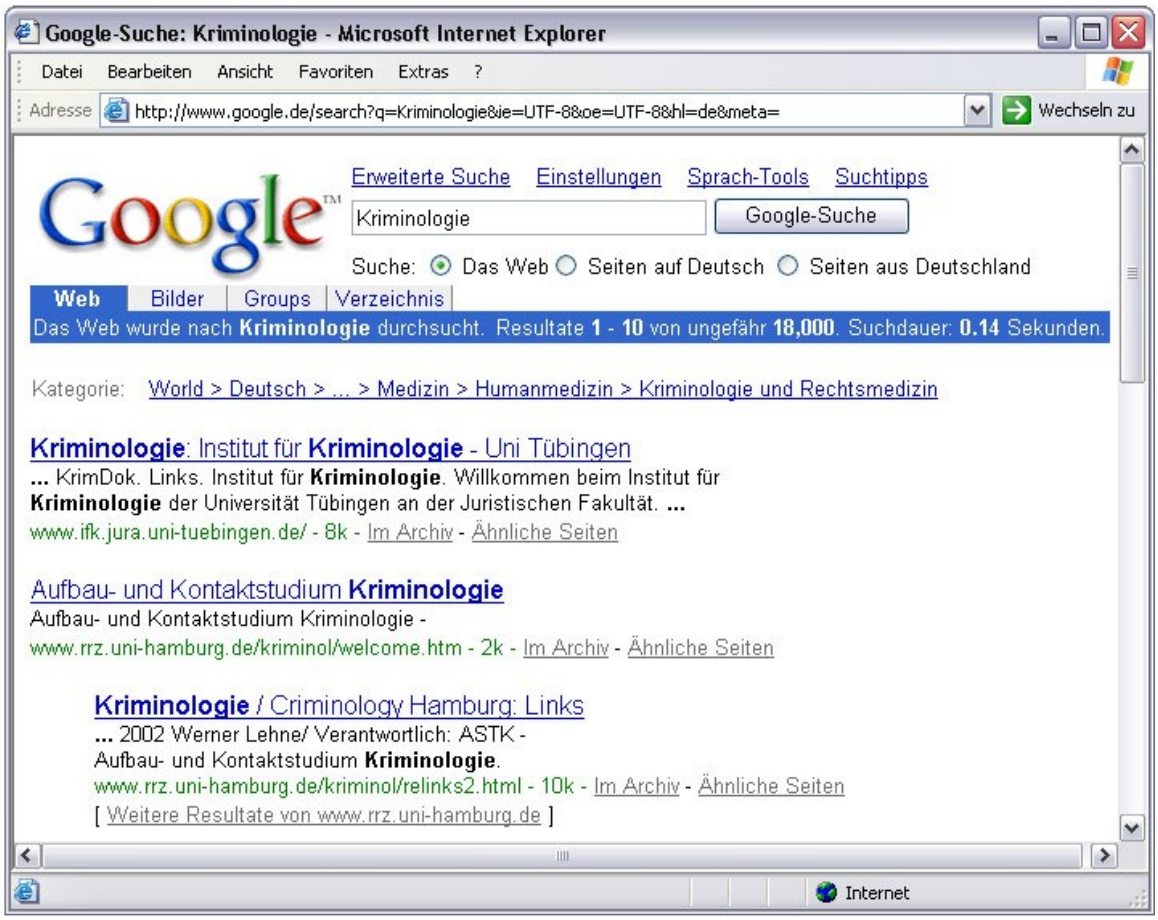


Abbildung 6 – Homepage des Suchdienstes *Google* mit Trefferliste

Auf den Homepages der Suchdienste befindet sich immer ein Eingabefeld - nicht zu verwechseln mit dem URL-Eingabefeld des Browsers - in welches man einzelne Suchbegriffe oder auch Suchphrasen eingeben kann. Per Mausklick wird dann eine Abfrage bei der Datenbank des Anbieters gestartet, woraufhin eine Trefferliste angezeigt wird, die diejenigen URLs anzeigt, die mit den Suchbegriffen korrelieren. Die gefundenen URLs werden in Form von Hyperlinks angezeigt. Als Hyperlinks (auch „Links") bezeichnet man die in einem Text farbig hervorgehobenen Verweise zu anderen Webseiten,

---

[52] Die meisten Suchdienste finanzieren sich über Werbeeinblendungen auf ihren Webseiten.
[53] Vgl. *Bager*, **c't** 23/1999, S. 159.

die man mit der Maus anklicken kann, wodurch der Browser unmittelbar dem Link folgt und die verknüpfte Seite ansteuert.

Hyperlinks findet man jedoch nicht nur in Trefferlisten von Suchdiensten, sondern auf fast jeder Homepage. Ähnlich den Fußnoten einer wissenschaftlichen Arbeit, können Links die Funktion haben, dem Leser weiterführende Informationen zu verschaffen. Auf zahlreichen privaten Homepages hat es sich zudem eingebürgert, eine Rubrik namens „Links" einzurichten, unter der der Content Provider seine favorisierten Webseiten auflistet, um den Besuchern seiner Seite Empfehlungen auszusprechen.

Mit Hyperlinks können nicht nur Verweise auf andere Webseiten gesetzt werden, sondern ein Link kann auch mit einer Datei jedweder Art verknüpft werden, so dass mit dem Anklicken dieses Links keine neue Seite geöffnet, sondern das Herunterladen einer Datei initiiert wird. Hierbei ist zu beachten, dass sich die Datei, mit der der Link verknüpft ist, nicht zwangsläufig auf dem Webserver befinden muss, auf dem auch die Homepage liegt. So kann auf einer Homepage, die ein Nutzer auf dem Webserver seines deutschen ISP eingerichtet hat, ein Link auf eine Datei sein, die sich auf einem Server in Burkina Faso befindet.

Viele Suchdienste stellen neben der Suchfunktion auch nach Interessengebieten geordnete Link-Listen („Web-Indizes") bereit und werden somit im klassischen Sinne als Informationsvermittler tätig.

II. E-Mail

Electronic Mail ist neben dem WWW der wohl bekannteste Dienst des Internet. Die „elektronische Post" wird von beinahe jeder Person genutzt, die über einen Internet-Zugang verfügt. Ihr größter Nutzen besteht darin, dass Nachrichten in wenigen Sekunden rund um den Globus versendet werden können, ohne Ressourcen in Anspruch zu nehmen, die sonst für den Transport eines realen Schriftstückes verbraucht würden[54]. In der E-Mail-Technologie spiegelt sich somit auch die vielzitierte Idee des „paperless Office" wider.

Jeder Internetnutzer bekommt im Regelfall eine individuelle E-Mail-Adresse von seinem ISP zugeteilt. Dabei hat sich folgender Standard etabliert: vorname.name@domain[55]. Abweichend von diesem Standard können vor dem „@"-Zeichen auch einzelne Namen oder Phantasienamen stehen. Verfügt eine Person über eine eingerichtete und registrierte E-Mail-Adresse, spricht man auch von einem E-Mail-Account.

Mit einer E-Mail können neben einfachen Textbotschaften (Plain Text) auch Dateien aller Art als Anhang (Attachment) zu diesem Text versendet werden. Die Größe der Dateien, die als Attachment mitgesendet werden dürfen, ist oftmals von den Betreibern der empfangenden Mailserver auf eine bestimmte Megabyte-Zahl begrenzt, um einer Verstopfung der Server vorzubeugen.

Neben einzelnen Botschaften, die sich Internetnutzer zusenden, gibt es auch die einfach zu realisierende Möglichkeit, Serienbriefe zu verschicken. Die Empfänger von Serien-E-Mails tragen

---

[54] Da E-Mail wesentlich schneller als die „echte" Post ist, wird letztere im Internet oftmals als „SnailMail" (Schneckenpost) bezeichnet.

[55] Das Zeichen „@" wird „at" (engl.) ausgesprochen und hat auch die entsprechende Bedeutung.

sich oftmals auf Webseiten in dafür vorgesehene Listen ein, sogenannte Mailinglisten. Hat jemand beispielsweise Interesse daran, immer über die neuesten Entwicklungen auf dem Gebiet der Rechtsprechung per E-Mail informiert zu werden, wird er im WWW nach einer entsprechenden Mailingliste suchen und sich dort eintragen.

Heutzutage sind Mail-Programme in den Standard-Browsern integriert, doch es gibt auch zahlreiche eigenständige Programme wie *Pegasus Mail* oder *Pine*. Typischerweise werden die Programme vom Nutzer so konfiguriert, dass sie auf seine bestehenden Accounts zugreifen.

Neben dem E-Mail-Account, den der Nutzer bei seinem ISP hat, kann er auch weitere Accounts bei den sogenannten Freemailer-Diensten eröffnen. Diese bieten die Einrichtung eines „web based E-Mail-Accounts" an, also eines E-Mail-Dienstes, der ohne Installation eines E-Mail-Programms komplett über eine Webseite genutzt werden kann. Unternehmen wie *Microsoft* (mit ihrem Dienst *MSN Hotmail*) oder *Global Message Exchange* (*GMX*) ermöglichen es jedem Internetnutzer ohne Überprüfung seiner wahren Identität, kostenlos eine E-Mail-Adresse freier Wahl bei ihnen zu registrieren.[56] Zwar wird im Zuge der Online-Registrierung auf den Webseiten der Freemailer fast immer die Angabe persönlicher Daten verlangt, jedoch gelingt es in den meisten Fällen, auch mit frei erfundenen Angaben (sogenannten Fake-Angaben) einen E-Mail-Account zu bekommen. Freemailer ermöglichen somit, E-Mails weitgehend anonym zu versenden. Das Versenden und Abrufen von E-Mails erfolgt über die Webseite eines Freemailers. Damit nicht jeder, der die E-Mail-Adresse eines anderen kennt, Zugriff auf den entsprechenden E-Mail-Account nehmen kann, ist der Zugang zur Webseite passwortgeschützt. Das Passwort erhält man bei der Registrierung der Adresse. In den geschützten Bereichen der Webseite befinden sich die ungelesenen Nachrichten sowie Eingabefelder und Buttons, anhand derer neue Nachrichten verfasst und abgeschickt werden können.

Für die Suche von E-Mail-Adressen gibt es eigene Suchmaschinen im WWW, deren Nutzung überwiegend kostenlos ist.[57] Einige ISPs bieten auf ihren Webseiten Suchmöglichkeiten nach den bei ihnen registrierten Nutzern an.

III. File Transfer Protocol (FTP)

Bei FTP handelt es sich um ein spezielles Datenübertragungsprotokoll, das ausschließlich dazu bestimmt ist, Dateien jedweder Art möglichst unkompliziert zwischen zwei Rechnern zu übertragen.[58] Hierbei wird auf eine weitgehende grafische Darstellung, wie man sie vom WWW kennt, verzichtet. Dateien wie Bilder oder Sound-Dateien werden bei einem FTP-Transfer nicht sichtbar bzw. hörbar, sondern erscheinen dem Nutzer des FTP-Dienstes nur in Form von Dateinamen auf dem Bildschirm.

Mit einem FTP-Programm (FTP-Client) stellt der Nutzer eine Verbindung zwischen seinem Rechner und einem FTP-Server her[59], und Daten aller Art können bidirektional übertragen werden. Beim

---

[56] Hinter dem @-Zeichen steht jedoch auch hier die Domain des Freemailers (z.B. „freddy@hotmail.com" oder „freddy@gmx.net").
[57] Z.B. http://people.yahoo.com oder http://mesa.rrzn.uni-hannover.de.
[58] Vgl. *Kossel*, **c't** 3/1999, S. 145.
[59] Wie bereits erwähnt, handelt es sich bei Servern grundsätzlich um Rechner, die einen Dienst oder Informationen bereitstellen. Ein FTP-Server stellt demnach Dateien zum Download bereit, die sich in der Regel auf der Festplatte dieses Servers befinden.

Versenden von Daten an den Server spricht man von einem Upload, das Herunterladen von einem Server wird als Download bezeichnet.

Bei zahlreichen FTP-Servern ist ein anonymer Zugang möglich; diese werden als Public FTPs oder „Pubs“ bezeichnet. Davon zu unterscheiden sind die privaten FTP-Server, die durch eine Passwortsperre gegen anonymen Zugang geschützt sind. Um einen privaten FTP zu „betreten“ (sich „einzuloggen“), muss man vom Verwalter des Servers einen sogenannten FTP-Account eingerichtet bekommen, der fast immer aus Benutzername („Login“) und Passwort („Pass“) besteht. Ein Account kann jedoch auch für eine Gruppe von Nutzern vergeben werden, die sich dann alle mit der gleichen Kombination aus Benutzernamen und Passwort einloggen.

Mit der entsprechenden Software kann jedermann auf dem eigenen Rechner einen FTP-Server einrichten, wobei der Zugang zu diesen FTPs in der Regel passwortgeschützt ist.

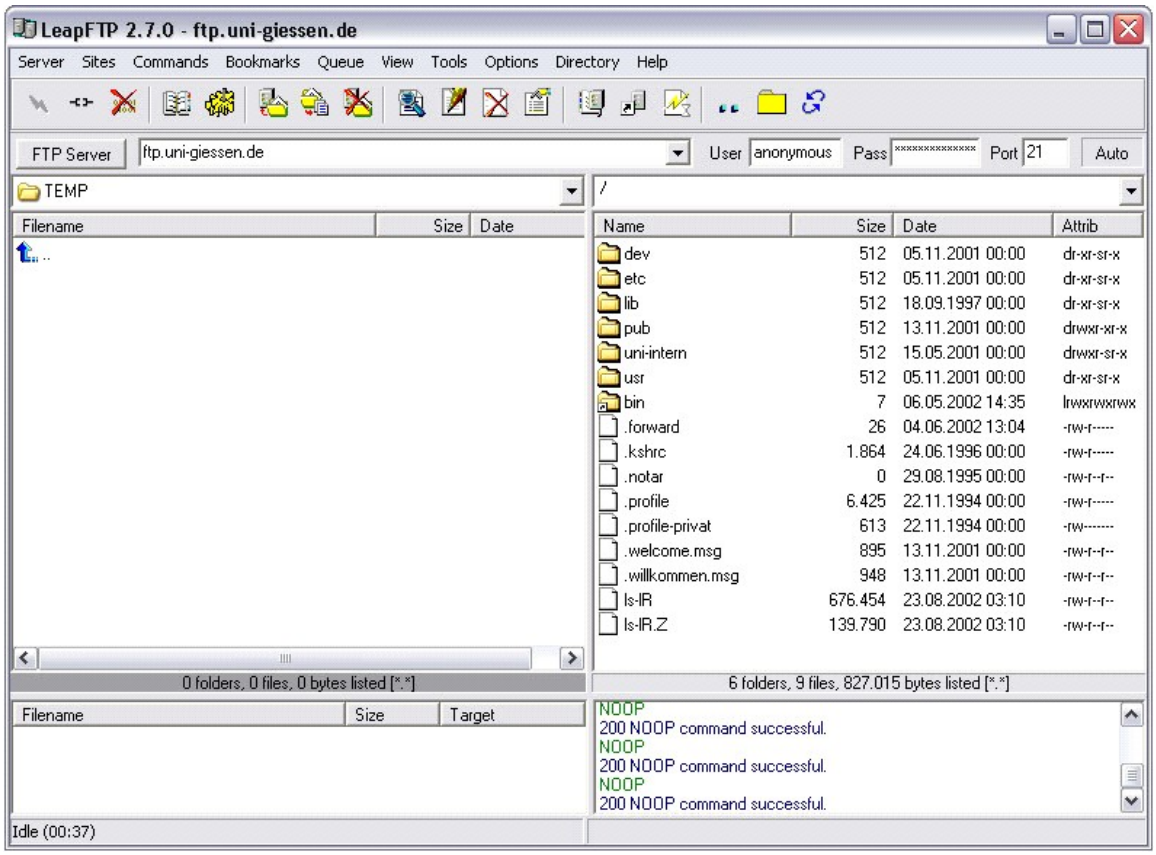


Abbildung 7 – typischer FTP-Client (*LeapFTP* – links Host / rechts Remote)

Zum Herstellen einer Verbindung zu einem FTP-Server benötigt man einen FTP-Client[60]. FTP-Clients sind überwiegend gleich aufgebaut: Charakteristisch ist die Aufteilung der Programmoberfläche in zwei Spalten. In der linken Spalte werden die Verzeichnisse und Dateien des eigenen Rechners (in diesem Zusammenhang auch „Host“) dargestellt. In der rechten Spalte werden die

[60] Weit verbreitete Clients sind *WSFtp, Cute FTP und Leap FTP.*

Verzeichnisse und Dateien des verbundenen FTP-Servers („Remote“) aufgelistet, die für einen Datentransfer bereitgestellt werden. Auf dem FTP-Server wird sich in den meisten Fällen auch ein Verzeichnis mit der Bezeichnung „Incoming“ oder „Upload“ befinden, in welches Daten hochgeladen werden können.

Das Verschieben von Dateien erfolgt auf denkbar einfache Weise: Die zu transferierende Datei – dargestellt in Form eines Dateinamens – wird mit gedrückter linker Maustaste von der linken in die rechte Spalte gezogen, woraufhin ein Upload initiiert wird. Diese Vorgehensweise wird als drag-and-drop bezeichnet und mittlerweile von beinahe allen FTP-Clients unterstützt. Sollte drag-and-drop nicht funktionieren, muss der Nutzer die zu transferierenden Dateien markieren und den Up- bzw. Download durch die Betätigung eines entsprechenden Buttons starten, der oftmals mit einem Pfeil beschriftet ist, der in die gewünschte Übertragungsrichtung zeigt.

IV. Newsgroups / UseNet

Der News-Dienst ist am ehesten mit einer großen Anzahl schwarzer Bretter zu vergleichen, auf denen jedermann Fragen, Meinungen und sonstige Verlautbarungen hinterlassen kann. Durch die Struktur dieser schwarzen Bretter ist es möglich, an eine zuerst „angeschlagene“ Nachricht („Thread“) weitere (Antwort-)Nachrichten („Replies“) anzuhängen, die Bezug auf die Ausgangsnachricht nehmen. Auf diese Weise entstehen häufig virtuelle Schlagabtausche zu strittigen Themen, weshalb das UseNet auch den Ruf eines weltweiten Diskussionsmediums genießt. Andere gängige Bezeichnungen des News-Dienstes sind „Forum“ oder „Conference“.

Im UseNet wird über alle erdenklichen Themen diskutiert, und für jedes Thema gibt es ein eigenes schwarzes Brett – eine sogenannte Newsgroup.

1998 soll es bereits über 20.000 Newsgroups gegeben haben[61], andere Schätzungen gingen sogar von bis zu 35.000 Newsgroups aus[62]. Heutzutage bieten die großen deutschen News-Server-Anbieter ihren Kunden Zugriff auf über 104.000 Newsgroups.[63]

Im UseNet werden jedoch nicht nur Diskussionen geführt oder Erfahrungen ausgetauscht, sondern es besteht auch die Möglichkeit, Dateien auf einen News-Server hochzuladen oder von ihm zu beziehen.

Die Erstellung neuer Newsgroups kann auf verschiedene Art und Weise erfolgen: Gibt es genug Interessenten für ein Thema, wird der Administrator des News-Servers – eventuell nach einer Abstimmung – die neue Gruppe einrichten. Bei den mit dem Kürzel „alt.“ beginnenden Newsgroups hat grundsätzlich jeder Teilnehmer die Möglichkeit, ohne Abstimmung und ohne Genehmigung des Serveradministrators ein neues Diskussionsforum auf dem News-Server zu gründen.

---

61 *Heinzmann/Ochsenbein*, Strafrechtliche Aspekte des Internet – Teil 1, **Kriminalistik** 1998, S. 515.
62 *Sieber*, Kontrollmöglichkeiten – Teil 1, **CR** 1997, S. 595.
63 Vgl. *Bager/Mansmann*, **c't** 18/2002, S. 103.

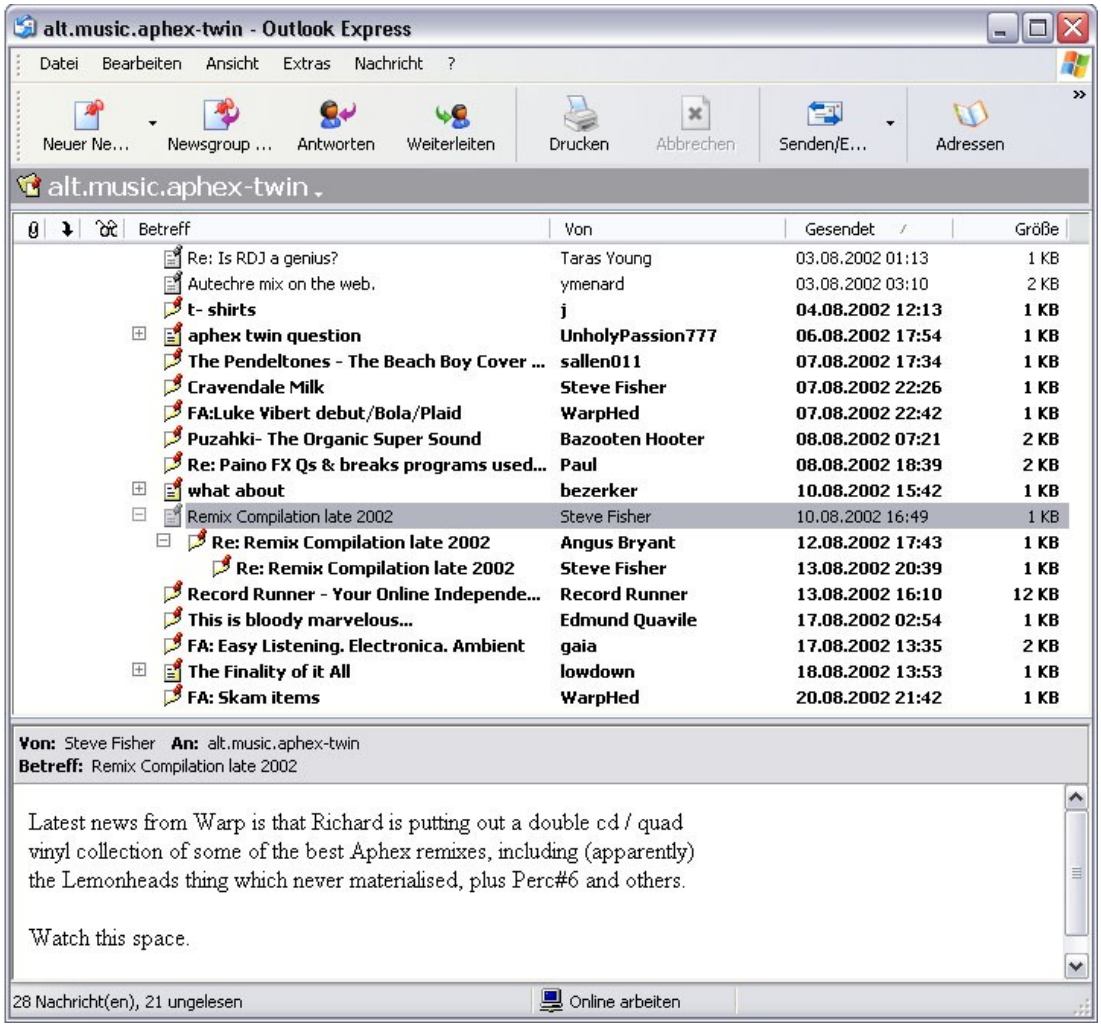


Abbildung 8 – Threads und Antworten in einer Newsgroup

Man unterscheidet grundsätzlich zwischen moderierten und unmoderierten Newsgroups. Bei ersteren gibt es eine Art Kontrollinstanz in Person eines Moderators. Dieser bekommt die neuen, bislang unveröffentlichten Nachrichten zunächst per E-Mail zugeschickt und entscheidet dann, ob diese in die Newsgroup aufgenommen werden. In der Praxis dominieren jedoch unmoderierte Newsgroups das UseNet, da zum einen angesichts der Vielzahl der täglichen Beiträge ein faktisch kaum zu bewältigender Arbeitsaufwand entsteht[64], und zum anderen nur wenig Interesse innerhalb der zensurkritischen Internet-Gemeinde besteht, alle Newsgroups moderieren zu lassen. Die Teilnehmer des News-Dienstes vertrauen eher auf die sogenannte Netiquette, ein Selbstregulierungs-Instrumentarium in Form von allgemeinen Höflichkeitsregeln, die von den Nutzern im Wesentlichen akzeptiert und eingehalten werden.[65]

Neben den zahlreichen öffentlichen News-Servern des UseNet gibt es auch Foren, die von den großen Online-Diensten exklusiv für ihre Kunden bereitgestellt werden (z.B. die *AOL*-Foren). Das UseNet und die privaten Foren werden überwiegend von Privatleuten genutzt.

---

[64] *Sieber*, Kontrollmöglichkeiten – Teil 1, **CR** 1997, S. 595 f.
[65] Eine Aufstellung der gebräuchlichsten Regeln findet sich z.B. unter http://www.easynews.de/support/usenet_html; siehe auch *Bager/Mansmann*, **c't** 18/2002, S. 104.

Programme, mit denen man Newsartikel lesen und verfassen kann, werden als Newsreader bezeichnet. Trotz der abnehmenden Bedeutung des UseNet sind Newsreader noch in den Standard-Browsern integriert. Bei den integrierten Newsreadern wurde jedoch die oben erwähnte Downloadmöglichkeit nur rudimentär integriert, so dass mit ihnen in erster Linie Textbotschaften von den News-Servern heruntergeladen werden. Allerdings gibt es eine Vielzahl eigenständiger Newsreader (z.B. *Xnews, NewsBin* oder *Forte Agent*), mit denen sich auch Dateien komfortabel aus dem UseNet herunterladen oder Dateien in das UseNet speisen lassen.

Die bereits mehrfach erwähnten News-Server sind Computersysteme, die rund um die Uhr riesige Mengen von Nachrichten speichern und bereitstellen müssen. Die Informationen eines News-Servers werden zu Hunderten anderer News-Server übertragen, es erfolgt also ein ständiger Abgleich zwischen den einzelnen Servern. Bei der Synchronisation der nach dem „Store-and-forward-Prinzip" funktionierenden News-Server gelangen neben neuen Nachrichten bestehender Newsgroups auch neu generierte Newsgroups automatisch auf weitere News-Server.

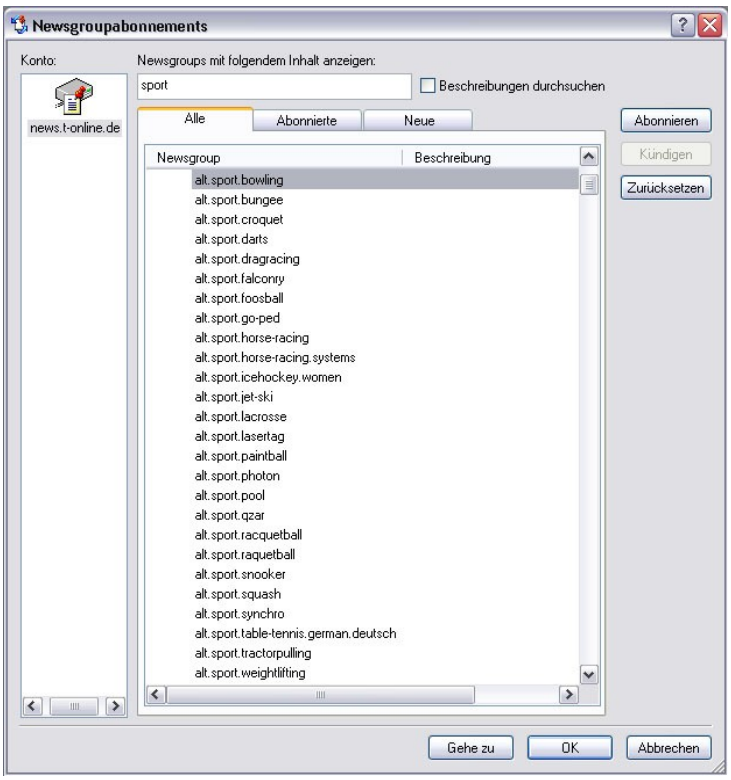


Abbildung 9 – alphabetische Auflistung von Newsgroups

Hat man die Verbindung zu einem News-Server hergestellt, kann man sich mit einem Befehl die komplette Liste aller auf diesem News-Server angebotenen Newsgroups anzeigen lassen. Die Namen der Gruppen lassen Rückschlüsse darauf zu, mit welchen Themen sich die Autoren der darin gesammelten Newsartikel befassen. Unter der Newsgroup „de.talk.jokes" finden sich demnach Witze in deutscher Sprache; eine Gruppe namens „alt.sport.bowling" wird englischsprachige Artikel enthalten, die sich mit der Sportart Bowling befassen.

In der Regel wird durch Doppelklicken auf den Namen einer gelisteten Newsgroup ein neues Fenster geöffnet, in dem dann die Überschriften (Threads) aller innerhalb dieser Newsgroup befindlichen

Artikel erscheinen. An einen Thread kann jedermann eine neue Nachricht anhängen, die auf diesen Bezug nimmt. Selbstverständlich kann man auch einen neuen Thread anlegen, um eine Diskussion zu entfachen oder nach der Lösung für ein Problem zu suchen. Ist der komplette Name einer Newsgroup bekannt, kann man diese bei den neueren Programmen direkt über ein Eingabefeld erreichen. Außerdem besteht die Möglichkeit, die Liste aller Newsgroups eines Servers vom Newsreader nach Schlüsselworten durchsuchen zu lassen.

V. Internet Relay Chat (IRC)

Der Internet Relay Chat gehört zu den wenigen Internet-Diensten, die eine Echtzeitkommunikation ermöglichen.[66] Bei dieser Kommunikationsform steht ein Netzwerk von IRC-Servern einer Reihe von Benutzern zur Verfügung, welche von ihrem Computer aus direkt Nachrichten in dieses Netzwerk schreiben können. Was sie schreiben, wird den anderen Benutzern sofort angezeigt. Somit ist der Chat am ehesten mit einer schriftlich geführten Telefonkonferenz zu vergleichen. Auf den IRC-Servern werden viele hundert verschiedene virtuelle Gesprächsräume (auch „Chatrooms“ oder „Channels“) bereitgestellt, die sich – ähnlich den Newsgroups – nach Interessengebieten unterscheiden. In den größten IRC-Netzen chatten bis zu 50.000 User gleichzeitig.

Jeder Nutzer, der an einem Chat teilnehmen möchte, muss sich unter einem frei zu wählenden Pseudonym („Nickname“ oder „Nick“) anmelden. Neben der Eingabe eines (Nick-)Namens müssen bei den meisten IRC-Programmen (IRC-Clients) auch E-Mail-Adresse und Name des Nutzers angegeben werden. Eine Überprüfung findet jedoch nicht statt, so dass der Nutzer auch erfundene Angaben (sogenannte Fake-Angaben) machen kann.

Alles, was in den Channel geschrieben wird, ist für die anderen Teilnehmer sichtbar. Aktuelle Beiträge fügen sich – ähnlich wie bei einem Ticker – an die bereits lesbaren Äußerungen an. Vor den Äußerungen steht das Pseudonym des Autors in Klammern, so dass man erkennen kann, von wem der Beitrag stammt. Weiterhin besteht die Möglichkeit, ein Privatgespräch (Query) zwischen zwei Nutzern in einem separaten Fenster zu führen, das nur die beiden Beteiligten sehen können.[67]

Manche IRC-Clients ermöglichen dem Nutzer die Einrichtung eines File-Servers („Full-Serve“ oder „F-Serve“). Über einfache Befehle kann jeder beliebige Chat-Partner direkten Zugriff auf die Festplatte des Server-Betreibers nehmen. Hierbei kann sich der Empfänger gezielt Dateien heraussuchen und herunterladen.

In den Chatrooms befinden sich nicht nur menschliche Nutzer, sondern auch sogenannte Bots (Kurzform von Robots). Bots sind kleine Programme, die die Anwesenheit eines realen Nutzers vortäuschen sollen, und überwiegend auf Rechnern laufen, die per Standleitung mit dem Internet verbunden sind. Daher können sich Bots rund um die Uhr mit einem beliebigen (Nick-)Namen in

---

[66] Andere Dienste, über die man in Echtzeit kommunizieren kann, sind z.B. die sogenannte IP-Telefonie oder das Video-Conferencing.

[67] Normalerweise erfolgt die gesamte Kommunikation über einen IRC-Server, allerdings können sich zwei Nutzer über das spezielle *UNIX*-Datenprotokoll DCC (Direct Client-to-Client) auch direkt miteinander verbinden. DCC wird in erster Linie genutzt, um Dateien zu übertragen, jedoch lassen sich ebenso Privatgespräche über DCC führen. Per DCC ausgetauschte Daten bleiben sowohl dem Betreiber des IRC-Servers als auch den IRC-Operatoren verborgen. IRC-Operatoren (auch „IRC-Ops“) sind Personen, die bei der Administration eines IRC-Servers mitwirken. Sie haben weit mehr Rechte und Eingriffsmöglichkeiten als ein normaler User.

einem Chatroom aufhalten. Die Eigentümer (Bot-Owner) setzen Bots aus unterschiedlichen Gründen ein: Der wichtigste Grund besteht darin, einen Channel offen zu halten. Bedingt durch die Struktur der älteren IRC-Netzwerke besteht ein Channel nur so lange, wie sich tatsächlich Nutzer darin aufhalten. Mit dem Verlassen des letzten Nutzers verschwindet auch der Chatroom. Dadurch soll verhindert werden, dass sich „tote" Channels auf den IRC-Servern anhäufen, was einen unnötigen administrativen Aufwand bedeutet. Um also zu sichern, dass ein Channel dauerhaft bestehen bleibt, werden Bots in ihnen platziert. Ein Bot kann auch dazu dienen, die gesamte in einem Channel geführte Konversation für seinen abwesenden Eigentümer aufzuzeichnen. Schließlich gibt es Bots, die per DCC Dateien versenden können. Die sogenannten DCC-Bots automatisieren den F-Serve-Zugriff dergestalt, dass sich jeder Teilnehmer des Channels anhand simpler Befehle („Triggers"), die an den Bot gerichtet werden, Dateien zuschicken lassen kann.

Bedingt durch die rein schriftliche Kommunikation hat sich innerhalb der Internet-Gemeinde die Verwendung zahlreicher Abkürzungen und von sogenannten Emoticons etabliert. Bei einem Emoticon (Kombination aus den englischen Begriffen „Emotion" und „Icon") handelt es sich um eine getippte Zeichenfolge, die Gefühle schriftlich ausdrücken soll. Das bekannteste Emoticon ist wohl ein lachendes Gesicht, das aus einem Doppelpunkt, einem Gedankenstrich und einer geschlossenen Klammer besteht.

```
<net-freak> ...lach' mal wieder! :-)
```

Abbildung 10 – Emoticon

Um mit wenig Aufwand möglichst schnell zu kommunizieren, sind im IRC viele Akronyme und Abkürzungen gebräuchlich. Die meisten Ausdrücke entstammen der amerikanischen Umgangssprache[68]. Hier ein Überblick über die wichtigsten und gebräuchlichsten Abkürzungen[69]:

Abkürzung	*Englische Bedeutung*	*Deutsche Bedeutung*
afaik	as far as i know	soweit ich weiß
brb	be right back	bin gleich zurück
btw	by the way	übrigens
faq	frequently asked questions	häufig gestellte Fragen
lol	laughing out loud (oder) lots of laughter	laut lachend (oder) heftiges Lachen
np	no problem	keine Ursache
thx	Thanks	Danke

Abbildung 11 – gebräuchliche Abkürzungen im IRC

[68] Vgl. *Blümel/Soldo*, S. 110.
[69] Eine umfassende Sammlung von Abkürzungen und Akronymen findet sich unter http://www.ucc.ie/acronyms.

Wie bei den Newsgroups gibt es neben dem öffentlichen IRC exklusive Chats wie z.B. den *AOL*-Chat, und auch der IRC-Dienst wird fast ausschließlich von Privatpersonen genutzt.[70]

Programme, mit denen man am IRC teilnehmen kann, sind ausnahmsweise nicht in den neueren Browsern integriert. Die meisten IRC-Clients sind ähnlich aufgebaut: Im Hauptfenster werden die aktuellen Beiträge angezeigt, die nach und nach „hereintickern". In einer Spalte am rechten Rand des Bildschirmes sind die (Nick-) Namen aller Teilnehmer aufgelistet, die sich derzeit im Channel befinden. Betrachtet man die Auflistung genauer, wird man feststellen, dass sich vor den Namen einiger Teilnehmer @- oder +-Zeichen befinden. Diese Zeichen lassen Rückschlüsse auf den Status der Teilnehmer zu: Teilnehmer, die ein „@" vor dem Namen stehen haben, sind die Channel-Operatoren (Ops). Diese haben Befugnisse, die über die Befugnisse der normalen Nutzer hinausgehen[71]. Das „+" vor einem Namen ist eine Art virtueller Orden.[72] Freunde der Channel-Operatoren oder Operator-Anwärter bekommen es als Zeichen persönlicher Verbundenheit oder Anerkennung von den etablierten Channel-Operatoren verliehen.

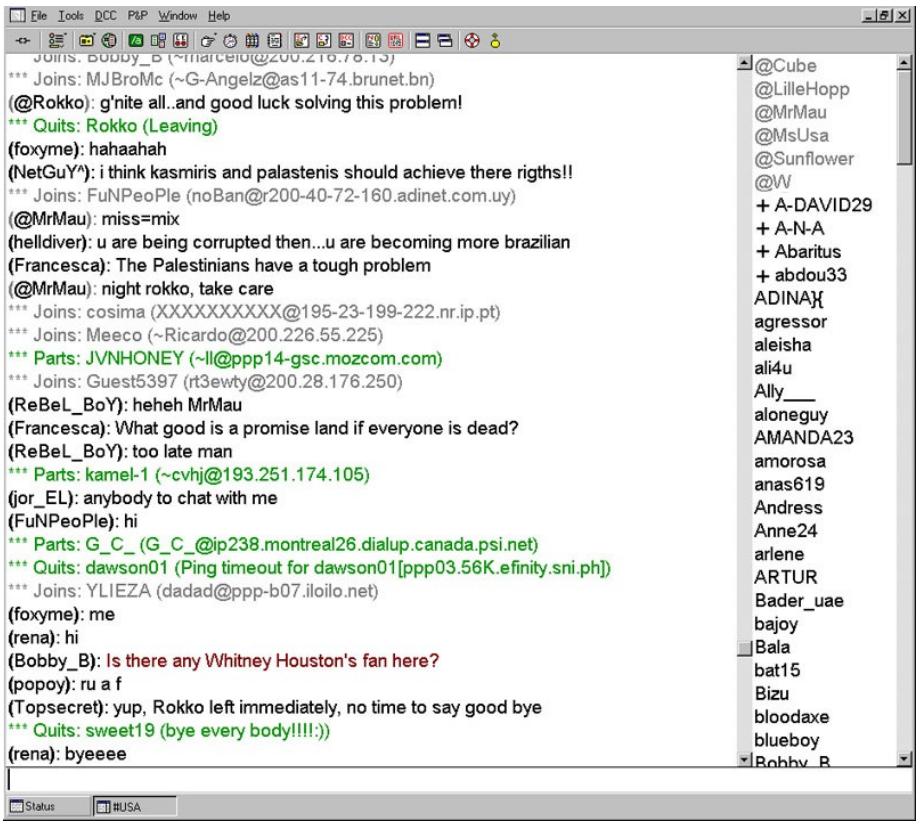


Abbildung 12 – typischer IRC-Client (*mIRC*)

---

[70] In seltenen Fällen kommt es vor, dass ein Fernsehsender einen Live-Chat im IRC einrichtet, um den Zuschauern gewisse Interaktionsmöglichkeiten zu bieten.

[71] So können sie beispielsweise unerwünschte Gäste aus dem Channel entfernen (Kick) oder gar für eine längere Zeit verbannen (Ban). Des Weiteren können sie die Überschrift („Topic") eines Channels ändern. Diese wird am oberen Rand des Hauptfensters angezeigt und enthält oftmals Neuigkeiten oder Hinweise für die regulären Teilnehmer des Chat. Neben weiteren administrativen Eingriffsmöglichkeiten, können Channel-Operatoren den Status der Teilnehmer ändern, also beliebigen anderen Nutzern ein „@" oder ein „+" verleihen bzw. entziehen,

[72] Die ursprüngliche Bedeutung des „+" (auch „Voice") ist eine andere: Wenn ein „Op" einen bestimmten Modus (moderated) für den gesamten Channel einstellt, können nur noch „Ops" und die Träger eines „+"-Zeichens lesbare Nachrichten in den Channel schreiben. Nicht „gevoicte" Teilnehmer werden zwangsläufig ignoriert. Dieser Modus wird jedoch kaum noch eingesetzt, so dass dem „+" mittlerweile die oben beschriebene Bedeutung zukommt.

Am unteren Ende des Hauptfensters befindet sich ein einzeiliges Eingabefeld, in welches man die eigenen Beiträge eingeben kann. Mit der Eingabetaste (Return) wird der Beitrag in den Channel abgeschickt und erscheint daraufhin ganz unten als aktuellster Eintrag. In das Eingabefeld lassen sich auch Befehle eingeben. Mit entsprechenden Befehlen, die immer mit dem Zeichen „/“ beginnen müssen, kann man unter anderem DCC-Bots fernsteuern oder ein Privatgespräch initiieren. Mit dem Befehl „*/join #flatrates*“ wird man unmittelbar den gewünschten Channel betreten.[73] Kombiniert man den Join-Befehl mit einem Channelnamen, den es bislang nicht gab, gründet man einen Channel dieses Namens. Die Gründung von Channels ist im IRC jedermann erlaubt.

Die Serverstruktur, durch die sich die User per Tastatur zeitgleich und nahezu grenzenlos unterhalten können, wird meist von Universitäten unterhalten. Es gibt jedoch nicht nur ein einzelnes großes Netzwerk für den IRC, sondern eine Vielzahl von unabhängigen Netzen. Efnet und Undernet sind hierunter die größten IRC-Networks.[74] Das größte europäische Netz ist mit über 120 Servern das IRCnet.[75]

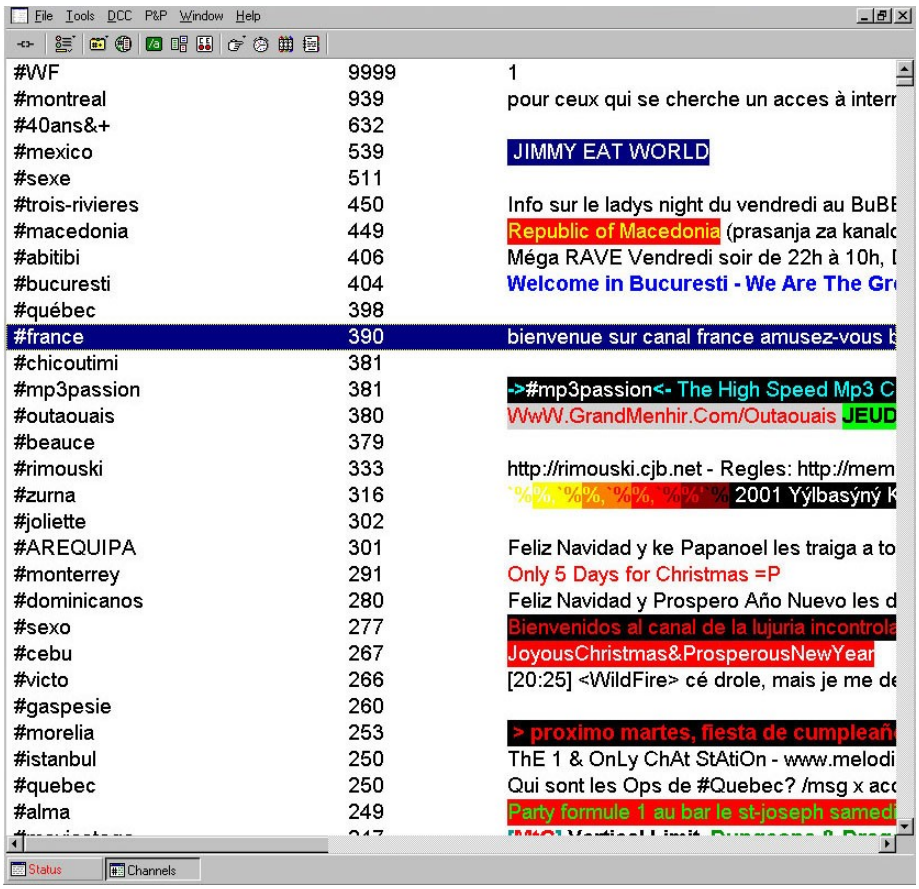


Abbildung 13 – Auflistung von Channels eines IRC-Servers

[73] Das Zeichen „#“ steht für Channel.
[74] *Decius/Panzieri*, S. 2.
[75] Brauch, Kaputt gespielt, **c't** 11/2000, S. 110.

Um an einem Chat teilzunehmen, muss sich der Nutzer als erstes für ein IRC-Netz (Efnet, Dalnet, Undernet, IRCnet etc.) entscheiden, in dem er sich aufhalten will. Hat er die Verbindung mit einem IRC-Server des entsprechenden Netzes hergestellt, kann er über den Befehl „*/list*“ eine Auflistung aller bestehenden Channels des IRC-Servers abrufen. In der Liste werden neben dem Namen des Channels die aktuelle Anzahl der Teilnehmer des Channels sowie das momentane „Topic“ aufgeführt.

VI. Instant Messaging (am Beispiel von *ICQ*[76])

ICQ (sprich „I Seek You") ist ein kleines Programm, das dem Nutzer anzeigen kann, welche seiner Freunde zur selben Zeit online sind wie er. Mit *ICQ* lässt sich eine Liste („Buddy-List“) erstellen, die alle Personen enthält, über deren Internet-Anwesenheit man informiert werden möchte. Sämtliche Personen müssen ebenfalls *ICQ* installiert haben. *ICQ* kann immer dann im Hintergrund laufen, wenn eine Internet-Verbindung besteht. In einem kleinen Programmfenster wird die Buddy-List angezeigt, die rote und blaue (Nick-) Namen enthalten kann. Ein blau dargestellter Name bedeutet, dass der betreffende „Buddy“ gerade online ist; ein roter Name signalisiert, dass der Nutzer entweder offline ist, seine Auflistung temporär nicht wünscht oder sein *ICQ*-Programm deaktiviert hat.

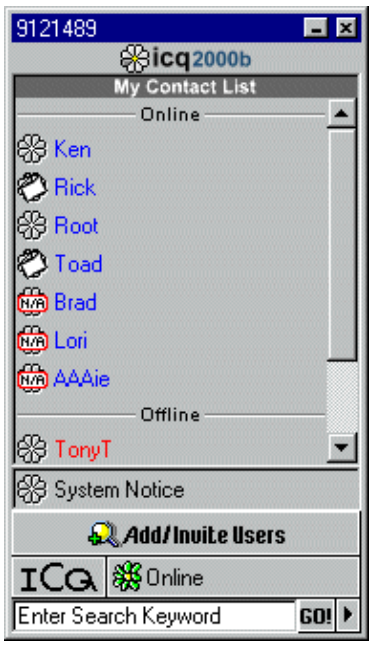


Abbildung 14 – ICQ-Client

Jeder neue *ICQ*-Nutzer bekommt bei der Anmeldung auf der *ICQ*-Homepage eine individuelle Nummer zugeteilt – die sogenannte Universal Identification Number (UIN). Anhand einer UIN kann man einen Nutzer in die eigene Buddy-List eintragen, so dass Personen, die dauerhaft in

---

[76] *ICQ* wurde ursprünglich vom israelischen Softwarehersteller *Mirabilis* entwickelt, der 1998 von *AOL* übernommen wurde. *ICQ Inc.* ist der einzige Anbieter von *ICQ;* mittlerweile gibt es allerdings neben *ICQ* weitere Instant-Messaging-Programme, die mehr oder weniger über eine ähnliche Funktionalität verfügen. Zu nennen ist vor allem der *MSN Messenger.*

Kontakt bleiben wollen, einfach ihre UINs austauschen können. Bei der Registrierung einer neuen UIN über den *ICQ*-Server sind Fake-Angaben möglich.

Außer der Information über den Online-Status von Freunden bietet *ICQ* zusätzliche Kommunikationsdienste: Zwischen zwei Nutzern können auch kurze Nachrichten (Messages) verschickt werden. Diese werden beim Eintreffen optisch und auf Wunsch auch akustisch angekündigt. Das „Messaging" funktioniert nicht nur, wenn Sender und Empfänger gleichzeitig online sind, sondern auch in Abwesenheit des Empfängers. Dieser bekommt die Nachricht dann zugestellt, sobald er wieder online ist. Des Weiteren gibt es den *ICQ*-Chat. Ähnlich dem IRC können hier *ICQ*-Nutzer miteinander einen Chatroom gründen und in Echtzeit kommunizieren. Über eine zusätzliche Funktion können Nutzer außerdem Adressen von Webseiten an andere *ICQ*-Teilnehmer versenden („URL Messaging"). Eine weitere wichtige Nutzungsmöglichkeit von *ICQ* ist der File Transfer, mit dem Dateien aller Art zwischen zwei Nutzern übertragen werden können.

E. Überblick über die verschiedenen Daten, die Gegenstand von strafbaren Handlungen i.S.d. §§ 106 ff. UrhG sind

I. Software

Mit der illegalen Verbreitung von Computerprogrammen über das Internet beschäftigt sich der zweite Teil dieser Arbeit ausführlich.

II. Musik in CD-Qualität

Raubkopierte Musikdateien machen neben raubkopierter Software den größten Teil der unerlaubten verwerteten Dateien aus, die im Internet erhältlich sind. Das recht junge Phänomen der Online-Musikpiraterie wird im dritten Teil der Arbeit dargestellt und analysiert.

III. Kinofilme / Videofilme

Durch Fortschritte auf dem Gebiet der Datenreduktion ist es mittlerweile möglich, ganze Spielfilme in digitalisierter Form auf die Größe einer herkömmlichen CD-ROM (650 bzw. 700 Megabyte) zu reduzieren[77]. Zwar handelt es sich bei 650 Megabyte noch immer um eine große Datenmenge, doch Besitzer von schnellen Standleitungen haben schon heute genügend Bandbreite, um sich eine solche Datei binnen kurzer Zeit herunterzuladen. Bevorzugter Vertriebsweg der Filmpiratengruppen sind private FTP-Server. Außerhalb der Piratengruppen finden Filmkopien hauptsächlich über P2P-Netzwerke Verbreitung.

Meistens werden analoge Videofilme digitalisiert oder DVD-Filme[78] in die entsprechenden Formate umgewandelt. Mittlerweile ist es unter Filmpiraten üblich, dass sie aktuelle Kinofilme mit digitalen Videokameras während einer Vorstellung heimlich von der Leinwand abfilmen. Bei diesen Kopien

---

[77] Bevorzugte Formate sind in diesem Zusammenhang AVI- (DivX- bzw. XviD-codiert) oder MPEG-Dateien.
[78] Bei der Digital Versatile Disc (DVD) handelt es sich um einen optischen Datenträger, der bei gleicher Größe einer CD-ROM bis zu 17,08 Gigabyte Daten speichern kann; der derzeitige Standard liegt bei 4,7 Gigabyte pro DVD.

(„Cam Releases“) sind oftmals die Köpfe der Zuschauer am unteren Bildrand sichtbar und Geräusche aus dem Publikum zu hören. Auf diese Weise gelangen Hollywood-Filme schon Wochen vor ihrem offiziellen Kinostart nach Deutschland. Eine solche über das Internet nach Europa transferierte Kopie des Films *„Star Wars – Episode One“* soll erstmalig der Grund dafür gewesen sein, dass die Besucherzahl in deutschen Lichtspielhäusern bei einer bedeutenden Hollywood-Produktion weit hinter den Erwartungen zurückblieb.

IV. (Licht-)Bilder

Beim größten Teil raubkopierter Bilder handelt es sich unstreitig um pornographische Darstellungen. Bilder einschlägiger Männermagazine werden entweder von den Homepages dieser Zeitschriften heruntergeladen oder selbst digitalisiert („eingescannt“), um sie dann auf unautorisierten Webseiten zu verbreiten. In der Regel werden die Bilder als komprimierte JPG-Dateien verbreitet, weshalb sie verhältnismäßig klein sind.

Neben Bildern aus dem pornographischen Bereich sind auch Cliparts und teure Werbefotografien Gegenstand von unerlaubten Verwertungshandlungen. Bei Cliparts handelt es sich um Grafiken und Symbole, die meist bei teurer Grafik-Software mitgeliefert werden. Werbefotografien werden häufig von Werbeagenturen benötigt, und für die Erlaubnis, eine einzige Aufnahme zu verwenden, müssen die Werbeagenturen nicht selten mehrere hundert Euro als Nutzungsentgelt an eine spezialisierte Bildagentur bezahlen.

Da Fotografien für den professionellen Einsatz eine hohe Auflösung haben müssen, sind sie mehrere Megabyte groß. Daher werden entsprechende Raubkopien häufig über private FTP-Server verbreitet.

V. Schriftwerke[79]

Auch Bücher („E-Books“) und andere Publikationen werden in Form von TXT-, HTML- oder PDF-Dateien ohne Erlaubnis der Urheber über das Internet verbreitet.[80] Ein Buch mit 200 Seiten ist als TXT-Datei nur wenige Kilobyte groß, so dass es problemlos auf Webseiten zum Download angeboten werden kann.

Eines der ersten Werke, das diesbezüglich für Schlagzeilen sorgte, war das Buch *„Riding The Bullet“* des US-Autors *Stephen King*. Obwohl es vom Herausgeber ausschließlich als kopiergeschützte PDF-Datei vertrieben wurde, stand bereits kurze Zeit nach dem Verkaufsstart eine ungeschützte Version des Werkes auf zahlreichen illegalen Webseiten zum Download bereit.[81] Ähnlich erging es dem vorletzten Werk des deutschen Autors *Martin Walser*. Dessen *„Tod eines Kritikers“* wurde von Raubkopierern bereits vor der offiziellen Veröffentlichung eingescannt und als PDF-Datei massenhaft online verbreitet.

---

[79] Streng genommen gehören auch Computerprogramme zu den Schriftwerken, siehe § 2 Abs. 1 Nr. 1 UrhG.
[80] Vgl. hierzu *Rink*, **c't**, 6/1999, S. 192 ff.
[81] Vgl. **ZDNet News** (Int.) vom 29.03.2000, http://zdnet.com.com/2100-11-519549.html?legacy=zdnn.

VI. Fonts

Bei Fonts handelt es sich um digitale Schriftartdateien. Vorwiegend Werbeagenturen kaufen sich die Rechte an Schriften, um diese bei ihrer täglichen Arbeit verwenden zu dürfen. Eine einzelne Schrift kann bis zu mehreren hundert Euro kosten. Einzelne Fonts – in der Regel TTF-Dateien – sind recht klein, so dass sie ebenfalls leicht über Webseiten verbreitet werden können.

VII. Ton- bzw. Klangdateien („Sounds" oder „Samples")

Raubkopierte Samples sind überwiegend digitalisierte Klänge oder Klangfolgen, die im Bereich der Musikproduktion eingesetzt werden.[82] Neben gängigen Formaten wie WAV und MP3 werden auch professionelle Formate wie das *AKAI*-Sampler-Format von den Sound-Piraten verbreitet. Auch Synthesizer-Klänge (sogenannte Presets) werden raubkopiert und über das Internet verbreitet. Da die Größe der einzelnen Formate stark variiert, kommen sowohl Homepages als auch FTP-Server und P2P-Netzwerke für die illegale Verbreitung in Betracht.

VIII. Kompositionen

Musikalische Kompositionen werden meist auf Homepages in Form von Midifiles oder Notationen angeboten. Midifiles sind kleine MID-Dateien, die digitale Informationen über die Notation von Musikstücken enthalten, und die man mit einer Standard-Soundkarte hörbar machen kann. Hierbei steuert das Midifile einen auf der Soundkarte befindlichen Klangerzeuger.

IX. Sonstige Daten mit Werkcharakter

Hierunter fallen Darstellungen wissenschaftlicher oder technischer Art wie Forschungsergebnisse oder technisches Know-how in Form von Zeichnungen, Plänen, Skizzen, Tabellen oder plastischen Darstellungen. Diese Daten sind hinsichtlich der massenhaften Verbreitung über das Internet kaum von Bedeutung und spielen eher im Zusammenhang mit Industriespionage eine Rolle.

---

[82] Zu den Grundlagen der Sampling-Technik siehe *Münker*, S. 6 ff.; zur urheberrechtlichen Schutzfähigkeit von Sounds bzw. Samples siehe (bei ebendiesem) S. 45 ff.

F. Methodik

Die vorliegende Arbeit enthält umfangreiche Beschreibungen der in geheimen Gruppen agierenden Raubkopiererszene[83]. Diese beruhen größtenteils auf Nachforschungen des Verfassers und sind daher nicht durchgehend mit Quellennachweisen auf andere Autoren versehen. Im Folgenden wird zusammenfassend dargelegt, welche empirisch-kriminologischen Forschungsmethoden angewendet wurden, um die entsprechenden Informationen zu erhalten.

I. Dokumenten-Inhaltsanalyse

Die wichtigste Grundlage für den kriminologischen Erkenntnisgewinn bezüglich der Tätigkeit von Raubkopierer-Gruppen bildete die inhaltliche Auswertung sogenannter NFO-Dateien[84].

Da eine Totalerhebung nicht möglich ist - eine Erfassung aller aktiven Gruppen scheitert vor allem an der starken Dynamik[85] und Internationalität[86] der Szene sowie daran, dass diese überwiegend im Verborgenen operieren - erfolgte eine Teilerhebung, basierend auf einer Wahrscheinlichkeitsauswahl (probability sampling).

Um einen möglichst hohen Grad der Randomisierung zu erzielen, wurden über einen mehrjährigen Zeitraum – von September 1998 bis Mai 2003 - aus drei unterschiedlichen Quellen so viele NFO-Dateien wie möglich zusammengetragen.

Als besonders geeignet zum Bezug von NFO-Dateien haben sich sogenannte Release-Info-Seiten[87] erwiesen. Weitere Quellen waren P2P-Netzwerke[88] und FTP-Server.

Insgesamt wurden 1.472 NFO-Dateien ausgewertet, die von 254 Warez-Gruppen und 48 MP3-Gruppen in Umlauf gebracht wurden.

---

83 Siehe unten Teil 2, A. ff. und Teil 3, A. ff.

84 Hierbei handelt es sich um Raubkopien beiliegende Textdateien, siehe unten Teil 2, A. IV. 5. Ausgewertet wurde stets der komplette Inhalt der NFO-Dateien, d.h. – sofern vorhanden – die obligatorischen Angaben zu Beginn des Textes („Release Name, Publisher, Cracker, Supplier, Packer, Ripper, Tester, Protection, Disks, Release Date / Store (Street) Date, Platform (OS), Type, Rating, Language, Size / Disks, Format, File Naming“ etc.), die näheren Angaben zur Veröffentlichung („Release Information“), Installationshinweise („Installation Notes“), Hinweise der Gruppen zur eigenen Geschichte / zu aktuellen Begebenheiten / zum (un)erwünschten Umgang mit dem Release („Group Info / News / Notes“), die Auflistungen von FTP-Servern im Zugriff der Gruppen („Site(s) / Distribution Info“), Angaben zu Mitgliederakquise und Kontaktmöglichkeiten („Requests, Contact Information“) und Grüße („Group Greets“).

85 Während einige Gruppen über einen Zeitraum von mehreren Jahren unzählige Raubkopien veröffentlichen und so zu einer "festen Größe" innerhalb der Szene werden, tun sich zahlreiche Gruppen nur für ein einziges Release oder nur für wenige Wochen zusammen. Das Phänomen dieser kaum wahrzunehmenden "Eintagsfliegen" macht es unmöglich, eine Grundgesamtheit zu erfassen.

86 Innerhalb der vorliegenden Arbeit konnten nur Informationsquellen in englischer, deutscher, spanischer und französischer Sprache berücksichtigt werden. Zwar wird in der Szene vornehmlich Englisch gesprochen, es ist jedoch davon auszugehen, dass vor allem im asiatischen Bereich Raubkopierergruppen aktiv sind, die ausschließlich in ihrer Landessprache kommunizieren. Dieser Umstand bedingt, dass die in der Arbeit getroffenen Aussagen erstrangig für den angloamerikanischen Raum und für Westeuropa Gültigkeit besitzen.

87 Auf diesen Webseiten wird tagesaktuell gelistet, welche Raubkopie von welcher Raubkopierergruppe veröffentlicht wurde; siehe unten Teil 2, A. V. 4. Als Quellen für den Bereich der Softwarepiraterie dienten vor allem die Seiten *ISOnews, dupecheck* und *NFOrce*; für den Bereich der Musikpiraterie die Seiten *mp3hq, dupecheck* und *NG-Index*.

88 *Gnutella*, *Fasttrack*, *eDonkey2000* und *Overnet*.

Ebenfalls zum Erkenntnisgewinn beigetragen hat die Inhaltsanalyse von Beiträgen in diversen Szene-Foren[89]. Obgleich die den Foren zu entnehmenden Informationen überwiegend subjektiven Charakter haben, lassen sich dort regelmäßig wertvolle Hinweise auf objektivere und zitierfähige Quellen finden. Denn häufig tauschen die Szenemitglieder – beispielsweise nach Razzien oder Hausdurchsuchungen - in den Foren Online-Verweise zu Zeitungs-, Verbands- oder Regierungsberichten aus, die sich mit der Bekämpfung der Raubkopiererszene befassen.

Schließlich konnten 82 E-Mail-Spam-Nachrichten, in denen nichtlizenzierte Computerprogramme zum Kauf angeboten wurden, ausgewertet werden. Diese sind zwischen April 2002 und Mai 2003 unverlangt an die E-Mail-Accounts des Verfassers bei der *Universität Gießen, GMX* und *T-Online* gesendet worden.

II. Distanzierte, verdeckte Beobachtung

Durchgeführt wurden auch distanzierte, verdeckte Beobachtungen. Zum einen erstreckten sich diese auf den Bereich der Echtzeitkommunikation – hier vor allem auf das Mitlesen der Beiträge und die Analyse des Nutzerverhaltens in IRC-Channels[90]. Zum anderen erfolgten Analysen des Nutzerverhaltens auf öffentlichen und privaten FTP-Servern[91].

III. Befragungen

Vornehmlich um gewonnene Erkenntnisse zu validieren, wurden kombinierte Befragungen durchgeführt. Sowohl Informanten- als auch Täterbefragungen fanden statt. Zu den befragten Informanten (= Nichttäter) zählten Informatiker, Richter, Staatsanwälte, Rechtsanwälte, Polizisten, Mitarbeiter der Jugendgerichtshilfe, Mitarbeiter von Access-Providern und Verbandsvertreter. Die Informationen wurden im Rahmen zwangloser informeller Gespräche gewonnen. Die gleiche Art der Befragung wurde bei Szeneangehörigen angewendet; hier fanden die Gespräche jedoch nicht von Angesicht zu Angesicht statt, sondern anonym per Internet Relay Chat[92].

---

89 Zu erwähnen ist vor allem das Forum von *ISOnews*.

90 Ausgewählt wurden Chaträume in den IRC-Netzwerken Efnet, Undernet und Dalnet anhand ihrer Channelnamen; bevorzugt aufgesucht wurden Channels, die die Begriffe „Warez“, „Crack“, „FTP“ und „mp3“ enthielten.

91 Untersucht wurden vor allem die Pub- und Incoming-Verzeichnisse der FTP-Server der Universitäten in Gießen, Rostock und Weimar, die vor allem an Wochenenden von Raubkopierern zur temporären Ablage von Releases genutzt wurden. Zugangsdaten privater FTP-Server ließen sich häufig den Channel-Topics einschlägiger IRC-Channels entnehmen.

92 Während es bis Ende 2000 relativ leicht möglich war, in einschlägigen Chaträumen sogar mit Gruppenmitgliedern in Kontakt zu treten, hat zunehmender Verfolgungsdruck in der Folgezeit bewirkt, dass sich die Täter komplett in private Netzwerke zurückgezogen haben.

Teil 2 – Internet-Softwarepiraterie

A. Beschreibung und Struktur der sogenannten Warez-Szene

I. Welche Software wird über das Internet verbreitet?

In den Mustervorschriften der *WIPO*[93] für den Schutz von Computersoftware wird ein Computerprogramm als „eine Folge von Befehlen" definiert, „die nach Aufnahme in einen maschinenlesbaren Träger fähig sind zu bewirken, dass eine Maschine mit informationsverarbeitenden Fähigkeiten eine bestimmte Funktion oder Aufgabe oder ein bestimmtes Ergebnis anzeigt, ausführt oder erzielt".[94]

Neben Computerspielen fällt hierunter auch Anwendungssoftware (Applikationen) aller Art. Grundsätzlich ist raubkopierte Software für sämtliche PC-Betriebssysteme im Umlauf. Aber auch Konsolenspiele – hauptsächlich für die *SONY Playstation* und die *Microsoft Xbox* – sind auf zahlreichen FTP-Servern als Raubkopien zu finden. Eine weitere Art der illegal verbreiteten Software ist Emulator-Software. Hierbei handelt es sich um Programme, die Spielecomputer und Konsolen (z.B. *Nintendo N64* oder *SNES*) auf einem PC dergestalt simulieren, dass man die spezielle Hardware dieser Geräte nicht benötigt. Passend zu diesen Emulatoren sind über das Netz auch raubkopierte Konsolenspiele („Roms") zu beziehen.

Exkurs – Software und Lizenzmodelle:

Man unterscheidet grundsätzlich die folgenden Arten der (legalen) Distribution von Software und der damit verbundenen Lizenzierung.[95]

Kostenpflichtige Software

Mit dem Erwerb des Programms (überwiegend auf CD-ROM) erwirbt der Käufer das Recht, die Software auf eine bestimmte Art und Weise zu nutzen. In den meisten Fällen[96] sind die Lizenzvereinbarungen so ausgestaltet, dass man nur eine Sicherheitskopie anfertigen und die Software lediglich auf einem Rechner installieren darf[97]. Jede weitere Kopie oder Installation – auf einem weiteren eigenen Rechner und erst recht die Weitergabe an Dritte – ist nicht mehr durch die Lizenz gedeckt und somit rechtswidrig. In der Regel ist kein Umtausch möglich, weshalb der Trend zu sogenannten Trial-Versionen geht. Diese auch als „Demo-" oder „Test-Version" bezeichneten Programme laufen meist nur für 30 oder 90 Tage ab dem Zeitpunkt ihrer Erstinstallation. Neben dieser zeitlichen Nutzungsbeschränkung können Hersteller auch funktionale Nutzungsbeschränkungen an den Trial-

---

93 *Weltorganisation für den Schutz geistigen Eigentums / World Intellectual Property Organization*, http://www.wipo.org.
94 § 1 Abs. 1 der *WIPO*-Mustervorschriften für den Schutz von Computersoftware, abgedruckt in **GRUR** 1979, S. 306 f. (auch in **GRUR Int.** 1978, 290 ff.).
95 Vgl. *Blümel/Soldo*, S. 124 f.
96 So z.B. in den Endbenutzer-Lizenzverträgen der folgenden (Standard-)Programme: *Microsoft Windows XP Professional* (Lizenzvertrag, Punkt 1, Abschnitt 5), *Microsoft Internet Explorer 6* (Lizenzvertrag, Punkt 1, Abschnitt 5), *Microsoft Office 2002* - bestehend aus *Outlook 2002, Powerpoint 2002, Word 2002* und *Access 2002* (Lizenzvertrag, Punkt 5), *Symantec Norton Utilities 2002* (Lizenzvertrag, Punkt 1 B.), *Adobe PhotoShop 7* (Lizenzvertrag, Punkt 2.3), *Adobe Acrobat Reader 5* (Lizenzvertrag, Punkt 2.3), *Realnetworks RealOne Player 2* (Lizenzvertrag, Punkt 1 a) (III)).
97 Vgl. das Urteil des *LG Bochum* vom 12.03.1998 (Az. 8 O 3/98), abgedruckt in **CR** 1998, S. 381 zu Spielesoftware: Es ist unzulässig, ohne ausdrückliche Genehmigung des Rechtsinhabers Sicherungskopien von urheberrechtlich geschützten Computerspielen anzufertigen. Grundsätzlich ergeben sich die zustimmungsbedürftigen Handlungen aus § 69c UrhG, die Ausnahmen finden sich in den §§ 69d und 69e UrhG - siehe hierzu ausführlicher Teil 2, C. I. 1.

Versionen vornehmen. In diesem Fall sind einzelne Programmroutinen deaktiviert, so dass beispielsweise mit dem Programm gearbeitet werden kann, die Arbeitsergebnisse jedoch nicht abgespeichert werden können.

Gefällt dem Kunden das Programm während der Evaluierungsphase, kann er es später durch den Erwerb einer Voll-Lizenz unbeschränkt nutzen. Im Zuge des Kaufes wird er vom Softwarehersteller einen Code erhalten, mit dem er die bislang deaktivierten Programmbestandteile der Trial-Version freischalten kann, so dass er eine uneingeschränkte Vollversion erhält. Der überwiegende Teil der legal über das Internet vertriebenen Programme wird auf diese Art und Weise angeboten (Download einer Trial-Version > Installation > Evaluierungsphase > Kauf oder Deinstallation).

Shareware

Unter den Begriff der Shareware fallen Programme, die der Autor zum Ausprobieren und Kopieren freigibt. Die Programme dürfen und sollen an Freunde und Bekannte weitergegeben werden, können jedoch nicht ohne Zustimmung des Autors auf einer Shareware CD-ROM oder anderweitig veröffentlicht werden.

Shareware ist urheberrechtlich geschützt, alle Rechte liegen beim Autor der Software. In der Regel wird der Nutzer berechtigt, diese Software eine bestimmte Zeit lang kostenfrei auszuprobieren. Will er sie länger nutzen, muss er den Autor kontaktieren und eine bestimmte Lizenzgebühr (Registrierungsgebühr) bezahlen.[98]

Freeware[99]

Programme, die der Autor unter bestimmten Auflagen zur kostenfreien Benutzung und Weitergabe freigegeben hat, werden als Freeware bezeichnet. Häufige Auflagen sind, dass der Nutzer Student oder Mitarbeiter an einer Hochschule ist, oder dass das Programm nicht kommerziell genutzt wird. Liegen die vom Inhaber des Urheberrechts bestimmten Voraussetzungen der kostenfreien Nutzung nicht vor, muss der Anwender eine Lizenzgebühr entrichten. Eine Unterart der Freeware ist die sogenannte Donationware oder Donateware. Hier ist mit dem Bereitstellen der Software die Bitte des Programmierers verbunden, ihm bei Gefallen des Programms eine freiwillige Spende zukommen zu lassen.

Zur Freeware zählt außerdem die sogenannte Adware. Diese Programme sind ebenfalls kostenlos erhältlich, allerdings bessern die Programmierer ihr Gehalt auf, indem sie Werbeanzeigen in ihren Programmen platzieren. Besonders häufig ist Adware bei Programmen anzutreffen, die online genutzt werden. Dann liegt über der Anzeige in der Regel ein Hyperlink, der beim Anklicken der Anzeige zur Webseite des Sponsors führt.

---

[98] *Blümel/Soldo*, S. 125.

[99] Ausführungen zur Free- und Open-(Source-)Software finden sich unten in Teil 2, C. V. 3. (Exkurs). Das Besondere an dieser Art der Software ist, dass ihr Quellcode öffentlich zugänglich ist.

Public Domain Software[100]

Obwohl Public Domain Software den Ruf genießt, ohne Einschränkung für jedermann frei nutzbar zu sein, kann sie dennoch urheberrechtlichen Schutz genießen[101].

Die Besonderheit bei Public Domain Software besteht darin, dass der Rechtsinhaber die allgemeine Benutzung gestattet hat. Diese Gestattung ist urheberrechtlich als Einräumung eines einfachen Nutzungsrechts i.S.d. § 31 Abs. 2 UrhG am Vervielfältigungs- und Verbreitungsrecht zu qualifizieren. Die Nutzungseinräumung kann vertraglich mit Einschränkungen verbunden sein; so wird dem Nutzer häufig die Bearbeitung der Public Domain Software untersagt.[102]

Abschließend ist anzumerken, dass viele der legal über das Internet vertriebenen Programme eine Mischform der oben genannten Vertriebsformen und Lizenzrechte darstellen.

II. Historische Betrachtung

Seit es kommerzielle Software gibt, gibt es auch Raubkopien. Schon mit den ersten Homecomputern (*Commodore VC 20, C64* und *AMIGA*-Serie) entwickelte sich eine beachtliche Raubkopiererszene: Hunderttausende von Kindern und Jugendlichen tauschten Computerspiele auf Schulhöfen und im Bekanntenkreis. Bei sogenannten Kopierparties trafen sich oftmals mehrere hundert Computerfreaks aus aller Welt mitsamt ihren Rechnern, um raubkopierte Programme auf Disketten auszutauschen.[103]

Das Duplizieren der Disketten erforderte damals keine geistigen Höchstleistungen: Jedermann konnte ohne überdurchschnittliches Wissen oder besondere Gerätschaften Kopien der Original-Disketten anfertigen, auf denen das Programm vom Hersteller ausgeliefert wurde. Als Reaktion hierauf entwickelten die Softwarehersteller die ersten Kopierschutzmechanismen:

Um ein Programm zu nutzen, musste man fortan Informationen eingeben, zu denen nur der ehrliche Käufer Zugang hatte. Besonders beliebt bei *C64*-Programmen war der sogenannte Doc-Check, ein Kopierschutzverfahren, bei dem der Nutzer während der Programminstallation aufgefordert wurde, sich den Freischaltungs-Code aus dem Handbuch zusammenzusuchen („ ...bitte geben sie nun den 23. Buchstaben auf Seite 12 des Handbuchs ein."). Die Raubkopierer reagierten prompt und verteilten von nun an die Programme mitsamt Fotokopien der Handbücher, was bei den Empfängern der Raubkopien umso beliebter war, da sie nunmehr noch eine Bedienungsanleitung zu ihrer Software erhielten. In der Folgezeit wurden die Kopierschutzmechanismen komplexer. Neben der Einführung spezieller Überlänge-Disketten, die eine größere Anzahl beschriebener Sektoren enthielten als handelsübliche Disketten[104], wurde auch der Doc-Check weiterentwickelt: Die Nutzer mussten ihre Codes von Blättern ablesen, die so gedruckt waren, dass man mit den damals üblichen Fotokopierern keine lesbaren Kopien erstellen konnte (z.B. schwarze Schrift auf rotem Untergrund).

---

100 Die hier vorgenommene Einteilung besitzt keine Allgemeingültigkeit; so zählen manche Autoren die Public Domain Software zur Freeware, vgl. Schricker-*Loewenheim*, § 69c UrhG, Rdnr. 3; zur Terminologie siehe auch *Marly*, S. 125 ff. und *Redeker*, Rdnr. 59.

101 Zum urheberrechtlichen Schutz von Computerprogrammen siehe unten Teil 2, C. I. 1.

102 Schricker-*Loewenheim*, § 69c UrhG, Rdnr. 3.

103 *Schultz*, S. 123.

104 Z.B. beim *ATARI ST*.

Doch auch diese Maßnahmen sollten vergebens bleiben, denn vor allem der Protest der entnervten ehrlichen Nutzer führte dazu, dass einige Dritt-Unternehmen Programme entwickelten, mit denen man automatisch die Kopierschutzabfragen der beliebtesten Computerspiele überspringen konnte, sofern man den korrekten Code einmal eingegeben hatte.

Über Jahre hinweg – hauptsächlich in den 80er Jahren – wurde die Verbreitung von Raubkopien mittels Kleinanzeigen in Computerzeitschriften organisiert.[105] Experten schätzten die Zahl der verdächtigen Anzeigen in EDV-spezifischen Zeitschriften zu Hochzeiten auf ca. 400[106]. Ein massives Vorgehen gegen verdächtig erscheinende Anzeigen, das hinsichtlich der Methode seiner Durchführung allerdings nicht unumstritten war[107], brachte einen überraschend starken Erfolg: Die Zahl der verdächtig erscheinenden Kleinanzeigen ging extrem zurück, und der Vertrieb über Zeitungsannoncen hat heute fast keine Bedeutung mehr. Die meisten Computerzeitschriften unterziehen sich mittlerweile einer Art freiwilliger Selbstkontrolle und veröffentlichen keine Annoncen mehr, wenn nicht seitens des Anbieters schriftlich versichert wird, dass die aufgeführten Programme mit gültiger Lizenz veräußert werden.[108]

Aufgrund des gewachsenen Verfolgungsdrucks wurden die Geschäfte unter der Hand weitergeführt. Anfang der 90er Jahre war eine Verlagerung zu neuen Vertriebsformen wie dem sogenannten Ameisenhandel zu beobachten.[109] Als Ameisenhandel wird der bandenmäßig betriebene und organisierte Verkauf von raubkopierten Disketten auf Flohmärkten bezeichnet.[110]

Mit der Einführung der CD-ROM Anfang der 90er Jahre konnte dem Raubkopieren für eine gewisse Zeit ein Riegel vorgeschoben werden. Die Programme – vor allem Spiele – waren mittlerweile so groß, dass Kopien auf Disketten äußerst unpraktisch wurden, und CD-Rekorder (sogenannte CD-Brenner) waren für private Nutzer nahezu unerschwinglich.

Das Blatt wendete sich erneut mit der zunehmenden Ausbreitung von Mailbox-Systemen (Bulletin Board Systems – BBS) und später mit der Ausbreitung von CD-Brennern im Consumer-Bereich. Die ersten Mailboxnetze (z.B. das FidoNet) entstanden mit der Einführung des Modems in die PC-Sparte. In Grundzügen sind Mailboxen mit den FTP-Servern des Internet zu vergleichen, allerdings muss man Mailboxen direkt per Telefonnummer anwählen, und die Bedienung der Systeme ist wesentlich unkomfortabler. In Mailboxen wurden weltweit raubkopierte Computerprogramme zum Download angeboten, jedoch war es nicht für jedermann möglich, sich in diese einzuwählen. Viele Nutzer beklagten sich über die hohen Verbindungsgebühren für weit entfernte Mailboxen und langsame Modems, mit denen sie Bit für Bit Daten auf die eigenen Rechner kopierten. Nicht selten mussten sie zusätzlich stündliche Gebühren an die Mailboxbetreiber entrichten oder als Gegenleistung andere raubkopierte Programme im BBS hinterlassen. In der Zeit vor der massenhaften Nutzung des Internet spielten Mailboxen bei der Verbreitung von Raubkopien eine wichtige Rolle[111]. In Deutschland soll es einschlägige Boards gegeben haben, die mit über 15 Telefonanschlüssen gleichzeitig online waren.[112] Parallel zu den Bulletin Boards etablierte sich eine

---

105 *Vassilaki*, Multimediale Kriminalität, **CR** 1997, S. 289
106 *Gravenreuth*, Neue Formen der Softwarepiraterie, **CR** 1995, S. 309.
107 Siehe dazu unten Teil 2, C. III. 1. c) (4).
108 *Schultz*, S. 117.
109 *Gravenreuth*, Neue Formen der Softwarepiraterie, **CR** 1995, S. 309.
110 *Sieber*, Missbrauch der Informationstechnik, Teil 1, I. B. 5. a).
111 *Gravenreuth*, Neue Formen der Softwarepiraterie, **CR** 1995, S. 310.
112 *Sieber*, Missbrauch der Informationstechnik, Teil 1, I. B. 5. a).

professionelle Raubkopier- und Produktfälscherszene, die bis heute schwunghaften Handel mit selbstgebrannten CD-ROMs treibt, die den Originalen oft täuschend ähnlich sehen. Regelmäßig werden Händler von Computerhardware dabei ertappt, wie sie raubkopierte Software als kostenlose Zugabe zu Hardwarekomponenten vertreiben.[113]

Seit dem großen Internet-Boom von 1996 ist der internationale „Raubkopie-Markt" förmlich explodiert, denn ein Großteil der Aktivitäten von Softwarepiraten wurde ins Netz verlagert[114]. Die Raubkopiererszene im Internet besteht im Kern aus zahlreichen kleineren Zusammenschlüssen von Softwarepiraten, sogenannten Warez-Groups[115], deren Tätigkeit und innere Organisation im Folgenden näher beschrieben werden.

III. Tätigkeit von Warez-Gruppen

Hauptziel der Gruppen ist es, in sogenannten Releases lauffähige Software kostenlos über das Internet zu verbreiten, die normalerweise kostenpflichtig zu erwerben wäre.[116] Folglich werden Public Domain Software und Freeware nicht von Warez-Gruppen veröffentlicht.

Innerhalb der Warez-Szene haben sich einige Gruppen auf das Veröffentlichen spezieller Software spezialisiert. Typische Ausrichtungen sind vor allem Spiele („Gamez"), Grafiksoftware („Graphic-Appz") und Audiobearbeitungssoftware („Audioappz"). Auch Teile von Gruppen („Sublabels" oder „Divisions") können die verschiedenen Bereiche abdecken.

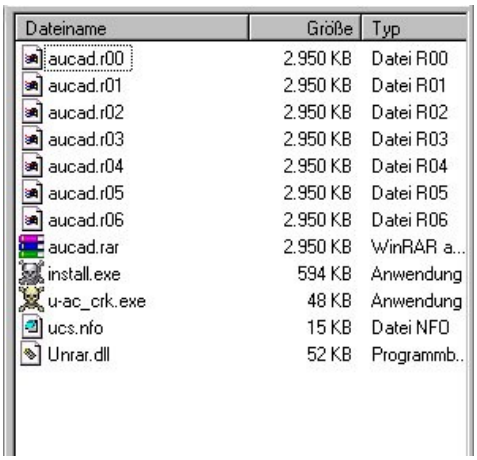


Abbildung 15 – entpacktes Warez-Release

Ein typisches Warez-Release enthält neben den Dateien, aus denen das raubkopierte Programm besteht, mehrere Textdateien, die Informationen über das Release oder die veröffentlichende Gruppe

---

113 Vgl. *Sieber*, Missbrauch der Informationstechnik, Teil 1, I. B. 5. a).
114 *Kürten*, **PC-Intern** 8/1999, S. 33.
115 Warez ist eine Kurzform von (Soft-)Ware(s) – zur Schreibweise siehe unten Teil 2, A. VIII. 1.
116 Zur vielschichtigen Motivation der Softwarepiraten siehe unten Teil 2, A. VIII. 3. – vorab sei angemerkt, dass der Großteil der Warez-Gruppen keine finanziellen Interessen verfolgt.

enthalten. All diese Dateien sind in der Regel zu einer einzelnen gepackten ZIP- oder RAR-Datei[117] zusammengefasst. Nur wenn es sich um große Programme handelt (vor allem bei Spielen), bestehen Releases aus mehreren durchnummerierten Paketen.

IV. Die Mitglieder der Gruppen / Arbeitsteilung innerhalb der Gruppen

1. Supplier

Der Supplier hat die Aufgabe, die Originalversion eines Programms zu beschaffen. Besonders begehrt in der Warez-Szene sind Programme, die noch nicht auf dem (legalen) Markt erhältlich sind. Sogenannte Zero-Day-Releases tragen dazu bei, den Ruf einer Gruppe zu erhöhen.[118] Der Ego-Shooter[119] *Unreal* war eines der zahlreichen Spiele, die schon lange im Internet zu finden waren, bevor sie in den Handel kamen.[120] Auch Kopien von *D**m II*[121] wurden bereits Wochen vor der Markteinführung im Internet gesichtet. Gerüchten zufolge handelte es sich um eine Testkopie für eine britische Spielezeitschrift, die den Ursprung für die Raubkopien darstellte[122]. Erst kürzlich war der Presse zu entnehmen, dass auch das aktuelle Betriebssystem *Windows XP* von *Microsoft* bereits mehrere Wochen vor dem offiziellen Verkaufsstart sowohl online als auch im asiatischen Straßenhandel erhältlich war[123].

Oft werden auch schon Vorabversionen von Programmen (Alpha- oder Beta-Versionen) veröffentlicht, die nur an Angestellte der jeweiligen Softwarehersteller oder ausgesuchte Programmtester verteilt wurden. Da die Vorab-Tester nicht zwangsläufig bei den Softwareherstellern beschäftigt sind, kommt es häufig vor, dass Alpha- oder Betaversionen in die Hände von Warez-Gruppen fallen. Vorabversionen von Software ermöglichen schon lange vor der Markteinführung einen Einblick in die Entwicklungsarbeit der Softwarehersteller, weshalb Tester als Gruppenmitglieder äußerst willkommen sind.[124] Allerdings sind Vorabversionen regelmäßig mit zahlreichen Programmfehlern („Bugs“) behaftet, so dass einige „qualitätsorientierte“ Warez-Gruppen überhaupt keine Alpha- oder Beta-Versionen veröffentlichen. Es soll bereits vorgekommen sein, dass Gruppen via Telefonnetz in die Computernetze der Softwarehäuser eingebrochen sind, um die gut gehüteten Software-Entwicklungen zu stehlen und sie dann vor der Auslieferung an die Kunden als Raubkopien zu veröffentlichen.[125]

Der typische Supplier arbeitet selbst im Computerbereich (Softwarehersteller, Softwarehandel etc.) und nimmt von dort Software mit nach Hause. Auch Arbeiter in CD-Presswerken und Lagerarbeiter

---

117 ZIP-Dateien werden mit dem Programm *WinZip* erstellt, und ermöglichen eine Reduzierung der ursprünglichen Dateigröße. Daher wird in diesem Zusammenhang auch vom „Packen“ gesprochen. RAR-Dateien entstehen beim Packen einer Datei mit der Software *WinRAR*., deren Funktionsweise mit der von *WinZip* vergleichbar ist.
118 Zero-Day bedeutet, dass die veröffentlichte Software keinen Tag alt bzw. auf dem Markt ist.
119 Als Ego-Shooter (auch „First-Person-Shooter“) werden Spiele bezeichnet, die aus der Ich-Perspektive wahrgenommen werden, und deren Ziel das Töten von virtuellen Gegnern ist.
120 *Kürten*, **PC-Intern** 8/1999, S. 33.
121 Dieses Computerspiel ist indiziert, weshalb das Abdrucken seines vollständigen Namens in Deutschland untersagt ist.
122 *McCandless*, **Wired Magazine** 5.04 – April 1997.
123 Vgl. **Heise Online News** vom 25.09.2001, http://www.heise.de/newsticker/meldung/21317.
124 *McCandless*, **Wired Magazine** 5.04 – April 1997.
125 Vgl. *Zimmermann*, S. 28.

in Softwareunternehmen kommen als Supplier in Betracht. Via Internet oder per Post[126] übermittelt der Supplier die „heiße Ware“ an den Cracker.

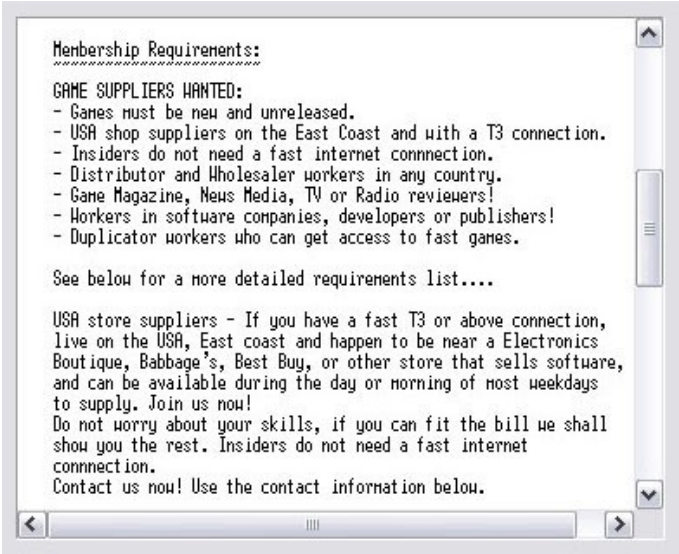


Abbildung 16 – Auszug aus einer Text-Datei einer Warez-Gruppe (NFO-Datei)

2. Cracker

In der Regel sind kommerzielle Programme kopiergeschützt. Es gibt eine Vielzahl von Maßnahmen, die die Programmierer in ihre Software einbauen, um sie vor unbefugter Weitergabe und Nutzung zu schützen. Aufgabe des Crackers ist es, diese Maßnahmen zu finden und sie unschädlich zu machen.

Das Rückgängigmachen von Kopierschutzmaßnahmen wird in der Szene auch als Reverse Engineering bezeichnet.[127] Da es nicht viele Personen gibt, die dieses beherrschen, sind Cracker nicht selten für verschiedene Gruppen tätig. Diese werden dann als "Affils"[128] des jeweiligen Crackers bezeichnet. Der Begriff des Crackers wird häufig mit dem des Hackers verwechselt oder gar synonym gebraucht. Ein Hacker hat jedoch nichts mit der Entfernung von Kopierschutzmaßnahmen bei Software zu tun.

Exkurs – Der Begriff des Hackers:

Nach einer traditionellen Definition versteht man unter Hacking das Eindringen in fremde Computersysteme, das nicht mit dem Ziel der Manipulation, Sabotage oder Spionage erfolgt, sondern aus Freude an der Überwindung von technischen Sicherheitsmaßnahmen. Immer kommt es jedoch zu einer Beeinträchtigung der formalen Geheimsphäre oder Integrität des betroffenen Computer-

---

126 Der Versandweg ist vor allem bei Programmen mit mechanischem Kopierschutz (Dongle) unumgänglich – siehe unten Teil 2, A. IV. 2. b) (6).
127 Siehe hierzu auch Schricker-*Loewenheim*, § 69e, Rdnrn. 5 und 6, der unter den Begriff des Reverse Engineering vor allem die Rückübersetzung von Objekt- in Quellcode (Dekompilierung) und das Anwenden von Techniken der Programmanalyse fasst.
128 Von affiliate (engl.) = als Mitglied aufnehmen, angliedern.

systems.[129] Im heutigen Sprachgebrauch erstreckt sich der Begriff des Hackens auch auf Computerspionage, Sabotage und die Fälschung von Hypertexten. Demnach gibt es nicht mehr nur den guten Hacker, der auf Sicherheitsrisiken in Computersystemen aufmerksam machen will[130], sondern ebenso den Hacker, der ausspionieren, sabotieren und zerstören will. Letzterer wird in der Szene auch als Crasher bezeichnet.[131] Crasher haben zuletzt durch die Distributed-Denial-of-Service-Attacken auf mehrere große Web-Portale auf sich aufmerksam gemacht.

In letzter Zeit mehren sich Berichte, in denen Täter, die auf fremde Webserver eindringen und Hypertexte fälschen bzw. verändern, als Cracker bezeichnet werden. Für die Journalisten, die sich für diesen Sprachgebrauch entschieden haben, sind Cracker so etwas wie „böse" Hacker. Während sie in Hackern Computerfreaks sehen, die aus sportlichem Ehrgeiz in fremde Computersysteme eindringen und dort keine Schäden anrichten, sind Cracker für sie Personen, die auf den fremden Systemen Sabotageakte verüben.

Wird in der vorliegenden Arbeit der Begriff des Crackers gebraucht, handelt es sich jedoch nicht um jemanden, der – aus welchem Grund auch immer – in fremde Computersysteme eindringen möchte, sondern um eine Person, die einen Software-Kopierschutz entfernt.

a) Haupttätigkeit des Crackers

Um Kopierschutzmaßnahmen zu entfernen, benötigt der Cracker eine hohe technische Kompetenz. Insbesondere muss er die Programmiersprachen Assembler (ASM) und *C++* sowie den Umgang mit Disassembler- und Debugging-Software beherrschen, um an den regelmäßig verschlüsselten Programmcode[132] zu gelangen, diesen zu analysieren und gegebenenfalls zu verändern. Mit dem Disassembler[133] wird der für Menschen kaum verständliche Objektcode des zu crackenden Programms in lesbaren Quellcode (auch: Sourcecode) umgewandelt. Diesen kann der Cracker mit dem Disassembler in kleinsten Schritten nach Algorithmen oder sonstigen Einträgen durchforsten, die Teil des Kopierschutzes sind. Da der Disassembler den Code lediglich darstellt, muss der Cracker zusätzlich einen Hex-Editor[134] benutzen, um Veränderungen am Code vorzunehmen.

Bei komplexeren Kopierschutzverfahren bedienen sich die Cracker in der Regel eines Debuggers[135]. Dieser überwacht den Programmcode und stellt ihn dar, während das zu crackende Programm ausgeführt wird. Ein Debugger hilft somit, die Vorgänge beim Programmablauf genauer zu verstehen; für Veränderungen am Programmcode muss der Cracker wiederum einen Hex-Editor betreiben.

---

[129] *Sieber*, Missbrauch der Informationstechnik, Teil 1, I. B. 3.
[130] Zu den Hackergruppen, die ihre Fähigkeiten in den Dienst einer guten Sache stellen, gehört der *Chaos Computer Club* (*CCC* – http://www.ccc.de). Auf seinen Veranstaltungen werden regelmäßig Vorträge gehalten, in denen die Schwächen der Computer- und Kommunikationstechnik praktisch vorgeführt werden – vgl. *Fremerey*, Gefahren und Chancen, **c't** 2/1999, S. 28.
[131] So schon bei *Gravenreuth*, Computerviren, Hacker, Datenspione, Crasher und Cracker, **NStZ** 1989, S. 205.
[132] Dieser wird auch als Objektcode oder Maschinencode („Maschinensprache") bezeichnet; je nach Verwendung unterscheidet man weiter zwischen z.B. Byte-Code oder Binärcode.
[133] Häufig genutzte Disassembler sind *W32dasm* und *IDA*.
[134] Z.B. *Hacker's View, Hexworks32 und Ultrahex*.
[135] Z.B. *Soft-Ice* und *UltraDebug*. Der eigentliche Sinn von Debugger-Software besteht darin, Programmfehler ausfindig zu machen; Bug (engl.) = Fehler.

Auch Kenntnisse in anderen Programmiersprachen sind unentbehrlich für einen ambitionierten Cracker. Dies gilt vor allem dann, wenn er die Entfernung der Kopierschutzmechanismen automatisieren will, indem er kleine Crack-Programme schreibt.[136]

b) Verschiedene Arten des Kopierschutzes und ihre Umgehung

(1) Seriennummern

Bei der Installation vieler Programme wird eine individuelle Seriennummer abgefragt. In ein Eingabefenster, das meist zu Beginn der Installation erscheint, muss der Käufer eine Seriennummer eingeben, die in der Regel auf der Hülle der Original-CD abgedruckt ist. Erst wenn das Programm eine richtige Seriennummer erkannt hat, wird mit der Installation fortgefahren.

Um eine funktionierende Seriennummer herauszufinden, sieht der Cracker zunächst nach, ob Seriennummern im Programmcode abgelegt sind, mit denen der Computer die vom Nutzer eingegebene Nummer vergleicht. Findet er diese Stelle im Code, muss er lediglich die Nummern auslesen und aufschreiben. Der Programmcode bleibt in diesem Fall unverändert, und die Gruppe kann das Programm zusammen mit einer Textdatei veröffentlichen, in der eine oder mehrere funktionierende Seriennummern erwähnt sind.

Liegen die Nummern nicht im Programmcode offen, muss der Cracker den Algorithmus ausfindig machen, anhand dessen die eingegebene Seriennummer validiert wird, um dann daraus gültige Seriennummern zu generieren. Eine weitere Möglichkeit besteht darin, die Installationsroutine des Programms durch Umprogrammierung so zu verändern, dass die Abfrage der Seriennummer vollständig unterbleibt. Diese Vorgehensweise ist deutlich aufwändiger und erfordert ein größeres Know-how des Crackers.

Warez-Gruppen veröffentlichen selten nur die Seriennummer eines Programms. Hierfür gibt es eine Vielzahl von Webseiten. Auf den sogenannten Serialz-Pages können riesige Listen mit funktionierenden Seriennummern abgerufen werden. Zuweilen gibt es auf solchen Seiten sogar eigene Suchmaschinen, mit denen sich Seriennummern für aktuelle Produkte leicht finden lassen. Die Seriennummern für diese Webseiten stammen allerdings nicht zwangsläufig von Crackern, die diese mit einem Disassembler ausgelesen haben. Zu einem großen Teil wird es sich um Nummern handeln, die von Personen in Umlauf gebracht werden, die im Softwarebereich tätig sind und sie von Originalverpackungen abgelesen haben.

(2) Registrierungscodes („RegCodes“ oder „Keys“)

Der Registrierungscode ist der typische Kopierschutz für Shareware. Shareware ist in der Regel voll funktionsfähig, muss jedoch beim Hersteller registriert werden, wenn man mit ihr länger als für eine gewisse Evaluierungsphase weiterarbeiten will. Zur Erinnerung daran, dass das Programm registriert werden soll, öffnen sich beim Starten, Beenden oder bei der Nutzung dieser Software in regelmäßigen Abständen kleine Fenster (sogenannte Nagscreens[137] oder Reminder) mit Hinweisen zur Registrierung. Möchte der Nutzer das Programm registrieren, wird er per Kreditkarte einen

---

[136] Siehe unten Teil 2, A. IV. 2. c) (3).
[137] Von nag (engl.) = nerven.

verhältnismäßig geringen Geldbetrag an den Hersteller zahlen und im Gegenzug einen Registrierungscode erhalten. Nach der Eingabe dieses Codes werden die Nagscreens nicht mehr erscheinen. In den meisten Fällen handelt es sich um einen Code, der aus einem Namen und einem Passwort besteht, wobei das Passwort in einem mathematischen Zusammenhang zu dem Namen steht. Häufig wird es anhand eines geheimen Algorithmus aus dem Namen generiert. Um die Reminder zu beseitigen, gibt es verschiedene Ansätze:

Zunächst besteht die Möglichkeit, Registrierungscodes von registrierten Nutzern zu erfahren und diese zu veröffentlichen. Der Endnutzer kann in diesem Fall die Shareware-Version, die er auf der Webseite des Softwareherstellers heruntergeladen hat, manuell registrieren. Hierbei kommt es jedoch regelmäßig vor, dass ein Code ab einem gewissen Zeitpunkt nicht mehr von dem Programm akzeptiert wird, da er auf einer schwarzen Liste („Blacklist“) in dessen Programmcode steht. Denn sobald ein findiger Programmierer erfährt, dass ein Registrierungscode im Umlauf ist, mit dem man seine Programme illegal freischalten kann, integriert er eine Blacklist in die Versionen, die er zukünftig zum Download anbietet. Damit verschafft er sich jedoch nur einen kurzen Vorsprung vor den Warez-Gruppen.

Um Blacklisting von vornherein zu vermeiden, verfolgen Cracker andere Ansätze: Sind ihnen mehrere funktionierende Keys bekannt, können sie versuchen, den Algorithmus herauszufinden, der aus einem beliebigen Namen ein gültiges Passwort generiert. Gelingt ihnen diese schwierige Aufgabe, können sie einen funktionierenden Key generieren und das Programm mit diesem veröffentlichen. In der Regel gestalten die Cracker die veröffentlichten Keys so, dass sich ihr Pseudonym oder der Name ihrer Gruppe darin wiederfindet (z.B. CrAksTeR / 355314151235).

Weiterhin kann der Cracker auch einen sogenannten Keymaker oder Key Generator („KeyGen“) programmieren. Hierbei handelt es sich um ein kleines Programm, das aus einem beliebigen Namen den passenden Code generiert, der dann tatsächlich vom Programm wie ein legaler Key akzeptiert wird. Ein solcher Keymaker wird in einem Release mitveröffentlicht und bietet dem Endnutzer die Möglichkeit, sich mit seinem eigenen Namen zu registrieren. Cracker, die in der Lage sind, funktionierende Keymaker zu programmieren, genießen in der Szene große Anerkennung.

Ein weiterer Ansatz besteht darin, das Programm so zu verändern, dass keine Reminder mehr aufgerufen werden. Als Ergebnis wird die Gruppe das „bereinigte“ Programm veröffentlichen.

Anstatt das gesamte Programm zusammen mit einem Key oder einem Keymaker zu veröffentlichen, kann der Cracker auch ein kleines Programm schreiben, mit dem der Endnutzer das „jungfräuliche“ Programm selbst modifizieren kann, nachdem er es von der Homepage des Softwareherstellers heruntergeladen hat. Ein solches Programm nennt man Crack oder Patch. Die kleinen Programme (in der Regel eine EXE- oder COM-Datei) werden in das Programmverzeichnis des installierten Sharewareprogramms kopiert und dort durch einen Doppelklick gestartet. Auf diese Weise werden einzelne Programmbestandteile in der gewünschten Form verändert („gepatcht“ bzw. „gecrackt“).[138] Das Programmieren von Cracks ist weit verbreitet. Durch den Umstand, dass sie nur wenige Kilobyte groß sind, können sie schnell und unauffällig verteilt werden. Das passende Shareware-Programm kann sich der Endnutzer von den Webseiten der Programmierer herunterladen. Aus

---

[138] Cracks und Patches können immer dann zum Einsatz kommen, wenn der Programmcode verändert werden soll – nicht nur im Zusammenhang mit der Beseitigung von Nagscreens.

diesem Grund veröffentlichen manche Gruppen ausschließlich Cracks und Keymaker. In ihren Releases sind typischerweise die URLs der Webseiten angegeben, auf denen die zu crackenden oder zu registrierenden Shareware-Versionen zum Download bereit liegen.

(3) Trial-Versionen mit zeitlicher Nutzungsbeschränkung

Es gibt zwei Varianten der zeitlichen Nutzungsbeschränkung: Entweder versagt das Programm seinen Dienst nach Erreichen eines bestimmten Datums bzw. nach einer festgelegten Anzahl von Tagen, die seit der Installation vergangen sind, oder die Beschränkung ist an die Anzahl der Programmstarts („Aufrufe") gebunden.

Ist für diese Art der Software eine Registrierung vorgesehen, lässt sich der Ablauf des Zeitlimits durch die Eingabe eines Codes stoppen. Der Cracker hat hierbei die gleichen Umgehungsmöglichkeiten wie bei der registrierungspflichtigen Software, die durch Reminder geschützt ist. Hierbei entspräche das Entfernen der Nagscreen-Aufrufe dem Deaktivieren oder Irreführen der Zeit-Routine (des sogenannten Counters).

(4) Trial-Versionen mit Einschränkung der Funktionen

Um potentiellen Käufern einen Eindruck von einem Programm zu verschaffen, reicht es oftmals aus, eine Demo-Version bereitzustellen, die nur einen Teil der Funktionen der Vollversion enthält. Lässt sich die uneingeschränkte Funktionsfähigkeit durch die Eingabe eines Registrierungscodes herstellen, kann der Cracker wie bei den beiden zuvor beschriebenen Kopierschutzmaßnahmen vorgehen. Das Umprogrammieren läge hierbei im Aktivieren der abgeschalteten Programmmodule.

Eine besondere Einschränkung der Funktionsweise nahm der Audiosoftwarehersteller *Sonic Foundry* bei den Demo-Versionen seiner *XFX* Plug-Ins vor. Die Programme geben in gewissen Abständen laute Zufallstöne von sich und verhindern so den sinnvollen Einsatz in einer Audioproduktion. Um diesen Kopierschutz zu umgehen, müsste der Cracker den „Zufallston-Generator" im Programmcode ausfindig machen und deaktivieren.

Ohne Erfolg wird der Cracker allerdings bei sogenannter Crippleware[139] bleiben. Demo-Versionen gelten als „crippled", wenn bestimmte Module des Programms (z.B. das Modul für das Abspeichern) nicht nur deaktiviert, sondern vom Hersteller gänzlich aus dem Programmcode entfernt wurden. Die Bereitstellung von Crippleware zum freien Download gehört somit zu den Maßnahmen, die zumindest solche Gruppen treffen, die ausschließlich Cracks veröffentlichen.

(5) CD-Abfragen

Viele Programme – vor allem Spiele – laufen nur, wenn die mitgelieferte Original-CD im Laufwerk des Computers liegt. Dies gilt in der Regel nur für den ersten Programmstart, doch einige Programme verlangen bei jeder Nutzung oder in unregelmäßigen Abständen nach der Original-CD. Im Programmcode befinden sich sogenannte Sprungadressen, die bei verschiedenen Aktionen des

---

[139] Cripple (engl.) = Krüppel.

Anwenders aufgerufen werden können und die Überprüfung veranlassen, ob ein Zugriff auf die Original-CD möglich ist. Um diesen Kopierschutz zu umgehen, muss der Cracker sämtliche CD-Abfragen aus dem Programmcode entfernen.

Ist der Kopierschutz zu komplex, weil beispielsweise starke Verschlüsselung zum Einsatz kommt, verzichten viele Cracker auf seine Entfernung. Dies bedeutet jedoch nicht, dass das Programm nicht als Raubkopie veröffentlicht werden kann: Immer häufiger und mit steigenden Übertragungsgeschwindigkeiten werden komplette Inhalte von CDs zum Download bereitgestellt. Diese sogenannten Image- oder ISO-Files („ISOs“)[140], die meist im BIN-Format vorliegen, kann der Endnutzer mit einem CD-Rekorder brennen und erhält so eine 1:1-Kopie der Original-CD.[141] Um ein funktionierendes Image zu erstellen, muss die CD-ROM exakt ausgelesen werden. Dies wird zunehmend erschwert, indem die Hersteller immer häufiger physische Manipulationen wie Bohrungen oder andere Markierungen auf der Datenseite der CD-ROM vornehmen oder bewusst logische Fehler im Dateisystem implementieren[142]. Liest das Laufwerk eine derart manipulierte CD-ROM aus, schaltet sich seine eingebaute Fehlerkorrektur ein und sorgt dafür, dass eine fehlerbereinigte Image-Datei geschrieben wird. Erstellt man von diesem Image eine neue CD-ROM, sind die Manipulationen nicht mehr vorhanden. Der Kopierschutz bemerkt, dass es sich nicht um eine Original- CD handelt und verweigert den Start der Software. Daher muss der Cracker solche Soft- und Hardwarekomponenten zum Auslesen verwenden, die in der Lage sind, die Fehlerkorrekturdaten, die dem Laufwerk einen Fehler auf dem Medium vorgaukeln, 1:1 mitzukopieren.[143] Auch wenn ein Kopierschutzverfahren darauf beruht, dass digitale Signaturen in den sogenannten Subchannels einer CD-ROM abgelegt werden (so z.B. bei *SecuROM, ProtectCD, Laserlock* und *LibCrypt*), muss der Cracker die notwendigen Werkzeuge besitzen, um Subchannels vollständig auszulesen.

Die ISO-Szene ist im Vergleich zur sogenannten Rip-Szene[144] (noch) recht klein, da die zu übertragenden Datenmengen sehr groß sind; für ein Programm muss der Endnutzer rund 600 Megabyte herunterladen. Auch wird von vielen Nutzern der Zwang als lästig empfunden, ständig eine CD-ROM einlegen zu müssen, weshalb sie gecrackte Programme bevorzugen. Zudem hat nicht jeder Nutzer einen CD-Brenner zur Verfügung.

Die Anhänger der ISO-Szene profitieren von zahlreichen Webseiten, auf denen Hunderte eingescannter CD-Cover zum Download angeboten werden. Diese können sich die ISO-Piraten zu Hause ausdrucken und als Inletts für die selbstgebrannten CDs verwenden.

---

[140] Benannt sind ISO-Files nach dem internationalen Industriestandard ISO 9660. Das ISO 9660 File System ermöglicht es, dass ein- und dieselbe CD-ROM auf verschiedenen Computerplattformen gelesen werden kann.
[141] Notwendig sind ISO-Files z.B. bei Raubkopien der Spiele für die *SONY Playstation.*
[142] *Zota*, Klonverbot – Kopierschutz als Rettung vor Gelegenheitskopierern, **c't** 2/2002, S. 91.
[143] *Zota*, Klonverbot – Kopierschutz als Rettung vor Gelegenheitskopierern, **c't** 2/2002, S. 91.
[144] Unter einem „Rip“ versteht man eine Programmversion, die von ihrem ursprünglichen Datenträger losgelöst ist. „Rips“ sind in der Regel um ein Vielfaches kleiner als „ISOs“.

#	PICTURE	SITE DESCRIPTION	IN	OUT
1	Audio, Video +Spiele Cover	**Dark´s CoverPage** Over 30.000 High-Quality Cover online --- PC - Audio - PSX - PS2 - DC - VHS - DVD - VCD --- Searchengine --- Printing-Software --- Darktown Request Board --- Chat --- Link-List --- Take a look at the best german Coversite	1523	4302
2	GAMES	**Coverworld** Coverworld 25.000 Labels.Audio Covers, Dreamcast Covers, Psx Covers , PS2, Pc, Audio , CD and DVD Labels Searchergine!	1421	6165
3	cd.cover.++	**cd.cover.++** FREE and easy to use software that prints cd covers. claimed as the best. direct internet covers search / upload. scanner support. cd/dvd/neato and customizable formats. text overlay. skinable. for w9x/me/nt/2000. latest version : version 1.3 [10.10.2001]	880	2689
4	MORE	**Label Land** If you after labels then this is the place to come! Thousands of PC , PSX, PS2, DC, VCD + DVD labels. Plus more!	774	2561
5	The CoverSite For all your cover needs.	**The CoverSite** More then 30000 covers and labels for Audio, Dreamcast, DVD, PC, Playstation, Playstation 2, Video CD and VHS. Also with a fast searchengine to find the covers you need.	707	3348
6	Cover - World	**Cover - World** 30.000 Audiolabels, Playstation 2, PSX, DVD, VCD, Games, PC - Covers and Covers Search Engine from a data base up to 80.000 Labels	379	2043

Abbildung 17 – Linkliste zu „Cover-Sitez“

(6) Dongles („Hardware Locks“ oder „Keys“)

Teure Programme werden nicht selten mit einem mechanischen Kopierschutz (Dongle) versehen. Dongles werden zusammen mit der Original-CD ausgeliefert. Sie sind kaum größer als eine Streichholzschachtel und werden entweder auf den seriellen oder den parallelen Schnittstellenadapter des Computers gesteckt. Neuere Modelle können häufig an den USB-Port angeschlossen werden. Dongles enthalten elektronische Bauteile, die mit dem dazugehörigen Programm korrespondieren. Ein donglegeschütztes Programm wird nur laufen, wenn das Dongle auf dem entsprechenden Port an der Computerrückseite steckt. Somit verhindert es die zeitgleiche Nutzung einer einzelnen Programmlizenz auf mehreren Rechnern und die Erstellung von Raubkopien. Die meisten Dongles sind völlig transparent, sie machen also den Schnittstellenadapter, den sie belegen, nicht nutzlos. An der Dongle-Rückseite befindet sich dann eine Anschlussmöglichkeit, die das Durchschleifen von Daten erlaubt.

Ähnlich wie bei CD-Abfragen können Dongle-Abfragen bei zahlreichen Programmoperationen vorgenommen werden. So kann beispielsweise immer dann, wenn etwas Erarbeitetes abgespeichert werden soll, vorher überprüft werden, ob das Dongle tatsächlich vorhanden ist. Bekommt das Programm nicht die erwartete Rückmeldung vom Dongle, quittiert es seinen Dienst. Denkbar ist auch, dass ein Programm das Dongle etwa alle 150 Mausklicks abfragt oder jedes Mal, wenn gedruckt wird oder immer, wenn der Nutzer eine dunkle Farbe für seinen Desktop-Hintergrund auswählt. Ist die Antwort des Dongles falsch oder kommt nicht an, schließt sich das Programm automatisch.

Die gesamte Kommunikation zwischen Programmcode und Dongle ist mit aufwändigen Algorithmen verschlüsselt. Nichts außer einem Elektronenmikroskop kann den Algorithmus aus dem Speicher (ROM)[145] des Dongles extrahieren. Allerdings ist diese Vorgehensweise mit einem enormen

---

[145] Read Only Memory.

technischen Aufwand verbunden und funktioniert auch nur bei sogenannten ASIC[146]-Dongles. Hinzu kommt, dass in die meisten Dongles Sicherungssysteme integriert sind, die das Dongle zerstören, sobald man versucht, das Gehäuse mechanisch zu öffnen.

Es gibt weltweit nur wenige Cracker, die eine Dongle-Protection dergestalt entfernen können, dass das Programm ohne Dongle fehlerfrei arbeitet.[147] Dennoch gelingt es ihnen immer wieder. Ein Ansatz besteht darin, sämtliche Dongle-Abfragen im Programmcode aufzuspüren und zu entfernen. Die Verbindung zwischen Dongle und Programm soll aufgebrochen werden, damit das Programm auch ohne Dongle genutzt werden kann. Diese Vorgehensweise ist jedoch dann problematisch, wenn nicht nur das Vorhandensein des Dongles überprüft wird, sondern das Dongle auch Rechenoperationen übernimmt oder Informationen bereithält, die für den Betrieb des Programms essentiell sind. 1992 war eine Raubkopie von *Autodesks 3D Studio* im Umlauf, die zunächst vollkommen lauffähig erschien. Allerdings fiel jedes mit dem Programm erstellte 3D-Objekt nach einigen Stunden der Nutzung in seine Polygone zusammen. Klugerweise nutzte *Autodesk* das mit dem Originalprogramm ausgelieferte Dongle, um im Programm eine dynamische Vektortabelle zu erzeugen, ohne die kein Objekt mit mathematisch korrekter Geometrie berechnet werden konnte. Zahlreiche Newsgroups und das offizielle *Autodesk*-Forum wurden mit Fragen nach dem vermeintlichen Programmfehler in *3D Studio* überflutet.[148] Kurze Zeit später gelang es einer Warez-Gruppe, einen funktionierender Crack zu veröffentlichen, der allerdings auf einem anderen Ansatz als auf dem Entfernen der Dongle-Abfragen beruhte: Der Programmierung eines virtuellen Dongles. Das Schreiben eines virtuellen Dongles („Dongle-Emulator“ oder „Pseudo-Dongle“) gehört zu den größten Herausforderungen für einen Cracker. Hierbei handelt es sich um ein kleines Programm, das dem geschützten Programm vorgaukelt, ein reales Hardware-Dongle sei an die Schnittstelle angeschlossen. Ein virtuelles Dongle wird in den Hauptspeicher geladen und gibt die korrekten Antworten zu jeder Abfrage des Programms. Um die richtigen Antworten auf die entsprechenden Fragen zu finden, muss der Cracker die gesamte Kommunikation zwischen Dongle und Programm überwachen. Zu diesem Zweck gibt es spezielle Analyseprogramme, welche allerdings nur den verschlüsselten Code sichtbar machen. Gelingt es dem Cracker, diesen Code zu „knacken“, oder findet er durch Ausprobieren einige richtige Antworten heraus, erstellt er eine möglichst umfangreiche Frage-/Antwort-Tabelle, die er dann in den Programmcode des virtuellen Dongles implementiert.

Trotz ihrer guten Schutzwirkung ist der Trend zu Dongles rückläufig. Das liegt vor allem daran, dass donglegeschützte Software nicht über das Internet vertrieben werden kann. Maßnahmen, die den Online-Vertrieb erschweren, werden von Vertretern der „New Economy“ als kontraproduktiv eingestuft.[149]

---

146 Application Specific Integrated Circuit.
147 Vgl. *McCandless*, **Wired Magazine** 5.04 – April 1997 , der für 1997 von drei oder vier Crackern ausging, die hierzu in der Lage waren.
148 *McCandless*, **Wired Magazine** 5.04 – April 1997.
149 Vgl. das Interview mit *Lohmeier* (*Microsoft*) bei *Puscher*, **internet world** 1/1999, S. 36.

Abbildung 18 – Szene-Seite mit Informationen zu Dongles

Als Quasi-Dongle können auch einzelne Hardwarekomponenten fungieren: Für Aufregung sorgte die Entscheidung *Microsofts*, in Deutschland nur noch OEM-Versionen[150] von *Windows* auszuliefern, die ausschließlich auf einem bestimmten PC oder PC-Typ lauffähig sind.[151] Bei diesen Versionen wird bei der Neuinstallation zur Erkennung der zugehörigen Hardware der Zeichensatz des jeweiligen Herstellers im BIOS[152] abgefragt. Fällt die Abfrage negativ aus, bricht die Installation unmittelbar ab. Da neben den OEM-Versionen auch weiterhin Versionen von *Windows* vertrieben werden, die nicht an bestimmte Hardwarekomponenten gekoppelt sind, wird deutlich, dass diese Maßnahme nicht gegen Internet-Softwarepiraterie gerichtet ist. *Microsoft* will wohl eher verhindern, dass die dem PC beigelegten, preisreduzierten *Windows*-Versionen von Computerhändlern getrennt weiterverkauft oder auf anderen Rechnern installiert werden.

(7) Online-Registrierung und Online-Updates

Zum Installieren oder Aktualisieren („Updaten“) mancher Programme muss eine Internetverbindung zu einem Server des Herstellers bestehen. Dieser überwacht den kompletten Vorgang, indem er unter anderem eingegebene Passworte oder Registrierungscodes mit einer Datenbank abgleicht und

---

150 Original Equipment Manufacturer. Diese Programmversionen dürfen nur in Verbindung mit einem PC verkauft werden, auf dem sie vorinstalliert sind.
151 **c't** 25/1999, S. 47.
152 Basic Input Output System. Das BIOS befindet sich in einem Chip auf der Hauptplatine (Motherboard) des PCs und bildet die grundlegende Schnittstelle zur Hardware des Rechners. Es enthält wichtige – meist änderbare – Grundeinstellungen für die Hardwarekonfiguration, die für das Betriebssystem und alle darauf aufsetzenden Applikationen bindend sind.

bei fehlender Übereinstimmung den Installationsvorgang abbricht. Beim Online-Update liegen die Dateien, aus denen das Update besteht, auf dem Server bereit, mit dem der Nutzer verbunden ist.

Online-Registrierung und Online-Updates sind derzeit nicht allzu weit verbreitet, da nicht jeder Nutzer über einen Internet-Zugang verfügt. In Zukunft ist jedoch damit zu rechnen, dass sich dieser Kopierschutz stärker etablieren wird. Um das Erfordernis einer Online-Registrierung zu umgehen, muss ein Cracker den Programmcode so verändern, dass sich das Programm auch ohne Verbindung zum Internet installieren lässt. Möchte eine Warez-Gruppe die Dateien eines Online-Updates veröffentlichen, wird sie in der Regel einen registrierten Nutzer „vorschicken". Bei diesem müssen die heruntergeladenen, neuen Daten von den alten separiert werden, um ein eigenständiges Update zu erstellen. Hierfür gibt es spezielle Programme (TCP/IP-Viewer), die den gesamten Datenverkehr zwischen einem Server und einem Client protokollieren.

(8) Mischformen (z.B. „Online-Dongles")

Weiterhin existieren auch Kombinationen der gängigen Kopierschutzmaßnahmen. Zu erwähnen sind in diesem Zusammenhang vor allem „Online-Dongles". Bei diesen übernimmt ein Internet-Server die Aufgabe eines Hardware-Dongles. Demnach kann das Programm nicht ohne Verbindung zum Internet gestartet und betrieben werden.

Eines der ersten Programme, die erfolgreich mit einem Online-Server-Check versehen wurden, war der Ego-Shooter *Qu**e 3*[153] von *ID-Software* (*Q3*). Da das Spiel in erster Linie online gespielt wird, lag es nahe, jene Server, die die Spieler zueinander führen, auch für die Abfrage einer gültigen Seriennummer (CD-Key) zu nutzen.

Neben den von *ID-Software* betriebenen Master- und Authentication-Servern gibt es zahlreiche private *Q3*-Server, auf denen das eigentliche Spiel stattfindet. Master- und Authentication-Server listen dem Spieler auf Wunsch sämtliche verfügbaren *Q3*-Server auf und übernehmen somit neben der CD-Key-Abfrage eine wichtige Vermittlungsfunktion. Der CD-Key, der sich auf der Hülle der Original-CD befindet, muss bereits bei der ersten Installation eingegeben werden und wird bei jedem neuen Spiel vom Authentication-Server überprüft, wobei die Abfrage vom *Q3*-Server initiiert wird. Während der Spielzeit wird der Key untrennbar mit der IP-Adresse des Spielers verknüpft und auf dem Server vermerkt. Erst fünf Minuten nach dem Verlassen des Spiels hört der Server auf, die Kombination aus Seriennummer und IP-Adresse zu überprüfen. Diese Vorgehensweise verhindert, dass sich mehrere Nutzer gleichzeitig mit der selben Seriennummer auf dem Masterserver anmelden können.

Beim Online-Server-Check gleicht der Authentication-Server den vom Käufer eingegebenen CD-Key mit einer Datenbank ab, in der die Keys aller ausgelieferten Spiele gespeichert sind. Bei Eingabe eines unbekannten CD-Keys bekommt der Nutzer eine Fehlermeldung und kann nicht online spielen.

Um diesen ausgefeilten Kopierschutz zu umgehen, haben die Cracker zwei völlig verschiedene Ansätze verfolgt: Zunächst fanden sie heraus, wie eine gültige Seriennummer beschaffen sein musste, damit sie bei der Eingabe nicht vom Programm zurückgewiesen wurde, und sie programmierten die

---

[153] Dieses Computerspiel ist indiziert, weshalb das Abdrucken seines vollständigen Namens in Deutschland untersagt ist.

ersten Keymaker für *Q3*. Wollte der Nutzer einer Raubkopie mit einem generierten Key online spielen, blieb er fast immer erfolglos, da der generierte Key in den meisten Fällen nicht in der Datenbank des Masterservers vermerkt war. Denn die Beschaffenheit des Keys – eine 16-stellige Kombination aus Buchstaben und Zahlen – lässt eine weitaus größere Zahl gültiger Keys zu als jemals Kopien von *Q3* verkauft werden könnten. Gelingt dem Nutzer der Raubkopie bei der Benutzung des Keymakers ein höchst unwahrscheinlicher Zufallstreffer, und er generiert eine bestehende und somit in der Datenbank vermerkte Seriennummer, ist noch immer nicht sichergestellt, dass er tatsächlich damit spielen kann. Solange der redliche Besitzer mit dem gleichlautenden Original-Key online ist, wird der Raubkopierer die Fehlermeldung „Someone is using this CD key" erhalten. Umgekehrt gilt dasselbe, denn sobald sich der unredliche Nutzer eingeloggt hat, wird der redliche Besitzer vor verschlossenen Türen stehen. In der möglichen Benachteiligung des redlichen Käufers liegt leider der grundlegende Nachteil dieses äußerst wirksamen Kopierschutzes. Da mit der zuvor beschriebenen Methode das Online-Spielen nur selten möglich ist, ließen sich die Cracker etwas anderes einfallen: Sie entwickelten einen Crack, der den Online-Server-Check gänzlich aus dem Servermodul des Programms entfernt. Ein gecrackter *Q3*-Server lässt nunmehr auch Spieler ohne gültigen CD-Key zu, weil eine Überprüfung beim Authentication-Server nicht mehr initiiert wird. Zusätzlich entwickelten die Cracker kleine Programme („Cracked Servers Detector" und „Cracked Servers Scanner"), mit denen sich der Nutzer der Raubkopie eine Reihe gecrackter Server auflisten lassen konnte.

Das Beispiel zeigt deutlich, dass der Einfallsreichtum der Softwarehersteller oftmals vom Einfallsreichtum der Cracker übertroffen wird. Doch im Fall von *Q3* gab das aufwändige Kopierschutzverfahren dem Hersteller einen entscheidenden zeitlichen Vorsprung, der ihm zahlreiche Verkäufe der Original-CD sichern konnte.

(9) Hardwaregestützte Software

Wird Software speziell für die Arbeit mit bestimmten Hardwarekomponenten geschrieben, liegt ein besonders effektiver Kopierschutz vor. Denn ohne die entsprechende Hardware ist die Software wertlos, da man sie nicht mit anderer oder vergleichbarer Hardware betreiben kann. Das Programm *Sound Designer* von *Digidesign* benötigt beispielsweise eine *Audiomedia*-Soundkarte, um zu laufen. Ein Cracker müsste einen universellen Soundkartentreiber programmieren, damit das Programm von jedermann nutzbar würde. Hier stünde der Aufwand in keinem Verhältnis zum Ergebnis, so dass derartige Programme fast nie von Crackern modifiziert werden.

Allerdings kommt es vor, dass hardwaregestützte Software unmodifiziert von Warez-Gruppen veröffentlicht wird. In diesem Fall ziehen nur solche Nutzer einen Vorteil daraus, die im Besitz der entsprechenden Hardware sind und sich die Software quasi als Zubehör kaufen müssten.

c) Weitere Tätigkeiten des Crackers

(1) Debugging

In seltenen Fällen kommt es vor, dass Cracker Programmfehler (Bugs) entdecken, die schon in der Originalversion vorhanden waren. Sind diese Fehler zu beheben, werden sie vom Cracker bereinigt, er nimmt sogenannte Bugfixes vor.

Das Debugging durch den Cracker hat paradoxerweise zur Folge, dass der Besitzer der Raubkopie im Endeffekt ein besseres Programm in den Händen hält als der Käufer des Originalprogramms.

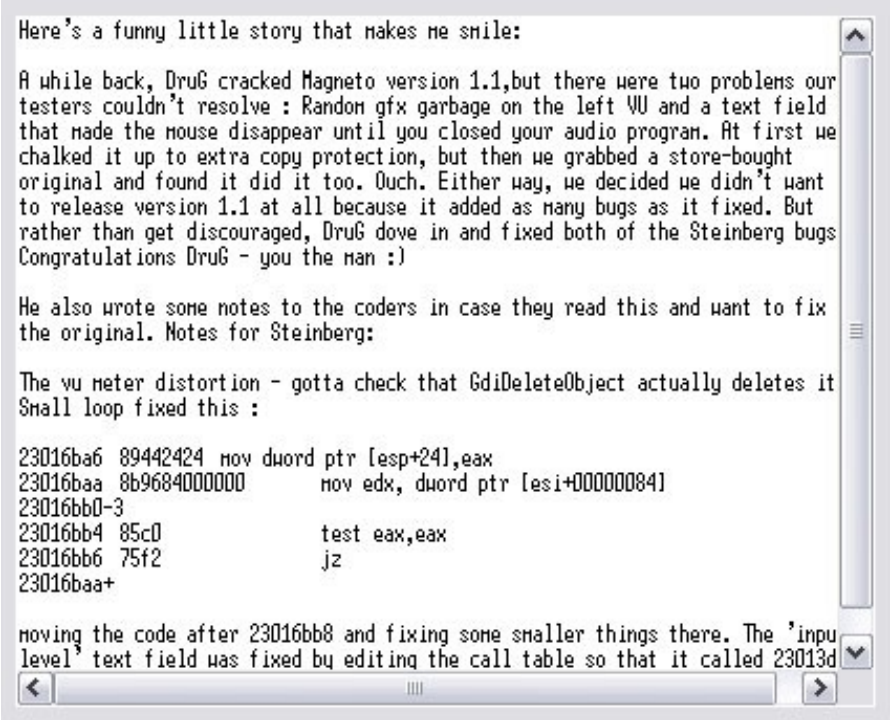


Abbildung 19 – Auszug aus einer NFO-Datei mit Hinweisen für den Softwarehersteller (*Steinberg AG, Hamburg*)

(2) Implementieren von neuen Programmoptionen (Features)

Das Ergänzen von Programmen um neue Möglichkeiten ist eher die Ausnahme. Doch immer, wenn ein Cracker solche Veränderungen vornimmt, sorgt es für Aufsehen in der Warez-Szene – und nicht nur dort: Vor einigen Jahren veränderte ein Cracker der Gruppe *Inner Circle* den Newsreader *Agent* des Herstellers *Forte* dergestalt, dass diejenigen, die eine Nachricht in einer Newsgroup veröffentlichten, einen wesentlich höheren Grad an Anonymität erzielten. Als Nebeneffekt verringerte sich der Spam[154] um ungefähr zwei Drittel. Die Verbesserung wurde so positiv aufgenommen, dass sogar solche Nutzer diese „Spezialversion" benutzten, die üblicherweise nichts mit der Warez-Szene zu tun hatten. Als Reaktion hierauf implementierte *Forte* das neue Feature in die nachfolgenden Versionen.[155]

---

[154] Datenmüll in Form unnützer Nachrichten, die die Newsgroups verstopfen.
[155] *McCandless*, **Wired Magazine** 5.04 – April 1997.

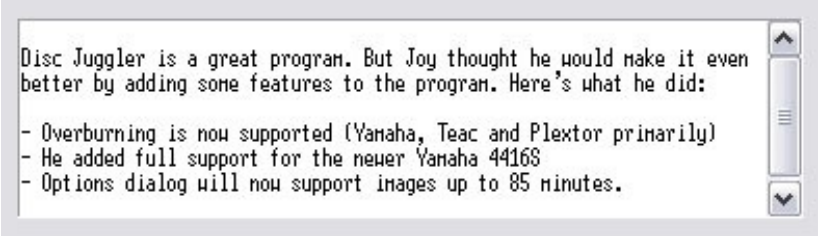


Abbildung 20 – Auszug aus einer NFO-Datei

Mit dem Beseitigen von Bugs und dem Implementieren neuer Features verschaffen sich Cracker ein sehr hohes Ansehen in der Szene, was wiederum den Gruppen zugute kommt, denen sie angehören.

(3) Schreiben von Cracking-Programmen, Tutorials und "Crackmes"

Cracker können auch kleine Hilfsprogramme (z.B. „Time-Limit Remover" oder „CD-Check Remover") schreiben, mit denen jedermann standardmäßige Kopierschutzmaßnahmen entfernen kann. Diese Programme sind auf einschlägigen Webseiten zu finden, funktionieren jedoch nur bei wenigen und relativ primitiven Schutzmechanismen. Ein erfahrener Cracker wird daher keines dieser Hilfsmittel einsetzen.

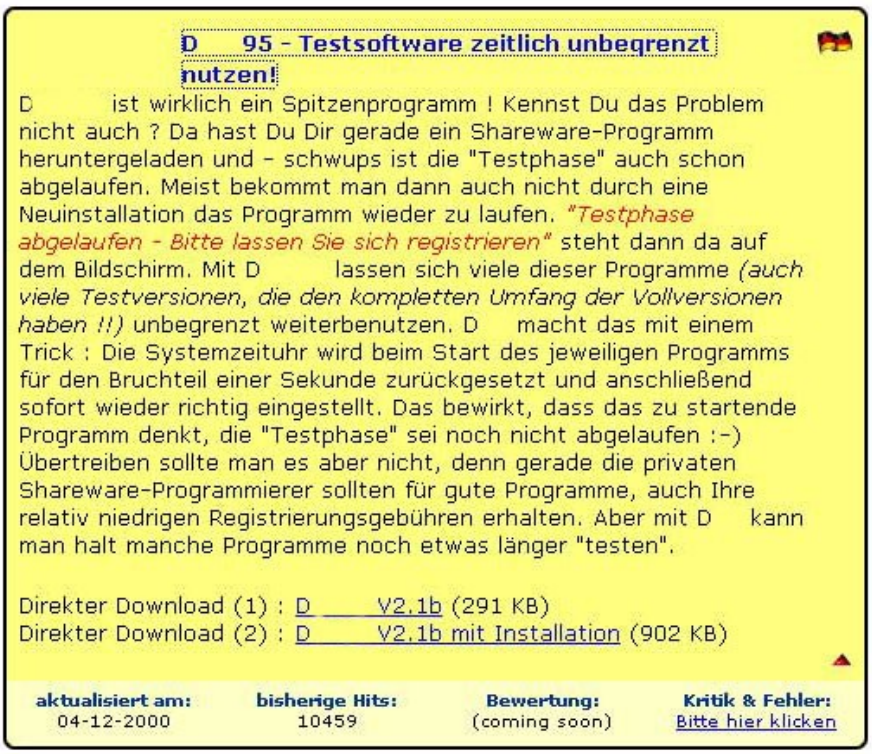


Abbildung 21 – Web-Angebot über einen „Time-Limit Remover"

Manchmal kommt es vor, dass Cracker Anleitungen zum Cracken schreiben („Cracking-Tutorials") und diese auf Underground-Webseiten veröffentlichen. Hier findet sich für beinahe jede Art des Kopierschutzes eine Anleitung zum Entfernen. Die Texte enthalten häufig weltanschauliche Überlegungen und philosophisch angehauchte Gedankenspiele, und nicht selten weisen die Autoren

zu Beginn darauf hin, dass sie sich jeglicher Haftung für den Missbrauch der nachfolgenden Informationen entziehen.

```
The Cracking Manual

Written By The Cyborg - April 3, 1992

DISCLAIMER
The author of this text shall hold no liability for special, incidental, or
consequential damages arising out of or resulting from the use/misuse of the
information in this file.

INTRODUCTION
Welcome to the wonderful world of cracking. What is cracking? If you don't know
and you're reading this, ask yourself why? Anyway, cracking is the art of removing
copy protected coding from programs. Why do this? In recent years, software
companies have been fighting to keep copy protection in their software to avoid
their work to be illegally copied. Users feel that such copy protection is
ridiculous in that it violate their own rights to make backups of their sometimes
expensive investments. Whichever side you may favour, this manual will go into
some detail on removing copy protection from programs. If you feel offended by
this, then I would suggest you stop here.
Please note, I do not endorse cracking for the illegal copying of software. Please
take into consideration the hard work and effort of many programmers to make the
software. Illegal copying would only increase prices on software for all people.
Use this manual with discretion as I place into your trust and judgement with the
following knowledge.
…
```

Abbildung 22 – Auszug aus einem Cracking Tutorial

```
HOW TO CRACK, by +ORC, A TUTORIAL

LESSON C (1) - How to crack, Cracking as an art

[BARCODES] [INSTANT ACCESS]
First of all, let me stress the importance of cracking in our everyday life.
Cracking it's not just about software, it's about information, about all patterns
of life. To crack is to refuse to be controlled and used by others, to crack is to
be free. But you must also be yourself free from petty conventions in order to
crack properly.
You must learn to discern cracking possibilities all around yourself, and believe
me, the development of this ghastly society brings every day new codes,
protections and concealing mechanisms.
All around us grows a world of codes and secret and not so secret patterns. Codes
that are at times so familiar and common that we do not even notice them any
more... and yet they are there to fool us, and yet they offer marvellous cracking
possibilities.
Let's take as an striking example BARCODES... those little lines that you see on
any book you buy, on any bottle you get, on any item around you... do you know how
they work? If you do not you may be excused, but you cannot be excused if you
never had the impulse to understand them... crackers are curious by nature...
heirs of an almost extinct race of researchers that has nothing in common with the
television slaves and the publicity and trend zombies around us. Cracker should
always be capable of going beyond the obvious, seek knowledge where others do not
see and do not venture.
```

Abbildung 23 – Auszug aus einem Cracking Tutorial

Als Aufnahmeprüfung für neue Cracker oder für szene-interne Cracking-Wettbewerbe werden von erfahrenen Crackern sogenannte Crackmes[156] veröffentlicht. Wie der Name vermuten lässt, handelt es sich hierbei um kleine Programme, die einen schwer zu crackenden Kopierschutz enthalten. Gelingt es einem Cracker, den Kopierschutz zu umgehen, indem er beispielsweise einen funktionierenden Keymaker schreibt, hat er sich für die Mitgliedschaft in der Gruppe qualifiziert, die das Crackme herausgegeben hat.

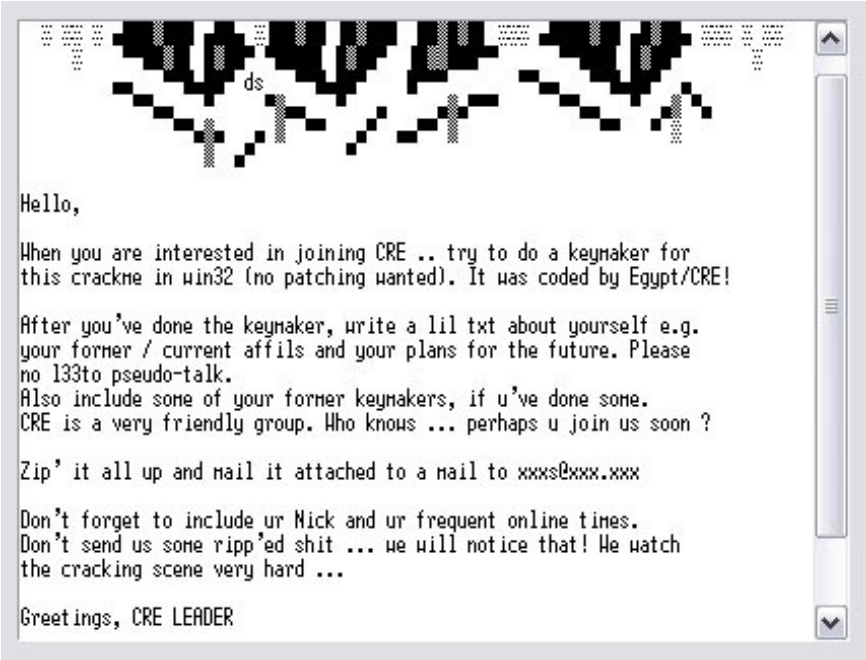


Abbildung 24 – Begleittext zu einem „Crackme“

3. (Beta-)Tester

Um zu gewährleisten, dass die gecrackten Programme auch auf unterschiedlich konfigurierten PC-Systemen laufen, werden Vorabversionen (Beta-Cracks) der Warez-Releases an verschiedene Gruppenmitglieder oder Freunde der Gruppe gegeben. Diese müssen die Programme auf ihren Rechnern installieren und ausgiebig testen. Fehler, die auf einen schlechten Crack hindeuten, müssen beim Cracker gemeldet werden, damit dementsprechend nachgebessert werden kann. Wird das Programm von den Testern als lauffähig befunden, kann es an den Packager weitergegeben werden.

4. Packager

Da ein Programm für eine schnelle Datenübertragung so klein wie möglich sein soll, aber uneingeschränkt lauffähig sein muss, werden überflüssige Programmbeigaben („Addons“) wie Videos oder Hilfedateien vom Packager (auch „Packer“ oder „Ripper“) entfernt[157]. Danach wird es meist in ein oder mehrere RAR-, ZIP- oder ACE-Dateien gepackt. Unter Umständen wird es vorher

---

[156] Von “crack me“ (engl.).
[157] Vgl. *Ye*, **Wired Magazine** 4.07 – Juli 1996.

noch mit anderen Komprimierungsverfahren behandelt, um durch doppeltes Packen möglichst kleine Dateien zu erhalten. Die einzelnen Dateien werden in der Regel mit Dateinamen versehen, die Rückschlüsse auf die veröffentlichende Gruppe zulassen. So wäre es typisch für eine Gruppe namens Underground Cracking Service, ihre Dateinamen mit „u“ beginnen zu lassen (z.B. „u-w98-1.zip“). Manche Gruppen programmieren eigene Installationsroutinen (Installer), in denen sie sich „verewigen“ oder künstlerisch betätigen.

In den meisten Installationsroutinen sind die Cracks schon implementiert, so dass ein manuelles Modifizieren der Programmdateien durch den Nutzer entfällt.

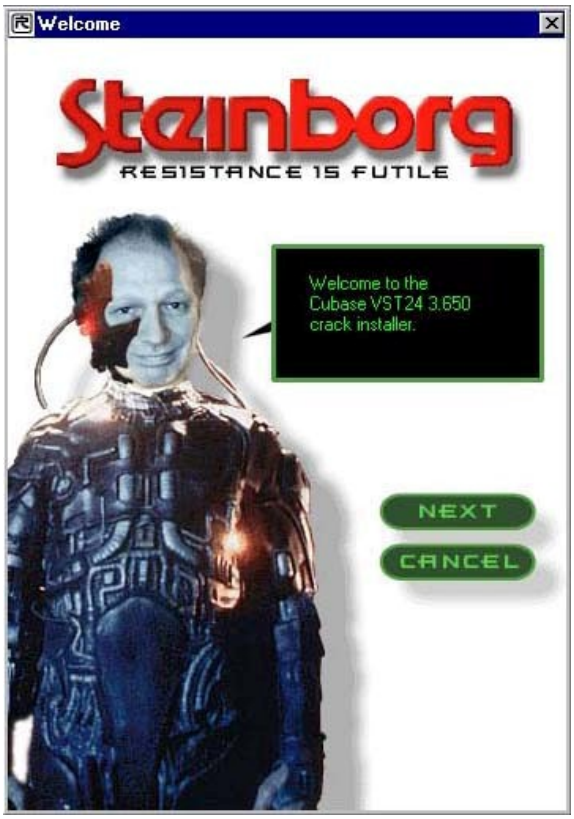


Abbildung 25 – Crack-Installer mit Verunglimpfung des Geschäftsführers des bereits erwähnten Softwareherstellers *Steinberg AG*.

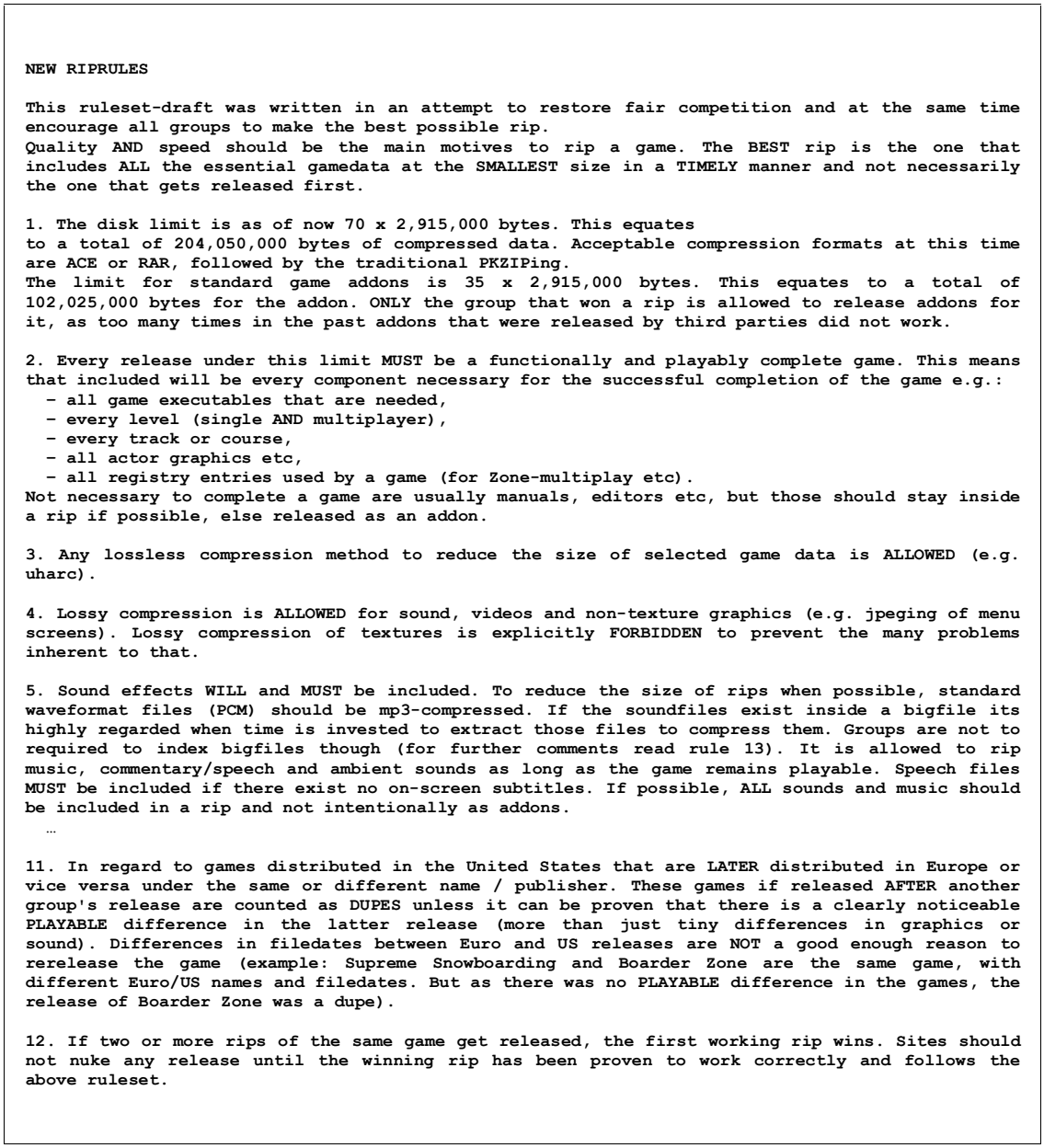
Verwenden die Packager die ursprünglichen Installationsroutinen der Hersteller, entfernen sie häufig die Lizenzbestimmungen aus dem Installer, oder sie bewirken ein Überspringen des Fensters, dass normalerweise die Lizenzhinweise enthält.

In der Warez-Szene gelten strikte Regeln, an die sich die Packager zu halten haben. Aufgestellt werden diese Regeln meist von den Führungspersönlichkeiten mehrerer Gruppen, und ein Bruch dieser „Rip-Rules“ hat zur Folge, dass das veröffentlichte Programm überall gelöscht wird[158].

Programme, die keinen Kopierschutz enthalten, bekommt der Packager direkt vom Supplier übersandt, da ihr Code nicht modifiziert werden muss.

---

[158] Siehe unten Teil 2, A. IV. 7.



NEW RIPRULES

This ruleset-draft was written in an attempt to restore fair competition and at the same time encourage all groups to make the best possible rip.
Quality AND speed should be the main motives to rip a game. The BEST rip is the one that includes ALL the essential gamedata at the SMALLEST size in a TIMELY manner and not necessarily the one that gets released first.

1. The disk limit is as of now 70 x 2,915,000 bytes. This equates
to a total of 204,050,000 bytes of compressed data. Acceptable compression formats at this time are ACE or RAR, followed by the traditional PKZIPing.
The limit for standard game addons is 35 x 2,915,000 bytes. This equates to a total of 102,025,000 bytes for the addon. ONLY the group that won a rip is allowed to release addons for it, as too many times in the past addons that were released by third parties did not work.

2. Every release under this limit MUST be a functionally and playably complete game. This means that included will be every component necessary for the successful completion of the game e.g.:
- all game executables that are needed,
- every level (single AND multiplayer),
- every track or course,
- all actor graphics etc,
- all registry entries used by a game (for Zone-multiplay etc).

Not necessary to complete a game are usually manuals, editors etc, but those should stay inside a rip if possible, else released as an addon.

3. Any lossless compression method to reduce the size of selected game data is ALLOWED (e.g. uharc).

4. Lossy compression is ALLOWED for sound, videos and non-texture graphics (e.g. jpeging of menu screens). Lossy compression of textures is explicitly FORBIDDEN to prevent the many problems inherent to that.

5. Sound effects WILL and MUST be included. To reduce the size of rips when possible, standard waveformat files (PCM) should be mp3-compressed. If the soundfiles exist inside a bigfile its highly regarded when time is invested to extract those files to compress them. Groups are not to required to index bigfiles though (for further comments read rule 13). It is allowed to rip music, commentary/speech and ambient sounds as long as the game remains playable. Speech files MUST be included if there exist no on-screen subtitles. If possible, ALL sounds and music should be included in a rip and not intentionally as addons.

…

11. In regard to games distributed in the United States that are LATER distributed in Europe or vice versa under the same or different name / publisher. These games if released AFTER another group's release are counted as DUPES unless it can be proven that there is a clearly noticeable PLAYABLE difference in the latter release (more than just tiny differences in graphics or sound). Differences in filedates between Euro and US releases are NOT a good enough reason to rerelease the game (example: Supreme Snowboarding and Boarder Zone are the same game, with different Euro/US names and filedates. But as there was no PLAYABLE difference in the games, the release of Boarder Zone was a dupe).

12. If two or more rips of the same game get released, the first working rip wins. Sites should not nuke any release until the winning rip has been proven to work correctly and follows the above ruleset.

Abbildung 26 – Auszug aus sogenannten Rip-Rules für Spielesoftware

5. Leader

Dem Titel entsprechend haben die Leader (auch „Seniors“) innerhalb der Gruppen den höchsten Status inne. Ihre Aufgabe besteht in der Koordination der gesamten Gruppenaktivität. Hierfür stellen sie eigene Regeln auf, nach denen sich die Mitglieder zu richten haben. Ein Bruch dieser Regeln führt häufig zum Ausschluss aus der Gruppe.

Oft handelt es sich bei den Leadern um die Gründungsmitglieder einer Gruppe („Founder“). Den Leader-Status können die Gruppenmitglieder jedoch auch über eine lange Zugehörigkeit oder besondere Verdienste erlangen. Neben der Koordination sind sie oftmals für das Erscheinungsbild der Gruppe und den Inhalt der Textdateien (NFO-Dateien) verantwortlich, die regelmäßig ein Release begleiten. Der Dateiname dieser Textdateien richtet sich in den meisten Fällen nach dem Gruppennamen (z.B. „ucs.nfo“).

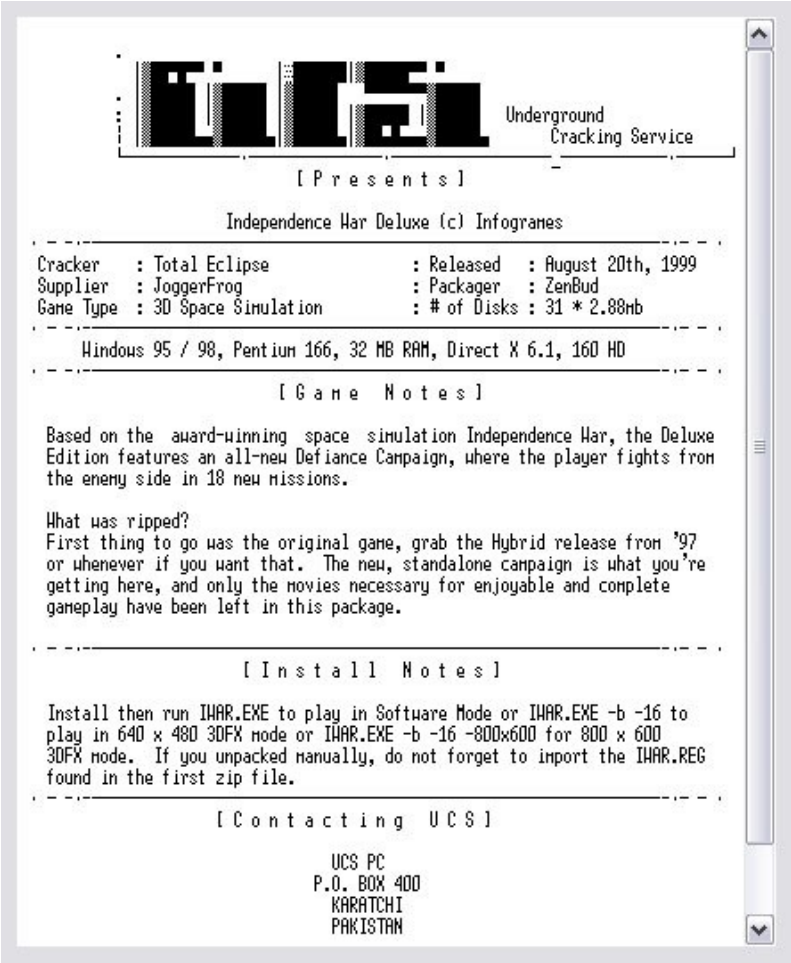


Abbildung 27 – typische NFO-Datei mit außergewöhnlicher Kontakt-Information

NFO-Dateien haben mehrere Funktionen: Zunächst enthalten sie eine Beschreibung des veröffentlichten Programms sowie Hinweise zur richtigen Installation (z.B. Keys oder Seriennummern). Vor allem, wenn ein Programm mit einem Crack modifiziert werden muss, findet sich in der entsprechenden NFO-Datei eine kurze Anleitung.

Häufig enthalten NFO-Dateien kritische Anmerkungen (Reviews) der Gruppenmitglieder zur veröffentlichten Software. Des Weiteren nutzen Warez-Gruppen ihre NFO-Dateien, um befreundeten Gruppen Respekt zu zollen, konkurrierende Gruppen zu verhöhnen oder Personen aus der Szene zu grüßen. Auch die „Moral" oder Philosophie einer Gruppe kann ihren Ausdruck in diesen Textdateien finden. In seltenen Fällen informieren die Autoren ihre Leser über aktuelle Geschehnisse, die für die Internet-Gemeinde von Bedeutung sind.[159]

Früher wurden in NFO-Dateien regelmäßig die Pseudonyme der Mitglieder sowie ihr gruppeninterner Status aufgelistet. Durch den gewachsenen Verfolgungsdruck gehen die Gruppen jedoch dazu über, hierauf zu verzichten.

---

[159] Z.B. bei der umstrittenen Markteinführung des *Intel Pentium III* – siehe hierzu unten Teil 2, C. III. 4. b).

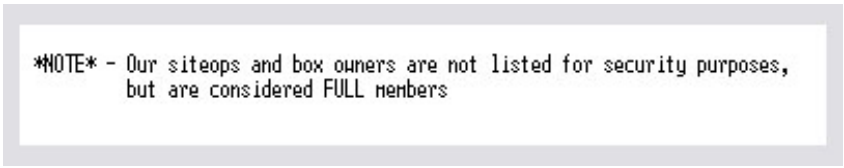


Abbildung 28 – Auszug aus einer NFO-Datei

Neben den NFO-Dateien werden den Releases noch weitere Textdateien beigelegt, die sogenannten DIZ-Dateien. Sie enthalten eine kurze Zusammenfassung des Inhalts der NFO-Datei; wichtig sind vor allem Angaben zu Namen und Version des raubkopierten Programms, zur Anzahl der gepackten Dateien und zur veröffentlichenden Gruppe.

6. Kuriere

Ist das Programm gepackt und mit NFO- und DIZ-Dateien versehen, soll es so weit wie möglich auf szeneinternen Servern verbreitet werden, um den Ruhm der Gruppe zu mehren und die anderen Gruppen teilhaben zu lassen. Zu diesem Zweck gibt es Kuriere (auch „Couriers“, „Spreader“ oder „Currys“), die die Releases rund um den Erdball verschieben. Bei den verwendeten Servern handelt es sich fast ausschließlich um private FTP-Server. Sofern dort regelmäßig die aktuellen Releases einer Gruppe hochgeladen werden, werden sie als Distros[160] (auch „Dizzies“) bezeichnet. Mithilfe spezieller Programme wie *FlashFXP*[161] können FTP-Server quasi ferngesteuert werden. So können selbst Kuriere, die keine schnelle Anbindung ans Internet haben, große Datenmengen direkt zwischen zwei fremden Servern mit hoher Bandbreite verschieben.

Neben den gruppeneigenen Kurieren gibt es ganze Kuriergruppen, die jedoch nicht direkt mit den Warez-Gruppen zusammenarbeiten. Diese sogenannten FXP-Groups bedienen sich lediglich der Releases der Warez-Gruppen und verteilen sie auf zahlreichen öffentlichen FTP-Servern („Pubs“). Die Adressen der Server werden von den Kuriergruppen in WWW-Foren („FXP-Boards“) bekannt gegeben. Innerhalb dieser Vereinigungen herrschen wiederum eigene Regeln. So muss beispielsweise jedes Mitglied bei einer Art Aufnahmeprüfung nachweisen, dass er innerhalb eines bestimmten Zeitraums eine gewisse Mindestmenge an Daten verschieben kann. „Erfolgreiche“ Kuriere erhalten als Gegenleistung für ihre Tätigkeit Zugang zu großen und schnellen privaten FTP-Servern, auf denen die Gruppen ihre Releases zuerst ablegen. Größere Kuriergruppen unterhalten darüber hinaus eigene „Zero-Day-Server“, von denen aus die Mitglieder neue Veröffentlichungen weiterleiten.

In der Regel werden Releases bei ihrem Weg durch das Internet von verschiedenen Kuriergruppen befördert. Um dem Endnutzer der Raubkopie mitzuteilen, wer ihm das Release ein Stück näher gebracht hat, legt jede Kuriergruppe den Programmdateien eine eigene NFO-Datei bei oder kennzeichnet das zur Ablage erstellte Verzeichnis auf dem jeweiligen „Pub“ mit dem Gruppennamen.

---

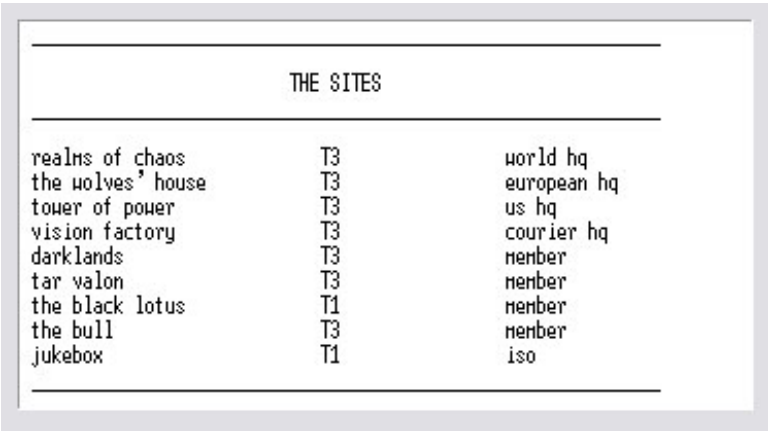
160 Abgeleitet von distribute (engl.) = verteilen.
161 FXP steht für File Exchange Protocol.

Damit gewährleistet ist, dass die beförderten Dateien vollzählig und unbeschädigt sind, erstellen die Kuriere häufig SFV-Dateien[162], die gemeinsam mit dem Release weitergegeben werden. SFV-Dateien enthalten Informationen über die Größe und Anzahl der zu einem Release gehörenden Dateien. Öffnet man sie mit einem speziellen Programm, wird ein sogenannter CRC-Check[163] initiiert, bei dem die vorhandenen Dateien mit den in der SFV-Datei vermerkten Dateien verglichen werden. Signalisiert das SFV-Programm Übereinstimmung, weiß der Nutzer, dass er ein vollständiges Release heruntergeladen hat.

7. Serveradministratoren („Siteops“)[164]

Warez-Gruppen unterhalten in der Regel eine Reihe von FTP-Servern, die nur für den internen Gebrauch bestimmt sind. Hierüber verschieben sie beispielsweise ungecrackte Programme oder die Vorabversionen von Releases („Pre-Dumps“). Auch Releases anderer Gruppen werden auf diesen Servern für die Gruppenmitglieder bereitgestellt. Da solche Server ständig verwaltet und gepflegt werden müssen, gibt es Gruppenmitglieder, die ausschließlich hierfür zuständig sind – die sogenannten Siteops.

Die Gruppen sind immer auf der Suche nach schnellen permanenten Servern, die sie für ihre Zwecke nutzen können. In NFO-Dateien wird daher regelmäßig nach Personen gesucht, die eine solche Anbindung unentgeltlich zur Verfügung stellen können. Die „gruppeneigenen“ FTP-Server werden oft als Headquarters bezeichnet, und in NFO-Dateien findet sich nicht selten eine Auflistung dieser Server, die nur dazu dient, sich mit der weltweiten Verfügbarkeit von schnellen Standleitungen zu brüsten. Die Adressen der Server werden jedoch stets geheimgehalten.



THE SITES

realms of chaos	T3	world hq
the wolves' house	T3	european hq
tower of power	T3	us hq
vision factory	T3	courier hq
darklands	T3	member
tar valon	T3	member
the black lotus	T1	member
the bull	T3	member
jukebox	T1	iso

Abbildung 29 – Auszug aus einer NFO-Datei[165]

---

[162] SFV steht für Simple File Validator. In einer *Windows*-Umgebung werden SFV-Files bevorzugt mit dem Programm *Win-SFV32* erstellt.
[163] CRC steht für Cyclic Redundancy Check.
[164] Kurzform der Worte „Site Operator“.
[165] „T1“ und „T3“ stehen für die Bandbreiten der entsprechenden Server. Eine T1-Standleitung hat eine maximale Übertragungsrate von 1,5 MBit/s; bei einem Server mit T3-Anbindung liegt die Rate bei 45 MBit/s.

Neben der Einrichtung und Verwaltung von FTP-Accounts kümmern sich die Siteops hauptsächlich um Ordnung auf „ihren“ Servern. Hierzu gehört unter anderem das Löschen („Nuken“) von Programmen, die zuvor von einer anderen Gruppe in der selben Programmversion veröffentlicht wurden, die doppelt auf den Server hochgeladen wurden, bei denen NFO-, DIZ- oder SFV-Dateien fehlen oder bei denen in sonstiger Weise gegen die „Rip-Rules“ verstoßen wurde.

8. Coder

Einzelne Gruppen legen ihren Releases sogenannte Demos (auch „Cracktros“)[166] bei. Demos sind kleine Programme, die kurze Animationen ablaufen lassen, nachdem man sie gestartet hat. In diesen meist echtzeitberechneten Grafiken wird häufig die Gruppe gepriesen – z.B. durch rotierende Logos, Totenköpfe oder sonstige psychedelische Sequenzen. Die Programmierer von Demos nennt man Coder, und der wichtigste Grund für das Programmieren von Demos liegt darin, die Geschicke des Coders unter Beweis zu stellen[167].

Abbildung 30 – Standbild einer Demo-Sequenz („Cracktro“)

Erstmals tauchten Demos in den frühen 80er Jahren auf – schon damals als Intro-Sequenzen gecrackter Computerspiele.[168] Mit zunehmender Leistungsfähigkeit der Heimcomputer wurden die Intros der gecrackten Spiele immer eindrucksvoller, so dass sie ab einem gewissen Zeitpunkt

---

[166] „Cracktro“ ist eine Kurzform der Begriffes Crack-Intro.
[167] *Green*, **Wired Magazine** 3.07 – Juli 1995.
[168] Ein umfangreiches „Szene-Archiv“ mit dem Schwerpunkt Grafik/Coding findet sich unter http://www.defacto2.net.

selbständig in einer eigenen Demo-Szene veröffentlicht wurden. Noch heute finden vornehmlich in Nordeuropa Demo-Parties statt, wo sich Hunderte von Computerfreaks treffen, um sich die neuesten Kunstwerke mit Musikuntermalung auf Großleinwänden anzusehen. Auf diesen Parties wird man, abgesehen von Verstößen gegen Betäubungsmittelgesetze, keine illegalen Aktivitäten beobachten können. Dennoch gab es seit jeher enge Verbindungen zwischen der Demo- und der Softwarepiraten-Szene. So wurden in den frühen Tagen der Softwarepiraterie Demos als Quasi-Währung gegen raubkopierte Programme getauscht.[169]

Abbildung 31 – Standbild einer Demo-Sequenz („Cracktro“)

Neben den Demo-Codern gibt es in einigen Gruppen auch sogenannte Script-Coder. Diese versuchen, die zahlreichen Vorgänge zu automatisieren, die für die Erstellung eines Warez-Releases notwendig sind. Die von ihnen geschriebenen Programme werden als „Scripts“ bezeichnet.

---

169 *Green*, **Wired Magazine** 3.07 – Juli 1995.

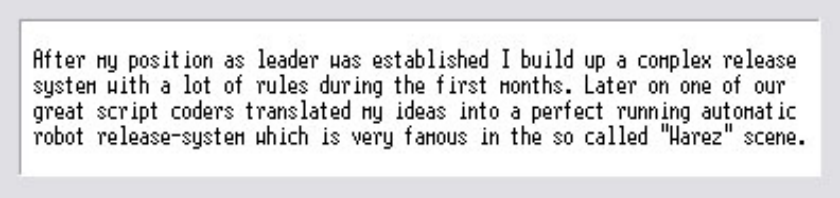


Abbildung 32 – Auszug aus einer NFO-Datei

V. Szenemitglieder ohne Gruppenzugehörigkeit

1. Leecher

Leecher bedeutet übersetzt soviel wie Schnorrer oder Nutznießer. Leecher tragen nichts zum Erhalt oder Funktionieren der Warez-Szene bei, sondern bedienen sich lediglich auf FTP-Servern oder auf Webseiten, ohne eine Gegenleistung zu erbringen. Sie sind in der Szene eher unbeliebt, dürften jedoch den größten Teil derselben ausmachen.

2. Trader

Trader handeln nach dem Tauschprinzip. Wenn sie sich beispielsweise etwas von einem FTP-Server herunterladen, laden sie im Gegenzug einige Releases auf diesen Server hoch, die der Betreiber des Servers noch nicht hat. Somit sorgen Trader neben den Kurieren dafür, dass Releases weite Verbreitung finden. Besonders engagierte Warez-Trader verbreiten Raubkopien auch ohne konkrete Gegenleistung, indem sie beispielsweise Webseiten ins Netz stellen, auf denen jedermann gecrackte Software herunterladen kann.

3. Profit-Pirates[170] (Warez-Sellers)

Wie der Name erahnen lässt, versuchen sich Profit-Pirates durch den Verkauf von Raubkopien, die sie sich über das Internet beschafft haben, zu bereichern. In der Regel werden Warez-Compilations auf CD gebrannt und zum Kauf angeboten. Dabei handelt es sich regelmäßig um Zusammenstellungen mehrerer Programme einer bestimmten Art (z.B. Game-Compilations) oder Sammlungen sämtlicher aktueller Releases.[171]

```
From: <adobe_special@hakone.eri.u-tokyo.ac.jp>
Subject: All Software/All The Time
Date: Wed, 28 Feb 2001 04:41:27

Adobe Web Collection
The adobe Webcollection is a cd with 9 software programs on it.
Adobe made this cd so you dont have to go and buy each product seperate.
This cd has 9 famous products of adobe on it.

Photoshop5.5, Illustrator8.0, Indesign, Premiere5.0, AfterEffects4.0, PageMaker6.5,
Golive4.0, AdobeDimensions3.0, Acrobat4.0
```

---

[170] Der Ausdruck stammt von *McCandless*, **Wired Magazine** 5.04 – April 1997.
[171] Vgl. *Puscher*, **internet world** 1/1999, S. 35.

```
Includes all serials and plugins. Note All programs are on 1 CD. This CD
has over a $2000 Retail Value.

Special 1 Time Offer: EVERYTHING is on one CD - $99.95
interested e-mail: adobecdoffer@email.com

Currently We Accept: Master Card & Visa - Orders ship withen 72/hrs
```

Abbildung 33 – E-Mail-Werbung eines japanischen Profit-Pirate

Die Käufer von Warez-CDs ersparen sich nicht nur die langen Downloadzeiten und die damit verbundenen Kosten, sondern auch die zeitaufwändige Suche nach den entsprechenden Releases. Neben Zeitungsannoncen und Mund-zu-Mund-Propaganda nutzen Profit-Pirates verstärkt das Internet, um Kunden für ihre Raubpressungen zu finden.

Abbildung 34 – Homepage eines Profit-Pirate

Da die meisten Warez-Gruppen ohne finanzielle Interessen arbeiten, wird es in der Szene nicht gern gesehen, wenn gecrackte Software verkauft wird. In den NFO-Dateien fast aller Gruppen werden Profit-Pirates verurteilt.[172]

Ein neues Betätigungsfeld haben Profit-Pirates in Online-Auktionen gefunden. Nach Studien der US-Branchenverbände *Software and Information Industry Association* (*SIIA*) und *Business Software Alliance*

[172] Siehe hierzu unten Teil 2, A. VIII. 1.

(*BSA*) soll mehr als 90% der auf Web-Auktionen angebotenen Software raubkopiert sein.[173] Beobachtet wurde das Angebot der Auktionshäuser *eBay*, *Yahoo-Auctions* und *Exite@Home,* die allerdings mit ihren Webseiten nur eine Plattform für die Auktionen zur Verfügung stellen. Die Verantwortung für den Handel liegt gemäß den Nutzungsbedingungen der Online-Auktionshäuser beim Verkäufer der versteigerten Waren.

Eine weitergehende Befürchtung der Softwareindustrie besteht darin, dass Profit-Pirates durch das Beobachten von Online-Auktionen an Namen und E-Mail-Adressen von potentiellen Warez-Kunden gelangen und sich somit Kundenkarteien für den direkten Verkauf gestohlener Software anlegen können.

4. Betreiber von Release-Info-Seiten („Dupecheck-Sites“)

Eine kleine Gruppe von Szenemitgliedern betreibt Webseiten, auf denen Listen abgerufen werden können, die sämtliche Releases der aktiven und inaktiven Warez-Gruppen aufführen.

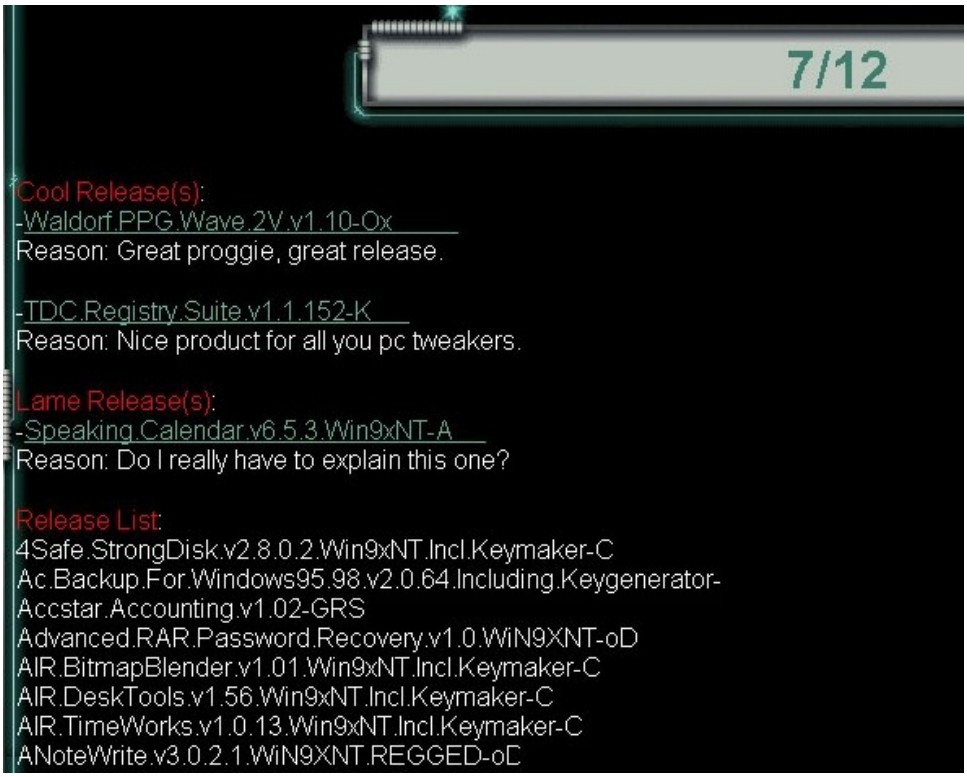


Abbildung 35 – Release-Info-Seite

Der Sinn dieser „Dupechecker“ besteht zum einen darin, den Tradern die Suche nach Programmen zu erleichtern, zum anderen können auch die Gruppen anhand der Listen überprüfen, ob die Software, die sie verbreiten wollen, bereits von einer anderen Gruppe veröffentlicht wurde. Die

---

[173] **Heise Online News** vom 12.04.2000, http://www.heise.de/newsticker/meldung/9041 und vom 15.11.2000, http://www.heise.de/newsticker/meldung/13218.

Einträge auf den Release-Info-Seiten sind in der Regel sehr aktuell und enthalten Informationen zur Version der Software, zur veröffentlichenden Gruppe und zum Zeitpunkt der Veröffentlichung. Auf „Dupecheck"-Seiten wird man niemals auf Downloadmöglichkeiten für raubkopierte Software stoßen, auch Werbebanner[174] sind eher die Ausnahme.

VI. Kommunikationswege der Warez-Szene

Um Hinweise auf Downloadmöglichkeiten zu erhalten bzw. zu geben und um sonstige Informationen auszutauschen, werden in der Warez-Szene vornehmlich die folgenden Kommunikationsmedien genutzt:

1. IRC

Die Mitglieder der Warez-Szene treffen sich in einschlägigen IRC-Channels, um miteinander zu kommunizieren und Raubkopien zu tauschen. Gruppenmitglieder kommen fast ausschließlich in privaten Channels zusammen, die ein Außenstehender nur mit einer expliziten Einladung oder mit einem geheimen Passwort betreten darf. Diese Channels sind so konfiguriert, dass sie auch nicht in der Liste der gesamten auf einem IRC-Server befindlichen Chatrooms auftauchen. Die Namen von Warez-Channels lassen nur bedingt auf ihren tatsächlichen Charakter schließen. Mehr und mehr wird dazu übergegangen, unverfängliche Namen für die Chaträume zu wählen (z.B. #painters anstelle von #warez-graphics). Über das Channel-Topic werden häufig Hinweise auf neue Releases oder auf Downloadmöglichkeiten gegeben. In manchen Channels sind DCC-Bots im Einsatz, die den Teilnehmern auf Befehl Textdateien zusenden, in denen Listen von FTP-Servern oder Webseiten zusammengestellt sind.

2. Instant Messaging Systeme

Mit Anwendungen wie *ICQ* werden hauptsächlich Adressen von Webseiten und FTP-Adressen ausgetauscht. Spezielle Chats, die sich mit Raubkopien beschäftigen, gibt es kaum, da die Chatrooms temporär sind und nur selten mehr als drei Nutzer beherbergen. „Szene-Profis" mögen Instant Messaging Systeme als Kommunikationsmedium nicht, weil man als User dieser Dienste recht leicht aufzuspüren ist. So gibt *ICQ* die aktuelle IP-Adresse aller Teilnehmer auf Nachfrage heraus, es sei denn, man hat diese Option explizit abgeschaltet. Zudem gilt *ICQ* in Fachkreisen als unsichere Anwendung, was Hackangriffe auf das eigene System betrifft.[175]

3. E-Mail

Wenn E-Mail als Kommunikationsmedium der Warez-Szene genutzt wird, dann meist in Verbindung mit Mailinglisten. Deren Betreiber senden regelmäßig E-Mails mit Hinweisen auf Download-

---

[174] Hierunter versteht man Werbegrafiken, die in der Regel dynamisch auf einer Webseite eingebunden werden, d.h. der angezeigte Inhalt stammt in der Regel von einem anderen Server und variiert ständig. Als Standardformat für Banner hat sich eine Größe von 400x40 oder 468x60 Pixeln etabliert.

[175] *Schuster*, **PC-Intern** 8/1998, S. 45.

möglichkeiten an die eingetragenen Empfänger. Enthalten die E-Mails Listen mit FTP-Servern, werden neben der IP-Adresse und den notwendigen Zugangsdaten oftmals Informationen über den Inhalt des Servers angegeben.

```
ù WLC ù [3686] <18 Feb 1998 21:58> Rated: 4
195.230.xxx.xxx / l:temp p:temp
corel draw 8, phototools 2, photoshop update, .....

ù WLC ù [3725] <19 Feb 1998 12:30> Rated: 4
194.248.xxx.xxx /d:/ l/p:warez port:66
Ignore the ratio message.. Demonstar, Dogz, Extreme pinball, ManxTT, Quake II,
Fighting Force - Ninja, AOE Campaigns, GTA-Stuff, Quake II Stuff, Toca Speech
AddOn, Croc, JediKnight Stuff, Lsl5, Nitro Racers 3D, Slamtilt Pinball, Shadows of
the Empire, Ten

ù WLC ù [3733] <19 Feb 1998 14:07> Rated: 5
131.183.xxx.xxx l:dominating p:NSX
only apps...nothing new

ù WLC ù [3757] <19 Feb 1998 20:36> Rated: 2
24.112.xxx.xxx /UPLOADS/O-DAY UPLOADS l:anon p:anon port:21
full of 0-day from 2/16-2/19

ù WLC ù [3862] <20 Feb 1998 19:53> Rated: 1
140.160.xxx.xxx / l/p:user
Adobe Illustrator 7.0, AOL punter, Communicator 4.04 Complete, Font FX, Hotmail
Express Notify, ICQ 98a, Kia Power Goo, McAffee Web Scan 3.12, mIRC 5.31, MPlifier
0.33, Tomb Raider 2, Virtual Places, Vivo Player, WarFTP 1.65, WinDAC 1.33, Winrar
2.02, Winzip 6.3
```

Abbildung 36 – Auflistung von FTP-Servern

4. UseNet

Auch im UseNet gibt es Newsgroups, in denen Informationen über Raubkopien ausgetauscht werden. Hierbei handelt es sich überwiegend um die sogenannten Binaries-Gruppen. Dem Namen nach sind diese Newsgroups zwar nur zum Download von Dateien bestimmt, doch sie dienen auch der Kommunikation. Häufig werden die einschlägigen Newsgroups von den Serveradministratoren der großen Internetprovider gesperrt, so dass sich der Nutzer bei einem kostenpflichtigen Dienst anmelden muss, wenn er Zugriff auf News-Server erhalten möchte, die alle Newsgroups enthalten.

5. WWW

Abgesehen von den bereits erwähnten Release-Info-Seiten hat das WWW aufgrund seiner vergleichsweise geringen Flexibilität eine untergeordnete Bedeutung als Kommunikationsmedium für die Warez-Szene. Im Web finden sich dennoch zahlreiche Webseiten mit Foren (z.B. sogenannte FXP-Boards[176]), Listen von FTP-Servern oder Links zu Download-Seiten. Zu den Webseiten gehören vor allem die sogenannten Top-Sites (Top 50, Top 100 etc.), auf denen Linklisten zu den angeblich populärsten Webwarez-Seiten abgerufen werden können.

---

[176] Siehe oben Teil 2, A. IV. 6.

Abbildung 37 – „Top-Site“

Abbildung 38 – „Top-Site“

VII. Wege der illegalen Softwaredistribution

1. WWW

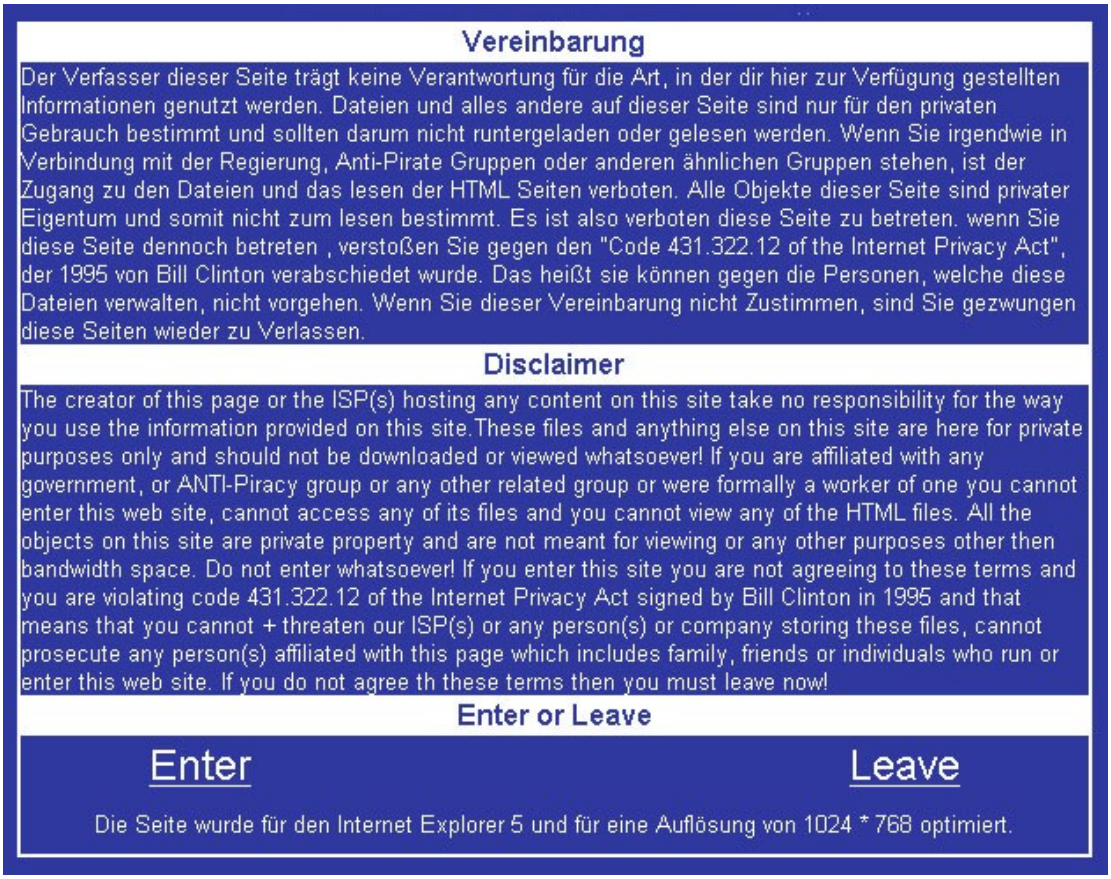
Im Gegensatz zu seiner untergeordneten Rolle als Kommunikationsmedium spielt das Web bei der Verbreitung von Raubkopien eine tragende Rolle. Warez-Pages sind im WWW weit verbreitet, und fast immer entsteht der Eindruck, dass sie sich in der Nähe einschlägiger kommerzieller Sex-Seiten befinden[177]. Das liegt vor allem daran, dass viele Betreiber von Warez-Seiten mit Werbung für pornographische Homepages Geld verdienen möchten. Daher stellen sie Werbebanner der entsprechenden Homepages – meist Bilder von spärlich bekleideten Frauen in eindeutigen Positionen – auf ihre Warez-Seite. Hinter den Bannern liegt ein Link, der direkt zum Anbieter der pornographischen Inhalte führt. Klickt ein Besucher der Warez-Seite auf das Banner, bekommt der Betreiber der Warez-Seite von dem Betreiber der Sex-Seite eine Vergütung. Üblicherweise wird monatlich die Anzahl der Besucher gezählt, die über die Warez-Seite auf die Sex-Seite gekommen sind. In diesem Zusammenhang wird auch von „Mouseclicks“ oder „Clicks“ gesprochen. Der Betreiber der beworbenen Seite zahlt dem Betreiber der Warez-Seite beispielsweise einen Cent pro Klick auf das Werbebanner.

Im untrennbaren Zusammenhang mit der Verbreitung von Raubkopien im WWW stehen auch die sogenannten Crackz- und Serialz-Seiten. Auf Crackz-Seiten können meist Hunderte von Cracks oder Keymakers zum Download angeboten werden, da sie sehr klein sind. Das Angebot dieser Webseiten ist typischerweise alphabetisch geordnet. Dies gilt auch für die meisten Seiten, auf denen Seriennummern und Registrierungscodes zum Download bereitstehen. Die Textdateien, die entsprechende Informationen enthalten, sind kleiner als Cracks und Keymaker, so dass eine noch mühelosere Verbreitung möglich ist.

Bei vielen Warez-Webseiten erscheint zu Anfang ein Hinweis des Betreibers, dass er keine Verantwortung für den Inhalt der Seite übernimmt. Diese als „Disclaimer“ bezeichnete Erklärung enthält sehr oft eine irrwitzige Rechtsbelehrung: Danach handle es sich bei der auf der Webseite zu beziehenden Software um Programme, die lediglich Anschauungs- und Bildungszwecken („educational purposes“) dienen, und die man zumindest für 24 Stunden legal auf dem eigenen Rechner behalten dürfe. Danach müssten sie jedoch umgehend gelöscht werden.

---

[177] *Puscher*, **internet world** 1/1999, 35.



Vereinbarung

Der Verfasser dieser Seite trägt keine Verantwortung für die Art, in der dir hier zur Verfügung gestellten Informationen genutzt werden. Dateien und alles andere auf dieser Seite sind nur für den privaten Gebrauch bestimmt und sollten darum nicht runtergeladen oder gelesen werden. Wenn Sie irgendwie in Verbindung mit der Regierung, Anti-Pirate Gruppen oder anderen ähnlichen Gruppen stehen, ist der Zugang zu den Dateien und das lesen der HTML Seiten verboten. Alle Objekte dieser Seite sind privater Eigentum und somit nicht zum lesen bestimmt. Es ist also verboten diese Seite zu betreten. wenn Sie diese Seite dennoch betreten , verstoßen Sie gegen den "Code 431.322.12 of the Internet Privacy Act", der 1995 von Bill Clinton verabschiedet wurde. Das heißt sie können gegen die Personen, welche diese Dateien verwalten, nicht vorgehen. Wenn Sie dieser Vereinbarung nicht Zustimmen, sind Sie gezwungen diese Seiten wieder zu Verlassen.

Disclaimer

The creator of this page or the ISP(s) hosting any content on this site take no responsibility for the way you use the information provided on this site.These files and anything else on this site are here for private purposes only and should not be downloaded or viewed whatsoever! If you are affiliated with any government, or ANTI-Piracy group or any other related group or were formally a worker of one you cannot enter this web site, cannot access any of its files and you cannot view any of the HTML files. All the objects on this site are private property and are not meant for viewing or any other purposes other then bandwidth space. Do not enter whatsoever! If you enter this site you are not agreeing to these terms and you are violating code 431.322.12 of the Internet Privacy Act signed by Bill Clinton in 1995 and that means that you cannot + threaten our ISP(s) or any person(s) or company storing these files, cannot prosecute any person(s) affiliated with this page which includes family, friends or individuals who run or enter this web site. If you do not agree th these terms then you must leave now!

Enter or Leave

Enter Leave

Die Seite wurde für den Internet Explorer 5 und für eine Auflösung von 1024 * 768 optimiert.

Abbildung 39 – Disclaimer einer Warez-Seite

GameCopy

IMPORTANT NOTICE

GameCopy ONLY supplies Information and Tools necessary to make a PERSONAL BACKUP of legally owned Game CD's. GameCopy cannot be held responsible if any of the information & files contained on this site is used in the pursuit of illegal activities such as copyright infringement or piracy.

Keep the following in mind when making a backup of an Original Game:

- You are LEGALLY ALLOWED to make a personal backup of an Original Game CD as long as you are the owner of the Original Game CD.
- You are NOT ALLOWED to sell, rent or give away any backups of copyrighted Games CD's, as this is not allowed by Copyright Laws.
- You MUST DESTROY any backups when you don't own the Original Game CD anymore (e.g. selling or giving it away)
- Before making a backup check, in the supplied manual or on the back of the CD, if there are special conditions for making a backup.

You are ONLY allowed to ENTER GameCopy if you need information to make a backup of an Original Game CD of which you are the legal owner.

ENTER

Abbildung 40 – Disclaimer einer Crack-Seite

Neben dem berühmten „24-Stunden-Disclaimer“ hat sich vor allem auf deutschen Warez-Seiten eine eher amüsante Rechtsbelehrung etabliert: In diesem Disclaimer wird eindringlich darauf hingewiesen, dass sich derjenige, der sich Raubkopien von der Seite herunterlädt, nach § 108 StGB strafbar macht. Dass § 108 StGB die Wählernötigung unter Strafe stellt, dürfte den wenigsten Seitenbetreibern und Besuchern bekannt sein.

Es hat den Anschein, dass viele Betreiber von Warez-Seiten tatsächlich dem Irrglauben erliegen, sich mit derartigen Disclaimern jeglicher rechtlicher Verantwortung entziehen zu können, denn diese Meinung ist in der Szene weit verbreitet und wird nur selten in Frage gestellt.

Abschließend ist anzumerken, dass die Warez-Gruppen nicht im WWW aktiv sind, was die Verbreitung ihrer Releases anbelangt. Sogenannte Webwarez sind in der Szene verpönt und werden fast ausschließlich von Personen bereitgestellt, die keinen direkten Kontakt zu den Gruppen haben, sich jedoch ihrer Releases bedienen.

[ich habe meine Seite aus mehreren Gründen geschlossen.....] ...ein weiterer Grund ist die aktuelle Lage in der deutschen Warez-Szene. Die Release-Groups boykottieren jede Seite auf der Ihre Releases zu finden sind. Ich habe in den letzten Tagen Emails von mindestens 10 Webmastern erhalten, die neue Projekte gestartet haben und fragten, ob ich sie einmal erwähnen könne. Doch nur kurze Zeit später kam eine weitere Mail in der sie mir schrieben, dass sie die Seite leider schließen mussten, da sich irgendein Mitglied von irgendeiner super-ultra-wichtigen Release-Group bei ihnen gemeldet hat und mit Gott-Weiß-Was gedroht hat wenn man die Seite nicht schließen würde....

Abbildung 41 – Auszug eines Textes von einer geschlossenen Warez-Seite

Abbildung 42 – Grafik aus einer NFO-Datei

2. FTP

Beim größten Teil der FTP-Server, die zur Verbreitung von Raubkopien eingesetzt werden, dürfte es sich um private FTP-Server handeln. Durch immer günstigere Standleitungen – vor allem in den Vereinigten Staaten – entstehen zunehmend schnelle „Kinderzimmerserver", die permanent als Software-Umschlagplätze fungieren können.

Neben sogenannten Leech-FTPs, auf denen sich jedermann frei bedienen kann, gibt es auch Server, die als „Ratio-FTPs" bezeichnet werden. Bei diesen ist die Serversoftware so eingestellt, dass einem Nutzer erst dann ein Download ermöglicht wird, wenn er zuvor etwas auf den Server hochgeladen hat. Demnach darf er sich bei einer Ratio von 1:5 fünf Megabyte an Daten herunterladen, wenn er zuvor ein Megabyte hochgeladen hat. Durch dieses System geht der Serverbetreiber sicher, dass er immer neue Software im Incoming- bzw. Uploads-Verzeichnis seines Servers vorfindet. In der Onjoin-Message[178] oder in Verzeichnissen bzw. Textdateien, die mit dem Namen „Requests" betitelt sind, äußern die Serverbetreiber meist Wünsche bezüglich der von ihnen gesuchten Software.

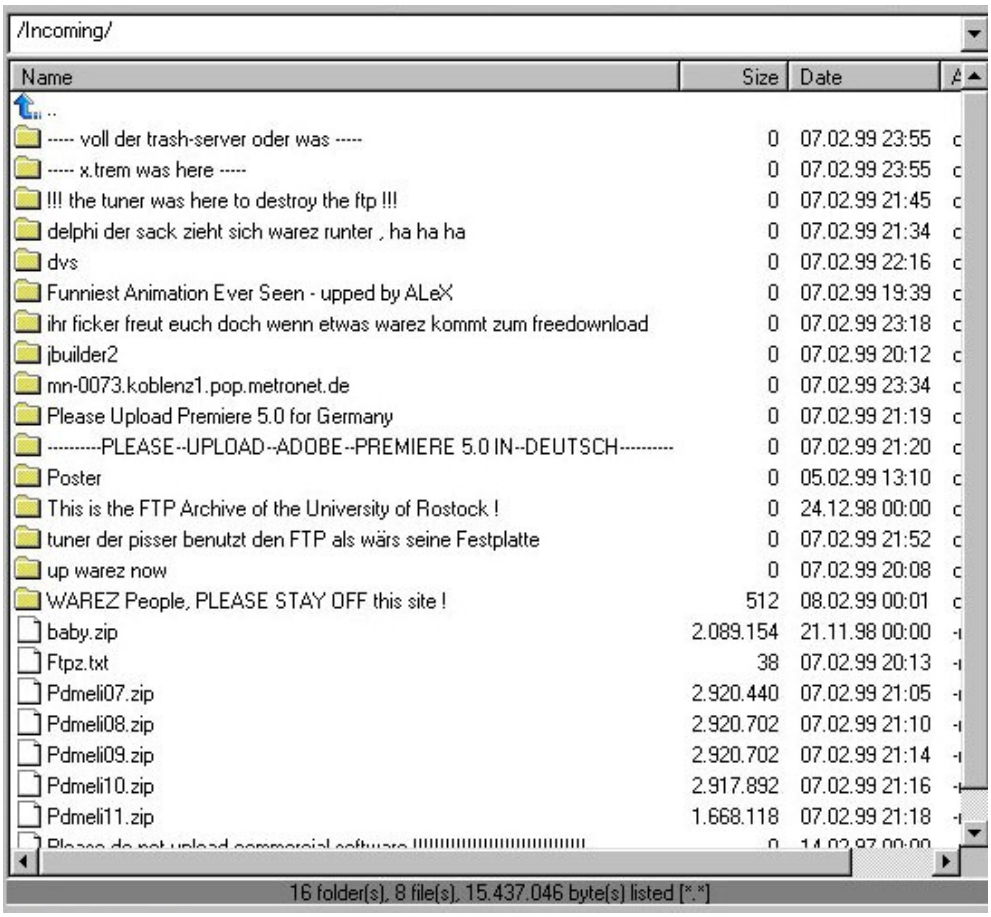


Abbildung 43 – Incoming-Verzeichnis des FTP-Servers der Universität Rostock (Februar 1999)

[178] „Betritt" man einen FTP-Server, bekommt man häufig im FTP-Client eine kurze Textbotschaft des Serverbetreibers angezeigt. Mit der Onjoin-Message werden üblicherweise die Gäste begrüßt und über den Besitzer bzw. seinen Server informiert.

Auch öffentliche FTP-Server („Pubs“) werden zum Verschieben von Raubkopien missbraucht.[179] Besonders Universitäten und große Unternehmen sind hiervon betroffen, da ihre Rechner mit einer enormen Bandbreite an das Internet angeschlossen sind.[180] Softwarepiraten nutzen die Incoming-Verzeichnisse der öffentlichen Server gerne als temporäre Ablagemöglichkeiten für Raubkopien.[181] In diesem Zusammenhang wird von „Dump-“, „Drop-“ oder „Swap-Sites“ gesprochen. Meist werden sie nur für kurze Zeit genutzt oder an Wochenenden, wenn die Serveradministratoren nicht im Dienst sind.

Damit die illegalen Aktivitäten möglichst lange unbemerkt bleiben, richten die Piraten oftmals unsichtbare Verzeichnisse auf den Public FTPs ein. Hierbei bestehen die Verzeichnisnamen aus Leerzeichen, wodurch sie für den Serveradministrator zunächst nicht sichtbar sind. Allerdings ergeben sich zahlreiche andere Hinweise, an denen sich der Missbrauch festmachen lässt. Die *SPA* hat die wichtigsten Warnhinweise für Administratoren von öffentlichen FTP-Servern auf ihrer Webseite zusammengestellt:

Sieben Warnzeichen für Piraterie:

1. Stark erhöhter FTP-Dateiverkehr (Traffic) in einem Verzeichnis
2. Erweiterte Verzeichnisstrukturen
3. Übermäßiger Traffic bei einzelnen Downloadvorgängen
4. Benutzung der Begriffe *Warez, Cracker* oder *Hacker*
5. Bereitstellen von Seriennummern für kommerzielle Software
6. Erhöhte Zugriffszahlen auf bestimmte Bereiche
7. Anhäufung von verdächtigen oder versteckten Dateien bzw. Verzeichnissen

Abbildung 44 – Warnhinweise der *SPA* für FTP-Administratoren[182]

3. UseNet

Neben den bereits erwähnten Binaries-Newsgroups werden Raubkopien auch über unverdächtig benannte Gruppen wie beispielsweise *soc.culture.russian* im UseNet verbreitet.[183] Die Bedeutung des UseNet als Medium zur Verbreitung von Software ist jedoch rückläufig, da das Herunterladen aus den Newsgroups weniger komfortabel ist als das Laden aus dem WWW oder von FTP-Servern.

---

[179] „Pubs“ werden vornehmlich von sogenannten FXP-Groups genutzt, siehe oben Teil 2, A. IV. 6.
[180] Vgl. *Kürten,* **PC-Intern** 8/1998, S. 37.
[181] Vgl. das Interview mit *Maletzky* vom Rechenzentrum der *Universität Rostock* in **PC-Intern** 8/1998, S. 34.
[182] Quelle: http://www.spa.org (übersetzt aus dem Englischen).
[183] **Chip** 9/98, S. 56.

4. IRC

Auch der IRC wird für den Austausch von Raubkopien nur in geringem Umfang genutzt. Wenn gecrackte Software im IRC „verschoben“ wird, dann über DCC-Datentransfer zwischen zwei Teilnehmern, F-Serve oder über DCC-Bots.

Zuweilen gibt es Channels, die vollständig automatisiert erscheinen. Hier befinden sich zahlreiche DCC-Bots, die Dateien an die Teilnehmer verschicken können. Über ein bestimmte Kommandos („Trigger“) kann der Chatter die Bots fernsteuern und sich beispielsweise eine Mitteilung zuschicken lassen, in der er Informationen über die erhältliche Software und die Bedienung der Bots findet.

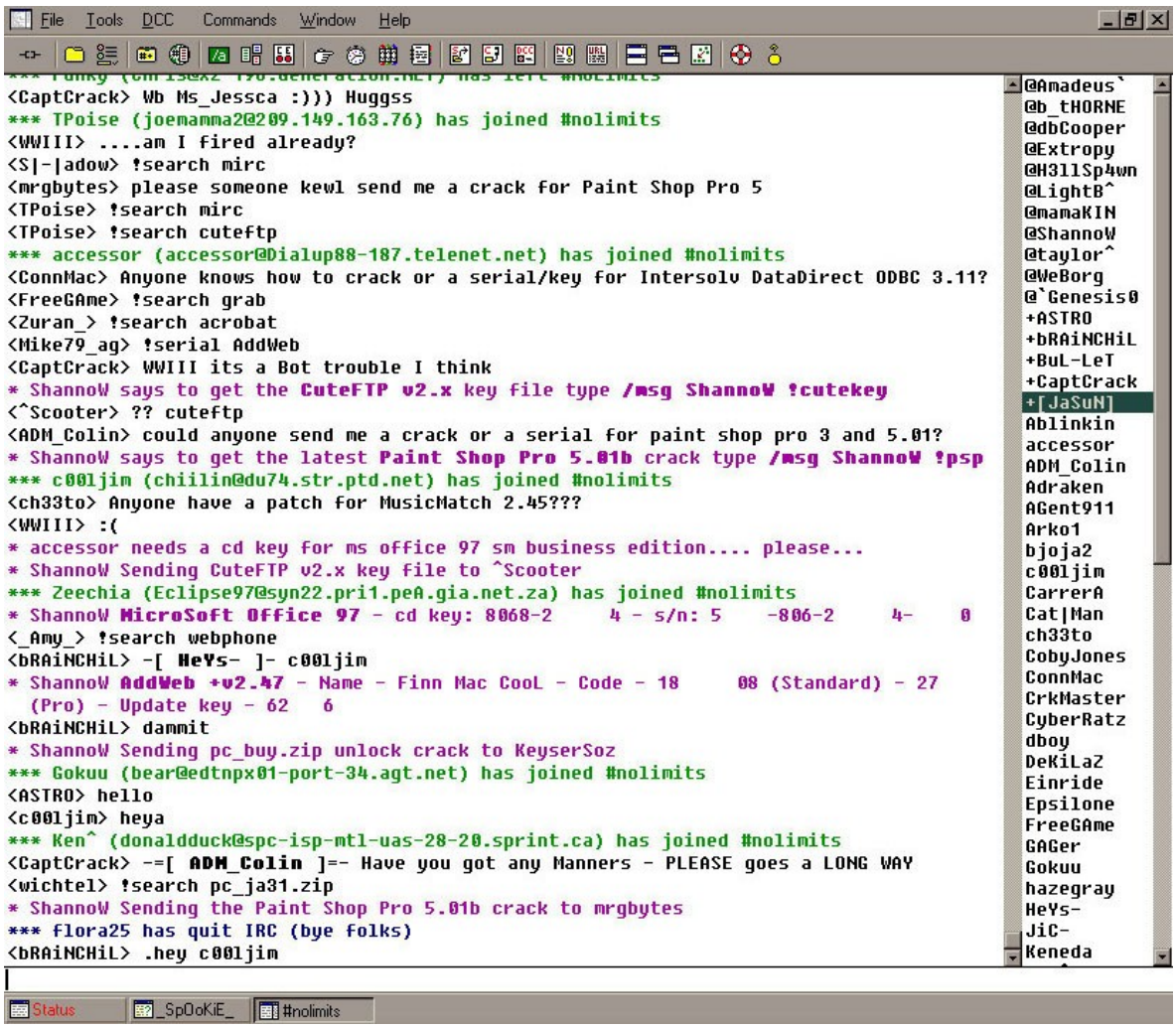


Abbildung 45 – IRC-Channel mit automatisierter Ausgabe von Seriennummern

5. E-Mail

Als E-Mail-Attachments werden Raubkopien nur selten versendet. Zwar soll es Mailinglisten geben, über die täglich aktuelle Releases an die Empfänger verschickt werden, aber durch die regelmäßige Beschränkung der Mailserver auf eine bestimmte Dateigröße pro E-Mail sind der Verbreitung

Grenzen gesetzt. Mit zunehmenden Bandbreiten und Speicherressourcen könnte sich dies jedoch schon in naher Zukunft ändern.

6. Instant Messaging Systeme

Zwar können mit den meisten Instant Messaging Systemen auch Daten übertragen werden, dennoch kommt diese Funktion kaum zum Einsatz, da der Datentransfer über diese Dienste in der Regel langsam und unzuverlässig ist.

7. Peer-to-Peer-Filesharing-Systeme (P2P-Systeme)

P2P-Programme werden zunehmend genutzt, um Raubkopien zu tauschen. Allerdings werden sie weder von Warez-Gruppen noch von Personen genutzt, die gewerbsmäßig mit Raubkopien handeln. Hier stellen Tausende von Internetnutzern anderen Internetnutzern alle Arten von Dateien zur Verfügung, die sich auf ihren heimischen Festplatten befinden. In der letzten Zeit ist ein Trend zu beobachten, wonach sich in P2P-Netzen verstärkt ISO-Dateien von Computerprogrammen befinden. Im Gegensatz zur in der Gruppenszene erhältlichen Software handelt es sich jedoch überwiegend um sogenannte Topseller, also die ganz bekannten und begehrten Programme; spezielle oder unbekanntere Software lässt sich kaum über P2P-Systeme beziehen.

Die große Popularität der P2P-Systeme resultiert aus dem Musik- und Filmtausch, weshalb sich ein Abschnitt im dritten Teil dieser Arbeit ausführlich mit ihnen auseinandersetzt.

VIII. Phänomenologische Betrachtung der Warez-Szene

1. Subkulturelle Besonderheiten

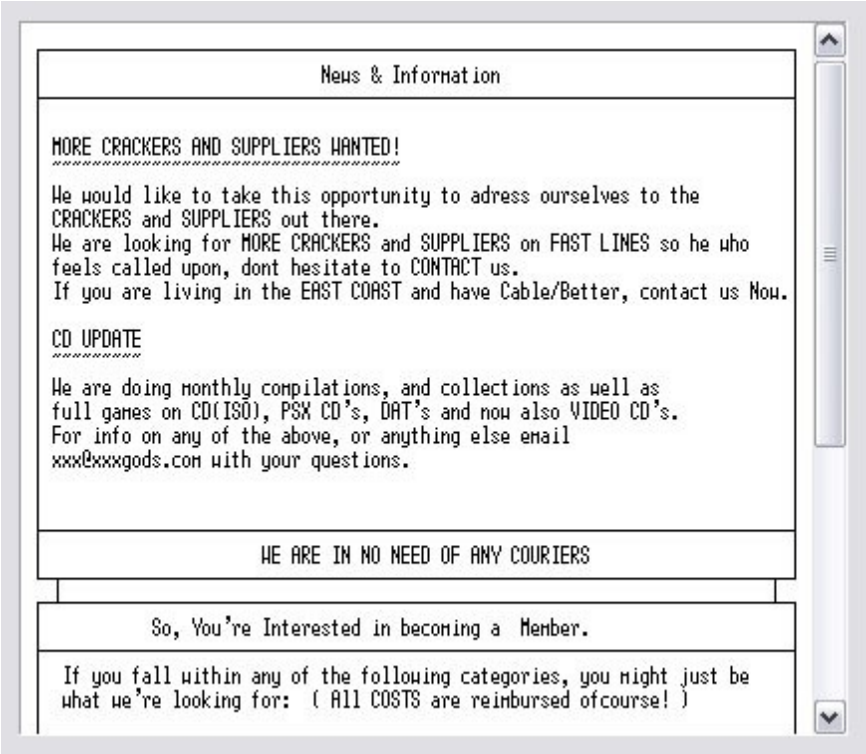
Große Teile der Internetgemeinde sind von einer anarchischen Grundtendenz geprägt[184], wovon auch die Warez-Szene nicht ausgenommen bleibt. Die Mehrheit der Szenemitglieder stellt althergebrachte Autoritäten in Frage und fühlt sich als Teil einer alternativen Gesellschaftsform. Das Leben in dieser regelrechten Computer-Subkultur[185], die ihre eigenen Regeln und Gepflogenheiten hat, bewirkt überdies einen starken Zusammenhalt. Prägend sind ebenfalls die vermeintliche Sicherheit und Anonymität, die das Internet seinen Nutzern bietet. Hierdurch ist es unter anderem möglich, sich seinem virtuellen Gegenüber nach eigenen Vorstellungen zu präsentieren.

Bei den Warez-Gruppen selbst fallen Parallelen in der Organisation und Planung zu betriebswirtschaftlichen Unternehmungen und zur organisierten Kriminalität auf. Zu erwähnen sind vor allem Stichworte wie Personenmehrheit, hierarchische Struktur, Arbeitsteilung, Gehorsam und Dauerhaftigkeit. Allerdings fehlt in den meisten Fällen ein wichtiges Hauptmerkmal: Fast alle Gruppen arbeiten ohne Gewinnorientierung. Den typischen „Berufsverbrecher“ wird man daher in Warez-Gruppen kaum antreffen. Anders sieht es dagegen bei den Profit-Pirates aus: Hier ist davon auszugehen, dass einige Raubkopierer von dem Erlös aus CD-Verkäufen ihren Lebensunterhalt bestreiten oder sich zumindest ein nicht unwesentliches Zubrot verdienen.

---

184 Vgl. *Hoeren*, Das Internet für Juristen, **NJW** 1995, S. 3298; *Meseke*, S. 529.
185 *Schultz*, S. 123.

Vorherrschendes Prinzip in der Warez-Szene ist und bleibt das Tauschprinzip. Von 254 vom Verfasser untersuchten Gruppen gab es lediglich zwei Gruppen, die in ihren NFO-Dateien ein finanzielles Interesse erkennen ließen.[186]


News & Information

MORE CRACKERS AND SUPPLIERS WANTED!

We would like to take this opportunity to adress ourselves to the CRACKERS and SUPPLIERS out there.
We are looking for MORE CRACKERS and SUPPLIERS on FAST LINES so he who feels called upon, dont hesitate to CONTACT us.
If you are living in the EAST COAST and have Cable/Better, contact us Now.

CD UPDATE

We are doing monthly compilations, and collections as well as full games on CD(ISO), PSX CD's, DAT's and now also VIDEO CD's.
For info on any of the above, or anything else email xxx@xxxgods.com with your questions.

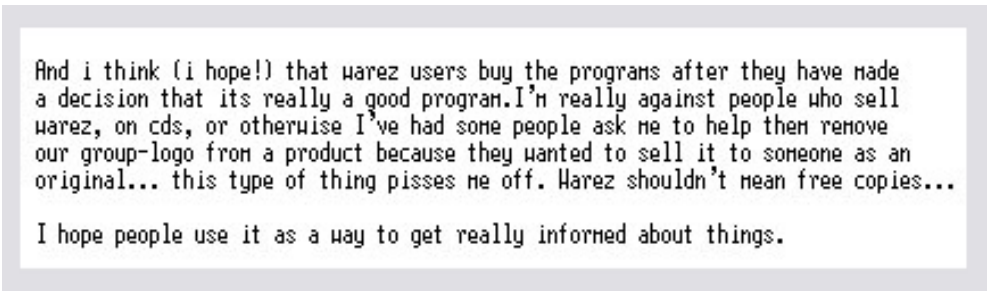
WE ARE IN NO NEED OF ANY COURIERS

So, You're Interested in becoming a Member.

If you fall within any of the following categories, you might just be what we're looking for: (All COSTS are reimbursed ofcourse!)

Abbildung 46 – Auszug aus einer NFO-Datei

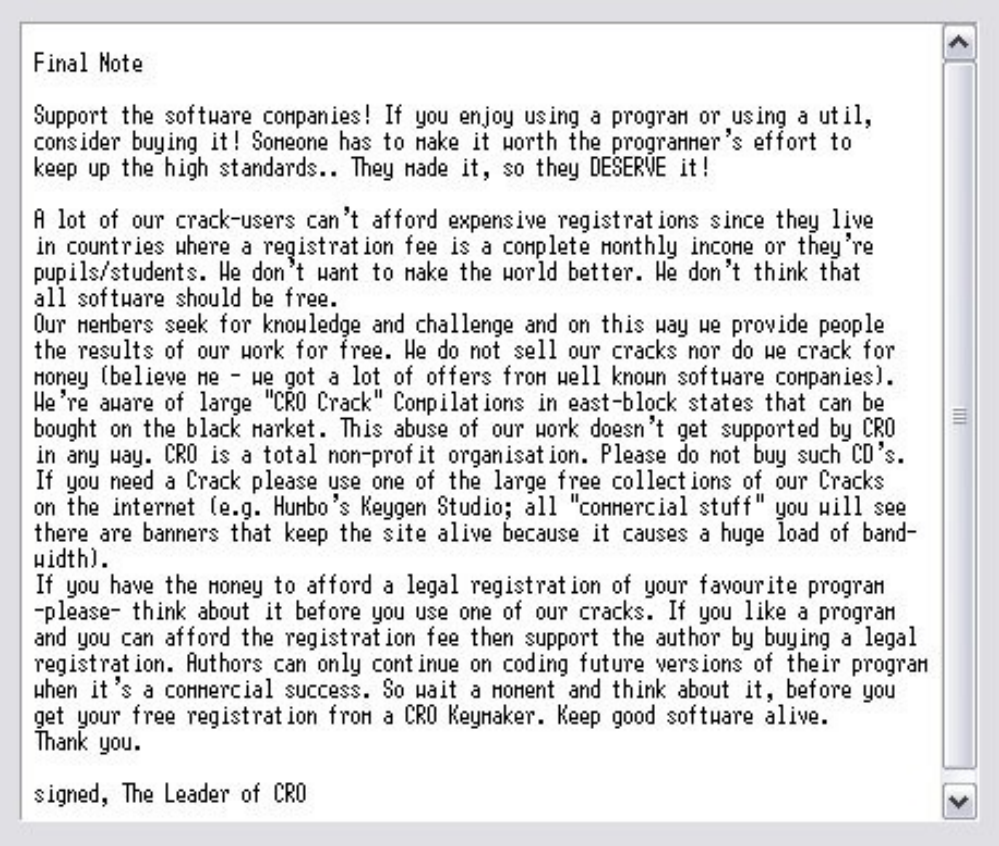
In der überwiegenden Zahl der Fälle wird das Verhalten von Profit-Pirates verurteilt und sogar zum rechtmäßigen Kauf von Software aufgefordert, sofern man diese häufig benutzen sollte.


And i think (i hope!) that warez users buy the programs after they have made a decision that its really a good program.I'm really against people who sell warez, on cds, or otherwise I've had some people ask me to help them remove our group-logo from a product because they wanted to sell it to someone as an original... this type of thing pisses me off. Warez shouldn't mean free copies...

I hope people use it as a way to get really informed about things.

Abbildung 47 – Auszug aus einer NFO-Datei

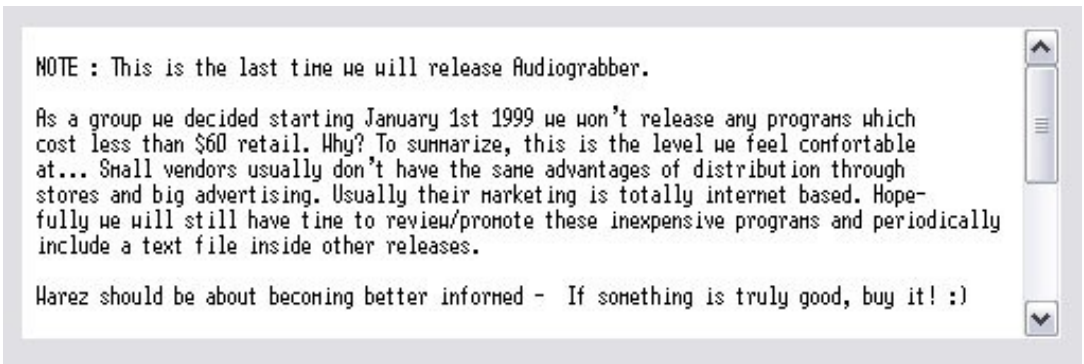
[186] Zur Methodik siehe Teil 1, F.



```
Final Note

Support the software companies! If you enjoy using a program or using a util,
consider buying it! Someone has to make it worth the programmer's effort to
keep up the high standards.. They made it, so they DESERVE it!

A lot of our crack-users can't afford expensive registrations since they live
in countries where a registration fee is a complete monthly income or they're
pupils/students. We don't want to make the world better. We don't think that
all software should be free.
Our members seek for knowledge and challenge and on this way we provide people
the results of our work for free. We do not sell our cracks nor do we crack for
money (believe me - we got a lot of offers from well known software companies).
We're aware of large "CRO Crack" Compilations in east-block states that can be
bought on the black market. This abuse of our work doesn't get supported by CRO
in any way. CRO is a total non-profit organisation. Please do not buy such CD's.
If you need a Crack please use one of the large free collections of our Cracks
on the internet (e.g. Humbo's Keygen Studio; all "commercial stuff" you will see
there are banners that keep the site alive because it causes a huge load of band-
width).
If you have the money to afford a legal registration of your favourite program
-please- think about it before you use one of our cracks. If you like a program
and you can afford the registration fee then support the author by buying a legal
registration. Authors can only continue on coding future versions of their program
when it's a commercial success. So wait a moment and think about it, before you
get your free registration from a CRO Keymaker. Keep good software alive.
Thank you.

signed, The Leader of CRO
```

Abbildung 48 – Auszug aus einer NFO-Datei

Einzelne Gruppen haben sich sogar dafür entschieden, keine Programme mehr zu veröffentlichen, die einen gewissen Verkaufspreis unterschreiten:



```
NOTE : This is the last time we will release Audiograbber.

As a group we decided starting January 1st 1999 we won't release any programs which
cost less than $60 retail. Why? To summarize, this is the level we feel comfortable
at... Small vendors usually don't have the same advantages of distribution through
stores and big advertising. Usually their marketing is totally internet based. Hope-
fully we will still have time to review/promote these inexpensive programs and periodically
include a text file inside other releases.

Warez should be about becoming better informed -  If something is truly good, buy it! :)
```

Abbildung 49 – Auszug aus einer NFO-Datei

Diese moralisch-ethischen Hinweise einzelner Gruppen ändern selbstverständlich nichts an der Tatsache, dass Profit-Pirates die Releases für kommerzielle Zwecke nutzen. Allerdings ist anzumerken, dass die Äußerungen der Gruppenmitglieder dazu beitragen, dass der Handel mit Raubkopien vom überwiegenden Teil der Szene nicht toleriert wird.

Zwischen den einzelnen Warez-Gruppen besteht ein fortwährender Wettstreit darüber, wer als erster eine lauffähige Version eines aktuellen Programms veröffentlicht.

Der Ruf einer Gruppe innerhalb der Szene ist für ihre Mitglieder außerordentlich wichtig. Gruppen, die schlechte Cracks veröffentlichen, laufen Gefahr, von konkurrierenden Gruppen in deren NFO-Dateien verspottet zu werden.[187] Um nicht als unprofessionell zu gelten, versuchen sie stets, zu verhindern, dass jemand nach einem mehrstündigen Download eine schlecht gecrackte Software bekommt. Der Mythos des „bad crack", der angeblich 1992 nach dem fehlerhaften Crack von *Autodesks 3D Studio* geboren wurde, ist seither Schrecken jeder Gruppe und wohl auch der Grund dafür, dass sämtliche Programme vor ihrer Veröffentlichung ausführlich beta-getestet werden.[188]

Je schwerer Programme zu cracken sind, um so spektakulärere Trophäen stellen sie dar.[189] Immer wieder rühmen sich Gruppen in NFO-Dateien mit der Überwindung eines als „uncrackbar" geltenden Kopierschutzes. Insbesondere das Cracken von donglegeschützten Programmen mehrt den Ruhm einer Gruppe außerordentlich.

Personen, die für den Erhalt der Szene arbeiten und aufgrund überlegenen Wissens ein hohes Ansehen genießen, werden als „Elite" oder „leet" bezeichnet. Das Gegenteil der Elite sind die sogenannten Lamer[190]. Ein Lamer ist eine Person, die einen naiven und ahnungslosen Eindruck vermittelt. Lamer ist ein gerne benutztes Schimpfwort in der Szene, und es wird häufig im Zusammenhang mit „unprofessionellem" Verhalten konkurrierender Warez-Gruppen gebraucht. Als besonders „lame" gilt es, Cracks anderer Gruppen zu stehlen und als eigene Cracks zu veröffentlichen. Das Anprangern und Verspotten anderer wird im Netz generell als „flaming" bezeichnet.

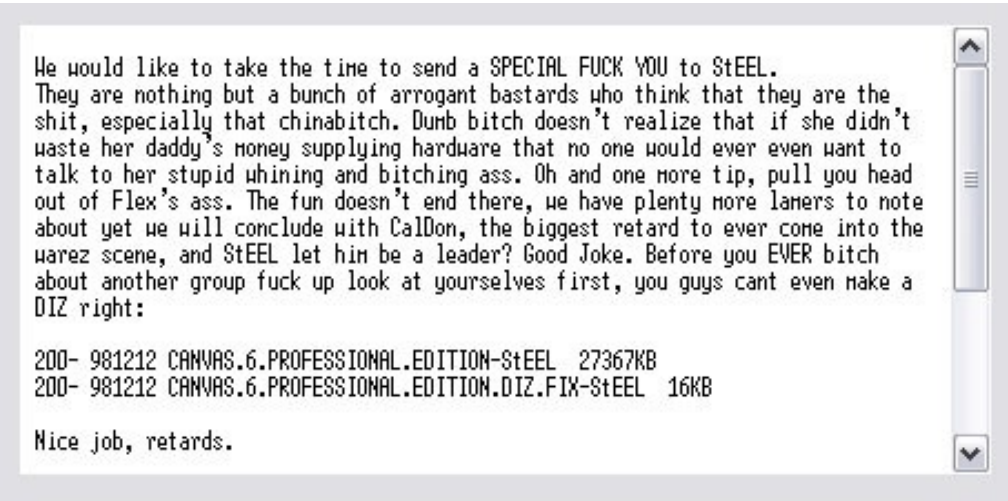
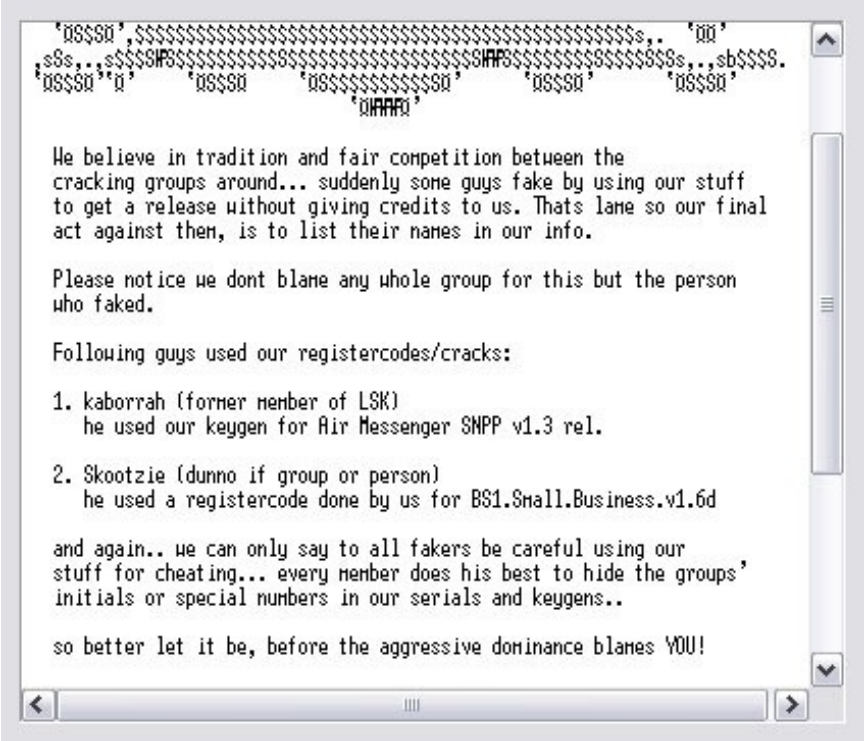


Abbildung 50 – Auszug aus einer NFO-Datei

---

187 *Kürten*, **PC-Intern** 8/1999, S. 33.
188 *McCandless*, **Wired Magazine** 5.04 – April 1997; siehe oben Teil 2, A. IV. 3.
189 *McCandless*, **Wired Magazine** 5.04 – April 1997.
190 Lamer (engl.) = Lahmer, Gelähmter.



```
  'QSSSQ',$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$s,.  'QQ'
,sSs,.,s$$$$SP$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$s,.,sb$$$$.
'QS$SQ''Q'    'QS$SQ     'QS$$$$$$$$$$$$$Q'     'QS$SQ'      'QS$SQ'
                          'QPPPQ'

We believe in tradition and fair competition between the
cracking groups around... suddenly some guys fake by using our stuff
to get a release without giving credits to us. Thats lame so our final
act against them, is to list their names in our info.

Please notice we dont blame any whole group for this but the person
who faked.

Following guys used our registercodes/cracks:

1. kaborrah (former member of LSK)
   he used our keygen for Air Messenger SNPP v1.3 rel.

2. Skootzie (dunno if group or person)
   he used a registercode done by us for BS1.Small.Business.v1.6d

and again.. we can only say to all fakers be careful using our
stuff for cheating... every member does his best to hide the groups'
initials or special numbers in our serials and keygens..

so better let it be, before the aggressive dominance blames YOU!
```

Abbildung 51 – Auszug aus einer NFO-Datei

Gruppenmitglieder werden in der Szene wie Popstars verehrt.[191] Einen besonders hohen Status nehmen Leader und Cracker ein, deren Image vornehmlich durch die Inhalte von NFO-Dateien geprägt ist. Die Beliebtheit der Mitglieder ist unter anderem durch einen Umstand bedingt, den man als „Robin-Hood-Phänomen" bezeichnen kann: Nach Ansicht vieler Szenemitglieder nehmen die Gruppen den reichen Softwarekonzernen etwas weg und geben es den „armen" Computernutzern.

Für die meisten Anhänger der Szene ist die Mitgliedschaft in einer der Warez-Gruppen das ultimative Ziel. Zum einen würden sie ebenfalls ein hohes Maß an Anerkennung erlangen, da sie für die vermeintlich Guten arbeiten, und zum anderem würden sie direkt „an der Quelle" sitzen.

In jedem Internet-Dienst, den die Warez-Szene für ihre Zwecke nutzt, haben sich eigene Verhaltensregeln etabliert. Im UseNet gilt beispielsweise Crossposting als „lame" Verhaltensweise. Crossposting bedeutet das mehrfache (parallele) Veröffentlichen eines Newsartikels in verschiedenen Newsgroups. Auch in IRC-Channels gelten gewisse Verhaltensregeln: So wird es in vielen Channels nicht gern gesehen, wenn offen nach FTP-Servern oder Webseiten gebettelt wird. Auch das Bekanntgeben von Downloadmöglichkeiten ist verpönt, sofern der Bekanntgebende diese nicht selbst geschaffen hat.

Die grundlegende Sprache der Warez-Szene ist Englisch. Allerdings hat sich in Teilen der Szene ein eigenständiger Jargon entwickelt, der vor allem von den jüngeren Szenemitgliedern verwendet wird. Da die überwiegende Internet-Kommunikation in Schriftform geführt wird, fällt vor allem die

---

[191] *McCandless* spricht von „Warez Gods", **Wired Magazine** 5.04 – April 1997.

Schreibweise dieser eigenen Sprache auf: Z wird anstelle von S benutzt, K anstelle von C, PH anstelle von F und J anstelle von G. Auch erfolgt eine willkürliche Groß- und Kleinschreibung („i'M MajiK SkuLLz, KinG oF ThE FileZ").[192] Worte wie Appz, Gamez, Serialz und Crackz sind feste Bestandteile des Szene-Wortschatzes. Hinzu kommen die bereits erwähnten Emoticons, anhand derer der Schreibende seine Gefühle mit kurzen Zeichenfolgen ausdrücken kann.

An den Logos der Gruppen, die meist als „Briefköpfe" in den NFO-Dateien fungieren, kann man erkennen, dass die Szene auch von der Graffiti-Kultur der frühen 80er Jahre beeinflusst ist. Diese in sogenannter ASCII-Art erstellten Schriftzüge und Gebilde bestehen meist aus Tastatur-Sonderzeichen und sollen den Wiedererkennungswert einer Gruppe erhöhen und ein gewisses Image erzeugen.

Grundsätzlich finden sich bei Warez-Gruppen auch Parallelen zu Hacker-Gruppen – vor allem, was den Status der Mitglieder, deren Kodex und typische Gruppenmechanismen anbelangt.[193]

2. Täterkreis

Die Mitglieder der Warez-Szene sind schätzungsweise zwischen 12 und 60 Jahren alt, wobei der größte Teil im Bereich zwischen 20 und 35 Jahren anzusiedeln ist.[194] Dies gilt insbesondere für Gruppenmitglieder, denn selten haben sich jüngere Computernutzer das erforderliche Know-how angeeignet. Die jüngeren Raubkopierer wird man eher in der Gamez-Szene finden. Die Quote der männlichen Täter überragt die der weiblichen deutlich. Einer Einschätzung des Verfassers zufolge sind in der Szene über 95% Männer vertreten[195]. Diese Beobachtungen decken sich weitgehend mit den Erkenntnissen aus den polizeilichen Kriminalstatistiken der letzten Jahre zur Softwarepiraterie in Deutschland:

Schlüssel	***Straftaten(-gruppen)***	***Tatverdächtige***						
		Insges. (100%)	männl.	weibl.	Kinder (< 14)	Jugendl. (14 – 18)	Heranw. (18 – 21)	Erwachsene (21 & älter)
			(in %)					
7151	Softwarepiraterie (private Anwendung)	330	95,5	4,5	0,3	10,0	9,4	80,3
7152	Softwarepiraterie (in Form gewerbsmässigen Handelns)	212	92,5	7,5	0,0	4,2	4,7	91,0

Abbildung 52 – Auszug aus der PKS 1998[196] – Geschlechts- und Altersstruktur im Bereich der Softwarepiraterie (Bereich: Bundesgebiet insgesamt)

---

192 Vgl. *Pogue,* **Macworld.com**, Oktober 1997.
193 Auch im Slang der beiden Szenen gibt es Parallelen, vgl. *Slatalla/Quittner*, **Wired Magazine** 2.12 – Dezember 1994.
194 Vgl. hierzu *McCandless*, **Wired Magazine** 5.04 – April 1997.
195 Siehe hierzu Teil 1, F.
196 Veröffentlicht auf der Webseite des *BKA*, http://www.bka.de/pks/pks1998/index2.html.

Schlüssel	*Straftaten(-gruppen)*	*Tatverdächtige*						
		Insges. (100%)	männl.	weibl.	Kinder (< 14)	Jugendl. (14 – 18)	Heranw. (18 – 21)	Erwachsene (21 & älter)
			(in %)					
7151	Softwarepiraterie (private Anwendung)	542	93,9	6,1	1,7	16,1	14,4	67,9
7152	Softwarepiraterie (in Form gewerbsmäs-sigen Handelns)	338	91,7	8,3	0,0	5,0	10,4	86,4

Abbildung 53 – Auszug aus der PKS 1999[197] – Geschlechts- und Altersstruktur im Bereich der Softwarepiraterie (Bereich: Bundesgebiet insgesamt)

Schlüssel	*Straftaten(-gruppen)*	*Tatverdächtige*						
		Insges. (100%)	männl.	weibl.	Kinder (< 14)	Jugendl. (14 – 18)	Heranw. (18 – 21)	Erwachsene (21 & älter)
			(in %)					
7151	Softwarepiraterie (private Anwendung)	708	94,6	5,4	1,7	16,4	17,1	64,8
7152	Softwarepiraterie (in Form gewerbsmäs-sigen Handelns)	277	94,2	5,8	0,0	5,0	9,0	81,9

Abbildung 54 – Auszug aus der PKS 2000[198] – Geschlechts- und Altersstruktur im Bereich der Softwarepiraterie (Bereich: Bundesgebiet insgesamt)

Schlüssel	*Straftaten(-gruppen)*	*Tatverdächtige*						
		Insges. (100%)	männl.	weibl.	Kinder (< 14)	Jugendl. (14 – 18)	Heranw. (18 – 21)	Erwachsene (21 & älter)
			(in %)					
7151	Softwarepiraterie (private Anwendung)	793	94,3	5,7	0,6	16,4	15,9	67,1
7152	Softwarepiraterie (in Form gewerbsmäs-sigen Handelns)	234	95,3	4,7	0,0	9,4	4,3	86,3

Abbildung 55 – Auszug aus der PKS 2001[199] – Geschlechts- und Altersstruktur im Bereich der Softwarepiraterie (Bereich: Bundesgebiet insgesamt)

---

[197] Veröffentlicht auf der Webseite des *BKA*, http://www.bka.de/pks/pks1999/index2.html.
[198] Veröffentlicht auf der Webseite des *BKA*, http://www.bka.de/pks/pks2000/index2.html.
[199] Veröffentlicht auf der Webseite des *BKA*, http://www.bka.de/pks/pks2001/index2.html.

Schlüssel	Straftaten(-gruppen)	Tatverdächtige						
		Insges. (100%)	männl.	weibl.	Kinder (< 14)	Jugendl. (14 – 18)	Heranw. (18 – 21)	Erwachsene (21 & älter)
			(in %)					
7151	Softwarepiraterie (private Anwendung)	1039	91,6	8,4	1,2	10,7	9,5	78,6
7152	Softwarepiraterie (in Form gewerbsmäs-sigen Handelns)	443	88,9	11,1	0,2	10,4	9,3	80,1

Abbildung 56 – Auszug aus der PKS 2002[200] – Geschlechts- und Altersstruktur im Bereich der Softwarepiraterie (Bereich: Bundesgebiet insgesamt)

Dennoch scheint es auch Gruppen zu geben, deren Führungsriege ausschließlich aus Frauen besteht:

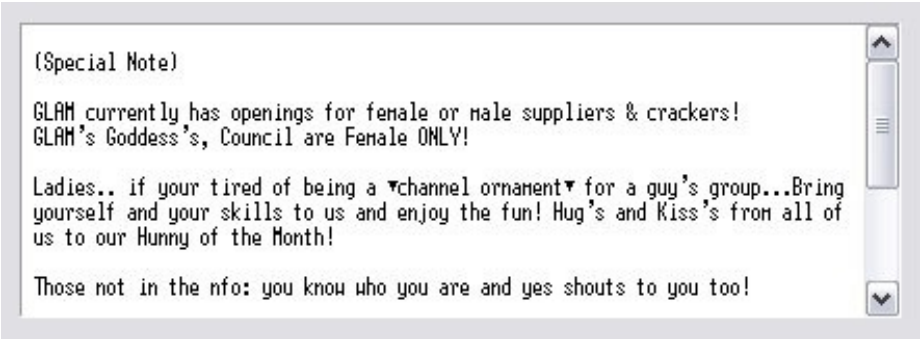


Abbildung 57 – Auszug aus einer NFO-Datei

Allerdings ist zu bezweifeln, dass es sich tatsächlich um weibliche Täter handelt. Im Internet – besonders im IRC – kommt es nicht selten vor, dass sich zumeist homophile Männer mit einer weiblichen Identität versehen. Die Psychologen sprechen in diesem Zusammenhang vom Phänomen des Gender-Swapping[201]. Eine Nachprüfbarkeit ist beinahe ausgeschlossen, weshalb zahlreiche Nutzer dauerhaft eine Scheinidentität aufrechterhalten können.

Die Herkunft der Täter ist in erster Linie auf Staaten begrenzt, in denen Computernetze und Rechner der Bevölkerung zugänglich sind. Dabei handelt sich vornehmlich um Industriestaaten.

Vergleichbar mit anderen Computerdelikten erfordert die Aktivität in der Warez-Szene eine bestimmte Anpassungsfähigkeit, entsprechendes Know-how und ein gewisses Mindestmaß an Intelligenz. Angesichts des mittlerweile erreichten technologischen Standards, der schnellen und allgemeinen Verfügbarkeit technischer Grundvoraussetzungen sowie deren leichter Handhabung

---

[200] Veröffentlicht auf der Webseite des *BKA*, http://www.bka.de/pks/pks2002/index2.html.
[201] Vgl. *Suler*, Rider.edu.

sind die Hürden jedoch nicht allzu hoch gesteckt.[202] Dies gilt allerdings nur eingeschränkt für die Mitglieder von Warez-Gruppen: Bei Crackern wird es sich in der Regel um überdurchschnittlich intelligente Täter mit hohem technischem Know-how handeln. Auch die Personen, die koordinative Funktionen übernehmen, zeichnen sich in der Regel durch hohe Flexibilität und überdurchschnittliches Organisationsvermögen aus.

Bei den meisten Gruppenmitgliedern handelt es sich um gutsituierte, weiße Männer mit geregeltem Berufs- und Familienleben[203], die häufig beruflich im Computerbereich tätig sind. Gerüchten zufolge sollen viele Cracker im realen Leben als Programmierer – also auch „für die andere Seite" – arbeiten. Diese Gerüchte erscheinen keinesfalls abwegig, denn gerade gute Cracker besitzen Fähigkeiten, die auf dem Arbeitsmarkt äußerst gesucht sind und zudem vortrefflich entlohnt werden. Bei den meisten Softwarepiraten dürfte es sich außerdem um gewaltlose und sozial unauffällige Täter handeln.[204]

3. Tätermotivation

Die in Warez-Gruppen zusammengeschlossenen Täter handeln vorrangig mit dem Ziel, Anerkennung und Selbstbestätigung zu erlangen.[205] Die veröffentlichte Software kann im Grunde mit einem Geschenk verglichen werden, das Zeugnis für die Stärke und das mächtige Erscheinungsbild des Gebers ablegen soll.[206] Die Bewunderung, die den Aktivisten der Warez-Szene von Mitstreitern und Anhängern entgegengebracht wird, kann ihnen helfen, Minderwertigkeitsgefühle und sonstige Defizite zu kompensieren. Das Selbstwertgefühl wird in besonderem Maße erhöht, wenn ihnen andere Gruppen oder Cracker Respekt („Kudos") zollen.[207]

Viele Szenemitglieder genießen auch das Gefühl, etwas sehr Exklusives und Elitäres zu tun. Menschen außerhalb der Szene müssen oft einige Wochen länger warten, bis eine Software auf dem legalen Markt erscheint, und sie können erst recht nicht jedes erhältliche Programm ausprobieren, da es ihre finanziellen Mittel übersteigen würde.

```
I love getting my hands on some new game that everyone has been hyping
and giving it a run, or having someone say to me, 'Man, did you see that
game? It looks real cool - I can't wait till it comes out,' and being
able to reply, 'Yeah, I have it, but it's not that great.'
```

Abbildung 58 – Auszug aus einem Interview mit einem Mitglied einer Warez-Gruppe

---

202 Vgl. *Harbort*, **Kriminalistik** 1996, S. 197 und *Vassilaki*, Multimediale Kriminalität, **CR** 1997, S. 299, der von „Massenkriminalität" spricht.
203 Vgl. hierzu *McCandless*, **Wired Magazine** 5.04 – April 1997.
204 *Vassilaki*, Multimediale Kriminalität, **CR** 1997, S. 300.
205 Oftmals ist auch von „Fame" – (engl.) = Ruhm – die Rede. In diesem Zusammenhang sei auf die Thesen *Goldhabers* verwiesen, der das Modell der „Attention Economy" entwickelt hat. *Goldhaber* geht davon aus, dass Geld und materielle Güter in der „neuen Ökonomie" des Internet ihre zentrale Rolle verlieren werden, und sich stattdessen eine „Aufmerksamkeitsökonomie" entwickelt – vgl. *Sietmann*, Goldhaber-Interview, **c't** 13/2000, S. 52 f.
206 *McCandless*, **Wired Magazine** 5.04 – April 1997.
207 *Kürten*, **PC-Intern** 8/1999, S. 33.

Die „echten Programmknacker“ wollen sich in der Regel nicht selbst bereichern. Sie behaupten, dass einzig und allein das Cracken des Programms für sie zähle. Man kann die Situation am ehesten mit einem sportlichen Wettbewerb vergleichen: Die Gegner sind sowohl die hochbezahlten Programmierer der Softwarehersteller, die sich alles Erdenkliche einfallen lassen, um ihre Programme vor dem Zugriff von Softwarepiraten zu schützen[208], als auch die Cracker der anderen Gruppen. In den bereits dargestellten Regeln der Szene kommt deutlich zum Ausdruck, dass die Gruppen mit sportlichem Ehrgeiz wetteifern. Von nicht zu unterschätzender Bedeutung ist hierbei der Umstand, dass der Wettbewerb zwischen den Gruppen durch das Internet einen globalen Charakter erhält. Jeden Tag und mit jedem neuen Release werden „Weltmeisterschaften“ ausgetragen. Derjenige, der es als erster schafft, das entsprechende Programm zu cracken, kann sich rühmen, dass es auf der ganzen Welt keine andere Person gibt, die ihm zuvorgekommen ist.

Die technische Herausforderung, das sogenannte Challenge-Motiv, ist in der Regel gepaart mit dem Interesse an teurer Software und einem lang währenden Computerhobby.[209]

Ein Vermögensvorteil ist bei großen Teilen der Szene nicht mehr grundsätzlich Ziel der Tat.[210] Zwar erhalten die Gruppenmitglieder die gecrackte Software zu ihrer Verfügung, allerdings verdienen sie nichts an der Verbreitung der Programme. Insoweit kann zu Recht von einem kriminologischen Phänomen gesprochen werden.[211] Hiervon ausgenommen sind freilich Personen, für die eine Raubkopie ein Substitut für den Erwerb eines Originalprogramms darstellt, da sie lediglich das Geld für die Anschaffung einer lizenzierten Kopie sparen wollen. Erst recht ausgenommen sind Profit-Pirates, die mit Bereicherungsabsicht handeln und möglichst viel Geld mit dem Verkauf von Raubkopien verdienen möchten. Ähnliche Interessen haben auch die Betreiber von Webseiten, sofern sie Bannerwerbung auf ihren Seiten platzieren oder Kaufangebote für Raubkopien unterbreiten.

Ein weiteres Motiv für die Beschaffung von Raubkopien liegt in der bei vielen Menschen ausgeprägten Sammelleidenschaft. Ihnen geht es in erster Linie um die Freude an Komplettieren und Besitzen. Kaum ein richtiger Sammler kennt all die Programme, die er sich aus dem Internet heruntergeladen hat, denn der größte Teil wird niemals auf seinem Rechner installiert werden.[212] Die Festplatten und CD-ROMs dieser Leute gleichen Briefmarkenalben. Sie sind vollgestopft mit Programmen, die nur zur Ansicht und Triebbefriedigung dienen.[213]

Nicht nur im Zusammenhang mit der gesteigerten Sammelleidenschaft einzelner Nutzer kann von zwanghaftem Internet-Nutzungsverhalten gesprochen werden. Zwar ist die Einordnung des häufig

---

[208] *Schultz*, S. 117, 124.
[209] *Schultz*, S. 123.
[210] *Vassilaki*, Multimediale Kriminalität, **CR** 1997, S. 298; siehe oben Teil 2, A. VIII 1. und 3.
[211] Wie bereits ausführlich beschrieben wurde, hat die Szene ein aufwändiges und nach betriebswirtschaftlichen Gesichtspunkten optimiertes System zur Herstellung und weltweiten Distribution von Raubkopien entwickelt. Typischerweise wäre zu erwarten, dass der hohe zeitliche und logistische Aufwand sowie das ständige Entdeckungsrisiko nur in Kauf genommen würden, um eine monetäre Gegenleistung zu erhalten.
[212] Vgl. *Pogue*, **Macworld.com**, Oktober 1997.
[213] *McCandless*, **Wired Magazine** 5.04 – April 1997.

mit „Online-“ oder „Internetsucht“ bezeichneten Phänomens[214] als Krankheit (Internet Addiction Disorder – IDA) in Fachkreisen umstritten[215], dennoch ist davon auszugehen, dass es verschiedene Arten von pathologischem Internetgebrauch gibt[216].

Die US-Psychologin *Kimberley Young*, die zu den führenden Vertretern der „Sucht-Theorie“ gehört, unterscheidet fünf Erscheinungsformen von Internet-Abhängigkeit[217]:

- cybersexuelle Abhängigkeit
- Abhängigkeit nach Online-Beziehungen /-kontakten
- Abhängigkeit nach Online-Gaming / -Shopping / -Gambling etc.
- Informationssucht
- Computersucht

Nach *Young* sei die Hälfte aller Internetsüchtigen bereits in der Vergangenheit drogen- oder alkoholabhängig gewesen. Die Palette der Süchtigen reiche vom 13-jährigen Teenager bis zum 70-jährigen Rentner, wobei Frauen etwas häufiger betroffen sein sollen als Männer und auf der Suche nach einer virtuellen Partnerschaft zahllose Stunden in Chaträumen und auf Kontakt-Webseiten verbringen. Männer seien eher an Videospielen und pornographischen Webseiten interessiert.[218]

Fragt man nach den grundlegenden Ursachen für eine zwanghafte Internetnutzung, erscheint vor allem der folgende Erklärungsansatz nachvollziehbar:

Der Cyberspace verhilft labilen Charakteren zur Flucht aus unbequemen realen Lebenssituationen. Diese Pseudoauthentizität im virtuellen Raum kann Stimulans sein und Sedativum, zu Suchteffekten und Realitätsverschiebung führen. Je perfekter sich künstliche Welten präsentieren, desto größer wird die Gefahr des Wirklichkeitsverlusts; labile Charaktere können sich im Cyberspace verlieren.[219]

---

214 Siehe hierzu *Hahn/Jerusalem*, die „Internetsucht oder Internetabhängigkeit als eine stoffungebundene Abhängigkeit“ definieren, „die dann als vorhanden gilt, wenn: 1. über längere Zeitspannen der größte Teil des Tageszeitbudgets zur Internetnutzung verausgabt wird (Einengung des Verhaltensraums), 2. die Person die Kontrolle über ihre Internetnutzung weitgehend verloren hat bzw. Versuche, das Nutzungsausmaß zu reduzieren oder die Nutzung zu unterbrechen, erfolglos bleiben oder erst gar nicht unternommen werden – obwohl das Bewusstsein für dadurch verursachte persönliche oder soziale Probleme vorhanden ist (Kontrollverlust), 3. im zeitlichen Verlauf eine Toleranzentwicklung zu beobachten ist, d.h. die „Verhaltensdosis“ zur Erreichung der angezielten positiven Stimmungslage gesteigert werden musste, 4. Entzugserscheinungen als Beeinträchtigungen psychischer Befindlichkeit (Unruhe, Nervosität, Unzufrie-denheit, Gereiztheit, Aggressivität) und psychisches Verlangen („craving“) nach der Internetnutzung als Folge zeitweiliger, längerer Unterbrechung der Internetnutzung auftreten, 5. wegen der Internetaktivitäten negative soziale Konsequenzen in den Bereichen Arbeit und Leistung sowie soziale Beziehungen (z.B. Ärger mit Freunden oder Arbeitgeber) eingetreten sind.“

215 Vgl. *Eichenberg/Ott*, **c't** 19/1999, S. 106 ff.

216 Die bislang veröffentlichten wissenschaftlichen Studien kommen zu den Ergebnissen, dass zwischen 3 und 12,7% aller Internetnutzer von einer Abhängigkeit betroffen sind, vgl. *Zimmerl*, m.w.N., wobei zu beachten ist, dass der hohe Wert aus einer Studie stammt, die sich auf den Online-Chat beschränkte. Die übrigen Studien kommen im Mittel auf einen Prozentsatz von 4,53, was sich mit den Ergebnissen der Beobachtungen und Befragungen des Verfassers deckt, vgl. hierzu Teil 1, F. (Methodik).

217 Vgl. http://netaddiction.com/whatis.htm.

218 Vgl. das Interview mit *Young*, in **FOCUS** 10/1999, 204.

219 Interview mit *Bonfadelli*, **FOCUS** 7/1999, S. 196 f.

Weitere Umstände, die Katalysatoren für eine Suchtentwicklung sein können, sind Langeweile, soziale Isolation sowie eine allgemeine Faszination für das „Paralleluniversum Internet“[220]. Auch die weitgehende Anonymität der Internetnutzer begünstigt eine Abhängigkeit: In den körperlosen Chatrooms und Newsgroups ist niemand alt oder hässlich, niemand hat zu exzentrische Interessen, als dass sich nicht Gleichgesinnte finden ließen. Die virtuelle Welt verlockt dazu, in immer neue Identitäten zu schlüpfen. Körperlich behinderte Menschen können sich als Topsportler ausgeben, und Farbige können im Cyberspace ein Leben als Weiße führen und umgekehrt. In der virtuellen Welt fühlt sich jeder kompetent, wichtig und produktiv.[221] Der Schutzschild der Anonymität vermag außerdem zu enthemmen. Nutzer können ungesühnt mit den Verhaltensweisen ihres realen Lebens brechen. Sie können beispielsweise leicht in den Besitz pornographischer Darstellungen gelangen, ohne einen schmuddeligen Sexshop zu betreten oder die prüfenden Blicke der Supermarkt-Kassiererin ertragen zu müssen.[222]

Auch das innerhalb der Warez-Szene beobachtete, zwanghaft erscheinende Verhalten zahlreicher Nutzer deutet darauf hin, dass es unterschiedliche Ursachen für deren außergewöhnlich intensive Online-Nutzung gibt. So kann man bei zahlreichen Gruppenmitgliedern tatsächlich eine Abhängigkeit nach Online-Beziehungen bzw. -kontakten feststellen. Typische Gruppenmechanismen - vor allem Zusammengehörigkeitsgefühl und Gruppenzwang - das Gefühl, einem Geheimbund anzugehören und der Reiz, etwas Verbotenes zu tun, sind Faktoren, die zweifellos eine derartige Abhängigkeit begünstigen.

Von einer Computersucht im weiteren Sinne kann man sprechen, wenn das Cracken selbst zur Obsession geworden ist: Cracker berichten häufig, dass sie nicht eher vom Computer lassen können, bis ein Programm vollständig vom Kopierschutz befreit ist.

Auch fühlen sich zahlreiche Warez-Sammler unbefriedigt, wenn sie nicht mindestens ein neues Programm pro Tag herunterladen können. Immer wieder trifft man Nutzer im IRC an, die nach einer bestimmten Datei betteln, um endlich ihre Sammlung vervollständigen zu können.[223] Viele Softwarepiraten überschreiten sogar eine wöchentliche Online-Zeit von 60 Stunden. Sie verbringen jede freie Minute vor dem Rechner, der meist als FTP-Server rund um die Uhr mit dem Internet verbunden ist.

Von vielen „Netaholics“ wird die eigene Abhängigkeit gar nicht erkannt. In der Warez-Szene mag dies vor allem daran liegen, dass ein Leben als „Otaku“ als äußerst erstrebenswert gilt. Die Bezeichnung Otaku erhalten in Japan vornehmlich junge Männer, die einer Technikobsession verfallen sind und die meiste Zeit ihres Lebens mit Computern und Spielekonsolen verbringen. Ein echter Otaku zeichnet sich dadurch aus, dass er die Computersysteme beherrscht, mit denen er sich

---

220 Vgl. *McCandless*, **Wired Magazine** 5.04 – April 1997 und *Harbort*, **Kriminalistik** 1996, S. 194, der von einer „virtuellen Parallelwelt“ spricht.
221 Vgl. *Shaffer*, bei *Wrede*, **FirstSurf** vom 15.09.1997.
222 Vgl. *Engel*, **AfP** 1996, S. 220. Die vom Datennetz ausgehende Anonymität ist es auch, die die Täter in Verbindung mit der Leichtigkeit der Tatbegehung zur Tatwiederholung verleitet, *Vassilaki*, Multimediale Kriminalität, **CR** 1997, S. 299.
223 Vgl. *McCandless*, **Wired Magazine** 5.04 – April 1997.

beschäftigt.[224] Anders als im abendländischen Kulturkreis werden Otakus in Asien verehrt und genießen ein hohes gesellschaftliches Ansehen.

Typisch für beinahe alle Täter ist ein fehlendes oder kaum vorhandenes Unrechtsbewusstsein.[225] Software wird von weiten Teilen der Internet-Gemeinde als Allgemeingut angesehen. In den Köpfen der Täter sind verschiedenartigste Neutralisierungsmechanismen aktiv, mit denen sie ihre Taten rechtfertigen:[226]

Viele Internetnutzer haben aufgrund ihrer anarchistischen Grundeinstellung große Konzerne als Feindbild. Sie sehen es nicht als verwerflich an, die vermeintlichen Ausbeuter um ein paar Kopien ihrer Produkte zu erleichtern. Für sie ist es ein Akt von gewaltlosem Terrorismus oder die simple Einstellung „Fuck You, *Microsoft*!".[227] Verstärkt wird der Unmut gegenüber großen Softwareherstellern durch diverse Verschwörungstheorien. In der Computerwelt kursiert beispielsweise das hartnäckige Gerücht, dass die wirklichen Erfinder und Verbreiter von Computerviren Softwarehersteller waren, die ihre Originalprogramme aufwerten wollten, indem sie die im Umlauf befindlichen Raubkopien mit Viren infizierten.[228] Auch werden Hersteller von Antiviren-Software als Schöpfer von Viren vermutet. Diese sollen gezielt solche Viren in Umlauf bringen, die nur mit den eigenen Programmen erfolgreich bekämpft werden können. Weit verbreitet ist darüber hinaus die Ansicht, dass die Softwarehersteller ihren Umsatz gar nicht mit dem Verkauf der Software selbst machen, sondern in erster Linie mit Schulungen, Wartungsverträgen und dem Verkauf bzw. der Lizenzierung von gedrucktem Begleitmaterial. Aus diesem Grund würde den Unternehmen durch Raubkopien kein nennenswerter Schaden zugefügt.

Als besonders unfair werden die Lizenzbestimmungen der Softwaredistributoren empfunden, wonach in der Regel ein Umtauschrecht ausgeschlossen ist. Die Konsumenten sind es gewohnt, dass sie die meisten Produkte, die man im Geschäft kauft, bei Unzufriedenheit zurückbringen kann. Dass dies bei Software nicht möglich ist, wird von vielen Computernutzern als Ärgernis angesehen.[229] Hohe Softwarepreise und mangelhafte Kundenbetreuung sind ebenfalls Argumente, die von Raubkopierern zur Legitimation ihrer Taten angeführt werden.[230]

Einer besonders naiven, jedoch häufig vertretenen Ansicht zufolge liegt im Kopieren von Software keine Wegnahme, weshalb für die Rechtsinhaber kein Anlass zur Klage über Softwarediebstahl bestünde.[231] Auf diese Fehlinterpretation der Vorzüge der Digitaltechnik braucht an dieser Stelle nicht näher eingegangen zu werden.

Besonders beliebt zur Rechtfertigung von Verstößen gegen das Urheberrecht waren vor Einführung der Flatrates die hohen, von der Nutzungsdauer abhängigen Onlinekosten. Vor allem in Deutschland

---

224 Vgl. *Kube*, **Kriminalistik** 1996, S. 624.
225 Vgl. *Eisenberg*, § 58, Rdnr. 67; *Zimmermann*, S. 29.
226 Welche der hier angeführten Überlegungen tatsächlich von Bedeutung sind, wird im weiteren Verlauf der Arbeit dargestellt – siehe Teil 2, B. II.
227 *McCandless*, **Wired Magazine** 5.04 – April 1997.
228 Vgl. *Schultz*, S. 126.
229 Vgl. *McCandless*, **Wired Magazine** 5.04 – April 1997.
230 Vgl. *Neumann*, **Wired Magazine** 3.10 – Oktober 1995.
231 Vgl. *Pogue*, **Macworld.com**, Oktober 1997.

mussten Internetnutzer tief in die Tasche greifen, um am Leben im globalen Dorf teilzunehmen.[232] Ein „Netaholic" hatte nicht selten monatliche Onlinekosten von über 1.000 DM (entspricht ca. 511 €) und war erst dann beruhigt, wenn er sich einen entsprechenden Gegenwert in Form von Software heruntergeladen hatte. Nach dem Motto „es ist doch egal, welchem Großkonzern ich mein Geld in den Rachen werfe – der *Telekom* oder *Microsoft*" – handeln auch heute noch viele Raubkopierer.

Nicht nur von Anhängern der Warez-Szene sondern auch von Softwareherstellern und Programmierern wird regelmäßig die Behauptung aufgestellt, dass die Hardware-Industrie ein starkes Interesse daran hat, dass es die Warez-Szene gibt. Demnach würden weit weniger Leute einen Computer kaufen, wenn sie jedes Programm legal erwerben müssten.[233] Denn um vernünftig mit einem Computer zu arbeiten, müsste ein Nutzer mindestens noch einmal so viel Geld für Software ausgeben.

Der bereits bei der Tätermotivation erwähnte Altruismus einzelner Gruppenmitglieder dient diesen auch als Neutralisierungsmechanismus. Die Behauptung, Software zu veröffentlichen, um „armen" Computerkids zu helfen, erscheint allerdings nicht besonders glaubwürdig, geht es doch in erster Linie um die Bewunderung und Dankbarkeit der Beschenkten, die die Gruppenmitglieder ernten wollen.[234]

Nach den Aussagen zahlreicher Gruppen profitieren Softwarehersteller von der in den NFO-Dateien betriebenen „Underground-Promotion". Eine gute Kritik einer Warez-Gruppe gelte als Gütesiegel für eine Software, denn kaum jemand kenne sich besser mit Software aus als die Warez-Experten. Darf man den Äußerungen eines Group-Leaders Glauben schenken, ist es tatsächlich schon vorgekommen, dass sich ein Softwarehersteller mit der Bitte an eine Gruppe gewandt hat, seine Software als Raubkopie zu veröffentlichen, um die Bekanntheit der Software zu erhöhen. Dieser Sachverhalt erscheint insoweit glaubwürdig, als sich der Wert einer Marke unter anderem nach ihrer Bekanntheit richtet. Gerade über das Internet ist eine internationale Bekanntheit leicht zu erlangen. Von dieser besonderen Art des Marketing machte auch der renommierte Softwarehersteller *Kaspersky Lab* Gebrauch, indem er auf seiner Webseite die NFO-Datei einer Crackergruppe veröffentlichte, in der eines seiner Anti-Virus-Programme äußerst positive Kritiken erhielt. Unter dem Motto „einer Empfehlung aus dem unbestechlichen Untergrund kann man getrost vertrauen" warb *Kaspersky Lab* für sein Produkt.

Vor allem Jugendliche argumentieren, dass sie sich die Software, die sie tauschen, niemals hätten leisten können und daher nie gekauft hätten.[235] Insofern sei das Tauschgeschäft kein Substitut für einen Kauf, und dem Hersteller sei somit kein Schaden entstanden. Ähnlich argumentieren auch solche Raubkopierer, die aus Sammelleidenschaft gecrackte Software aus dem Internet laden. Bei

---

[232] Nach der Veröffentlichung der Studie „Communications Outlook 1999" der *Organization for Economic Co-operation and Development (OECD)* wurde befürchtet, dass Deutschland wegen der hohen Zugangspreise den Anschluss an die Internet-Entwicklung verlieren könnte. In einem Vergleich der 29 *OECD*-Mitgliedsländer belegte Deutschland bei den Web-Zugriffskosten zur Hauptzeit (bis 20 Uhr) nur den 22. Platz und zur Nebenzeit sogar nur den 28. Platz, vgl. **FOCUS**, 17/1999, S. 164. Dieser Entwicklung wirken mittlerweile vor allem sogenannte Flatrate-Angebote entgegen; zum Begriff der Flatrate siehe Teil 1, C. II.

[233] Vgl. *Schultz*, S. 117.

[234] Vgl. *Schultz*, S. 124.

[235] Vgl. *Pogue*, **Macworld.com**, Oktober 1997.

ihnen handle es sich ebenfalls nicht um einen Ersatz für Originalsoftware, sondern um Prestigeobjekte, die sie nicht wirklich brauchen und für die sie niemals Geld ausgeben würden.

Eine andere Motivation haben Personen in den Ländern der sogenannten Dritten Welt. Meist haben diese kein Geld für Originalsoftware, so dass sie nur über Raubkopien mit den entsprechenden Programmen in Berührung kommen. Ähnliches berichten Computerfreaks aus der ehemaligen DDR: Durch Einfuhrverbote für westliche Produkte gelangten nur vereinzelt Exemplare der begehrten West-Software in den Osten, so dass eine weitere Verbreitung ausschließlich durch Raubkopien erfolgen konnte. Um kopiergeschützte Programme weitergeben zu können, begannen zahlreiche Computerbegeisterte mit dem Cracken. Viele von ihnen sollen mittlerweile in internationalen Warez-Gruppen tätig sein.

Eine vergleichbare Situation liegt noch heute in den anderen Ländern des ehemaligen Ostblocks vor.[236] Besonders in Russland gibt es zahlreiche Warez-Gruppen, die mit Hilfe des Internet weltweit agieren. Diese Gruppen sehen in Softwarepiraterie eine legitime Chance, den Anschluss an die etablierten – und oftmals wegen angeblicher Ausbeutung oder aus Neid gehassten – Industriestaaten nicht zu verlieren oder in der Entwicklung aufzuholen. In einem Interview berichtet ein chinesischer Cracker, dass er sich für den Fall, dass er von den Behörden ertappt werden sollte, eine schlagkräftige Ausrede zurechtgelegt habe: „Ich werde behaupten, dass ich die ausländischen Teufel schädige, um der Kommunistischen Partei zu helfen, Geld für den Erwerb ausländischer Hochtechnologie zu sparen".[237]

Die unterschiedlichen Jugendschutzbestimmungen der einzelnen Länder werden ebenfalls gerne herangezogen, um illegale Kopien von Computerspielen zu rechtfertigen. Denn die an den deutschen Markt angepassten Spezialversionen von indizierten Computerspielen sind in der Spielerszene äußerst unbeliebt. Existiert daneben noch eine „ungeschnittene" Originalfassung – meist aus den USA – schnellen die Zahlen von Raubkopien erfahrungsgemäß in die Höhe.[238]

B. Bedeutung und Schaden

I. Angaben über Fälle von (Internet-)Softwarepiraterie und über den Schaden

1. Angaben der *Business Software Alliance* (*BSA*[239])

Die *BSA* hat zwischen Juni 1996 und Mai 1998 einen weltweiten Anstieg der Internet-Dokumente zum Thema „Warez" von 10.000 auf 285.000 beobachtet.[240] Eine derartige Stichwortsuche vom Januar 1999 ergab bereits über 900.000 Dokumente mit Hinweisen auf illegale Software; in Europa

---

236 *Horvath*, **Telepolis** vom 18.12.1997.
237 *Ye*, **Wired Magazine** 4.07 – Juli 1996.
238 Vgl. *Gorman/Lober*, **c't** 11/1999, S. 85.
239 Die *BSA* ist eine Organisation, die im Auftrag von Softwareherstellern gegen Softwarepiraterie vorgeht. Eine ausführliche Darstellung des Internet-Engagements der *BSA* findet sich unten ab Teil 2, C. III. 1. b).
240 Vgl. das Interview mit *Schwarz* (*BSA*), **PC-Intern** 8/1998, S. 37.

lag die Zahl der Dokumente bei 82.000, im deutschsprachigen Raum bei 9.912.[241] Für August 1999 recherchierte der Verband, dass sich im gesamten Internet über 2,2 Millionen verdächtige Dokumente befanden.

Nach *Frank Steinhoff*, Geschäftsführer von *Adobe Systems* in Deutschland und Sprecher der deutschen *BSA,* ist „der direkte Schaden der Internet-Piraterie kaum zu beziffern, übersteigt aber mittlerweile die traditionelle Softwarepiraterie". *Steinhoff* weiter: „Rechnet man beispielsweise damit, dass in Deutschland von jeder der 18.000 illegalen Sites täglich Software im Wert von nur 250 DM (entspricht ca. 128 €) heruntergeladen wird, erreicht der jährliche Schaden über 1,6 Milliarden DM" (entspricht ca. 0,82 Milliarden €).[242]

Gemäß den Angaben der *BSA* zur gesamten Softwarepiraterie (Internet-Piraterie plus sonstige „Offline-Softwarepiraterie") lag die Raubkopierate in Deutschland 1997 bei 33%. Demnach wurde jede dritte Softwarekopie – primär im gewerblichen Bereich – illegal genutzt, wodurch ein direkter Schaden von knapp 891 Millionen DM (entspricht ca. 455 Millionen €) entstanden sein soll.[243] Neben den direkten Schäden in Form von Umsatzeinbußen werden immer wieder auch die Folgeschäden der Softwarepiraterie beklagt: So hatte die Raubkopierate in Deutschland aus dem Jahr 1996 in Höhe von 36% nach Aussage der *BSA* zur Folge, dass 27.000 Arbeitsplätze nicht geschaffen wurden und knapp 2,5 Milliarden DM (entspricht ca. 1,28 Milliarden €) Steuermindereinnahmen entstanden.[244] Eine Studie der Unternehmensberatung *Price Waterhouse* im Auftrag der *BSA* hat ergeben, dass jeder Arbeitsplatz bei einem Softwarehersteller zusätzlich 5,9 Arbeitsplätze in vor- und nachgelagerten Industrien bedeutet, beispielsweise in Verpackung und Logistik oder bei Distributoren, Fachhändlern und Systemhäusern.[245]

Gemäß den im Mai 1999 veröffentlichten Zahlen für das Jahr 1998 ist die deutsche Raubkopierate im Vergleich zu 1997 von 33% auf 28% erneut gesunken. Dies soll noch immer einem Schaden von 839 Millionen DM (entspricht ca. 429 Millionen €) entsprechen, allerdings wurde für diese Erhebung nur sogenannte Business-Software berücksichtigt, also keine Spiele, Nachschlagewerke etc..[246]

In einer aktuelleren Einschätzung vom Juni 2002 geht die *BSA* davon aus, dass der Anteil illegal genutzter Software in Deutschland wieder um sechs Prozentpunkte auf 34% gestiegen sei. Auch weltweit sei die Zahl der Raubkopien im zweiten Jahr in Folge gewachsen. Einer Untersuchung zufolge läge sie jetzt bei 40%. Der Schaden für die globale Volkswirtschaft sei jedoch von 12,26 Milliarden auf 10,97 Milliarden US-Dollar zurückgegangen.[247]

---

241 http://www.bsa.de.
242 Vgl. *Puscher*, **internet world** 1/1999, S. 35.
243 Die Raubkopierate definiert sich als der Anteil der Raubkopien am Gesamtvolumen der in einem bestimmten Zeitraum installierten Software.
244 Vgl. das Interview mit *Schwarz* (*BSA*), **PC-Intern** 8/1998, S. 37.
245 Die Studie findet sich unter http://www.bsa.de/presse/pics/bsafinal.pdf.
246 **c't** 12/1999, S. 34.
247 **Heise Online News** vom 10.06.2002, http://www.heise.de/newsticker/meldung/28101.

2. Angaben der *Software Publishers Association* (*SPA*[248])

Joshua Bauchner, Prozess-Koordinator bei der *SPA*, ging bereits 1997 davon aus, dass täglich Raubkopien im Wert von 5 Milliarden US-Dollar über Tausende von Internet-Seiten verschoben werden.[249] Nach Schätzungen der *SPA* aus demselben Jahr soll täglich neue Software im Wert von 5 Millionen US-Dollar gecrackt und ins Netz gespeist worden sein.[250]

Fast 40% aller Installationen auf der Welt sollen 1998 ohne Lizenz stattgefunden haben, was einem Schaden von 11,4 Milliarden US-Dollar entsprechen soll.[251] Nach Berechnungen der *SPA* ist der Schaden in den USA besonders groß, es folgen die asiatischen Staaten China, Japan und Korea, und dann schließt auch schon Deutschland als Spitzenreiter in Europa an – mit einem Raubverlust von 509 Millionen US-Dollar. Die höchste relative Rate an Raubkopien sollen die osteuropäischen Staaten mit bis zu 90% (Russland) und die asiatischen Länder mit ungefähr 96% (China) erreichen.

Für Deutschland wird in Übereinstimmung mit den Aussagen der *BSA* eine Raubkopierate von 33% genannt. Als Trend ist zu erkennen, dass zwar die Raubkopieraten sinken, der Schaden jedoch ansteigt. Dieser Zuwachs wird mit dem steigenden Marktvolumen im Bereich Software erklärt.[252]

	Raubkopierate			***Verluste durch Piraterie***		
	1997	1998	1999	1997	1998	1999
Belgien / Lux.	36%	35%	36%	$ 51.485	$ 53.401	$ 77.371
Dänemark	32%	31%	29%	$ 45.787	$ 42.069	$ 59.184
Deutschland	33%	28%	27%	$ 508.884	$ 479.376	$ 652.379
Finnland	38%	32%	30%	$ 37.754	$ 36.126	$ 50.594
Frankreich	44%	43%	39%	$ 407.900	$ 425.205	$ 548.408
Griechenland	73%	74%	71%	$ 44.546	$ 55.385	$ 67.708
Großbritannien	31%	29%	26%	$ 334.527	$ 464.771	$ 679.506
Holland	48%	45%	44%	$ 195.098	$ 195.778	$ 264.400
Irland	65%	56%	51%	$ 46.847	$ 60.986	$ 117.892
Italien	43%	45%	44%	$ 271.714	$ 356.879	$ 421.434
Norwegen	46%	40%	37%	$ 104.337	$ 72.452	$ 87.568
Österreich	40%	38%	36%	$ 41.620	$ 51.164	$ 66.929
Portugal	51%	43%	47%	$ 40.991	$ 36.109	$ 49.920
Schweden	43%	38%	35%	$ 127.051	$ 119.073	$ 131.358
Schweiz	39%	33%	33%	$ 92.898	$ 76.471	$ 107.068

---

248 Die *SPA* ist ein Verband ähnlich der *BSA* – siehe unten Teil 2, C. III. 1. a).
249 Vgl. *Pogue*, **Macworld.com**, Oktober 1997.
250 Vgl. *McCandless*, **Wired Magazine** 5.04 – April 1997.
251 Die nachfolgenden Angaben der *SPA* beziehen sich auf die allgemeine Softwarepiraterie, denn bei den Erhebungen der *SPA* findet keine Trennung zwischen Internet-Softwarepiraterie und herkömmlicher Softwarepiraterie statt.
252 Vgl. *BSA*-Pressemeldung vom 25.05.2000, http://www.bsa.de/presseecke/2000/Bs050-08.html.

Spanien	59%	57%	53%	$ 167.288	$ 235.100	$ 247.650
West-Europa	39%	36%	34%	$ 2.518.726	$ 2.760.337	$ 3.629.371

Abbildung 59 – Raubkopieraten und Verluste durch Softwarepiraterie (online und offline) in West-Europa (Angaben in tausend US-Dollar); Quelle: *SIIAs* Report on Global Software Piracy 2000[253]

	1997	***1998***	***1999***
West-Europa	$ 2.519	$ 2.760	$ 3.630
Zentral-Europa	$ 561	$ 640	$ 409
Nordamerika	$ 3.074	$ 3.196	$ 3.631
Lateinamerika	$ 978	$ 1.045	$ 1.128
Asien / Pazifik	$ 3.916	$ 2.955	$ 2.792
Mittlerer Osten	$ 206	$ 190	$ 284
Afrika	$ 186	$ 190	$ 194
Weltweit	$ 11.440	$ 10.976	$ 12.163

Abbildung 60 – durch Softwarepiraterie (online und offline) entgangene Einnahmen (Angaben in tausend US-Dollar); Quelle: *SIIAs* Report on Global Software Piracy 2000[254]

3. Angaben von *Microsoft* Deutschland

Für 1998 bezifferte *Microsoft* den Schaden, der der gesamten deutschen Software-Industrie durch Softwarepiraterie entstanden ist, auf ca. 800 Millionen DM (entspricht ca. 409 Millionen €), wobei das Ausmaß der Internet-Piraterie noch nicht eingerechnet wurde. Alleine der weltweit durch Online-Piraterie verursachte Schaden habe sich für dasselbe Jahr auf mindestens 12 Milliarden US-Dollar belaufen.[255]

4. Angaben aus der Polizeilichen Kriminalstatistik (PKS)

Der PKS-Schlüssel „Softwarepiraterie" wurde 1991 geschaffen. Vor diesem Zeitpunkt wurden die entsprechenden Delikte unter dem Sammelschlüssel der „Urheberrechtsverletzungen" gezählt. Somit sind erst seit 1991 Aussagen über den Umfang dieser Delikte mit Hilfe der PKS möglich.[256] Mittlerweile werden unter den PKS-Schlüsselnummern 7151 und 7152 Daten zur Softwarepiraterie

---

[253] Siehe vorige Fußnote.
[254] Die Studie steht unter http://www.siia.net/estore/GPR-00.pdf zum Download bereit.
[255] Interview mit *Lohmeier* (*Microsoft*), **PC-Intern** 8/1998, S. 36 f.
[256] Vgl. *Paul*, **NJW-CoR** 1995, S. 44.

im privaten und gewerbsmäßigen Bereich erhoben. Zu beachten ist hierbei, dass in der PKS nicht zwischen Fällen mit Internetbezug und den verbleibenden Fällen unterschieden wird.

1997 wies die Statistik 1.318 Fälle von Softwarepiraterie aus, was in etwa 3% der gesamten polizeilich erfassten Computerkriminalität entsprach.[257] Im Vergleich dazu waren in der PKS von 1991 – also noch vor dem Internet-Boom von 1996 und der weiten Verbreitung von Personal Computern – bereits 1.046 Fälle von Softwarepiraterie ausgewiesen.[258] 1998 konnte in der PKS sogar ein Rückgang der erfassten Fälle verzeichnet werden, der sich bei den Delikten im privaten Bereich auf 33,7% und bei den Delikten im gewerbsmäßigen Bereich auf 62,6% belief.

Schlüssel	*Straftaten(-gruppen)*	*erfasste Fälle*		*Veränderung*		*Aufklärungsquote*	
		1998	1997	absolut	In %	1998	1997
7151	Softwarepiraterie (private Anwendung)	362	546	-184	-33,7	96,4	99,3
7152	Softwarepiraterie (in Form gewerbsmäßigen Handelns)	289	772	-483	-62,6	98,3	98,8

Abbildung 61 – Auszug aus der PKS 1998[259] – Fallentwicklung und Aufklärung (Bereich: Bundesgebiet insgesamt)

Schlüssel	*Straftaten (-gruppen)*	*erfasste Fälle*			*Tatortverteilung in %*			
		insges.	Versuche in %*	Straftaten-anteil in %	bis 20	20 - 100	100 - 500	über 500
					(Tsd. Einwohner pro Gemeinde)			
7151	Softwarepiraterie (private Anwendung)	362	0,8	0,8	25,7	20,4	19,1	33,4
7152	Softwarepiraterie (in Form gewerbsmäßigen Handelns)	289	1,0	0,6	41,5	16,3	16,6	25,6

Abbildung 62 – Auszug aus der PKS 1998 – bekannt gewordene Fälle (Bereich: Bundesgebiet insgesamt);
*Anm.: 100% entsprechen alle Delikte im Bereich Computerkriminalität

Der starke Anstieg bei der Softwarepiraterie im Jahr 1999 um 168,5% bei Schlüssel 7151 bzw. 333,2% bei Schlüssel 7152 resultiert nach Angaben des *BKA* aus „komplexen Ermittlungsvorgängen mit zahlreichen Einzelfällen“.

---

[257] PKS 1997, veröffentlicht auf der Webseite des *BKA*, http://www.bka.de/pks/pks1997/index2.html; *S. Jaeger*, Computerkriminalität erneut gestiegen, **c't** 17/98, S. 176.
[258] *Schultz*, S. 118.
[259] Veröffentlicht auf der Webseite des *BKA*, http://www.bka.de/pks/pks1998/index2.html.

Schlüssel	Straftaten(-gruppen)	erfasste Fälle		Veränderung		Aufklärungsquote	
		1999	1998	absolut	In %	1999	1998
7151	Softwarepiraterie (private Anwendung)	972	362	610	168,5	98,9	96,4
7152	Softwarepiraterie (in Form gewerbs-mäßigen Handelns)	1252	289	963	333,2	99,2	98,3

Abbildung 63 – Auszug aus der PKS 1999[260] – Fallentwicklung und Aufklärung (Bereich: Bundesgebiet insgesamt)

Schlüssel	Straftaten (-gruppen)	erfasste Fälle			Tatortverteilung in %			
		insges.	Versuche in %*	Straftaten-anteil in %	bis 20	20 - 100	100 - 500	über 500
					(Tsd. Einwohner pro Gemeinde)			
7151	Softwarepiraterie (private Anwendung)	972	0,6	2,1	17,4	14,3	9,9	58,4
7152	Softwarepiraterie (in Form gewerbs-mäßigen Handelns)	1252	0,7	2,8	71,2	7,1	9,7	11,7

Abbildung 64 – Auszug aus der PKS 1999 – bekannt gewordene Fälle (Bereich: Bundesgebiet insgesamt);
*Anm.: 100% entsprechen alle Delikte im Bereich Computerkriminalität

Schlüssel	Straftaten(-gruppen)	erfasste Fälle		Veränderung		Aufklärungsquote	
		2000	1999	absolut	In %	2000	1999
7151	Softwarepiraterie (private Anwendung)	1361	972	389	40,0	97,3	98,2
7152	Softwarepiraterie (in Form gewerbs-mäßigen Handelns)	937	1252	-315	-25,2	99,6	99,2

Abbildung 65 – Auszug aus der PKS 2000[261] – Fallentwicklung und Aufklärung (Bereich: Bundesgebiet insgesamt)

[260] Veröffentlicht auf der Webseite des *BKA*, http://www.bka.de/pks/pks1999/index2.html.
[261] Veröffentlicht auf der Webseite des *BKA*, http://www.bka.de/pks/pks2000/index2.html.

Schlüssel	Straftaten (-gruppen)	erfasste Fälle			Tatortverteilung in %			
		insges.	Versuche in %*	Straftaten-anteil in %	bis 20	20 - 100	100 - 500	über 500
					(Tsd. Einwohner pro Gemeinde)			
7151	Softwarepiraterie (private Anwendung)	1361	0,2	2,4	23,7	21,5	9,3	45,1
7152	Softwarepiraterie (in Form gewerbsmäßigen Handelns)	937	0,4	1,7	17,3	31,1	20,9	30,5

Abbildung 66 – Auszug aus der PKS 2000 – bekannt gewordene Fälle (Bereich: Bundesgebiet insgesamt);
*Anm.: 100% entsprechen alle Delikte im Bereich Computerkriminalität

Schlüssel	Straftaten(-gruppen)	erfasste Fälle		Veränderung		Aufklärungsquote	
		2001	2000	absolut	In %	2001	2000
7151	Softwarepiraterie (private Anwendung)	1672	1361	311	22,9	99,2	97,3
7152	Softwarepiraterie (in Form gewerbsmäßigen Handelns)	410	937	-527	-56,2	96,1	99,6

Abbildung 67 – Auszug aus der PKS 2001[262] – Fallentwicklung und Aufklärung (Bereich: Bundesgebiet insgesamt)

Schlüssel	Straftaten (-gruppen)	erfasste Fälle			Tatortverteilung in %			
		insges.	Versuche in %*	Straftaten-anteil in %	bis 20	20 - 100	100 - 500	über 500
					(Tsd. Einwohner pro Gemeinde)			
7151	Softwarepiraterie (private Anwendung)	1672	0,4	2,1	41,6	22,7	22,1	13,4
7152	Softwarepiraterie (in Form gewerbsmäßigen Handelns)	410	2,2	0,5	23,4	48,0	12,9	14,6

Abbildung 68 – Auszug aus der PKS 2001 – bekannt gewordene Fälle (Bereich: Bundesgebiet insgesamt);
*Anm.: 100% entsprechen alle Delikte im Bereich Computerkriminalität

[262] Veröffentlicht auf der Webseite des *BKA*, http://www.bka.de/pks/pks2001/index2.html.

Schlüssel	Straftaten(-gruppen)	erfasste Fälle		Veränderung		Aufklärungsquote	
		2002	2001	absolut	In %	2002	2001
7151	Softwarepiraterie (private Anwendung)	1947	1672	275	16,4	96,1	99,2
7152	Softwarepiraterie (in Form gewerbsmäßigen Handelns)	780	410	370	90,2	95,1	96,1

Abbildung 69 – Auszug aus der PKS 2002[263] – Fallentwicklung und Aufklärung (Bereich: Bundesgebiet insgesamt)

Schlüssel	Straftaten-(gruppen)	erfasste Fälle			Tatortverteilung in %			
		insges.	Versuche in %*	Straftaten-anteil in %	bis 20	20 - 100	100 - 500	über 500
					(Tsd. Einwohner pro Gemeinde)			
7151	Softwarepiraterie (private Anwendung)	1947	0,5	3,4	41,6	22,1	11,9	21,6
7152	Softwarepiraterie (in Form gewerbsmäßigen Handelns)	780	0,6	1,4	18,1	19,2	27,7	32,6

Abbildung 70 – Auszug aus der PKS 2002 – bekannt gewordene Fälle (Bereich: Bundesgebiet insgesamt);
*Anm.: 100% entsprechen alle Delikte im Bereich Computerkriminalität

II. Interpretation der Angaben

Zur Ermittlung der von *BSA* und *SPA* veröffentlichten Raubkopieraten werden stets zwei Datenbestände verglichen: Der Softwarebedarf und die tatsächlichen Softwarelizenzierungen.[264] Die Differenz zwischen dem ermittelten Bedarf und legal erworbener Software ergibt demnach den Anteil der Raubkopien. Diese Methode liefert mitunter aufsehenerregende Ergebnisse: So sollen in Europa Mitte bis Ende der 80er Jahre pro eingesetztem PC durchschnittlich nur 0,5 Computerprogramme verkauft worden sein.[265] Allerdings ist dieses Berechnungsverfahren nicht frei von einigen gravierenden Schwachstellen:

Um den Bedarf an Software zu ermitteln, muss die Zahl der verkauften PC-Systeme in den beobachteten Ländern geschätzt werden. Dass es sich hierbei um eine äußerst schwierige Aufgabe handelt, ist offenkundig. Während es beispielsweise in den USA auch für Privatleute üblich ist, PC-Komplettsysteme zu kaufen, gibt es in Deutschland eine signifikante Gruppe von Computernutzern, die sich ihre Rechner aus Einzelkomponenten selbst zusammenbauen. Ein weiterer Umstand, der die Koppelung des Softwarebedarfs an die Anzahl verkaufter PC-Systeme in Frage stellt, ist der seit

---

263 Veröffentlicht auf der Webseite des *BKA*, http://www.bka.de/pks/pks2002/index2.html.
264 Die bislang größte Studie dieser Art wurde 1998 vom Consulting-Unternehmen *International Planning and Research Corporation* (*IPR*) im Auftrag der *BSA* und *SPA* (bzw. *SIIA*) erstellt. Ein Dokument mit ausführlichen Angaben zur Erhebungsmethodik kann über die Webseite der *BSA* (http://www.bsa.de) angefordert werden.
265 Vgl. *Sieber*, Missbrauch der Informationstechnik, Teil 1, I. B. 5.

einigen Jahren anhaltende Free-Software-Boom[266]. Man muss davon auszugehen, dass für zahlreiche verkaufte Rechner überhaupt kein Bedarf an kostenpflichtiger Software besteht. Besonders der Server-Markt zeigt deutlich, dass sich freie Betriebssysteme wie *Linux* bereits etabliert haben.

Die Schwächen der Erhebungsmethodik scheinen auch einzelnen Vertretern der deutschen *BSA* bewusst zu sein. Erst kürzlich räumten sie in Gesprächen mit der Fachpresse ein, nichts Genaueres über das wahre Ausmaß des Problems zu wissen. Derzeit würden sie an der Entwicklung einer brauchbaren Methode arbeiten, um die Größe des Problems und auch die Wirkung ihrer Arbeit messbar zu machen.[267] Dass die Verbände dennoch die Ergebnisse vorbezeichneter Studien veröffentlichen, mag an ihrem nachvollziehbaren Interesse liegen, ein möglichst düsteres Bild der Situation zu zeichnen.

Zahlreiche journalistische Veröffentlichungen zu dem durch Softwarepiraterie entstandenen Schaden enthalten Angaben, die ebenfalls auf falschen Überlegungen beruhen. Bei der Entwicklung neuer Erhebungsmethoden sollten diese Fehler von vornherein ausgeklammert werden. Kernfrage muss immer sein, welche Raubkopie im konkreten Fall tatsächliches Substitut für eine Originallizenz welchen Wertes ist.

Nicht bedacht wird bei den Schadensberechnungen oftmals, dass nicht jede aus dem Internet heruntergeladene Raubkopie tatsächlich ein Ersatz für den Kauf eines Originalprogramms ist. Die Zahlen beruhen meist auf der Annahme, dass für jede im Umlauf befindliche Raubkopie gezahlt würde, wenn man der Softwarepiraterie einen Riegel vorschieben könnte. Jedoch könnten sich insbesondere jugendliche Raubkopierer die Originalprogramme gar nicht leisten. Vor allem teure Spezialsoftware, die ebenfalls von Warez-Gruppen veröffentlicht wird, ist in den Händen der meisten Raubkopierer wertlos, da ihr Einsatz auf den heimischen Amateur-PCs keinen Nutzen bringt.

Es ist höchst fraglich, ob durch einen „Warez-Addict" ein tatsächlicher Schaden entsteht, obgleich er eine Raubkopie-Sammlung im Wert von einigen Millionen US-Dollar besitzt. Dass er seine Sammelleidenschaft durch den Erwerb von Lizenzen befriedigen würde, ist weder vorstellbar noch möglich. Insofern haben einige der bei der Tätermotivation dargestellten Neutralisierungsmechanismen einen wahren Kern. Dies gilt freilich nur in Bezug auf die fehlerhaften Schadensberechnungen, deren Ergebnisse häufig in den Medien verbreitet werden.

Auch die Angaben aus der PKS zur Softwarepiraterie sind nur bedingt geeignet, das wahre Ausmaß des Problems zu erfassen, da die PKS kein echtes Spiegelbild der Verbrechenswirklichkeit bietet, sondern eine Aussage darüber, wie viele Fälle eines bestimmten Delikts in einem bestimmten Jahr polizeibekannt wurden. Bei Antragsdelikten wie der Softwarepiraterie spiegelt sie zusätzlich die Anzeigebereitschaft der Strafantragsberechtigten wider.[268] Betrachtet man die in der PKS ausgewiesenen - trotz des deutlichen Anstiegs in 2002 - extrem niedrigen Fallzahlen, liegt die Vermu-

---

[266] Vgl. unten Teil 2, C. V. 3. (Exkurs).
[267] *Fremerey*, Rauben und Kopieren, **c't** 8/2000, S. 102.
[268] *Paul*, **NJW-CoR** 1995, S. 45.

tung nahe, dass es sich bei der privaten und gewerbsmäßigen Softwarepiraterie um Delikte mit einem enormen Dunkelfeld[269] handelt.

Diese Vermutung wird durch die Ergebnisse der Gießener Delinquenzbefragungen bestätigt, die seit 1976 regelmäßig von der *Kriminologischen Professur* des Fachbereichs Rechtswissenschaften der *Justus-Liebig-Universität Gießen* durchgeführt werden[270]. Kern dieser Befragungen sind sogenannte Self-Report-Erhebungen[271] bei Studierenden der Rechtswissenschaften aus den ersten Semestern.[272]

Bei der Befragung im Wintersemester 1994/1995 gaben 80% der befragten Studierenden an, bereits Software raubkopiert zu haben.[273] Den veröffentlichten Befragungsergebnissen lässt sich jedoch nicht entnehmen, dass auch nur einer der Befragten in diesem Zusammenhang „polizeiauffällig" wurde, d.h. Kontakt mit der Strafjustiz bzw. Polizei wegen des Verdachts unerlaubter Verwertung urheberrechtlich geschützter Werke oder anderer einschlägiger Delikte hatte.[274] Der Verfasser hält die ermittelte Quote für einen realistischen Wert, geht jedoch davon aus, dass sich bei einer aktuellen Befragung eine noch höhere Lifetime-Deliktsprävalenz zeigen würde.[275] Diese Prognose ergibt sich vor allem aus der Beobachtung der technischen Entwicklung der letzten Jahre, die bewirkt hat, dass CD-Kopiertechnologie mittlerweile für jedermann verfügbar ist. Dies war Mitte der neunziger Jahre nicht der Fall war. Gleiches gilt für den Zugang zum Internet, der heutzutage für Studenten zum Alltag gehört und die Verschaffung von Raubkopien erheblich erleichtert.

Ein Paradoxon stellt die Tatsache dar, dass bestimmte Computerprodukte erst aufgrund von Raubkopien verkauft werden. Insbesondere auf Computerliteratur spezialisierte Verlage stoßen mit ihrem Angebot in Marktlücken, die sich erst durch die Softwarepiraterie aufgetan haben. Bücher mit ausführlichen Anleitungen für die Nutzung von Software finden reißenden Absatz, da raubkopierte Software häufig ohne Begleitmaterial erworben wird.[276] Allerdings ergeben sich in diesen Fällen keine anrechenbaren Vorteile für den Hersteller der Software, denn die positiven Effekte auf die Verlagswirtschaft mindern seinen Schaden definitiv nicht.

---

[269] Zu den Begriffen Dunkelfeld und Dunkelfeldforschung siehe *Kreuzer*, S. 101 ff.. Nach *Kreuzer* umfasst das Dunkelfeld „die Kriminalität, die sich ereignet, ohne ins Hellfeld des strafjustiziell Verfolgten zu gelangen. Dunkelfeldforschung enttabuisiert, versucht Licht in das Dunkel menschlichen normabweichenden Verhaltens zu bringen […]" (S. 102).
[270] Die Ergebnisse der Befragungen seit dem Wintersemester 1999/2000 stehen als PDF-Dokumente unter http://www.uni-giessen.de/~g11039/material.htm zur Verfügung.
[271] Hierunter versteht man ein Verfahren in der Dunkelfeldforschung, das die Verbreitung von Delinquenz nicht mittels Kriminalstatistiken, Einschätzungen Dritter oder sonstiger indirekter Informationen erfasst, sondern Auskünfte von Personen zu eigenem Verhalten erbittet, vgl. *Wittich/Görgen/Kreuzer*, S. 1.
[272] In der Regel handelt es sich um eine schriftliche, standardisierte Erhebung. Unter Zusicherung von Anonymität werden Fragebögen im Rahmen einer universitären Veranstaltung verteilt, ausgefüllt und wieder eingesammelt. Zur genauen Erhebungsmethodik siehe die jeweilige Einleitung der einzelnen Befragungsergebnisse.
[273] *Wittich/Görgen/Kreuzer*, S. 84 (Tabelle 33); das Raubkopieren von Software war im Rahmen der Befragung unter den Studenten mit weitem Abstand die Delinquenzform mit der größten Lifetime-Deliktshäufigkeit, vgl. S. 86 (Tabelle 34).
[274] Obwohl die Frage nach „Raubkopieren von Software" in den Delinquenzbefragungen der Jahre 1999 bis 2003 (siehe Fn. 270) nicht gestellt wurde - der Schwerpunkt der Befragungen liegt im Bereich der Betäubungsmitteldelinquenz - lassen sich dennoch Schlüsse auf die Größe des Dunkelfelds ziehen. Denn bei der Frage nach persönlicher Polizeiauffälligkeit hatten die Befragten die Möglichkeit, den Grund für stattgefundene „Polizeikontakte" anzugeben. Bemerkenswert ist, dass keiner der 2.992 Befragten (Summe der Befragten in den Wintersemestern 1999 bis 2002 und Teilnehmer der Online-Befragung 2001) angab, wegen Urheberrechtsdelikten polizeiauffällig geworden zu sein.
[275] Von Interesse sind daher die Ergebnisse der laufenden Online-Befragung („Gießen-Madison-Online-Survey" 2003, http://www.uni-giessen.de/~g11039/pdf/online_survey_2003.pdf) der *Kriminologischen Professur* in Gießen. Bei dieser Befragung wurde die Frage nach dem Raubkopieren von Software wieder gestellt.
[276] *Schultz*, S. 117.

Dass die Verwendung illegaler Kopien im privaten Bereich häufig dazu führt, dass die gleiche Software für den geschäftlichen Einsatz erworben wird, trifft sicherlich für viele Einzelfälle zu. Vorschläge jedoch, wonach man den beschriebenen „Werbeeffekt" mit den ermittelten Schadenssummen gegenrechnen müsse, sind abzulehnen, da solche Effekte nicht zutreffend betriebswirtschaftlich zu erfassen sind.

Microsoft-Mitbegründer *Bill Gates* soll in diesem Zusammenhang einmal gesagt haben, dass, solange in China Software raubkopiert werde, es gefälligst seine eigene sein solle.[277] Aussagen wie diese stützen die weit verbreitete Vermutung, dass die Verbreitung von Raubkopien im Hinblick auf spätere Marktanteile nützliche Effekte für die Industrie haben kann.

Das Auszählen von Internet-Dokumenten zum Thema Warez ist aus mehreren Gründen nicht geeignet, genaue Informationen über die tatsächliche Verbreitung von Raubkopien im WWW zu erlangen: Bei der Stichwortsuche, die meist über eine Suchmaschine erfolgt, werden als Ergebnis alle Webseiten angezeigt, die den entsprechenden Suchbegriff enthalten. Gibt man also das Stichwort „Warez" ein, wird man eine lange Liste mit Webseiten erhalten, die allesamt vermeintliche Downloadmöglichkeiten bieten. Zu beachten ist jedoch, dass längst nicht auf jeder der aufgelisteten Homepages Raubkopien zu finden sind. Dies liegt zunächst daran, dass es viele Webseiten gibt (z.B. die sogenannten Top-Sites), die lediglich Listen von anderen Homepages zusammenstellen, ohne selbst Raubkopien anzubieten. Weiterhin ist es unter Betreibern von Warez-Seiten weit verbreitet, nur Links einzurichten, die mit Dateien von anderen Warez-Seiten verknüpft sind, anstatt die illegalen Dateien auf die eigene Seite zu stellen. Auf diese Weise kommt es vor, dass eine einzelne Raubkopie auf vielen unterschiedlichen Seiten zum Download angeboten wird. In den wenigsten Fällen befinden sich die illegalen Dateien im Webspace der offerierenden Seite – nur in diesem Fall kann man von „direct downloads" sprechen.

Ein weiteres Problem sind „tote Links". Hierunter versteht man Verknüpfungen, die nicht mehr zum vorgesehenen Ziel führen. Klickt man auf einen toten Link, der für einen Download vorgesehen war, ergibt sich kein Datentransfer, sondern es erscheint eine Fehlermeldung. Tote Links entstehen immer dann, wenn Dateien entfernt, umbenannt oder verschoben wurden. Da diese Vorgänge durch permanente Veränderungen (Aktualisierungen etc.) gerade in der schnelllebigen Warez-Szene an der Tagesordnung sind, entstehen täglich Tausende toter Links.

Ein zusätzlicher Schwachpunkt der Stichwortsuche besteht darin, dass nicht nur Dokumente mit rechtswidrigem Inhalt angezeigt werden, sondern beispielsweise auch Webseiten, die sich mit der Bekämpfung von „Warez" befassen.

Schließlich darf nicht vergessen werden, dass selbst die populärsten Suchmaschinen nur jeweils einen kleinen Ausschnitt der im Web enthaltenen Dokumente erfassen. Zudem wurde bei den Indizes der Suchmaschinen eine thematische und geographische Schieflage festgestellt. Danach indizieren die großen Suchmaschinen bevorzugt kommerzielle amerikanische Seiten sowie populäre Homepages, also solche, auf die bereits viele andere Seiten verweisen.[278]

---

[277] *Ermert*, „Das Kopieren von digitalen Inhalten lässt sich nicht verhindern", **c't** 12/2001, S. 55.
[278] Nach der Studie „Accessibility of Information on the Web" von *Lawrence* und *Giles* vom Februar 1999, vgl. **Heise Online News** vom 08.07.1999, http://www.heise.de/newsticker/meldung/5374.

Die Stichwortsuche liefert demnach lediglich Hinweise darauf, wie es um die Bekanntheit der Warez-Szene im WWW bestellt ist. Sofern sie über einen längeren Zeitraum erfolgt, kann sie als Index für die zukünftige Entwicklung herangezogen werden. Eine eigene vierteljährliche Stichwortsuche nach vier einschlägigen Szene-Begriffen über den großen Suchdienst *Altavista*[279] hat zu folgenden Ergebnissen geführt:

	„warez“	*„crackz“*	*„serialz“*	*„gamez“*
01/1999	668.243*	58.431	41.897	138.550
04/1999	671.770	50.790	36.750	122.150
07/1999	1.071.260	133.470	46.940	149.600
10/1999	2.488.200	182.430	79.580	185.020
01/2000	401.395	36.240	22.720	65.735
04/2000	485.260	45.345	24.605	83.975
07/2000	509.415	51.030	29.745	96.805
10/2000	324.005	47.990	26.805	80.390
01/2001	396.190	44.425	24.115	115.180
04/2001	524.800	43.576	16.703	163.435
07/2001	392.410	27.319	16.136	123.573
10/2001	390.428	26.461	15.611	123.907
01/2002	619.384	129.977	21.415	503.398
04/2002	332.693	64.093	84.360	131.540
07/2002	599.056	89.292	158.943	238.220
10/2002	638.012	94.735	173.213	286.222
01/2003	3.659.903	1.284.991	722.953	1.446.298
04/2003	1.992.891	525.368	500.302	567.995

Abbildung 71 – Stichwortsuche bei *Altavista.com;* *Anzahl der gefundenen Dokumente (Webseiten und Unterseiten).

Da der Index von *Altavista* – wie man der obigen Suchwortstatistik entnehmen kann – über mehrere Monate nicht aktualisiert wurde, und da es mittlerweile Suchdienste gibt, die in Punkto Aktualität und Geschwindigkeit dem Dienst von *Altavista* überlegen sind[280], wurde ab Oktober 2001 eine zweite, vierteljährliche Stichwortsuche bei der Suchmaschine *Google*[281] begonnen.

---

[279] http://www.altavista.com.
[280] Vgl. **Heise Online News** vom 28.11.2001, http://www.heise.de/newsticker/meldung/23014.
[281] http://www.google.de – *Google* gilt derzeit als der leistungsfähigste Suchdienst im WWW.

	„warez“	*„crackz“*	*„serialz“*	*„gamez“*
10/2001	878.000*	68.300	63.800	463.000
01/2002	1.010.000	101.000	58.800	608.000
04/2002	2.950.000	540.000	502.000	973.000
07/2002	11.400.000	1.970.000	2.330.000	2.740.000
10/2002	16.300.000	4.600.000	3.200.000	4.010.000
01/2003	25.400.000	6.310.000	5.660.000	5.930.000
04/2003	21.100.000	5.550.000	4.970.000	5.340.000

Abbildung 72 – Stichwortsuche bei *Google.de;* *Anzahl der gefundenen Dokumente (Webseiten und Unterseiten).

Man wird den Schaden, den die Softwareindustrie durch Internet-Piraterie erleidet, wohl niemals beziffern können. Wie sie derzeit erfolgt, ist die Berechnung von Raubkopieraten kein geeignetes Instrumentarium zur Wahrheitsfindung. Eine wesentlich höhere Aussagekraft bezüglich der Raubkopieraten bei professionellen Anwendern hätten individuelle Erhebungen bei Unternehmen, Behörden oder Computerschulen. Eine Möglichkeit zu solchen Erhebungen bietet sich für die Verbände immer dann, wenn es im Zuge eines Ermittlungsverfahrens wegen Softwarepiraterie zu einer richterlich angeordneten Durchsuchung der entsprechenden Organisation kommt.

Die steigende Bekanntheit der Szene im WWW liefert allerdings schon jetzt einen Hinweis darauf, dass das Problem an Gewicht gewinnt, zumal täglich Tausende neuer Internetnutzer hinzukommen.

C. Bekämpfung und Überwachung von Online-Softwarepiraterie

I. Rechtslage in Deutschland

1. Der urheberrechtliche Schutz von Computerprogrammen

Grundsätzlich zählen Computerprogramme zu den durch das UrhG geschützten (Sprach-) Werken, § 2 Abs. 1 Nr. 1 UrhG. Ihr urheberrechtlicher Schutz setzt demnach die Merkmale des § 2 Abs. 2 UrhG voraus.[282] Danach wird auch die sogenannte kleine Münze geschützt; das Programm muss Originalität in dem Sinne aufweisen, dass es das Ergebnis eigener geistiger Arbeit und nicht alltäglich ist.[283] Zu beachten ist weiterhin die Einschränkung durch § 69a Abs. 3 S. 2 UrhG, wonach zur

---

[282] Siehe hierzu auch § 69a Abs. 3 S. 1 UrhG, der § 2 Abs. 2 UrhG inhaltlich aufgreift. Dass § 69a Abs. 3 S. 1 UrhG entgegen der Formulierung in § 2 Abs. 2 UrhG den Begriff der „eigenen“ geistigen Schöpfung enthält, bedeutet keine inhaltliche Abweichung vom Schutzerfordernis einer „persönlichen“ geistigen Schöpfung i.S.v. § 2 Abs. 2 UrhG, Schricker-*Loewenheim*, § 69a UrhG, Rdnr. 14.

[283] Urteil des *OLG München* vom 25.11.1999 (Az. 29 U 2437/97), **CR** 2000, S. 429, 430; Urteil des *OLG München* vom 27.05.1999 (Az. 6 U 5497/98), **CR** 1999, S. 688, 689; Urteil des *OLG Hamburg* vom 12.03.1998 (Az. 3 U 228/97), **CR** 1999, S. 298; Urteil des *OLG Hamburg* vom 12.03.1998 (Az. 3 U 226/97), **CR** 1998, S. 332, 333; Urteil des *OLG Frankfurt* vom 09.09.1997 (Az. 11 U 6/1997), **CR** 1998, S. 525; Urteil des *OLG Karlsruhe* vom 13.06.1994 (Az. 6 U 52/94), **GRUR** 1994, S. 726, 729; *Wiebe*, **BB** 1993, S. 1097; *Dreier*, Verletzung urheberrechtlich geschützter Software nach der Umsetzung der EG-Richtlinie, **GRUR** 1993, S. 782; *Ullmann*, **CR** 1992, S. 642 f.; *Dreier*, Rechtsschutz von Computerprogrammen, **CR** 1991, S. 578. Nicht ausdrücklich vom Schutz der kleinen Münze sprechend, aber die Anforderungen an die Schutz-

Bestimmung der Schutzfähigkeit keine anderen Kriterien – wie etwa qualitative oder ästhetische Gesichtspunkte – anzuwenden sind. Der gewährte Schutz gilt für alle Ausdrucksformen eines Computerprogramms. Ideen und Grundsätze, die einem Element eines Computerprogramms zugrunde liegen, einschließlich der den Schnittstellen zugrunde liegenden Ideen und Grundsätze, sind nicht geschützt, § 69a Abs. 2 UrhG.

Zu den geschützten Ausdrucksformen gehören die Programmdaten des Objektcodes und des Quellcodes sowie die innere Struktur und Organisation eines Computerprogramms.[284] So sind beispielsweise die konkrete Sammlung, Auswahl und Gliederung der Befehle und die Art, wie Unterprogramme und Arbeitsroutinen aufgeteilt und mit Verzweigungsanweisungen verknüpft werden, dem Urheberschutz zugänglich.[285] § 69a Abs. 1 UrhG erfasst Computerprogramme in jeder Gestalt. Es kommt nicht darauf an, ob sie auf CD-ROM, Festplatte, Diskette oder auf einem anderen Datenträger gespeichert sind.

Bis zum Beginn der 90er Jahre bot das Urheberrechtsgesetz lediglich einen gewissen zivilrechtlichen Schutz[286] für Computerspiele[287]. In der Folgezeit verbesserte der Gesetzgeber den Schutz des

---

fähigkeit von Computerprogrammen entsprechend absenkend: Urteil des *BGH* vom 06.07.2000 (Az. I ZR 244/97 – „OEM-Versionen"), **NJW** 2000, S. 3571, 3572; Urteil des *BGH* vom 24.02.2000 (Az. I ZR 141/97 – „Programmfehlerbeseitigung"), **GRUR** 2000, S. 866, 868; Urteil des *BGH* vom 14.07.1993 (Az. I ZR 47/91 – „Buchhaltungsprogramm"), **GRUR** 1994, S. 39; Urteil des *OLG Frankfurt* vom 18.05.2000 (Az. 6 U 63/99), **CR** 2000, S. 581; Urteil des *OLG Frankfurt* vom 03.11.1998 (Az. 11 U 20/98), **CR** 1999, S. 7 f.

284 Vgl. Urteil des *BGH* vom 14.07.1993 (Az. I ZR 47/91), **GRUR** 1994, S. 39, 40 f. (eine eigenschöpferische Leistung können darstellen: „Gestaltung", „Datenstrukturen", „Bildschirmgestaltung", „Struktur und die Aufteilung des Programms selbst"); Urteil des *BGH* vom 04.10.1990 (Az. I ZR 139/89 – „Betriebssystem"), **BGHZ** 112, S. 264, 277 („[…] wobei es für den Urheberrechtsschutz von Computerprogrammen im allgemeinen auf die Form und Art der Sammlung, Einteilung und Anordnung des Materials ankommt."); Urteil des *OLG Düsseldorf* vom 29.06.1999 (Az. 20 U 85/98), **CR** 2000, S. 184 (der Schutz umfasst den „Programmcode und die innere Struktur und Organisation des Programms"); Urteil des *OLG Celle* vom 09.09.1993 (Az. 13 U 105/93), **CR** 1994, S. 748, 749 f. (vom Schutz umfasst sein können: „Auswahl, Sammlung, Sichtung, Anordnung und Einteilung der Anweisungen an ein Computersystem"); *Lehmann / Tucher*, **CR** 1999, S. 703 (für den Schutz des Source- bzw. Quellcodes); *Günther*, **CR** 1994, S. 612 („Programmcode" und „innere Struktur und Organisation des Programms"); *Wiebe*, **BB** 1993, S. 1095 f. (geschützt sein können: „Objektform, Mikrocode, Programmstruktur, Organisation des Programmablaufs, konkrete Anordnung der Befehle, Befehlsgruppen und Unterprogramme").

285 Siehe auch Schricker-*Loewenheim*, § 69a UrhG, Rdnrn. 10 (schutzfähige Elemente) und 12 (nicht schutzfähige Elemente).

286 Die Ansprüche des Urhebers gegen Rechtsverletzungen sind in den §§ 97 ff. UrhG geregelt. § 97 Abs. 1 UrhG enthält einen deliktischen Anspruch zum Schutz vor materiellen Schäden. Er schützt vor allem die Persönlichkeitsrechte der Urheber und Schutzrechtsinhaber, die Verwertungsrechte der Urheber und die verwertungsrechtlichen Berechtigungen der Schutzrechtsinhaber. Bei Wiederholungsgefahr besteht ein verschuldensunabhängiger Anspruch auf Unterlassung und Beseitigung der Beeinträchtigung. Da sich die Aufklärung von Urheberrechtsverletzungen erfahrungsgemäß recht schwierig gestaltet, ist darüber hinaus ein allgemeiner Anspruch auf Auskunft und Rechnungslegung (§ 259 BGB i.v.m. § 242 BGB) gewohnheitsrechtlich anerkannt. Schließlich sieht die Vorschrift einen verschuldensabhängigen Schadensersatzanspruch vor. Sind dessen Voraussetzungen gegeben, hat der Verletzte drei Möglichkeiten, um den Schaden zu berechnen: Er kann den konkreten Schaden gemäß § 249 ff. BGB (einschließlich des entgangenem Gewinns) ersetzt verlangen, er kann die Herausgabe des Verletzergewinns verlangen oder er kann im Rahmen einer sogenannten Lizenzanalogie (Fiktion eines Lizenzvertrags) angemessene Lizenzgebühren vom Verletzer einfordern.
§ 97 Abs. 2 UrhG regelt den Ersatz immaterieller Schäden, die bei Beeinträchtigungen des Urheberpersönlichkeitsrechts entstanden sind; Rechtsfolge ist eine Entschädigung in Geld. Nicht anspruchsberechtigt gemäß Abs. 2 ist der Lizenznehmer, da ihm das erhebliche persönliche Interesse fehlt.
§ 98 UrhG sieht einen Anspruch auf Vernichtung oder Überlassung (gegen eine angemessene Vergütung) der nichtlizenzierten Vervielfältigungsstücke vor. Dieser Anspruch ist verschuldensunabhängig, wie auch der Anspruch aus § 99 UrhG, aufgrund dessen der Verletzte die Vernichtung oder Überlassung von Vorrichtungen, die zur rechtswidrigen Herstellung von Vervielfältigungsstücken bestimmt sind oder benutzt wurden.

287 Ausführlich zum Schutz von Computerspielen: *Poll/Brauneck*, **GRUR** 2001, S. 389 ff.

geistigen Eigentums in der Informationstechnik durch die Umsetzung der „Richtlinie des Rates der Europäischen Gemeinschaft über den Rechtsschutz von Computerprogrammen“ vom 14.05.1991[288], indem er durch das Urheberrechts-Änderungsgesetz vom 09.06.1993[289] die Tatbestandsmerkmale „Werk“ und „Vervielfältigung“ erheblich erweiterte. Nunmehr fallen beinahe alle Standard-Computerprogramme unter den Werkbegriff des Urheberrechts, und die nur vorübergehende Vervielfältigung wird von § 69c Nr. 1 UrhG erfasst.

Zu beachten ist, dass die zentralen strafrechtlichen Vorschriften des UrhG (§§ 106 ff. UrhG) zivilrechtsakzessorisch sind. Demnach ist die Zivilrechtslage maßgeblich, wenn es um das Vorliegen bestimmter Tatbestandsmerkmale wie z.B. Werk, Bearbeitung, Umgestaltung, Vervielfältigung, Verbreitung oder öffentliche Wiedergabe geht.[290] Problematisch sind die Auswirkungen der Zivilrechtsakzessorietät, wenn bestimmte Merkmale im Zivilrecht zugunsten eines umfassenden Urheberschutzes erweiternd ausgelegt werden.[291] Das Heranziehen gleicher Maßstäbe für das Urheberstrafrecht kann dazu führen, dass das Bestimmtheitsgebot aus Art. 103 Abs. 2 GG verletzt wird.[292] Daher gebieten verfassungsrechtliche Erwägungen, dass ein Strafgericht bei ungeklärter Rechtslage eine gegenüber der zivilrechtlichen Auslegung engere Auslegung vorzunehmen hat – zumindest so lange sich keine höchstrichterliche Rechtsprechung zu den entsprechenden Fragen herausgebildet hat.[293]

Abweichend von den Vorgaben der EU-Richtlinie[294] sind in Deutschland auch unerlaubte Verwertungshandlungen gemäß § 106 UrhG und Eingriffe in verwandte Schutzrechte gemäß § 108 UrhG unter Strafe gestellt, wenn sie im privaten Bereich stattfinden.[295] Für die gewerbsmäßige unerlaubte Verwertung urheberrechtlich geschützter Werke verweist § 108a UrhG auf die genannten Tatbestände und sieht ein erhöhtes Strafmaß vor.[296]

Unter den Schutz des Urheberrechtsgesetzes fallen nicht nur fertige Vollversionen von Programmen, sondern auch das Entwurfsmaterial, vgl. § 69a Abs. 1 UrhG. Hierzu gehören die Vorstufen des Pro-

---

288 Richtlinie 91/250/EWG, **ABl. EG** Nr. L 122 vom 17.05.1991, S. 42 ff.
289 Zweites Gesetz zur Änderung des Urheberrechtsgesetzes vom 09.06.1993, **BGBl. I** 1993, S. 910 ff.
290 Siehe hierzu auch die Ausführungen in Teil 2, C. I. 3. b) (1) (a) und Teil 2, C. I. 3. b) (4) – jeweils m.w.N.
291 Vgl. Wandtke/Bullinger-*Hildebrandt*, § 106 UrhG, Rdnr. 28.
292 In seinem Beschluss vom 10.01.1995, **BVerfGE** 92, S. 1, 12, führt das *Bundesverfassungsgericht* (*BVerfG)* aus: (die Verpflichtung aus Art. 103 Abs. 2 GG) „soll sicherstellen, dass die Normadressaten vorhersehen können, welches Verhalten verboten und mit Strafe bedroht ist. Sie soll andererseits gewährleisten, dass die Entscheidung über strafwürdiges Verhalten im voraus vom Gesetzgeber und nicht erst nachträglich von der vollziehenden oder der rechtsprechenden Gewalt gefällt wird. Insoweit enthält Art. 103 Abs. 2 GG einen strengen Gesetzesvorbehalt, der die Strafgerichte auf die Rechtsanwendung beschränkt. [...] Der mögliche Wortsinn des Gesetzes markiert die äußerste Grenze zulässiger richterlicher Interpretation. Da Art. 103 Abs. 2 GG die Vorhersehbarkeit der Strafdrohung für den Normadressaten garantieren will, ist die Grenze aus dessen Sicht zu bestimmen“.
293 Wandtke/Bullinger-*Hildebrandt*, § 106 UrhG, Rdnr. 28.
294 Siehe Fn. 288.
295 Vgl. *Dannecker*, **BB** 1996, S. 1290. Gleiches gilt für das unerlaubte Anbringen von Urheberbezeichnungen gemäß § 107 UrhG, jedoch ist die Anwendung dieser Vorschrift auf Werke der bildenden Künste (vgl. § 2 Abs. 1 Nr. 4 UrhG) beschränkt, Wandtke/Bullinger-*Hildebrandt*, § 107 UrhG, Rdnr. 1; Schricker-*Haß*, § 107 UrhG. Rdnrn. 10 und 3. Hierzu zählen Computerprogramme nicht (vgl. § 2 Abs. 1 Nr. 1 UrhG). Gleiches gilt für Werke der Musik i.S.d. § 2 Abs. 1 Nr. 2 UrhG.
296 Hinzuweisen ist am Rande auf die §§ 110 und 111 UrhG. Nach § 110 UrhG können Gegenstände, auf die sich eine Straftat nach den §§ 106, 107 Abs. 1 Nr. 2, §§ 108 bis 108b bezieht, eingezogen werden. § 111 UrhG sieht vor, dass auf Antrag des Verletzten eine Verurteilung wegen Verstoßes gegen die §§ 106 bis 108b UrhG öffentlich bekanntgemacht wird, sofern er ein berechtigtes Interesse darlegen kann.

gramms, insbesondere also das Flussdiagramm (Datenflussplan), in dem der Lösungsweg in Form einer grafischen Darstellung des Befehls- und Informationsablaufs wiedergegeben wird. Andere Dokumentationen von Vor- und Zwischenstufen gehören ebenso zum Programm, wobei es nicht darauf ankommt, ob sie in digitaler oder grafischer Form niedergelegt sind.[297] Der Schutz von Entwurfsmaterial wird allerdings nur ausnahmsweise eine Rolle spielen, da von den Warez-Gruppen meist fertige Programme oder Vorabversionen vervielfältigt werden, in denen die Vorstufen bereits enthalten sind. § 106 UrhG schützt ausdrücklich auch die Bearbeitungen und Umgestaltungen eines Werkes, weshalb erst recht unerlaubt modifizierte Computerprogramme erfasst werden.

Begleitmaterial wie Handbücher, Bedienungsanleitungen, Wartungsbücher und sonstige Unterlagen, das dem Benutzer zur Information und richtigen Bedienung des geschützten Programms überlassen wurde, gehört dagegen nicht zum Computerprogramm. Es kann jedoch selbständig nach § 2 Abs. 1 Nr. 1 UrhG als Sprachwerk oder nach § 2 Abs. 1 Nr. 7 UrhG als wissenschaftlich-technische Darstellung geschützt sein.[298] Ähnlich verhält es sich mit der Benutzeroberfläche eines Programms (Graphical User Interface – GUI[299]). Auch sie zählt nicht zum Computerprogramm, kann allerdings ihrerseits nach § 2 Abs. 1 Nr. 1 UrhG oder nach § 2 Abs. 1 Nr. 7 UrhG urheberrechtlichen Schutz genießen.[300]

Gemäß § 69c UrhG hat der Rechtsinhaber, also der Autor bzw. Softwarehersteller, das ausschließliche Recht, Computerprogramme zu vervielfältigen, zu ändern und zu verbreiten. Dritte dürfen dies nur mit ausdrücklicher Genehmigung des Rechtsinhabers. Die in den §§ 45 ff. UrhG gezogenen Schranken des Urheberrechts – insbesondere also die Vervielfältigung zum privaten Gebrauch gemäß § 53 Abs. 1 UrhG[301] – gelten nicht für Computerprogramme.[302]

Die Ausschließlichkeitsrechte des Urhebers finden Ihre Grenzen jedoch in Handlungen, die zum bestimmungsgemäßen Gebrauch des Programms erforderlich sind.[303] Diese sind in der Regel in den Lizenzvereinbarungen festgeschrieben. In den meisten Fällen gilt, dass pro Computer und installierter Softwarekopie bzw. pro Anwender eine Lizenz zu erwerben ist.[304] In zahlreichen Lizenzverträgen ist explizit gestattet, eine Sicherungskopie der Software anzufertigen[305], was allerdings lediglich die Gesetzeslage wiedergibt. Denn nach § 69d Abs. 2 UrhG darf die Erstellung einer Sicherungskopie durch eine Person, die zur Benutzung des Programms berechtigt ist, nicht vertraglich untersagt werden, wenn sie für die Sicherung künftiger Benutzung erforderlich ist. § 69g Abs. 2 UrhG erklärt vertragliche Bestimmungen, die im Widerspruch zu § 69d Abs. 2 UrhG stehen, für nichtig. Eine Sicherungskopie darf – außer im Sicherungsfall – niemals als Arbeitskopie dienen.

---

297 Schricker-*Loewenheim*, § 69a UrhG, Rdnr. 5.
298 Schricker-*Loewenheim*, § 69a UrhG, Rdnr. 6.
299 Das GUI ist eine textlich-grafische Gestaltung der Bildschirmoberfläche, die die Bedienung des Programms vereinfachen soll. Es wird durch das Computerprogramm erzeugt, stellt aber selbst kein Computerprogramm dar.
300 Schricker-*Loewenheim*, § 69a UrhG, Rdnrn. 7 und 26.
301 Zu Sinn, Zweck und rechtlicher Ausgestaltung der sogenannten Privatkopie siehe unten Teil 3, C. I. 1.
302 Vgl. Amtl. Begr. **BT-Drucks.** 12/4022, S. 8 f.
303 Zu beachten ist in diesem Zusammenhang § 31 Abs. 5 UrhG (Zweckübertragungstheorie).
304 So z.B. in den Endbenutzer-Lizenverträgen der folgenden (Standard-)Programme: *Microsoft Windows XP Professional* (Lizenzvertrag, Punkt 1, Abschnitt 1), *Microsoft Internet Explorer 6* (Lizenzvertrag, Punkt 1, Abschnitt 1), *Microsoft Office 2002* - bestehend aus *Outlook 2002, Powerpoint 2002, Word 2002* und *Access 2002* (Lizenzvertrag, Punkt 1, Abschnitt 1), *Symantec Norton Utilities 2002* (Lizenzvertrag, Punkt 1 A.), *Adobe PhotoShop 7* (Lizenzvertrag, Punkt 2.1 i.V.m. Punkt 4), *Adobe Acrobat Reader 5* (Lizenzvertrag, Punkt 2.1 i.V.m. Punkt 4), *Realnetworks RealOne Player 2* (Lizenzvertrag, Abschnitt 1 und Punkt 1 a) (I)).
305 Siehe Fn. 96.

Das Vorhandensein von Sicherungskopien setzt daher zwingend eine vorhandene Originalsoftware voraus. Auf jeden Fall ist es immer unzulässig, von entliehenen oder gekauften Programmen "Sicherungskopien" zu fertigen, die dann nach Rückgabe bzw. Verkauf der Originalsoftware weiter benutzt werden können.

Das sogenannte Fehlerberichtigungsrecht in § 69d Abs. 1 UrhG gestattet schließlich, Programmfehler selbst zu beheben, sofern eine derartige Umarbeitung nicht im Lizenzvertrag verboten wurde.

2. Strafrechtsschutz von Computerprogrammen außerhalb des Urheberrechts[306]

Neben dem urheberrechtlichen Schutz können Computerprogramme insbesondere patentrechtlichen, markenrechtlichen und wettbewerbsrechtlichen Schutz genießen.[307] § 69g Abs. 1 UrhG stellt ausdrücklich klar, dass die urheberrechtlichen Regelungen „die Anwendung sonstiger Rechtsvorschriften auf Computerprogramme, insbesondere über den Schutz von Erfindungen, […] Marken und den Schutz gegen unlauteren Wettbewerb einschließlich des Schutzes von Geschäfts- und Betriebsgeheimnissen […] unberührt“ lassen.

Das Urheberrecht soll nicht nur die Alimentation und Belohnung eines Urhebers gewährleisten, sondern es soll vor allem dem Schutz seiner Persönlichkeit dienen, § 11 UrhG. Des Weiteren soll es sich förderlich auf die kulturelle Entwicklung auswirken und wirtschaftliche Investitionen schützen.[308] Während Schutzgegenstand des Urheberrechts somit die geistigen und materiellen Interessen des Urhebers sind[309], schützt das Patentrecht neben Investitionen in die Entwicklung und Forschung von Produkten vor allem den technischen Fortschritt[310]. Des Weiteren soll es – nicht zuletzt als Gegenleistung für die Offenlegung seines geistigen Eigentums – eine Ent- bzw. Belohnung für den Erfinder gewährleisten und einen Anreiz für diesen hinsichtlich weiterer Erfindungen schaffen.[311]

---

306 Im Folgenden werden ausschließlich Strafvorschriften aus dem Bereich des gewerblichen Rechtsschutzes abgehandelt; zu einschlägigen Straftatbeständen aus dem StGB siehe unten Teil 2, C. 3. b) (2) (b) und (c).

307 Allerdings kommt den Strafvorschriften des PatG, des MarkenG und des UWG im Vergleich zu den §§ 106 ff. UrhG in der Praxis eine deutlich untergeordnete Bedeutung zu, wenn es um die Verfolgung der in Teil 2, A. beschriebenen Taten geht.

308 Vgl. Schricker-*Schricker*, Einl. UrhG, Rdnrn. 8 und 14.

309 Hierzu zählen u.a. seine persönlichen Beziehungen zum Werk.

310 Siehe hierzu die Ausführungen des X. Senats des *BGH* im Beschluss vom 17.10.2001 (Az. X ZB 16/00 – „Suche fehlerhafter Zeichenketten“), **BGHZ** 149, S. 68, 74: „[...] dass das Patentrecht geschaffen wurde, um durch Gewährung eines zeitlich beschränkten Ausschließlichkeitsschutzes neue, nicht nahegelegte und gewerblich anwendbare Problemlösungen auf dem Gebiet der Technik zu fördern“.

311 Diese Aussage ist in Verbindung mit den sogenannten Patentrechtstheorien („Eigentumstheorie, Offenbarungstheorie, Belohnungstheorie und Anspornungstheorie“) zu sehen; die Theorien schließen einander nicht aus, sondern stehen in Zusammenhang miteinander und ergänzen sich, so bei: *Busse*, Einl. PatG, Rdnrn. 55-59 m.w.N.; lesenswert in diesem Kontext ist auch der Beschluss des *BGH* vom 12.02.1987 (Az. X ZB 4/86), **BGHZ** 100, S. 67, 70 f. („Der Grund für die Verleihung des Ausschließlichkeitsrechts ‚Patent’ wird im wesentlichen einerseits in der Anerkennung einer besonderen Leistung im Bereich der Technik und andererseits in der – auch als Ansporn für weitere Leistungen zu verstehenden – Gewährung einer Gegenleistung dafür gesehen, dass der Erfinder den technischen Fortschritt und das technische Wissen der Allgemeinheit bereichert hat“); ebenso: Urteil des *BGH* vom 11.07.1996 (Az. X ZR 99/92 – „Klinische Versuche“), **GRUR** 1996, S. 109, 114 („patentwürdige Bereicherung der Allgemeinheit“).

Zweck des Markenschutzes ist vorrangig die Gewährleistung der Unterscheidungsfunktion eines Kennzeichens im Interesse des Anbieters (Werbefunktion), der Verbraucher (Irreführungsschutz) und der Allgemeinheit.[312]

Das Wettbewerbsrecht[313] schließlich soll Unternehmen („Mitbewerber"), die übrigen Marktteilnehmer (einschließlich der Verbraucher) und die Allgemeinheit vor unlauterem und unerlaubtem Verhalten im geschäftlichen Bereich schützen, um die Funktionsfähigkeit der Wettbewerbsordnung zu sichern.[314]

a) Patentrechtlicher Schutz

Das Patentrecht enthält mit § 142 PatG eine Strafnorm, die dem Schutz von Computerprogrammen dienen kann. Obwohl der Wortlaut des § 1 Abs. 2 Nr. 3 PatG vorsieht, dass „Programme für Datenverarbeitungsanlagen" nicht als Erfindungen i.S.v. § 1 Abs. 1 PatG angesehen werden, sind Computerprogramme nicht schlechthin unpatentierbar[315]. Das sogenannte Patentierungsverbot für Computerprogramme soll nur dann eingreifen, wenn Schutz für Programme für Datenverarbeitungsanlagen „als solche" begehrt wird, vgl. § 1 Abs. 3 PatG.[316] Damit sind alle Computerprogramme nichttechnischer Natur vom Patentschutz ausgenommen.[317] Soweit Computerprogramme jedoch zur Lösung eines konkreten technischen Problems Verwendung finden, sind sie – in dem entsprechenden Kontext – grundsätzlich patentfähig.[318] Somit können auch

---

312 Vgl. *Fezer*, Einl. MarkenG, Rdnr. 30 ff.. Siehe auch Schricker-*Schricker*, Einl. UrhG, Rdnr. 35: „Beim Markenschutz geht es nicht um den Schutz geistiger Schöpfungen, sondern um denjenigen von Unterscheidungszeichen für Waren und Dienstleistungen. Eine Marke zu wählen und zu gestalten, mag eine schöpferische Leistung sein; aber hierauf kommt es für den Schutz nicht an."

313 In diesem Zusammenhang ist hierunter das Recht gegen unlauteren Wettbewerb (Lauterkeitsrecht) zu verstehen; dies ist zu unterscheiden vom Recht gegen Wettbewerbsbeschränkungen (Kartellrecht), das ebenfalls zum Wettbewerbsrecht zählt. Zur Unterscheidung und Abgrenzung siehe *Baumbach/Hefermehl*, Allg., Rdnr. 76 ff.

314 Vgl. HK Wettbewerbsrecht-*Klippel*, Einl. 2 (E 2), Rdnr. 2; *Baumbach/Hefernehl*, Einl. UWG, Rdnr. 41 ff. und Allg., Rdnr. 76 f.. Zum Schutz der Allgemeinheit vor „Auswüchsen des Wettbewerbs" siehe Urteil des *BGH* vom 06.12.2001 (Az. I ZR 284/00 – „HIV Positive"), **GRUR** 2002, S. 360; Beschluss des *BGH* vom 13.12.1999 (Az. X ZB 11/98 – „Logikverifikation"), **BGHZ** 144, 255, 266; Urteil des *BGH* vom 06.10.1999 (Az. I ZR 46/97 – „Giftnotruf-Box"), **GRUR** 2000, 237, 238; Urteil des *BGH* vom 03.12.1998 (Az. I ZR 119/96 – „Hormonpräparate"), **BGHZ** 140, S. 134, 138 f.

315 Beschluss des *BGH* vom 07.06.1977 (Az. X ZB 20/74 – „Prüfverfahren"), **GRUR** 1978, S. 102.

316 Innerhalb der juristischen Literatur wird nicht einheitlich beurteilt, wann lediglich ein – nicht schutzfähiges – „Programm als solches" vorliegt. Zum Meinungsstand: *Melullis*, **GRUR** 1998, S. 845 ff. m.w.N.; *Melullis* selbst versteht unter "Programm als solches" lediglich den zugrunde liegenden, von einer technischen Funktion noch freien Programminhalt („Computerprogramm als solches ist […] mithin das außertechnische Konzept; d.h. die der Umsetzung in eine Handlungsanweisung an den Rechner vorausgehende Konzeption" – S. 852).

317 Urteil des *BGH* vom 04.10.1990 (Az. I ZR 139/89 – „Betriebssystem"), **BGHZ** 112, S. 264, 277. Das Erfordernis der sogenannten Technizität einer Erfindung gilt nicht nur für Computerprogramme, sondern ist Voraussetzung für alle Patentbegehren, *Mes*, § 1 PatG, Rdnr. 9 ff.. Danach muss die Erfindung "technischen Charakter" besitzen und einen "technischen Beitrag" zum Stand der Technik leisten; vgl. hierzu: Beschluss des *BGH* vom 25.03.1986 (Az. X ZR 8/85 – „Schweißgemisch"), **GRUR** 1986, S. 531; Beschluss des *BGH* vom 22.06.1976 (Az. X ZB 23/74 – „Dispositionsprogramm"), **GRUR** 1977, S. 96; Beschluss des *BGH* vom 27.03.1969 (Az. X ZB 15/67 – „Rote Taube"), **GRUR** 1969, S. 672.

318 Beschluss des *BGH* vom 17.10.2001 (Az. X ZB 16/00 – „Suche fehlerhafter Zeichenketten"), **BGHZ** 149, S. 68, 75 - siehe in diesem Zusammenhang auch die weiteren Ausführungen des X. Senats des *BGH* zu den bereits entschiedenen Fällen, die im Rahmen einer Gesamtbetrachtung herangezogen werden können: „Danach kann ein Programm patentiert werden, wenn es in technische Abläufe eingebunden ist, etwa dergestalt, dass es Messergebnisse aufarbeitet, den Ablauf technischer Einrichtungen überwacht oder sonst steuernd bzw. regelnd nach außen wirkt (Beschluss vom 13.05.1980 (Az. X ZB 19/78 – „Antiblockiersystem"), **GRUR** 1980, S. 849, 850. Den in der Regel dem Patentschutz zugänglichen Lehren vergleichbar ist auch ein Verfahren, mit dem vermittels einer Datenverarbeitungsanlage durch Prüfung und Ver-

Programme, die im Zusammenhang mit anderen Bestandteilen eine Erfindung bilden, patentrechtlichen Schutz genießen.[319]

Weiter ist für einen patentrechtlichen Schutz erforderlich, dass neben der bereits angesprochenen Technizität die weiteren Voraussetzungen des § 1 Abs. 1 PatG vorliegen: Demnach muss die Erfindung „neu" (§ 3 PatG / Art. 54 EPÜ) sein[320], auf einer „erfinderischen Tätigkeit" (§ 4 PatG / Art. 56 EPÜ) beruhen[321] und „gewerblich anwendbar" (§ 5 PatG / Art. 57 EPÜ) sein[322].

Das Vorliegen der Voraussetzungen wird nach Einreichung der Patentanmeldung vom Patentamt geprüft, und bei positivem Ergebnis kann eine Erfindung patentiert werden. Das Patent ist das territorial begrenzte und auf 20 Jahre[323] beschränkte ausschließliche subjektive Recht, eine Erfindung zu benutzen, und es entsteht, anders als das Urheberrecht, nicht mit der Schöpfung des Werkes, sondern erst durch staatlichen Erteilungsakt.

Während der 20-jährigen Schutzdauer gilt auch der strafrechtliche Schutz des § 142 PatG. Dessen Abs. 1 Nr. 1 stellt u.a. das Herstellen, Anbieten, Inverkehrbringen, Gebrauchen und Besitzen von patentrechtlich geschützten Erzeugnissen ohne Zustimmung des Patentinhabers unter Strafe. § 142 PatG ist demnach einschlägig, wenn patentrechtlich geschützte Computerprogramme von Raubkopierern vervielfältigt und zum Kauf angeboten werden. Der dreijährige Strafrahmen des Abs. 1 wird gemäß § 142 Abs. 2 PatG auf 5 Jahre Freiheitsstrafe ausgedehnt, sofern der Täter gewerbsmäßig handelt.

Welche Anforderungen in Zukunft an die Patentfähigkeit von Computerprogrammen zu stellen sind, hängt maßgeblich davon ab, welche Entwicklung die Gesetzgebung auf europäischer Ebene nimmt. Am 20.02.2002 wurde von der Kommission ein Vorschlag für eine Richtlinie[324] über die Patentierbarkeit computerimplementierter Erfindungen vorgelegt, die nicht zuletzt dem Umstand Rechnung tragen soll, dass sich trotz der Gültigkeit ähnlicher Rechtsvorschriften in den

---

gleich von Daten ein Zwischenschritt im Rahmen der Herstellung technischer Gegenstände erledigt werden kann, wenn diese Lösung durch eine auf technischen Überlegungen beruhende Erkenntnis und deren Umsetzung geprägt ist (Beschluss des *BGH* vom 13.12.1999 (Az. X ZB 11/98 – „Logikverifikation"), **BGHZ** 143, S. 255, 264). Gleiches trifft zu, wenn die Lehre die Funktionsfähigkeit der Datenverarbeitungsanlage als solche betrifft und damit das unmittelbare Zusammenwirken ihrer Elemente ermöglicht (Beschluss des *BGH* vom 11.06.1991 (Az. X ZB 13/88 – „Seitenpuffer"), **BGHZ** 115, S. 11, 21). Auch Anweisungen, die einen bestimmten Aufbau einer Datenverarbeitungsanlage lehren oder vorsehen, eine solche Anlage auf eigenartige Weise zu benutzen (vgl. Beschluss des *BGH* vom 22.06.1976 (Az. X ZB 23/74 – „Dispositionsprogramm"), **BGHZ** 67, S. 22, 29 f.), müssen die Voraussetzungen des Patentierungsausschlusses nicht notwendig erfüllen".

319 Vgl. *Redeker*, Rdnr. 80; siehe auch das Urteil des *BGH* vom 04.02.1992 (Az. X ZR 43/91 – „Tauchcomputer"), **GRUR** 1992, S. 430, 432, wonach „der gesamte Erfindungsgegenstand unter Einschluss einer etwaigen Rechenregel" zu berücksichtigen ist.

320 Dies ist der Fall, wenn die Erfindung nicht zum Stand der Technik gehört. Unter dem Stand der Technik sind alle Kenntnisse zu verstehen, die vor dem Zeitpunkt der (Patent-)Anmeldung einer unbegrenzten Anzahl von Personen zugänglich gemacht worden sind, § 3 PatG.

321 Nach dem Wortlaut des § 4 S. 1 PatG gilt eine Erfindung als „auf erfinderischer Tätigkeit beruhend", wenn sie sich für den Fachmann nicht in naheliegender Weise aus dem Stand der Technik ergibt. Ausführlich zur „erfinderischen Tätigkeit" in der neueren Rechtsprechung des *BGH*: *Jestaedt*, **GRUR** 2001, S. 939 ff.

322 § 5 Abs. 1 PatG erklärt eine Erfindung als gewerblich anwendbar, wenn ihr Gegenstand auf irgendeinem gewerblichen Gebiet einschließlich der Landwirtschaft hergestellt oder benutzt werden kann.

323 Zum Vergleich: Das Urheberrecht erlischt 70 Jahre nach dem Tod des Urhebers (post mortem auctoris), § 64 UrhG.

324 Richtlinie des Europäischen Parlaments und des Rates über die Patentierbarkeit computerimplementierter Erfindungen, KOM (2002), 92 endg., http://europa.eu.int/comm/internal_market/en/indprop/comp/com02-92de.pdf.

Mitgliedstaaten eine uneinheitliche Rechtsprechung und Praxis der Patentämter in Bezug auf die Schutzfähigkeit von Computerprogrammen entwickelt haben.[325]

b) Markenrechtlicher Schutz

Für den Schutz von Software kann außerdem das Markenrecht von Bedeutung sein. Geschützt werden in diesem Zusammenhang nicht die Programme selbst, sondern nur die Marke, unter der sie und dazugehöriges Begleitmaterial vertrieben werden; unterschieden wird insbesondere zwischen Wortzeichen, Bildzeichen und Zeichen, die aus Worten und Bildern zusammengesetzt sind.[326] Schutzfähig sind diese nur dann, wenn keines der Schutzhindernisse gemäß §§ 8 ff. MarkenG vorliegt[327] und sich das Zeichen einer konkreten Verwendung zuordnen lässt[328].

Markenschutz entsteht entweder durch die Eintragung eines Zeichens als Marke in das vom Patentamt geführte Register (§ 4 Nr. 1 MarkenG), durch die Benutzung eines Zeichens im geschäftlichen Verkehr, soweit das Zeichen innerhalb beteiligter Verkehrskreise als Marke Verkehrsgeltung erworben hat (§ 4 Nr. 2 MarkenG) oder durch die im Sinne des Artikels 6^{bis} der Pariser Verbandsübereinkunft zum Schutz des gewerblichen Eigentums[329] notorische Bekanntheit einer Marke (§ 4 Nr. 2 MarkenG). Die Schutzdauer einer eingetragenen Marke beginnt mit dem Anmeldetag und endet 10 Jahre nach dem Ablauf des Monats, in den der Anmeldetag fällt, § 47 Abs. 1 MarkenG. Sie kann jedoch um jeweils 10 weitere Jahre gegen Zahlung entsprechender Gebühren verlängert werden, § 47 Abs. 2 MarkenG.

Neben dem Markenschutz ist auch der Schutz geschäftlicher Bezeichnungen im MarkenG verankert. Von Bedeutung ist im Zusammenhang mit Computerprogrammen der Schutz von Werktiteln, die gemäß § 5 Abs. 1 MarkenG zu den geschäftlichen Bezeichnungen zählen. Obwohl der Wortlaut des § 5 Abs. 3 MarkenG den Titelschutz auf „Namen oder besondere Bezeichnungen von Druckschriften, Filmwerken, Tonwerken, Bühnenwerken oder sonstigen vergleichbaren Werken“ beschränkt, hat der *Bundesgerichtshof (BGH)* einen Titelschutz auch für Computerprogramme zugelassen[330]. Der Titelschutz beginnt mit der ersten Benutzung, ausnahmsweise mit der Einführungswerbung oder Vorankündigung eines Produkts.[331]

---

325 So ein Teil der Begründung des Richtlinienvorschlags, KOM (2002) 92, S. 1 f.
326 *Redeker*, Rdnrn. 101 und 107 zu § 3 Abs. 1 MarkenG.
327 So ist es z.B. erforderlich, dass den Zeichen eine gewisse Unterscheidungskraft für die Waren oder Dienstleistungen, für die sie bestimmt sind, zukommt, § 8 Abs. 2 Nr. 1 MarkenG, oder dass sie nicht gegen die öffentliche Ordnung oder die guten Sitten verstoßen, § 8 Abs. 2 Nr. 5 MarkenG.
328 Hierfür gibt es ein System von Waren- bzw. Dienstleistungsklassen, die sogenannte Nizza-Klassifikation („Abkommen von Nizza über die internationale Klassifikation von Waren und Dienstleistungen für die Eintragung von Marken“ vom 15. Juni 1957) diese ist einzusehen auf der Internetpräsenz des *Deutschen Patent- und Markenamts (DPMA)* unter http://www.dpma.de/suche/klass/wd/abkommen.html. Dort findet sich ebenfalls eine Auflistung sämtlicher Klassen: http://www.dpma.de/suche/klass/wd/einteilung.html. Von Bedeutung für Markenanmeldungen im Bereich Computerprogramme sind vor allem die Klassen 9 und 42.
329 Sogenannte Pariser Verbandsübereinkunft, einzusehen auf der Internetseite *Transpatent.com*, unter http://transpatent.com/archiv/152pvue/pvue.html.
330 Siehe hierzu vor allem die Entscheidungen „FTOS“ (*BGH*-Urteil vom 24.04.1997 (Az. I ZR 233/94), **GRUR** 1997, S. 902, 903) und „PowerPoint“ (*BGH*-Urteil vom 24.04.1997 (Az. I ZR 44/95), **NJW** 1997, S. 3313, 3314); a.A. *Redeker*, Rdnr. 108 m.w.N.
331 Wandtke/Bullinger-*Grützmacher*, § 69g UrhG, Rdnr. 17.

Bestimmte Beeinträchtigungen von Marken- und Titelschutz sind durch die §§ 143 ff. MarkenG mit Strafe bedroht. Gemeinsames Tatbestandsmerkmal aller kennzeichenrechtlichen Straftatbestände ist allerdings, dass die Verletzungshandlungen widerrechtlich im „geschäftlichen Verkehr" vorgenommen werden müssen[332]. Demnach ist § 143 MarkenG vor allem dann einschlägig, wenn Profit-Pirates auf Webseiten für Produktfälschungen bzw. nichtlizenzierte Downloads mit den Logos und Bezeichnungen der Softwarehersteller werben oder entsprechende Produkte mit geschützten Kennzeichen versehen und versenden.

c) Wettbewerbsrechtlicher Schutz

Bezogen auf Computerprogramme kann grob zwischen dem wettbewerbsrechtlichen Schutz vor Kopien bzw. Nachahmungen, dem wettbewerbsrechtlichen Schutz vor Irreführung und dem wettbewerbsrechtlichen Geheimnisschutz unterschieden werden.[333] Zur ersten Fallgruppe gehört beispielsweise das Überwinden von Kopierschutz, das Erstellen von Kopien oder Nachahmungen sowie das Inverkehrsetzen von bzw. Handeltreiben mit Kopien oder Nachahmungen wettbewerbsrechtlich geschützter Computerprogramme[334], wobei stets ein Handeln im geschäftlichen Verkehr zu Zwecken des Wettbewerbs vorliegen muss, damit die zivilrechtlichen Sanktionsmöglichkeiten des UWG – die Geltendmachung von Unterlassungs-, Beseitigungs- und Schadensersatzansprüchen[335] – wahrgenommen werden können.[336] Strafrechtlich sind die aufgezählten Handlungen jedoch nicht durch das UWG sanktioniert, weshalb die Fallgruppen der Irreführung und des Geheimnisverrats für die vorliegende Arbeit von größerer Bedeutung sind.

So sieht § 4 Abs. 1 S. 1 UWG eine Freiheitsstrafe von bis zu zwei Jahren oder eine Geldstrafe vor, wenn jemand in der Absicht, den Anschein eines besonders günstigen Angebots hervorzurufen, in öffentlichen Bekanntmachungen oder in Mitteilungen, die für einen größeren Kreis von Personen bestimmt sind, über geschäftliche Verhältnisse, insbesondere über die Beschaffenheit, den Ursprung, die Herstellungsart oder die Preisbemessung von Waren oder gewerblichen Leistungen, über die Art des Bezugs oder die Bezugsquelle von Waren, über den Besitz von Auszeichnungen, über den Anlass oder den Zweck des Verkaufs oder über die Menge der Vorräte wissentlich unwahre und zur Irreführung geeignete Angaben macht. Demnach kann sich in den Fällen, in denen Profit-Pirates einem größeren Kundenkreis[337] Raubkopien bzw. Plagiate anbieten, eine Strafbarkeit aus § 4 UWG

---

[332] *Fezer*, § 143 MarkenG, Rdnr. 13; maßgeblich für die Begriffsbestimmung des „geschäftlichen Verkehrs" ist § 14 MarkenG, wonach unter „Handeln im geschäftlichen Verkehr" jede wirtschaftliche Tätigkeit auf dem Markt zu verstehen ist, die der Förderung eines eigenen oder fremden Geschäftszwecks zu dienen bestimmt ist. Die Absicht der Gewinnerzielung ist hierbei nicht erforderlich, *Fezer*, § 14 MarkenG, Rdnr. 41.

[333] Eine ähnliche Differenzierung wird vorgenommen von *Redeker*, Rdnr. 113 ff.; siehe auch Wandtke/Bullinger-*Grützmacher*, § 69g UrhG, Rdnr. 18 ff.

[334] *Redeker*, Rdnrn. 114, 115, 119 und 121; zur wettbewerbsrechtlichen Schutzfähigkeit von Computerprogrammen siehe *Redeker*, Rdnr. 116; danach ist nicht der dem Programm zugrunde liegende Algorithmus schutzfähig, wohl aber das entwickelte Programm (als ganzes) und die entwickelten Begleitmaterialien. Das Programm muss das Ergebnis betrieblicher Investitionen sein und „Merkmale aufweisen, die geeignet sind, entweder auf die betriebliche Herkunft oder auf Besonderheiten des Erzeugnisses hinzuweisen". Nicht verlangt wird eine „eigenschöpferische Entwicklung" (UrhG) oder eine „Erfindung" (PatentG).

[335] Die entsprechenden Anspruchsgrundlagen ergeben sich aus § 1 i.V.m. § 13 Abs. 2 UWG (Unterlassung), § 1 i.V.m. § 13 Abs. 6 UWG (Schadensersatz) und § 1 UWG i.V.m. § 1004 BGB analog (Beseitigung).

[336] Des Weiteren ist zu beachten, dass der Schutz aus § 1 UWG nicht gegenüber privaten Konsumenten und Endverbrauchern besteht, Wandtke/Bullinger-*Grützmacher*, § 69g UrhG, Rdnr. 25.

[337] Unter dem Tatbestandsmerkmal „für einen größeren Personenkreis bestimmte Mitteilungen" ist zu verstehen, dass die Mitteilungen sich nicht an alle, sondern lediglich an eine im voraus unbestimmte und unbegrenzte Mehrheit von Perso-

ergeben, sofern sie in ihren Werbe-E-Mails oder auf ihren Webseiten den Eindruck vermitteln, dass Originalprodukte zu günstigen Konditionen verkauft werden[338].

Die Vorschriften der §§ 17, 18 und 20 UWG normieren den strafrechtlichen Schutz von Betriebs- bzw. Geschäftsgeheimnissen[339] (§ 17 UWG) und von Vorlagen bzw. Vorschriften technischer Art (§ 18 UWG) vor Verrat, Ausspähung und unerlaubter Verwertung[340]. Während für die Tathandlungen gemäß § 17 Abs. 1 UWG und § 18 UWG nur Personen als Täter in Frage kommen, denen Geheimnisse bzw. Vorlagen oder technische Vorschriften vom Inhaber des geschützten Geschäftsbetriebes anvertraut bzw. zugänglich gemacht worden sind, sieht § 17 Abs. 2 UrhG auch für solche Täter eine Strafe vor, die nicht zwangsläufig im Lager des Geschädigten stehen, sondern diesem auch völlig unbekannt sein können. Damit erfasst der wettbewerbsrechtliche Schutz ausnahmsweise Handlungen Privater zu persönlichen Zwecken, zu denen u.a. das Ausspähen eines Geheimnisses aus Eigennutz zählt, vgl. § 17 Abs. 2 Nr. 1 a) UWG[341].

3. Strafbarkeit von „Online-Softwarepiraten“ nach geltendem Recht[342]

Wie der bisherigen Darstellung entnommen werden kann, ermöglichen die umfassenden Nutzungsmöglichkeiten des Internet eine Vielzahl von Handlungen, die im Zusammenhang mit Softwarepiraterie stehen können. Welche dieser Handlungen Tatbestände des geltenden deutschen Straf- und Nebenstrafrechts erfüllen, wird nachfolgend erörtert. Vorab ist jedoch zu klären, inwieweit deutsches Strafrecht überhaupt Anwendung findet, wenn Straftaten über das Internet begangen werden.

a) Anwendbarkeit deutschen Strafrechts

Von den Spezialfällen der §§ 6 und 7 StGB abgesehen, richtet sich die Anwendbarkeit des deutschen Strafrechts nach dem in § 3 StGB geregelten Territorialitätsprinzip und der in § 9 StGB normierten Ubiquitätstheorie: Gemäß § 3 StGB gilt das deutsche Strafrecht für Taten, "die im Inland begangen werden". Nach § 9 Abs. 1 StGB ist eine Tat "an jedem Ort begangen, an dem der Täter gehandelt hat oder im Falle des Unterlassens hätte handeln müssen, oder an dem der zum Tatbestand gehörende Erfolg eingetreten ist oder nach der Vorstellung des Täters eintreten sollte". Voraussetzung für das Eingreifen des deutschen Strafrechts ist somit entweder eine Tathandlung (§ 9 Abs. 1, 1. Alt. StGB) oder ein Erfolg (§ 9 Abs. 1, 3. Alt. StGB) auf deutschem Staatsgebiet.

---

nen, jedoch gegebenenfalls auch nur an bestimmte Personengruppen wenden, HK Wettbewerbsrecht-*Ekey*, § 4 UWG, Rdnr. 7.

338 Siehe hierzu unten Teil 2, C. 3. c) (2).

339 Computerprogramme können sowohl Geschäfts- oder Betriebsgeheimnisse enthalten als auch darstellen, *Baumbach/Hefermehl*, § 17 UWG, Rdnr. 9; siehe hierzu auch die Ausführungen unter Teil 2, C. I. 3. b) (2) (d).

340 § 20 UWG bezieht sich auf die §§ 17 und 18 UWG und stellt den Versuch der Verleitung zu diesen Delikten, das Annehmen des Erbietens zu diesen Delikten, das Erbieten zu diesen Delikten und das Bereiterklären zu diesen Delikten auf Ansinnen eines anderen unter Strafe, siehe auch Fn. 379.

341 Diese Tatmodalität wird vor allem von Crackern verwirklicht, siehe unten Teil 2, C. I. 3. b) (2) (d).

342 Nachtrag: Die vorliegende Arbeit wurde am 26.05.2003 als Dissertation eingereicht. Dieses Datum markiert folglich den Stand der Bearbeitung. Am 10.09.2003 ist das Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft (**BGBl.** I 2003, S. 1774-1788) in Kraft getreten, weshalb die Überschrift nunmehr folgendermaßen zu verstehen ist: „Strafbarkeit von Online-Softwarepiraten nach bis zum 10.09.2003 geltenden Recht“. Zur Relevanz der Änderungen des UrhG für die nachfolgende Darstellung siehe den Nachtrag in Fn. 433.

Unproblematisch sind solche Fälle, in denen der Täter in Deutschland handelt, indem er zum Beispiel von Deutschland aus Raubkopien auf einen ausländischen Server überträgt. Hier besteht unzweifelhaft ein deutscher Tathandlungsort i.S.v. § 9 Abs. 1, 1. Alt. StGB.

Fraglich ist allerdings, wann der Erfolg einer vom Ausland aus begangenen Tat (§ 9 Abs. 1, 3. Alt. StGB) auf deutschem Staatsgebiet eingetreten ist. Während die Anwendung des § 3 i.V.m. § 9 StGB im Bereich der klassischen Erfolgsdelikte und im Bereich der konkreten Gefährdungsdelikte keine Schwierigkeiten bereitet, ist die Anwendung der Norm auf Verbreitungs- und Äußerungsdelikte – also auf abstrakte Gefährdungsdelikte – umstritten[343]: Werden diese vom Ausland aus verübt, so haben sie nach einer verbreiteten Ansicht keinen inländischen Erfolgsort i.S.v. § 9 Abs. 1 StGB; eine Bestrafung nach deutschem Recht scheidet aus.

Eine andere Meinung sieht den Erfolgsort überall dort, wo die Realisierung der Gefahr möglich ist. Demzufolge wäre § 3 i.V.m. § 9 StGB bei allen Verbreitungs- und Äußerungsdelikten im Internet einschlägig, die vom Ausland aus verübt werden.

Eine dritte Ansicht differenziert anhand der Technologie, die bei der Verbreitung der rechtswidrigen Inhalte zum Einsatz kommt: Danach ist beim Zugänglichmachen von strafbaren Inhalten im Internet ein Tathandlungserfolg im Sinne der §§ 3, 9 StGB gegeben, wenn strafbare Inhalte durch sogenannte Push-Technologien[344] nach Deutschland übermittelt werden, nicht jedoch schon dann, wenn Daten nur auf ausländischen Servern gespeichert und durch Pull-Technologien[345] von Deutschland aus abgerufen werden.

Die zuletzt dargestellte Ansicht ist vorzugswürdig. Sie vermeidet eine „Sonder-Dogmatik“ für Internet-Delikte und führt zu sachgerechten Ergebnissen.[346] Denn folgt man der zuerst dargestellten, restriktiven Auffassung, hätte man keine strafrechtliche Handhabe gegen Täter, die vom Ausland aus gezielt deutsche Server als Ablagemöglichkeit für rechtswidrige Inhalte nutzen oder E-Mails mit entsprechenden Inhalten nach Deutschland senden. Im Ausland operierende Kriminelle könnten deutsche Host-Service-Provider mit rechtswidrigen Daten regelrecht überschwemmen, ohne strafrechtliche Konsequenzen von Seiten des deutschen Staates befürchten zu müssen.[347] Ebenfalls abzulehnen ist die zweite Auffassung, deren konsequente Anwendung zu dem Ergebnis führen würde, dass praktisch alle weltweit verfügbaren Web-Angebote dem deutschen Strafrecht unterfielen. Im Hinblick auf die damit einhergehende weltweite Verfolgungspflicht der deutschen Behörden

---

343 Ausführlich zu diesem Meinungsstreit: *Sieber*, Internationales Strafrecht im Internet, **NJW** 1999, S. 2065 ff. m.w.N., der die nachfolgend als „dritte Ansicht“ bezeichnete Meinung vertritt; die Frage nach der Behandlung der Verbreitungs- und Äußerungsdelikte ist für die vorliegende Arbeit relevant, sofern man in der Verwirklichung des Verbreitungstatbestandes des § 106 UrhG ein abstraktes Gefährdungsdelikt sieht.

344 Beim Einsatz von Push-Technologien werden Daten vom Ausland aus aktiv auf Computersysteme in Deutschland übermittelt (sogenannte Uploads).

345 Daten werden von Deutschland aus von ausländischen Servern „gezogen“ (Downloads).

346 Vgl. *Tröndle/Fischer*, § 9 StGB, Rdnr. 7a.

347 Diese Argumentation gilt nur bedingt für § 106 UrhG, da dieser sowohl die unerlaubte Verbreitung als auch die unerlaubte Vervielfältigung und öffentliche Wiedergabe geschützter Werke unter Strafe stellt. Ein Täter, der eine Raubkopie vom Ausland aus auf einem öffentlichen deutschen News-Server ablegt, verwirklicht zwangsläufig beide Tatbestände des § 106 UrhG, wobei der Erfolgsort der unerlaubten Vervielfältigung in Deutschland liegt, was wiederum eine Anwendbarkeit deutschen Strafrechts ermöglicht. Dennoch handelt es sich in Bezug auf andere („typische“) Äußerungs- und Verbreitungsdelikte um eine schlagkräftige Argumentation.

sowie auf die damit verbundenen völkerrechtlichen Probleme schießt diese Ansicht über das Ziel hinaus. Würden andere Staaten diesem Modell folgen, unterlägen alle Web-Angebote einer Vielzahl von Strafrechtsordnungen. Damit würde sich – zumindest in der Theorie – für den Bereich des Internet die jeweils strengste nationale Strafrechtsordnung durchsetzen.[348] Dies kann jedoch nicht ernsthaft erwünscht sein, hält man sich beispielsweise vor Augen, welches Konfliktpotential sich alleine aus dem Spannungsverhältnis zwischen den Veröffentlichungen der liberalen westlichen Presse und den Strafrechtsordnungen einzelner islamisch-fundamentalistischer Staaten ergibt.

b) Handlungen der Mitglieder von Cracker-Gruppen

(1) Alle Mitglieder

(a) § 106 Abs. 1 UrhG[349]

Nach § 106 UrhG wird derjenige mit einer Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, der in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk, eine Bearbeitung oder eine Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt. Hierbei ist eine Gewinnabsicht nicht erforderlich.

Zur Bestimmung des Begriffs Vervielfältigung ist § 16 UrhG heranzuziehen.[350] Hierunter versteht man die Herstellung eines körperlichen Gegenstandes, der das Werk in sinnlich wahrnehmbarer Weise wiedergibt.[351] Eine Vervielfältigung liegt grundsätzlich immer dann vor, wenn ein Computerprogramm auf ein anderes Speichermedium übertragen wird. Bei der Datenübertragung per Internet wird immer eine bitgenaue Kopie der zu versendenden bzw. zu empfangenden Datei erstellt, so dass sämtliche Upload- und Downloadvorgänge eine urheberrechtlich relevante Vervielfältigung zur Folge haben. Ob das vervielfältigte Programm in seiner ursprünglichen Form, mit Veränderungen im Kopierschutz oder gar in verbesserter Form übertragen wird, ist unerheblich, da vom Schutz des § 106 UrhG auch Bearbeitungen und Umgestaltungen von Computerprogrammen erfasst werden[352]. Somit erfüllt jedes Gruppenmitglied, auf dessen Festplatte ein Programm gespeichert wird, den Tatbestand der unerlaubten Vervielfältigung i.S.v. § 106 Abs. 1 UrhG.

Nach der überwiegenden Rechtsauffassung in der Literatur[353] liegt eine Verletzung des ausschließlichen Vervielfältigungsrechts auch dann vor, wenn das Computerprogramm benutzt wird; hierbei stellt das Laden des Programms in den Hauptspeicher des Computers (Random Access Memory –

---

348 *Sieber*, Internationales Strafrecht im Internet, **NJW** 1999, S. 2067.
349 Zu Bedenken an der Verfassungsmäßigkeit der §§ 106 ff. UrhG siehe die Ausführungen in Teil 2, C. V. 2. und C. I. 1.
350 Der zivilrechtliche und der strafrechtliche Vervielfältigungsbegriff sind insoweit identisch, Schricker-*Haß*, § 106 UrhG, Rdnr. 3.
351 Vgl. **BT-Drucks.** 4/270, S. 47; Urteil des *BGH* vom 04.10.1990 (Az. I ZR 139/89 – „Betriebssystem"), **GRUR** 1991, S. 449, 453; Urteil des *BGH* vom 01.07.1982 (Az. I ZR 119/80 – „Presseberichterstattung und Kunstwerkwiedergabe II"), **GRUR** 1983, S. 28, 29; Urteil des *BGH* vom 03.07.1981 (Az. I ZR 106/79 – „Masterbänder"), **GRUR** 1982, S. 102, 103; Urteil des *BGH* vom 18.05.1955 (Az. I ZR 8/54), **BGHZ** 17, S. 266, 270.
352 Allerdings ist eine (sukzessive) Vervielfältigung von Teilen einer Datei nur strafbar, wenn jeweils urheberechtlich schutzfähige Werkteile vervielfältigt werden, vgl. Wandtke/Bullinger-*Hildebrandt*, § 106 UrhG, Rdnrn. 12 und 14 m.w.N.
353 *Ulmer/Kolle*, **GRUR Int.** 1982, S. 489 ff.; *Kindermann*, **GRUR** 1983, S. 150 ff.; *Haberstumpf*, **GRUR** 1982, S. 142 ff.; *Gravenreuth*, Juristisch relevante technische Fragen zur Beurteilung von Computer-Programmen, **GRUR** 1986, S. 720 ff.; die höchstrichterliche Rechtsprechung hat die Frage mehrfach ausdrücklich offen gelassen, so *Heymann*, **c't** 8/2000, S. 107.

RAM[354]) den urheberrechtlich relevanten Vervielfältigungsvorgang dar[355]. Somit können auch solche Fälle erfasst werden, in denen Programme direkt von CD-ROM oder Diskette ausgeführt werden, ohne dass sie zuvor auf der Festplatte gespeichert wurden.

(b) § 108a UrhG

§ 108a UrhG wurde durch das „Gesetz zur Änderung von Vorschriften auf dem Gebiet des Urheberrechts“ vom 24.06.1985[356] neu in das Urheberrechtsgesetz eingefügt, um dem wachsenden Problem der organisierten Kriminalität und Bandenkriminalität in den Bereichen der Videopiraterie und des Raubdrucks entgegenzuwirken. Im Gegensatz zu § 106 UrhG handelt es sich bei § 108a UrhG um ein Offizialdelikt, die Verfolgung bedarf daher keines Strafantrags, vgl. § 109 UrhG.

Die Norm sieht in Absatz 1 für die unerlaubte gewerbsmäßige Verwertung von urheberrechtlich geschützten Werken eine Freiheitsstrafe von bis zu fünf Jahren oder eine Geldstrafe vor. Gewerbsmäßig im Sinne der Vorschrift handelt, wer die Tatbestände der §§ 106 bis § 108 UrhG in der Absicht verwirklicht, sich durch wiederholte Begehung dieser Taten eine fortlaufende Einnahmequelle von einiger Dauer und einigem Umfang zu verschaffen.[357] Die verbotene Handlung braucht nicht die Haupteinnahmequelle zu sein, ein bloßer Nebenerwerb kann genügen.[358] Allerdings darf es sich nicht um ein ganz geringfügiges Nebeneinkommen handeln, denn dann fehlt es an dem notwendigen Umfang.[359] Eine Gewinnsucht des Täters ist nicht erforderlich, für die Absicht genügt dolus eventualis.[360]

Da die überwiegende Zahl der Cracker-Gruppen nicht aus finanziellen Motiven handelt, kommt eine Anwendung des § 108a UrhG nur bei den wenigen Gruppen in Betracht, die mit ihrer Tätigkeit Profit erzielen wollen. Daher bleibt es bei einer Strafbarkeit der Einzelpersonen nach § 106 Abs. 1 UrhG, der weite Strafrahmen des § 108a StGB kann nur in Einzelfällen ausgeschöpft werden.

(c) § 129 StGB

Fraglich ist, ob sich die Mitglieder der bis ins kleinste Detail durchorganisierten Warez-Gruppen gemäß § 129 Abs. 1 StGB der Bildung einer bzw. der Beteiligung an einer kriminellen Vereinigung strafbar machen. Die Vorschrift des § 129 StGB findet nur dann Anwendung, wenn es sich um eine im Inland bestehende Vereinigung handelt, oder wenn zumindest eine inländische (Teil-)

---

354 Das RAM ist ein volatiler Direktzugriffsspeicher für Computersysteme, bei dem die Daten in beliebiger Reihenfolge abgerufen oder eingeschrieben werden können. Teile jedes Programms, das auf einem Rechner ausgeführt wird, werden für die Dauer der Nutzung von der Festplatte in das RAM kopiert und dort zwecks schnellerem Zugriff bereitgehalten.
355 Siehe hierzu Wandtke/Bullinger-*Hildebrandt*, § 106 UrhG, Rdnr. 13 UrhG m.w.N., der sich mit gewichtigen Argumenten gegen eine Strafbarkeit in diesen Fällen ausspricht.
356 **BGBl. I** 1985, S. 1137 ff.
357 Urteil des *BGH* vom 08.11.1951 (Az. 4 StR 563/51), **BGHSt.** 1, S. 383; Urteil des *BGH* vom 02.12.1954 (Az. 3 StR 120/54), **GA** 1955, S. 212; Urteil des *Reichsgerichts* vom 05.05.1930 (Az. II 1009/29), **RGSt.** 64, S. 154; Urteil des *Reichsgerichts* vom 27.11.1923 (Az. IV 398/23), **RGSt.** 58, S. 19 ff.. Die Gewerbsmäßigkeit ist ein strafschärfendes persönliches Merkmal i.S.v. § 28 Abs. 2 StGB, Schricker-*Haß*, § 108a UrhG, Rdnr. 1.
358 Urteil des *BGH* vom 08.11.1951 (Az. 4 StR 563/51), **BGHSt.** 1, S. 383; Urteil des *BGH* vom 02.12.1954 (Az. 3 StR 120/54), **GA** 55, S. 212.
359 Vgl. Urteil des *BGH* vom 14.05.1975 (Az. 3 StR 124/75) bei *Dallinger*, **MDR** 1975, S. 725 – ergangen zu § 260 StGB (gewerbsmäßige Hehlerei).
360 Schricker-*Haß*, § 108a UrhG, Rdnr. 2 f.

Organisation besteht[361]. Demnach müsste sich zunächst ein nicht unwesentlicher Teil der Mitglieder dauerhaft in Deutschland aufhalten. § 129 Abs. 1 StGB sieht eine Freiheitsstrafe von bis zu fünf Jahren oder eine Geldstrafe vor, wenn der Zweck oder die Tätigkeit der Vereinigung darauf gerichtet sind, Straftaten zu begehen. Straftaten im Sinne des § 129 StGB sind grundsätzlich alle einen Straftatbestand erfüllenden Handlungen von einigem Gewicht[362], nicht dagegen bloße Ordnungswidrigkeiten[363]. Entscheidend ist demnach, ob es sich bei den in Serie begangenen unerlaubten Verwertungshandlungen um Straftaten von „einigem Gewicht" handelt. Im Vergleich zu den typischerweise von § 129 StGB erfassten Fällen[364] erscheinen die nebenstrafrechtlichen Delikte aus dem Urheberrechtsgesetz in einer Gesamtbewertung weitaus weniger gefährlich für den Rechtsfrieden, weshalb es durchaus vertretbar ist, die Warez-Gruppen nicht als kriminelle Vereinigungen i.S.v. § 129 StGB zu klassifizieren. Dieses Ergebnis steht überdies in Einklang mit der Rechtsprechung des *BGH*, wonach bei der Anwendung des § 129 StGB eine Begrenzung auf solche Organisationen geboten ist, die eine erhebliche Gefahr für die öffentliche Sicherheit oder für die Volksgesundheit darstellen.[365]

Sollte eine Gesamtbewertung im Einzelfall dennoch zum Ergebnis kommen, dass eine kriminelle Vereinigung vorliegt[366], ist zu beachten, dass § 129 Abs. 4 StGB ein erhöhtes Strafmaß für die Rädelsführer bzw. Hintermänner der Gruppe vorsieht.

(2) Cracker

(a) § 106 Abs. 1 UrhG

Da Cracker die Programme nicht nur modifizieren, sondern zunächst auf ihren Rechner laden und später an andere Gruppenmitglieder weiterleiten, verwirklichen sie regelmäßig den Vervielfältigungstatbestand des § 106 Abs. 1 UrhG.

(b) § 202a StGB

Die Cracker einer Gruppe machen sich in der Regel auch gemäß § 202a StGB strafbar, wenn sie sich den Programmcode einer Software zugänglich machen; z.B. zur Entfernung von Dongle-Abfragen aus dem Code[367] oder zur Analyse des Codes im Vorfeld der Entwicklung eines Umgehungsprogramms.

---

361 Schönke/Schröder-*Lenckner*, § 129 StGB, Rdnr. 4.
362 Beschluss des *BGH* vom 17.11.1981 (Az. 3 StR 221/81(s)), **NStZ** 82, S. 68.
363 Schönke/Schröder-*Lenckner*, § 129 StGB, Rdnr. 6.
364 Zu nennen sind z.B. ausländer- und fremdenfeindlich motivierte Taten, vgl. *Tröndle/Fischer*, § 129 StGB, Rdnr. 5.
365 Urteil des *BGH* vom 21.12.1977 (Az. 3 StR 427/77(s)), **BGHSt** 27, S. 325 ff.; Beschluss des *BGH* vom 04.08.1995 (Az. 2 BJs 183/91 – 3 StB 31/95), **NJW** 1995, S. 3395 ff.; Urteil des *BGH* vom 14.04.1981 (Az. 1 StR 676/80), **NStZ** 1981, S. 303 ff.
366 Nach Ansicht des Verfassers ist dies erst dann zu erwägen, wenn Fälle des § 108a UrhG vorliegen, und nachweislich wirtschaftliche Schäden von bedeutendem Umfang entstanden sind.
367 Seit 1989 entspricht es gefestigter Rechtsprechung, dass die Umgehung eines Dongles eine „Urheberrechtsverletzung" darstellt (zuletzt *OLG Düsseldorf*, Urteil vom 27.03.1997 (Az. 20 U 51/96), veröffentlicht bei *JurPC.de* unter http://www.jurpc.de/rechtspr/19980065.htm; siehe auch die ausführliche Betrachtung von *Raubenheimer*, Zunehmende Bedeutung des Hardware Locks in der jüngsten deutschen Rechtsprechung, *Wibu.de* – m.w.N.). Mangels Zustimmung des Urheberrechtsinhabers stellen die Programmveränderungen eine Verletzung des exklusiven Bearbeitungsrechts nach § 69c Nr. 2 UrhG dar.

Der Tatbestand des § 202a StGB ist verwirklicht, wenn jemand sich oder einem anderen unbefugt Daten verschafft, die nicht für ihn bestimmt sind, und die gegen unberechtigten Zugang besonders gesichert sind. Konsequenz kann eine Freiheitsstrafe von bis zu drei Jahren oder eine Geldstrafe sein. Unter den Begriff der Daten fallen auch Computerprogramme bzw. die in ihnen enthaltenen Daten.[368] Die besondere Zugangssicherung, die von § 202a Abs. 1 StGB verlangt wird, besteht in der heutzutage üblichen Kompilierung des Programmcodes. Hierbei handelt es sich um eine Art Verschlüsselung[369], die von Herstellerseite vorgenommen wird, um zu verhindern, dass der Quellcode von der Konkurrenz analysiert und kopiert wird. Nur wenn der Kopierschutz lediglich die maschinelle Herstellung von Kopien verhindern soll, und der Programmcode selbst über den Bildschirm ohne Einsatz spezieller Dekompilier-Programme für den Anwender zugänglich ist, scheidet eine Bestrafung nach § 202a StGB aus. In diesen – mittlerweile äußerst seltenen – Fällen sind die Daten unmittelbar wahrnehmbar und somit nicht besonders gegen unberechtigten Zugang gesichert.[370] Als „verschafft" gelten die Daten, sobald der Täter von ihnen – in entschlüsselter Form – durch optische bzw. akustische Wahrnehmung Kenntnis genommen hat.[371] Da der Cracker fast ausschließlich mit dem entschlüsselten Code arbeitet, liegt dieses Merkmal in der Regel unproblematisch vor.

In den meisten Lizenzvereinbarungen ist festgeschrieben, dass das Dekompilieren und Deassemblieren des jeweiligen Programms nicht gestattet ist.[372] Setzt sich der Cracker dennoch über den Willen des Herstellers hinweg, so macht er sich durch den Zugriff auf die gesicherten Daten unter Überwindung der Zugangssicherung des Ausspähens von Daten schuldig. Ein Cracker wird sich in diesem Fall nicht mit Erfolg auf § 69e UrhG (Dekompilierung) berufen können, wonach das Dekompilieren unter engen Voraussetzungen nicht vertraglich untersagt werden darf.[373]

Im Falle von Entdonglierungsmaßnahmen scheidet eine Berufung auf das Fehlerberichtigungsrecht des § 69d Abs. 1 UrhG als Rechtfertigung selbst dann aus, wenn durch ein Dongle Fehler in anderen Programmen oder bei Druckvorgängen hervorgerufen werden. Schließlich besteht die Möglichkeit, das Dongle vorübergehend vom Druckerport abzuziehen, wenn es Konflikte bei der Nutzung anderer Programme verursacht. Das *OLG Karlsruhe* hat den Gebrauch einer Software mit dem dazugehörigen Dongle als bestimmungsgemäß definiert, obwohl es in dem zu entscheidenden Fall

---

368 Schönke/Schröder-*Lenckner*, § 202a StGB, Rdnr. 3.
369 Streng genommen ist es eine Übersetzung von Quellcode in Objektcode. Die entsprechende Rückübersetzung wird als Dekompilierung bezeichnet, Schricker-*Loewenheim*, § 69e UrhG, Rdnr. 4; siehe hierzu auch Teil 2, A. IV. 2.
370 Vgl. *Schultz*, S. 119; Schönke/Schröder-*Lenckner*, § 202a StGB, Rdnr. 4.
371 Schönke/Schröder-*Lenckner*, § 202a StGB, Rdnr. 10.
372 So z.B. in den Endbenutzer-Lizenverträgen der folgenden (Standard-)Programme: *Microsoft Windows XP Professional* (Lizenzvertrag, Punkt 2, Abschnitt 8), *Microsoft Internet Explorer 6* (Lizenzvertrag, Punkt 2, Abschnitt 8), *Microsoft Office 2002* - bestehend aus *Outlook 2002, Powerpoint 2002, Word 2002* und *Access 2002* (Lizenzvertrag, Punkt 2, Abschnitt 5), *Symantec Norton Utilities 2002* (Lizenzvertrag, Punkt 1 B. – "nicht berechtigt"), *Adobe PhotoShop 7* (Lizenzvertrag, Punkt 3), *Adobe Acrobat Reader 5* (Lizenzvertrag, Punkt 3), *Realnetworks RealOne Player 2* (Lizenzvertrag, Punkt 2 a) (II)).
373 Das Vorliegen der Voraussetzungen des § 69e Abs. 1 UrhG würde die Rechtswidrigkeit der Datenausspähung entfallen lassen, vgl. Schönke/Schröder-*Lenckner*, § 202a StGB, Rdnr. 11 („unbefugt" bezieht sich auf das „allgemeine Deliktsmerkmal der Rechtswidrigkeit"); Lackner/Kühl-*Kühl*, § 202a StGB, Rdnr. 7 („Erfolgt ein Eingriff in urheberrechtlich zulässiger Weise (§§ 69a ff. UrhG), so ist er nicht unbefugt"). Nach § 69e UrhG darf das Dekompilieren zum Beispiel dann nicht untersagt werden, wenn sich jemand selbständig Informationen beschaffen will, die zur Herstellung der Interoperabilität zwischen dem dekompilierten und einem anderen Programm erforderlich sind, Schricker-*Loewenheim*, § 69e UrhG, Rdnr. 1 ff.

durch die Verwendung des Dongles zu Funktionsstörungen kam.[374] Da die Fehlerberichtigung nur dann gesetzlich gestattet wird, wenn sie ebendiesem bestimmungsgemäßen Gebrauch dient, schließt die Entfernung des Dongles eine Berufung auf das Fehlerberichtigungsrecht per se aus.[375] Ein Dongle selbst stellt also keinen Programmfehler i.S.d. § 69d Abs. 1 UrhG dar.

(c) § 303a StGB

In den Fällen, in denen Kopierschutzroutinen aus dem Programmcode entfernt oder in sonstiger Weise manipuliert werden, ist eine Veränderung von Daten gegeben, die gemäß § 303a Abs. 1, 4. Alt. StGB strafbar sein kann[376]. Eine Datenveränderung im Sinne der Vorschrift liegt vor, wenn fremde Daten einen anderen Informationsgehalt (Aussagewert) erhalten, und dadurch der ursprüngliche Verwendungszweck beeinträchtigt wird. Die Veränderung kann durch Teillöschungen, inhaltliches Umgestalten gespeicherter Daten oder Hinzufügen weiterer Daten geschehen.[377]

Problematisch wirkt das Erfordernis der Fremdheit der Daten, wenn sich diese im Herrschaftsbereich des Täters auf einem tätereigenen Datenträger befinden. Legt man jedoch bei der Klärung dieser Frage eine urheberrechtliche Betrachtungsweise zugrunde, erscheint eine weite Ausdehnung des genannten Erfordernisses vertretbar: Selbst der redliche Käufer einer Software erwirbt kein Eigentum an dem Programm, sondern lediglich ein Nutzungsrecht (Lizenz). Das eigentümerähnliche Recht, die Programmdaten nach freiem Belieben zu verändern oder zu löschen, hat ausschließlich der urheberrechtlich Berechtigte. Der Cracker – als Nutzer ohne Lizenz – erhält keinerlei Verfügungsberechtigung bezüglich Programm und Kopierschutz, weshalb die Daten für ihn fremd bleiben.

Da lediglich ein intaktes Kopierschutzsystem dem Autor bzw. dem Softwarehersteller einen wesentlichen Teil seiner Einkünfte sichern kann, hat er auch das für § 303a StGB erforderliche unmittelbare Interesse an der Unversehrtheit der Daten.

---

[374] Urteil des *OLG Karlsruhe* vom 10.01.1996 (Az. 6 U 40/95), abgedruckt in **CR** 1996, S. 341, 342; zustimmend: *Raubenheimer*, Anmerkung zum Urteil des *OLG Karlsruhe* von 10.01.1996 (a.a.O.), **CR** 1996, S. 343; ablehnend: *M. M. König*, Zur Zulässigkeit der Umgehung von Software-Schutzmechanismen, **NJW** 1995, S. 3295;

[375] So auch das *OLG Düsseldorf*, Urteil vom 27.03.1997 (Az. 20 U 51/96), **CR** 1997, S. 338, wonach „das Entdonglieren nicht dem durch § 69d Abs. 1 UrhG gesicherten bestimmungsgemäßen Gebrauch" entspreche; ebenso die Vorinstanz, *LG Düsseldorf*, Urteil vom 20.03.1996 (Az. 12 O 849/93), **CR** 1996, S. 738; *Raubenheimer*, Anmerkung zum Urteil des LG Düsseldorf vom 20.03.1996, **CR** 1996, S. 740; *ders.*, Die jüngste Rechtsprechung zur Umgehung/Beseitigung eines Dongles, **NJW-CoR** 1996, S. 174 ff.; a.A.: *M. M. König*, Zur Zulässigkeit der Umgehung von Software-Schutzmechanismen, **NJW** 1995, S. 3295; *ders.*, Anmerkung zum Urteil des LG Mannheim vom 20.01.1995, **NJW-CoR** 1995, S. 191; *F. A. Koch*, Das neue Softwarerecht und die praktischen Konsequenzen, **NJW-CoR** 1994, S. 296; Urteil des *LG Mannheim* vom 20.01.1995 (Az. 7 O 197/94), **NJW** 1995, S. 3322.

[376] Denkbar ist auch die Verwirklichung der ersten Alternative („Löschen"), vgl. *Gravenreuth*, Computerviren, Hacker, Datenspione, Crasher und Cracker, **NStZ** 1989, S. 206. In diesem Zusammenhang ist allerdings zu beachten, dass sich die Tathandlungen des § 303a StGB in vielfacher Weise überschneiden, was der erklärten Absicht des Gesetzgebers entspricht, Daten vor jeder denkbaren Beeinträchtigung umfassend zu schützen, vgl. **BT-Drucks.** 10/5058, S. 34. Löschen und Unbrauchbarmachen sind nur bestimmte Unterformen des Veränderns.

[377] Schönke/Schröder-*Stree*, § 303a StGB, Rdnr. 4.

Folglich kommt – bei einer weiten Auslegung des Datenbegriffs – eine Anwendung des § 303a Abs. 1 StGB in Betracht[378].

(d) § 17 UWG

Eine Strafbarkeit der Cracker kann sich darüber hinaus aus § 17 Abs. 2 UWG ergeben.[379] Nach § 17 Abs. 2 Nr. 1 a) UWG wird mit einer Freiheitsstrafe von bis zu drei Jahren oder mit Geldstrafe bestraft, wer sich durch Anwendung technischer Mittel zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Geschäftsbetriebs Schaden zuzufügen, ein Geschäfts- oder Betriebsgeheimnis unbefugt verschafft oder sichert. Mit anderen Worten stellt diese Alternative der Norm die mit technischen Mitteln bewirkte Ausspähung eines Geheimnisses unter Strafe. Täter kann jede Person sein, beispielsweise ein Beschäftigter des Geheimnisträgers während des Dienstverhältnisses.[380]

Beinahe alle kommerziellen Computerprogramme, sowohl Individual- als auch Standardsoftware, unterfallen dem Schutz von § 17 UWG.[381] Dies gilt unzweifelhaft für die Fälle, in denen ein Programm marktlich verwertet wird, und sein Programmcode durch Kompilierung geheimgehalten werden soll.[382] Nur wenn etwas Geheimgehaltenes praktisch zum Allgemeingut – also offenkundig – geworden ist, kann man nicht mehr von einem Geheimnis sprechen.[383] Bei der weitaus überwiegenden Zahl der kommerziellen Programme ist jedoch die Geheimhaltung des Programmcodes beabsichtigt und liegt folglich im Interesse des Herstellers. Etwas anderes gilt nur für solche Produkte, deren Quellcodes vom Hersteller oder Programmierer bewusst offengelegt werden.[384]

Ein Computer, auf dem eine Disassembler-Software oder andere Tools zur Datenanalyse installiert sind, fällt unproblematisch unter den Begriff des „technischen Mittels“ aus § 17 Abs. 2 Nr. 1 a) UWG.

---

[378] Wohl auch Hoeren/Sieber-*Bechtold*, 7.11, Rdnr. 66; zu den verfassungsrechtlichen Bedenken bezüglich einer weiten Begriffsauslegung im Strafrecht siehe Teil 2, C. I. 1.

[379] Im Zusammenhang mit § 17 UWG ist stets § 20 UWG zu beachten. Dieser bezieht sich auf die §§ 17 und 18 UWG und stellt die folgenden vier Verhaltensweisen unter Strafe: Versuch der Verleitung zu einer Tat nach §§ 17, 18 UWG durch einen Hintermann (Abs. 1, 1. Alt., vgl. HK Wettbewerbsrecht-*Kotthoff*, § 20 UWG, Rdnr. 2); Annahme des Erbietens eines Hintermannes, eine Tat nach §§ 17, 18 UWG zu begehen (Abs. 1, 2. Alt., vgl. HK Wettbewerbsrecht-*Kotthoff*, § 20 UWG, Rdnr. 3); Erbieten des Verräters, eine Tat nach §§ 17, 18 UWG zu begehen (Abs. 2, 1. Alt., vgl. HK Wettbewerbsrecht-*Kotthoff*, § 20 UWG, Rdnr. 4); Bereiterklären des Verräters zu einer Tat nach §§ 17, 18 UWG auf Ansinnen eines anderen (Abs. 2, 2. Alt., vgl. HK Wettbewerbsrecht-*Kotthoff*, § 20 UWG, Rdnr. 5). § 20 UWG sieht eine Freiheitsstrafe von bis zu zwei Jahren oder eine Geldstrafe vor.

[380] Vgl. *Baumbach/Hefermehl*, § 17 UWG, Rdnr. 25.

[381] Vgl. *Baumbach/Hefermehl*, § 17 UWG, Rdnr. 9; siehe hierzu auch oben Teil 2, C. I. 2. c).

[382] Zu den geschützten Geschäfts- und Betriebsgeheimnissen können neben dem nicht offenkundigen Quellcode die Konzeption, Algorithmen, Daten-, Ein- und Ausgabeformate, besonders wichtige Programmdaten und sonstiges technisches Know-how zählen, vgl. Wandtke/Bullinger-*Grützmacher*, § 69g, Rdnr. 29 m.w.N.

[383] Nach der Rechtsprechung liegt Offenkundigkeit dann vor, wenn eine Tatsache allgemein bekannt ist, oder jeder Interessierte sich diese Tatsache mit lauteren Mitteln und ohne größere Schwierigkeiten verschaffen kann, Urteil des *BayObLG* vom 28.08.1990 (Az. 4 St 250/89), **GRUR** 1991, S. 694, 695; Urteil des *Reichsgerichts* vom 29.11.1907 (Az. V 709/07), **RGSt** 40, S. 406, 407; Urteil des *Reichsgerichts* vom 01.11.1939 (Az. I 94/38), **GRUR** 1939, S. 733, 735; siehe auch HK Wettbewerbsrecht-*Kotthoff*, § 17 UWG, Rdnr. 7.

[384] Zur sogenannten Open-Source-Software siehe unten Teil 2. C. V. 3. (Exkurs).

Da sich die Cracker der Warez-Gruppen – anders als Industriespione – nicht zu wettbewerblichen Zwecken Kenntnis von den Betriebs- bzw. Geschäftsgeheimnissen der Softwarehersteller und Programmierer verschaffen wollen, bleibt zu prüfen, ob sie aus Eigennutz, zugunsten eines Dritten oder in Schädigungsabsicht handeln. Aus Eigennutz handelt, wer irgendeinen, nicht notwendigerweise vermögenswerten Vorteil für sich erstrebt. Es reicht aus, wenn der Täter seine Lage persönlich als gebessert empfindet, mag sie auch sachlich gar nicht gebessert sein.[385] Das Handeln zugunsten eines Dritten erfasst solche Fälle, in denen der Täter weder zu Wettbewerbszwecken, noch aus Eigennutz, noch in Schädigungsabsicht gehandelt hat.[386] Um in Schädigungsabsicht zu handeln, muss der Täter die zielgerichtete Absicht haben, den Geheimnisinhaber zu schädigen.[387] Da in beinahe allen Fällen ein Handeln aus Eigennutz vorliegen wird[388], kommt den beiden anderen subjektiven Tatbestandsmerkmalen eine untergeordnete Bedeutung zu.

An den Delikten der Cracker ist Beihilfe gemäß § 27 StGB möglich. Als Gehilfe kommt jedes andere Gruppenmitglied in Betracht, das dem Cracker vorsätzlich Hilfe geleistet hat. Vor allem in der Tätigkeit der Supplier ist eine strafrechtlich relevante Beihilfehandlung zu erblicken.[389]

(3) Packager / Ripper

Erhält ein Packager vom Cracker ein bereits modifiziertes, (re-)kompiliertes Programm und bringt dieses in ein versendungsfertiges Format, macht er sich lediglich einer unerlaubten Vervielfältigung nach § 106 UrhG strafbar. Sofern ein Packager allerdings den Programmcode entschlüsselt, um überflüssige Programmbeigaben zu entfernen, kommt auch für ihn zusätzlich eine Strafbarkeit nach den §§ 202a, 303a StGB und § 17 Abs. 2 UWG in Betracht.

(4) Kuriere

Kuriere und Siteops erfüllen eindeutig den Vervielfältigungstatbestand des § 106 Abs. 1 UrhG, indem sie die Releases der Gruppen auf zahlreichen FTP-Servern ablegen. Fraglich ist, ob sie mit den Uploads ebenfalls den Verbreitungstatbestand der Norm erfüllen.

---

385 *Baumbach/Hefermehl*, § 17 UWG, Rdnr. 20.
386 Dies ist z.B. bei einem ideologisch motivierten Täter der Fall, vgl. *Baumbach/Hefermehl*, § 17 UWG, Rdnr. 21.
387 *Baumbach/Hefermehl*, § 17 UWG, Rdnr. 22.
388 Zu den Motiven der Cracker wird immer die Erlangung von Anerkennung innerhalb der Gruppe bzw. der Warez-Szene gehören. Da die Veröffentlichung eines Cracks in der Regel nicht anonym sondern pseudonym – mit dem (Nick-) Namen des Crackers – erfolgt, wird sein Ansehen in der Szene objektiv und subjektiv erhöht.
389 Diese können sich auch selbst gemäß § 17 UWG strafbar machen, wenn sie ein noch nicht veröffentlichtes Computerprogramm für die Gruppe „organisieren". Denn auch Computerprogramme als solche (und nicht nur der in ihnen verborgene Inhalt) können als Geheimnis schutzfähig sein, sofern sie marktlich verwertet werden sollen, *Baumbach/Hefermehl,* § 17 UWG, Rdnr. 9. Steht ein Supplier im Lager des Geschädigten (i.d.R. der Softwarehersteller), ergibt sich seine Strafbarkeit aus § 17 Abs. 1 UWG, andernfalls ist § 17 Abs. 2 UWG einschlägig. Eine Strafbarkeit aus § 18 UWG (Vorlagenfreibeuterei) scheidet aus, da als Tatobjekt nur Vorlagen oder Vorschriften technischer Art in Betracht kommen, die dem Täter im geschäftlichen Verkehr vor der Tat (unbefugte Verwertung oder Mitteilung an Dritte) anvertraut wurden. Diese sind für Warez-Gruppen nicht von Interesse; wie bereits dargelegt, werden von ihnen bevorzugt lauffähige Computerprogramme veröffentlicht.

Der Verbreitungsbegriff des § 69c Nr. 3 UrhG[390], der für die Konkretisierung einer Handlung nach § 106 Abs. 1, 2. Handlungsalternative UrhG heranzuziehen ist, umfasst nur die Verbreitung von Werkstücken in körperlicher Form.[391] Demnach fallen Computerprogramme nur dann in den Anwendungsbereich der Vorschrift, wenn sie auf CD-ROMs oder sonstigen digitalen Datenträgern verbreitet werden. Die reine Datenfernübertragung von Computerprogrammen kann nach h.M.[392] nicht als Verbreitung i.S.d. § 17 UrhG gewertet werden, denn „über die Netze gehen Bits, nicht Materie"[393]. Die Verbreitung in unkörperlicher Form fällt allerdings unter die in § 15 Abs. 2 UrhG (Recht der öffentlichen Wiedergabe) geregelten Fälle. Die öffentliche Wiedergabe eines Werkes ohne Einwilligung des Berechtigten ist genau wie die Vervielfältigung und Verbreitung gemäß § 106 Abs. 1 UrhG strafbar. Da die Online-Übertragung nicht explizit in § 15 Abs. 2 UrhG aufgeführt ist, spricht man auch von einem „unbenannten Recht der öffentlichen Wiedergabe"[394].

Nach der Legaldefinition des § 15 Abs. 3 UrhG ist die Wiedergabe eines Werkes öffentlich, wenn sie für eine Mehrzahl von Personen bestimmt ist, es sei denn, dass der Kreis dieser Personen bestimmt abgegrenzt ist und sie durch gegenseitige Beziehungen oder durch Beziehung zum Veranstalter persönlich untereinander verbunden sind. Hierbei ist zu beachten, dass der Öffentlichkeitsbegriff des § 15 Abs. 3 UrhG nicht einheitlich zu verstehen ist, sondern den Besonderheiten der jeweiligen Wiedergabeart angepasst werden muss.[395]

Übertragen auf den zu untersuchenden Sachverhalt bedeutet dies, dass eine öffentliche Wiedergabe immer dann vorliegt, sobald die Dateien auf einem oder mehreren Servern abgelegt werden, wo eine Vielzahl von Personen Zugriff auf sie hat, zu welchen der Hochladende keine persönlichen Beziehungen unterhält.[396] Der Upload von Computerprogrammen ohne Einwilligung des Berechtigten kann also das Verbreitungsrecht aus § 15 Abs. 1 Nr. 2 UrhG verletzen, was bei Vorsatz zu einer Strafbarkeit gemäß § 106 Abs. 1, 3. Handlungsalternative UrhG führt.

---

[390] Dieser entspricht nach der Gesetzesbegründung der Verbreitung gemäß § 17 UrhG, Amtl. Begr. **BT-Drucks.** 12/4022, S. 11; hierunter versteht man wiederum Inverkehrbringen und Anbieten gegenüber der Öffentlichkeit, Wandtke/Bullinger-*Grützmacher*, § 69c UrhG, Rdnrn. 25-27.

[391] Vgl. Amtl. Begr. **BT-Drucks.** 4/270, S. 47; Urteil des *BGH* vom 23.02.1995 (Az. I ZR 68/93 – „Mauerbilder"), **GRUR** 1995, S. 673, 676; Urteil des *BGH* vom 15.05.1986 (Az. I ZR 22/84 – „Videofilmvorführung"), **GRUR** 1986, S. 742, 743; Urteil des *BGH* vom 16.06.1971 (Az. I ZR 120/69 – „Konzertveranstalter"), **GRUR** 1972, S. 141; Wandtke/Bullinger-*Heerma*, § 17 UrhG, Rdnr. 5; Schricker-*Loewenheim*, § 17 UrhG, Rdnr. 4. Die zitierten Quellen beziehen sich zwar auf § 17 UrhG, beachte jedoch die vorige Fußnote.

[392] *Waldenberger,* Zur zivilrechtlichen Verantwortlichkeit für Urheberrechtsverletzungen im Internet, **ZUM** 1997, S. 176, 178; Schricker-*Loewenheim*, § 69c UrhG, Rdnr. 25; *ders.*, **GRUR** 1996, S. 830, 835; Hoeren/Sieber-*Gahrau*, 7.1, Rdnr. 77; *Dreier* in *Schricker*, Urheberrecht auf dem Weg in die Informationsgesellschaft, S. 128 f.; *Becker*, ZUM 1995, S. 231, 244; Wandtke/Bullinger-*Grützmacher*, § 69c UrhG, Rdnr. 29; a.A.: Fromm/Nordemann-*Vinck*, § 69c, Rdnr. 5; *Mäger*, **CR** 1996, S. 524, der für eine extensive Auslegung der §§ 17 Abs. 2, 69c Nr. 3 UrhG plädiert.

[393] Hoeren/Sieber-*Gahrau*, 7.1, Rdnr. 77.

[394] *Waldenberger,* Zur zivilrechtlichen Verantwortlichkeit für Urheberrechtsverletzungen im Internet, **ZUM** 1997, S. 178; Schricker-*Loewenheim*, § 69c UrhG, Rdnr. 25; *Dreier* in *Schricker*, Urheberrecht auf dem Weg in die Informationsgesellschaft, S. 133 f.

[395] *J. Schneider,* Urheberrechtsverletzungen im Internet bei Anwendung des § 5 TDG, **GRUR** 2000, S. 970.

[396] Bereits zwei Nutzer können eine „Mehrzahl von Personen" i.S.d. § 15 Abs. 3 UrhG bilden, vgl. Fromm/Nordemann-*Nordemann*, § 15 UrhG, Rdnr. 4; Wandtke/Bullinger-*Heerma*, § 15 Rdnr. 22; der *BGH* hat diese Frage in seinem Urteil vom 11.07.1996 (Az. I ZR 22/94 – „Rundfunkempfang im Krankenhauszimmer"), **GRUR** 1996, S. 875, 876, angesprochen, jedoch nicht abschließend dazu Stellung genommen. Ein Angebot an Einzelpersonen ist im Rahmen des § 15 Abs. 3 UrhG nicht ausreichend, vgl. das Urteil des *BGH* vom 13.12.1990 (Az. I ZR 21/89 – „Einzelangebot"), **GRUR** 1991, S. 316, 317 - ergangen zu § 17 Abs. 1 UrhG.

Fraglich ist die strafrechtliche Beurteilung der Handlungen von Kurieren, wenn keine kompletten Programme, sondern nur Umgehungsprogramme (Cracks oder Keymaker) von ihnen verbreitet werden.[397] Denn hierbei handelt es sich um eigens hergestellte Programme, die meist keinen Code des Originalprogramms enthalten, weshalb eine Bestrafung der Kuriere wegen Vervielfältigung oder öffentlicher Wiedergabe dieser Umgehungsprogramme aus § 106 Abs. 1 UrhG ausscheidet.[398] Denkbar ist in diesen Fällen nur noch Anstiftung oder Beihilfe zu einer strafbaren Verwertungshandlung desjenigen, der das Umgehungsprogramm ausführt.[399]

Sofern die Kuriere widerrechtlich in fremde Computersysteme eindringen, um diese als Ablageorte für Raubkopien zu missbrauchen, kommt außerdem eine Strafbarkeit gemäß §§ 202a StGB (Ausspähen von Daten), 303a StGB (Datenveränderung), 303b StGB (Computersabotage) und § 17 UWG (Verrat von Geschäfts- oder Betriebsgeheimnissen) in Betracht.

c) Handlungen der Betreiber von Webseiten und permanenten FTP-Servern

(1) Strafrechtliche Verantwortlichkeit

Der Gesetzgeber hat 1997 mit dem Informations- und Kommunikationsdienstegesetz (IuKDG)[400] eine Regelung über die Verantwortlichkeit für Informationen geschaffen, die im Internet angeboten werden. Das IuKDG ist ein Artikelgesetz, welches in seinen ersten drei Artikeln (Teledienstegesetz – TDG, Teledienstedatenschutzgesetz – TDDSG und Signaturgesetz – SigG) neue Regelungsmaterien enthielt und in sechs weiteren Artikeln bereits bestehende Regelungsbereiche anpasste – unter anderem das Strafgesetzbuch, das Ordnungswidrigkeitengesetz, das Gesetz über die Verbreitung jugendgefährdender Schriften und das Urheberrechtsgesetz.

Das Teledienste- und das Teledienstedatenschutzgesetz (= Art. 1 und 2 IuKDG) sind in Ansehung der sogenannten E-Commerce-Richtlinie[401] durch Art. 1 und 3 des Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (EEG) vom 09.11.2001 wesentlich überarbeitet und ergänzt worden: Die §§ 8-11 TDG regeln nunmehr die zivilrechtliche, strafrechtliche und verwaltungsrechtliche Verantwortlichkeit der Betreiber von Telediensten (auch

---

397 Zu den Begriffen siehe oben Teil 2, A. IV. 2. b) (2); die Frage, ob Cracks und Keymaker als Computerprogramme selbst urheberrechtlichen Schutz genießen, muss verneint werden, denn ein Schutz für Programme, die einzig und alleine dazu dienen, die Durchsetzung der Verwertungsrechte der Urheber bzw. Rechtsinhaber zu unterbinden, ist unvereinbar mit der ratio legis des UrhG. Ein Hinweis auf die nicht vorhandene Schutzfähigkeit der Umgehungsprogramme liefert insbesondere § 69f Abs. 2 UrhG: Danach kann der Rechtsinhaber verlangen, dass solche Mittel vernichtet werden, die allein dazu bestimmt sind, die unerlaubte Beseitigung oder Umgehung technischer Programmschutzmechanismen zu erleichtern. Etwas anderes gilt jedoch für CD-Brennprogramme, die in der Lage sind, gewisse Kopierschutzmechanismen von Software-CD-ROMs zu überlisten. Denn diese Programme manipulieren nicht den geschützten Programmcode, sondern bewirken lediglich, dass der CD-Brenner in einem Modus arbeitet, der den Kopierschutz überwindet.

398 Allerdings muss ein Cracker den Programmcode des Originalprogramms entschlüsseln und analysieren, um einen Crack oder Keymaker zu programmieren. Insofern wird der Herstellungsprozess immer eine oder mehrere strafbare Handlungen enthalten, die von den §§ 202a StGB und 17 Abs. 2 UWG erfasst werden – siehe oben Teil 2, C. I. 3. b) (2) (b) und (d).

399 Siehe unten Teil 2, C. I. 3. d) (2); allerdings werden nur in Ausnahmefällen die Anforderungen an den erforderlichen Anstifter- bzw. Gehilfenvorsatz erfüllt sein.

400 Das IuKDG wird häufig auch als Multimediagesetz bezeichnet.

401 Richtlinie des Europäischen Parlaments und des Rats vom 08.06.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs im Binnenmarkt, Richtlinie 2000/31/EG, **ABl. EG** Nr. L 178/1 vom 17.07.2000, S. 1 ff.

„Diensteanbieter“) und ersetzen den in der Auslegung umstrittenen § 5 TDG a.F., der am 01.08.1997 durch Art. 1 IuKDG geschaffen wurde.

Gemäß § 3 Nr. 1 TDG ist unter dem Begriff des Diensteanbieters „jede natürliche oder juristische Person“ zu verstehen, „die eigene oder fremde Teledienste zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt“. Unter den Begriff des Teledienstes fallen gemäß § 2 Abs. 1 TDG alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind, und denen eine Übermittlung mittels Telekommunikation zugrunde liegt. Hierzu gehören nach Abs. 2 insbesondere Angebote im Bereich der Individualkommunikation (z.B. Telebanking, Datenaustausch), Angebote zur Information oder Kommunikation, soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht (Datendienste, z.B. Verkehrs-, Wetter-, Umwelt- und Börsendaten, Verbreitung von Informationen über Waren und Dienstleistungsangebote), Angebote zur Nutzung des Internets oder weiterer Netze, Angebote zur Nutzung von Telespielen sowie Angebote von Waren und Dienstleistungen in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit.

Die Betreiber von Homepages bzw. FTP-Seiten schaffen Angebote zum Datenaustausch, indem sie sowohl die Informationen als auch die Gestaltung ihrer Seiten festlegen und diese ins Netz stellen, weshalb ihre Tätigkeit als Bereithaltung eines eigenen Teledienstes zu qualifizieren ist.[402] Wer also in Eigenregie Webseiten oder FTP-Server einrichtet, von denen Raubkopien heruntergeladen werden können, ist als sogenannter Content Provider gemäß § 8 Abs. 1 TDG für die eigenen Informationen seiner Seite in vollem Umgang strafrechtlich verantwortlich.

Vor der Umsetzung der E-Commerce-Richtlinie gab es Tendenzen in Literatur und Rechtsprechung, wonach die Verantwortlichkeitsregeln des TDG nicht auf den Bereich des Urheberrechts angewendet werden sollten.[403] Die herrschende Meinung[404] sah hingegen in den Verantwortlichkeitsregelungen des TDG zu Recht vorgeschaltete „Filter“ für alle Rechtsgebiete[405]. Mit der Neufassung des TDG dürfte sich dieser Streit erledigt haben. Die neue Vorschrift des § 11 TDG gilt eindeutig auch für urheberrechtlich geschützte Werke, denn im Gegensatz zu dem in § 5 Abs. 2 TDG a.F. verwendeten Begriff der „Inhalte“ werden von § 11 TDG nunmehr „Informationen“ in einem weit verstandenen Sinn erfasst[406].

---

402 Vgl. *Flechsig/Glaser*, **CR** 1998, S. 354 – für die Betreiber von Webseiten.

403 z.B. *Schaefer/Rasch/Braun*, **ZUM** 1998, S. 454 f.; *Waldenberger*, Teledienste, Mediendienste und die „Verantwortlichkeit“ der Anbieter, **MMR** 1998, S. 127; *Lehmann*, **CR** 1998, S. 232; *Heghmanns*, **JA** 2001, S. 78, wonach § 5 TDG a.F. kein Vorfilter, sondern ein Strafausschließungsgrund sei, der seine Berechtigung nur für das Zivilrecht, aber nicht für das Strafrecht habe; *LG München* I, das in seinem Urteil vom 17.11.1999 (Az. 20 Ns 465 Js 173158/95), **NJW** 2000, S. 1051, § 5 TDG a.F. als schuldbegrenzende Sondervorschrift verstand, vgl. *Kühne*, **NJW** 2000, S. 1004; *OLG München*, Urteil vom 08.03.2001 (Az. 29 U 3282/00), **MMR** 2002, S.375 ff.

404 Stellvertretend : *Sieber*, Verantwortlichkeit im Internet, S. 114 ff.; *Gounalakis/Rhode*, **NJW** 2000, S. 2169. Die gegenteilige Ansicht lässt sich weder mit dem Wortlaut noch mit dem Gesetzeszweck vereinbaren. Dass das TDG seit jeher als vorgelagerter „Filter“ – auch vor der (neben-)strafrechtlichen Prüfung – anzusehen ist, ergibt sich unter anderem aus der Begründung des Regierungsentwurfes (**BT-Drucks.** 13/7385, S. 20) und der Stellungnahme des *Bundesrates* zum TDG (**BT-Drucks.** 13/7385, 51).

405 Hierunter fällt unter anderem das Deliktsrecht als eines der wichtigsten Anwendungsgebiete, was auch die (zivilrechtliche) Haftung für schuldhafte Urheberrechtsverletzungen einschließt, *Decker*, **MMR** 1999, S. 8.

406 *Waldenberger*, Anm. zum Urteil des *OLG München* vom 08.03.2001 (Az. 29 U 3282/00), **MMR** 2001, S. 379; *Hoeren*, Anm. zum Urteil des *OLG München* vom 08.03.2001 (Az. 29 U 3282/00), **MMR** 2001, S. 380.

Die Verantwortlichkeitsregelungen des TDG sind somit auf Tatbestandsebene platziert.

(2) Anbieten von Raubkopien

Nicht nur die Verbreitung in unkörperlicher Form, sondern auch das Bereithalten bzw. Zur-Verfügung-Stellen von urheberrechtlich geschützten Daten ist als öffentliche Wiedergabe gemäß § 15 Abs. 2 UrhG einzustufen.[407] Soweit der Täter mit Vorsatz und ohne Genehmigung bzw. Einwilligung des Rechtsinhabers handelt, kann er nach § 106 Abs. 1, 3. Handlungsalternative UrhG bestraft werden.[408]

Bei FTP-Servern wird der Tatbestand der öffentlichen Wiedergabe jedoch nur dann erfüllt sein, sofern die bereitgestellten Raubkopien auch von Personen heruntergeladen werden können, zu denen der Betreiber des Servers keine persönliche Beziehung unterhält, § 15 Abs. 3 UrhG. Dies wird bei einem Public-FTP-Server immer der Fall sein, allerdings nicht, wenn der Täter nur temporär einen FTP-Server auf seinem Rechner einrichtet, um gezielt mit persönlich bekannten Einzelpersonen Software zu tauschen.

Ähnlich verhält es sich mit öffentlichen und passwortgeschützten Webseiten. Während erstere eindeutig unter den Tatbestand der öffentlichen Wiedergabe subsumiert werden können, sind die passwortgeschützten Seiten davon ausgenommen, sofern nur persönliche Bekannte des Betreibers Zugang zu den Informationen hinter der Passwortsperre haben.

Anstiftung zur Vervielfältigung scheidet aus, weil der öffentlich Wiedergebende gar nicht weiß, ob und wen er i.S.v. § 26 StGB zum Download „bestimmt", ihm folglich der hinreichend konkretisierte Vorsatz bezüglich einer anzustiftenden Person fehlt.[409]

Anders als die freien Downloadangebote erfüllt der gewerbsmäßige Handel mit Warez-CDs über Webseiten immer den Tatbestand des § 108a UrhG. Eine Strafbarkeit von Profit-Pirates, die Plagiate oder Compilation-CDs feilbieten, die geschützte Kennzeichen tragen, kann sich ferner aus den §§ 142 Abs. 1 Nr. 1 i.V.m. Abs. 2 PatG[410], 143 MarkenG[411] und 4 UWG[412] ergeben.

(3) Anbieten von Umgehungsprogrammen und Registrierungsinformationen

Das Bereitstellen von Cracks, Keymakern, Registrierungscodes oder Seriennummern ohne die dazugehörigen Programme zum freien Download ist nur strafbar, wenn hierin eine Teilnahme an einem Delikt des Herunterladenden liegt (§ 106 Abs. 1 UrhG, §§ 26 bzw. 27 StGB). Der Besitz und das Vervielfältigen von Umgehungsprogrammen alleine ist nicht strafbar, was sich unter anderem aus

---

407 *J. Schneider,* Urheberrechtsverletzungen im Internet bei Anwendung des § 5 TDG, **GRUR** 2000, S. 970; Schwerdtfeger-*Kreuzer*, S. 200; Wandtke/Bullinger-*Heerma*, § 15, Rdnr. 17.
408 Schwerdtfeger-*Kreuzer*, S. 292.
409 *Heghmanns*, **JA** 2001, S. 72; etwas anders gilt, wenn sich das Angebot an einen individuell bestimmbaren Personenkreis richtet, was jedoch bei privaten FTP-Servern und Web-Accounts der Fall sein dürfte, vgl. Schönke/Schröder-*Cramer*, § 26, Rdnr. 14.
410 Siehe hierzu oben Teil 2, C. I. 2. a).
411 Siehe hierzu oben Teil 2, C. I. 2. b).
412 Siehe hierzu oben Teil 2, C. I. 2. c).

der gesetzlichen Wertung des § 69f Abs. 2 UrhG ergibt, der eine abschließende Regelung zu den Umgehungsprogrammen trifft.

(4) Bereitstellen von Release-Informationen

Auch die Betreiber von schlichten Release-Info-Seiten können sich nur als Teilnehmer an den späteren Taten ihrer Seitenbesucher strafbar machen. Ob der notwendige Gehilfen- bzw. Anstiftervorsatz des Seitenbetreibers gegeben ist, und ob eine Hilfeleistung bzw. das Hervorrufen eines Tatentschlusses bewirkt wird, hängt maßgeblich von der Art der verbreiteten Informationen und von der Gestaltung der jeweiligen Seite ab. So versuchte der Betreiber der bekanntesten Release-Info-Seite *iSONEWS*, ein aus dem US-Bundesstaat Virginia stammender College-Student, mit ausgewählten Maßnahmen, sich den Vorwürfen des „contributory copyright infringement" zu entziehen.[413] Zum einen wurden aus den zum Download angebotenen NFO-Dateien alle Registrierungsinformationen entfernt. Zum anderen gab es 15 Foren-Moderatoren, die regelmäßig solche Forumsbeiträge löschten, die Anfragen nach bzw. Hinweise zu Downloadmöglichkeiten für Raubkopien enthielten.

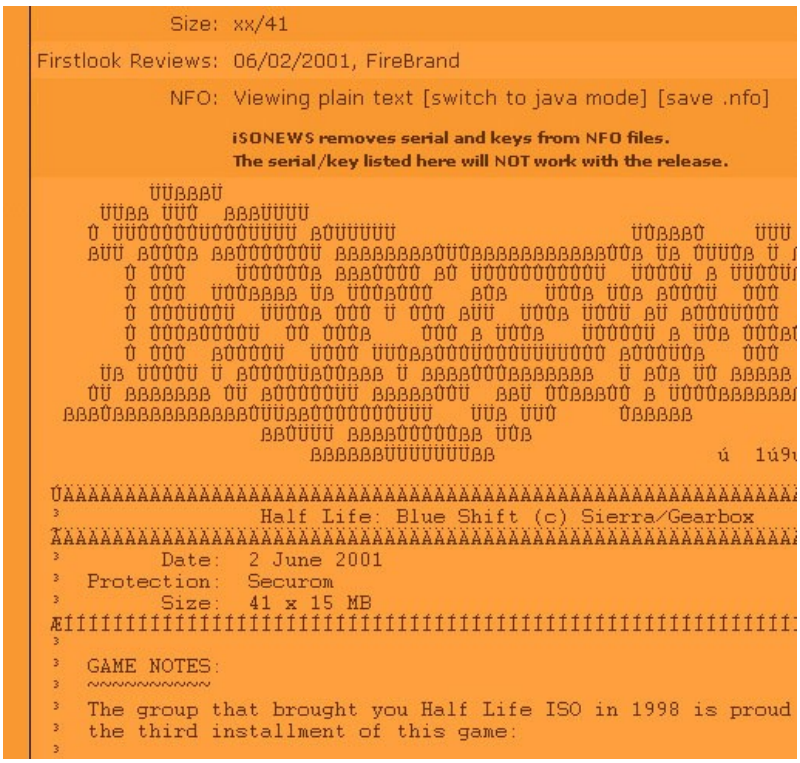


Abbildung 73 – Hinweis der Betreiber von *iSONEWS*

---

[413] In den USA findet seit einiger Zeit ein Rechtsstreit zwischen *iSONEWS* und der *SEGA Corporation* statt. Nach Einschätzung der von *iSONEWS* beauftragten Anwältin sieht *SEGA* im Betrieb des Forums Beihilfe zu Urheberrechtsverletzungen – **Wired News** vom 04.10.2000, http://www.wired.com/news/technology/0,1282,39218,00.html.
Die Seite http://www.isonews.com wurde mittlerweile von den US-Bundesbehörden geschlossen, allerdings nicht wegen des Vorwurfs der Beihilfe zu unerlaubten Verwertungshandlungen („contributory copyright infringement"), sondern weil der Betreiber über seine Seite auch sogenannte Mod-Chips verkaufte. Mod-Chips sind elektronische Bauteile, die in Spielekonsolen wie die *SONY Playstation* oder *Microsoft Xbox* eingelötet werden und die Geräte unter anderem dahingehend modifizieren, dass sie neben den gekauften Spielen auch selbstgebrannte Spiele-CDs oder DVDs akzeptieren.

Das reine Auflisten von Releasenamen und –daten ist demnach straflos, währenddessen das zusätzliche Veröffentlichen von „unzensierten“ NFO-Dateien regelmäßig in den strafrechtlich relevanten Bereich fallen dürfte.

(5) Haftung für (Hyper-)Links

Auf einschlägigen Webseiten finden sich häufig auch Hyperlinks zu anderen Warez-Seiten, auf denen Raubkopien verbreitet werden. Fraglich ist daher, inwieweit das Setzen von Links zu einer strafrechtlichen Verantwortlichkeit des Homepage-Betreibers führen kann. Hyperlink-Verfasser wurden in Deutschland bislang grundsätzlich mit Zugangsanbietern (Access-Providern) gleichgesetzt, da sie ebenfalls eine technische Vermittlung zu fremden Inhalten ermöglichen. Die strafrechtliche Beurteilung der Verantwortlichkeit für rechtswidrige Informationen auf den „verlinkten“ Seiten richtet sich folglich nach den §§ 8 ff. TDG[414]:

Liegt eine reine Zugangsvermittlung vor, ist der Link-Setzer gemäß § 9 Abs. 1 TDG von der strafrechtlichen Verantwortlichkeit ausgenommen, sofern er die Übermittlung nicht veranlasst, den Adressaten der übermittelten Information nicht ausgewählt und die übermittelten Informationen nicht ausgewählt oder verändert hat. Das Herstellen eines Links im Sinne eines Hinweises auf Angebote Dritter ist selbst ebenso wenig eine urheberrechtlich relevante Nutzungshandlung wie der Hinweis auf weiterführende Literatur in einem wissenschaftlichen Aufsatz. Die eigentliche Nutzung erfolgt erst durch denjenigen, der dem Hinweis nachgeht.[415]

Soweit Links jedoch Bestandteile von eigenen Botschaften sind, wenn sich also der Hyperlink-Verfasser mit dem Link die Inhalte der verknüpften Seite geistig zu eigen macht, kommen die Regeln über die eigenen Inhalte zur Anwendung (§ 8 Abs. 1 TDG). Zwar ist im Gesetzeswortlaut nur von „eigenen Informationen“ die Rede, doch den Gesetzesmaterialien zum TDG[416] lässt sich entnehmen, dass unter eigenen Inhalten nicht nur selbst hergestellte Inhalte zu verstehen sind, sondern auch von Dritten hergestellte Inhalte, die sich der Anbieter zu eigen macht.[417] Dies wird bei sogenannten Inline-Links besonders deutlich, bei denen es dem Leser kaum oder gar nicht auffällt, dass er bereits eine fremde Internetseite aufgerufen hat, weil sie in einem Rahmen (Frame) erscheint, der noch zu der Seite gehört, auf der er den Link gefunden hat. Gleiches gilt, wenn der Anbieter die fremde Seite zur Ergänzung seines eigenen Angebots verwendet, welches ohne die zusätzliche Information unvollständig bleiben würde.[418]

Für die Verantwortlichkeit nach § 8 Abs. 1 TDG ist weiterhin erforderlich, dass der Täter in Kenntnis der näheren Umstände handelt. Nach dem Urteil des *AG Berlin-Tiergarten* vom 30.06.1997[419] im sogenannten Radikal-Fall macht sich nur derjenige strafbar, der per Link auf eine Seite mit

---

414 Auch die Neufassung des TDG enthält keine klaren Regelungen zur Haftung von Hyperlinks, aber es spricht nichts dagegen, wie bisher eine Analogie zum Zugangsanbieter vorzunehmen.
415 Hoeren/Sieber-*Lütje*, 7.2, Rdnr. 168.
416 **BT-Drucks.** 13/7385 vom 09.04.1997, S. 19 f.
417 Zu den Begrifflichkeiten: Vor der Umsetzung der E-Commerce-Richtlinie enthielt das TDG in § 5 a.F. den Begriff der Inhalte, der mittlerweile durch den weiteren Begriff der Informationen ersetzt wurde.
418 Vgl. das Urteil des *LG Lübeck* vom 24.11.1998 (Az. 11 S 4/98), **CR** 1998, S. 650.
419 Urteil des *AG Berlin Tiergarten* vom 30.06.1997 (Az. 260 DS 857/96), zu finden bei *Netlaw.de* unter http://www.netlaw.de/urteile/agb_01.htm.

rechtswidrigem Inhalt verweist, wenn er auch weiß, dass dort ein rechtswidriger Inhalt vorhanden ist. Die Angeklagte, die eine Webseite mit politischen Inhalten ins Web gestellt hatte, wurde schließlich freigesprochen, weil sie den umstrittenen Link gesetzt hatte, bevor die rechtswidrigen Inhalte auf der verlinkten Seite abgelegt wurden. Eine Strafbarkeit durch Unterlassen – sie hätte verpflichtet sein können, die Links fortwährend zu überprüfen – wurde abgelehnt, da kein pflichtwidriges bzw. gefahrerhöhendes Vorverhalten (Ingerenz) nachzuweisen war, welches eine solche Pflicht begründet hätte.

Ob sich der Hyperlink-Verfasser dem Vorwurf der täterschaftlichen Begehung der durch die Zielseiten verwirklichten Straftat oder der Teilnahme hieran in Form der Beihilfe aussetzt, ist eine Abwägungsfrage im Einzelfall. Indizien hierfür können die optische Gestaltung des Links, seine thematische Inbezugnahme zum eigenen Angebot sowie die Elemente und der Inhalt der eigenen Stellungnahme sein, die sich auf die Zielseiten beziehen.[420]

Um sich einer strafrechtlichen Verantwortlichkeit zu entziehen, folgen die Ersteller von Homepages deshalb immer häufiger dem Expertenrat[421] und bringen in der Link-Sektion ihrer Webseite Hinweise an, durch die sie sich ausdrücklich von den fremden Inhalten der verlinkten Seiten distanzieren.[422]

Die derzeitige Rechtsprechung[423] zur Verantwortlichkeit von Hyperlink-Verfassern führt zu befriedigenden Ergebnissen. Beinahe auf jeder Homepage findet sich eine Link-Sammlung, die Verweise zu den unterschiedlichsten Webseiten enthält. Vor allem bei großen Seiten ist man nicht in der Lage, den kompletten Inhalt zu überprüfen. Hinter einer verlinkten Adresse liegen oft Hunderte von Einzelseiten – auf sogenannten tieferen Linkebenen – deren Inhalt sich erfahrungsgemäß ständig verändert. Um den Rahmen der Verantwortlichkeit nicht ausufern zu lassen, ist daher eine Beschränkung der für das „Zueigenmachen" in Frage kommenden Inhalte auf die sogenannte erste Linkebene unabdingbar.[424] Eine Einbeziehung weiterer Linkebenen würde dazu führen, dass der Verfasser eines Hyperlinks unter Umständen mehrere Wochen damit beschäftigt wäre, sämtliche Inhalte der verlinkten und der darunterliegenden Seiten zu überprüfen, wenn er sichergehen möchte, keine rechtswidrigen Inhalte anzubieten. Hinzu kommt schließlich, dass dem Laien die korrekte Beurteilung der entsprechenden Inhalte bezüglich ihrer Rechtmäßigkeit häufig äußerst schwer fallen dürfte.

Auch bei Warez-Seiten führt diese Rechtsprechung nicht zu unbilligen Ergebnissen, denn wenn der Sinn einer Seite ausschließlich oder überwiegend darin besteht, fremde Download-Angebote in Form von Hyperlinks zu vermitteln, kann sich der Betreiber nicht glaubhaft von diesen Angeboten distan-

---

420 *Flechsig/Glaser,* **CR** 1998, S. 358.
421 z.B. *Luckhardt*, Kennzeichen DE, **c't** 18/1999, S. 123.
422 Dass dies nicht immer zutreffend gelingt, zeigen die Beispiele bei Teil 2, A. VII. 1.
423 Stellvertretend: Urteil des *LG Lübeck* vom 24.11.1998 (Az. 11 S 4/98), abgedruckt in **CR** 1998, S. 650. Die Kammer hat danach unterschieden, ob sich der Link-Ersteller die fremde Seite „geistig zu Eigen" macht oder nicht. Das *LG* vertrat unter Hinweis auf § 5 Abs. 3 TDG a.F. die Auffassung, dass aufgrund der Veränderbarkeit dieser fremden Inhalte deren ständige Überprüfung auf rechtswidrige Inhalte durch den Linkenden rechtlich nicht zumutbar sei. Außerdem werde dies vom Internet-Benutzer typischerweise auch nicht erwartet.
424 Eine abweichende Auffassung vertrat das *LG Hamburg* im Urteil vom 12.05.1998 (Az. 312 O 85/98), **NJW-CoR** 1998, S. 302 f.. Danach traf den Hyperlink-Verfasser die volle Verantwortlichkeit für die Inhalte sämtlicher verlinkter und auch darunterliegender Seiten.

zieren, selbst wenn er einen Disclaimer[425] vor sein Angebot „schaltet". Er macht sich diese Inhalte dergestalt zu eigen, dass sie bedenkenlos wie eigene Inhalte gewertet werden können.

d) Handlungen der Endnutzer von Raubkopien („Leecher" und „Trader")

(1) Herunterladen oder Hochladen von Raubkopien

Wie bereits ausgeführt wurde, findet immer dann, wenn Raubkopien herunter- oder hochgeladen werden, eine strafbare Vervielfältigung i.S.d. § 106 Abs. 1 UrhG statt. Hierbei ist es gleichgültig, ob eine Datei aus einer Newsgroup, aus dem IRC, von einem FTP-Server, einem anderen Nutzer oder einer WWW-Seite stammt. Ort der Vervielfältigung ist entweder der Rechner des Täters (beim Download) oder der Zielrechner eines Datentransfers (beim Upload), während der Handlungsort immer beim Täter – „an der Tastatur" – liegt.

Im Einzelfall kann es berechtigte Zweifel am Vorsatz des Täters geben, denn oftmals ist eine Unterscheidung zwischen urheberrechtsfreier Software und Raubkopien für ihn nicht möglich. Dies gilt vor allem für Homepages, auf denen beide Arten von Software kommentarlos nebeneinander zum Download angeboten werden. Da die Strafbestimmungen des UrhG neben vorsätzlichem auch rechtswidriges und schuldhaftes Handeln verlangen, lässt ein Irrtum über die Einordnung des Programms als Public Domain bzw. Free- oder Shareware im Regelfall aufgrund einer analogen Anwendung von § 16 StGB den Schuldvorwurf und damit die Strafbarkeit entfallen; der Täter erliegt einem sogenannten Erlaubnistatbestandsirrtum.[426] Nur wenn der Herunterladende weiß, dass es typischerweise keine Vollversion des entsprechenden Programms zum freien Download geben kann, hat er den für § 106 UrhG erforderlichen Vorsatz.

(2) Herunterladen und Benutzen vom Umgehungsprogrammen

Der bloße Download von Umgehungsprogrammen ist nicht strafbar. Fraglich ist, ob das Modifizieren eines Programms mit einem Crack oder Patch eine strafrechtlich relevante Handlung darstellt. Hierbei wird der Crack in das Verzeichnis des zu verändernden Programms kopiert und durch Doppelklicken ausgeführt. Nach Sekundenbruchteilen ist der Programmcode der „Zielanwendung" verändert. Da bei dieser Vorgehensweise der Programmcode für den Raubkopierer nicht einsehbar wird, scheidet eine Strafbarkeit nach den §§ 202a StGB und 17 Abs. 2 UWG aus.

Zivilrechtlich betrachtet, liegt mangels Zustimmung des Urheberrechtsinhabers wegen Verletzung des exklusiven Bearbeitungsrechts aus § 69c Nr. 2 UrhG eine Urheberrechtsverletzung vor. Sieht man in der Bearbeitung eine Vervielfältigung des Originalwerkes in veränderter Form[427], wird man bereits über diese „Konstruktion" zu einer Strafbarkeit nach § 106 UrhG kommen.

---

425 Siehe oben Teil 2, A. VII. 1.
426 Hoeren/Sieber-*Sieber*, 19, Rdnr. 457 – die zivilrechtliche Verpflichtung zur Leistung von Schadensersatz wegen (fahrlässiger) Urheberrechtsverletzung nach § 97 Abs. 1 UrhG bleibt davon jedoch unberührt.
427 Vgl. Schricker-*Loewenheim*, § 23 UrhG, Rdnr. 6.

Sofern abweichend hiervon nicht bereits im Cracken das unerlaubte Herstellen eines Vervielfältigungsstückes gesehen wird, wird spätestens mit dem Aufruf des modifizierten Programms eine strafbare Vervielfältigungshandlung vorgenommen.[428]

Je nachdem, wie das jeweilige Umgehungsprogramm auf den Code des veränderten Programms einwirkt, ist darüber hinaus eine Strafbarkeit des Ausführenden wegen Datenveränderung gemäß § 303a Abs. 1, 1. oder 4. Alt. StGB gegeben.[429]

Nutzt eine Person ein Werk, nachdem sie technische Schutzmaßnahmen oder Rechteinformationen entfernt hat, wird darin mitunter auch ein Computerbetrug zu Lasten des Programmanbieters i.S.d. § 263a StGB gesehen.[430] Ebenso kann ein Erschleichen von Leistungen i.S.d. § 265a Abs. 1, 1. Alt. StGB vorliegen.[431]

(3) Herunterladen und Verwenden von illegalen Registrierungsinformationen

Wie das Herunterladen von Umgehungsprogrammen ist auch das Herunterladen von Registrierungsinformationen nicht mit Strafe bedroht. Schwieriger ist die strafrechtliche Beurteilung der unautorisierten Verwendung von Registrierungsinformationen. Mit dem Eintragen einer fremden oder rechtswidrig generierten Seriennummer in ein Programm wird kein unerlaubtes Vervielfältigungsstück hergestellt. Denn hierbei wird der Programmcode nicht verändert oder in sonstiger Weise bearbeitet, gehört es doch zur bestimmungsgemäßen Nutzung des Programms, dass Registrierungsinformationen in die dafür vorgesehenen Felder eingetragen werden. Der Unterschied liegt lediglich in der Herkunft der Informationen.

Da mangels Datenveränderung auch der weit gefasste § 303a StGB ausscheidet, kann sich eine Strafbarkeit allenfalls aus § 106 UrhG ergeben, wenn der Nutzer das unlauter registrierte Programm startet, also im Hauptspeicher vervielfältigt[432]. Dieser Vorgang ist nicht von der Einwilligung des Berechtigten i.S.v. § 106 UrhG gedeckt. Diese erstreckt sich selbstverständlich nur auf die Vervielfältigung der unberührten Demo-Version oder einer lizenzierten Programmversion und nicht auf die Vervielfältigung einer illegal registrierten Version.

---

428 Vorausgesetzt, man folgt der h.M. in der Literatur, vgl. Fn. 353.
429 Wohl auch Hoeren/Sieber-*Bechtold*, 7.11, Rdnr. 66; zu den Tatbestandsvoraussetzungen des § 303a StGB siehe Teil 2, C. I. 3. b) (2) (c).
430 Hoeren/Sieber-*Bechtold*, 7.11, Rdnr. 66; krit.: *Beucher/Engels*, **CR** 1998, S. 104 f.; ein Computerbetrug ist beispielsweise dann gegeben, wenn ein Täter die Aktivierungspflicht einer Software aushebelt und diese nutzt, ohne im Besitz einer gültigen Lizenz zu sein. Umgeht ein Nutzer mit gültiger Lizenz die (Online-)Aktivierung, weil er diese z.B. aus Datenschutzgründen ablehnt, liegt hierin mangels Vermögensschaden kein Fall des § 263a StGB.
431 Hoeren/Sieber-*Bechtold*, 7.11, Rdnr. 66.
432 Wieder ist Voraussetzung, dass man mit der h.M. im Laden des Programms eine Vervielfältigung erblickt, vgl. Teil 2, C. I. 3. b) (1) (a).

4. Strafbarkeit von „Online-Softwarepiraten“ nach zu erlassendem Recht[433] (Betrachtung de lege ferenda)

Am 22.05.2001 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[434] erlassen, deren Frist für die Umsetzung in nationales Recht der Mitgliedstaaten am 22.12.2002 endete.

Mit der Richtlinie bzw. ihrer Umsetzung soll die Ratifikation der beiden *WIPO*[435]-Verträge *WIPO* Copyright Treaty (WCT) und der *WIPO* Performances and Phonograms Treaty (WPPT) vorbereitet werden.[436] Die völkerrechtlichen Verträge wurden Ende Dezember 1996 auf einer diplomatischen Konferenz der *WIPO* in Genf verabschiedet und schaffen den Rahmen für ein einheitliches Urheberrecht der unterzeichnenden Staaten. Beide Verträge sehen – weltweit erstmals auf multilateraler Ebene – Vorschriften zum Schutz technischer Schutzmaßnahmen und Informationen über die Rechtewahrnehmung vor. Während der WCT Fragen des Urheberschutzes behandelt, geht es beim WPPT um den Schutz ausübender Künstler und Tonträgerhersteller.[437] In den USA sind die Änderungs-vorgaben aus den Verträgen bereits im Oktober 1998 mit der Verabschiedung des Digital Millennium Copyright Act (DMCA) umgesetzt worden.

An der Umsetzung der EU-Richtlinie in deutsches Recht wird derzeit gearbeitet. Am 18.03.2002 veröffentlichte das *Bundesministerium der Justiz* zunächst einen Referentenentwurf zur Neuregelung des Urheberrechts in der Informationsgesellschaft[438]. Am 16.08.2002 legte die *Bundesregierung* einen ersten Regierungsentwurf[439] zur Änderung des Urheberrechts vor und beschloss am 31.07.2002 in einer Kabinettssitzung, diesen dem *Bundestag* zur Beratung zuzuleiten. Auf eine Stellungnahme des *Bundesrates* vom 27.09.2002[440] zu diesem ersten Regierungsentwurf folgte am 6.11.2002 eine Gegenäußerung der *Bundesregierung* sowie ein zweiter Regierungsentwurf[441]. Dieser wurde am 11.04.2003 vom *Deutschen Bundestag* per Gesetzesbeschluss angenommen.[442]

Der Regierungsentwurf sieht für die §§ 15 ff. UrhG einige Neuregelungen und Klarstellungen bezüglich der Verwertungsarten vor, die sich aus den Nutzungsmöglichkeiten des Internet ergeben:

---

433 Nachtrag: Die vorliegende Arbeit wurde am 26.05.2003 als Dissertation eingereicht. Dieses Datum markiert folglich den Stand der Bearbeitung. Am 10.09.2003 ist das Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft (**BGBl.** I 2003, S. 1774-1788) in Kraft getreten. Die nachfolgend skizzierten, geplanten Änderungen des Urheberrechtsgesetzes sind seitdem allesamt geltendes Recht. Abweichungen vom letzten Regierungsentwurf (vgl. Fn. 441), die für die Darstellung von Bedeutung sind, haben sich nicht ergeben.

434 Richtlinie 2001/29/EG, **ABl. EG** L 167/11 vom 22.06.2001, S. 10 ff.

435 *Weltorganisation für den Schutz geistigen Eigentums / World Intellectual Property Organization*, http://www.wipo.org.

436 Die Verträge finden sich unter http://www.wipo.int/clea/docs/en/wo/wo033en.htm (WCT) und http://www.wipo.int/clea/docs/en/wo/wo034en.htm (WPPT).

437 Hoeren/Sieber-*Bechtold*, 7.11, Rdnr. 31.

438 Veröffentlicht beim *Institut für Urheber- und Medienrecht e.V.*, http://www.urheberrecht.org/topic/Info-RiLi/ent/RefEntw_Infoges_18_3_02.pdf.

439 **BR-Drucks.** 684/02.

440 Veröffentlicht beim *Institut für Urheber- und Medienrecht e.V.*, http://www.urheberrecht.org/topic/Info-RiLi/ent/stellungnahme_br.rtf.

441 **BT-Drucks.** 15/38; auch veröffentlicht beim *Institut für Urheber- und Medienrecht e.V.*, http://www.urheberrecht.org/topic/Info-RiLi/ent/1500038.pdf.

442 **BR-Drucks.** 271/03; auch veröffentlicht beim *Institut für Urheber- und Medienrecht e.V.*, http://www.urheberrecht.org/topic/Info-RiLi/ent/Bundesrat_Drucksache_271_03.pdf.

Der neu entworfene § 19a UrhG räumt dem Urheber das „Recht der öffentlichen Zugänglichmachung“ ein. Danach hat er das Recht, sein Werk drahtgebunden oder drahtlos der Öffentlichkeit in einer Weise zugänglich zu machen, dass es Mitgliedern der Öffentlichkeit von Orten und zu Zeiten ihrer Wahl zugänglich ist. Zur Öffentlichkeit gehört jeder, der nicht mit demjenigen, der das Werk verwertet, oder mit den anderen Personen, denen das Werk in unkörperlicher Form wahrnehmbar oder zugänglich ist, durch persönliche Beziehungen verbunden ist, vgl. § 15 Abs. 3 UrhG des Entwurfs.

§ 15 Abs. 2 UrhG des Entwurfs erfasst in seiner Nr. 2 das Recht der öffentlichen Zugänglichmachung aus § 19a UrhG des Entwurfs, so dass die neue Verwertungsart unter das Recht der unkörperlichen öffentlichen Wiedergabe fällt. Somit wird klargestellt, dass das öffentliche Anbieten eines Werkes über das Internet nicht unter das Verbreitungsrecht des § 17 UrhG zu subsumieren ist, sondern dass in Einklang mit der h.M.[443] das Recht der öffentlichen Wiedergabe berührt ist. Nach der Definition des geplanten § 22 UrhG ist das Recht der Wiedergabe von Funksendungen und der Wiedergabe von öffentlicher Zugänglichmachung das Recht, Funksendungen und auf öffentlicher Zugänglichmachung beruhende Wiedergaben des Werkes durch Bildschirm, Lautsprecher oder ähnliche technische Einrichtungen öffentlich wahrnehmbar zu machen.

Entsprechend dieser grundlegenden Ergänzung der Verwertungsrechte wird daher im Regierungsentwurf eine Neufassung des § 69c UrhG für den Bereich der Computerprogramme vorgeschlagen: In einer neu hinzugefügten Nr. 4 des § 69c UrhG soll der Rechtsinhaber das ausschließliche Recht erhalten, sein Computerprogramm drahtgebunden oder drahtlos öffentlich wiederzugeben sowie es in der Weise öffentlich zugänglich zu machen, dass es Mitgliedern der Öffentlichkeit an Orten und zu Zeiten ihrer Wahl zugänglich ist.

In § 44a UrhG sieht der Entwurf wichtige Ausnahmen vom Vervielfältigungsrecht vor, die in erster Linie Network- und Access-Providern zugute kommen werden. Danach sind vorübergehende Vervielfältigungshandlungen vom Vervielfältigungsrecht ausgenommen, wenn sie flüchtig oder begleitend sind und einen integralen und wesentlichen Teil eines technischen Verfahrens darstellen. Ihr alleiniger Zweck muss es sein, eine Übertragung in einem Netz zwischen Dritten durch einen Vermittler oder eine rechtmäßige Nutzung eines Werkes oder eines sonstigen Schutzgegenstands zu ermöglichen, wobei die Vervielfältigungshandlungen keine eigenständige wirtschaftliche Bedeutung haben dürfen.

Bislang ging das deutsche Recht davon aus, dass Zwischenspeicherungen Vervielfältigungshandlungen sind, Provider also urheberrechtliche Verwertungshandlungen vornehmen.[444] Zwar gelangen Access-Provider und Zwischenvermittler über die Verantwortlichkeitsregelungen des TDG in den Genuss einer Haftungsbefreiung, aber eine urheberrechtliche Klarstellung i.S.d. Regierungsentwurfs würde den Widerspruch beseitigen. Temporäre Vervielfältigungen von Software im Arbeitsspeicher eines Computers fallen nur dann unter die Ausnahmeregelung des geplanten § 44a UrhG, wenn sie im Rahmen einer rechtmäßigen Nutzung des Werkes geschehen. Somit wäre

---

443 Siehe Fn. 392.
444 Vgl. *Bayreuther*, **ZUM** 2001, S. 828 ff. m.w.N.

das Vervielfältigungsrecht des § 69c Nr. 1 UrhG weiterhin verletzt, wenn ein Nutzer eine unrechtmäßig registrierte oder veränderte Programmversion startet.

Mit § 108b des Regierungsentwurfs soll eine neue Strafvorschrift in das UrhG eingeführt werden, die unerlaubte Eingriffe in technische Schutzmaßnahmen (Kopierschutzsysteme) und in zur Rechtewahrnehmung erforderliche Informationen unter Strafe stellt. Die Norm bezieht sich auf die geplanten §§ 95a und 95c UrhG, in denen die unzulässigen Handlungen aufgeführt werden. Allerdings soll dem § 69a UrhG ein fünfter Absatz angefügt werden, wonach die neuen §§ 95a bis 95c UrhG auf Computerprogramme keine Anwendung finden sollen. Nach den Begründungen der Entwürfe von *Justizministerium* und *Bundesregierung* erstreckt die Urheberrechtsrichtlinie diesen Rechtsschutz nicht auch auf den Bereich der Computerprogramme. Schon im Hinblick auf erhebliche Probleme im Verhältnis zu § 69d Abs. 2 UrhG (Erstellung einer Sicherheitskopie) und § 69e UrhG (Dekompilierung) sei eine über die Richtlinienumsetzung hinausgehende Ausdehnung des Rechtsschutzes für die genannten Maßnahmen auf Software nicht angezeigt.[445]

5. Rechtsprechung in Deutschland

Gerichtsverfahren gegen Internet-Softwarepiraten sind selten geblieben. In den Verfahren ging es meist um die gewerbsmäßige unerlaubte Verwertung urheberrechtlich geschützter Werke nach § 108a UrhG. Das Internet spielte in diesem Zusammenhang nur dann eine Rolle, wenn es als Vertriebsmedium für Raubkopien gegen Bezahlung genutzt wurde oder wenn Kontakte für spätere „Offline-Geschäfte" über das Internet geknüpft wurden. Zur Höchststrafe des § 108a UrhG von fünf Jahren Freiheitsentzug wurde – soweit ersichtlich – bisher kein Softwarepirat verurteilt, wohl aber zu Geldstrafen, die sich nach dem Monatseinkommen des Täters und dem entstandenen Schaden richten. Hinzu kommen in der Regel zivilrechtliche Forderungen von der Herstellerseite, welche die strafrechtlichen bei weitem übertreffen können.

Strafverfahren gegen Internetnutzer, die sich zu eigenen Zwecken Raubkopien (kein gewerbsmäßiges Handeln gemäß § 108a UrhG) aus dem Internet heruntergeladen haben, wurden bislang nicht geführt[446].

II. Allgemeine Voraussetzungen einer effektiven Bekämpfung

1. Besonderheiten der Online-Kriminalität / Zukunftsprognose

Versuche, das Internet zu kontrollieren, gestalten sich als sehr schwierig, da es weder eine übergreifende organisatorische, finanzielle, politische noch operationale Verwaltung gibt.[447] Letztlich zeichnet niemand verantwortlich für den internationalen Gesamtkomplex Internet. Lediglich das

---

[445] Referentenentwurf (Fn. 438), S. 37; Regierungsentwurf vom 16.08.2002 (Fn. 439), S. 53 und Regierungsentwurf vom 6.11.2002 (Fn. 441), S. 37 f.

[446] Die Angaben beruhen auf einer Expertenbefragung des Verfassers am *Amtsgericht Frankfurt am Main* (Stand: 07/2002) und Recherchen in den Pressearchiven der deutschen Webseiten der folgenden Verbände bzw. Organisationen: *BSA, GVU, VUD*. Im Rahmen der Expertenbefragung wurden zwei Jugendstrafrichter und der für die Geschäftsverteilung der Frankfurter Strafgerichte zuständige Richter hinsichtlich entsprechender Strafprozesse sowie ein Oberstaatsanwalt und ein Mitarbeiter der Jugendgerichtshilfe Frankfurt am Main hinsichtlich entsprechender Ermittlungsverfahren (einschließlich eventueller Verfahrenseinstellungen gemäß §§ 153 ff. StPO) befragt.

[447] *Harbort*, **Kriminalistik** 1996, S. 195.

bereits erwähnte *W3C* stellt die größtmögliche Annäherung des dezentralen Netzes an eine Führungsstruktur dar. Seit Oktober 1994 berät der Zusammenschluss von Managern und Wissenschaftlern mit über 300 Mitgliedsorganisationen (Unternehmen, Nonprofit-Organisationen und Regierungsbehörden aus aller Welt) rund um den Gründer des Konsortiums *Tim Berners-Lee* über die Entwicklung des Internet und spricht unverbindliche Empfehlungen aus. Die Empfehlungen besitzen allerdings eine hohe moralische Autorität und werden in der Regel befolgt. Operationsbasis des *W3C* ist das *Massachusetts Institute Of Technology (MIT)* in Boston.[448] Die Aufgaben des *W3C* sind auf verschiedene Arbeitsgruppen verteilt. So wurde beispielsweise in der Gruppe „Technik" die Standardisierung von HTML vorangetrieben und in der Gruppe „Technologie und Gesellschaft" das *PICS*-System[449] erarbeitet.

Die technische Beschaffenheit des Internet eröffnet den Online-Tätern ungeahnte Möglichkeiten, die eine Bekämpfung dementsprechend erschweren. Das Verbrechen wird nicht nur schneller, es verbreitet sich auch in einem größeren Maßstab als je zuvor.[450] Folgende Aspekte sind charakteristisch für Online-Kriminalität: [451]

- Zwischen dem Aufenthaltsort des Täters und dem Tatort braucht kein Zusammenhang mehr zu bestehen.

- Tathandlungen können zeitgleich über Ländergrenzen hinweg vorgenommen werden.

- Die Täter können sich weitgehend anonym im Netz bewegen, wobei die Vorbereitung der Tatbegehung im nahezu spurenlosen Bereich geschieht.

- Schließlich besteht die Möglichkeit, kriminelle Automatismen bei unbegrenzter Multiplikation der Tatobjekte in Gang zu setzen.

Jimmy Dole von der Einheit *Computer Investigation & Technology* beim *New York Police Departement (NYPD)* beschreibt zutreffend einen weiteren Teil des Problems: „Man hat es mit gut informierten Kriminellen zu tun – die Bösen sind für gewöhnlich dem Gesetz einen Schritt voraus"[452]. Auf der Täterseite sind oft Technik-Freaks am Werke – jung, intelligent und mit der Technologie vertraut. Diese Personen leben regelrecht im Netz, weshalb sie sich dort entsprechend gut auskennen. So ist es kaum verwunderlich, dass sich High-Tech-Kriminelle nur selten im Schleppnetz polizeilicher Patrouillen auf der Datenautobahn verfangen[453].

---

[448] *Garfinkel*, Wer regiert das Internet?, **konr@d** April/Mai 1999, S. 56 f.
[449] Beim *PICS*-System (http://www.w3.org/pics) handelt es sich um eine Software zur selektiven Zugangsteuerung, mit Hilfe derer Eltern und Lehrern eine Kontrolle darüber haben, was Kinder im Internet sehen können und was nicht. Über sogenannte Ratings (Beurteilungen) werden Webseiten zunächst katalogisiert und geordnet. Die installierte *PICS*-Software ermöglicht dem minderjährigen Surfer nur Zugang zu solchen Webseiten, die als ungefährlich eingestuft wurden, indem sie die angesteuerte Webadresse online mit den *PICS*-Datenbanken abgleicht – weitere Ausführungen zum Thema Rating finden sich unten in Teil 2, C. III. 9. a) (2).
[450] Vgl. das Interview mit *Charney,* geführt von *Schulzki-Haddouti*, World Wide Fahndung, **c't** 15/1999, S. 74.
[451] Vgl. *Kube*, **Kriminalistik** 1996, S. 622.
[452] *Radcliffe*, **CNN interactive** vom 15.12.1998.
[453] *Kube*, **Kriminalistik** 1996, S. 624 f.

Hindernisse bei der Verfolgung ergeben sich darüber hinaus durch das häufige Erfordernis internationaler Amtshilfe. Das Vorgehen gegen Serverbetreiber erweist sich als besonders schwierig, wenn die Server in Ländern stehen, in denen das Urheberrecht von Software nicht strafrechtlich geschützt ist (z.B. Libyen, Bulgarien oder Iran). Ein gerne gebrauchtes Beispiel ist in diesem Zusammenhang ein Warez-Server, der sich in einem arabischen Land befindet: „Fordern Sie einen arabischen Polizisten auf, einen Landsmann festzunehmen, weil er ein US-amerikanisches Unternehmen schädigt – vergessen Sie es!“[454].

Auch was die Zugangsanbieter betrifft, ergeben sich je nach Rechtsordnung unterschiedliche Probleme. In einigen Ländern kann man die Provider zur Mithilfe zwingen, in anderen Ländern lediglich darum bitten. Bedeutsam wird dies, wenn ein Provider seine Hilfe verweigert.[455] Bittet ein inländisches Gericht ein ausländisches Gericht um Hilfe, handelt es sich meist um einen langwierigen Prozess, weshalb die Bemühungen der Ermittler oftmals vergebens sind. Denn Warez-Server existieren in den meisten Fällen nicht lange unter derselben Adresse, da sich die Zugangsdaten schnell in der Szene herumsprechen, und die Server in der Folge regelrecht verstopft werden. Die Siteops ändern daher turnusmäßig die Passworte und die Ports, wenn sie eine übermäßige Frequentierung ihres Servers bemerken. Bis die entsprechenden Amtshilfeanträge bewilligt sind, gibt es die meisten der ins Visier genommenen Seiten längst nicht mehr.[456]

Eine weitere Besonderheit der Online-Kriminalität ist, dass es auch innerhalb des Internet einen Underground und einen Overground gibt. Hierbei ist das jedermann zugängliche WWW am ehesten als Overground zu bezeichnen, geheime FTP-Server, Chatrooms und Mailing-Listen als Underground. Da die hohen Sicherheitsvorkehrungen der Untergrund-Szene eine Bekämpfung zusätzlich erschweren, stellenweise gar unmöglich machen, sollte daran gelegen sein, diese Szene so klein wie möglich zu halten. Das Abwandern von Personen aus dem Overground in den Underground würde einen massiven Kontrollverlust bedeuten, was bei der gezielten Ausübung von Verfolgungsdruck berücksichtigt werden muss.

Wenn es nicht gerade um die – derzeit als besonders wichtig angesehene – Bekämpfung von Kinderpornographie oder von Rechtsextremismus geht, ist die Internetgemeinde äußerst empfindlich, was jegliche Art der Überwachung anbelangt. Die Gerüchte um *ECHELON*, *ENFOPOL* und *Carnivore* haben gezeigt, dass in diesem Zusammenhang mit massivem Widerstand der Internetnutzer zu rechnen ist.

ECHELON gilt als das weltweit größte elektronische Überwachungssystem, mit dem die Geheimdienste der USA, Großbritanniens, Australiens, Kanadas und Neuseelands jedes Telefongespräch, jede E-Mail und jegliche Faxkommunikation in praktisch jedem Land abhören können sollen.[457] Offiziell gibt es *ECHELON* gar nicht, allerdings war es Anfang 2000 Gegenstand einer Anhörung des Ausschusses für Bürgerrechte des Europäischen Parlaments, in dessen Abschlussbericht vom 05.09.2001 die Existenz des internationalen Abhörsystems bestätigt wurde.[458] Bereits im März 2000

---

[454] *McCandless*, **Wired Magazine** 5.04 – April 1997.
[455] Vgl. das Interview mit *Charney*, geführt von *Schulzki-Haddouti*, World Wide Fahndung, **c't** 15/1999, S. 74.
[456] Vgl. das Interview mit *Lobmeier* – Sprecherin von *Microsoft* zum Thema Softwarepiraterie, in: *Puscher*, **internet world** 1/1999, S. 35.
[457] *Rötzer*, FBI, **Telepolis** vom 07.10.1999.
[458] Vgl. *Schulzki-Haddouti*, Das Ende der Schweigsamkeit, **c't** 19/2001, S. 44.

räumte der ehemalige *CIA*-Direktor *James Woolsey* bei einer Presskonferenz vor ausländischen Journalisten die Aufklärungsarbeit mittels *ECHELON* ein; diese sei jedoch vorwiegend auf Wirtschaftsspionage ausgerichtet.[459]

Bei *ENFOPOL* handelt es sich um die *Europäische Arbeitsgruppe für Polizeiliche Zusammenarbeit*, die die Pläne der EU zur Überwachung der Telekommunikation umsetzen soll. Danach müssen Provider beispielsweise auf eigene Kosten Abhörschnittstellen einrichten und relevante Daten innerhalb weniger Sekunden den Behörden zuliefern.[460]

Das vom *FBI* eingesetzte Lauschsystem *Carnivore* ist zur Integration in den Rechenzentren von ISPs konzipiert und kann Daten, die bestimmten Kriterien genügen, aufzeichnen, ohne dass Empfänger und Absender etwas davon mitbekommen.[461]

ECHELON, *ENFOPOL* und *Carnivore* sind der Schrecken all jener Internetnutzer, die um den Verlust ihrer Anonymität fürchten. Aus diesem Grund gibt es zahlreiche Personen und Vereinigungen, die Informations-Webseiten erstellt haben, die sich mehr oder weniger sachlich mit dem Thema auseinandersetzen.[462]

Der technische Fortschritt wird es mit sich bringen, dass die Zeitfenster, in denen eine Tat beobachtet werden kann, immer kleiner werden, denn in Zukunft ist auch für den durchschnittlichen Internetnutzer mit einem starken Anstieg der Übertragungsraten zu rechnen. Der heutige Quasi-Standard ISDN ermöglicht es bei weitem nicht, die multimedialen Möglichkeiten des Internet voll auszuschöpfen. Daher sind seit Mitte 2000 in den größten deutschen Ballungszentren und seit 2001 auch in den ländlicheren Regionen der Republik ADSL-Anschlüsse verfügbar. Die bei ADSL zum Einsatz kommende Übertragungstechnik nutzt das alte Kupferleitungsnetz der *Telekom*, weshalb eine flächendeckende Einführung ohne größeren Aufwand möglich ist.[463]

Weitere neue Übertragungsverfahren, die noch größere Bandbreiten ermöglichen, stehen kurz vor der Marktreife. Hierzu gehört unter anderem die Übertragungstechnik VDSL (Very-High-Bit-Rate Digital Subscriber Line), die ebenso wie ADSL mit den bestehenden Kupferleitungen funktioniert.[464] Auch Stromnetze („Internet aus der Steckdose“[465]), reine photonische Netze (Lichtleiterübertragung) und TV-Kabelnetze[466] werden in naher Zukunft für die schnelle Anbindung an das Internet genutzt. Datenübertragung per Funk und Satellit wird ebenfalls zunehmend eine Rolle spielen.

---

[459] **Heise Online News** vom 12.03.2000, http://www.heise.de/newsticker/meldung/8511.
[460] *I. Schneider*, Horchposten im Netz, **FOCUS** 13/1999, S. 264.
[461] http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm.
[462] Z.B.: http://www.epic.org.
[463] Nach dem Jahresbericht 2001 der *Regulierungsbehörde für Telekommunikation und Post (RegTP)* waren Ende 2001 rund 2,07 Millionen ADSL-Anschlüsse geschaltet, wovon rund 2 Millionen Anschlüsse von der *Telekom* bereitgestellt wurden. Die anderen 43 DSL-Anbieter verwalteten die restlichen Anschlüsse. Bei der *RegTP* sieht man im DSL-Markt ein Potential von 20 Millionen Kunden, **c't** 4/2002, S. 37.
[464] VDSL soll zwölfmal schneller im Download (10 MBit/s) und achtzigmal schneller beim Upload als ADSL sein, **ZDNet News** vom 08.02.2002, http://www.zdnet.de/news/tkomm/0,39023151,2104010,00.htm.
[465] Die *Powerline*-Technik überträgt die Daten mit derzeit bis zu 4,5 MBit/s über das Stromnetz. Mittelfristig wird mit Übertragungsraten von bis zu 20 MBit/s gerechnet. Allerdings gibt es das Angebot bisher nur in Essen, Mühlheim/Ruhr, Ellwangen und Mannheim; nach dem bereits erwähnten Jahresbericht der *RegTP* gab es Ende 2001 ca. 2000 *Powerline*-Anschlüsse.
[466] Während Internetzugänge über das TV-Kabelnetz in den USA weit verbreitet sind, steckt die Entwicklung in Deutschland noch in den Kinderschuhen. Doch die Prognosen sind günstig, denn mit über 17,7 Millionen Haushalten ist

2. Welche Spuren hinterlässt ein Online-Täter?

Im Bereich der Softwarepiraterie ist es besonders wichtig, festzustellen, wer im großen Stil illegale Downloadmöglichkeiten bereitstellt. Stößt man auf eine entsprechende Seite, ist deren WWW bzw. FTP-Adresse der einzige Hinweis auf ihren Ursprung. Die zugrundeliegende IP-Adresse lässt sich über einen sogenannten Trace-Route[467] herausfinden, der alle Hops (Sprünge über Router), die auf dem Weg vom eigenen Rechner zur entsprechenden Seite liegen, in Textform darstellt. Der letzte Hop führt in der Regel zu der permanenten IP-Adresse des Servers, der die illegalen Inhalte bereitstellt. Der Trace-Route-Befehl liefert zusätzlich eine geographische Zuordnung der passierten Rechner und Router. Über ein DOS-Fenster oder mit Hilfe eines speziellen Programms (z.B. *Visual Route*) lässt er sich am einfachsten ausführen.

Um Informationen über den Betreiber der illegalen Seite zu erlangen, ist es notwendig, herauszufinden, wem der Server gehört, der die ermittelte Adresse hat. Meist wird es sich beim Eigentümer des Servers um einen Host-Service-Provider handeln. Über eine Anfrage bei den Network Information Centers (NICs)[468] lässt sich herausfinden, auf wen die entsprechende Domain registriert ist. Neben dem Namen des Registrierten sind dort auch Anschrift und E-Mailadresse gelistet, so dass leicht mit ihm in Kontakt getreten werden kann. Handelt es sich um einen Host-Service-Provider, kann dieser anhand des verdächtigen URLs leicht herausfinden, welcher seiner Kunden die illegalen Inhalte verbreitet. Schwieriger hingegen ist es bei Host-Service-Providern, die anonymen Webspace anbieten: Diese können zwar die illegalen Seiten von ihren Servern herunternehmen, eine Identifikation des Urhebers ist jedoch mangels einer authentifizierten Vertragsbeziehung zwischen Provider und Nutzer kaum möglich.[469]

Betrachtet man die Verfolgungspraxis im Bereich der Softwarepiraterie, scheint die Identifikation des Nutzers, der sich von zu Hause aus einwählt, eher von untergeordneter Bedeutung zu sein. Bei anderen Arten der Online-Kriminalität – vor allem bei der Kinderpornographie und Staatsschutzdelikten – ist die Identifikation des Täters jedoch äußerst wichtig, so dass die Grundlagen im Folgenden kurz dargestellt werden sollen:

Dass man sich im Internet völlig anonym bewegen könne, ist ein weit verbreiteter Irrglaube. Jeder Internetnutzer hat für die Zeit seines Netzaufenthalts eine eigene, unverwechselbare IP-Adresse, die er bei der Einwahl von seinem ISP bezieht. Bei jedem Dienst, den der Nutzer in Anspruch nimmt, werden Daten in beide Richtungen übertragen. Beim Betrachten einer Homepage beispielsweise werden die Bild- und Textdateien an die IP-Adresse des Betrachters gesendet, die Steuerbefehle zur Navigation auf der Homepage werden vom Betrachter an die IP-Adresse des Webservers geschickt. Anhand eines Protokolls kann der Betreiber der Webseite die IP-Adressen sämtlicher Besucher

---

das deutsche Fernsehkabelnetz das größte Europas. Gemäß den Angaben aus dem Jahresbericht der *RegTP* gab es Ende 2001 ca. 30.000 Kabel-TV-Anschlüsse mit Online-Anbindung.

467 Trace-Route ist ein Befehl, über den man den Weg von IP-Paketen durch das Internet zu ihrem Ziel angezeigt bekommt.

468 Registrierungsstellen für Domain-Namen. Z.B. http://www.nic.de für .DE-Domains, http://www.nic.com und http://www.nic.net und für .com-, .net- und .org-Domains.

469 Interessant ist auch die Möglichkeit der sogenannten Domain-Rückwärtssuche, wie sie z.B. bei http://www.profifinder.de angeboten wird. Dort kann man beispielsweise abfragen, welche .de-Domains eine bestimmte Person besitzt. Die offiziellen Domain-Registrare lassen solche Recherchen in der Regel aus datenschutzrechtlichen Gründen nicht zu.

seiner Seite einsehen. Die IP-Adresse eines Nutzers ist also für die Gegenstelle einer Datenübertragung sichtbar. Dies gilt für beinahe alle Dienste des Internet. Um herauszufinden, welche natürliche Person sich hinter der jeweiligen IP-Adresse verbirgt, sind jedoch weitere Schritte notwendig. Wird der Rechtsverstoß eines Nutzers beobachtet, benötigt man zunächst seine IP-Adresse und den genauen Zeitpunkt der Tat. Denn aufgrund der dynamischen Vergabe von IP-Adressen ist es möglich, dass unter derselben Adresse, mit der eine Straftat begangen wurde, wenige Sekunden später eine andere (unbescholtene) Person online sein kann. Somit ist einem bestimmten User nur dann eine IP-Adresse zuzuordnen, wenn der exakte Zeitpunkt einer Rechtsverletzung feststeht und gewährleistet ist, dass keine zeitlichen Verzerrungen bestehen.

Mit der Hilfe des Trace-Route-Befehls lässt sich in den meisten Fällen problemlos der Rechnername bzw. der Einwahlknoten des ISP finden, der zur herausgefundenen IP-Adresse gehört. Informationen, um den entsprechenden Provider zu kontaktieren, kann man auch in diesem Fall über eine Anfrage bei den Network Information Centers erhalten. Mit der IP-Adresse kann der Provider schließlich eine genaue Zuordnung vornehmen, da bei ihm sämtliche Daten anfallen, die eine Identifikation des Täters ermöglichen.[470] Hierbei ist zu beachten, dass diese Zuordnung immer nur zu einem Vertrag des Providers mit einem bestimmten Kunden führt. Der Täter kann genauso gut ein Verwandter oder Freund des Vertragspartners sein, der dessen Account nutzt. Ein Missbrauch des Accounts durch Hacker oder Faker[471] ist ebenso denkbar und muss bei den weiteren Ermittlungen in Erwägung gezogen werden.

Hält sich eine verdächtige Einzelperson im IRC auf, kann man ihre IP-Adresse selbst dann ermitteln, wenn man keinen Zugriff auf die Logfiles des IRC-Servers hat[472]:

Über den Befehl „/whois [(Nick-)Name des Verdächtigen]“ erhält man die Netzadresse des Nutzers. Hieraus gehen in der Regel das Herkunftsland, der Provider und eine personenbezogene Information über den Zugang des Providers hervor – ein mögliches Ergebnis könnte „target@ppp13.stud.uni-weimar.de“ sein. Diese Adresse ist ein Beispiel für einen dynamischen Internet-Zugang, wobei der Teil “target“ als einziger vom Nutzer frei wählbar ist. Alles, was hinter dem @-Zeichen steht, gilt als nicht veränderbar. „ppp13“ steht im Beispiel für den „Einwahlknoten Modem 13“, und bei „stud.uni-weimar.de“ handelt es sich um die Domain der Universität Weimar mit deutscher Länderkennung am Ende. Befindet sich hinter dem @-Zeichen anstatt der ausgeschriebenen Domain eine IP-Adresse in Zahlenform, hilft ein DNS-Lookup weiter (/dns [(Nick-)Name] oder /dns [IP-Adresse]), über den man den Namen des Servers erhält. Die nötigen Informationen für die Kontaktaufnahme mit dem ISP, zu dem die Serveradresse gehört, lassen sich wiederum über das zuständige Network Information Center beziehen. Infomationen über Personen, die den IRC bereits verlassen haben, können durch den Befehl „/whowas [(Nick-)Name]“ abgefragt werden.

Mit dieser Methode lassen sich schätzungsweise 99% der tatsächlichen IP-Adressen aller IRC-User ermitteln. Über eine Anfrage beim Provider der IP-Adresse, wer zu einem bestimmten Zeitpunkt mit der ermittelten IP-Adresse online war, lässt sich schließlich ein Kunde des Providers ermitteln.

---

[470] *Decius/Panzieri*, S. 9.

[471] Siehe die Darstellung im Anschluss und Abbildung 74.

[472] Das Nachfolgende gilt nach wie vor für die großen und populären Netze wie EfNet, DalNet, UnderNet oder IRCNet. Bei neueren IRC-Netzwerken wie dem EU-IRCNet ist zur Bestimmung einer IP-Adresse eines Nutzers erforderlich, dass man den Status eines IRC-Ops innehat.

Entgegen der gängigen Meinung[473], dass sich der Teil der Netzadresse nicht verfälschen lässt, der sich hinter dem @-Zeichen befindet, hat ein Teil der IRC-User verschiedene Wege gefunden, dies doch zu bewerkstelligen. Vor allem in Hackerkreisen werden Methoden ausgetauscht, mit denen diese Art der Anonymisierung, die häufig als „Spoofing" bezeichnet wird, möglich ist.[474] In den meisten Fällen fälscht der Täter seine IP-Adresse bzw. den Server- und Domain-Namen, indem er zwischen sich und den IRC-Server einen dritten, meist fremden, Stellvertreter-Rechner („Proxy" oder „Socks Server") zwischenschaltet. Er gibt sich somit als der Server aus, der direkt mit dem IRC-Server verbunden ist.[475] Im IRC erscheint bei einer whois-Abfrage nur die IP-Adresse des fremden Rechners. Lediglich am Ort des zwischengeschalteten Rechners kann man nachvollziehen, wo sich der Täter tatsächlich befindet.

Das Zwischenschalten von Rechnern ist bei fast allen Internet-Diensten möglich. Um eine möglichst hohe Anonymität zu erzielen, haben findige User die Technik des sogenannten Proxy-Chaining entwickelt. Dabei werden häufig bis zu acht Proxy-Server in Reihe zwischen User und Zielrechner geschaltet. Stehen diese Rechner zu allem Überfluss in Japan oder Russland, ist eine Aufdeckung der wahren Identität des Users nahezu unmöglich, zumal die häufig illegal eingerichteten Proxy-Server so konfiguriert sind, dass sie keine Verbindungen per Logfiles protokollieren.

Erfreulicherweise sind diese Techniken nicht allzu weit verbreitet. Lediglich um ihre Sicherheit besorgte Hacker und Mitglieder von Warez-Gruppen entziehen sich der Gefahr einer Identifikation, indem sie niemals „ungespooft" ins Netz gehen.

Eine weitere Eigenschaft des IRC, die ihn zu einem äußerst schwer kontrollierbaren Dienst macht, ist die Möglichkeit der direkten Datenübertragung zwischen zwei Nutzern. Denn der Datentransfer per DCC hinterlässt keine Spuren, die von außen sichtbar sind.[476]

Probleme bei der Identifikation der User können auch die bereits erwähnten Fake-Accounts bereiten. Hierunter versteht man Internetzugänge, die unter Angabe von frei erfundenen oder gestohlenen persönlichen Daten eingerichtet wurden. Große Online-Dienste legen Computerzeitschriften häufig Werbe-CD-ROMs bei, mit denen jedermann ohne Überprüfung seiner Identität eine gewisse Anzahl „Internet-Freistunden" erhält. Doch nicht nur derartige Lockangebote verhelfen Nutzern zu Fake-Accounts: In zahlreichen Fällen bedienen sich die Faker mit Hilfe sogenannter Trojaner[477] fremder Zugangskennungen, oder sie beantragen unter Angabe falscher Kontendaten oder Kreditkarten-nummern neue Accounts über die Webseiten einzelner Provider. Letzteres hat sich für viele deutsche ISPs zu einem ernstzunehmenden wirtschaftlichen Problem entwickelt und zog die Einleitung zahlreicher Strafverfahren wegen Betrugs nach sich.

---

473 So z.B. *Decius/Panzieri*, S. 7.
474 Vgl. *McClure/Scambray*, **CNN interactive** vom 25.01.1999.
475 Vgl. *Kossel*, **c't** 3/1999, S. 143.
476 *Diesler*, **CHIP** 11/1995, S. 55; lediglich die beteiligten Nutzer und deren Provider haben die Möglichkeit, die Daten zu sehen – die Daten laufen quasi am IRC-Server vorbei.
477 Als Trojaner bezeichnet man Programme, die beispielsweise als E-Mail-Attachment getarnt in ein fremdes Computersystem eingeschleust werden, dort heimlich eine Hintertür öffnen und selbsttätig sensible Daten wie Login-Informationen und Passwörter an den Angreifer versenden.

```
Hallo Leute !
Da in letzter immer mehr nach I-net Fakez fragen (im IRCnet), habe ich mich
entschieden eine kurze Anleitung zu schreiben wie man Fakez bei TDF macht.
Als Erstes : Es ist nicht schwer und dauert nur 2 Minuten!

- - - Schritt 1 - - -
Über DFÜ-Netzwerk bei TDF einwählen.
Nummer : 08*******
login: ******
pass: ******

- - - Schritt 2 - - -
Netscape, Internet Explorer oder anderen Browser starten und auf
http://*******.****.net gehen.

- - - Schritt 3 - - -
Bogen ausfüllen mit Phantasie Namen und Adressen. Eigene Rufnummer löschen! Login
und Pass wählen. Die Kontonummer ist eine beliebige 7-stellige Zahl , die
Bankleitzahl eine 8-stellige Zahl , nicht beliebig (siehe Ende des Textes).

- - - Schritt 4 - - -
Verbindung beenden und mit
Nummer : 08******
login: dein erstelltes
pass: dein gewähltes
einwählen.

- - - Schritt 5 - - -
spass haben ohne Kostendruck !

Bankleitzahlen für den Fake :
300***** CITIBANK PRIVATKUNDEN REGION D*******
300***** CITIBANK PRIVATKUNDEN REGION H*******
300***** CITIBANK PRIVATKUNDEN REGION M******

Have Phun, Smokey
thanks to : muffin, ratboy, TDF, deutsche Gesetzgebung
```

Abbildung 74 – Anleitung zum Provider-Betrug (sogenanntes Faking-Tutorial)

Während es vor wenigen Jahren nicht möglich war, Faker zu identifizieren, die über eine analoge Vermittlungsstelle mit dem Telefonnetz verbunden wurden, fällt die Ermittlung der Betrüger heute leicht, da die Netzbetreiber im vollständig digitalisierten deutschen Telefonnetz grundsätzlich bei jedem Gespräch die Rufnummern erfassen – selbst wenn der Nutzer die Anzeige seiner Rufnummer bei der Gegenstelle unterdrückt hat. Schwierig wird es nur dann, sofern die betroffenen Provider nicht die Rufnummerndaten, sondern rufnummernunabhängige Zugangsdaten für die Rechnungsstellung heranziehen.[478]

Erhebt der geschädigte Provider die Rufnummerndaten, kann es dennoch Probleme bei der Identifikation geben, wenn sich der Täter beispielsweise von einem Hotelzimmer oder von einem Anschluss aus einwählt, zu dem mehrere Personen Zugang haben.

Ein weiteres Hindernis für die Identifikation von Online-Kriminellen, die sich durch das WWW bewegen, stellen sogenannte Anonymisierungsdienste dar. Diese meist kommerziellen Dienste garantieren ihren Kunden größtmögliche Anonymität, indem sie gezielt die Spuren der Surfer

---

[478] **c't** 21/2000, S. 48.

verwischen. Unternehmen wie *Anonymizer*[479], *CyberArmy* oder *Lucent* speichern keine Cookies, blocken Java- und JavaScript-Zugang und entfernen sämtliche Identifizierungshinweise. Sie behalten Logfiles lediglich für 48 Stunden und zeichnen nicht einmal die zugrundeliegende IP-Adresse auf.[480] Für eine monatliche Pauschale ermöglichen die meisten Anonymisierungsdienste den angemeldeten Nutzern, sich absolut anonym durch das Internet zu bewegen. Zur Verschleierung der Verbindung setzen die Dienste unterschiedliche Verfahren ein:

Häufig wandern die IP-Pakete über mehrere Server eines eigenen Netzwerkes, bevor sie zum Ziel gelangen. Dabei agiert der Server am Ende der Kette als Stellvertreter (Proxy) des Surfers. Zuweilen wird sogar starke Verschlüsselung für die Kommunikation zwischen den einzelnen Relais-Stationen eingesetzt, so dass auf dem Weg weder Abhören noch eine Analyse der übertragenen Pakte möglich ist. So bietet z.B. der Anonymisierdienst *Rewebber* optional Verbindungen über Secure Socket Layer (SSL) an. Hierbei wird die Kommunikation vom Browser verschlüsselt und die Authentizität des Anonymisier-Servers überprüft. Sofern eine direkte SSL-Verbindung zum *Rewebber* ohne SSL-Zwangsproxy des Providers möglich ist, kann der Provider den Datenverkehr nicht mehr überwachen oder kontrollieren.

Besonders ausgefeilte Verfahren zur Anonymisierung wurden für den E-Mail-Dienst entwickelt. Neben Freemailer-Diensten[481] und simplen Remailer-Diensten[482], die beide keine hundertprozentige Anonymisierung des Absenders bewirken können, gibt es mit *Cypherpunk* (Typ-I-Remailer) und *Mixmaster* (Typ-II-Remailer) wirklich anonyme Remailer. Obwohl sich die beiden Typen in der Praxis deutlich unterscheiden, funktionieren sie nach dem gleichen Prinzip: Der Nutzer schickt seine E-Mail an einen Remailer-Server. Dieser entfernt sämtliche Daten aus der Mail, die Rückschlüsse auf den Absender zulassen könnten und schickt sie an einen anderen Remailer weiter. Erst nachdem die Mail eine vorher definierte Zahl von Remailern durchlaufen hat, landet sie schließlich im Postfach des Adressaten.[483] Sind die Server entsprechend konfiguriert, bilden sie eine sogenannte Mixkaskade, bei der ein außenstehender Beobachter nicht in der Lage ist, festzustellen, welche eingehende Nachricht mit welcher ausgehenden Nachricht identisch ist. Ein „Mix" sammelt die eingegangenen Nachrichten und sendet sie schubweise weiter. Dabei achtet er darauf, dass in einem Schub nicht viele Nachrichtenpakete des gleichen Absenders verschickt werden, um die Anonymität der anderen zu wahren. Außerdem werden die Nachrichten umsortiert, um eine direkte Zuordnung von Eingang und Ausgang zu verhindern.[484] Neben der aufwändigen Gestaltung des Versandweges kommt bei beiden Remailertypen starke Verschlüsselung zum Einsatz. Während *Cypherpunk* mit den Verschlüsselungsalgorithmen von *PGP*[485] arbeitet, benutzt *Mixmaster* ein proprietäres Verschlüsselungsmodul. Es ist mit an Sicherheit grenzender Wahrscheinlichkeit davon auszugehen, dass die auf diese Weise versendeten Nachrichten nur beim Versender und beim Empfänger in Klarform vorliegen.

---

[479] In der Internet-Gemeinde hält sich hartnäckig das Gerücht, dass *Anonymizer* insgeheim von einer US-Behörde betrieben wird, vgl. *Demuth*, **c't** 6/2000, S. 197; *Glaser*, E-Mail und die Detektive, **konr@d** 4/1999, S. 109.
[480] *McClure/Scambray*, **CNN interactive** vom 25.01.1999; zum Begriff des Cookies siehe Fn. 591.
[481] Siehe oben Teil 1, D. II.
[482] Ein simpler Remailer ist ein Dienst, der Nachrichten auf Umwegen (über Relaisstationen) zum Ziel leitet.
[483] *Bleich*, Selbstverdunkelung, **c't** 16/2000, S. 156.
[484] Ausführlich zur Funktionsweise von Mix-Verfahren: *Federrath/Berthold/Köhntopp/Köpsell*, **c't** 16/2000, S. 149 ff.
[485] Siehe unten Teil 2, C. III. 8. b).

In den meisten Fällen ist der Provider der Schlüssel zur Deutung der im Datennetz aufgegriffenen Spuren, da bei ihm die notwendigen Daten zusammenlaufen. Welche Datenerhebungen durch die Provider zulässig sind, welche Daten unter welchen Voraussetzungen übermittelt werden dürfen, und wann die Diensteanbieter bereits erhobene Daten löschen müssen, ist im Teledienstedatenschutzgesetz (TDDSG) geregelt. Das Gesetz unterscheidet drei Typen von anfallenden Daten:

Bei Bestandsdaten (§ 5 TDDSG) handelt es sich um alle personenbezogenen Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses über die Nutzung von Telediensten erforderlich sind – insbesondere also Name, Anschrift und Bankverbindung des Kunden.

Zu den Nutzungsdaten (§ 6 Abs. 1 TDDSG), die häufig auch als Inhaltsdaten bezeichnet werden, gehören alle Daten, die dem Nutzer die Inanspruchnahme von Telediensten ermöglichen; z.B. aufgerufene URLs, zugeordnete IP-Adresse oder Routen-Daten. Die Nutzungsdaten fallen in Form von sogenannten Logfiles an. Hierbei handelt es sich um Protokolle in Textform, die von den Computersystemen generiert werden, welche den Kunden den Zugang ermöglichen.[486] Der Diensteanbieter hat diese Daten grundsätzlich nach Beendigung des jeweiligen Nutzungsvorgangs zu löschen, vgl. § 4 Abs. 4 S. 1 Nr. 2 TDDSG. Nach Aussage des früheren Bundesbeauftragten für den Datenschutz *Jacob* dürfe ein Provider „in keinem Fall mit Blick auf eine eventuelle Strafverfolgung vorsorglich speichern, wer wann welche IP-Nummer hatte“[487]. Die Provider sind somit nach geltendem Recht nicht verpflichtet, Nutzungsdaten über einen längeren Zeitraum zu speichern und für die Strafverfolgungsbehörden „vorzuhalten“. Nur wenn dem Diensteanbieter bereits während der Nutzung tatsächliche Anhaltspunkte vorliegen, dass seine Dienste von bestimmten Nutzern in der Absicht in Anspruch genommen werden, das Entgelt nicht oder nicht vollständig zu entrichten, darf er die Daten so lange nutzen und verarbeiten, wie es für die Durchsetzung seiner Ansprüche gegen entsprechende Nutzer erforderlich ist, § 6 Abs. 8 S. 1 TDDSG. Ansonsten ist eine längere Speicherung von Nutzungsdaten nur statthaft, wenn der Betroffene eingewilligt hat.[488] Insoweit gelten die allgemeinen Geschäftsbedingungen der Provider.

Der Umgang mit den Nutzungsdaten wirft nicht zuletzt deshalb massive daten-schutzrechtliche Probleme auf, als ihre Überprüfung einen Abhörvorgang erforderlich macht, der die Vertraulichkeit der Kommunikation verletzt.

Unter den Begriff der Abrechnungsdaten (§ 6 Abs. 4 TDDSG – auch „Verbindungsdaten“) fallen schließlich solche Daten, die für die Abrechnung der Teledienste notwendig sind, also in erster Linie Informationen darüber, wer an einem Telekommunikationsvorgang beteiligt war, und wann dieser stattgefunden hat. Nach § 6 Abs. 4 TDDSG darf der Diensteanbieter diese Daten nur über das Ende des Nutzungsvorgangs hinaus nutzen und verarbeiten, soweit sie für die Abrechnung mit dem Nutzer erforderlich sind. Wurden die Daten erhoben, um auf Wunsch des Nutzers Einzelnachweise über die Verbindungen zu führen, so müssen sie spätestens 6 Monate nach Versendung dieser Einzelnachweise gelöscht werden, es sei denn, die Forderung wurde bestritten oder nicht bezahlt, § 6 Abs. 7 TDDSG.[489]

---

[486] Zu den gängigen Logfile-Formaten siehe *Köhntopp/Köhntopp*, **CR** 2000, S. 250 ff.
[487] *S. Jaeger*, Gesetze und Lücken, **c't** 4/2000, S. 234.
[488] *S. Jaeger*, Gesetze und Lücken, **c't** 4/2000, S. 234.
[489] Vgl. *S. Jaeger*, Kleingedrucktes, **c't** 19/1999, S. 264.

Entgegen der landläufigen Einschätzung hinterlässt der Online-Täter im Normalfall eine breite Datenspur[490]. Sicher gibt es Möglichkeiten, weniger Spuren zu hinterlassen, doch so anonym, wie das Internet erscheint, ist es lange nicht mehr. Es liegt auf der Hand, dass die beschriebenen Anonymisierdienste die Arbeit der Ermittler erheblich erschweren[491], doch werden nur wenige Nutzer freiwillig auf ihren Einsatz verzichten, zumal Politik und Recht (vgl. § 4 Abs. 6 TDDSG) zur anonymen bzw. pseudonymen Nutzung von Telediensten ermutigen.

Die dargestellten Unwägbarkeiten und Schwierigkeiten erfordern fast immer eine Hausdurchsuchung beim Verdächtigen, um stichhaltige Beweise zu erlangen.[492] Denn die Zuordnung von Verbindungs- und Bestandsdaten durch den Provider liefert lediglich Hinweise auf potentielle Täter.

3. Einordnung der Bekämpfungsmaßnahmen / Arten der Kriminalitätsvorbeugung

Bei der Entwicklung des Internet wurde offensichtlich nicht erahnt, welche umfangreichen Nutzungsmöglichkeiten es wenige Jahre später für jedermann und somit auch für Computerkriminelle bieten würde. In die Internet-Technologie wurden kaum Vorkehrungen integriert, die die Missbrauchsmöglichkeiten des Mediums einschränken. In diesem Zusammenhang ist in erster Linie an die weitgehend gewährte Anonymität der Nutzer untereinander zu denken, die mittlerweile für die meisten User zu einem unverzichtbaren Charakteristikum des Netzes geworden ist.

Die derzeitigen Bekämpfungsmöglichkeiten sind auf rein reaktive Maßnahmen beschränkt. Da jedoch das proaktive Aufspüren und Analysieren des eigentlichen Problems prinzipiell wichtiger ist als das Nachbessern mit ad hoc-Lösungen[493], muss untersucht werden, inwieweit präventive Bekämpfungsansätze zu verwirklichen sind. Vor allem in der proaktiven Technikprävention besteht ein erhebliches Vorbeugungspotential. Es ist erfolgversprechender, die reale und virtuelle Welt von Menschen zu verändern als einzelne kriminell gefährdete Technik-Freaks oder technik-orientierte „Teilzeit- und Fulltime–Kriminelle“ durch Aufklärung und Überzeugungsarbeit in ihrem Verhalten nachhaltig zu beeinflussen[494]. Dies gilt erst recht für den Bereich der Softwarepiraterie, in dem das Unrechtsbewusstsein der Täter beinahe gegen Null geht[495].

Grundsätzlich können drei Ebenen technologieorientierter Kriminalitätsvorbeugung unterschieden werden[496]:

- Die Ebene der reaktiven Prävention – das staatliche Präventionshandeln orientiert sich konventionell an der stattgefundenen Kriminalität, ist also reaktiv.

- Die Ebene der proaktiven Prävention nach Technologieeinführung – hierbei handelt es sich um Prävention, die erfolgt, bevor der Täter die neue Technik ausnutzt. Sie setzt unter

---

490 *Köhntopp/Köhntopp*, **CR** 2000, S. 257.
491 *Meseke*, S. 529.
492 Vgl. *Janovsky*, **Kriminalistik** 1998, S. 503.
493 *Kube*, **Kriminalistik** 1996, S. 618.
494 *Kube*, **Kriminalistik** 1996, S. 625.
495 Siehe oben Teil 2, A. VIII. 3.
496 *Kube/Bach/Erhardt/Glaser*, **ZRP** 1990, S. 301 f.

anderem die systematische Beobachtung der strafrechtsrelevanten technischen Entwicklung voraus.

- Die Ebene der proaktiven Prävention vor der Technologieeinführung – die Umsetzung kriminalistischer Präventionserkenntnisse in technische Systeme vor deren Markteinführung.

Da das Internet als eigenständige Technologie bereits eingeführt ist, stellt sich die Frage, inwieweit sich Kriminalitätsvorbeugung auf der Ebene der proaktiven Prävention nach Technologieeinführung überhaupt noch verwirklichen lässt. Ansetzen kann diese Art der Prävention nur an den technischen Neuerungen, die die Internet-Technologie schrittweise verändern. Das wohl wichtigste Beispiel ist in diesem Kontext die bevorstehende Einführung eines neuen Internetprotokolls, das neben einigen notwendigen Verbesserungen auch in der Lage sein soll, die Anonymität der Nutzer aufzuheben[497]. Bedingt durch den Umstand, dass solch tiefgreifende technische Veränderungen in der Grundstruktur der Internetkommunikation nur selten vorgenommen werden, bieten sich kaum weitere Anknüpfungspunkte für eine proaktive Prävention.

Nachfolgend werden dennoch sämtliche Maßnahmen (präventiv und repressiv) zur Bekämpfung der Internet-Softwarepiraterie hinsichtlich ihrer Effektivität untersucht und beurteilt.

III. Betrachtung der Maßnahmen, die offiziell von privater und staatlicher Seite eingesetzt werden bzw. eingesetzt werden sollen

1. Arbeit der Verbände und Anwälte von Softwareherstellern

Zusammenschlüsse von Softwareherstellern nehmen die wichtigste Rolle im Kampf gegen Internet-Softwarepiraterie ein. Neben den beiden großen internationalen Vereinigungen *Software & Information Industry Association (SIIA)* und *Business Software Association (BSA)* gibt es eine Vielzahl kleinerer Verbände, die sich meist anhand der Branchenzugehörigkeit ihrer Mitglieder unterscheiden (z.B. Verbände für Hersteller von Spiele- und Unterhaltungssoftware, Musiksoftware etc.).

a) Maßnahmen der *Software & Information Industry Association* (*SIIA*)[498] bzw. *Software Publishers Association* (*SPA*)[499]

Die *SIIA* entstand am 01.01.1999 aus einer Fusion der *Software Publishers Association* (*SPA*) und der *Information Industry Association* (*IIA*). Hauptaufgaben des Verbandes sind Repräsentation, Beratung und Wahrnehmung der urheberrechtlichen Interessen der über 1.400 Mitgliedsunternehmen. Der Name *SPA* wird auch nach der Fusion weitergeführt, die *SPA* ist nunmehr die offizielle Division der *SIAA* zu Bekämpfung aller Arten von Softwarepiraterie.

Schon vor der Fusion mit der *IIA* war die in Washington D.C. ansässige *SPA* die bekannteste Organisation im Kampf gegen Softwarepiraterie. Unter ihrem damaligen Direktor *Ken Wasch*, der

---

[497] Ausführliche Information zum sogenannten IPv6 finden sich unten in Teil 2, C. III. 3.
[498] http://www.siia.net.
[499] http://www.spa.org.

mittlerweile Präsident der *SIIA* ist, nahm die *SPA* über Jahre hinweg die Interessen ihrer Mitglieder wahr, zu denen neben der Bekämpfung der Softwarepiraterie jene Aufgaben gehörten, die mittlerweile von der Dachorganisation *SIIA* übernommen werden – z.B. Vertretung der Softwarehersteller bei GATT-Verhandlungen, Veröffentlichung von Marktdaten, Herausgabe eines Newsletters für Mitglieder etc.. Neben den jährlichen Mitgliedsbeiträgen, die die Mitgliedsunternehmen an die *SIIA* zu entrichten haben, finanziert sich die *SPA* über Einnahmen aus Razzien bei Unternehmen, die Raubkopien auf ihren Rechnern einsetzen. Bis zu 100.000 US-Dollar Strafe müssen die ertappten Unternehmer pro raubkopiertem Produkt (nicht pro Kopie) an die *SPA* zahlen. Kritiker monieren, dass das Geld nicht an die Softwarehersteller zurückfließt, sondern dass sich die *SPA* über Razzien direkt „die Taschen fülle".[500] Bereits 1993 „erwirtschaftete" die Vereinigung 3,6 Millionen US-Dollar durch die Beilegung von angedrohten oder eingeleiteten Gerichtsverfahren gegen Softwaresünder. Nach erfolgreichen Razzien werden im Regelfall Pressemitteilungen von der *SPA* herausgegeben, die bei den betroffenen Unternehmen für eine empfindliche Rufschädigung sorgen können. Diese Vorgehensweise findet ebenfalls keine ungeteilte Zustimmung.[501]

Speziell zur Bekämpfung der Internet-Softwarepiraterie wurde von der *SPA* eine Kampagne namens *Internet Anti-Piracy Campaign (IAPC)* ins Leben gerufen. Hauptziel ist es, die Zusammenarbeit mit ISPs, Serverbetreibern und Endnutzern zu pflegen und zu fördern. Zur Kampagne gehört unter anderem Aufklärungsarbeit in Schulen, Universitäten und Unternehmen. Auch über die Homepage der *SIIA/SPA*[502] wird Öffentlichkeitsarbeit geleistet. Hier finden sich neben Informationen zur aktuellen Rechtslage Hinweise darauf, wie man sein Unternehmen oder zu administrierende Server vor dem Missbrauch durch Softwarepiraten schützen kann.

Über eine kostenlose Telefon-Hotline oder per E-Mail kann jedermann anonym Urheberrechtsverstöße bei der *SPA* melden. Nicht selten erhält die *SPA* Hinweise von verärgerten ehemaligen Angestellten, die sich an ihrem früheren Arbeitgeber rächen wollen. In diesem Fällen schickt die *SPA* entweder eine Abmahnung (einen sogenannten Cease and Desist Letter) oder beantragt eine Anhörung, bei der die Betreiber des verdächtigten Unternehmens darlegen müssen, dass jedes einzelne Programm lizenziert wurde; andernfalls strengt sie direkt einen Prozess an. In 5% aller Fälle – nämlich dann, wenn offen-sichtlich ist, dass urheberrechtliche Bestimmungen verletzt wurden – wird sofort eine Razzia veranlasst.[503]

Abmahnungen richtet die *SPA* auch an Betreiber von illegalen Internetseiten. 1995 wurden pro Woche ungefähr zehn Cease and Desist Letters an Betreiber von Warez-Homepages geschickt. Mittlerweile dürfte sich die Zahl der Abmahnungen auf ein Vielfaches erhöht haben. Ungefähr 90% der Serverbetreiber schließen die Seiten daraufhin freiwillig und unmittelbar; sollte dies nicht der Fall sein, wird ein Prozess eingeleitet.[504] Um an die Adressen der Betreiber der entsprechenden Seiten zu

---

[500] *Fryer*, **Wired Magazine** 3.05 – Mai 1995.
[501] Vgl. *Fryer*, **Wired Magazine** 3.05 – Mai 1995.
[502] http://www.siia.net/piracy/default.asp.
[503] *Fryer*, **Wired Magazine** 3.05 – Mai 1995.
[504] *Pogue*, **Macworld.com**, Oktober 1997.

gelangen, ist eine enge Zusammenarbeit mit den Providern unabdingbar. Sofern klar ersichtliche Rechtsverstöße vorliegen, und der Betreiber der Seite nicht erreichbar ist, können die Provider die illegalen Seiten im Auftrag der *SPA* selbst von ihren Servern nehmen. Das Unschädlichmachen einer Internet-Seite wird im Szenejargon als „Busting" oder „Bust" bezeichnet und ist trotz des reaktiven Charakters als eine der derzeit effektivsten Maßnahmen gegen Internet-Softwarepiraterie anzusehen.

b) Maßnahmen der *Business Software Alliance* (*BSA*)[505] und von *Microsoft*

1992 übertrugen die Firmen *Microsoft, Lotus, WordPerfect, Aldus* und *Autodesk* ihre Bemühungen auf die ebenfalls in Washington D.C. ansässige *BSA*, da ihnen die Arbeit der *SPA* nicht effektiv genug erschien. Die *BSA* genießt aufgrund der großen Namen in ihrer Mitgliederliste einen eher elitären Ruf und gilt in Fachkreisen als verlängerter Arm für die Durchsetzung der Interessen von *Microsoft*[506]. Mitglieder der *BSA* in Deutschland sind unter anderem *Adobe Systems, Apple Computer, Attachmate, Autodesk, Corel, Juhu Media, Microsoft, Symantec* und *Visio*. Wie bei der *SPA* fließt auch bei der *BSA* das Geld aus Prozessen und Vergleichen in einen eigenen Fonds zurück. Mit Niederlassungen in 55 Ländern ist die Arbeit der *BSA* internationaler ausgerichtet als die der *SIIA*. Die deutsche Niederlassung der *BSA* kümmert sich schwerpunktmäßig um Delikte im Inland[507].

Microsoft unterhält eine eigene Anti-Piracy Division, die eng mit der *BSA* zusammenarbeitet. In Europa leiten fünf Chefermittler die Verfolgung von Softwarepiraten. Die Namen der Ermittler sind nicht bekannt, gleiches gilt für die Namen der zeitweise mit Ermittlungen beauftragten Detekteien. Nach Angaben des Leiters der deutschen *Microsoft*-Ermittler ist "das Geschäft [...] nicht ganz ungefährlich – vor allem bei Ermittlungen in Osteuropa".[508]

Die Aktivitäten der *BSA* und von *Microsoft* gliedern sich grob in die folgenden Bereiche: Reduzierung der Raubkopierate durch eigene Ermittlungen im Vorfeld von strafrechtlichen und zivilrechtlichen Gerichtsverfahren, internationale Zusammenarbeit mit Behörden und Providern, Aufklärungsarbeit und schließlich Einflussnahme auf die urheberrechtliche Gesetzgebung.

(1) Eigene Ermittlungen

Ziel der Ermittlungen ist in erster Linie, illegale Webseiten aufzuspüren und zu sperren. In letzter Zeit gibt die *BSA* verstärkt Hinweise direkt an die Provider, um schnellstmöglich die Schließung der Warez-Seiten zu erreichen. In manchen Fällen werden die entsprechenden Informationen direkt zur Strafverfolgung an die Behörden weitergegeben. Nach ersten Erfolgen in den USA setzt die *BSA* mittlerweile auch in Europa verdeckte Internet-Ermittler ein, um Piratenseiten aufzuspüren. Nach Aussage von *Georg Herrnleben*, dem Europa-Chef der *BSA*, arbeiten 15 Computerspezialisten an einem geheimen Ort in London, die für die *BSA* mit Hilfe von Suchmaschinen rund um die Uhr das Internet nach verdächtigen Websites durchkämmen[509].

---

505 http://www.bsa.org, http://www.bsa.de.
506 Vgl. *Fryer*, **Wired Magazine** 3.05 – Mai 1995.
507 *Fremerey*, Rauben und Kopieren, **c't** 8/2000, S. 99.
508 **Heise Online News** vom 15.08.2001, http://www.heise.de/newsticker/meldung/20189.
509 **Heise Online News** vom 15.08.2001, http://www.heise.de/newsticker/meldung/20189.

1997 bewirkte der Verband in den USA 17 Razzien, 25 Verurteilungen und 63 Schließungen von Webseiten[510], 1999 sollen es bereits 1.808 Seiten gewesen sein, die dank *BSA*-Initiative vom Netz genommen wurden[511]. Von Januar bis August 2001 seien allein von der europäischen *BSA* 2.500 Webseiten geschlossen worden.[512]

Die Zahl der Angebote, die zwischen August 2000 und April 2001 auf Initiative von *Microsoft* aus dem Internet entfernt wurden, lag bei beachtlichen 38.068.[513] Um illegale Online-Angebote aufzuspüren, setzt *Microsoft* ein speziell entwickeltes Überwachungsprogramm (*Internet Monitoring Tool*) ein, das 24 Stunden täglich im Einsatz ist. Angeblich wird mit Hilfe dieses Tools ein Großteil der Sucharbeit automatisiert, so dass pro Tag mehrere Hundert illegale Seiten identifiziert und lokalisiert werden können.[514] Von März 1999, als *Microsoft* das *Internet Monitoring Tool* entwickelt hat, bis April 2001 sollen insgesamt 79.091 illegale Angebote aus dem Internet beseitigt worden sein. Im Durchschnitt würden monatlich 4.756 Angebote aus dem Web genommen.[515] Durch Einsatz des Überwachungs-Tools seien außerdem 132 Personen ausfindig gemacht worden, die noch vor der offiziellen Einführung von *Windows 2000* bei einem Auktionsanbieter gefälschte CD-ROMs mit dem Betriebssystem offerierten.[516]

In enger Zusammenarbeit mit *Microsoft* führt die *BSA* seit Anfang 1999 eine erfolgreiche Kampagne gegen Internet-Softwarepiraten durch, die sich nicht nur gegen die Betreiber von Warez-Seiten, sondern auch gegen die bereits erwähnten Anbieter von Raubkopien und Plagiaten auf Online-Auktionen richtet. Insgesamt sind nach Angaben von *Microsoft* seit Beginn der Kampagne 43.000 illegale Internetseiten vom Netz genommen worden. Gegen die Betreiber von über 7.500 Websites in 33 Staaten der Erde seien rechtliche Schritte eingeleitet worden. *Microsoft* selbst habe 680, die *BSA* bereits 2.274 sogenannte Takedown Notices verschickt, also Aufforderungen, illegale Software von den entsprechenden Servern zu nehmen. In 64 Fällen habe man Razzien durchgeführt, in 17 Fällen Klage eingereicht.[517]

Eliminierte WWW-Seiten werden von den *BSA*-Ermittlern bis auf die Startseite „ausgeräumt". Auf der Startseite wird ein *BSA*-Logo abgelegt und darauf hingewiesen, dass die Homepage aufgrund illegaler Aktivitäten geschlossen wurde. Auf diese Weise werden die Besucher der Seite von der Aktivität der *BSA* in Kenntnis gesetzt und auf die Illegalität ihres Tuns hingewiesen.

---

[510] Vgl. das Interview mit *Schwarz* (*BSA*), **PC-Intern** 8/1998, S. 37.
[511] *Fremerey*, Rauben und Kopieren, **c't** 8/2000, S. 100.
[512] **Heise Online News** vom 15.08.2001, http://www.heise.de/newsticker/meldung/20189.
[513] **ZDNet News** vom 04.04.2001, http://www.zdnet.de/news/software/0,39023144,2056132,00.htm.
[514] **ZDNet News** vom 03.08.2000, http://www.zdnet.de/news/software/0,39023144,2052803,00.htm.
[515] **ZDNet News** vom 04.04.2001, http://www.zdnet.de/news/software/0,39023144,2056132,00.htm.
[516] **Heise Online News** vom 02.08.2000, http://www.heise.de/newsticker/meldung/11001.
[517] **Heise Online News** vom 02.08.2000, http://www.heise.de/newsticker/meldung/11001.

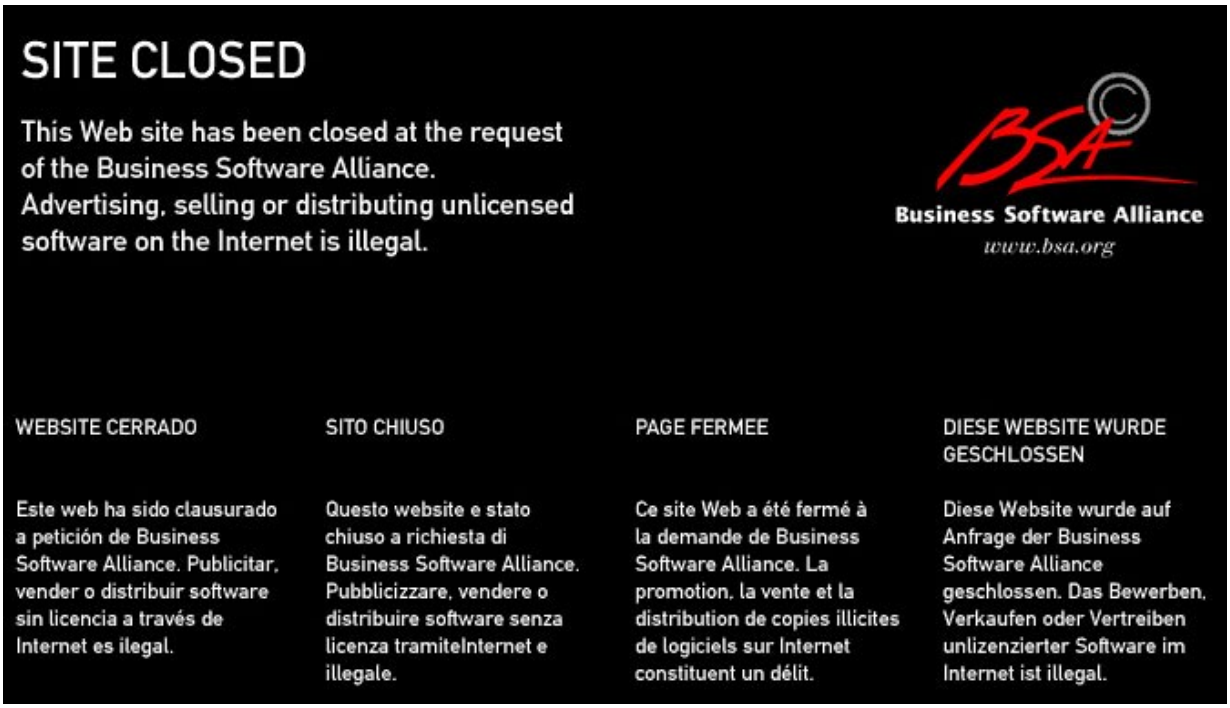


Abbildung 75 – mehrsprachige „Takedown Notice" der *BSA*[518]

Auch die *BSA* und *Microsoft* haben Hotlines eingerichtet, bei denen jedermann Verstöße gegen das Urheberrecht melden kann. Die Nummern der gebührenfreien Telefonhotlines werden nicht nur über die Webseiten sondern auch über Zeitungsannoncen und Mailings verbreitet. Eingehende Anrufe werden nach Aussage der Ermittler vertraulich behandelt. Hinweise können ebenfalls durch das Ausfüllen von vorgefertigten Online-Formularen auf den Homepages gegeben werden. Bis Ende 2000 erreichten die *BSA* in Deutschland 1.318 Hinweise auf illegale Softwareangebote im Internet. Rund 47% der Hinweise wurden vom Softwareverband zurückverfolgt und 93% der entsprechenden Seiten geschlossen.[519] Bei der *Microsoft* Anti-Piracy Hotline gehen monatlich durchschnittlich 1.300 Anrufe ein.[520]

Zu den Maßnahmen der *BSA* gehört weiterhin das Aussprechen von Warnungen, die einem eventuellen Strafverfahren vorgelagert sind. Wird der *BSA* eine E-Mail-Adresse bekannt, die in Zusammenhang mit einer oder mehreren unerlaubten Verwertungshandlungen stehen soll, wird eine E-Mail folgenden Inhalts von der *BSA* an die betreffende Adresse gesendet:

---

[518] Die Abbildung zeigt die österreichische Domain "Warez.at", die nach Angaben der BSA "ein Zentrum der europäischen Softwarepiraterie" war. Auf der Seite wurden vor der Schließung zahlreiche Links zu Raubkopien angeboten und ständig aktualisiert. Auf dem Webspace von Warez.at selbst gab es keine illegale Software zum Herunterladen – **Heise Online News** vom 18.10.2001, http://www.heise.de/newsticker/meldung/21933.
[519] **Heise Online News** vom 07.02.2001, http://www.heise.de/newsticker/meldung/15100.
[520] **ZDNet News** vom 04.04.2001, http://www.zdnet.de/news/software/0,39023144,2056132,00.htm.

Die Business Software Alliance (BSA) hat eine Mitteilung erhalten, dass Ihre E-Mail-Adresse wahrscheinlich dazu genutzt wurde, illegale Aktivitäten zu koordinieren, die im Zusammenhang mit urheberrechtlich geschützten Computerprogrammen der BSA-Mitglieder stehen.
Die BSA repräsentiert die führenden internationalen Hersteller von PC-Software, u.a. Apple, Adobe, Attachmate, Autodesk, Bentley Systems, Corel, Macromedia, Microsoft, Symantec und Visio.
Die Mitglieder der BSA untersagen die Übertragung, Bereitstellung, Upload und Download von nichtlizenzierten Kopien ihrer Produkte. Gleiches gilt für Kauf- und Vertriebsangebote über solche Kopien sowie für entsprechende Werbung. Auch das Erstellen von (Hyper-)Links zu solchen Produktkopien ist untersagt.
Wir nehmen jegliche Art von Urheberrechtsverstößen sehr ernst und verfolgen jedes Jahr Tausende von Firmen und Einzelpersonen wegen solcher Verstöße. Wir fordern Sie auf, Ihre E-Mail- und Internetaktivitäten gründlich zu überprüfen, damit keine Rechtsverstöße von Ihnen ausgehen.

Abbildung 76 – Text einer E-Mail-Verwarnung der *BSA*[521]

(2) Internationale Zusammenarbeit mit Behörden und Providern / Schulungen

Neben der eigenen Fahndung im Internet unterstützt die *BSA* die Arbeit der staatlichen Ermittlungsbehörden. Zur kooperativen Zusammenarbeit des Verbandes mit speziellen Polizeieinheiten gehören unter anderem von der *BSA* organisierte Polizeikongresse und technische Seminare zur Weiterbildung der Behördenangestellten.

Ebenfalls gefördert wird die Zusammenarbeit mit den Internetprovidern. Diese werden angehalten, illegale Einspeisungen über ihre Datenwege zu kontrollieren und zu verhindern, sowie die Ermittlungen durch Herausgabe technischer Informationen, beispielsweise von Internetadressen, zu unterstützen.

(3) Aufklärungsarbeit / Öffentlichkeitsarbeit

Über die Webseiten der *BSA* wird gezielt über das Thema Internet-Softwarepiraterie aufgeklärt. Dort finden sich neben der Belehrung zur geltenden Rechtslage auch Ratschläge für den „normalen Surfer“ zum Schutz vor Raubkopien:

10 Tips zum Schutz vor illegaler Software aus dem Internet

1. Informieren Sie sich bei besonders verlockenden Angeboten
Software, die erheblich unter den üblichen Marktpreisen angeboten wird, ist mit Sicherheit illegal. Informieren Sie sich deshalb vor dem Kauf: Etwa bzgl. Originalverpackung, Lieferumfang, Dokumentation, Lizenz- und Upgradebedingungen. Erkundigen Sie sich nach marktüblichen Preisspannen, beispielsweise in Katalogen, Fachzeitschriften oder im Fachhandel.

2. Bezahlen Sie beim Online-Softwarekauf mit Kreditkarte
Entgegen vieler Warnungen zum Zahlungsverkehr mit Kreditkarte, empfiehlt sich insbesondere beim Online-Shopping dieses Zahlungsmittel. Denn sollten Sie illegale Software erhalten und diese nicht zurückbringen können, dann kann anhand der Kreditkartenabwicklung die Transaktion oft zurückverfolgt und rückgängig gemacht werden.

3. Das Online-Herunterladen von Software direkt von der Webseite eines Herstellers oder Händlers wird immer beliebter und ist meistens legal. Finger weg von folgenden Online-Angeboten:
- OEM-Software (Original Equipment Manufacturer) Diese Versionen dürfen nur in Verbindung mit einem PC, vorinstalliert, verkauft werden.
- AE-Software (Academic Edition) Für sogenannte Schul- oder Studentenversionen müssen Sie sich erst beim Hersteller qualifizieren, bevor Sie die Software direkt oder im Fachhandel beziehen dürfen.
- NFR-Software (Not-for-Resale) Diese Programme sind ausschließlich für Werbezwecke und nicht für den Verkauf bestimmt.
- Demo- und Testsoftware Derart deklarierte Produkte sind nur zu Test- und Demonstrationszwecken gedacht,

[521] Übersetzt aus dem Englischen.

üblicherweise zeitlich befristet einsatzfähig (time bombed) und entsprechen nicht der Vollversion.
- Beta-Software Ähnliches gilt für Vorab-Versionen neuer Software – es handelt sich dabei ebenfalls um Testsoftware, die nicht für den Verkauf bestimmt ist.

4. Laden Sie keine 'Cracks' oder 'Warez'
'Cracks' sind Programme, die den Kopierschutz einer Software knacken. Kaufen Sie keine 'Cracks' oder Programme, die damit illegal verändert wurden.
'Warez' ist das Internet-Stichwort für illegale Software. Laden Sie keine unter diesem Stichwort angebotenen Programme auf Ihren Rechner.

5. Verdächtig – Compilation-CDs mit Software verschiedener Hersteller
Eine Zusammenstellung verschiedenster Software von unterschiedlichen Herstellern ist unüblich. Vergewissern Sie sich direkt beim Hersteller über offiziell gebündelte Softwareangebote und Partnerschaften mit anderen Herstellern.

6. Vorsicht bei umfangreichen Softwarepaketen eines Herstellers
Gleiches gilt für Compilation-CDs, die mit einer umfangreichen, hochwertigen Software-Sammlung eines Herstellers 'unglaublich günstig' angeboten werden – der tatsächliche Wert beläuft sich aber nicht selten auf mehrere tausend Mark. Erkundigen Sie sich auch hier direkt beim Hersteller über aktuell angebotene Softwarepakete.

7. Prüfen Sie die CD-Qualität einfach und schnell
Illegale Compilation-CDs, also auch über das Internet bestellte Software- Sammlungen, unterscheiden sich generell deutlich von kommerziellen, legalen CD-Angeboten: Das Label ist oft handbeschriftet bzw. mit lasergedruckten oder fotokopierten Aufklebern versehen. Der Schriftzug 'CD-R Format für 'Recordable' (bespielbar) ist zu erkennen. CDs dieser Art sind zumeist goldfarben und tragen die Aufschrift des CD-Herstellers (z.B. Sony, Maxell, TDK etc.).

8. Illegaler Handel über Online-Auktionen und -Kataloge
Neben kostenlosen Angeboten im Web gibt es vermehrt Händler, die sich durch den Verkauf illegaler Software in speziellen Online-Auktionen und -Katalogen bereichern. Das ist illegal.

9. Überprüfen Sie die gelieferte Software genau
Achten Sie besonders darauf, dass Sie eine Lizenzvereinbarung erhalten und dass die Lieferung die dazugehörige Dokumentation umfasst.

10. Unterstützen Sie die BSA
Wenn Sie der Meinung sind, dass auf bestimmten Webseiten illegal mit Software gehandelt wird, melden Sie diesen Verdacht der BSA in Deutschland über die gebührenfreie Hotline **0130-171801**.
Illegaler Softwareeinsatz ist mit hohen Risiken verbunden: Auf polizeiliche oder zivile Durchsuchungen folgen Gerichtsverfahren und Schadensersatzforderungen oder sogar Gefängnis.

Abbildung 77 – Aufklärungshinweise von der Homepage der *BSA* (http://www.bsa.de)

Ebenfalls im Zuge von Aufklärungsmaßnahmen versandte *Microsoft* bereits in mehreren Kampagnen Briefe an zahlreiche deutsche Unternehmen. Die Briefe enthalten meist die Aufforderung, in ein beigelegtes Formblatt eine detaillierte Aufstellung über sämtliche im Unternehmen verwendete *Microsoft*-Software einzutragen und genau aufzuschlüsseln, auf wie vielen Rechnern sie jeweils installiert sei und wie viele Lizenzen man wann erworben habe. Ebenfalls enthalten sie Hinweise auf mögliche Schadensersatzforderungen und strafrechtliche Konsequenzen, obwohl keine Verdachtsmomente gegen die betreffenden Nutzer vorliegen. Wird auf ein solches Schreiben nicht reagiert, erhält der Empfänger in der Regel nach zwei Wochen eine Mahnung; eventuell folgen nach Ablauf einer weiteren Frist Anrufe von *Microsoft*.[522]

In Nordrhein-Westfalen versandte *Microsoft* im Mai 2001 derartige Briefe. Die Kampagne richtete sich insgesamt an 75.000 Unternehmen mit bis zu 100 Mitarbeitern und weniger als 50 PCs. Die Adressen der Unternehmen stammten zum Teil aus *Microsoft*s Kundendatenbank, aber auch Betriebe,

---

[522] *H. Schulz*, Winquisition, **c't** 25/2001, S. 54.

die bislang keine *Microsoft*-Programme registriert haben, wurden angeschrieben.[523] Die Rücklaufquote betrug immerhin 20%.[524]

Die beschriebenen Kampagnen stehen vor allem in der Kritik, weil *Microsoft* in den meisten Fällen keinen Anspruch auf Auskunft habe[525], und die Schreiben in einem Tonfall gehalten seien, der eher an ein Ermittlungsverfahren als an wohlgemeinte Aufklärung erinnere.[526] Die Verärgerung, mit der ehrliche Kunden auf die unterschwellige Anschuldigung der Raubkopiererei reagieren, nimmt *Microsoft* jedoch bewusst in Kauf: *Birgit Strobel*, zuständig für Presse- und Öffentlichkeitsarbeit zum Thema Pirateriebekämpfung, nahm folgendermaßen Stellung zur Kritik: „Um das Bewusstsein dafür zu wecken, dass der Einsatz nicht-lizenzierter Software kein Kavaliersdelikt ist, muss man schon scharfe Worte wählen; nur das Aufzeigen möglicher Konsequenzen erzeugt den Druck, der nötig ist, um konkretes Handeln zu bewirken".[527]

(4) Einflussnahme auf die Gesetzgebung

Im Kampf gegen die Internet-Softwarepiraterie setzt sich die *BSA* in erster Linie für eine Harmonisierung der Urhebergesetze auf internationaler Ebene ein, denn die Schaffung einer einheitlichen rechtlichen Basis wird als unbedingte Voraussetzung einer erfolgreichen internationalen Verfolgung angesehen.

Weitere Forderungen der *BSA* umfassen striktere Copyright-Gesetze, die sowohl das zeitlich begrenzte wie auch permanente Anfertigen von Kopien abdecken, sowie mehr Verantwortung der Service-Provider für Web-Inhalte und keine generelle Haftungsbeschränkung für selbige.

c) Maßnahmen anderer Verbände bzw. Unternehmen und von Anwälten

(1) *Gesellschaft zur Verfolgung von Urheberrechtsverletzungen* (*GVU*)

Auch die deutsche *Gesellschaft zur Verfolgung von Urheberrechtsverletzungen* (*GVU*)[528] ist im Kampf gegen Softwarepiraterie aktiv. Die in Hamburg ansässige Organisation steht der Polizei seit ihrer Gründung 1984 bei Ermittlungen zur Seite. Die *GVU* hat es sich primär zur Aufgabe gemacht, Verletzungen von Urheber-, Urhebernutzungs- oder Leistungsschutzrechten an Bildtonträgern (Videokassetten etc.) zu verhindern oder zumindest Vorarbeiten für eine Bestrafung der Täter zu leisten. In Zusammenarbeit mit anderen Verbänden setzt sich die *GVU* mittlerweile verstärkt für den Kampf gegen Softwarepiraten ein.

---

523 Im Sommer 1997 sandte die *BSA* Briefe ausschließlich an die Besitzer registrierter *Microsoft*-Produkte, in denen besonders auffällig die Konsequenzen für den illegalen Einsatz von Software geschildert wurden. Zahlreiche Kunden fühlten sich zu Unrecht der Softwarepiraterie verdächtigt, weshalb die Resonanz auf diese Kampagne entsprechend negativ ausfiel – vgl. *Brors*, **c't** 26/1998, S. 17.
524 *H. Schulz*, Winquisition, **c't** 25/2001, S. 54.
525 Dies ist zutreffend, es sei denn, der Kunde hat ein sogenanntes Volumenlizenzangebot abgeschlossen, bei dem er sich vertraglich zur Auskunft verpflichtet hat – *H. Schulz*, Winquisition, **c't** 25/2001, S. 54.
526 *H. Schulz*, Winquisition, **c't** 25/2001, S. 54.
527 *H. Schulz*, Winquisition, **c't** 25/2001, S. 54; *Siering*, Lizenz-Kontrolle, **c't** 14/2001, S. 30.
528 http://www.gvu.de.

Die *GVU* beschäftigt ein eigenes Ermittler-Team von ehemaligen Polizeibeamten, EDV-Spezialisten und Juristen, um den illegalen Handel mit Entertainment-Software wie Computergames und digitalen Spielfilm-CDs zu unterbinden. "Wir arbeiten aber nicht nur am Computer. Wenn wir auf verdächtige Angebote im Internet stoßen, beginnen verdeckte Ermittlungen vor Ort, z.B. Testkäufe bei den Händlern. Ist die Ware illegal, werden die Behörden eingeschaltet", so *GVU*-Ermittlungsleiter *Bernd Kulbe*. Sein zehnköpfiges Team sorgte im Jahr 2000 für die Einleitung von rund 1.000 Strafverfahren.[529]

Bei einer routinemäßigen Überwachung des Internet ist der *GVU* 1999 ein großer Schlag gegen einen Ring von Profit-Pirates gelungen. Die Ermittler wurden auf eine Gruppe von professionell agierenden Softwarepiraten aufmerksam, die Compilation-CDs[530] hergestellt und über das Internet angeboten hatten. Nach Testkäufen und Observationen griff die Kriminalpolizei ein und konnte 54.000 CD-Sets sicherstellen, die unter dem Namen *„Akira"* vertrieben wurden.[531]

(2) *Verband der Unterhaltungssoftware Deutschland (VUD)*

Ebenfalls eng zusammen mit der Kriminalpolizei arbeitet der *Verband der Unterhaltungssoftware Deutschland* (*VUD*)[532]. Mit über 1.000 Mitgliedern ist der *VUD* der größte Zusammenschluss der Softwarebranche auf nationaler und europäischer Ebene. Der *VUD*, der vor allem die Interessen der Hersteller von Computerspielen vertritt, ist besonders stark von den Auswirkungen der Softwarepiraterie betroffen. Neben Raubkopien, die von Privatpersonen an Freunde weitergegeben werden (insbesondere bei der sogenannten Schulhofpiraterie[533]), ist dem *VUD* vor allem die gewerbliche Herstellung und Verbreitung von CD-ROMs ein Dorn im Auge.

Die deutschen Verbände sind hinsichtlich der Bekämpfung der Internet-Softwarepiraterie nicht mit den großen internationalen Verbänden zu vergleichen. Ihre Arbeit beschränkt sich meist auf das Geben von Hinweisen an Polizei bzw. Staatsanwaltschaften und auf das Bereitstellen von Informationen zur (Urheber-) Rechtslage auf den eigenen Homepages. Die eigentlichen Bestrebungen fokussieren sich auf die Bekämpfung der Produktpiraterie, wobei die *GVU* in besonderem Maße gegen Film- bzw. Videopiraterie vorgeht.

(3) *Interactive Digital Software Association (IDSA)*

Die Interactive Digital Software Association (IDSA)[534] ist ebenfalls ein Verband für Softwarehersteller aus dem Bereich Video- und Computerspiele für Konsolen und PCs. Die Fahnder der *IDSA* sind im Internet aktiv, wobei sich das Engagement nicht nur direkt gegen Warez-Gruppen, sondern auch gegen Produktpiraten (Produktfälscher) richtet, die über das Internet für Mailorder von Raubkopien

---

[529] **Heise Online News** vom 15.08.2001, http://www.heise.de/newsticker/meldung/20189.
[530] Siehe oben Teil 2, A. V. 3.
[531] **c't** 3/2000, S. 60.
[532] http://www.vud.de.
[533] Nach Angaben des *VUD* werden 50% aller Raubkopien über den Schulhof vertrieben, vgl. **ZDNet News** vom 22.10.1999, http://www.zdnet.de/news/business/0,39023142,2049323,00.htm.
[534] http://www.idsa.com.

werben. Präsident der *IDSA* ist derzeit *Doug Lowenstein*, dessen Name in der Warez-Szene mehrfach an ungewöhnlichen Stellen auftauchte. Seine Kommentare zu einem Prozess[535] gegen einzelne Softwarepiraten hatten zur Folge, dass er selbst als Supplier in den nächsten NFO-Dateien der Warez-Gruppe erwähnt wurde. Solche „humoristischen Attacken" sind keine Seltenheit in der Szene. Auch *CCS*[536]-Chef *Dave Powell* ist eine beliebte Zielscheibe für Hohn und Spott der Softwarepiraten.

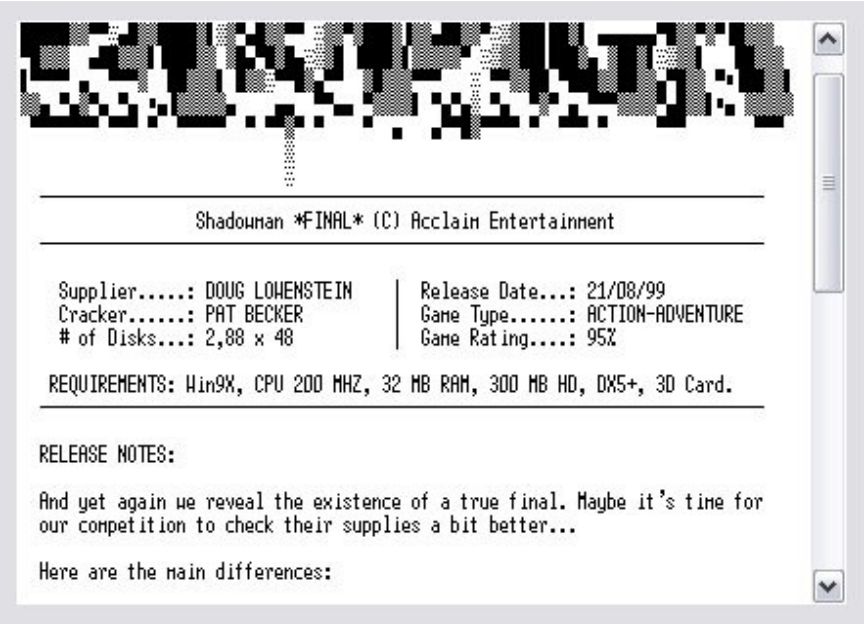


Abbildung 78 – Auszug aus einer NFO-Datei

(4) Anwälte

Nicht nur Verbände nehmen die Interessen der von Piraterie betroffenen Unternehmen wahr. Viele Softwarehersteller beschäftigen ganze Stäbe von Detektiven und Anwälten damit, Täter ausfindig zu machen und zur Rechenschaft zu ziehen. In der Regel wird zunächst eine Abmahnung mitsamt einer Aufforderung versendet, die bis jetzt entstandenen (Ermittlungs-)Kosten zu zahlen. Wenn der Täter sich nicht fügt, wird ein Zivil- oder Strafprozess angestrengt.

Um Beweise zu erlangen, fordern manche Anwälte inkognito Listen bei Raubkopierern an.[537] Werden Raubkopien über Webseiten zum Kauf angeboten, hinterlassen die Täter dort in der Regel eine E-Mailadresse, über die man leicht mit ihnen in Kontakt treten kann. In der Vergangenheit soll es vorgekommen sein, dass ein Anwalt aus Süddeutschland zumeist jugendliche Täter zum Raubkopieren von Computerspielen verleitete, indem er gefälschte Briefe als Antwort auf Zeitungsannoncen versendete, mit denen die Jugendlichen Tauschpartner gesucht hatten. Als Absender wählte er meist Mädchennamen, und die Inhalte der orthographisch mangelhaften Briefe appellierten an das Mitleid und das Ehrgefühl der naiven Täter, welche in den meisten Fällen ihre Listen oder gar

---

[535] http://www.idsa.com/releases/MODELcase.html.
[536] Siehe unten Teil 2, C. III. 1. c) (5).
[537] **GameStar** 12/1998, S. 79.

Programme an die vermeintlichen Mädchen schickten. Diese erhielt jedoch realiter der Anwalt, der sofort eine Abmahnung verfasste, die mit einer Kostennote von durchschnittlich 399 DM (entspricht ca. 204 €) belegt war.[538] Nachdem diese Vorgehensweise der Öffentlichkeit bekannt wurde, fielen die Reaktionen äußerst negativ aus, und der nicht unumstrittene Anwalt hat bis heute bei Teilen der Internetgemeinde mit dem Ruf eines „Abzockers" zu kämpfen. Unbestritten handelt es sich bei der beschriebenen Praxis um eine effektive Methode, Softwarepiraten zur Leistung von Schadensersatz zu veranlassen und einzuschüchtern, allerdings hinterlässt sie insoweit einen bitteren Beigeschmack, als ein Anwalt bewusst die Rolle eines „agent provocateur" einnimmt[539].

Anzumerken ist schließlich, dass die beschriebene Methode nur bei Profit-Pirates Erfolg verspricht. Der größte Teil der Internet-Softwarepiraten meidet Schnittstellen zur realen Welt, welche sich erst durch finanzielle Transaktionen ergeben.

(5) Private Copyright-Überwachungsdienste

Mittlerweile haben zahlreiche privatwirtschaftliche Unternehmen und Detekteien das Aufspüren von Raubkopien als Marktlücke entdeckt und bieten den Softwareherstellern ihre kostenpflichtigen Dienste an.

Großes Engagement im Kampf gegen Internet-Piraten legt der *Copyright Control Service* (*CCS*) an den Tag. Beim *CCS* handelt es sich um ein Unternehmen mit Sitz in England, das seine Dienste bevorzugt Herstellern von professioneller Musiksoftware anbietet. Ungefähr 80% der Pro-Audio-Softwarehersteller arbeiten mit dem *CCS* zusammen.

Nach Aussage von Geschäftsführer *Dave Powell* hat der *CCS* bewirkt, dass in 12 Monaten ganze 5.000 Webseiten geschlossen wurden und rund 500.000 raubkopierte Computerprogramme aus dem Netz entfernt wurden. Hierzu pflegt *Powell* „Fasttrack Relationships" mit 1.000 Providern weltweit.[540]

Wenn ein *CCS*-Ermittler ein rechtswidriges Internetangebot ausgemacht hat, beauftragt er in der Regel zunächst eine Anwaltskanzlei damit, den entsprechenden Provider unter Strafandrohung aufzufordern, den Namen und die Anschrift des Kunden mitzuteilen. Sobald dem *CCS* diese Informationen vorliegen, was meist binnen 48 Stunden der Fall ist, wird ein Abmahnschreiben an den Verletzer gesendet. Hierin verlangen die Anwälte 3.000 US-Dollar, um die Kosten für die Arbeit des *CCS* zu decken, plus 1.000 US-Dollar für jeden einzelnen (Urheber-)Rechtsverstoß. Im Gegenzug erklären sie sich bereit, auf den Rechtsweg zu verzichten, falls der Täter den Forderungen nachkommt. Andernfalls wird Klage erhoben.[541] Angesichts der Rechtslage in den USA, die für jede

---

[538] So dargestellt von *Zimmermann*, S. 29 ff., der das Aufspüren und Denunzieren von Softwaresündern durch Anwälte als Ausnutzen einer Marktlücke bezeichnet. Die Praktiken des Münchener Anwalts stellen für ihn einen Verstoß gegen die guten Sitten dar. Eine angeblich echte Kopie eines der umstrittenen Briefe findet sich unter http://homepage.ruhr-uni-bochum.de/martin.vogel/prog/tanja.jpg.

[539] Dies gilt vor allem dann, wenn ein Anwalt ohne Einwilligung des Rechtsinhabers jugendliche Raubkopierer auffordert, für ihn Programmkopien anzufertigen. In diesen Fällen liegt bereits mit der Vervielfältigung eines Programms eine vollendete Tat gemäß § 106 UrhG vor, was zu einer Strafbarkeit des Anwalts wegen Anstiftung führt. Denn der „agent provocateur" ist nur dann mangels Anstiftervorsatz von einer strafrechtlichen Verantwortlichkeit frei, wenn er es lediglich zu einem Versuch der Tat kommen lassen will, vgl. Schönke/Schröder-*Cramer/Heine*, § 26 StGB, Rdnr. 20. Zu den rechtlichen Bedenken an dem oben beschriebenen Vorgehen siehe auch *V. König*, **c't** 1/1994. S. 46 f.

[540] **Wired News** vom 29.01.2000, http://www.wired.com/news/technology/0,1282,33940,00.html.

[541] *Learmonth*, **The Industry Stadard Europe**, Ausgabe vom 16.02.2001.

einzelnen Copyrightverstoß eine Strafe i.H.v. 100.000 US-Dollar vorsieht, handelt es sich dabei um ein recht faires Angebot.

Trotz intensivster Bemühungen, über den IRC Mitglieder sogenannter Audiowarez-Gruppen aufzuspüren, ist dem *CCS* in monatelangen Recherchen nur ein Einzeltäter ins Netz gegangen: Ein in Köln lebender Softwarepirat hatte im IRC mit der Qualität seiner Cracks geprahlt und Raubkopien in das UseNet eingespeist, woraufhin *CCS* den Access-Provider des Crackers kontaktierte und diesen bat, Backups der entsprechenden Logfiles zu machen[542].

Die Arbeit des *CCS* ist allerdings nicht unumstritten, da neben Warez-Seiten diverse Diskussionsforen aus dem Bereich Musikproduktion geschlossen wurden, in denen angeblich Informationen über die Verwendung und Beschaffung von Raubkopien ausgetauscht wurden. Mit diesen Maßnahmen traf der *CCS* vor allem bei den US-amerikanischen Internetnutzern einen empfindlichen Nerv, da sie die Schließung der Foren als einen klaren Verstoß gegen den verfassungsrechtlichen Grundsatz der „freedom of speech" ansahen.

Andere Copyright-Überwachungsdienste sind z.B. *Software Army International*, *Timeservice* oder *SECUMA*. In der Regel bieten sie neben Internetrecherchen auch weiterführende Ermittlungen wie Observationen und Testkäufe an.

Alles in allem entsprechen die von den Verbänden und Anwälten geschnürten Maßnahmenpakete dem aktuellen Stand der Entwicklung. Man hat erkannt, dass die größte Gefahr hinsichtlich der Verbreitung von Raubkopien vom WWW ausgeht und bekämpft Warez-Webseiten mit einem entsprechenden Engagement. Für die Kontrolle der wesentlich unzugänglicheren Bereiche des Internet werden kaum Ressourcen verschwendet. Sämtliche Maßnahmen richten sich in erster Linie gegen Unternehmen, die illegale Software einsetzen und gegen Betreiber von Internetseiten, über die Raubkopien verbreitet werden. Der private Endnutzer von Raubkopien wird nicht von den Verbänden und Herstelleranwälten verfolgt, sofern er ohne Gewinnabsicht handelt.

Die Vorgehensweise ist auch in wirtschaftlicher Hinsicht sinnvoll: *Microsoft* wurden zwischen Januar 2000 und April 2001 insgesamt bei Vergleichen und Gerichtsurteilen 19,8 Millionen € zugesprochen.[543]

Allerdings fällt immer wieder auf, dass der Umgang mit Informationen zum Thema Raubkopien in der Öffentlichkeit ungeschickt wirkt. Dies ist insofern nachvollziehbar, als eine ständige Gratwanderung zwischen dem Warnen vor illegaler Software und dem gleichzeitigen Wecken von Neugier unternommen werden muss. Denn die Verwendung einschlägiger Szenebegriffe an der falschen Stelle kann auch zur Folge haben, dass sich bisher unbescholtene Nutzer auf die Suche nach Raubkopien machen. Bei dem bereits mehrfach erwähnten geringen Unrechtsbewusstsein bezüglich raubkopierter Computerprogramme ist dies nicht unwahrscheinlich. Absolut verfehlt – ja geradezu paradox – ist es, die bereits erwähnten „Aufklärungsbriefe" ausgerechnet an registrierte Nutzer zu schicken. Auch Telefonhotlines und Online-Meldeformulare stehen nicht zu Unrecht in der Kritik. Durch solche Einrichtungen können Racheakte und Denunziationen eine völlig neue Dimension erlangen, da sie weitgehend anonym ausgeführt werden können.

---

[542] **KEYBOARDS Online News** vom 09.09.1999, http://www.keyboards.de.
[543] **ZDNet News** vom 04.04.2001, http://news.zdnet.de/story/0,,t101-s2056132,00.html.

2. Entwicklungsstrategische Maßnahmen von Softwareherstellern

a) Kopierschutzmaßnahmen

Es gilt zu bezweifeln, dass neue Arten des Kopierschutzes dem Problem einen Riegel vorschieben können. Die Erfahrung zeigt, dass es kaum einen unüberwindbaren Kopierschutz gibt.[544] Nach der zutreffenden Aussage von *Mike Wilson* – Geschäftsführer des Softwareherstellers *Ion Storm* – verschaffen Kopierschutzmaßnahmen den Unternehmen lediglich einen kurzen zeitlichen Vorsprung vor den Crackern: "copy protection schemes are just speed bumps"[545]. Beträgt dieser Vorsprung allerdings eine größere Zeitspanne, ist das primäre Sicherungsziel der Softwarehersteller erreicht. Da das Interesse an einer Raubkopie in den meisten Fällen ungefähr vier Wochen nach Markteinführung der Software nicht mehr vorhanden ist, muss ein Kopierschutz für ebendiese Frist greifen.[546] Es ist jedoch eher selten, dass eine Software für mehrere Wochen „ungecrackt" bleibt. Spätestens am Tag der Markteinführung sind die ersten illegalen Kopien im Internet zu finden. Etwas anderes gilt lediglich für aufwändige Dongle-Cracks oder Programme, die durch Online-Server-Checks geschützt sind.

Außerhalb des Internet haben Kopierschutzmaßnahmen noch immer ihre volle Berechtigung. Durch neue effektive Systeme wie *Laserlock*[547], *Safedisk*[548], *Securom*[549], *DiscGuard*[550] und *CD-Cops*[551] wird dem normalen Anwender das Vervielfältigen einer Original-CD-ROM mittels eines CD-Brenners unmöglich gemacht. Diese Maßnahmen, die beim Kampf gegen die sogenannte Schulhofpiraterie Wirkung zeigen, sind jedoch im Hinblick auf das Internet obsolet, da die Programme durch die Cracker vom physikalischen Datenträger losgelöst und verändert werden. Mit dem Know-how, über das ein durchschnittlicher Cracker verfügt, können die erwähnten Kopierschutzsysteme leicht überwunden werden.

b) Zwangsaktivierung

Nicht zuletzt wegen der Entwicklung, die von der Distribution auf CD-ROM zum reinen Online-Vertrieb von Software führt, werden ständig neue Konzepte entwickelt, die das Kopieren von Software uninteressant machen sollen. Ein neuer und populärer Ansatz ist in diesem Zusammenhang die sogenannte Zwangsaktivierung. Bislang waren die Kunden gewohnt, Standardsoftware nach dem Kauf sofort ohne jede Einschränkung einsetzen zu können, mittlerweile gibt es jedoch einige Programme, die nur für eine bestimmte Zeit uneingeschränkt nutzbar sind. Ist eine gewisse Frist

---

544 *McCandless*, **Wired Magazine** 5.04 – April 1997.
545 *McCandless*, **Wired Magazine** 5.04 – April 1997.
546 Vgl. **ZDNet News** vom 22.10.1999, http://www.zdnet.de/news/business/0,39023142,2049323,00.htm.
547 http://www.laserlock.com.
548 http://www.c-dilla.com.
549 http://www.sonydadc.com.
550 http://www.discguard.com.
551 http://www.linkdata.com.

abgelaufen bzw. wurde eine bestimmte Anzahl von Programmstarts ausgeführt[552], versagt die Software ihren Dienst und muss beim Hersteller freigeschaltet werden.[553]

Microsoft hat mit der Einführung von *Windows XP* erstmals ein Betriebssystem veröffentlicht, das zwangsaktiviert werden muss. Nach der ersten Installation läuft es für 30 Tage, dann muss der User über das Internet oder per gebührenfreier Telefonnummer bei *Microsoft* einen Aktivierungscode anfordern, der sein Betriebssystem endgültig aktiviert. Der Aktivierungscode wird vom Hersteller unter Einbeziehung einer sogenannten Produkt-ID berechnet, die auf jedem Rechner individuell generiert wird. Die Produkt-ID enthält entgegen den Befürchtungen zahlreicher Anwender keine personenbezogenen Daten; es werden jedoch die Seriennummern des Systemlaufwerks, des CD-ROM-Laufwerks, der Grafikkarte, der Festplatte, des SCSI-Hostadapters, des IDE-Controllers, die CPU-ID, die MAC-Adresse[554] des Netzwerk-Adapters, der vorhandene Arbeitsspeicher und das Vorhandensein einer Docking-Möglichkeit für die Erstellung dieser ID abgefragt. Dabei verwendet *Microsoft* aber nicht die tatsächlichen Kennungen wie die MAC-Adresse, sondern einen daraus gebildeten Hashwert[555], aus dem sich keine Rückschlüsse auf konkrete Hardware-Spezifikationen ziehen lassen. Die Hashwerte fließen verschlüsselt in die Produkt-ID ein. Nach Erkenntnissen des Berliner Unternehmens *Fully Licensed* können bei einem *Windows-XP*-Rechner bis zu drei Hardwarekomponenten ausgetauscht werden, bevor eine neue Aktivierung fällig wird.[556]

Die Aktivierung ist im Gegensatz zu einer Registrierung[557] anonym möglich, und bei der Online-Aktivierung werden laut Angaben von *Microsoft* keine personenbezogenen Daten übermittelt und/oder gespeichert[558].

Auch das aufwändige Aktivierungsverfahren von *Microsoft* ist nicht gegen Umgehungsmöglichkeiten gefeit: Bereits wenige Tage nach dem offiziellen Start der endgültigen *Windows-XP*-Versionen kursierten im Internet zwei verschiedene Umgehungsprogramme, mit denen sich unlizenzierte Versionen des Betriebssystems aktivieren ließen. Beim ersten Programm handelt es sich um ein 700 Kilobyte großes Patch, das den Aktivierungszwang gänzlich abschaltet, sobald es im abgesicherten Modus ausgeführt wird. Das zweite Tool ist ein Keymaker, der in einem komplexen Prozess gültige CD-Schlüssel generiert. Wird ein solcher Schlüssel bei der Installation von *Windows XP* als Produkt-ID angegeben, lässt sich die Kopie per Telefon oder Internet-Verbindung freischalten[559].

---

552 Dies gilt z.B. für *Microsofts Office XP*, das sich nach der Installation 50mal starten lässt, bevor es seinen Dienst weitgehend einstellt, vgl. *Siering*, Des Käufers Pflichten, **c't** 13/2001, S. 46 f.

553 Zu den zivilrechtlichen Fragen bzw. Bedenken bezüglich der Aktivierung von Software siehe *Runte*, **CR** 2001, S. 657 ff.

554 MAC steht für Media Access Control. Bei einer MAC-Adresse handelt es sich um eine 48-Bit-lange ID-Nummer, mit der jede Netzwerkkarte (Ethernet-Adapter-Karte) vom Hersteller versehen wird. MAC-Adressen gelten als weltweit eindeutig und unverwechselbar, allerdings kommt es vor, dass die Hersteller bei Kartenkontingenten, die für unterschiedliche Kontinente bestimmt sind, die selben MAC-Adressen verwenden.

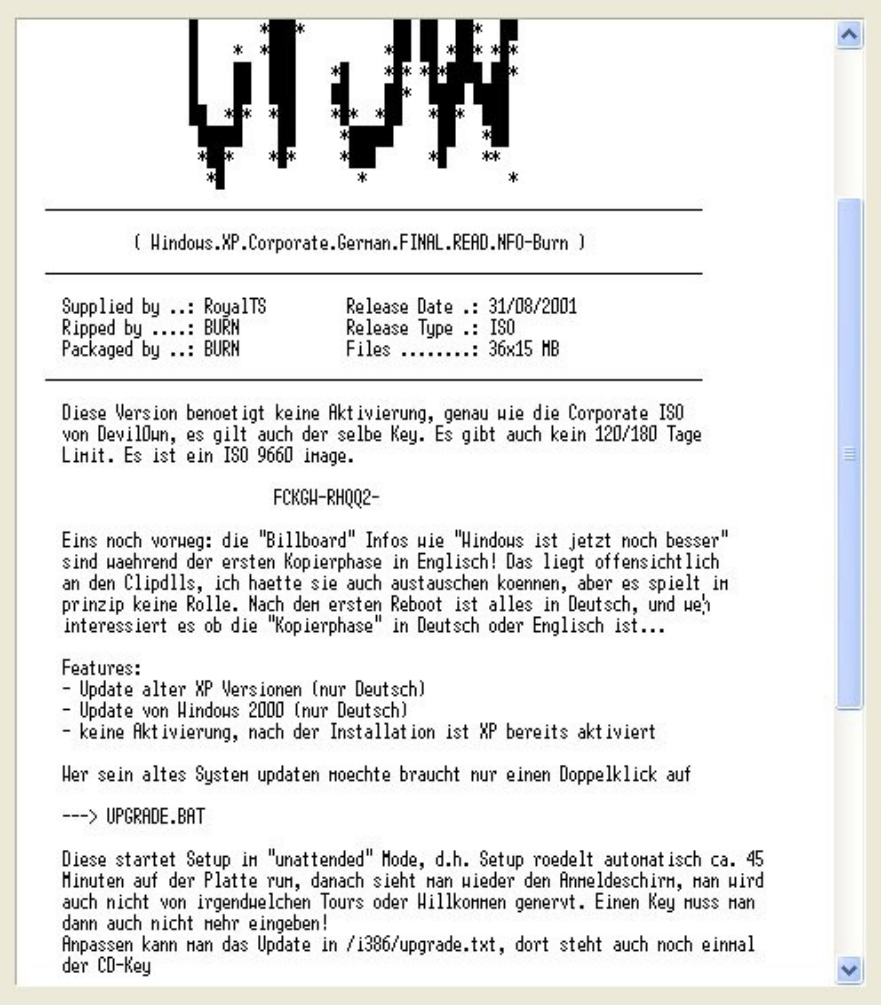
555 Unter einem Hashwert ist in dem geschilderten Zusammenhang die komprimierte Version einer Datei zu verstehen. Der Hashwert entsteht dadurch, dass eine beliebige Datei jeder Größe mit Hilfe eines mathematischen Verfahrens komprimiert wird.

556 *Bremer*, **c't** 15/2001, S. 17.

557 Zur *Windows*-Registrierung siehe Teil 2, C. IV. 2.

558 http://www.microsoft.com/germany/ms/produktaktivierung. Siehe hierzu auch *Siering*, Kaufen verbindet, **c't** 9/2001, S. 132, wo *Witte* eine andere Vorgehensweise als rechtlich bedenklich einstuft. Nach bisheriger Rechtsprechung sei jedenfalls ein „überraschender Zwang zur Registrierung mittels persönlicher Daten" unzulässig.

559 **Heise Online News** vom 12.02.2002, http://www.heise.de/newsticker/meldung/24775.



(Windous.XP.Corporate.German.FINAL.READ.NFO-Burn)

Supplied by ..: RoyalTS Release Date .: 31/08/2001
Ripped by ....: BURN Release Type .: ISO
Packaged by ..: BURN Files .....: 36x15 MB

Diese Version benoetigt keine Aktivierung, genau wie die Corporate ISO von DevilDun, es gilt auch der selbe Key. Es gibt auch kein 120/180 Tage Limit. Es ist ein ISO 9660 image.

FCKGW-RHQQ2-

Eins noch vorweg: die "Billboard" Infos wie "Windous ist jetzt noch besser" sind waehrend der ersten Kopierphase in Englisch! Das liegt offensichtlich an den Clipdlls, ich haette sie auch austauschen koennen, aber es spielt in prinzip keine Rolle. Nach den ersten Reboot ist alles in Deutsch, und wer interessiert es ob die "Kopierphase" in Deutsch oder Englisch ist...

Features:
- Update alter XP Versionen (nur Deutsch)
- Update von Windous 2000 (nur Deutsch)
- keine Aktivierung, nach der Installation ist XP bereits aktiviert

Wer sein altes System updaten moechte braucht nur einen Doppelklick auf

---> UPGRADE.BAT

Diese startet Setup im "unattended" Mode, d.h. Setup roedelt automatisch ca. 45 Minuten auf der Platte rum, danach sieht man wieder den Anmeldeschirm, man wird auch nicht von irgendwelchen Tours oder Willkommen genervt. Einen Key muss man dann auch nicht mehr eingeben!
Anpassen kann man das Update in /i386/upgrade.txt, dort steht auch noch einmal der CD-Key

Abbildung 79 – Auszug aus einer NFO-Datei

Um das Problem der illegalen bzw. nicht erfolgten Aktivierung nachträglich in den Griff zu bekommen, hat *Microsoft* das erste Service-Pack[560] für *Windows XP* („SP1“) so präpariert, dass es solche Betriebssysteme erkennt, die mit einer gestohlenen Seriennummer installiert wurden, und den Update-Vorgang verweigert. Bei Betriebssystemen, die zwar mit einer legal erworbenen Seriennummer installiert wurden, der Aktivierungszwang jedoch mittels eines Patches beseitigt wurde, lässt sich das Service-Pack installieren, allerdings beginnt eine neue Aktivierungsfrist von 30 Tagen zu laufen.

Diese Maßnahme von *Microsoft* wird nicht verhindern können, dass Nutzer nichtlizenzierter Programmversionen in den Genuss des Service-Packs kommen. Denn bereits wenige Tage nach der offiziellen Bereitstellung des Service-Packs befanden sich illegal modifizierte Service-Packs im Umlauf, die sich – befreit von jeglichen „Online-“ oder „Offline-Checks“ – ohne Überprüfung der Seriennummer installieren ließen.

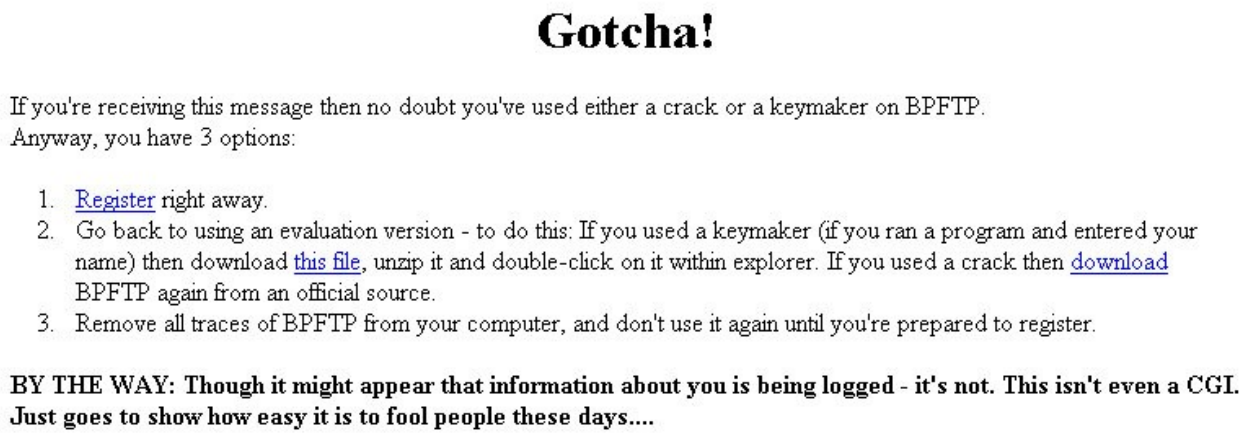
---

[560] Service-Packs enthalten in der Regel Programmaktualisierungen (Updates) und Fehlerbereinigungen (Bugfixes). Sie werden vom Hersteller einer Software nachgeliefert bzw. zum Download bereitgestellt.

c) Piracy Reminder, Schadroutinen etc.

Einzelne Softwarehersteller modifizieren ihre Programme dergestalt, dass sie eine von den Lizenzbestimmungen abweichende Behandlung „bemerken“ und entsprechend reagieren.

So setzt beispielsweise *BulletProof Software*, der Hersteller des populären FTP-Clients *BulletProof FTP,* sogenannte Gotcha-Screens ein, um Nutzer raubkopierter *BulletProof*-Programme zu verwarnen: „Bemerkt“ eine Demo-Version von *BulletProof FTP*, dass sie unrechtmäßig registriert wurde, legt sie einen Schlüssel in der Registry[561] des Computers ab (z.B. unter dem Eintrag „runonce“), der beim nächsten Aufruf des Webbrowsers veranlasst, dass automatisch eine Webseite angesteuert wird, die den ertappten Nutzer auffordert, das Programm entweder zu registrieren oder den ursprünglichen Zustand wieder herzustellen.



Gotcha!

If you're receiving this message then no doubt you've used either a crack or a keymaker on BPFTP.
Anyway, you have 3 options:

1. Register right away.
2. Go back to using an evaluation version - to do this: If you used a keymaker (if you ran a program and entered your name) then download this file, unzip it and double-click on it within explorer. If you used a crack then download BPFTP again from an official source.
3. Remove all traces of BPFTP from your computer, and don't use it again until you're prepared to register.

BY THE WAY: Though it might appear that information about you is being logged - it's not. This isn't even a CGI. Just goes to show how easy it is to fool people these days....

Abbildung 80 – „Gotcha-Screen“ von *BulletProof Software*

Auch die Programmierer des Computerspiels *Black & White* haben eine Routine in ihre Software eingebaut, die erkennen kann, ob der Nutzer eine legale Kopie oder eine Raubkopie verwendet:

---

[561] Bei der Registry handelt es sich um die zentrale Datenbank eines (Windows-)Betriebssystems, in der alle Arten von Konfigurationseinstellungen abgespeichert werden.

Abbildung 81 – „Gotcha-Screen“ des populären Spiels *„Black & White“*

Inzwischen beginnen einige Hersteller damit, ihre Installationsroutinen im System nach bereits installierten Umgehungs- oder Kopierprogrammen suchen zu lassen[562]. Sobald diese entdeckt werden, verweigern die Programme ihre Installation. Erst nach vollständiger Entfernung der unerwünschten Tools lässt sich eine Installation ohne Probleme durchführen.

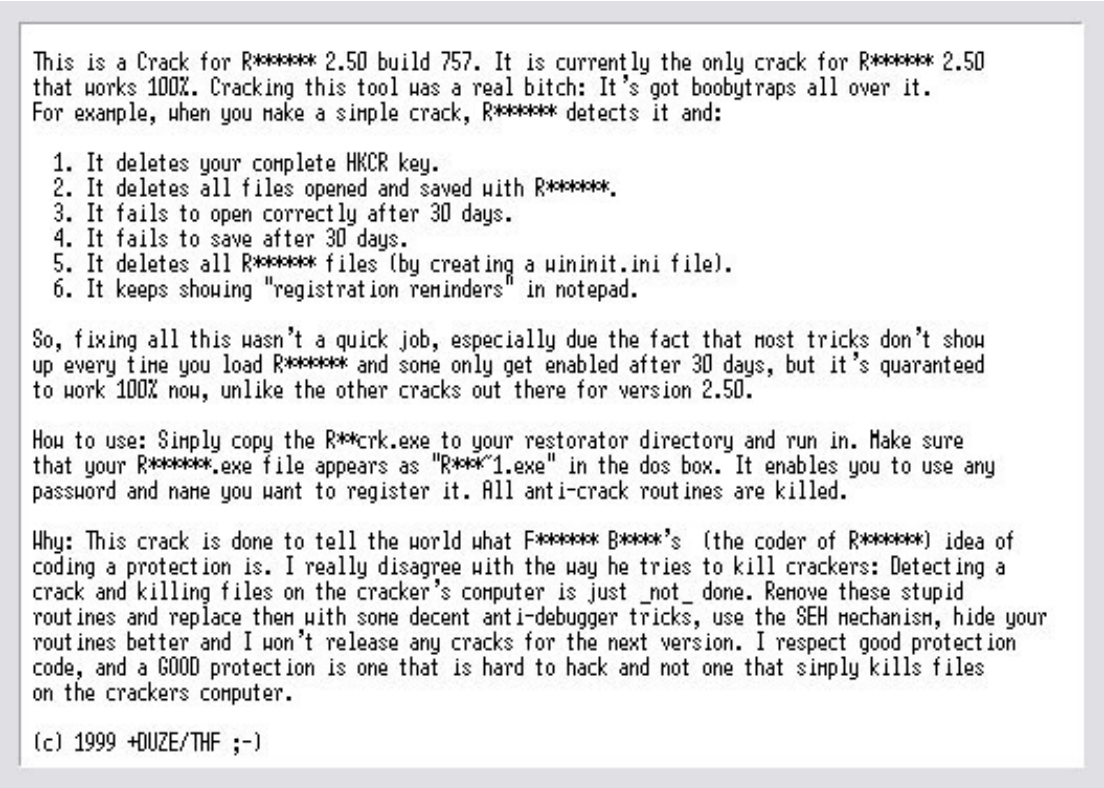
Mit einem ähnlichen „Trick“ verschaffte sich ein deutscher CAD[563]-Softwarehersteller in der Vergangenheit einige neue Lizenzen: Als dem Hersteller bekannt wurde, dass sich ein Dongle-Crack für seine Software im Umlauf befand, verbreitete er präparierte Demo-Versionen einer aktualisierten Programmversion. Nach der Installation der Demo-Version durchsuchte ein Teil des Programms den Rechner des Anwenders nach dem Crack, bzw. nach dem veränderten Programmcode der älteren Programmversion. Sobald die Routine fündig wurde, zeigte sie dem überraschten Nutzer ein Fenster, in welchem sinngemäß mitgeteilt wurde, dass der Nutzer zu einem kleinen Kreis zufällig ausgewählter Anwender der Demo-Version gehöre, der gratis eine registrierte Vollversion erhalten würde, sofern er ein vorbereitetes Formular ausdrucken, ausfüllen und an den Hersteller senden würde. Auf diese Weise erhielt das Unternehmen zahlreiche Zuschriften mitsamt Namen und Anschriften der ertappten Nutzer; anstelle einer Vollversion erhielten diese jedoch neben der Androhung von rechtlichen Schritten eine Rechnung über eine Lizenz der gecrackten Software. Angeblich soll auch eine Rechnung an den *Bundesnachrichtendienst* herausgegangen sein, die – so wie alle anderen Rechnungen – ohne weitere Umschweife beglichen wurde.

---

[562] *Zota*, Klonverbot, **c't** 2/2002, S. 93.
[563] CAD = Computer Aided Design; mit CAD-Programmen lassen sich virtuelle 3D-Modelle von Gegenständen erzeugen. Typische Einsatzgebiete sind z.B. Architekturdesign und Entwicklung von High-Tech Produkten.

Derartige Maßnahmen haben sicherlich einen gewissen Charme, allerdings ist zu bezweifeln, dass sich der verhältnismäßig hohe Aufwand auszahlt. Denn mittlerweile haben auch die Cracker Kenntnis von diesen „Tricks“ erlangt, weshalb es immer schwerer werden dürfte, hiermit Erfolg zu haben.

Deutlich aggressiver gehen andere Hersteller das Problem an, indem sie in ihren Programmen sogenannte Schadroutinen einbauen. Hierunter versteht man Programmaktivitäten, die von bestimmten Ereignissen ausgelöst werden, und bei denen Daten auf dem Rechner des Anwenders manipuliert oder gar zerstört werden.



```
This is a Crack for R****** 2.50 build 757. It is currently the only crack for R****** 2.50
that works 100%. Cracking this tool was a real bitch: It's got boobytraps all over it.
For example, when you make a simple crack, R****** detects it and:

  1. It deletes your complete HKCR key.
  2. It deletes all files opened and saved with R******.
  3. It fails to open correctly after 30 days.
  4. It fails to save after 30 days.
  5. It deletes all R****** files (by creating a wininit.ini file).
  6. It keeps showing "registration reminders" in notepad.

So, fixing all this wasn't a quick job, especially due the fact that most tricks don't show
up every time you load R****** and some only get enabled after 30 days, but it's guaranteed
to work 100% now, unlike the other cracks out there for version 2.50.

How to use: Simply copy the R**crk.exe to your restorator directory and run in. Make sure
that your R******.exe file appears as "R***~1.exe" in the dos box. It enables you to use any
password and name you want to register it. All anti-crack routines are killed.

Why: This crack is done to tell the world what F****** B****'s  (the coder of R******) idea of
coding a protection is. I really disagree with the way he tries to kill crackers: Detecting a
crack and killing files on the cracker's computer is just _not_ done. Remove these stupid
routines and replace them with some decent anti-debugger tricks, use the SEH mechanism, hide your
routines better and I won't release any cracks for the next version. I respect good protection
code, and a GOOD protection is one that is hard to hack and not one that simply kills files
on the crackers computer.

(c) 1999 +DUZE/THF ;-)
```

Abbildung 82 – Auszug aus einer NFO-Datei

Solange die Schadroutine nur Daten des eigenen Programms befällt, sind solche Maßnahmen sicher gerechtfertigt. Anders ist die Situation jedoch zu beurteilen, wenn weitere Daten auf dem Rechner des Anwenders betroffen sind. In diesen Fällen ist eine Strafbarkeit des rachsüchtigen Programmierers nach § 303a StGB wegen Datenveränderung nicht auszuschließen.

Es soll jedoch auch Routinen geben, die nur den eigenen Code befallen. Für das Spiel *Operation Flashpoint* wurde im Frühjahr 2001 vom Hersteller angekündigt, dass es einen neuartigen Kopierschutz namens *Fade* enthalten würde. Erkennt *Fade* nach dem Programmstart, dass eine kopierte Programmversion vorliegt, soll sich der Kopierschutz zunächst unauffällig verhalten. Raubkopierer würden ihn bei einer flüchtigen Überprüfung der Kopie nicht bemerken. Das Spiel soll auf gewohnte Weise starten, erst nach gewisser Zeit greife *Fade* ein und verändere nach und nach Elemente des Spiels, bis dieses irgendwann überhaupt nicht mehr nutzbar sei. Nach Auskunft des

Herstellers soll sich *Fade* im Code des Spiels innerhalb eines konventionellen Kopierschutzverfahrens verbergen, um Crackern den Zugriff und das Umgehen zu erschweren. Ob *Fade* tatsächlich existiert, wird in der Warez-Szene bezweifelt. Schenkt man dem Urteil in einer NFO-Datei Glauben, handelte es sich bei der Ankündigung lediglich um ein Marketing-Manöver:

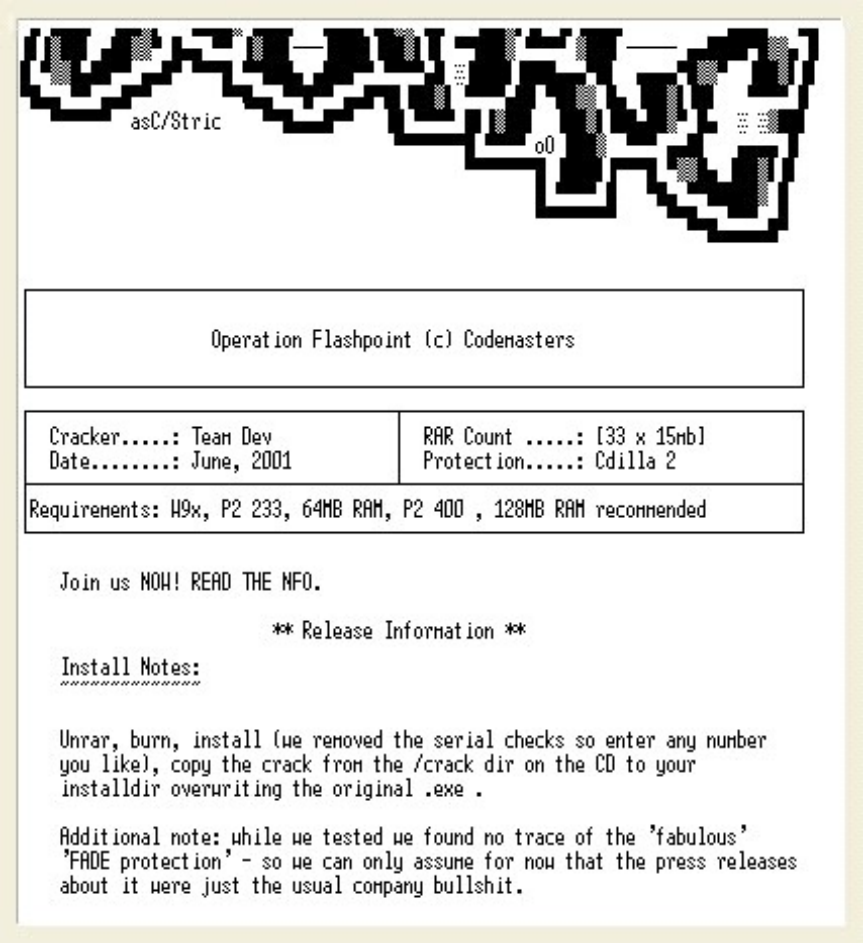


Abbildung 83 – Auszug aus einer NFO-Datei

d) Softwaremiete – insbesondere Application Service Providing

Application Service Providing ist ein recht neues Geschäftsmodell, bei dem Computerprogramme den Nutzern über das Internet gegen eine monatliche Miete zur Verfügung gestellt werden.[564] Die Anwendungen werden im Regelfall über einen Webbrowser aufgerufen, wodurch eine übergreifende Plattformkompatibilität gewährleistet ist. Der Nutzer schließt einen Mietvertrag mit einem Application Service Provider (ASP), der die zu mietenden Programme auf seinen Terminal-Servern installiert hat. Da ein Grossteil der Rechenoperationen auf dem Rechner des Providers ausgeführt werden, muss der Nutzer selbst keinen Hochleistungsrechner besitzen; es genügt ein durchschnittlich ausgestatteter und konfigurierter Computer („Thin Client"). Allerdings ist für flüssiges Arbeiten eine

---

564 Einen ausführlichen Überblick über Application Service Providing bieten *Bager/Kossel*, **c't** 7/2001, S. 190 ff.

schnelle und permanente Internetanbindung unabdingbar. Zur Zeit unternehmen mehrere große Softwarehersteller die ersten Gehversuche im Geschäftsbereich ASP, für den äußerst günstige Prognosen getroffen werden.[565]

Neben Plattform- und Hardwareunabhängigkeit bietet Application Service Providing weitere Vorteile: Die Softwarehersteller sparen zum einen Kosten für die Herstellung und den Vertrieb von CD-ROMs und Handbüchern ein, zum anderen lassen sie die administrativen Aufgaben für die Vermietung von den ASPs erledigen. Für die Nutzer verringert sich die Schwelle, ein Programm zu wechseln, da bei einem Wechsel kein Kaufpreis mehr zu entrichten ist, sondern die Miete lediglich an ein anderes Unternehmen bzw. für ein anderes Produkt entrichtet wird. Darüber hinaus entfallen die oftmals komplizierten Installationen und der Zwang zu Software-Updates. Schließlich hat die Vermietung von Software an registrierte Kunden den positiven Nebeneffekt, dass keine Raubkopien mehr hergestellt werden können, wenn sich entscheidende Programm-Module auf dem Server des Providers befinden.

Erwartungsgemäß ist auch das Konzept des ASP angreifbar: Denkbar ist die Bereitstellung von Applikationen auf Piratenservern oder die Möglichkeit, sich ohne die entsprechenden Zugangsrechte mit einem Terminal-Server zu verbinden und diesen widerrechtlich zu nutzen – beispielsweise durch illegal generierte Login-Daten oder durch die Mehrfachnutzung von legalen Accounts. Dennoch sind die Missbrauchsmöglichkeiten vergleichsweise gering, zumal man das Authentifizierungsverfahren mit starker Kryptographie und weiteren Maßnahmen – wie die Überprüfung der IP-Adresse des Anwenders über eine sogenannte Hostmask-Erkennung – sehr sicher machen kann.

Ob sich die Softwaremiete per Internet letztlich in Deutschland durchsetzen wird, liegt maßgeblich daran, wie sich die rechtlichen Rahmenbedingungen entwickeln: Das Rechtsverhältnis zwischen Vermieter und Mieter einer Software bestimmt sich hierzulande nach den §§ 535 ff. BGB, so dass der Vermieter fortwährend für Mängel an der Mietsache haftet. Sind Mängel vorhanden, bzw. treten sie erst nach Jahren in Erscheinung, so muss er diese kostenlos beseitigen. Da auf die Gebrauchsfähigkeit der Software abgestellt wird, gilt dies auch für eine später eintretende Gebrauchsunfähigkeit – etwa durch Änderung der Steuergesetze bei einer Buchhaltungssoftware. Liegen Fehler bereits bei der Überlassung vor, was bei Software nicht untypisch ist, kann der Mieter gemäß § 536a BGB (§ 538 BGB a.F.) von Anfang an Schadensersatz verlangen.[566] Vor dem Hintergrund, dass es eine fehlerfreie Software selten oder nie gibt, sind dies doch beachtliche Unwägbarkeiten für Unternehmen, die Software vermieten wollen. Daher wird sich Application Service Providing in Deutschland wohl erst dann etablieren können, wenn sich die Softwarehersteller per Sondervereinbarungen (AGB) in eine günstigere rechtliche Situation bringen können als jene, die das Mietrecht derzeit vorgibt.

e) Softwaredesign

Zu den erfolgreichsten Maßnahmen der Softwarehersteller gehört eine vorausschauende Software-Entwicklung. Dies gilt vor allem für Unternehmen, die aufgrund ihrer Marktposition in der Lage

---

565 Zu erwähnen ist vor allem das Unternehmen *Microsoft*, das im Rahmen der sogenannten *NET-Initiative* (http://www.asp.net) bereits einen Teil seiner Produkte an ASPs lizenziert. Neben dem klassischen Modell, bei dem ein monatlicher Mietzins entrichtet wird, soll mit der Initiative auch ein sogenanntes Pay-per-Use-System etabliert werden, bei dem die Nutzung stundenweise abgerechnet werden kann.

566 *M. M. König*, Schuss nach hinten, **c't** 16/1999, S. 163.

sind, Standards zu etablieren. So enthalten die beiden derzeit wichtigsten Internet-Programme, der *Microsoft Internet-Explorer* und *Netscape*, zwar einen Newsreader jedoch keinen IRC-Client. Auf diese Weise ist gewährleistet, dass der schwer zu kontrollierende IRC keinen weiteren Zulauf erhält. Wie wirkungsvoll diese Maßnahme ist, sieht man daran, dass der IRC trotz des anhaltenden Internet-Booms im Verhältnis zum WWW deutlich weniger Zulauf erfahren hat. Überdies sind die enthaltenen Newsreader in ihrer Funktionsfähigkeit dergestalt eingeschränkt, dass sich Dateien aus den Binary-Newsgroups nur sehr umständlich herunterladen lassen.

Beide Browser sind auch nur bedingt geeignet, um große Dateien aus dem WWW herunterzuladen, da sie die Funktion „Download Resume" nicht unterstützen. Darunter ist die Möglichkeit zu verstehen, einen unterbrochenen Downloadvorgang an der Stelle wieder aufzunehmen, wo er „abgerissen" ist, anstatt den gesamten Download von vorne beginnen zu müssen. Vor allem bei großen Dateien, die über eine langsame Verbindung heruntergeladen werden, kommt es häufig vor, dass ein Download wegen Überlastung des Datennetzes stehen bleibt und schließlich vom Browser beendet wird. Um den Download dennoch in mehreren Etappen durchführen zu können, gibt es zwar sogenannte Downloadmanager, diese gehören jedoch nicht zum Lieferumfang der Browser oder der großen Betriebssysteme.

3. Maßnahmen der *Internet Engineering Task Force (IETF)*[567]

Die *Internet Engineering Task Force* ist eine große internationale Gemeinschaft von Netzwerkdesignern, Netzwerkbetreibern, Forschern und Unternehmen, die sich mit der Weiterentwicklung der Internetarchitektur beschäftigt und das reibungslose Funktionieren des Internet gewährleisten will. Der Zugang zur *IETF* steht jedem Interessierten offen. Die technische Arbeit der *IETF* findet in Arbeitsgruppen statt, die nach verschiedenen Themen aufgegliedert sind (z.B. Routing, Transport, Security etc.). Ein großer Teil der Aufgaben wird über Mailing-Listen abgewickelt, und dreimal jährlich werden große Zusammenkünfte der Mitglieder organisiert.

Die *IETF* entwickelt keine gezielten Maßnahmen gegen Online-Kriminalität, sondern arbeitet an der Schaffung technischer Standards, von denen jedoch einige geeignet sind, Online-Kriminalität merklich zu erschweren. Von besonderer Bedeutung ist in diesem Zusammenhang die Tätigkeit der Arbeitsgruppe *Authentication, Authorization and Accounting*, die – in erster Line für den E-Commerce – eine Möglichkeit schaffen will, Internetnutzer sicher zu identifizieren, um finanzielle Transaktionen gefahrlos vornehmen zu können (Authentifizierung).[568] Die Authentifizierung, die als Nebeneffekt die Aufhebung der weitgehenden Anonymität der Internetnutzer zur Folge haben könnte, soll durch die Einführung eines neuen TCP/IP (Internet Protocol Version 6 – IPv6) erreicht werden.[569] Der eigentliche Grund für die Umstellung des jetzigen IPv4 auf IPv6 liegt allerdings in der Erschöpfung des Adressraumes von IPv4: Als das IPv4 in den 80er Jahren entwickelt wurde, war das Ausmaß der heutigen Internetnutzung nicht absehbar. Obwohl die 32 Bit langen IPv4-Adressen theoretisch über 4 Milliarden Hosts und über 16 Milliarden Netzwerke adressieren können, kann dies durch die

---

[567] http://www.ietf.org.
[568] http://www.ietf.org/html.charters/aaa-charter.html.
[569] Technische Informationen zum Nachfolgeprotokoll von IPv4 finden sich bei *Leitner*, **c't** 16/2001, S. 202 ff.; siehe auch http://playground.sun.com/pub/ipng/html/ipng-main.html.

ursprünglich starre Einteilung in Class-A-, Class-B- und Class-C-Adressen praktisch bei weitem nicht erreicht werden: Durch die Reservierungen einzelner Werte für verschiedene Unternehmen, Organisationen und zu wissenschaftlichen Zwecken können nicht die vollen mathematischen Möglichkeiten des 32-Bit-Wertes genutzt werden.[570] Die *Address Lifetime Expectation Working Group (ALE WG)* der *IETF* hat bereits im Juli 1994 prognostiziert, dass der gesamte IPv4-Adreßraum zwischen 2005 und 2011 erschöpft sein wird. Die Gründe für die steigende Nachfrage nach IP-Adressen liegen unter anderem im anhaltenden Internet-Boom (vor allem im asiatischen Bereich). Sofern sich die Visionen zahlreicher Technologie-Entwickler bestätigen sollten, wonach in naher Zukunft beinahe jedes technische Gerät (z.B. Kraftfahrzeuge oder Haushaltsgeräte) eine eigene IP-Adresse besitzen soll, ist ebenfalls mit einem enormen Bedarf an neuen IP-Adressen zu rechnen.[571] Um diesem Dilemma zu begegnen und andere zukunfts-weisende Eigenschaften in das Protokoll einzubinden, hat die *IETF* Ende 1990 beschlossen, ein Nachfolgeprotokoll für IPv4 zu suchen. In der Folgezeit wurden mehrere verschiedene Versionen des IP-Next-Generation (IPnG) entwickelt. Auf dem *IETF*-Meeting im Juli 1994 in Toronto fiel die Entscheidung zugunsten einer revidierten Version des sogenannten Simple Internet Protocol Plus (SIPP), dessen neuer Name IPv6 wurde.[572]

Neben der Vergrößerung des Adressraumes von 32 auf 128 Bit gibt es weitere Änderungen, durch die sich IPv6 von IPv4 unterscheiden wird[573]:

Über eine Vereinfachung des Header-Formats (optionale Verkleinerung) wird die Verarbeitungsgeschwindigkeit eines IPv6 Paketes optimiert und sein Bandbreitenbedarf minimiert. Durch die Möglichkeit des sogenannten Flow-Labelling können Datenströme mit einer Markierung versehen werden. Damit kann der Absender eine spezielle Behandlung seiner Pakete durch die Router auf dem Weg zum Ziel fordern (Quality of Service – QoS).

Eine weitere wichtige Neuerung ist die bereits erwähnte Unterstützung von Authentifizierung und Verschlüsselung. Werden diese Optionen entsprechend umgesetzt, soll es möglich sein, Urheber rechtswidriger Inhalte aufzufinden, sofern dies rechtlich geboten ist.[574] In der Diskussion befindlich ist unter anderem der Vorschlag, die MAC-Adresse[575] der Ethernet-Karte des Anwenders in den „Briefumschlag" der Datenpakete einzubauen.[576] Allerdings ist dieser Vorschlag bei der Netzgemeinde auf derart heftige Kritik gestoßen, dass die *IETF* Ende Februar 2001 mit dem RFC 3041 einen neuen Standard vorgestellt hat, der den Surfern helfen soll, Datenspuren zu verwischen.[577] Dabei sollen zufällig ausgewählte IP-Nummern anstelle fester Kennungen gewählt werden können, um die Privatsphäre der Nutzer zu stärken und hauptsächlich privatwirtschaftlichen Datensammlern das Leben schwerer zu machen. "Bei jedem Hochfahren eines Rechners oder sogar noch öfter werden die Nummern neu durchgemischt", erläutert das Verfahren *Hans Peter Dittler*, der als stell-

---

[570] *Sietmann*, Nummernspiele, **c't** 9/1999, S. 186.
[571] *Ermert*, IPv6 auf allen Kanälen, **c't** 1/2000, S. 32.
[572] In den Requests For Comments (RFCs) 1752 und 1883 wurden die Spezifikationen des IPv6 festgelegt. Bei den RFCs handelt es sich um eine Reihe von Anmerkungen zum Internet, die seit 1969 (damals für das *ARPA*-Net) gesammelt werden. Inzwischen gibt es über 3000 RFCs. Neben Vorschlägen zur Verbesserung oder Standardisierung der Internet-Technologie werden auch von der *IETF* (und anderen) beschlossene Spezifikationen als RFC veröffentlicht – vgl. http://www.rfc-editor.org/overview.html.
[573] Siehe http://www.ipv6.org m.w.N.
[574] *Sieber*, Missbrauch der Informationstechnik, Teil 3, III. 3.
[575] Siehe Fn. 554.
[576] *Krempl*, Generalüberholung für das Internet, **c't** 20/1999, S. 214.
[577] http://www.ietf.org/rfc/rfc3041.txt.

vertretender Vorsitzender der deutschen Abteilung der *Internet Society* die Entwicklung des neuen Protokolls begleitet. Vor allem Surfern, die von zu Hause aus ins Netz gehen, würde damit ein Stück Anonymität zurückgegeben.[578]

Es bleibt abzuwarten, ob der neue Standard zur Adressgeheimhaltung allgemeine Akzeptanz findet, denn vor allem die Verbrechensbekämpfung im Internet könnte extrem erschwert werden. Der Erfolg von RFC 3041 hängt maßgeblich von der allgemeinen Verfügbarkeit von IPv6 ab, die bislang nicht abzusehen ist. Um die Kompatibilität des IPv6 mit der großen Menge von bereits installierten IPv4-Hosts und –Routern zu gewährleisten, entwickelte die *IETF* die folgende Migrationsstrategie: Grundprinzip soll ein sogenannter Dual-Stack sein, bei dem IPv4-Hosts und –Router zusätzlich um einen IPv6-Stack ergänzt werden. Somit wird die vollständige Kompatibilität zu noch nicht aufgerüsteten Systemen gesichert. Durch sogenanntes Tunneling sollen IPv6-Pakete auch über reine IPv4-Topologien versendet werden können. Das „Abschalten" von IPv4 ist folglich erst in vielen Jahren oder gegebenenfalls gar nicht zu erwarten. Allerdings ist damit zu rechnen, dass von einem bestimmten Zeitpunkt an nur noch IPv6-Adressen neu vergeben werden.

Zusammenfassend lässt sich festhalten, dass mit der Einführung bzw. Weiterentwicklung des neuen Internet-Protokolls effektive Maßnahmen im Kampf gegen Online-Kriminalität ergriffen werden könnten[579], zumal sie auf der Ebene der technologieorientierten Kriminalitätsvorbeugung ansetzen. Dennoch ermöglicht die äußerst lange und unumgängliche Migrationsphase weiterhin Schlupflöcher für Online-Kriminelle, weshalb die Strafverfolger an den bisherigen Verfolgungsmethoden festhalten müssen.

Exkurs – „Recht auf Anonymität"?

Es handelt sich nicht nur um technische Hindernisse, die der Einführung von IPv6 im Weg stehen. Immer dann, wenn Maßnahmen bekannt werden, die die Anonymität der Internet-nutzer aufheben sollen, formiert sich ein breiter Widerstand innerhalb der Netzgemeinde. Kern der zahlreichen Diskussionen ist die Frage, ob Anonymität besonderen rechtlichen Schutz verdient.

Zweifellos bietet eine anonyme Nutzung des Internet zahlreiche Vorteile: Ähnlich wie bei den *Anonymen Alkoholikern* oder bei der Telefonseelsorge tauschen sich Opfer in zahlreichen Online-Diskussionsforen aus, ohne ihre Identität offenlegen zu müssen.[580] Gerade im Bereich von gesundheitlichen Problemen und Krankheiten kommt dem Internet als Kommunikationsmedium eine große Bedeutung zu. Durch die Möglichkeit anonymer Beteiligung an diesen Foren können sich Patienten erstmalig ohne Schamgefühl oder Angst über ihre Leiden informieren und austauschen.

Selbst wenn keine therapeutische Hilfe benötigt wird, kann ein Gedankenaustausch unter dem Schleier der Anonymität ein harmloser Zeitvertreib oder die Gelegenheit sein, unausgereifte Gedankensplitter erst einmal zu testen, bevor man den eigenen Ruf damit in der realen Welt aufs

---

[578] **Heise Online News** vom 28.02.2001, http://www.heise.de/newsticker/meldung/15655.
[579] Vgl. auch *Vassilaki*, Multimediale Kriminalität, **CR** 1997, S. 301 und *Sieber*, Missbrauch der Informationstechnik, Teil 3, III. 3., der von „technischen Sicherheitsstandards mit Zugriffskontrollsystemen" spricht.
[580] *Mayer*, **NJW** 1996, S. 1786.

Spiel setzt[581]. Menschen, die in einem intoleranten sozialen Umfeld leben, können ihre moralischen oder religiösen Anschauungen äußern und diskutieren, ohne mit persönlichen Konsequenzen rechnen zu müssen. Mancher freut sich gar daran, einmal nicht politisch korrekt sein zu müssen.

Schließlich ist anonyme Internetnutzung auch für die Forschung bedeutsam; beispielhaft zu erwähnen sind anonyme Self-report-Erhebungen in der kriminologischen Forschung.

Die genannten Beispiele geben nur einen Bruchteil der Fälle wieder, in denen ein gesetzestreuer Bürger von der Anonymität des Internet profitiert. Oftmals wird kritisiert, dass die ganze Bevölkerung ihre Privatsphäre verlieren soll, nur weil ein „paar Promille der Bevölkerung es nicht lassen können, solchen Schmutz zu konsumieren"[582]. Ebenso werden Vergleiche mit der realen Welt angestellt: Niemand verlange ernsthaft, dass künftig alle Briefsendungen und Päckchen geöffnet werden, um ihren Inhalt zu überprüfen. Auch auf politischer und rechtlicher Ebene erhält das „Prinzip Anonymität" Rückendeckung: In Deutschland soll das Grundrecht auf informationelle Selbstbestimmung[583] den „gläsernen Bürger" verhindern. So ist in § 4 Abs. 6 TDDSG festgeschrieben, dass der Diensteanbieter dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen hat, soweit dies technisch möglich und zumutbar ist. *Joachim Jacob,* der frühere Bundesbeauftragte für den Datenschutz, äußerte im Hinblick auf die Entwicklungen im europäischen Datenschutzrecht, dass das Grundprinzip der anonymen Internetnutzung nicht verändert werden darf[584].

Sofern sich in der Zukunft eine Möglichkeit ergeben sollte, die Anonymität der Internetnutzer aufzuheben, darf diese auf keinen Fall jedermann zur Verfügung stehen. Denn von einer Person, die das Internet intensiv nutzt, lässt sich ein umfassendes Persönlichkeitsprofil erstellen, sofern man ihre Wege durch das Netz verfolgt. In den falschen Händen können derartige Informationen zu einer existentiellen Bedrohung für die Privat- und Intimsphäre des Betroffenen werden. Daher sollte die Aufdeckung der Identität eines Internetnutzers nur staatlichen Stellen möglich sein, rechtsstaatlich abgesichert sein und nur dann erfolgen, wenn die beobachtete Rechtsverletzung eine gewisse Schwere erreicht.

4. Maßnahmen von Hardwareherstellern

a) Internettaugliche Hardware nach der PC-Ära

Einige Experten gehen davon aus, dass in spätestens zehn oder fünfzehn Jahren in den meisten Haushalten eine Art Hybridmedium aus TV, PC, Telefon und vielleicht noch anderen Elementen

---

581 *Engel*, **AfP** 1996, S. 223.
582 Vgl. *Engel*, **AfP** 1996, S. 224.
583 Mit dem sogenannten Volkszählungsurteil vom 15.12.1983 (Az. 1 BvR 209/83), **BVerfGE** 65, S. 1 ff., hat das *BVerfG* das Recht auf informationelle Selbstbestimmung als neuen Aspekt des allgemeinen Persönlichkeitsrechts hervorgehoben. Das Grundrecht ist Ausfluss der Menschenwürde (Art. 1 Abs. 1 GG) sowie der allgemeinen Handlungsfreiheit (Art. 2 Abs. 1 GG) und soll gewährleisten, dass jeder Bürger grundsätzlich selbst darüber entscheiden kann, ob er personenbezogene Daten preisgibt.
584 Vgl. das Interview bei *Schulzki-Haddouti*, Das Prinzip Anonymität, **c't** 9/1999, S. 46.

stehen wird.[585] Der klassische PC, wie wir ihn heute kennen, soll früher oder später von Geräten abgelöst werden, die leichter zu bedienen und eventuell portabel sind (sogenannte Wearables). Schon heute sind Geräte im Handel, mit denen man im WWW surfen kann, indem man sie einfach an das heimische Fernsehgerät und an die Telefonleitung bzw. das Kabelnetz anschließt. Diese sogenannten Set-Top-Boxen avancieren zunehmend zur Multimedia-Station im eigenen Heim und bieten neben dem WWW-Zugang weitere Funktionen wie E-Mail, Adressbuch, Terminplaner, Anrufbeantworter, Faxgerät etc.. Das Angebot an WWW-Seiten, die mit den Set-Top-Boxen angesehen werden können, wird in der Regel von einer Redaktion ausgewählt. Auf diese Weise ist gewährleistet, dass kaum Webseiten mit rechtswidrigen Inhalten zu den Nutzern der Boxen vordringen können. Auch durch den Umstand, dass die schwer zu kontrollierenden Bereiche des Internet (UseNet, IRC, FTP) nicht für die Besitzer von Set-Top-Boxen zugänglich sind, beschränken sich die Möglichkeiten illegaler Internetnutzung auf ein Minimum. Obwohl in der Regel technische Gründe oder ergonomische Erwägungen dafür verantwortlich sind, dass kritische Bereiche des Internet ausgeklammert werden und dass eine redaktionelle Selektion des WWW-Angebotes erfolgt, ist dies ein möglicher Weg, um künftig Verstöße gegen die Vorschriften des UrhG zu verhindern.

Im Hinblick darauf, dass die neuen Hybridmedien in naher Zukunft der breiten Masse einen Zugang zum Internet verschaffen könnten, ist es besonders wichtig, bei der (Weiter-)Entwicklung dieser Technologien anzusetzen. Hier liegt ein großes proaktives Präventionspotential, das dazu beitragen kann, illegale Internetnutzung zu verringern.

b) Implementierung individueller Hardwarekennungen

In weiten Teilen der PC-Gemeinde hat die Markteinführung des *Intel Pentium III* Anfang 1999 für Unruhe gesorgt, da der Prozessor erstmals eine per Software auslesbare Seriennummer (Processor Serial Number – PSN) enthielt.[586] Anhand der 96 Bit langen Nummer ist es möglich, jeden einzelnen Prozessor individuell zu identifizieren und – über entsprechende Datenbanken – auch dessen Besitzer.[587] Mit der Implementierung der PSN versprach *Intel* den Kunden mehr Sicherheit beim E-Commerce und beim Informationsaustausch über das Internet. Ein weiterer Grund für die Implementierung der PSN lag vermutlich darin, dass *Intel* seit längerer Zeit massive Probleme mit gestohlenen, illegal geklonten und übertakteten Prozessoren hatte, die unter ihrem Warenzeichen auf dem grauen Markt verkauft wurden.

Nach der Markteinführung schlugen weltweit Daten- und Verbraucherschützer Alarm, weil sie befürchteten, dass die *Pentium III* PSN den Nebeneffekt haben könnte, die Anonymität jener Internetnutzer aufzuheben, die mit einem *Pentium III* online gehen. Angesichts eines Marktanteils von 85%, den *Intel* damals im Bereich der Mikroprozessoren hatte, befürchteten sie die Entstehung des „gläsernen Surfers". *Barry Steinhardt* von der *American Civil Liberties Union* sah in der PSN eine unerwünschte Möglichkeit, Einzelpersonen in Datennetzen zu verfolgen[588], andere Kritiker (z.B.

---

[585] Vgl. das Interview mit *Bonfadelli*, **FOCUS** 7/1999, S. 196 f. sowie die Prognose der *Gesellschaft für Unterhaltungs- und Kommunikationselektronik* (*GFU* – http://www.gfu.de) in den **Heise Online News** vom 27.12.1999, http://www.heise.de/newsticker/meldung/7388.

[586] Die individuelle Seriennummer wurde bereits bei der Herstellung elektronisch in den Chip implementiert (als sogenanntes PROM).

[587] *W. Schulz*, US-Datenschützer: „Big-Brother inside", **VDI nachrichten** vom 05.02.1999, S. 15.

[588] Vgl. *W. Schulz*, US-Datenschützer: „Big-Brother inside", **VDI nachrichten** vom 05.02.1999, S. 15.

vom *Electronic Privacy Information Center – EPIC*[589]) gaben zu bedenken, dass Unternehmen und Online-Anbieter versuchen würden, einen Großteil ihrer Kunden anhand der Kennzahlen ihrer Rechner zu beobachten und zu profilieren. Aufgrund der zahlreichen Proteste gab *Intel* ein kleines Programm heraus und versicherte, dass der Anwender damit einstellen könne, ob er das Auslesen der Seriennummer erlauben wolle. Diese Darstellung hatte sich jedoch als falsch erwiesen. Einem Prozessorexperten der deutschen Computerfachzeitschrift *c't* war es gelungen, eine Software zu schreiben, die den Auslesebefehl trotz manueller Deaktivierung erfolgreich geben konnte[590]. Ein solches Programm könnte man beispielsweise als *ActiveX*-Applet auf jeder erdenklichen Webseite platzieren, wo es die PSNs sämtlicher Besucher mit einem *Pentium III*-Prozessor in einem vollständig auslesbaren Cookie[591] platziert[592]. Auf diese Weise kann jeder Anwender individuell identifiziert werden, ohne dass er es ausdrücklich zugelassen hat bzw. überhaupt bemerkt. Die Sicherheitslücke beruht auf Besonderheiten der Systemarchitektur des Prozessors, die seit einiger Zeit dokumentiert waren. Kurz darauf bestätigte *Intel* die Erkenntnisse als richtig.[593]

Eine verlässlichere Möglichkeit, das unerwünschte Auslesen der PSN zu verhindern, besteht darin, die Abschaltmöglichkeit konfigurierbar in das BIOS[594] des Rechners zu integrieren. Nur so ist ein softwareseitiges Einschalten zu verhindern.[595] Beinahe alle PC-Hersteller hatten schnell reagiert und boten mit neueren BIOS-Revisionen ihrer Hauptplatinen eine entsprechende Abschaltfunktion an. Fraglich ist allerdings, wie viele Internetnutzer überhaupt von der PSN wissen und wenn ja, ob sie in der Lage sind, diese auszuschalten. Denn der durchschnittliche Computernutzer ändert nur selten die vorgegebenen BIOS-Einstellungen. Vorausgesetzt, dass eine individuelle Hardwarekennung aktiviert und auslesbar ist, lässt sie sich tatsächlich für die Kriminalitätsbekämpfung nutzbar machen. Immer dann, wenn eine Kennung in Verbindung mit einer Rechtsverletzung auftaucht, bestünde die Möglichkeit, den Täter über entsprechende Datenbanken zu identifizieren. Der Zugang zu diesen Datenbanken, mit Hilfe derer eine Zuordnung von Kennung und Hardwarekäufer bzw. –besitzer möglich ist, müsste den Strafverfolgungsbehörden offen stehen. Fraglich ist jedoch die rechtliche Zulässigkeit der Erstellung und Unterhaltung entsprechender Datenbanken, zumal diese unter Mithilfe von privaten Hardwareverkäufern erfolgen müsste. Auch ist zu beachten, dass Computerfreaks früher oder später einen Weg finden werden, Hardwarekennungen zu fälschen[596], weshalb die identifizierte Zielperson nicht unbedingt identisch mit dem Täter sein muss.

In datenschutzrechtlicher Hinsicht und im Hinblick auf die Anonymitätsdiskussion begegnen Hardwarekennungen denselben Bedenken wie IPv6. Der Chip-Hersteller *Intel* zog bereits die

---

589 http://www.epic.org.
590 Hierbei handelte es sich um einen sogenannten Ring-3-Befehl, vgl. *Gwennap*, Editorial **Microprocessor Report** vom 15.02.1999.
591 Cookies sind kleine Text-Dateien, die automatisch von Webseiten auf dem Rechner des Surfers angelegt werden. Normalerweise werden sie dazu benutzt, wiederkehrende Besucher auf Webseiten zu identifizieren. Sie enthalten in der Regel keine persönlichen Daten, sondern es wird von den Webseiten eine zufällige Nummer vergeben, die es ermöglicht, einen erneuten Besuch des Surfers festzustellen. Weiterführende Informationen zu Cookies finden sich bei *Köhntopp/ Köhntopp*, **CR** 2000, S. 252.
592 Vgl. **Wired News** vom 11.03.1999, http://www.wired.com/news/technology/0,1282,18395,00.html.
593 *Persson*, **c't** 5/1999, S. 16.
594 Siehe Fn. 152.
595 *Persson*, **c't** 5/1999, S. 16.
596 Für die PSN des *Pentium III*: *Gwennap*, Editorial **Microprocessor Report** vom 15.02.1999.

Konsequenzen aus den weltweiten Protesten nach der Einführung der Seriennummer beim *Pentium III:* Der im Herbst 2000 eingeführte *Pentium 4* enthält nach Angaben von *Intel* keine integrierte Seriennummer mehr.

5. Maßnahmen der Strafverfolgungsbehörden

Die Strafverfolgungsbehörden spielen im Kampf gegen Internet-Softwarepiraterie eine eher untergeordnete Rolle. Sie schreiten in der Regel erst bei Fällen unerlaubter gewerbsmäßiger Verwertung urheberrechtlich geschützter Werke gemäß § 108a UrhG ein oder wenn die Anti-Piraterie-Organisationen der Softwarehersteller Hinweise auf hinreichend tatverdächtige Personen gegeben haben.

Gegen den „privaten Endnutzer" von Raubkopien gehen die Strafverfolgungsbehörden im Regelfall nicht vor. Insofern besteht eine Diskrepanz zwischen Gesetzeslage und Verfolgungspraxis, auf die im weiteren Verlauf der Arbeit noch eingegangen werden soll.[597]

a) Anlassabhängige Ermittlungen

Hinweise Dritter auf Softwarepiraten sind der häufigste Grund für das Einschreiten der Polizeibehörden. Die meisten Hinweise erhalten die Behörden von Anwälten betroffener Softwarehersteller, die auf verdächtige Web-Angebote oder Zeitungsannoncen antworten und sich die auffallend günstige Software schicken lassen. Sofern es sich dabei nicht um Originale handelt, wird der Sache nachgegangen. Oft geben Beamte anderer Einsatzbereiche Hinweise an die entsprechenden Dezernate, wenn sie zufällig fündig wurden – beispielsweise in der Wohnung eines Ladendiebs, in der sich neben der Kaufhausbeute selbstgebrannte Raubkopien fanden oder bei einem Drogenhändler, der zufällig Mitglied in einem Softwarepiratenring war. Auch Neid unter Jugendlichen führt in zahlreichen Fällen zum „Verpfeifen" von Mitschülern bei der Polizei.[598]

Weit weniger Hinweise als zu Profit-Pirates gibt es zu den Mitgliedern von Warez-Gruppen. Das mag vor allem daran liegen, dass diese überwiegend ohne Bereicherungsabsicht arbeiten, weshalb sie den Underground nicht verlassen müssen. Denn wann immer ein Raubkopierer Geld für seine Ware erhalten will, muss er eine Verbindung zur realen Welt schaffen, die ihn leicht der Entdeckung preisgeben kann – z.B. anhand des Wegs des Geldflusses bei Bezahlung per Kreditkarte[599]. Aus diesem Grund gab es in Deutschland bislang kaum durchschlagende Erfolge im Kampf gegen Warez-Gruppen. Lediglich die Enttarnung und Auflösung einer Gruppe namens *Section 8*, die allerdings nicht im Internet aktiv war, gelang der Kriminalpolizei in den 80er Jahren.[600] Die Gruppe beschränkte sich nicht auf das Verbreiten von gecrackter Software, ihr wurde ebenfalls das Streben nach finanziellem Gewinn zum „Verhängnis".

Weitaus größeren Erfolg beim Vordringen zu den Gruppenstrukturen hatten US-amerikanische Behörden 1996 in der groß angelegten Aktion „Cyberstrike", in der beinahe die gesamte

---

[597] Siehe unten Teil 2, C. V. 2.
[598] Vgl. **GameStar** 12/1998, S. 76.
[599] Vgl. *McCandless*, **Wired Magazine** 5.04 – April 1997.
[600] *Schultz*, S. 124.

nordamerikanische Warez-Szene zeitweise ausgelöscht wurde.[601] „Cyberstrike“ richtete sich jedoch nur begrenzt gegen Ziele im Internet, in erster Linie wurde gegen Personen vorgegangen, die in diversen Mailbox-Netzen aktiv waren.

Der erste größere Schlag gegen eine im Internet operierende Warez-Gruppe gelang den US-Strafverfolgungsbehörden im Sommer 1999.[602] Im Rahmen der Operation „I.P. Initiative“, einer gemeinsamen Aktion von *FBI*, den US-Zollbehörden und dem US-Justizministerium, kam es zu einer Hausdurchsuchung bei einem mutmaßlichen Mitglied der auf Computerspiele spezialisierten Gruppe *PARADIGM*, bei welcher ein Rechner, Festplatten, CD-ROMs und andere wichtige Beweismittel beschlagnahmt wurden. Das beschlagnahmte Material lieferte Hinweise auf weitere Mitglieder von *PARADIGM,* unter anderem in den USA, Kanada, England, Deutschland, Holland, Dänemark, Norwegen, Portugal, Schweden und Russland. Zur Einleitung strafrechtlicher und zivilrechtlicher Maßnahmen übergaben die US-Behörden die Beweismittel an die Strafverfolgungsbehörden in den entsprechenden Ländern. Die Verantwortlichen der „I.P. Initiative“ waren zunächst zuversichtlich, dass sich während der weiteren Ermittlungen aufgrund dieses „Busts” Spuren auftun würden, die zur Zerschlagung anderer Warez-Gruppen führen würden, was sich jedoch bislang als unbestätigte Hoffnung erwies. Offenbar war die Polzeiaktion nicht einmal das wirkliche Ende für *PARADIGM*, denn wie sich aus zahlreichen NFO-Dateien entnehmen ließ, formierten sich die verbliebenen Mitglieder rasch unter einem neuem Gruppennnamen, um mit ihrem verbotenen Tun fortzufahren.

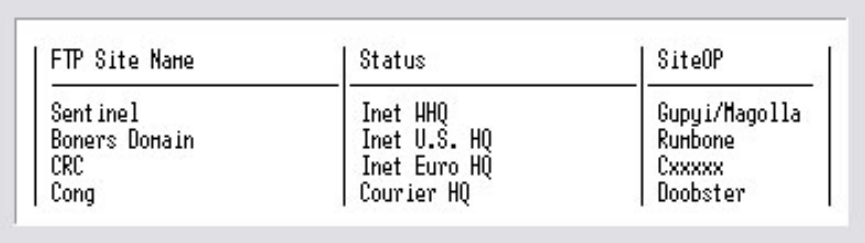
Darüber, wie es zur Enttarnung des Gruppenmitglieds kam, geben die offiziellen Presseerklärungen keinen Aufschluss. Unbestätigten Informationen aus einem Szene-Forum[603] zufolge kamen die entscheidenden Hinweise von dem Spielesoftwarehersteller *Electronic Arts* (*EA*), der als größter Konzern der Branche in besonderem Maße von Piraterie betroffen ist. Bei Nachforschungen, wie es möglich sei, dass Spiele von *EA* bereits vor dem offiziellen Erscheinungsdatum in der Warez-Szene verbreitet wurden, fiel der Verdacht auf einen Mitarbeiter in einer Test-Abteilung von *EA*, dem vorgeworfen wurde, als Supplier für *PARADIGM* fungiert zu haben und zudem vertrauliche Informationen über die Sicherheitsvorkehrungen bei *EA* an die Szene weitergegeben zu haben. Es erfolgte eine Überwachung der gesamten Kommunikation der verdächtigen Person durch das *FBI*, wodurch man schließlich auf den Kontaktmann von *PARADIGM* stieß. In dessen Wohnung soll schließlich die oben erwähnte Durchsuchung stattgefunden haben. Andere Gerüchte deuten darauf hin, dass ein “Szene-Maulwurf” für die Busts verantwortlich ist. Es soll sich hierbei um eine Person handeln, die selbst einmal der Softwarepiraterie überführt wurde und nun für einige Softwarehersteller arbeitet, um zivilrechtlichen Schadensersatzansprüchen zu entgehen.

In den Monaten Januar und Februar 2000 gelang dem *FBI* ein weiterer Schlag gegen die organisierte Softwarepiraterie. Durch den Hinweis eines Informanten aus Chicago erlangten die Beamten Zugang zu einem FTP-Server, der sich an der Universität von Sherbrooke in der kanadischen Provinz Quebec befand. Bei der Durchsicht der Verzeichnisse des als „Sentinel“ bezeichneten Servers entdeckten die Ermittler über 5.000 raubkopierte Computerprogramme im Wert von etwa 1,2

---

601 **Computerwoche** 8/1997, S. 25.
602 Vgl. die *EA*-Pressemeldung vom 06.08.1999, http://retailsupport.ea.com/corporate/pressreleases/piracy.html.
603 Siehe hierzu Teil 1, F.

Millionen US-Dollar[604] sowie zahlreiche MP3-Dateien. Genutzt wurde die FTP-Seite hauptsächlich von den Mitgliedern der weltweit operierenden Warez-Gruppe *Pirates With Attitudes (PWA)*.



FTP Site Name	Status	SiteOP
Sentinel	Inet HHQ	Gupyi/Magolla
Boners Domain	Inet U.S. HQ	Runbone
CRC	Inet Euro HQ	Cxxxxx
Cong	Courier HQ	Doobster

Abbildung 84 – Auszug aus einer NFO-Datei von *PWA*

PWA galt als eine der am längsten aktiven und straffsten organisierten Gruppen. Bereits Jahre vor dem großen Internet-Boom hatten die *PWA*-Mitglieder über private Bulletin Board Systems Raubkopien verbreitet und ausgetauscht. Den kanadischen Server, zu dem rund 100 Personen Zugang hatten, stellten zwei Universitätsangehörige der Gruppe seit 1995 zur Verfügung. Die beiden Verdächtigen kooperierten bereits seit März 1999 mit dem *FBI*, wodurch die Ermittler zahlreiche belastende Logfiles sammeln konnten. Die Spuren führten zu 17 Tatverdächtigen, unter denen sich nach Angaben der Bundespolizei 12 *PWA*-Mitglieder befanden. Bei 5 Tatverdächtigen handelte es sich um Angestellte des Chip-Herstellers *Intel*, die Computerhardware bereitgestellt haben sollen, um im Gegenzug Zugang zu „Sentinel" zu erhalten. Ebenfalls enttarnt wurde ein ehemaliger Mitarbeiter von *Microsoft*. Dieser soll Raubkopien von Produkten seines damaligen Arbeigebers auf den FTP-Server hochgeladen haben, sowie einem der Köpfe von *PWA* namens „Marlenus" Zugang zum internen *Microsoft*-Unternehmensnetz verschafft haben. „Marlenus", der mit bürgerlichem Namen *Robin Rothberg* heißt und als Softwareentwickler bei *NEC* arbeitete, wurde ebenfalls vom *FBI* aufgespürt. Dem in Massachussetts lebenden Softwarepiraten war es über einen Zeitraum von acht Jahren gelungen, den Strafverfolgern zu entkommen. Ob die 17 Tatverdächtigen mit ihren Handlungen Geld verdient haben, ist unklar. Die ermittelnde Staatsanwältin lehnte es ab, hierzu nähere Auskünfte zu erteilen.

Den bislang größten Ermittlungserfolg innerhalb der Warez-Szene erzielten die US-Behörden Anfang Dezember 2001. In der Operation „Buccaneer" zerschlugen die Beamten in einer konzertierten Aktion von *FBI*, den US-Zollbehörden und dem US-Justizministerium eine Warez-Gruppe namens *DrinkOrDie*. Nach 15-monatigen Undercover-Ermittlungen kam es zur Durchsuchung von rund 100 Wohnungen, Unternehmen und Universitätsräumen in sechs Ländern und zur Beschlagnahme von über 130 Rechnern, auf denen sich schätzungsweise 50 Terabyte Raubkopien

---

[604] Nach Schätzungen des *FBI*, vgl. **Heise Online News** vom 05.05.2000, http://www.heise.de/newsticker/meldung/9377.

befanden[605]. Nach Informationen des US-Justizministeriums wurden dabei rund 40 Mitglieder der Gruppe identifiziert[606].

DrinkOrDie wurde 1993 in Russland gegründet und entwickelte sich Mitte der 90er Jahre zu einer der aktivsten und bekanntesten Warez-Gruppen. Ruhm über die Szene hinaus erlangte sie etwa durch die Veröffentlichung von *Windows 95* vor dem offiziellen Verkaufsstart sowie durch das Umgehen des *Sentinel*-Dongles[607]. Zu den Mitgliedern von *DrinkOrDie*, die in das Fadenkreuz der Ermittler gerieten, gehörten erwartungsgemäß fast ausnahmslos Computerspezialisten aus Unternehmen und Universitäten im Alter von 20 bis 35 Jahren. Diese hatten hunderte raubkopierter Programme und Filme auf den ihnen zugänglichen Systemen gespeichert und per Internet zur Verfügung gestellt. Illegale Dateien wurden zum Beispiel auf Rechnern der Universität von Los Angeles, des *Massachusetts Institute of Technology* und der *Bank of America* gefunden.[608]

Abbildung 85 – NFO-Datei von *DrinkOrDie*

Gegen zwei der Gruppenmitglieder wurden im Mai 2002 vor einem US-Gericht die bislang höchsten Strafen für organisierte Internet-Softwarepiraterie verhängt. *John Sankus*, zum Tatzeitpunkt 28 Jahre alt, wurde als Leader von *DrinkOrDie* zu einer Haftstrafe von 46 Monaten verurteilt, *Barry Erickson*, 35-jähriger System-Ingenieur beim Softwarehersteller *Symantec* und Supplier für *DrinkOrDie*, erhielt eine Freiheitsstrafe von 33 Monaten.[609] Die Täter bekannten sich allesamt schuldig, und nach Angaben der US-Zollbehörde kooperierten fast alle Verdächtigen mit den Behörden. Die meisten der verhörten Täter lieferten freiwillig weitere Details über andere Gruppenmitglieder.[610]

---

605 **CNET News** vom 19.12.2001, http://news.cnet.com/news/0-1005-200-8233279.html.
606 Pressemeldung der US-Regierung, http://www.usdoj.gov/criminal/cybercrime/warezoperations.htm.
607 *Röttgers*, Piraten hinter Gittern, **Telepolis** vom 28.02.2002.
608 **Heise Online News** vom 24.01.2002, http://www.heise.de/newsticker/meldung/24258.
609 Pressemeldung der US-Regierung, http://www.cybercrime.gov/sankusSent.htm.
610 **CNET News** vom 19.12.2001, http://news.cnet.com/news/0-1005-200-8233279.html.

Abbildung 86 – Szene-Informationen zum Status einzelner FTP-Server unmittelbar nach der Operation „Buccaneer“

Parallel zur Operation „Buccaneer“ führten die US-Behörden zwei weitere Aktionen gegen die Warez-Szene durch, die Operation „Bandwidth“ und die Operation „Digital Piratez“. Der Operation „Bandwidth“ ging eine zweijährige Undercover-Ermittlung voraus, die schließlich dazu führte, dass mehr als 30 Haftbefehle für die Vereinigten Staaten und Kanada erlassen wurden. Die Piraten gingen den Ermittlern aufgrund eines Servers ins Netz, der von den Behörden eigens zu diesem Zweck eingerichtet und überwacht wurde. Nach Angaben des *FBI* wurden mehr als 144.000 Programme über die Seite verschoben. Die Aktion richtete sich in erster Linie gegen Mitglieder der Gruppe *RogueWarriorz;* gegen die zahlreichen Warez-Trader, die den Server ebenfalls nutzten, wurden keine Haftbefehle erlassen. Die vom *FBI* in New Hampshire durchgeführte Operation „Digital Piratez“ zielte ebenfalls auf die Verhaftung von höherrangigen Mitgliedern der Warez-Szene ab und führte zu 12 Haftbefehlen in den Vereinigten Staaten.[611]

Die großen Aktionen der US-Behörden hatten tatsächlich einen Stillstand in der gesamten Warez-Szene bewirkt, allerdings haben sich die verbliebenen Gruppen nach mehrwöchigem Abwarten reorganisiert und wieder damit begonnen, Programme zu veröffentlichen. Dass die Aktionen keine längerfristigen Folgen hatten, mag auch damit zusammenhängen, dass *DrinkOrDie* entgegen der Einschätzung der Ermittler und Vertreter der Software- und Filmindustrie nicht (mehr) zu den wichtigen Gruppen in der Warez-Szene gehörte[612]. Tatsächlich war das Engagement von *DrinkOrDie* in den letzten Jahren stark zurückgegangen. Nach Angaben eines Szenekenners stammten von den von Mai bis Dezember 2001 veröffentlichten 40.865 Warez-Releases nur 411 von *DrinkOrDie.*[613]

---

611 **CNET News** vom 19.12.2001, http://news.cnet.com/news/0-1005-200-8233279.html.
612 So erklärte *Valenti* von der *Motion Picture Association of America (MPAA)* gegenüber der Presse, dass die Zahl der Websites, die illegal Hollywood-Filme zum Download anbieten, seit der Zerschlagung der Gruppe um 45% gesunken sei, siehe *Röttgers*, Piraten hinter Gittern, **Telepolis** vom 28.02.2002.
613 vgl. *Röttgers*, Piraten hinter Gittern, **Telepolis** vom 28.02.2002.

Nicht gegen Mitglieder von Warez-Gruppen, sondern gegen Warez-Trader richtete sich eine Aktion der US-Polizei im November 1999. 25 in den USA lebende Teilnehmer des IRC-Channels #warez4cable wurden von der *BSA* überführt.[614] Der Channel existierte im NewNet, welches mit ungefähr 4.000 Nutzern verhältnismäßig geringe Besucherzahlen verzeichnet. Die *BSA* hatte den Channel über mehrere Wochen beobachtet und von den F-Servern der Beteiligten Raubkopien heruntergeladen. Sämtliche Aktivitäten der Ermittler sowie die IP-Adressen der Channelteilnehmer wurden aufgezeichnet. Bei späteren Hausdurchsuchungen wurden die Computer der angezeigten Chatter beschlagnahmt.

Nicht immer führt jedoch eine IP- oder E-Mail-Adresse zur exakten (Wohn-)Adresse des Täters, weshalb häufig der Einfallsreichtum der Ermittler gefragt ist. Eine Gruppe von Gymnasiasten hatte in Deutschland einen florierenden Warez-CD-Versand unterhalten. Bei den weiteren Ermittlungen konnte lediglich die Anschrift eines Häuserblocks ausfindig gemacht werden. Welche Wohnung von den Tätern genutzt wurde, erfuhren die Verfolger mit einem klassischen Detektivtrick: Sie strichen unsichtbare fluoreszierende Farbe auf das Postfach, in dem die Umschläge mit den Geldscheinen eingingen und durchwanderten den Wohnblock so lange mit Spezialbrillen, bis sie Farbspuren an der Tür der Täterwohnung ausfindig machen konnten.[615]

Abschließend kann man festhalten, dass Mitglieder von Warez-Gruppen, die ohne Bereicherungsabsicht arbeiten, den Fahndern entweder zufällig ins Netz gehen oder dann, wenn sie von Personen aus den eigenen Reihen verraten werden. Konkrete Hinweise oder extreme Nachlässigkeit der Täter sind die häufigsten Fallstricke für die Softwarepiraten. Das Internet bietet auch weiterhin genügend Möglichkeiten, um anonym zu bleiben. Welch geringen Eindruck die aufwändigen Maßnahmen der Strafverfolger bei den Warez-Gruppen hinterlassen, zeigen die oben erwähnten Aktionen der US-Behörden: Wenige Wochen oder gar Tage nach einem „Bust" wurden wieder neue Programme von den verbliebenen Gruppenmitgliedern veröffentlicht. Meist wird der Gruppenname gewechselt, und nicht selten folgen humoristische Andeutungen in den nächsten NFO-Dateien.

Dem wachsenden Verfolgungsdruck ist es zuzuschreiben, dass sich die Sicherheitsvorkehrungen der Gruppen auf einem sehr hohen Niveau befinden. Wie bereits erwähnt, zeichnen sich die Täter durch besondere Flexibilität und durch großes technisches Know-how aus. Man kann getrost davon ausgehen, dass auf öffentlichen IRC-Servern keine Gruppenmitglieder mehr unter ihren Gruppenpseudonymen anzutreffen sind und dass verstärkt Kryptographie für die Kommunikation zum Einsatz kommen wird.

---

[614] Pressemeldung der *BSA*, http://www.bsa.org/usa/press/newsreleases/1999-11-16.171.phtml.
[615] *Fremerey*, Rauben und Kopieren, **c't** 8/2000, S. 99.

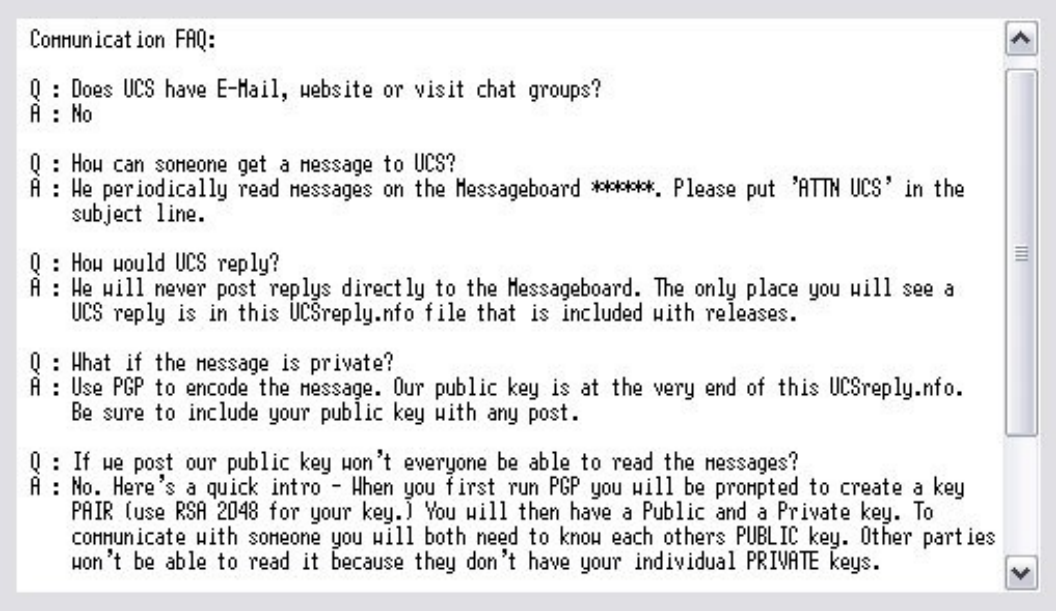


Abbildung 87 – Auszug aus einer NFO-Datei

b) Anlassunabhängige Ermittlungen

Nur wenige Strafverfolger – wie zum Beispiel die Beamten des Dezernats Wirtschaftsdelikte in der Münchener Kriminalpolizeidirektion 2 – suchen selbsttätig im Internet nach Angeboten von Profit-Pirates[616]. Das Hauptaugenmerk der Internet-Fahnder richtet sich in Deutschland auf verbotene Pornographie und politischen Extremismus.

Seit Januar 1999 recherchieren auch zwölf Beamte des *BKA* in Wiesbaden verdachtsunabhängig im Internet. Derzeit konzentriert sich die Arbeit der *Zentralstelle für anlassunabhängige Recherche in Datennetzen (ZaRD)* vor allem auf Kinderpornographie, eine zunehmende Ausweitung auf andere Straftaten ist allerdings zu erwarten. Verstärkt wird die Wiesbadener Einheit von acht Beamten, die in Meckenheim bei Bonn das Netz nach links- und rechtsextremistischen Aufrufen durchsuchen. In einem ersten Resümee bezeichnete der Erste Direktor des *BKA Leo Schuster* die Erfolge der Internet-Fahndungsstelle als eindrucksvoll.[617]

Die *ZaRD* operiert rund um die Uhr in allen Datennetzen, das heißt nicht nur im Internet, sondern auch in speziellen Netzen von Online-Diensten. Die Internet-Recherche erstreckt sich grundsätzlich auf alle Dienste (WWW, IRC, FTP etc.). Bei der Kontrolle des IRC liegt der Schwerpunkt auf den drei großen Netzen DalNet, EfNet und UnderNet. In Eilfällen erledigt das *BKA* die Beweiserhebung, -sicherung und -dokumentation. Ansonsten stellt es die örtliche Zuständigkeit für die entsprechenden Fälle fest, und eventuell werden andere deutsche oder ausländische Behörden benachrichtigt. Die rechtliche Grundlage für die verdachtsunabhängigen Recherchen im Bereich der Medien- und Teledienste bildet die Aufgabennorm des § 2 Abs. 2 Nr. 1 i.V.m. § 2 Abs. 1 BKAG[618].

---

[616] Vgl. **GameStar** 12/1998, S. 76.
[617] *Schulzki-Haddouti*, Polizei im Netz, **c't** 13/1999, S. 16.
[618] Sofern eine Recherche zu einem Eingriff in das allgemeine Persönlichkeitsrecht eines Betroffenen führt, greifen als Befugnisnormen § 7 Abs. 1 bzw. § 7 Abs. 2 BKAG, vgl. Ahlf-*Ahlf*, § 7 BKAG, Rdnr. 6; a.A.: *Janssen*, S. 151 ff. und 173,

Bei ihren Ermittlungen im Pädophilen-Milieu setzen die Beamten des *BKA* vor allem auf die abschreckende Wirkung der sogenannten Internet-Streife. Jeder potentielle Vertreiber von Kinderpornographie soll aufgrund einer verstärkten Präsenz der Ermittlungsbehörden verunsichert werden[619]. Dies gilt vor allem für den IRC und WWW-Chaträume. Da den deutschen Beamten – im Gegensatz zu den *FBI*-Kollegen in den USA – verdeckte Ermittlungen untersagt sind, dürfen sie beispielsweise keine illegalen Dateien im Internet anbieten. Ein Auftreten mit einem szenetypischen Pseudonym fällt allerdings noch nicht unter den Begriff der verdeckten Ermittlung.[620]

Ob die Internet-Streife im Bereich der Raubkopierer-Szene ähnliche Erfolge erzielen würde, erscheint fraglich. Zunächst kann man davon ausgehen, dass die Mitglieder der Warez-Szene besser als die meisten Pädophilen mit der Internet-Technologie vertraut sind, so dass sie schneller feststellen werden, mit wem sie es zu tun haben. Daher wird oftmals Stillschweigen herrschen, wenn Nichteingeweihte einen einschlägigen Chatraum betreten. Zudem wird man in den entsprechenden Chaträumen keine Drahtzieher der Raubkopierer-Szene auffinden, sondern nur Trader und Leecher[621]. Gruppenmitglieder, die den IRC nutzen, haben ihre Kommunikation in den meisten Fällen in unsichtbare und überdies passwortgeschützte Channels oder gar auf eigene, nicht-öffentliche IRC-Server verlagert.

Spezielle Suchmaschinen, die das Angebot des WWW nach Raubkopien absuchen, sind zwar im Einsatz, werden allerdings nicht von der Polizei sondern von den Herstellerverbänden betrieben. Dennoch handelt es sich hierbei um eine wirkungsvolle Methode, um die Verbreitung von Raubkopien im Internet einzudämmen.

Da sich die betroffenen Verbände äußerst intensiv mit der Verfolgung von Softwarepiraten befassen, könnte die Polizei nur mit unverhältnismäßig hohem Personal- und Kostenaufwand eine ähnliche Arbeit leisten. Solange die Zusammenarbeit der Polizei mit den Verbänden funktioniert – wenn also den Hinweisen der Herstellerverbände auf adäquate Weise nachgegangen wird – ist die Errichtung polizeieigener Internet-Softwarepiraterie-Bekämpfungseinheiten nicht erforderlich.

c) Internationale polizeiliche Zusammenarbeit

Die von den meisten Wissenschaftlern zur effektiven Bekämpfung der Internetkriminalität geforderte verstärkte internationale Zusammenarbeit der Strafverfolgungsbehörden wird derzeit vorangetrieben.[622] Auf europäischer Ebene arbeitet das *BKA* mit *Interpol* (bzw. deren *European Working Party on Information Technology Crime*) zusammen und ist im Expertenkomitee der Europäischen Union für Datennetzkriminalität (*PC-CY*) vertreten. Die europäischen Regierungen haben Mitte November 2001 mit der Unterzeichnung des sogenannten Budapester Abkommens einen

---

der entgegen der gängigen Praxis zum Ergebnis kommt, dass das *BKA* keine rechtsstaatliche Kompetenz zur Durchführung von anlassunabhängigen Ermittlungen im Internet hat. Im Bereich der Gefahrenabwehr seien ausschließlich die Länder zuständig.

619 *Decius/Panzieri*, S. 9 f.

620 Zur Zulässigkeit polizeilicher Teilnahme an der Internet-Kommunikation vgl. *Ochsenbein*, **Kriminalistik** 1998, S. 686.

621 Vgl. oben Teil 2, A. V. 1. und 2.

622 Vgl. die vorgeschlagenen Maßnahmen von *Sieber*, Missbrauch der Informationstechnik, Teil 3, III. 3.

wichtigen Schritt zur Verbesserung der internationalen polizeilichen Zusammenarbeit unternommen.[623] Unterzeichnet haben das Abkommen neben Vertretern aus 26 Europaratsländern auch Repräsentanten aus den USA, Kanada, Japan und Südafrika.[624]

Das Cybercrime-Abkommen gilt als erstes internationales Vertragswerk, das jene Straftaten definiert, die mit Hilfe des Internet verübt werden können. Neben dem illegalen Abhören, dem Eindringen und Stören von Computersystemen, dem Stehlen, Manipulieren oder Löschen von Daten stellt das Abkommen das Herstellen, Verbreiten und Verfügbarmachen von Kinderpornographie sowie Verbrechen, die unter Ausnutzung von Computer-Netzwerken begangen werden können (Betrug, Geldwäsche, Vorbereitung terroristischer Akte), unter Strafe.[625] Artikel 10 der Konvention erfasst außerdem Vergehen gegen das Urheberrecht und das Umgehen von Kopierschutzsystemen, was sich aus der Einbeziehung der *WIPO*-Verträge WCT und WPPT ergibt[626]. Mit der Unterzeichnung der Konvention verpflichten sich die Länder, die aufgeführten Straftatbestände in ihre nationale Gesetzgebung aufzunehmen und unter anderem dafür zu sorgen, dass eine lückenlose Überwachung der Internetkommunikation in Echtzeit möglich ist. Des Weiteren regelt die Konvention grenzüberschreitende Amtshilfe sowie die Einrichtung eines rund um die Uhr tätigen internationalen Kontaktnetzwerkes.

Die EU-Mitgliedstaaten arbeiten außerdem in der Arbeitsgruppe *High-Tech Crime* zusammen mit den übrigen G8-Staaten (Japan, Kanada, Rußland und USA) an der Einigung auf gemeinsame Handlungsmuster für die Strafverfolgung im Internet.[627] Damit will man erreichen, dass auch die in anderen Mitgliedstaaten sichergestellten Beweise vor inländischen Gerichten verwertet werden können. Grundsätzlich ist dies eine Ermessensfrage der Gerichte. Da sich die Fahnder jedoch in einer juristischen Grauzone bewegen, wollen sich die G8-Staaten auf ein einheitliches rechtliches Konzept einigen, um Beweisdaten regelmäßig austauschen und internationale Fälle gemeinsam lösen zu können. Die Anpassung nationaler Rechtsnormen an die Vereinbarungen der Arbeitsgruppe *High-Tech Crime* sowie die Harmonisierung stark abweichender rechtlicher Situationen gehört zu den grundlegenden Zielen der Expertenkommission.

Zu den ersten Maßnahmen der G8-Arbeitsgruppe gehörte die Einrichtung einer 24-Stunden-Kontaktgruppe, um die Zusammenarbeit zwischen den nationalen Strafverfolgern über Landesgrenzen und Zeitzonen hinweg sicherzustellen. Die Kontaktleute können sich direkt an die Experten des anderen Landes wenden, und binnen 24 bis 48 Stunden erhalten sie die Daten, nach denen sie gefragt haben. Innerhalb eines Landes funktioniert die Kontaktgruppe folgendermaßen: Wenn jemand beipielsweise in den USA Hilfe benötigt, wendet er sich direkt an seinen Kontaktmann in der 24-Stunden-Kontaktgruppe. Dieser setzt sich umgehend mit dem jeweiligen Kontaktmann in dem anderen Land in Verbindung. Wenn er selbst eine Anfrage aus dem Ausland erhält, muss er sichergehen, dass ihm das nationale Recht erlaubt, die benötigten Daten zu erhalten und herauszugeben. Auf diese Vorgehensweise hat man sich geeinigt, da ein direkter Zugriff auf ausländ-

---

623 Die Konvention findet sich unter http://conventions.coe.int/treaty/en/treaties/html/185.htm.
624 **c't** 25/2001, S. 34
625 Vgl. **Heise Online News** vom 23.11.2001, http://www.heise.de/newsticker/meldung/22923.
626 Siehe Teil 2, C. I. 4.
627 Die G8-Arbeitsgruppe schließt keine formalen Abkommen. Die Diskussionsergebnisse der Mitglieder werden jedoch schriftlich niedergelegt und an entsprechende Stellen weitergeleitet. So erhielt der EU-Rat im Vorfeld des Cybercrime-Abkommens auch Vorschläge und Anregungen von der G8-Arbeitsgruppe – Vgl. das Interview mit *Charney*, bei *Schulzki-Haddouti*, World Wide Fahndung, **c't** 15/1999, S. 75.

dische Daten problematisch ist, sofern hierzu keine völkerrechtlichen Vereinbarungen getroffen wurden; die grenzüberschreitende Anfrage (Transborder Search) gilt in den meisten Fällen als Angelegenheit nationaler Souveränität, die nicht angetastet werden soll[628].

d) Zusammenarbeit mit der Providerindustrie

Im Dezember 1998 lud das *BKA* erstmals eine große Anzahl deutscher Providervertreter ein, um ihnen eine Selbstverpflichtungserklärung vorzustellen. Nach dem Wortlaut der Erklärung sollten die Provider selbst aktiv werden und die eigenen Datenbestände mit Hilfe von Suchprogrammen auf verdächtige Inhalte hin durchforsten und Tatverdächtige zur Anzeige bringen.[629] Bereits im Vorfeld der Veranstaltung wurde das Papier scharf kritisiert, da es über die gesetzlichen Pflichten des IuKDG hinausgehe, die Provider unverhältnismäßig wirtschaftlich belasten würde und zudem nicht frei von datenschutzrechtlichen Bedenken sei.[630] Die Selbstverpflichtungserklärung wurde schließlich nicht unterzeichnet, nachdem insbesondere der Verband der deutschen Internet-Wirtschaft *Eco* den Vorschlag des *BKA* zurückgewiesen hatte. Ein Sprecher von *Eco* lies verlauten, dass man weder Bedarf noch eine gesetzliche Rechtfertigung für eine derartige Erklärung sehe.

Bei einer zweiten Veranstaltung des *BKA* im Februar 2000 verabschiedeten rund 160 Vertreter von Online-Unternehmen eine gemeinsame Erklärung „zur Verhütung und Bekämpfung von Kriminalität im Internet“.[631] Bei der Erklärung handelt es sich im Wesentlichen um eine gemeinsame Willensbekundung, nicht jedoch um ein Verpflichtungspapier. Der Erste Direktor des *BKA Leo Schuster* bezeichnete das Papier als „in seiner Unverbindlichkeit beispielhaft“, es diene jedoch dazu, Berührungsängste abzubauen.

Auf beiden *BKA*-Veranstaltungen kam mehrmals zur Sprache, dass die Zusammenarbeit mit den Providern in Deutschland bislang äußerst unproblematisch verlaufen sei. Angesichts dieser positiven Entwicklung kann man auf eine Selbstverpflichtung der Provider zu selbsttätiger Fahndung vorerst verzichten; zumal ein größeres Verbrechensvorbeugungspotential in der Aufklärungsarbeit durch die Provider liegt.[632]

Exkurs – Selbstkontrolle und Codes of Conduct

Formelle Grundlage der Selbstkontrolle von Internet-Providern sind häufig sogenannte Codes of Conduct (Verhaltenskodizes). Oft werden diese von Providerverbänden festgeschrieben, allerdings kann eine solche Vereinbarung auch zwischen Providern und staatlichen Stellen getroffen werden. Ebenfalls ist eine Mitwirkung staatlicher Stellen bei der Erstellung solcher Kodizes denkbar. Durch die Verhaltenskodizes verpflichten sich die Mitglieder in der Regel dazu, der legalen Nutzung des Internets besondere Aufmerksamkeit zu widmen, im Rahmen des Möglichen und Zumutbaren rechtswidrige Inhalte zu unterbinden, Meldestellen zu schaffen, sich um die Identifizierung ihrer

---

628 Interview mit *Charney*, bei *Schulzki-Haddouti*, World Wide Fahndung, **c't** 15/1999, S. 75.
629 **ZDNet News** vom 17.12.1998, http://news.zdnet.de/story/0,,t532-s2045757,00.html.
630 Vgl. *Schulzki-Haddouti*, Internet-Hilfssheriffs, **c't** 1/1999, S. 16.
631 Veröffentlicht auf der Webseite des *BKA* (http://www.bka.de). Die Erklärung erstreckt sich auch auf Verstöße gegen das Urheberrecht.
632 Siehe unten Teil 2, C. V. 3.

Kunden zu bemühen und bestimmte Straftaten bei den Behörden zu melden. Verstöße gegen diese Pflichten haben in der Regel Sanktionen zur Folge, deren Spektrum von bloßen Hinweisen mit Abhilfeaufforderungen über Mißbilligungen bis zu öffentlichen Rügen reicht. Im Wiederholungsfall ist regelmäßig mit dem Ausschluss aus dem Verband zu rechnen.[633]

Von besonderem Interesse dürften in der Zukunft die Codes of Conduct sein, die von international tätigen Online-Diensten aufgestellt werden. Deren Kodizes könnten als sogenanntes Softlaw die Vorläufer international harmonisierter Regelungen sowie das Modell für ein weltweit harmonisiertes Strafrecht werden.[634] Hiervon abzugrenzen sind freiwillige Maßnahmen der Provider in Eigeninitiative, die im Folgenden dargestellt werden.

6. Freiwillige Maßnahmen von Providern

Unternehmen, die jedermann die kostenlose Erstellung von Homepages anbieten, haben in der Regel detailliert ausgearbeitete Benutzerbestimmungen, die den Nutzern vor der Einrichtung ihrer Homepage in Form eines Online-Formulars zur Zustimmung vorgelegt werden. Diese Bestimmungen, die oftmals als „Member Policy" betitelt sind, enthalten zahlreiche Hinweise darauf, welche Inhalte auf den Homepages geduldet werden und welche Inhalte der Nutzer nicht hochladen darf. Mit dem Akzeptieren der Benutzerordnung erklärt sich der Nutzer weiterhin einverstanden, dass der Provider die Seite vom Netz nehmen darf, sobald der Nutzer gegen die freiwillige Selbstverpflichtung verstößt.

By using our services in any matter whatsoever, you agree to the following conditions.
CJB.NET may only be used for lawful purposes. Any use of these services which violates any local, state, federal, or international laws which may apply to CJB.NET, your local jurisdiction, or any jurisdiction that you or your site may be subject to is strictly prohibited.

[...]

CJB.NET reserves the right to refuse to post or to remove any information or materials, in whole or in part, that, in its sole discretion, are unacceptable, undesirable, or in violation of this agreement.

[...]

We do not allow the following:
- nudity, pornography, sexual material, hate propaganda or hate mongering, swearing, or fraudulent material or activity;
- any material that violates or infringes in any way upon the rights of others, including, without limitation, copyright or trademark rights;
- any material that is threatening, abusive, harassing, defamatory, invasive of privacy or publicity rights, vulgar, obscene, profane, indecent, or otherwise objectionable, or that violates any law or gives rise to any legal liability;
- material that promotes, encourages, or provides instructional information about illegal activities;
- any software, information, or other material that contains a virus, corrupted data, or any other harmful or damaging component;
- sending unsolicited e-mail or any other type of spam containing *any* reference to your web site or account.

Abbildung 88 – Beispiel für typische Nutzungsbedingungen eines Webspace-Providers (hier *CJB.net* – http://www.cjb.net)

633 *Sieber*, Die Verantwortlichkeit von Providern im Rechtsvergleich, **ZUM** 1999, S. 208.
634 *Sieber*, Die Verantwortlichkeit von Providern im Rechtsvergleich, **ZUM** 1999, S. 208.

Einige Anbieter von freien Homepages warten nicht erst, bis rechtswidrige Inhalte entdeckt werden, sondern versuchen von vornherein das Hochladen von Raubkopien zu verhindern. Dies erreichen sie zum Beispiel dadurch, dass Dateien mit den Endungen .DIZ und .NFO, wie sie für Warez-Releases typisch sind, nicht mehr auf den Webservern abgelegt werden dürfen.

Provider, die ihren Kunden einen News-Server bereitstellen, können ebenfalls Präventivmaßnahmen gegen die Verbreitung von Raubkopien ergreifen, indem sie zweifelhafte Newsgroups aus dem Angebot herausnehmen. Um herauszufinden, welche Newsgroups rechtlich bedenklich sind, kann sich der Provider zum Beispiel an die Empfehlungen von Organisationen wie *NewsWatch*[635] halten.

„Die Notbremse gezogen" haben kürzlich einige Universitäten in Deutschland. Die Hochschulen, die auch als Zugangsanbieter für ihre Studenten fungieren, mussten feststellen, dass beinahe ein Drittel des gesamten universitären Datenvolumens auf die Studentenwohnheime entfiel.[636] Die in den Wohnheimen untergebrachten Studenten sind durch Hochgeschwindigkeitszugänge mit dem Internet verbunden, und viele von ihnen luden hemmungslos riesige Datenmengen, in erster Linie urheberrechtlich geschützte Dateien wie Filme, Musik und Software, herunter. Die Verantwortlichen reagierten unterschiedlich auf die Situation: Bei den Universitäten Siegen und Stuttgart entschied man sich für die Sperrung einzelner Ports, um die Nutzung von Filesharing-Programmen zu verhindern, in Leipzig setzte man ein tägliches Transferlimit von 250 Megabyte. An der Universität Bonn erlaubte man pro Zugang 5 Gigabyte pro Monat.

Bei den Maßnahmen der universitären Rechenzentren handelte es sich nicht direkt um Maßnahmen zur Pirateriebekämpfung, da in erster Linie wirtschaftliche Gründe ausschlaggebend waren. Denn die Universitäten müssen die Übertragungskontingente beim *Deutschen Forschungsnetz (DFN)* ordern und bezahlen.

Die zuvor beschriebenen Maßnahmen der Webhosting-Provider bewirken in erster Linie, dass Anbieter illegaler Inhalte die entsprechenden Unternehmen meiden und auf andere Unternehmen mit schlechteren Schutzmaßnahmen zurückgreifen. Somit findet lediglich eine Verlagerung des Problems statt, weshalb alle Provider dazu angehalten werden sollten, ähnlich zu verfahren. Schlussendlich kann sich jedoch kein Provider davor schützen, dass Raubkopien auf seinen Servern abgelegt werden, zumal diese nicht immer auf den ersten Blick zu identifizieren sind. Es ist unmöglich, Millionen von Dateien genau auf ihren Inhalt hin zu analysieren. Da zahlreiche Dateien durch Umbenennen oder Verpacken getarnt sind, ist es mit einfachem Anschauen in der Regel nicht getan. Eine effektive Maßnahme besteht allerdings in der Begrenzung des Webspaces auf eine gewisse Dateigröße, die es für die Warez-Trader uninteressant macht, Programme dort abzulegen.

---

635 Informationen zu *NewsWatch* finden sich unter http://www.eco.de/ictf/newswatch/ziele/ziele_de.htm.
636 **c't** 15/2001, S. 54.

7. Freiwillige Maßnahmen von Public-FTP-Administratoren

Verwalter öffentlicher FTP-Server – vor allem von Universitäten und großen Unternehmen – haben beinahe täglich mit Raubkopien zu tun. Piraten aus aller Welt nutzen die ungeschützten Incoming-Verzeichnisse der schnellen Server als vorübergehenden Ablageplatz für illegale Software. An der Universität Rostock werden daher regelmäßig Kontrollen der öffentlich nutzbaren Server durchgeführt:[637] Entdecken die Verantwortlichen bei den Überprüfungen inakzeptable Dateien, werden diese unmittelbar gelöscht. Haben Nutzer der Uni-Rostock (meist Studenten) illegale Inhalte auf einen Universitätsserver hochgeladen, werden sie von der Rechner- und Netznutzung gesperrt, und es werden gegebenenfalls rechtliche Schritte eingeleitet.[638] Zeitweise wurde das Incoming-Verzeichnis[639] völlig gesperrt, da jedoch zahlreiche „ordentliche" Anwender dieses Verzeichnis nutzen wollten, musste man es wieder freigegeben. *Jörg Maletzky* vom Rechenzentrum der Universität Rostock erwog zwischenzeitlich, das Incoming-Verzeichnis wenigstens an den Wochenenden zu sperren, da in diesem Zeitraum die Überprüfungsmöglichkeiten eingeschränkt sind.

Falls man sich für eine Sperrung entscheidet, kann nur der Schreibzugriff auf das Verzeichnis verhindert werden. Alle anderen Möglichkeiten, wie Verbot des Lesezugriffs, Verstecken des Verzeichnisses oder Zugriffssteuerung über IP-Adressen würden den Nutzerservice verschlechtern; außerdem seien diese Maßnahmen nicht hundertprozentig sicher.[640]

Mittlerweile sind die meisten Universitäten zu einer Zugriffssteuerung per IP-Adresserkennung übergegangen. Hierbei können nur solche Nutzer, deren IP-Adresse in einen bestimmten Bereich fällt (z.B.: 134.176.***.***)[641], den FTP-Server nutzen. Diese können zwar immer noch den Server für illegale Aktivitäten missbrauchen, allerdings fallen deren Verbindungsdaten im selben Rechenzentrum an, so dass eine Identifikation der Täter ohne großen Aufwand möglich ist. Voraussetzung hierfür ist, dass sämtliche Aktivitäten auf dem FTP-Server protokolliert werden, was allerdings der Regelfall ist.

8. Rechtliche Maßnahmen zur Bekämpfung unerlaubter Verwertung von urheberrechtlich geschützten Werken per Internet

a) Verpflichtung von Providern zur Sperrung oder Filterung des Online-Angebots / Verantwortlichkeit der Diensteanbieter

Bereits untersucht wurde die strafrechtliche Verantwortlichkeit der unmittelbaren bzw. aktiven Täter. Grundsätzlich gilt dabei, dass alles, was offline strafbar ist, auch online strafbar sein muss. Fraglich ist, wer neben den unmittelbaren Tätern noch für Rechtsverstöße im Internet zur Rechenschaft gezogen werden kann. Von besonderem Interesse sind aus verschiedenen Gründen die Dienste-anbieter (Betreiber von elektronischen Kommunikationsdiensten und Netzwerken): Zum einen sind

---

[637] Vgl. das Interview mit *Maletzky* vom Rechenzentrum der Universität Rostock, **PC-Intern** 8/1999, S. 34.
[638] Geregelt ist dies in einer speziellen Benutzerordnung – Betriebsregelung und Benutzerordnung für das Daten-kommunikationsnetz der Universität Rostock (RUN) vom 02.02.2000, zu finden unter http://www.uni-rostock.de/Rechenzentrum.
[639] Beim Incoming- oder Upload-Verzeichnis handelt es sich um einen Speicherort für Dateien, für den in der Regel jedermann die Schreib- und Leserechte hat.
[640] Vgl. das Interview mit *Maletzky* vom Rechenzentrum Universität Rostock, **PC-Intern** 8/1999, S. 34.
[641] Ein bestimmter Adressbereich wird in diesem Zusammenhang auch als „IP-Range" oder „Hostmask" bezeichnet.

die unmittelbaren Täter oftmals schwer oder gar nicht zu identifizieren, zum anderen verfügen sie regelmäßig nicht über eine nennenswerte Haftungsmasse, falls es zu einem Zivilprozess kommt[642]. Gerade im Fall der Verbreitung von illegaler Software, bei der es fast immer um enorme Werte geht, ist ein solventer Klagegegner von Interesse für die geschädigten Unternehmen.

Eine mögliche Providerhaftung findet ihre Grundlage im TDG bzw. im Staatsvertrag über Mediendienste (MDStV)[643]. Auf die Verantwortlichkeitsregelungen der §§ 8 ff. TDG für Teledienste wurde bereits eingegangen;[644] Access-Provider und Webhosting-Provider fallen unstreitig in den Anwendungsbereich dieser Normen, vgl. § 2 Abs. 2 Nr. 2 und 3 TDG.

§ 8 Abs. 1 TDG sieht eine volle Verantwortlichkeit für Content Provider vor. Content Provider sind solche Anbieter, die eigene Inhalte zur Nutzung bereithalten. Hierzu gehören in erster Linie die Online-Service-Provider, die für ihre Kunden proprietäre Dienste und Informationen anbieten. Wie bereits dargelegt wurde, sind die Verantwortlichkeitsregelungen der §§ 8 ff. TDG der straf- und zivilrechtlichen Prüfung vorgelagert.[645] In persönlicher Hinsicht ist bei einer weiteren Prüfung auf die Inhaber oder Beschäftigten des jeweiligen Diensteanbieters abzustellen.[646]

Im TDG ist auch die Verantwortlichkeit der Diensteanbieter bezüglich fremder Informationen geregelt. Grob kann man zwischen der Haftung für fremde Informationen auf eigenen Servern und der Haftung für die Zugangsvermittlung zu fremden Informationen unterscheiden. Die Konstruktion, nach der die Diensteanbieter in die Pflicht genommen werden sollen, beruht in erster Linie auf dem Gedanken, dass sie sich der Beihilfe zur Verbreitung rechtswidriger Informationen durch Unterlassen schuldig machen.

(1) Haftung der Diensteanbieter für fremde rechtswidrige Informationen, die auf den eigenen Servern liegen

§ 11 TDG sieht vor, dass Diensteanbieter für fremde Informationen, die sie für einen Nutzer speichern, nicht verantwortlich sind, sofern sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben und ihnen im Falle von Schadensersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, oder sie unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie diese Kenntnis erlangt haben. Solange also der Diensteanbieter – in den meisten Fällen ein Webhosting-Provider – noch keine Kenntnis von einer rechtswidrigen, fremden Information auf seinem Server hat, ist er für die Rechtsgutsverletzung nicht verant-wortlich. Des Weiteren unterliegt der Anbieter keiner allgemeinen Pflicht zur Überprüfung

---

642 Vgl. *Sieber*, Kontrollmöglichkeiten – Teil 1, **CR** 1997, S. 581, der das *Bundesforschungsministerium* und den *Deutschen Bundestag* bei der Entwicklung des § 5 TDG a.F. beraten hat.

643 Die Zuständigkeiten im Bereich der neuen Medien sind auf Bund und Länder verteilt. Das IuKDG des Bundes regelt die Teledienste und der Medienstaatsvertrag der Länder die Mediendienste. Letztere unterscheiden sich von Telediensten darin, dass bei ihnen die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht. Die Aufspaltung der Verantwortlichkeitsregelungen wird insofern kritisiert, als die Grenzen zwischen den einzelnen Online-Dienstleistungen fließend sind, was für viele Unternehmen eine gewisse Rechtsunsicherheit bedeutet – vgl. *Schulzki-Haddouti*, Gemäßigtes Krötenschlucken, **c't** 18/1999, S. 81. Da Raubkopien ausschließlich über Teledienste vertrieben werden, ist für die weiteren Ausführungen nur die Anwendung des TDG von Interesse.

644 Siehe oben Teil 2, C. I. 3. c) (1).

645 Siehe oben Teil 2, C. I. 3. c) (1).

646 *Sieber*, Die rechtliche Verantwortlichkeit im Internet, III. 2. a).

der auf seinen Rechnern gespeicherten Dateien hinsichtlich der Rechtmäßigkeit, vgl. § 8 Abs. 2 S. 1 TDG[647]. Abweichende Ansichten sind aus verschiedenen Gründen nicht vertretbar:

Bei den eigenen Servern des Diensteanbieters wird es sich in den meisten Fällen um Webserver, Mailserver, News-Server und IRC-Server handeln. Das Auffinden rechtswidriger Inhalte wird sich dementsprechend schwierig gestalten. Zwar befinden sich die Rechner im Herrschaftsbereich des Providers, allerdings handelt es sich um einen unüberschaubaren und zudem stark dynamischen Datenbestand.

Die Qualifizierung verdächtiger Inhalte als rechtswidrig ist dem Laien kaum möglich und kann eigentlich nur von Juristen oder Spezialisten der Polizei in befriedigender Weise vorgenommen werden. Frühere Vorschläge, nach denen die Provider auf eigene Kosten Anwälte mit Gutachten zur Einstufung fragwürdiger Netzfunde beauftragen sollten, haben sich nicht durchgesetzt. Mit der Einrichtung einer zentralen Meldestelle durch das *BKA*, bei der auch die Provider Inhalte überprüfen lassen können, wurde ein wichtiger Schritt in die richtige Richtung getan. Denn wenn ein Service-Provider ohne genauere Überprüfung des Inhalts eine Webseite vom Netz nimmt, geht er immer das Risiko ein, vom Betreiber der Seite auf Schadensersatz verklagt zu werden oder Kunden zu verlieren.[648]

Ein weiteres großes Problem bei der Identifikation rechtswidriger Inhalte stellen die Umgehungsmöglichkeiten dar, die das Internet zum Schutz vor Entdeckung bietet. So ist es an der Tagesordnung, dass Betreiber von Warez-Webseiten die ZIP- oder RAR-Dateien, in denen die Raubkopien enthalten sind, dergestalt umbenennen, dass sie unverdächtig erscheinen. Der eingeweihte Nutzer lädt sich dann das vermeintliche Bild- oder Textdokument herunter und benennt es auf dem heimischen Rechner wieder in eine ZIP-Datei um. Auf diese Weise ist es unmöglich, per Augenschein oder durch computergestützte Filterung der Dateinamen auf den wahren Inhalt der Datei zu schließen. Nur eine ausführliche Analyse der Dateistruktur würde zu befriedigenden Ergebnissen führen, was allerdings bei Millionen einzelner Dateien einen irrwitzigen Personal- und Zeitaufwand bedeuten würde.

Eine Filterung, Analyse und Kontrolle der Kommunikation über einen IRC-Server (Echtzeitkommunikation) ist bereits aus technischen Gründen nicht möglich. Ein IRC-Server ist mit der Vermittlungsstelle einer Telefongesellschaft vergleichbar, d.h. die übertragenen Daten werden grundsätzlich nicht auf einem Computersystem zwischengespeichert, sondern nur durchgeschleust, so dass sie nach der Übertragung nicht mehr rekonstruiert werden können.[649] Da das Zwischenspeichern zu Kontrollzwecken eine zeitliche Verzögerung der Datenübertragung bewirkt, wären alle Formen der Echtzeitkommunikation wie IRC, Web-Chat, Internet-Telefonie und Internet-Videoconferencing nicht mehr realisierbar. Insbesondere die beiden zuletzt genannten Beispiele gelten gemeinhin als zukunftsträchtige Internetanwendungen, deren Entwicklung nicht ernsthaft in Frage gestellt werden darf.

---

[647] Dies entspricht auch der einhelligen Ansicht, vgl. *Vassilaki*, Was ich nicht weiß, **c't** 7/2002, S. 210; *Elschner/Schuhmacher*, DFN.de.

[648] *Heinzmann/Ochsenbein*, Strafrechtliche Aspekte des Internet – Teil 2, **Kriminalistik** 1998, S. 610 (Tabelle zu Sperrmöglichkeiten auf S. 604).

[649] *Sieber*, Kontrollmöglichkeiten – Teil 2, **CR** 1997, S. 660.

Stößt der Betreiber eines IRC-Servers auf einen verdächtigen Channelnamen oder erhält er einen Hinweis auf zweifelhafte Aktivitäten in einem bestimmten Channel, kann er zwar den entsprechenden „Gesprächsraum" sperren, er kann allerdings nicht verhindern, dass immer wieder neue Channels gegründet werden. Zudem ist fraglich, ob das Sperren eines Channelnamens in jedem Fall den gewünschten Erfolg bewirkt:[650] Wenige Sekunden der Auflösung des alten Channels kann ein Channel mit einem unverdächtigen Namen gegründet werden. Hierbei besteht die Gefahr, dass man Täter nur noch sehr schwer aufspüren kann, bzw. den Überblick über eine Szene verliert. Dies gilt insbesondere für Delikte wie Kinderpornographie, bei denen jeder Kontakt mit einem Straftäter weiterführende Hinweise liefern kann. Die Kontrolle privater Chatgespräche durch den Provider kollidiert zudem – ebenso wie die Kontrolle der E-Mail-Kommunikation – mit dem Fernmeldegeheimnis und ist ohne richterliche Anordnung unzulässig. Eine solche Maßnahme käme dem Unterfangen gleich, jeden Brief und jedes Päckchen von der Post öffnen zu lassen, um den Inhalt zu untersuchen. Bei der Kontrolle des E-Mail-Verkehrs ergeben sich ebenfalls ernstzunehmende technische Probleme. Dies liegt zum einen an der Menge der täglich verschickten E-Mails, zum anderen daran, dass die E-Mails nur für kurze Zeit auf den Mailservern zwischenlagern, bis sie vom Empfänger heruntergeladen und gelöscht werden. Auch die wachsende Anzahl verschlüsselter E-Mails macht eine Kontrolle der Inhalte unmöglich.

Bei den öffentlich zugänglichen Webseiten und Newsgroups bestehen die Schwierigkeiten beim Auffinden rechtswidriger Inhalte hauptsächlich in der Menge der zu untersuchenden Daten. Eine manuelle Überprüfung würde Hunderte von Arbeitskräften erfordern, die zudem über eine entsprechende Ausbildung verfügen müssten, um die strafrechtliche Relevanz der Inhalte zu beurteilen.[651] Computergestützte Filterprogramme liefern derzeit nur ungenügende Ergebnisse[652], weshalb anschließend eine zusätzlicher persönliche Überprüfung erfolgen müsste.[653]

Eine weitere Schwierigkeit besteht im sogenannten Store-and-forward-Prinzip, welches dem News-Dienst zugrunde liegt. Es bewirkt, dass eine Nachricht nicht mehr aufzuhalten ist, wenn wenige Minuten seit dem Abschicken verstrichen sind. Bereits dann ist sie weltweit auf einigen tausend News-Servern vorhanden, auf denen sich zehntausende von Newsgroups und Millionen von Einzelnachrichten befinden. Somit ist das Zeitfenster für die rechtzeitige Entdeckung einer rechtswidrigen Nachricht äußerst klein; Erfolge sind auf Zufallstreffer beschränkt.

Eine Kontrolle der Inhalte, die über eigene Server verbreitet bzw. ausgetauscht werden, ist den Service-Providern demnach gar nicht oder nur in unzumutbarer Weise möglich, weshalb eine Verpflichtung hierzu nicht entgegen dem Wortlaut in das Gesetz hineininterpretiert werden sollte.[654]

---

[650] So gefordert von *Decius/Panzieri*, S. 11.
[651] *Sieber*, Kontrollmöglichkeiten – Teil 2, **CR** 1997, S. 656.
[652] So im Ergebnis auch *Janssen*, S. 33 f. und 167.
[653] Siehe unten Teil 2, C. III. 8. a) (2) (b).
[654] Die damalige *Bundesregierung* erachtete es ebenfalls für „zunehmend unmöglich [...], alle fremden Inhalte im eigenen Dienstebereich zur Kenntnis zu nehmen und auf ihre Rechtmäßigkeit zu überprüfen", **BT-Drucks.** 13/7385 vom 09.04.1997, S. 20.

(2) Haftung für die Zugangsvermittlung zu fremden Inhalten

Fraglich ist, inwieweit ein Zugangsvermittler verhindern kann, dass rechtswidrige Inhalte von fremden Servern zum Kunden gelangen können, bzw. dass der Kunde auf diese zugreifen kann, und wann der Provider zu solchen Maßnahmen verpflichtet ist.

Von den §§ 9 und 10 TDG werden grundsätzlich alle Inhalte erfasst, die nicht von dem Anbieter selbst stammen und sich nicht auf dessen Servern befinden. Die Regelungen betreffen also den Access-Provider. Die §§ 9-10 TDG schließen die Verantwortlichkeit des Diensteanbieters bei der reinen Durchleitung und die Zwischenspeicherung zur beschleunigten Übermittlung (Caching) von Informationen aus. Dies setzt freilich voraus, dass er in keiner Weise mit den Informationen in Verbindung steht. Er darf also die Übermittlung nicht veranlasst haben und den Adressaten nicht ausgewählt oder die Informationen selektiert oder verändert haben, § 9 Abs. 1 TDG. Der Diensteanbieter muss allerdings gemäß § 10 Nr. 5 TDG den Zugang zu den im Rahmen des Caching übermittelten Informationen sperren, wenn er Kenntnis davon erhalten hat, dass die Informationen am Ursprungsort aus dem Netz entfernt worden sind, der Zugang zu ihnen gesperrt wurde, oder ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat.[655]

Somit haften weder der Provider noch seine Mitarbeiter für die zahlreichen rechtswidrigen Inhalte, die über das Internet von Servern auf der ganzen Welt abgerufen werden können. Dies gilt auch dann, wenn sie auf irgendeine Weise Kenntnis von bestimmten rechtswidrigen Inhalten unter Angabe der Adresse erhalten.[656]

Mit der Neuregelung des TDG ergibt sich eine neue Systematik für die Verantwortlichkeit der Access-Provider: Außer im Fall von gerichtlichen und verwaltungsbehördlichen Verfügungen tragen die Diensteanbieter keine Verantwortung für fremde Inhalte. Erst wenn eine Verfügung in Kraft tritt, muss der Anbieter solche Inhalte sperren oder entfernen.[657] Somit ergibt sich aus dem TDG keine allgemeine Verpflichtung der Provider zur Sperrung von Dateien auf anderen Servern.

Zuvor wurde die Ansicht vertreten, dass ISPs schon von Gesetzes wegen zur Sperrung des Zugangs zu rechtswidrigen Inhalten verpflichtet seien, ohne dass es einer besonderen Anordnung bedarf.[658] Diese Meinung stützte sich auf den Wortlaut des § 5 Abs. 4 TDG a.F., wonach „Verpflichtungen zur Sperrung der Nutzung rechtswidriger Inhalte nach den allgemeinen Gesetzen" unberührt bleiben, „wenn der Diensteanbieter unter Wahrung des Fernmeldegeheimnisses gemäß § 85 des Telekommunikationsgesetzes (TKG) von diesen Inhalten Kenntnis erlangt und eine Sperrung technisch möglich und zumutbar ist". Der neu eingeführte § 8 Abs. 2 S. 2 TDG enthält den Passus „technisch möglich und zumutbar" nicht mehr, Sperr- bzw. Filtermaßnahmen sind beschränkt auf freiwillige Kooperation sowie Gerichtsbeschlüsse und verwaltungsbehördliche Anordnungen für jeden Einzelfall.

Selbst wenn sich Network- oder Access-Provider in Zusammenarbeit mit der Content-Industrie entschließen sollten, Filtersysteme zu installieren, oder wenn eine Sperrverfügung gegen sie ergeht, ist

---

655 Vgl. *Vassilaki*, Was ich nicht weiß, **c't** 7/2002, S. 210.
656 Vgl. *Elschner/Schuhmacher*, DFN.de.
657 *Schulzki-Haddouti*, Trümpfe für den E-Commerce, **c't** 11/2000, S. 46.
658 So dargestellt bei *Schuhmacher*, DFN.de.

zu bezweifeln, dass die Sperr- bzw. Filtermaßnahmen beim jetzigen Stand der Technik den gewünschten Erfolg bringen.

(a) Kontrollmöglichkeiten von Network-Providern

Eine Kontrolle durch Network-Provider ist nur an wenigen Stellen möglich, beispielsweise an den Routern, die typischerweise an der „Auffahrt" zum transatlantischen Backbone benutzt werden oder an den sogenannten Peering-Punkten, an denen die großen Provider ihre Daten austauschen[659]. Wichtig ist in diesem Zusammenhang, die Eigenheiten des Internet-Protokolls zu berücksichtigen:

Eine zu versendende Datei wird zunächst in viele kleine Datenpakete aufgeteilt, diese werden mit Adressen versehen und auf den Weg geschickt. Unter Berücksichtigung der freien Leitungen berechnet das IP für jedes einzelne Datenpaket immer nur den Weg zum nächstgelegenen Router im Hinblick auf die Erreichung des Endzieles. Das Datenpaket wird mit jedem „Hop" dem Zielrechner ein Stück näher gebracht. Die verschiedenen Datenpakete einer einzelnen Nachricht (z.B. einer E-Mail) können dabei auf unterschiedlichen Wegen – und auch in unterschiedlicher Reihenfolge – ihr Ziel erreichen, wo sie vom Transfer Control Protocol (TCP) wieder in der richtigen Reihenfolge zusammengesetzt werden. Diese Datenübertragungstechnik hat zur Folge, dass die im Internet übermittelten Nachrichten – außer bei den Einwahlknoten oder zentralen Übertragungsstellen – nicht mit Sicherheit in vollständiger Form an irgendeinem Übertragungsknoten abgefangen und somit kontrolliert werden können. Diese Routingmethode geht auf das Protokoll des *ARPA-Net* zurück. Durch die nichthierarchische Konzeption des Netzes können die angeschlossenen Computersysteme auch bei Ausfall verschiedener Netzabschnitte selbständig alternative Datenverbindungen aufbauen. Eine Sperrmaßnahme an einem Router würde das Internet Protocol somit als einen Ausfall bzw. Störfall interpretieren und umgehen.[660] Eine Sperrung der Datenverbindung Moskau – Frankfurt wäre folglich wirkungslos, da die in Moskau angeforderten Daten über den Umweg Stockholm – Amsterdam – Essen nach Frankfurt gelangen würden. Somit scheidet eine Kontrolle durch die Network-Provider bereits durch die Eigenheit der Übertragungsprotokolle aus.

(b) Kontrollmöglichkeiten von Access-Providern

Durch die Herrschaft über die Einwahlknoten befinden sich Access-Provider in einer strategisch günstigeren Position. Allerdings bereitet ihnen das Auffinden und Klassifizieren von rechtswidrigen Inhalten die gleichen Probleme wie den Webhosting-Providern. Hinzu kommt, dass sich die zu kontrollierenden Daten nicht im Herrschaftsbereich des Access-Providers befinden, sondern ihn nur durchlaufen. Zwar können sich unter den Daten, die auf einem Proxy-Cache-Server des Access-Providers zwischengespeichert werden, auch rechtswidrige Inhalte befinden, jedoch werden diese nur für einen begrenzten Zeitraum vorgehalten, da die Datenfluktuation stark dynamisch und die Menge der Daten unüberschaubar ist.

---

[659] *Sieber*, Kontrollmöglichkeiten – Teil 2, **CR** 1997, S. 654.
[660] *Sieber*, Kontrollmöglichkeiten – Teil 1, **CR** 1997, S. 594.

Vielfach wurde und wird vorgeschlagen, Proxy-Cache-Server als Filtersysteme einzusetzen. Proxy-Cache-Server (oder nur Proxy-Server) sind in der Regel eigenständige Computersysteme, die sich zwischen dem Nutzer bzw. seinem Einwahlknoten und dem Internet befinden. Im Speicher der Server werden automatisch Kopien aller Daten abgelegt, die die Nutzer aus dem Internet abfragen. Sieht sich beispielsweise ein Nutzer eine Webseite in den USA an, werden die Bilder und die Textinformationen der Seite als Kopien auf dem Proxy-Cache-Server zwischengespeichert. Jeder andere Nutzer, der ebenfalls über diesen Server ins Internet geht (also jeder andere Kunde des Access Providers) und dieselbe Seite ansteuert, bezieht die Daten dann nicht aus den USA, sondern – wesentlich schneller und kostengünstiger – von dem Server in seiner Nähe. Die Daten werden allerdings nicht dauerhaft vorgehalten, ist ein gewisses Limit erreicht, ersetzen jüngere Dateien die älteren. Bei jeder Nutzeranfrage vergleicht die Software des Proxy-Cache-Servers das Erstellungsdatum der gecachten Datei mit der Originaldatei des Zielservers. Wird festgestellt, dass eine Datei des Zielservers aktueller ist, wird diese heruntergeladen und ersetzt die gecachte Datei.[661]

Durch Software-Modifikationen lässt sich ein Proxy-Cache-Server anders nutzbar machen als zur Entlastung des Netzes und zur Optimierung von Informationsprozessen: Der Proxy-Cache-Server, der sich zwischen Nutzer und Internet befindet, kann auch als Filter eingesetzt werden, da ihn sämtliche Abfragen der Nutzer durchlaufen müssen. Über den Vertrag mit dem Provider müsste sich der Nutzer damit einverstanden erklären, dass er nur gefilterte Inhalte erhält. Der einzige Weg ins Internet würde in diesem Fall über den Proxy-Server führen.[662] Erkennt der Server, dass eine Abfrage nicht beantwortet werden darf, bekommt der Nutzer die angeforderten Inhalte nicht angezeigt. Nur im Falle ihrer Unbedenklichkeit werden die eingehenden Daten an den Nutzer weitergeleitet.[663] Über die Programmierung kann man beispielsweise Anfragen an einzelne Hosts oder an Server in bestimmten Ländern bzw. Subnetzen sperren. Eine „schwarze Liste" mit URLs bzw. IP-Adressen könnte demnach gezielt aus dem Angebot herausgenommen werden. Allerdings ist die manuelle Erstellung einer solchen Liste angesichts der Masse von Webseiten unmöglich. Selbst die größten Suchmaschinen, die automatisiert mit der wertneutralen Katalogisierung des WWW beschäftigt sind, haben derzeit nur einen Teil aller Webseiten in ihren Datenbanken.

Daher wird von den Befürwortern des Filteransatzes eine automatisierte Filterung in Erwägung gezogen. Sogenannte Hautfilter-Programme und Programme zur Begriffsfilterung, die beim Zugangsanbieter installiert werden, sollen rechtswidrige Inhalte automatisch erkennen und deren Weiterleitung an den Kunden verhindern. Automatisierte Filtersysteme sind jedoch noch lange nicht geeignet, befriedigende Ergebnisse zu liefern: Zunächst würde ihr Einsatz zu drastischen Performanceverlusten bei Nutzern und Providern führen – insbesondere dann, wenn man nicht nur den Header der Dateien (Paketfilterung) überprüfen möchte, sondern auch den Inhalt auf der Anwendungsebene (z.B. Dateinamen, Dateityp etc.).[664]

Eine reine Begriffsfilterung – also eine Suche nach Schlüsselworten (z.B. nach dem Wort „Crackz" auf einer Homepage) – hat den Nachteil, dass verschlüsselte oder komprimierte Nachrichten sowie

---

661 Vgl. *Sieber*, Die rechtliche Verantwortlichkeit im Internet, IV. 4. d).
662 In diesem Fall spricht man auch von „Zwangsproxies".
663 *Sieber*, Kontrollmöglichkeiten – Teil 1, **CR** 1997, S. 590; die Bedenken, dass der Nutzer hinter einem Proxy-Cache-Server für die Außenwelt unsichtbar ist, wenn der Proxy-Cache-Server „im Auftrag des Nutzers" mit der Ziel-Webseite kommuniziert, sind insofern unbegründet, als man den Proxy-Server dergestalt einrichten kann, dass er die IP-Adresse des anfragenden Nutzers weiter übermittelt („IP-Forwarding").
664 *Sieber*, Kontrollmöglichkeiten – Teil 2, **CR** 1997, S. 660.

Binärdateien nicht erfasst werden. Das Bekanntwerden einer solchen Maßnahme hätte zudem die Einführung von Tarnbegriffen bzw. einer Geheimsprache zur Folge. Dies gilt insbesondere für die hochflexible Warez-Szene. Zu welch unbefriedigenden Ergebnissen eine Filterung nach Schlüsselworten führen kann, zeigt das folgende, häufig zitierte Beispiel: Als amerikanische Provider versuchten, auf ihren News-Servern Nachrichten mit dem Wort „Breast(s)" zu sperren, um sich pornographischer Angebote zu entledigen, kam es zu Protesten einer Gruppe von Frauen, die sich in einer entsprechenden Newsgroup bezüglich ihrer Brustkrebserkrankungen austauschten.[665]

Auch in Deutschland hat man ähnliche Erfahrungen gesammelt: Nachdem eine deutsche Universität alle Newsgroups mit der Bezeichnung „Sex" sperrte, wurde die dort geführte Gruppe „de.talk.sex" jahrelang unter der Bezeichnung „de.soc.verkehr" weitergeführt.[666]

Hautfilter-Programme analysieren Bilddateien und sperren ihre Weiterleitung, sobald der Anteil nackter Haut einen gewissen Prozentsatz übersteigt.[667] Es bedarf keiner weiteren Erläuterung, wenn in diesem Zusammenhang auf die Online-Angebote medizinischer Einrichtungen oder auf Hersteller von Bademoden verwiesen wird.[668]

Dass eine informationelle Abschottung mittels Firewall-Systemen wirkungslos ist, zeigen insbesondere die Fälle, in denen ganze Staaten versuchen, das Eindringen „systemunterwandernder" Informationen zu verhindern. Eine solche Abschottung betreiben derzeit neben China auch Ägypten, Singapur, Malaysia, Kuba, einige arabische Staaten und das weißrussische Belarus.[669]

Bei Firewall-Systemen (oder nur „Firewalls") handelt es sich um Hard- oder Softwaremodule, die zwischen ein Intranet und das Internet geschaltet werden, um einen unberechtigten Zugriff von außen auf die Daten des internen Netzes zu verhindern. Zu diesem Zweck verhindert eine Firewall zunächst den unkontrollierten Datenfluss aus dem Internet in das Intranet. Dies geschieht insbesondere durch eine Paketfilterung, die entweder Daten mit bestimmten Adressen (z.B. alle Adressen, die eine Länderkennung von westlichen Staaten enthalten) oder bestimmte Dienste sperrt.[670] Firewalls gelten als wirksamer Schutz vor Hacker-Angriffen, manche Unternehmen oder Behörden (z.B. die *NASA*) sind sogar durch mehrere Firewalls geschützt.

Chinesische Provider sind vom Staat zur Installation von Firewalls verpflichtet und mit weiteren strengen Auflagen und Meldepflichten konfrontiert. Jeder Bürger, der einen Internet-Anschluss beantragt, benötigt zudem eine polizeiliche Bescheinigung. Dennoch sind die Versuche, das Eindringen systemfeindlicher Informationen zu verhindern, wirkungslos. Führende Regimegegner wie *Wei Jingsheng* bestätigen, dass das Netz trotz staatlicher Überwachungsversuche nach wie vor als Kontakt- und Kommunikationsmedium für konspirativ arbeitende Menschenrechtsgruppen dient.[671] Hinzu kommt, dass sich zahlreiche Chinesen mit Satelliten-Telefonen in ausländische Netze einwählen und so vollen Zugriff auf das Internet erhalten. Regelmäßig kommt es vor, dass einzelne

---

665 *Sieber*, Kontrollmöglichkeiten – Teil 2, **CR** 1997, S. 658.
666 *Sieber*, Kontrollmöglichkeiten – Teil 2, **CR** 1997, S. 658.
667 Vgl. *Heinzmann/Ochsenbein*, Strafrechtliche Aspekte des Internet – Teil 2, **Kriminalistik** 1998, S. 602.
668 Vgl. *Gravenreuth*, Anmerkung zum Urteil des *AG München* vom 28.05.1998 (Az. 8340 Ds 465 Js 173158/95), **CR** 1998, S. 629.
669 Vgl. *Blittkowsky*, **c't** 9/1999, S. 76 f.
670 *Sieber*, Kontrollmöglichkeiten – Teil 1, **CR** 1997, S. 589.
671 *Blittkowsky*, **c't** 9/1999, S. 76.

Nutzer die unerwünschten digitalen Informationen in dem abgeschotteten Netz verbreiten. Durch das massenhafte Spiegeln (Mirroring) von westlichen Seiten wird die staatliche Zensur erfolgreich untergraben.

Dies macht deutlich, dass ein Zugriff auf ausländische Computersysteme durch den Nationalstaat nicht verhindert werden kann. Entsprechende Konzepte kommen daher allenfalls für Teilnetze mit thematisch begrenzten Aufgabenstellungen oder speziellen Aufgabengebieten in Betracht (z.B. Unternehmen oder Universitäten).[672] Will man eine Firewall zur Sperrung ganzer Dienste (IRC, FTP etc.) einsetzen, muss man den Zugriff der Kunden auf die üblicherweise verwendeten Ports sperren. Die Wirkung einer Portsperrung wäre jedoch mit Sicherheit nur von kurzer Dauer, da für die meisten Dienste die Portnummer frei wählbar ist. Außerdem zeichnet sich eine Entwicklung ab, wonach beinahe alle Dienste über einen Web-Browser über Port 80 genutzt werden können (z.B. Web-Chat). Angesichts der großen Bedeutung und überwiegenden Nutzung des WWW würde eine Sperrung von Port 80 einer Sperrung des gesamten Internets gleichkommen, weshalb dies niemand ernsthaft in Betracht zieht.

Es zeigt sich, dass die in der Diskussion befindlichen Sperr- bzw. Filtermaßnahmen der Access-Provider in den meisten Fällen nur temporären und lückenhaften Schutz bieten können. Darüber hinaus haben diese – oft als Zensur verstandenen – Maßnahmen weitere unerwünschte Nebeneffekte. Als *CompuServe* 282 problematische Newsgroups von den eigenen Servern verbannte, nachdem die deutsche Zentrale im November 1995 von der Kriminalpolizei durchsucht wurde, wurden die entsprechenden Newsgroups in der Folgezeit verstärkt aufgerufen.[673] Kenntnis von den indizierten Newsgroups hatten die neugierigen Internetnutzer durch die öffentliche Diskussion erhalten. Zugang erhielten sie über andere, zumeist öffentliche News-Server.

Ähnliches trug sich im Fall der sogenannten *Zündel*-Sites zu. Die Neonazi-Propagandaseiten sollten gesperrt werden, woraufhin einige Freespeech-Organisationen aus Protest die Seiten spiegelten (Mirroring) und von anderen Servern aus verfügbar machten.[674] Auch der sogenannte Radikal-Fall[675] ist ein Beispiel dafür, dass Sperrlisten zu Empfehlungskatalogen bzw. Qualitätssiegeln avancieren können.[676]

In Anbetracht der technischen und rechtspolitischen Bedenken bezüglich Sperr- bzw. Filtermaßnahmen wird deutlich, dass wirklicher Erfolg in der Bekämpfung von unerlaubter Verwertung urheberrechtlich geschützter Werke per Internet nur durch konsequentes Vorgehen gegen die Content Provider zu erzielen ist.

---

[672] *Sieber*, Kontrollmöglichkeiten – Teil 2, **CR** 1997, S. 659.
[673] *Sieber*, Kontrollmöglichkeiten – Teil 2, **CR** 1997, S. 665.
[674] Massenhaftes Mirroring von Webseiten findet auch in sogenannten Webarchiven statt. Unter http://www.archive.org/index.html wird beispielsweise seit 1996 ein Internet-Archiv geführt, bei dem man auf Webseiten aus vergangenen Jahren surfen kann; das Archiv enthält auch Seiten, die mittlerweile nicht mehr existieren, bzw. gesperrt wurden.
[675] Siehe oben Teil 2, C. I. 3. c) (5).
[676] *Sieber*, Kontrollmöglichkeiten – Teil 2, **CR** 1997, S. 666.

b) Kryptographie-Regulierung

Wie bereits erwähnt, hat der steigende Verfolgungsdruck dazu geführt, dass Warez-Gruppen immer häufiger verschlüsselt kommunizieren. Mit frei erhältlicher Verschlüsselungssoftware kann mittlerweile jeder normale Computerbesitzer seine E-Mails oder sonstige Dateien dergestalt verschlüsseln, dass sie für Dritte nicht mehr zugänglich sind. Ein heutiger „Standardschlüssel" ist schätzungsweise noch zehn Jahre lang vor Dechiffrier-Versuchen mittels Hochleistungscomputern gefeit.[677]

Der de-facto-Standard für Verschlüsselung und digitale Signaturen im Bereich der E-Mail-Kommunikation ist das Programm *Pretty Good Privacy (PGP). PGP* ist für den privaten Gebrauch als Freeware erhältlich und verwendet die sogenannte Public-Key-Kryptographie.[678] Anders als bei der symmetrischen Verschlüsselung, bei der die Passphrasen für Kodierung und Dekodierung identisch sind, braucht man sich bei der Public-Key-Kryptographie nicht mehr auf eine gemeinsame „Geheimsprache" zu verständigen, um verschlüsselt miteinander zu kommunizieren:

Bei der ersten Sitzung mit *PGP* generiert das Programm zwei individuelle Codes für den Benutzer. Einer der Schlüssel ist geheim und verbleibt immer auf dem eigenen Computer („Secret Key"), der zweite Schlüssel ist öffentlich („Public Key"). Letzteren muss man an jene Kommunikationspartner weitergeben, mit denen man verschlüsselte Informationen austauschen will. Die Übertragung kann nach persönlicher Absprache per Diskette oder per E-Mail erfolgen, per Download aus dem WWW oder auch über einen der eigens dafür eingerichteten Server. Solche Keyserver tun nichts anderes, als öffentliche *PGP*-Schlüssel zu sammeln und bereitzustellen.[679]

```
- – -----BEGIN PGP PUBLIC KEY BLOCK-----

Version: 2.7

mQA9Ai2wD2YAAAEBgJ18cV7rMAFv7P3eBd/cZayl8EEO6GYkhEO9SLJOw+DFyHg
Px5o+IiR2A6Fh+HguQAFEbQZZGVtbyA8ZGVtb0B3ZWxsLnNmLmNhLnVzPokARQIF
EC2wD4yR2A6Fh+HguB3xcBfRTi3D/2qdU3TosScYMAHfgfUwCelbb6wikSxoF5
ees9DL9QMzPZXCioh42dEUXP0g==
=sw5W

- – -----END PGP PUBLIC KEY BLOCK-----
```

Abbildung 89 – Beispiel für einen Public Key

Befindet sich der öffentliche Schlüssel des Nachrichtenempfängers im lokalen Schlüsselbund, lässt sich eine Nachricht mit diesem Schlüssel kodieren und absenden. In diesem Zusammenhang spricht man deshalb von zielorientierter Verschlüsselung.[680] Auf dem Weg durch das Internet ist die

---

[677] *Luckhardt*, Pretty Good Privacy – Teil 1, **c't** 12/1999, S. 212.
[678] Die ehemaligen Hersteller von *PGP*, *Network Associates, Inc. (NSI)*, haben Anfang 2002 bekannt gegeben, dass sie *PGP* nicht weiter entwickeln werden, dennoch ist das Programm tausendfach im Einsatz, weshalb sich die folgende Darstellung auf *PGP* bezieht. Hinzu kommt, dass sämtliche alternative Kryptographie-Lösungen, wie z.B. *GnuPG* oder der *OpenPGP* Standard, eine vergleichbare Funktionsweise besitzen. Ab November 2002 soll *PGP* vom neuen Eigentümer (*PGP Corporation*) in einer überarbeiteten Version veröffentlicht werden, die auch *Windows XP* unterstützt.
[679] *Luckhardt*, Pretty Good Privacy – Teil 1, **c't** 12/1999, S. 213.
[680] *PGP* verwendet mittlerweile ein sogenanntes DSS/DH-Schlüsselmodell (Digital Signature Standard & Diffie/ Hellmann); strenggenommen handelt es sich um ein sogenanntes *El-Gamal*-Schema, vgl. *Luckhardt*, Pretty Good Privacy – Teil 2, **c't** 13/1999, S. 208, m.w.N.

Nachricht vor Zugriffen Dritter geschützt, nur der geheime Gegenpart – der geheime Secret Key auf dem Rechner des Empfängers – kann die Operation rückgängig machen.

Neben der E-Mail-Verschlüsselung bieten bestimmte *PGP*-Versionen weitere Verschlüsselungsmöglichkeiten. Mit dem Tool *PGPdisk* können beliebige Daten auf der heimischen Festplatte verschlüsselt werden. Neben der Möglichkeit, chiffrierte virtuelle Laufwerke anzulegen (transparente Festplattenverschlüsselung)[681], erlaubt die Integration in das Kontextmenü des *Windows*-Explorers zudem die Bearbeitung aller Dateien eines ganzen Verzeichnisbaumes. Nach einer Verschlüsselung mit *PGPdisk* sind die ursprünglich unverschlüsselten Daten nicht wirklich von der Festplatte verschwunden. Die Löschfunktion des Betriebssystems markiert lediglich die Verzeichniseinträge einer Datei als ungültig. Die Daten selbst bleiben auf der Festplatte oder Diskette gespeichert und lassen sich mit speziellen Datenrettungstools ohne weiteres wiederherstellen, sofern die entsprechenden Sektoren nicht zwischenzeitlich neu beschrieben wurden. Für diesen Fall hat *PGP* eigene Löschfunktionen („Wipe", bzw. „Wipe Free Space"). Sie überschreiben zunächst mehrfach die Datensektoren, bevor sie die Verzeichniseinträge tilgen. Bei Anwendung beider Löschfunktionen ist eine Datenrekonstruktion so gut wie ausgeschlossen.[682] Stößt ein Ermittler auf derartig behandelte Daten, ist eine sofortige Entschlüsselung ohne Kenntnis des Secret Key unmöglich.

Wie weit *PGP* verbreitet ist, lässt sich nicht mit Sicherheit sagen. Die einzigen Rückschlüsse lassen die Keyserver zu: Mitte 1999 lagerten dort bereits über eine halbe Million *PGP*-Schlüssel.[683]

Zur Regulierung von Kryptographie werden weltweit unterschiedliche Ansätze verfolgt. Die USA setzten sich lange Zeit massiv für die Einführung des sogenannten Key Escrow und für internationale Exportbeschränkungen für Kryptographie-Software ein. Unter Key Escrow versteht man eine gesetzliche Verpflichtung, wonach jeder, der Kryptographie-Software nutzt, sämtliche Schlüssel bei einer staatlichen Stelle hinterlegen muss. Im Falle eines Verdachts könnten diese Stellen die gesamte Kommunikation des Verdächtigen entschlüsseln. Versuche, den Key Escrow gesetzlich zu verankern, sind allerdings in den USA gescheitert – ebenso wie ein Modell, wonach nur Verschlüsselungsverfahren zugelassen werden sollten, die eine Schlüsselrekonstruktion (Key Recovery) durch staatliche Stellen erlauben.[684]

Während in Deutschland Import und Export von Kryptographiesoftware seit jeher keinen Beschränkungen unterliegen[685], durften aus den USA lange Zeit nur solche Kryptographieprodukte exportiert werden, die mit einer Schlüssellänge von weniger als 56 Bit arbeiten[686]. Zum Vergleich: Ein standardmäßiger *PGP*-Schlüssel hat bereits eine Länge von 1024 Bit. Die US-Regierung befürchtete eine verheerende Wirkung auf Strafverfolgungsmöglichkeiten sowie einen Anstieg von Terrorismus und Drogenschmuggel. Im Ausschuss für Soldatenangelegenheiten wurde bereits darauf hingewiesen, dass die Überlegenheit des US-Militärs vor allem auf einem Informationsvorsprung und der

---

681 *Luckhardt*, Pretty Good Privacy – Teil 3, **c't** 16/1999, S. 172.
682 *Luckhardt*, Pretty Good Privacy – Teil 3, **c't** 16/1999, S. 173.
683 Etwa 80% davon waren bereits die neueren DSS/DH-Schlüssel, *Luckhardt*, Pretty Good Privacy – Teil 2, **c't** 13/1999, S. 210.
684 **c't** 18/1999, S. 20.
685 *Schulzki-Haddouti*, Grünes Licht für Kryptographie, **c't** 13/1999, S. 46.
686 **c't** 17/1999, S. 42.

Möglichkeit basiere, die Kommunikation des Feindes zu entschlüsseln.[687] Mittlerweile haben die USA ihre Exportbeschränkungen drastisch gelockert, nachdem sich die Industrieverbände (u.a. die *BSA*) über einen Wettbewerbsnachteil gegenüber den Softwareherstellern aus anderen Länden beschwert hatten.[688] Gemäß einem neuen Gesetzeszusatz dürfen US-amerikanische Softwarehersteller ihre Kryptographie-Programme nun auch an Endkunden oder Unternehmen außerhalb der USA verkaufen, ohne eine Lizenz beantragen zu müssen.[689]

Großbritannien verfolgt einen ähnlichen Kurs wie die USA. Gemäß einem Gesetzentwurf der britischen Regierung zum elektronischen Handel sollen Benutzer von Verschlüsselungssoftware gezwungen werden, auf Anforderung der Polizei Passwörter, geheime Schlüssel oder entschlüsselte Daten zu übergeben. Bei einer Weigerung soll eine bis zu zwei Jahre dauernde Haftstrafe drohen. Auch Provider sollen bestraft werden, wenn sie Betroffenen mitteilen, dass eine sogenannte Entschlüsselungsverfügung verhängt wurde.[690]

In Deutschland wird derzeit eine deutlich liberalere Kryptographie-Politik verfolgt. *Joachim Jacob*, der frühere Bundesbeauftragte für den Datenschutz, ließ bereits mehrfach verlauten, dass jeder das Recht haben solle, seine Kommunikation zu verschlüsseln.[691] Die Anwender müssten sich vor allem gegen illegales Ausspähen, Manipulieren oder Zerstören von Daten wehren können. Das Kabinett spricht in diesem Zusammenhang von jährlichen Schäden in Milliardenhöhe, weshalb die Regierung bestrebt sei, die „bisher geringe Sensibilisierung der Nutzer" zu verbessern.[692] Bereits im November 1998 haben 5 Landesbeauftragte für den Datenschutz 10 Punkte für einen Politikwechsel zum wirksameren Schutz der Privatsphäre vorgestellt. Unter anderem forderten sie hierin ein Grundrecht auf Datenschutz. Zudem solle die staatliche Politik wirksame Verschlüsselungsverfahren fördern und Überlegungen zu Kryptographiebeschränkungen einstellen.[693]

Selbst wenn in der Zukunft restriktivere Kryptographie-Regulierungen getroffen werden sollten, kann man davon ausgehen, dass auch diese Maßnahmen von den meisten Tätern umgangen werden können. Zum einen ist es leicht möglich, verschlüsselte Dateien durch schlichtes Umbenennen mit unverdächtigen Dateinamen zu versehen, zum anderen ist das Verpacken mit einem Archivierungsprogramm ebenso leicht zu realisieren. Als E-Mail-Attachment versendet, erregen diese Dateien nicht den geringsten Verdacht.

Ein anderer Trend lautet „Verstecken statt Verschlüsseln". Bei der sogenannten Steganographie (aus dem Griechischen für „verdecktes Schreiben") werden Daten unsichtbar in Dateien mit unverfänglichem Inhalt versteckt. In einer Trägerdatei (in der Regel eine Bild- oder Audiodatei) werden durch Veränderungen des niederwertigsten Bits eines Datenbytes die geheimen Informationen abgelegt (Least Significant Bit Methode)[694]. Diese Daten sind im Gegensatz zu herkömmlich

---

[687] **c't** 17/1999, S. 42.
[688] Vgl. **Wired News** vom 13.01.2000, http://www.wired.com/news/business/0,1367,33625,00.html.
[689] *Bleich*, Schlüsselfreigabe, **c't** 3/2000, S. 41.
[690] **Heise Online News** vom 13.07.1999, http://www.heise.de/newsticker/meldung/5425.
[691] Vgl. das Interview bei *Schulzki-Haddouti*, Das Prinzip Anonymität, **c't** 9/1999, S. 46.
[692] *Schulzki-Haddouti*, Grünes Licht für Kryptographie, **c't** 13/1999, S. 46.
[693] Vgl. **c't** 24/1998, S. 55.
[694] *Berger-Zehnpfund*, **Kriminalistik** 1996, 639; *Blümel/Soldo*, S. 158.

verschlüsselten Dateien nicht sofort als solche zu erkennen, weshalb Steganographie als eine sehr effektive Methode geheimer Kommunikation anzusehen ist.

In der Warez-Szene kommt Kryptographie hauptsächlich im Bereich der Kommunikation zum Einsatz. Es ist zwar schon vorgekommen, dass *PGP*-verschlüsselte Raubkopie-Dateien im UseNet angeboten wurden, allerdings wird diese äußerst ungewöhnliche Art der Distribution nicht eingesetzt, um potentiellen Strafverfolgern die Arbeit zu erschweren, sondern in erster Linie als „Anti-Lamer-Technoloie": Nur befreundete und anerkannte User, die auf einer geheimen Mailing-Liste stehen, bekommen die Public Keys per E-Mail zugesandt, mit denen sie die Software entschlüsseln können.[695]

Bei der Kryptographie-Debatte darf nicht übersehen werden, dass Verschlüsselung auch zusätzliche Verbrechensbekämpfungsmöglichkeiten bietet.[696] Dies gilt vor allem für den Bereich der Betrugsdelikte, die durch verschlüsselungsbasierte Verfahren wie die digitale Signatur deutlich erschwert bzw. verhindert werden können: Durch kryptographische Verfahren kann sowohl der Absender identifiziert als auch erkannt werden, ob an einer Nachricht manipuliert wurde. Hierzu signiert der Anwender das Dokument (genauer: eine kryptographische Prüfsumme) mit seinem geheimen Schlüssel. Dazu ist ausschließlich er in der Lage. Mit Hilfe seines öffentlichen Schlüssels kann jeder diese Signatur dekodieren und das Ergebnis mit einer neugenerierten Prüfsumme des erhaltenen Dokuments vergleichen.[697] Verschlüsselung gilt derzeit als die einzige Möglichkeit sicherer Authentifizierung im Internet. Zur Verhinderung von Wirtschaftsspionage gilt Kryptographie ebenfalls als effektives Mittel.

Zusammenfassend lässt sich festhalten, dass Kryptographieverbote de facto nur schwer durchsetzbar sind. Wenn Kriminelle verschlüsselt kommunizieren möchten, wird ihnen dies auf dem einen oder anderen Weg gelingen. Modelle, die den Nutzer von Kryptographiesoftware unter Strafandrohung dazu bewegen sollen, ihre Schlüssel im Verdachtsfall herauszugeben, verstoßen gegen elementare verfassungsmäßig garantierte Verfahrensgrundrechte. Niemand soll sich selbst belasten müssen.[698] Auch im englischen Rechtssystem ist es äußerst ungewöhnlich, dass unter Verdacht stehende Personen ihre Unschuld beweisen müssen, weshalb Abgeordnete aller Parteien sowie Industrie und Bürgerrechtler scharfe Opposition gegen den oben erwähnten Gesetzentwurf angekündigt haben.[699]

Kritiker in Deutschland befürchten zudem eine Aushöhlung des Grundrechts auf Post-, Brief- und Fernmeldegeheimnis nach Art. 10 Abs. 1 GG. Ebenso komme ein möglicher Eingriff in die Menschenwürde (Art. 1 Abs. 1 GG) in Betracht. Ein Kryptographieverbot käme einem Geheimnisverbot gleich, es wäre dann nicht mehr möglich, Tagebucheinträge oder intimste niedergeschriebene

---

695 *McCandless*, **Wired Magazine** 5.04 – April 1997.
696 Vgl. *Vassilaki*, Multimediale Kriminalität, **CR** 1997, S. 301.
697 *Luckhardt*, Pretty Good Privacy – Teil 1, **c't** 12/1999, S. 212.
698 So das Nemo-tenetur-Prinzip („nemo tenetur se ipsum accusare"). Das mit Verfassungsrang ausgestattete Recht hat z.B. in § 55 Abs. 1 StPO gesetzliche Auskleidung gefunden.
699 **Heise Online News** vom 13.07.1999, http://www.heise.de/newsticker/meldung/5425.

Gedanken vor fremdem Zugriff zu schützen. Sicher betroffen sei die allgemeine Handlungsfreiheit nach Art. 2 Abs. 1 GG.[700]

In erster Linie behindert „großflächige" Verschlüsselung geheimdienstliche Lauschvorhaben wie *ECHELON*. Die Arbeit der Strafverfolger scheint bislang nur wenig von Kryptographie beeinträchtigt worden zu sein. Hinzu kommt, dass bei einer Hausdurchsuchung bei einem Verdächtigen immer auch unverschlüsseltes Beweismaterial zu finden sein wird.

9. Weitere Maßnahmen

a) Softwarefilter oder Rating Systeme beim Anwender

Als Alternative zu den gesetzlichen Forderungen nach der Ausfilterung rechtswidriger Webinhalte werden verstärkt Maßnahmen diskutiert, die unter dem Begriff der freiwilligen Selbstkontrolle der Nutzer zusammengefasst werden können. Die Maßnahmen fokussieren sich in erster Linie auf die Reinhaltung des WWW. Hierbei gibt es grundsätzlich zwei Ansätze: Softwarefilter und Rating-Systeme. Beide setzen voraus, dass der Anwender eine Software auf seinem Rechner installiert bzw. aktiviert, welche fortan kontrolliert, was er aufrufen bzw. sehen kann.

(1) Softwarefilter

Hersteller von Softwarefiltern (z.B. *Net Nanny*[701], *Cybersitter*[702], *SurfControl*[703], *Cyberpatrol*[704] oder *WebWasher*[705]) vertreiben kommerzielle Programme, die in der Regel über eine kontextsensitive Filterung (Begriffsfilterung) verhindern sollen, dass rechtswidrige Inhalte auf den Bildschirm des Anwenders gelangen. Die Sperrung unerwünschter Seiten wird je nach Programm entweder über eine Echtzeit-Begriffsfilterung oder über den Abgleich aufgerufener URLs mit sogenannten schwarzen Listen erreicht. Diese Listen, die regelmäßig aktualisiert werden, kann der registrierte Nutzer beim Hersteller herunterladen. Einzelne Programme sind in der Lage, nicht nur eine Echtzeit-Begriffsfilterung von Webseiten (inklusive HTML-Code) vorzunehmen, sondern auch IRC-Chaträume, Newsgroups, FTP-Verbindungen und E-Mails zu überwachen. Die Begriffe, nach denen Inhalte ausgefiltert werden, können entweder vom Anwender selbst bestimmt werden, oder er wählt ein vorgefertigtes Begriffspaket aus.

Obwohl Softwarefilter in erster Linie zum Schutz von Kindern und Jugendlichen entwickelt wurden, können sie auch eingesetzt werden, um Verstößen gegen Urheberrechte vorzubeugen. So kann der Anwender neben Begriffen wie „Porn" oder „Sex" auch „Warez" oder „Crackz" auswählen. Vor allem für Unternehmen und öffentliche Einrichtungen, in denen die Angestellten Zugang zum Internet haben, bieten sich entsprechende Lösungen an. Allerdings liefern Softwarefilter häufig unbefriedigende Ergebnisse: Das Programm *Cybersitter* zensierte beispielsweise die Homepage einer Frau namens *Cindy Title Moore*, da es in ihrem Namen das Wort „tit" (ugs. (engl.) = weibliche Brust)

---

[700] *A. Koch*, Grundrecht auf Verschlüsselung?, **CR** 1997, S. 106 ff.
[701] http://www.netnanny.com.
[702] http://www.cybersitter.com.
[703] http://www.surfcontrol.com.
[704] http://www.cyberpatrol.com – *CyberPatrol* gehört mittlerweile zu *SurfControl*.
[705] http://www.webwasher.com.

erkannte.[706] Eingestellt auf feste Begriffe, die es auszufiltern gilt, werden dem Anwender auch regelmäßig solche Seiten vorenthalten, die sich mit der Aufklärung über strafrechtlich relevante Themen befassen. Zu nennen wären in diesem Zusammenhang die Seiten der großen Anti-Piracy-Organisationen oder „www.kinderporno.de", auf der Aufklärungsarbeit zum Thema geleistet wird. Ebenso sind Webseiten zur AIDS-Aufklärung betroffen, sofern auf ihnen detailliert sexuelle Praktiken beschrieben werden, die zur Übertragung des Virus beitragen können.[707] Für diese Fälle sollen sogenannte weiße Listen Abhilfe schaffen, in denen unbedenkliche Seiten notiert sind, die jedoch schwierig zu beurteilende Inhalte enthalten. Angesichts des unüberschaubaren Web-Angebots scheint es allerdings kaum durchführbar, alle betroffenen Seiten zu katalogisieren.

Leider liefern die meisten Programme äußerst unbefriedigende Ergebnisse, und ihre Sicherheitsvorkehrungen lassen sich verhältnismäßig einfach umgehen. Im Netz gibt es zahlreiche Seiten, auf denen detaillierte Informationen zur Umgehung sämtlicher Softwarefilter abgerufen werden können.[708] Vor allem die Schwächen der maschinellen Begriffsfilterung haben dazu geführt, dass verstärkt Modelle diskutiert werden, denen eine individuelle Inhaltsbewertung durch natürliche Personen zugrunde liegt. Hierzu gehören in erster Linie die sogenannten Rating-Systeme.

(2) Rating-Systeme

Bei Rating-Systemen handelt es sich ebenfalls um Filtermechanismen, die allerdings nicht auf einer reinen Begriffsfilterung basieren, sondern auf Selbsteinschätzungen der Content Provider. Die Betreiber der Webseiten sollen eine Bewertung der von Ihnen vermittelten Inhalte vornehmen und das Ergebnis an eine Organisation übermitteln, die die Seiten mitsamt Bewertungen katalogisiert. Schließlich werden die Angebote auf einer zuvor festgelegten Skala eingestuft. Möchte ein Anwender keine Gewaltdarstellungen sehen, entscheidet er sich für den entsprechenden Wert auf der Skala und aktiviert das Filterprogramm auf seinem Rechner. Von nun an werden ihm nur noch Webseiten angezeigt, die den gewünschten Bewertungskriterien entsprechen und die bei der Rating-Organisation registriert sind. Unregistrierte Webseiten werden komplett ausgeblendet. Entscheidet sich der Anwender für den höchsten Wert auf der Skala, können auch explizit pornographische Webseiten abgerufen werden.[709]

Als Rating-Organisationen kommen neben kommerziellen Anbietern auch Vereine, Gewerkschaften, Kirchen und andere gesellschaftliche Gruppen in Betracht. Diese könnten je nach Weltanschauung und Zielen eigene Bewertungssysteme (Schablonen) entwickeln, die sich der Anwender auf dem eigenen Rechner installieren kann, um unerwünschte Inhalte aus dem Internet auszufiltern.[710]

Derzeit kann der Internetsurfer noch selbst bestimmen, ob er ein Rating-System in Anspruch nehmen möchte oder nicht. Die Betreiber populärer Suchmaschinen wie *Lycos* oder *Yahoo* haben jedoch angekündigt, in der Zukunft möglicherweise nur noch solche Angebote in ihre Indizes aufzunehmen, die nach den Vorgaben des Rating-Systems *PICS (Platform for Internet Content Selection)*[711]

---

[706] *Sieber*, Kontrollmöglichkeiten – Teil 2, **CR** 1997, S. 657; weitere Beispiele für missglückte Begriffsfilterung finden sich in den **Wired News** vom 21.09.200, http://www.wired.com/news/culture/0,1284,38910,00.html und bei *Janssen*, S. 31 f.
[707] Vgl. *Pitscheneder*, Ethik-TÜV im Netz, **FOCUS** 39/1999, S. 228.
[708] Vgl. den Praxistest von *Brauch*, Schutz vor Schmutz?, **c't** 23/2000, S. 230 ff.
[709] Vgl. *Gruhler*, **Telepolis** vom 07.05.1998.
[710] Vgl. *Pitscheneder*, Ethik-TÜV im Netz, **FOCUS** 39/1999, S. 230.
[711] http://www.w3.org/pics.

registriert sind.[712] Wer also weiterhin seine Webseite in den großen Indizes gelistet haben möchte, müsste eine Bewertung seiner Seite vornehmen. Das Internet-Content-Rating würde somit eine völlig neue Dimension erreichen.

PICS ist das zur Zeit am weitesten verbreitete Rating-System. Es wurde 1996 unter der Schirmherrschaft des *W3C* entwickelt. Die Konzeption von *PICS* ähnelt der Funktionsweise der amerikanischen *V-Chip*-Technologie für TV-Programme: Indem die Programmverantwortlichen jugendgefährdende Sendungen indizieren, können die Eltern deren Ausstrahlung individuell verhindern.[713] Das *PICS*-System kann als eine Art technische Oberfläche angesehen werden, auf der verschiedene Schemata (Schablonen) eingesetzt und den speziellen Bedürfnissen gemäß konfiguriert werden können. Die zur Zeit populärsten Schemata *SafeSurf*[714] und das des *Recreational Software Advisory Council (RSACi)*[715] haben ihren Ursprung in den USA. Der *SafeSurf*-Standard ist die kommerzielle Variante, während der *RSACi*-Standard von einer unabhängigen Nonprofit-Organisation entwickelt wurde, die unter anderem von den Unternehmen *Disney*, *CompuServe*, *IBM, SPA, Dell, AT&T, Microsoft* und anderen Sponsoren aus dem Soft- und Hardwarebereich unterstützt wird.[716]

Nur wenige Anwender wissen, dass sowohl die *PICS*-Oberfläche als auch das *RSACi*-Schema in den meisten gängigen Webbrowsern (z.B. im *Microsoft Internet Explorer* und in *Netscape*) integriert sind. In den USA fördert der Provider *CompuServe* die Implementierung von *PICS* bereits seit 1996. Bei einem Vergleich des *SafeSurf*- mit dem *RSACi*-Schema wird deutlich, dass das *RSACi*-Schema mit seinen sehr engen Bewertungskriterien ursprünglich für Videospiele entwickelt wurde. Der Benutzer hat dort nur die vier Kategorien Gewalt, Nacktheit, Sex und (Fäkal-)Sprache zur Auswahl und kann diese in eine Skala mit fünf verschiedenen Graden einteilen – je nachdem, wie viel Gewalt oder Sex er für verträglich hält.[717]

Die Bewertungen des Betreibers einer bestimmten Webseite werden verborgen im Quelltext, in einem sogenannten Metatag, untergebracht. Wenn der Internetsurfer eine Seite anfordert, verifiziert der Browser, ob die Klassifizierungen der Metatags mit den vom Benutzer gewünschten Kriterien übereinstimmen. Hat er beispielsweise für die Rubrik "Sex" den Wert "0" eingegeben, sperrt der Browser alle Webseiten, die sexuell anstößig sind. Hat der Benutzer einmal seine Bewertungskriterien im Browser festgelegt, können sie bei beiden Schemata nur durch ein Passwort geändert werden.[718] Auf diese Weise ist sichergestellt, dass andere Nutzer desselben Rechners die Einstellungen des Passwortinhabers nicht verändern können.

Zwar können über die vier Kategorien des *RSACi*-Schemas Warez-Webseiten nicht explizit ausgeblendet werden, allerdings darf nicht vergessen werden, dass unregistrierte Seiten aller Art ausgeblendet werden, sobald man das Filtersystem aktiviert hat. Da nicht davon auszugehen ist, dass sich die Betreiber von Warez-Seiten bei einem Rating-Anbieter registrieren lassen, können Rating-

---

712 *Gruhler*, **Telepolis** vom 07.05.1998.
713 *Gruhler*, **Telepolis** vom 07.05.1998.
714 http://www.safesurf.com.
715 Die Organisation existiert in seiner ursprünglichen Form nicht mehr. Sie wurde 1999 Teil der *Internet Content Rating Association (ICRA)*, http://www.icra.org. Das *RSACi*-System wird jedoch weiterhin verwendet; z.B. im aktuellen *Internet Explorer 6*.
716 *Gruhler*, **Telepolis** vom 07.05.1998.
717 *Gruhler*, **Telepolis** vom 07.05.1998.
718 *Gruhler*, **Telepolis** vom 07.05.1998.

Systeme für die Verhinderung von Verstößen gegen die ausschließlichen Verwertungsrechte der Urheber bzw. Rechtsinhaber im WWW eine zunehmende Bedeutung haben. Zu befürchten ist jedoch, dass neben dem neuen, sauberen Internet ein „alternatives" Netz bestehen bleibt, dessen Nutzer auch ohne die großen Suchmaschinen auskommen werden.

Eine Verpflichtung der Nutzer zur Installation bzw. Aktivierung eines Rating-Systems kann im Vertrag mit dem ISP vereinbart werden, allerdings ist zu beachten, dass Rating-Systeme keine absolute Kontrolle versprechen. Aus diesem Grund wird den Betreibern von Suchdiensten eine Schlüsselrolle zukommen. Erst wenn alle großen Suchmaschinen nur noch bewertete Angebote in ihrem Trefferlisten anzeigen, kann von der Etablierung eines globalen Kontrollsystems gesprochen werden.

Zahlreiche Free-Speech-Initiativen sehen in den Bestrebungen der Industrie einen weitreichenden Eingriff in den freien Informationsfluss des Internet.[719] Rating-Kritiker sprechen gar von einer „Zensur durch die Hintertür". Sollten sich die großen Suchdienste tatsächlich auf das Ausgeben registrierter Angebote beschränken, wären Webmaster, die ihre Seiten einer möglichst großen Zahl von Surfern zugänglich machen wollen, gezwungen, die Inhalte schon aus reinem Selbsterhaltungstrieb *PICS*-kompatibel und somit möglichst moralkonform zu gestalten[720]. Der Internet-Experte *Simson Garfinkel* bezeichnet *PICS* sogar als "die effektivste globale Zensurtechnik aller Zeiten". Da die Zensur nicht mehr von der Staatsgewalt ausgehe, erscheine es als natürlicher Vorgang, wenn bestimmte Internetinhalte verschwänden[721]. In der Etablierung von Rating-Systemen liege eine fundamentale Veränderung der Netzarchitektur, die die Unterdrückung der Redefreiheit weitaus besser ermöglicht als nationale Gesetze allein. Jeder könne zum Zensor werden, nicht nur Regierungen sondern auch Internetprovider, Schulen oder Bibliotheken.[722]

Weitere Unstimmigkeiten ergeben sich aufgrund der Funktionsweise des Schemas: Da *PICS* nicht den inhaltlichen Kontext einer Seite erfassen kann, ist es möglich, dass auch unbedenkliche Inhalte gesperrt werden.[723] Durch den Umstand, dass das *RSACi*-Schema keinen Unterschied zwischen Kunst, Literatur und profanen Inhalten zulässt, könnten Online-Romane, -Büchereien, -Kunstmuseen und andere seriöse Quellen leicht als jugendgefährdend klassifiziert werden.[724]

Trotz der dargestellten Bedenken darf man den Jugendschutz im Internet nicht vernachlässigen. Wer sich im Internet auskennt, weiß, wie wichtig es ist, Kinder und Jugendliche von den Abgründen fernzuhalten, die sich am Rand des Netzes auftun. Daher ist die Entwicklung von Kontrollsystemen, die speziell auf den Jugendschutz zugeschnitten sind, unabdingbar. Besonders wichtig ist in diesem Zusammenhang, dass die Einstellungen bzw. Installationen, die der Systemadministrator auf dem Rechner vorgenommen hat, nicht ohne weiteres umgangen werden können. Da es für die meisten

---

719 Hierzu gehören die folgenden Organisationen: *American Civil Liberties Union* (http://www.aclu.org), *Global Internet Liberty Campaign* (http://www.gilc.org/speech/ratings/gilc-munich.html), *Privacy International* (http://www.privacy.org/pi), *Electronic Privacy Information Center* (http://www.epic.org), *Electronic Frontier Foundation* (http://www.eff.org) und *Netfreedom* (http://www.netfreedom.org).
720 *Gruhler*, **Telepolis** vom 07.05.1998.
721 *Garfinkel*, Good Clean PICS, **Hotwired Network** , Mai 1997.
722 Vgl. *Krempl*, Die große Filteroffensive, **Telepolis** vom 10.09.1999.
723 *Gruhler*, **Telepolis** vom 07.05.1998.
724 *Gruhler*, **Telepolis** vom 07.05.1998.

Anwender eher schwierig sein dürfte, selbst entsprechende Vorkehrungen zu treffen, sollten Möglichkeiten geschaffen werden, die es ihnen erleichtern. Statt der komplizierten und verwundbaren Einrichtung von Rating-Software beim Anwender könnten sich familienfreundliche Provider etablieren, die speziell für besorgte und technikunerfahrene Eltern eine Filterung bereits auf dem eigenen Proxy-Server vornehmen.[725] Anbieten würde sich auch eine in den *Microsoft Internet Connection Wizard* integrierte Schritt-für-Schritt-Anleitung zur Aktivierung von sicheren Zugangskontrollsystemen.

Ein bemerkenswerter Ansatz zum Jugendschutz kommt aus den USA. Im März 2002 wurde vom Kongress ein Gesetzentwurf namens .kids Implementation and Efficiency Act genehmigt, demzufolge eine Kinderzone im WWW errichtet werden soll. Unter der Domain .kid sollen nur Seiten online gestellt werden, die weder Pornographie noch gewalttätige Inhalte enthalten. Die Kinderzone startet als Subdomain von .us, da die *ICANN* trotz Druck von amerikanischer Seite die Top-Level-Domain .kid noch nicht auf den Weg gebracht hat. Das Unternehmen *NeuStar*, Verwalter der Domain .us, darf Seiten aus dem „Kindernetz" nehmen und soll sich nicht einmal vor rechtlichen Schritten der Betreiber fürchten müssen. Sofern sich keine grundlegenden Änderungen ergeben, können Internet-Filter bald wirksam alle Seiten außerhalb der Domain .kid.us blockieren.[726]

Da sämtliche Seiten, die mit einem aktivierten Rating-System erreichbar sind, bei der Rating-Organisation angemeldet wurden bzw. ein kompatibles Metatag im Quellcode enthalten, ist damit zu rechnen, dass auch Seiten mit urheberrechtsverletzenden Inhalten ausgeblendet werden. Dies ist insofern von Bedeutung, als gerade Kinder und Jugendliche ein großes Interesse an raubkopierten Computerspielen haben. Es kann zwar nicht verhindert werden, dass ein Content Provider seine rechtswidrigen Inhalte vorsätzlich als unbedenklich deklariert, allerdings kann man diesem Verhalten begegnen, indem vorsätzliche Falschbewertungen rechtlich sanktioniert werden. Dies setzt freilich voraus, dass die schwarzen Schafe auch entdeckt werden. Ein internationales Hotline-System erscheint als praktische Lösung.[727]

Die von den Free-Speech-Initiativen entworfenen, düsteren Zensur-Szenarien sind erst dann möglich, wenn die großen Suchdienste – als Stützpfeiler der Orientierung im WWW – geschlossen mit den Betreibern der Rating-Systeme kooperieren. Auf eine solche Kooperation wird jedoch höchstwahrscheinlich zugunsten derjenigen verzichtet werden, die umfassende Informationen beziehen möchten und ungefilterte Inhalte aufgrund ihres Alters seelisch verkraften können. Selbst wenn man wider Erwarten davon ausgeht, dass Rating-Systeme in Zukunft nicht nur für Kinder und Jugendliche sondern für jedermann von Bedeutung sind, wird man das WWW nicht völlig von Warez-Seiten befreien können. Schnell werden sich alternative Suchmaschinen etablieren, die nach entsprechenden Seiten suchen, und deren Trefferlisten nicht *PICS*- bzw. *RSACi*-kompatibel sein werden. Auch URLs, die unter der Hand ausgetauscht werden, können nicht von der Filterung

---

[725] *Ermert*, Antiautoritäres Filtersystem, **c't** 20/2000, S. 29.
[726] **Heise Online News** vom 08.03.2002, http://www.heise.de/newsticker/meldung/25466.
[727] Siehe den nachfolgenden Gliederungspunkt.

erfasst werden. Die Untergrund-Szene würde somit kaum merklich von den Filtermaßnahmen tangiert. Da jedoch über viele tausend, öffentlich zugängliche Webseiten Raubkopien verbreitet werden, macht es sich sicher bemerkbar, wenn man den Zugang zu diesen durch Rating-Systeme verhindert.

b) Einrichtung von Hotlines

Unter Hotlines sind Einrichtungen zu verstehen, die Hinweise von Nutzern auf problematische Netzinhalte entgegennehmen und bearbeiten. Die Hinweise können in der Regel telefonisch, per Fax oder per E-Mail übermittelt werden. Hotlines sollen sicherstellen, dass neben einer korrekten Bewertung der verdächtigen Inhalte auch wirksame Maßnahmen gegen die Verfügbarkeit der Inhalte ergriffen werden. Hierfür fungieren sie als Kommunikationskanäle zwischen Nutzern, Dienstanbietern, Selbstregulierungsinstitutionen, Organisationen, die Rating- und Filterdienste anbieten, und der Strafverfolgung.[728] Als Ergänzung zu Filtersystemen können Hotlines ebenfalls nützliche Dienste verrichten; beispielsweise um auf problematische Netzinhalte zu reagieren, die durch Filtermechanismen nicht ausgeblendet werden können oder um Falschklassifizierungen zu entdecken. Ein möglichst effektives Hotline-Verfahren sollte die folgenden Schritte umfassen – vorausgesetzt, es gibt keine Vorschriften, die eine direkte Weiterleitung an die Strafverfolgungsbehörden verlangen:[729]

- Der Internetnutzer meldet einen problematischen Inhalt an die Hotline, woraufhin er eine Eingangsbestätigung erhält.

- Die Hotline-Organisation überprüft die Meldung zunächst hinsichtlich formeller Kriterien. Außerdem wird überprüft, ob die Meldung die vom Nutzer angegebenen problematischen Inhalte tatsächlich aufweist.

- Wenn die (formellen) Kriterien erfüllt sind und die Überprüfung erfolgreich abgeschlossen ist, wird ein internes Bewertungsverfahren durchgeführt. Ziel dieses Verfahrens ist es, zu entscheiden, ob weitere Schritte notwendig sind. Aus Transparenzgründen sollten sich Nutzer über das Bewertungsverfahren informieren können.

- Wenn die Bewertung zu der Entscheidung führt, dass keine weiteren Maßnahmen notwendig sind, sollte der Nutzer über das Ergebnis des Verfahrens informiert werden. Falls weitere Maßnahmen beschlossen werden, muss der Provider kontaktiert werden. Hat sich dieser einem Selbstregulierungsverfahren unterworfen, ist es aus verfahrensrechtlichen Gründen notwendig, ihn anzuhören, oder aber er entscheidet sich einfach, die geforderten Schritte zu unternehmen (z.B.: Entfernung der fraglichen Inhalte). Falls zwingende rechtliche Gründe vorliegen, kann eine Weiterleitung an staatliche Behörden erforderlich sein. Solche Anbieter, die sich einem Selbstregulierungsverfahren unterworfen haben und die geforderten Maßnahmen ergreifen, sollten rechtlich privilegiert und von der Haftung

---

[728] So unterhält der Providerverband *eco* eine öffentliche Online-Hotline für Beschwerden rund um „illegale oder bedenkliche“ Inhalte im Internet, http://www.eco.de/servlet/PB/menu/1020201/index.html.

[729] Vgl. zu den nachfolgenden Punkten *Machill/Waltermann,* Memorandum der *Bertelsmann-Stiftung* zur Verantwortlichkeit im Internet.

freigestellt werden. Sofern der Anbieter auf ein Selbstregulierungs-verfahren verzichtet hat, hat die Kontaktaufnahme mit ihm lediglich den Charakter einer Information. Auch hier muss der Vorgang eventuell an die Strafverfolgung weitergeleitet werden, wenn es sich um illegale Inhalte handelt.

- Schließlich sollten das Verfahren dokumentiert und der Nutzer über das Ergebnis informiert werden. Es sollte ein internationales Netzwerk von Hotlines geschaffen werden, deren Zusammenarbeit durch ein Rahmenabkommen geregelt wird. Dieses sollte Mindeststandards für den Umgang mit den problematischen Netzinhalten festlegen und den Austausch von Informationen der Hotlines untereinander regeln. Das Verfahren der internationalen Zusammenarbeit kann dann so funktionieren, dass die Hotline des Landes, in dem der betreffende Inhalt ins Netz gestellt wurde, für dessen Beurteilung zuständig ist und gegebenenfalls dagegen aktiv wird. Diese Vorgehensweise stellt sicher, dass gegen Anbieter von Internetinhalten dann vorgegangen wird, wenn das Material im Herkunftsland illegal ist.

Hotlines sind unbestritten ein notwendiges Werkzeug zur Bekämpfung der Kriminalität im Internet. Daher gilt es, zunächst ein koordiniertes Netzwerk nationaler Hotlines zu schaffen, welche die in ihrem Territorium ansässigen Service-Provider informieren, wenn rechtswidrige Inhalte auf deren Servern festgestellt wurden.[730] Zur Etablierung anerkannter Hotlines ist es wichtig, dass diese eine breite gesellschaftliche Akzeptanz erfahren. Aufgabe des Gesetzgebers ist es hierbei, Verfahrensregeln zu schaffen, die die grundlegenden Werte des materiellen Rechts, des Verfahrensrechts sowie des Datenschutzes und der freien Meinungsäußerung respektieren.

IV. Betrachtung der Maßnahmen, über deren Einsatz spekuliert wird

Die nachfolgend beschriebenen Maßnahmen finden im Regelfall für die Bekämpfung der Raubkopiererszene keine gesetzliche Grundlage, weshalb sie in einem Rechtsstaat nicht als legitime Mittel in Frage kommen. Allerdings wird ihre Existenz in der Internetgemeinde und besonders innerhalb der Warez-Szene stark diskutiert. Obwohl die verdächtigten Organisationen und Unternehmen stets dementieren, dass sie zu den umstrittenen Maßnahmen greifen, gibt es zahlreiche Anhaltspunkte dafür, dass von einigen zumindest Informationen über die Verbreitung von Raubkopien gesammelt werden.[731]

1. Datenausspähung über Applets bzw. Controls in Webbrowsern

Um den Besuchern von Webseiten möglichst umfassende Interaktionsmöglichkeiten zu bieten, haben die Softwareentwickler sogenannte Applets bzw. Controls entwickelt. Hierbei handelt es sich um kleine Programme, die beim Besuch der entsprechenden Seite zumeist unbemerkt auf den heimischen Rechner geladen und dort gestartet werden. Auf diese Weise wird dem fremden Server

---

[730] *Sieber*, Kriminalitätsbekämpfung, Editorial **MMR** 7/1998.

[731] Für die Bekämpfung von schwerwiegenden Verbrechen sind die untersuchten Maßnahmen von besonderer Bedeutung, da hier die rechtlichen Voraussetzungen günstiger sind.

eine gewisse Kontrollmöglichkeit über den Rechner des Surfers eingeräumt, und es können aufwändige Präsentationen realisiert werden, indem auf die Ressourcen des heimischen Rechners zugegriffen wird. Bis heute haben sich drei Systeme als „Controlpaneele" durchgesetzt: *ActiveX* Controls von *Microsoft*, *JAVA* von *Sun Microsystems* und *JavaScript* Plug-Ins und Cookies[732] von *Netscape*[733]. *ActiveX* ist nur als Erweiterung für die Betriebssysteme von *Microsoft* gedacht, wohingegen *JavaScript* und *JAVA* als Erweiterung für das WWW-Angebot aller internetfähigen Plattformen entwickelt wurden.[734] Zwar können alle Applets oder Controls in den Sicherheitseinstellungen der gängigen Browser deaktiviert werden, allerdings muss der Surfer dann auf die (Audio-)Visualisierung zahlreicher Webseiten verzichten.[735]

Applets können auch im Hintergrund einer bestehenden Verbindung Daten vom Privatrechner unbemerkt zum fremden Server übertragen. Dies ist beispielsweise immer dann der Fall, wenn sich der Nutzer für ein Online-Update eines der bei ihm installierten Programme entscheidet. Hierbei werden zunächst Teile des lokalen Systems analysiert („Scannen" der Verzeichnisstruktur und der Registry[736]), um festzustellen, welche Dateien aktualisiert werden müssen. Anschließend werden die neuen Programmbestandteile automatisch auf den Privatrechner geladen, wo sie sich selbst installieren. Bei der Analyse des Systems kann selbstverständlich auch festgestellt werden, ob sich Raubkopien auf dem Rechner befinden.

2. Datenausspähung bei der *Windows*-Registrierung

Bei der Online-Registrierung des *Microsoft*-Betriebssystems *Windows 98* wurden individuelle Nutzerdaten an Microsoft übertragen, ohne dass die Kunden davon in Kenntnis gesetzt wurden. Die Registrierung einer Software ist ein freiwilliger Vorgang und bringt dem *Microsoft*-Kunden unter anderem Vorteile wie Zugang zu exklusiven Bereichen der *Microsoft*-Webseite und zum Software-Service, Produktinformationen per E-Mail sowie günstige Upgrade- und Erweiterungsangebote. Der sogenannte Registration Wizard (der Assistent zur Online-Registrierung) von *Windows 98* kommuniziert beim Registrierungsvorgang mit einem speziellen Server bei *Microsoft* – vergleichbar mit einem Browser, der mit einem Webserver kommuniziert.

In einer Log-Datei des Registration Wizards fand *Richard M. Smith* – Präsident des Softwareherstellers *Phar Lap* – die MAC-Adresse[737] seiner Netzwerkkarte. Der Experte stellte fest, dass die Nummer bei der Online-Registrierung aus der Registry ausgelesen und in Form eines Cookies an *Microsoft* übertragen wurde.[738] Dies geschah selbst dann, wenn der Benutzer explizit abgelehnt hatte, dass Daten über seine Hardware versendet werden.[739]

Smith beobachtete außerdem, dass seine Word- und Excel-Dokumente, die er auf *Windows 98* erstellt hatte, ebenfalls den „versteckten Fingerabdruck" enthielten. Später wurden MAC-Adressen auch in

---

[732] Siehe Fn. 591.
[733] *Blümel/Soldo*, S. 142 f.
[734] *Blümel/Soldo*, S. 145 f.
[735] Vgl. *Kossel*, **c't** 3/1999, S. 144 f.
[736] Siehe Fn. 561.
[737] Siehe Fn. 554.
[738] Vgl. **Wired News** vom 12.03.1999, http://www.wired.com/news/technology/0,1282,18405,00.html. Zum Begriff des Cookies siehe Fn. 591.
[739] *Siering*, Kaufen verbindet, **c't** 9/2001, S. 130-135.

Dokumenten gefunden, die mit *Office 97* auf *Windows 95* oder *NT* sowie Beta-Versionen von *Windows 2000* erstellt wurden. Vereinzelt fand sich die Kennung sogar in E-Mails, die mit *Microsofts Outlook Express* versendet wurden. Durch den Vergleich mit anderen Dateien, deren Herkunft bekannt ist, ließe sich etwa der Autor eines *Word*-Dokuments selbst dann ermitteln, wenn er dies nicht wünscht, und obwohl er die entsprechenden Angaben in den Datei-Eigenschaften gelöscht hat. Auch ließe sich so feststellen, welcher registrierte *Windows 98*-Anwender mit nicht registrierten *Microsoft*-Anwendungen arbeitet. *Smith* äußerte die Vermutung, dass *Microsoft* auf diesem Wege heimlich ein Verfahren zum Aufspüren von Raubkopierern vorbereiten wollte. Die Redmonder wiesen den Verdacht allerdings zurück und sprachen zunächst von einem „unbeabsichtigten Fehler im Software-Design“[740]. Später ließ die Geschäftsführung verlauten, dass man die IDs (bzw. GUIDs[741]) lediglich dazu verwendet habe, um die Produktregistrierungs-Datenbank zu organisieren bzw. die Orientierung in dieser zu erleichtern.[742]

Im Streit um die Datenausspähung bei der *Windows*-Registrierung verlangte die Regierung von Oberbayern als Datenschutzaufsichtsbehörde eine Stellungnahme von *Microsoft Deutschland*. Der Softwarehersteller erklärte die Sammlung der Nutzerdaten mit einem Programmierfehler und versprach, künftig den Empfang zu unterbinden und alle Kennungen zu löschen, die ohne Einverständnis gesammelt wurden.[743] Der bayrische Regierungsdirektor *Johann Steiner* hielt die Stellungnahme aus datenschutzrechtlicher Sicht für schlüssig und erklärte, dass sie den Bedenken Rechnung trage.[744] Die Behauptung *Microsofts,* die Nummern in den *Office*-Dokumenten seien unabhängig von den ID-Nummern, die bei der Registrierung übertragen werden, hat sich jedoch als falsch herausgestellt, da beide Kennungen die MAC-Adressen der Nutzer enthalten. Da die MAC-Adresse mittelbar auch den Inhaber der Netzwerkkarte identifiziert, hätte *Microsoft* den Anwender aus datenschutzrechtlichen Gründen vor dem Übertragen und Speichern informieren müssen[745]. Denn nach geltendem Recht ist die Übertragung von (Registrierungs-)Daten aus einem europäischen Land in Länder mit minderen Datenschutzvorschriften unzulässig, wozu unter anderem die USA gehören[746]: Versicherungen, Handel und Werbung sind nicht durch gesetzliche Datenschutzbestimmungen eingeschränkt. Im Gegensatz zur EU ist der Handel mit Kundenprofilen, Einkaufsgewohnheiten, Adressen etc. („Datamining“) auch ohne Erlaubnis der Kunden möglich. US-Unternehmen zahlen Milliarden für Verbraucherdaten, um gezieltes Marketing betreiben zu können.[747] Der geringe Datenschutzstandard in den Vereinigten Staaten basiert auf Selbstkontroll-Richtlinien der Industrie, die mangels einer übergeordneten Kontrolleinrichtung nicht konsequent angewendet werden.[748] US-Unternehmen sollen sich jedoch durch die Selbstverpflichtung auf neue Datenschutzkonzepte als „sichere Häfen“ für die Übermittlung aus EU-Staaten qualifizieren können. Die Unternehmen erklären dann beispielsweise, keine personenbezogenen Daten ohne die Einwilligung des Betroffenen zu sammeln oder zu verarbeiten. Strittig war bislang, wie die

---

740 *Persson/Siering*, **c't** 6/1999, S. 16.
741 Globally Unique Identifiers.
742 **Wired News** vom 12.03.1999, http://www.wired.com/news/technology/0,1282,18423,00.html.
743 **c't** 11/1999, S. 16.
744 **c't** 11/1999, S. 16.
745 Vgl. *Persson/Siering*, **c't** 6/1999, S. 16.
746 Vgl. *Schulzki-Haddouti*, Sichere Häfen, **c't** 4/1999, S. 42.
747 *Schulzki-Haddouti*, Sichere Häfen, **c't** 4/1999, S. 42.
748 Vgl. **c't** 7/1999, S. 58.

Kontrollen solcher Konzepte auszusehen hätten und wie Verstöße sanktioniert würden. Als Überwachungsinstanz war zwischenzeitlich die *Federal Trade Commission (FTC)* im Gespräch[749].

An der liberalen Situation hat auch das EU/US-Abkommen[750] vom Anfang des Jahres 2000 zum Thema Datenschutz nichts geändert. US-Unternehmen müssen sich danach nur freiwillig verpflichten, „sichere Häfen" (Safe Harbours) zu schaffen, also bestimmte Datenschutzregeln zu beachten, um Daten von EU-Bürgern verarbeiten zu dürfen. Die Verhaltenskodizes können von privaten Organisationen wie *TRUSTe*[751] oder *BBBOnline*[752] aufgestellt werden. Die *FTC* kann zwar wegen Betrugs einschreiten, wenn die Unternehmen die selbst gesetzten Datenschutzregeln missachten, doch sie ist nicht verpflichtet, den Klagen von einzelnen betroffenen Personen nachzugehen.

Dass *Microsoft* ausgerechnet seine registrierten Kunden ausspionieren soll, sorgte für besonderen Unmut in der Internet-Gemeinde. Der Protest zahlreicher Käufer bewirkte, dass bei der Online-Registrierung der zweiten Ausgabe von *Windows 98* (*Windows 98 SE*) die fragliche GUID nicht mehr übertragen wird. Der Kunde erhält allerdings weiterhin von *Microsoft* eine eindeutige ID bei der Registrierung, die nur von *Microsoft* selbst verwendet werden kann. Diese ID vergibt der *Microsoft*-Web-Server ebenfalls mit einem Cookie. Durch Umbenennen oder Löschen des Cookies kann der Nutzer jedoch vermeiden, dass sein Besuch auf den *Microsoft*-Webseiten bemerkt bzw. verfolgt wird.[753]

Um das neue *Microsoft*-Betriebssystem *Windows XP* ranken sich ebenfalls zahlreiche Gerüchte, wonach es seine Nutzer ausspionieren und unerlaubt aufs Internet zugreifen würde. In der Tat nutzt das Betriebssystem die Internetverbindung des Anwenders rege, um gewisse Serviceleistungen zu erbringen (Stellen der Uhr, *Windows*-Update, Versenden von Fehlerberichten etc.), allerdings konnte bislang noch nicht nachgewiesen werden, dass *Microsoft* diesmal gegen geltende Datenschutzbestimmungen verstößt. Die Gerüchte mögen sich nicht nur wegen der Vorkommnisse bei der *Windows-98*-Registrierung hartnäckig halten, auch missfällt vielen Kritikern, dass *Microsoft* zum Übertragen der Informationen bzw. für die Kontaktaufnahme proprietäre Protokolle nutzt und nicht detailliert über die Mechanismen aufklärt.[754]

Erkennbar ist, dass einige Softwarehersteller Möglichkeiten der Manipulation und Datenausspähung schaffen, die vom Benutzer nicht mehr ohne weiteres kontrolliert werden können – es sei dahingestellt, ob dies gewollt oder ungewollt geschieht.[755]

---

[749] **Heise Online News** vom 16.03.2000, http://www.heise.de/newsticker/meldung/8603.
[750] Vgl. die Informationsseite der EU-Kommission, http://europa.eu.int/comm/internal_market/privacy/index_en.htm.
[751] http://www.truste.com.
[752] http://www.bbbonline.com.
[753] Vgl. *Heib*, **c't** 15/1999, S. 88.
[754] Vgl. *Siering*, XPionage – *Windows XP* nährt Schnüffelvorwürfe, **c't** 2/2002, S. 48.
[755] *Blümel/Soldo*, S. 155.

3. Datenausspähung über Abstrahlungen von Computerhardware

Computer sind nicht nur Rechenmaschinen sondern auch kleine Sender. Sie verarbeiten Informationen als Spannungsimpulse, von denen mehrere Millionen pro Sekunde durch die Schaltungen rasen. Dabei werden elektromagnetische Wellen hoher Frequenz nach außen abgestrahlt. 1985 hat der niederländische Ingenieur *Wim van Eck* herausgefunden, dass man das Bild, das ein PC-Benutzer auf seinem (Röhren-)Monitor sieht, mit einem umgebauten Fernsehgerät empfangen kann.[756] Verantwortlich hierfür ist die Bildschirmelektronik. Sie erzeugt kräftige Hochspannungsimpulse, um den Monitor Bildpunkt für Bildpunkt mit Inhalt zu füllen. So kann man noch im Abstand von ca. 100 Metern die Abstrahlungen in lesbare Bilder verwandeln.

Militärs kennen die Methode schon lange, sie verlangen daher für sensible Aufgaben den Einsatz von speziell abgeschirmten TEMPEST-Rechnern („Temporary Emanation and Spurious Transmission" oder in Bezug auf militärischen Emissionsschutz „Transient ElectroMagnetic Pulse Emanations Standard")[757], die hermetisch gegen vagabundierende Strahlung abgedichtet sind. Günstigeren Schutz vor Peilsendern verspricht ein Gerät des Erfinders *Hans-Georg Wolf*. Das *secu-Dat DataSafety-Device* macht die kompromittierenden Emissionen unbrauchbar, indem es die Bitstrukturen verfälscht, die von Tastatur, Monitor und Grafikkarte abgestrahlt werden. Statt auf die üblichen TEMPEST-Schutzschilder auszuweichen, entwickelte *Wolf* bereits während seiner Tätigkeit für das DDR-Außenministerium einen kleinen Störsender, der die Originalstrahlen von *Robotron*-Rechnern mit zufallsgesteuerten Störsignalen überlagerte und so potentielle Lauscher an der Überwachung hinderte[758].

Mittlerweile gibt es sogar Programme, die einen Computer unbemerkt Daten emittieren lassen, ohne dass diese auf dem Bildschirm für den Besitzer sichtbar sind. Ein verstecktes sogenanntes Spread-Spectrum-Dither-Muster benötigt so wenig Platz auf dem Bildschirm, dass es sich auch in kommerzieller Software einsetzen ließe, um ständig die Lizenznummer plus einer rechnerspezifischen Kennung abzustrahlen. Damit könnte man von außerhalb eines Gebäudes mit einem Peiltrupp feststellen, ob nichtlizenzierte Software eingesetzt wird oder ob anderweitige Lizenzverstöße vorliegen.[759] Gerüchten zufolge hatte *Microsoft* bereits Interesse an dieser Technologie bekundet, die Pläne seien jedoch verworfen worden.[760]

4. Eingriffe in die IRC-Kommunikation

Im IRC gibt es Gruppen von meist jugendlichen Nutzern, die sich auf sogenannte Channel-Takeovers spezialisiert haben. Ziel ist die Übernahme der Kontrolle über einen fremden IRC-Channel durch „kriegerische" Mittel. Eine besondere Herausforderung stellen große und vermeintlich gut abgesicherte Channels dar. Erreicht eine Gruppe die Kontrolle über einen solchen Channel, wird dieser in der Regel für die ehemaligen Nutzer gesperrt. Der Zustand wird meist solange aufrechterhalten, bis die Takeover-Gruppen den Spaß an ihrem Kriegsspiel verloren haben.

---

[756] *Kuhn*, **c't** 24/1998, S. 91.
[757] Heute steht der Begriff TEMPEST für verschiedene Maßnahmen zur Verminderung kompromittierender Abstrahlungen bzw. zur Verhinderung unerwünschter Aufklärung der von ihnen transportierten Daten, vgl. *Weisse*, **c't** 3/2000, S. 115 – mit weiteren technischen Detail-Informationen.
[758] *Krempl*, Konzerne im Visier, **c't** 4/1999, S. 182.
[759] *Kuhn*, **c't** 24/1998, S. 97.
[760] Vgl. **DER SPIEGEL** 9/1998, S. 172.

In den großen IRC-Netzen DalNet und EfNet soll es bereits mehrfach vorgekommen sein, dass Anti-Piraterie-Organisationen Takeovers von Warez-Channels veranlasst haben, um die illegale Distribution von Raubkopien zu erschweren.

Um die Herrschaft über einen fremdkontrollierten Channel zu erlangen, müssen zunächst die aktuellen Channel-Operatoren ihren Status verlieren. Dies kann auf verschiedenen Wegen erreicht werden: Die simpelste Methode, einen Channel zu übernehmen, besteht darin, dass ein Mitglied der Takeover-Gruppe von den anderen Operatoren Operator-Status bekommt und alle anderen Operatoren mittels eines speziellen Scripts[761] entmachtet. Dieses sogenannte Massdeopping setzt häufig voraus, dass der „Verräter" ein gewisses Vertrauensverhältnis zu den anderen Operatoren aufbaut, weshalb es von langer Hand geplant werden muss. Deutlich schneller geht es über die „Op-Impersonation". Dabei gibt sich der Angreifer den (Nick-)Namen eines regulären Operators, der sich zur Zeit des Angriffs nicht im IRC-Netz befindet, und fordert im Channel einen anderen Operator auf, ihn zu „oppen". Hat ein Mitglied der feindlichen Gruppe Operator-Status erlangt, kann er gezielt andere Chatter zu Operator-Status verhelfen und unerwünschte Nutzer aus dem Channel verbannen. Um zu verhindern, dass ungebetene Nutzer den Channel betreten, kann der Channelmodus „Invite only" aktiviert werden, woraufhin nur noch solche Nutzer den Channel betreten können, die zuvor eine explizite Einladung erhalten haben.

Schwieriger wird ein Takeover, wenn die Angreifer keinen Operator in den eigenen Reihen haben. Mittels spezieller Programme aus der Crasher- bzw. Hackerszene („Wartools") werden Datenpakete an die IP-Adresse der Operatoren geschickt, um deren TCP/IP-Stack zu irritieren. Da der TCP/IP-Stack von *Windows 98* und *Windows 2000* Schwierigkeiten mit der Verarbeitung einiger seltener Pakettypen – wie z.B. ICMP-Pakete vom Typ 13[762] oder fragmentierte IGMP-Pakete[763] – hat, reagieren die Betriebssysteme mit einem schweren Ausnahmefehler, und das Opfer der Attacke wird vom Internet getrennt. Gelingt eine solche „Nuke-" (einzelne Datenpakete auf festgelegten Ports) oder „Flood-Attacke" (eine Vielzahl von Datenpaketen auf variablen Ports), verlässt der angegriffene Operator zwangsweise den Channel. Auf diese Weise werden die alten Operatoren Stück für Stück entmachtet, und der Channel wird herrenlos. Extremer ist es, wenn die Takeover-Gruppe absichtlich einen kompletten IRC-Server mittels Denial of Service attackiert, damit alle Operatoren auf diesem Server aus dem IRC verschwinden. Die Häufung solcher Attacken hat unter anderem dazu geführt, dass zahlreiche Betreiber von IRC-Servern das Handtuch warfen und den Betrieb ihrer Server einstellten.[764]

Auch über das Ausnutzen von Network Splits („Netsplits") können Dritte die Kontrolle über einen Channel erhalten. Bei einem Netsplit sind verschiedene IRC-Server nicht mehr miteinander

---

761 Einzelne Chat-Programme lassen sich durch Scripts erweitern, wodurch der Nutzer individuelle Anpassungen vornehmen kann oder Zugriff auf zusätzliche Funktionen erhält. Im Laufe der Jahre wurden auch zahlreiche Scripts entwickelt, die speziell auf die „IRC-Kriegsführung" ausgerichtet sind, sogenannte War-Scripts.

762 Das Internet Control Message Protocol ist eigentlich ein Hilfsprotokoll zur Übertragung von Fehler- und Informationsmeldungen, sowie von Timestamps. Das Versenden von ICMP-Nachrichtenpaketen zu Testzwecken wird als Pinging bezeichnet (Ping = Packet Internet Groper).

763 Das Internet Group Management Protocol ist für die Kommunikation zwischen Host-Rechnern und sogenannten Multicast-Routern vorgesehen, vgl. http://www.ietf.org/rfc/rfc1112.txt.

764 Vgl. *Brauch*, Kaputt gespielt, **c't** 11/2000, S. 110 ff. und das Interview mit dem deutschen IRCnet-Koordinator *Paulsen*, bei *Brauch*, „IRC wird irgendwie fortbestehen", **c't** 11/2000, S. 112 f.

verbunden, so dass mehrere unabhängige Channels mit dem gleichen Namen auf den verschiedenen IRC-Servern entstehen. Während des Splits läuft die Kommunikation getrennt weiter, sämtliche Nutzer eines abgesplitteten Servers können sich weiterunterhalten, und nichts von dem, was sie schreiben, wird an die anderen Server übermittelt. Die Ursache für einen Netsplit ist technischer Natur, in der Regel liegt es an einer Überlastung einzelner wichtiger Datenverbindungen.

Befindet sich das Netz im Split, bereitet die Takeover-Gruppe das sogenannte Nick-Colliding vor. Hierbei geben sie ihren Bots oder virtuellen Abbildern von sich („Clones“) die (Nick-)Namen der Operatoren, die entmachtet werden sollen. Dies ist allerdings nur dann möglich, wenn sich die Angreifer auf einem anderen, durch den Netsplit abgetrennten, Server befinden als die Operatoren. Ist die Ursache des Netsplits nach einigen Minuten behoben, erfolgt der sogenannte Rejoin der abgesplitteten IRC-Server. Bei der erneuten Zuordnung der wiedervereinten Nutzer zu den entsprechenden Channels erkennen die Server, dass der gleiche Nutzername mehrfach existiert und trennen automatisch beide Nutzer vom Netz. Gelingt es den Angreifern, sämtliche Operatoren zu „colliden“, befindet sich niemand mehr in der Position, den Channel zu verteidigen.

Takeovers von Warez-Channels lassen sich aufgrund der sehr flexiblen Struktur des IRC nicht wirklich als erfolgversprechende Maßnahmen gegen Online-Softwarepiraterie qualifizieren. Wenige Sekunden nach der Übernahme wird in den meisten Fällen ein „Ausweich-Channel“ von den Mitgliedern des übernommenen Channels gegründet, der entsprechend gut gegen Attacken von außen gesichert ist. Üblicherweise wird an den bisherigen Channelnamen eine „2“ angehängt, so dass sich die vertriebenen Nutzer anstatt in #hyperwarez im neugegründeten Channel #hyperwarez2 versammeln.

Auch die abschreckende Wirkung solcher Aktionen ist fraglich, da die Nutzer nicht unterscheiden können, ob es sich bei den „IRC-Kriegern“ um Takeover-Gruppen oder um Anti-Piraterie-Organisationen handelt.

V. Fazit / Eigener Ansatz

1. Zusammenfassung der effektivsten Maßnahmen

Die Anti-Piraterie-Verbände und die Strafverfolger fokussieren ihre Maßnahmen auf den richtigen Bereich des Internet, das WWW. Freie Downloadangebote, Web-Auktionen und Angebote von Profit-Pirates stellen derzeit das größte Problem für die Software-Industrie dar. Das Unschädlichmachen von Web-Angeboten ist somit als effektivste Maßnahme gegen Internet-Softwarepiraterie anzusehen. Den Kampf gegen die Piraten gewinnt man am ehesten durch den Kampf gegen die Distribution von Raubkopien[765], denn das Herstellen derselben geschieht im beinahe unzugänglichen Untergrund. Dessen Unterwanderung ist angesichts der zahlreichen Besonderheiten der Szene-Struktur nur partiell möglich und kann keine langfristigen Erfolge bringen. Die Kontrolle und

---

765 Vgl. *Ermert*, „Das Kopieren von digitalen Inhalten lässt sich nicht verhindern“, Gespräch mit *Anderson*, **c't** 12/2001, S. 54.

Überwachung der unzugänglicheren Netzbereiche erfordert überdies den Einsatz großer Ressourcen, der in keinem Verhältnis zu den Erfolgen steht.[766]

Auch in Anbetracht der technischen und rechtspolitischen Bedenken bezüglich Sperr- bzw. Filtermaßnahmen wird deutlich, dass wirklicher Erfolg in der Bekämpfung von unerlaubter Verwertung urheberrechtlich geschützter Werke im Internet nur durch konsequentes Vorgehen gegen die Content Provider zu erzielen ist. Besonders wichtig ist in diesem Zusammenhang die Zusammenarbeit mit den Webhosting-Providern und die internationale Zusammenarbeit der Behörden.

Ein reibungsloses Funktionieren der „Notice and Take Down Procedure", wonach Host-Service-Provider im Falle ihrer Benachrichtigung von rechtswidrigen Inhalten die entsprechenden Daten sperren oder löschen müssen, ist unerlässlich.[767] In Verbindung mit international vernetzten Hotlines und Meldestellen kann ein System geschaffen werden, das – unter Einbeziehung der Verbände und Nutzer – weltweit zu einer Beseitigung rechtswidriger Inhalte im Web führen kann[768].

Zugangsanbieter in die Pflicht zu nehmen, ist bereits aus wirtschaftlichen und rechtspolitischen Gründen verfehlt und verkennt die Besonderheiten der Internet-Topologie (Netzstruktur).

Administratoren von Schulen, Universitäten und Unternehmen können ebenfalls dazu beitragen, dass die Distribution von urheberrechtlich geschützten Dateien unterbunden bzw. erschwert wird. Portsperrungen und Transfervolumenbegrenzungen sind einfache und wirkungsvolle Maßnahmen, die ohne nennenswerten wirtschaftlichen Aufwand realisiert werden können.

Auf öffentlichen Web-Terminals empfiehlt sich die Aktivierung von Rating-Systemen, wobei ein hoher Umgehungsschutz gewährleistet sein sollte.

Softwarehersteller können anhand von Online-Authentifizierungsverfahren einen wertvollen Vorsprung vor den Crackern erlangen. Dies gilt insbesondere für Hersteller von Anwendungen, die regelmäßig online genutzt werden. Auch im Application Service Providing liegt ein großes Vorbeugungspotential, da hier die vermieteten Anwendungen permanent online genutzt werden müssen, was ein Kopieren unmöglich macht.

Herkömmliche Kopierschutzsysteme sind erfahrungsgemäß schnell überwunden. Selbst teure Kopierschutzmaßnahmen wie Dongles können nicht vor Online-Piraterie schützen. Etwas anderes gilt nur, wenn Programme mit Hardwarekomponenten verbunden sind, die derart aufwändige Operationen übernehmen, dass sie nicht von einem Emulator ersetzt werden können.

Die Hersteller sollten bei der Wahl der Kopierschutzmaßnahmen außerdem darauf achten, dass die Attraktivität der Originalkopie gegenüber der Raubkopie nicht zusätzlich durch die Maßnahmen

---

766 Vgl. auch die Einschätzung des Datenverarbeitungssachverständigen *Seitz*, bei *Fremerey*, Rauben und Kopieren, **c't** 8/2000, S. 99 f., der die Verfolgung von Softwarepiraten im Internet mit einem „Stochern im Nebel" vergleicht. Allein aufgrund der geringen Erfolgschancen sei es daher naheliegend, die Untergrundszene und gut getarnte Hobby-Kopierer außen vor zu lassen.

767 Vgl. *Sieber*, Die Verantwortlichkeit von Providern im Rechtsvergleich, **ZUM** 1999, S. 198.

768 So im Ergebnis auch *Janssen*, S. 174 f.

geschmälert wird. Ebenso sollte sich das Originalprodukt durch bestimmte Zusatz- und Serviceleistungen von der Raubkopie unterscheiden.

2. Juristische Schlussfolgerungen

Die Strafrechtsnormen des Urheberrechts unterscheiden zwischen privaten und gewerbsmäßigen unerlaubten Verwertungshandlungen. Ein gewerbsmäßiges Handeln i.S.d. § 108a UrhG liegt nur dann vor, wenn der Täter in der Absicht handelt, sich durch die wiederholte Begehung der Tat eine fortlaufende Einnahmequelle von einiger Dauer und einigem Umfang zu verschaffen. Die unerlaubte Verwertung im Rahmen eines Gewerbebetriebs für sich allein genügt noch nicht.[769] Folglich handelt es sich beim Einsatz von raubkopierter Software in Unternehmen oder zu Erwerbszwecken nicht zwangsläufig um eine gewerbsmäßige unerlaubte Verwertungshandlung nach § 108a UrhG. Eine präzise Unterscheidung beider Tatbestände ist wichtig, da der Einsatz von Raubkopien in Gewerbebetrieben und der gewerbsmäßige Handel mit Raubkopien oftmals synonym als „gewerbliche Urheberrechtsverletzungen" bezeichnet werden. Ist im Folgenden von gewerblichen oder gewerbsmäßigen unerlaubten Verwertungshandlungen die Rede, sind damit ausschließlich Taten i.S.d. § 108a UrhG gemeint.

Unerlaubte Verwertungshandlungen mit privatem und gewerbsmäßigem Hintergrund sind in ähnlichem Maße strafbar, die Gesetze sehen Freiheitsstrafen von bis zu drei bzw. fünf Jahren vor. Nach der jetzigen Verfolgungspraxis wird in erster Linie gewerbsmäßiger unerlaubter Verwertung nachgegangen, private unerlaubte Verwertung wird nur in Ausnahmefällen verfolgt; beispielsweise dann, wenn große Unternehmen ihre Netzwerke mit nichtlizenzierten Programmkopien ausstatten. Der Grund für das Abweichen der Verfolgungspraxis von der Rechtslage liegt zum einen darin, dass es sich beim Raubkopieren im privaten Bereich um ein sogenanntes Jedermannsdelikt handelt. Der überwiegende Teil aller Computernutzer – vor allem Kinder und Jugendliche – hat bereits nicht-lizenzierte Software eingesetzt; man könnte in fast jeder Familie fündig werden.[770] Nur selten wird ein entsprechender Strafantrag des Rechtsinhabers gemäß § 109 UrhG vorliegen, des Weiteren sind auch die Strafverfolgungsbehörden nicht daran interessiert, beispielsweise einen Jugendlichen zu kriminalisieren, nur weil auf seinem Rechner raubkopierte Spiele installiert sind. Nicht ohne Grund hat der Gesetzgeber für „gewerbsmäßige Straftaten im Urheberrecht" das Offizialdelikt des § 108a UrhG eingeführt und eine „Notwendigkeit der Lockerung des Antragserfordernisses in § 109 UrhG" für private unerlaubte Verwertungshandlungen gesehen.[771]

Hinzu kommt ein Kapazitätsproblem: Die Ressourcen, die den Strafverfolgern zur Verfügung stehen, reichen nicht annähernd aus, um auch nur einen Bruchteil der angesprochenen unerlaubten Verwertungshandlungen zu entdecken, geschweige denn wirksam zu bekämpfen. Der Einsatz der vorhandenen Kräfte, die für die Bekämpfung der Computerkriminalität eingesetzt werden können,

---

769 Schricker-*Haß*, § 108a UrhG, Rdnr. 2.
770 Vgl. hierzu auch die Ausführungen zur Dunkelfeldforschung, Teil 2, B. II.
771 **BT-Drucks.** 10/3360, S. 21 (Bericht der Abgeordneten *Saurin* und *Stiegler* zum Urheberrechts-Änderungsgesetz 1985, **BT-Drucks.** 10/837). Die Einführung des § 108a UrhG mit der hohen, fünfjährigen Strafdrohung wird dort mit der Notwendigkeit der Bekämpfung des „gewerbsmäßig kriminellen Verhaltens" (Anwachsen der Videopiraterie und des Raubdrucks) begründet. Die Urheberrechtsdelikte der §§ 106 bis 108 UrhG sind mittlerweile als Privatklagedelikte im Katalog des § 374 StPO enthalten, § 374 Abs. 1 Nr. 8 StPO.

fokussiert sich daher auf die gewerbsmäßigen Raubkopierer und auf andere, derzeit als wichtiger angesehene Delikte wie z.B. Kinderpornographie, Terrorismus oder Rechtsextremismus.

Würde mit der juristischen Keule ernst gemacht, wären die Deutschen ein „Volk der Vorbestraften".[772] Diese Überlegung mag auch der Grund dafür sein, dass selbst die großen Anti-Piraterie-Organisationen nicht dazu tendieren, unerlaubte Verwertungshandlungen von Einzelpersonen gerichtlich zu verfolgen.[773] Das primäre Ziel von *Microsoft Deutschland* sind ebenfalls nur diejenigen Raubkopierer, die aus ihrem Handeln einen gewerblichen Nutzen ziehen. Hierunter fasst *Microsoft* zum einen jene Händler, die durch professionellen, illegalen Softwarehandel ihren Umsatz steigern wollen und andererseits Unternehmen, die nur einen Teil ihrer Software lizenziert haben.[774]

Die beschriebene Diskrepanz zwischen Rechtslage und Verfolgungspraxis ruft vor allem aus kriminologischer Sicht Bedenken hervor. Als Konsequenz wird vielfach eine Entkriminalisierung der privaten Softwarekopierer gefordert.[775] Die Vertreter dieser Ansicht bezweifeln, dass das Strafrecht positiv-generalpräventive Wirkungen entfalten kann, wenn eine derart breite gesellschaftliche Akzeptanz einer Straftat vorliege wie bezüglich des unerlaubten Kopierens von Computerprogrammen.[776]

Auch unter dem Gesichtspunkt negativer Generalprävention bestehen Bedenken, ob die Sanktionsdrohung des § 106 UrhG potentielle Rechtsbrecher abzuschrecken vermag. Gemäß einer in der Kriminologie anerkannten Erfahrung kann Repression vorbeugend wirken[777]; allerdings muss gegenüber der Allgemeinheit (bzw. dem Einzelnen) durch eine „griffige Strafverfolgung" deutlich gemacht werden, dass die Rechtsordnung gesellschaftspolitisch gilt und auch durchgesetzt wird[778]. Aus der bloßen Existenz einer Strafnorm kann keine gravierende generalpräventive Wirkung erwachsen. Die Keule des Strafrechts wird daher als unpraktisch und unglaubwürdig angesehen.[779] Der Verzicht auf Ahndung und Strafverfolgung habe zur Folge, dass den Tätern bei der Begehung der Rechtsverletzungen häufig das Unrechtsbewusstsein fehle, und die Rechtsverstöße als Kavaliersdelikte eingestuft würden.[780]

Die Argumente sind insbesondere mit Blick auf Raubkopierer aus dem privaten Bereich nachvollziehbar: Für die Normtreue der Bevölkerung dürfte es nur schwer vermittelbar sein, dass zwar alle übrigen geistigen Schöpfungen zum privaten Gebrauch verwertet werden dürfen (§ 53 Abs. 1 UrhG)[781], nicht aber Computerprogramme, wenn und soweit sie urheberrechtlich geschützt sind.[782]

---

772 Vgl. *Schmitz/Preiß*, **c't** 8/2000, S. 113.
773 So z.B. die *SPA*, vgl. *Fryer*, **Wired Magazine** 3.05 – Mai 1995.
774 Interview mit *Lohmeier* (*Microsoft*), **PC-Intern** 8/1998, S. 36 f.
775 *Dannecker*, **BB** 1996, S. 1292; *Franzheim*, Überkriminalisierung durch Urheberrechtsnovelle, **CR** 1993, S. 101 ff.; ders., Strafrechtliche Konsequenzen der Urheberrechtsnovelle, **NJW-CoR** 1994, S. 160 ff.
776 Vgl. *Schultz*, S. 124.
777 Vgl. *Herberger*, S. 10 und 15 m.w.N.; siehe hierzu auch das Urteil des *BGH* vom 10.11.1954 (Az. 5 StR 476/54), **BGHSt** 7, S. 28, 32 , wonach vom Tatrichter bei der Strafzumessung ein Abschreckungsbedürfnis (der Allgemeinheit) strafschärfend als Nebenstrafzweck mitberücksichtigt werden kann. Anerkennung als Strafzweck erfährt Abschreckung ebenfalls im Urteil des *BVerfG* vom 21.06.1977 (Az. 1 BvL 14/76), **BVerfGE** 45, S. 187 ff.
778 Siehe hierzu Kube/Störzer/Timm-*Stümper*, S. 372.
779 Vgl. *Reiser*, **NJW-CoR** 1995, S. 54.
780 *Dannecker*, **BB** 1996, S. 1292.
781 Zu Sinn, Zweck und rechtlicher Ausgestaltung der sogenannten Privatkopie siehe unten Teil 3, C. I. 1.

Anders sieht es bei gewerbsmäßig handelnden Tätern aus. Hier ist davon auszugehen, dass die drohende Strafverfolgung als Risikofaktor und Abwägungsgesichtspunkt vor potentiellen Taten eine entscheidende Rolle spielt, und auch in der Gesellschaft stößt es weitgehend auf Zustimmung, wenn die gewerbsmäßige Ausbeutung fremder geistiger Leistungen nicht vom Staat toleriert wird[783].

Im Schrifttum wird darüber hinaus kritisiert, dass die starke Orientierung des deutschen Gesetzgebers auf dem Gebiet des Computerrechts an strafrechtlichen Normen nicht der international erhobenen Forderung entspricht, wonach der Schwerpunkt der Bekämpfung auf außerstrafrechtliche Präventivmittel gelegt werden müsse.[784] Bereits vor dem Internet-Boom wurde befürchtet, dass sich durch den Verzicht auf Präventivmaßnahmen die Computerstraftaten zu einem noch schwerer kontrollierbaren Massenphänomen ausweiten würden.[785] Diese Situation ist im Bereich der privaten unerlaubten Verwertung bereits eingetreten, denn die Strafverfolgungsorgane sehen sich nicht mehr in der Lage, mittels strafrechtlicher Sanktionen gegen solche Täter vorzugehen.[786] Da es bei der Frage der Bewältigung multimedialer Kriminalität primär um die Kontrolle von Handlungen gehe, also um eine Aufgabe, die den Zielen des Strafrechts fern liege, hätten Präventivmaßnahmen eine nicht zu unterschätzende Bedeutung[787]. Würden diese ergriffen, könnten nur noch Täter mit speziellen Kenntnissen unter Einsatz hoher krimineller Energie Computermanipulationen und sonstige Rechtsverstöße vornehmen.[788] Maßnahmen wie die Einführung technischer Sicherheitsstandards mit Zugriffskontrollsystemen, eine umfassende Aufklärung der betroffenen Systembenutzer sowie geeignete zivil- und öffentlich-rechtliche Rahmenbedingungen seien demnach deutlich wichtiger als Strafvorschriften[789]. Nur mit Hilfe der genannten Maßnahmen könnten Rechtsverstöße von solchen Tätern verhindert werden, die geringe kriminelle Energie einsetzen; das Strafrecht solle lediglich eine Reaktion auf schwerere Verstöße der Bürger bleiben.[790]

Eine andere Auffassung geht sogar noch einen Schritt weiter und fordert, dass die betroffenen Rechtsinhaber für jegliche Verstöße gegen Vorschriften des UrhG ganz auf den Zivilrechtsweg verwiesen werden sollen, um die Raubkopierer per Abmahnung oder Klage zur Unterlassung ihrer illegalen Handlungen zu zwingen oder aber um entstandene Schäden ersetzt zu bekommen.[791] Man kann sicher davon ausgehen, dass die erhoffte Denkzettelwirkung der Strafe in den meisten Fällen von den Schadensersatzforderungen des Geschädigten überlagert wird.[792] Führt man sich vor Augen, dass die Täter, die Raubkopien herstellen und verbreiten, in der Regel sozial gut integriert sind, wird die spezialpräventive Wirkung einer (Bewährungs-)Strafe häufig als gering einzuschätzen sein.[793]

---

[782] *Meier*, **JZ** 1992, S. 665; die Nichtanwendbarkeit des § 53 UrhG auf Computerprogramme ergibt sich aus § 69c Nr. 1 UrhG i.V.m. 69a Abs. 4 UrhG, die insoweit eine abschließende Regelung darstellen – siehe hierzu auch: Amtl. Begr. **BT-Drucks.** 12/4022, S. 8 f.
[783] Vgl. *Meier*, **JZ** 1992, S. 665.
[784] *Dannecker*, **BB** 1996, S. 1291; *Vassilaki*, Multimediale Kriminalität, **CR** 1997, S. 301.
[785] *Dannecker*, **BB** 1996, S. 1292.
[786] *Dannecker*, **BB** 1996, S. 1292.
[787] *Vassilaki*, Multimediale Kriminalität, **CR** 1997, S. 301.
[788] *Dannecker*, **BB** 1996, S. 1292.
[789] *Sieber*, Missbrauch der Informationstechnik, Teil 3, III. 3.; *Vassilaki*, Multimediale Kriminalität, **CR** 1997, S. 301.
[790] *Dannecker*, **BB** 1996, S. 1292.
[791] Vgl. *Schultz*, S. 124.
[792] *Meier*, **JZ** 1992, S. 664 f.
[793] Vgl. *Meier*, **JZ** 1992, S. 664.

Es darf allerdings nicht übersehen werden, dass ein Teil der dargestellten (liberalen) Auffassungen aus einer Zeit stammt, in der dem Internet noch keine nennenswerte Rolle im Bereich der Softwarepiraterie zukam. Mit der fortgeschrittenen Entwicklung reicht die grobe Einteilung der Täter in Schulhofpirat und professionellen Raubkopiedealer nicht mehr aus, so dass eine neue, differenzierte Betrachtungsweise erforderlich ist:

Stellte man sämtliche unerlaubten Verwertungshandlungen im privaten Bereich (d.h. solche ohne Gewinnerzielungsabsicht) straflos, würde man über das Ziel hinausschießen. Die Entwicklung hat einen neuen Tätertyp hervorgebracht. Das alte Abgrenzungsmerkmal der privaten bzw. gewerbsmäßigen unerlaubten Verwertung ist nicht mehr geeignet, die unterschiedliche Sozialschädlichkeit beider Tathandlungen widerzuspiegeln. Denn bei Betreibern von Webseiten, die Raubkopien für Millionen von Menschen öffentlich zugänglich machen, ist trotz des fehlenden Erwerbszwecks wohl kaum noch von einem privaten Rahmen auszugehen. Die Forderung, sämtliche Verwertungshandlungen im privaten Bereich straflos zu stellen, ist in diesem Kontext nicht mehr zeitgemäß. Da sich präventive Maßnahmen zur Zeit nur mit eingeschränktem Erfolg verwirklichen lassen, hat das Strafrecht nach wie vor seine Berechtigung.

Als Lösung böte sich an, Computerprogramme in den Anwendungsbereich des § 53 UrhG einzubeziehen, und somit denjenigen straffrei zu stellen, der zum privaten Gebrauch Softwarekopien erstellt.[794] Da die privaten Vervielfältigungsstücke gemäß § 53 Abs. 6 S. 1 UrhG weder verbreitet noch zu öffentlichen Wiedergaben benutzt werden dürfen, kommen besonders aktive Internetpiraten nicht in den Genuss der Privilegierung. Durch diese urheberrechtliche Gestaltung würde die Gesetzeslage mit der Verfolgungspraxis in Einklang gebracht.

Weil es sich bei Programmkopien, die im Unternehmen oder im Rahmen einer sonstigen Erwerbstätigkeit eingesetzt werden, nicht um Privatkopien i.S.d. § 53 UrhG handelt, würde die Gestaltung auch diesbezüglich nicht zu unbilligen Ergebnissen führen. Das Argument, wonach Computerprogramme nicht zu den von § 53 UrhG erfassten Werken zählen dürfen, da ihre digitale Form verlustfreie Vervielfältigungen ermöglicht[795], ist überholt: Mittlerweile liegen alle Werkarten digital

---

[794] Zu beachten ist, dass eine entsprechende Gestaltung nur auf europäischer Ebene umzusetzen wäre. Der Ausschluss der Privatkopie von Computerprogrammen rührt von der Richtlinie des Rates der Europäischen Gemeinschaft über den Rechtsschutz von Computerprogrammen (Richtlinie 91/250/EWG, **ABl. EG** Nr. L 122 vom 14.05.1991, S. 42 ff.) her. Siehe in diesem Zusammenhang auch Wandte/Bullinger-*Hildebrandt*, § 106 UrhG, Rdnr. 28 a.E., der schon nach der geltenden Rechtslage eine Straffreiheit für möglich hält: „Eine Bestrafung der Verwertung von Computerprogrammen im Rahmen des privaten Gebrauchs entsprechend § 53 dürfte mit Blick auf den Gleichheitsgrundsatz des Art. 3 Abs. 1 GG unzulässig sein".

[795] So z.B. bei Schricker-*Loewenheim* (1987), § 53 UrhG, Rdnr. 38 (zur Ratio Legis des § 53 Abs. 4 S. 2 a.F.): „Datenverarbeitungsprogramme sind im allgemeinen nur mit erheblichem Zeit- und Kostenaufwand zu erstellen, können dagegen mit den heutigen Vervielfältigungstechniken in kürzester Zeit und mit minimalem Aufwand kopiert werden". In Rdnr. 40 ist von der „erhöhten Verletzlichkeit von Datenverarbeitungsprogrammen gegenüber Piraterieakten" die Rede. Das von *Loewenheim* angeführte Argument des erheblichen Zeit- und Kostenaufwands beim Erstellen von Computerprogrammen verliert deutlich an Gewicht, wenn man sich vor Augen hält, wie viel Zeit und Geld beispielsweise im Rahmen aktueller Kinofilm- oder DVD-Produktionen benötigt wird.

vor und können ebenso vervielfältigt werden. Dennoch fallen sie auch in digitaler Form unter § 53 UrhG.[796]

Mit einer entsprechenden Ausnahme für das Urheberstrafrecht wäre – zumindest für den privaten Bereich – den rechtspolitischen Bedenken Rechnung getragen, die erstmals im Zusammenhang mit der Urheberrechtsnovelle von 1993[797] in der Literatur geäußert wurden. Kritische Juristen sahen in der Neufassung von § 106 UrhG einen Verstoß gegen das Bestimmtheitsgebot aus Art. 103 Abs. 2 GG: Da es von der Ausgestaltung einzelner Lizenzverträge abhänge, ob sich ein Lizenznehmer strafbar macht oder nicht (sogenannte Zivilrechtsakzessorietät), sei § 106 i.V.m. §§ 69a ff. UrhG zu unbestimmt.[798]

Durch die Ausweitung des Strafrechtsschutzes mit Hilfe der Urheberrechtsnovelle würden zivilrechtliche Vertragsverletzungen kriminalisiert und der für den Gesetzgeber geltende Grundsatz verletzt, wonach der Einsatz strafrechtlicher Mittel nur die ultima ratio sein darf.[799]

Die Grenze zwischen Straflosigkeit und Strafbarkeit beim privat Handelnden ist tatsächlich schwierig zu ziehen: Zum Raubkopierer wird der ahnungslose Anwender nach den Lizenzbestimmungen vieler Hersteller bereits dann, wenn er die erworbene Software gleichzeitig auf PC und Laptop einsetzt. Das Gleiche kann passieren, wenn Angestellte eines Unternehmens das im Büro verwendete Programm auch zu Hause einsetzen wollen.[800]

Ein Vergleich mit der englischen Rechtslage, die als Vorbild für die der Novellierung zugrundeliegende EU-Richtlinie[801] diente[802], zeigt, dass sich der Gesetzgeber durchaus anders hätte orientieren können: Nach Section 107 des Copyright, Designs and Patents Act von 1988 wird lediglich derjenige bestraft, der ohne Lizenz des Urheberberechtigten Raubkopien zum Zwecke des Verkaufs oder der Vermietung herstellt, oder sie zu nicht privaten Zwecken in das Vereinigte Königreich einführt oder sie innerhalb eines Unternehmens in der Absicht besitzt, eine unerlaubte Verwertungshandlung vorzunehmen. Ferner wird nach Section 107 mit Strafe bedroht, wer Raubkopien im Rahmen eines Geschäftsbetriebs verkauft oder verleiht. Es werden somit nur gewerbsmäßige unerlaubte Verwertungen sowie der Einsatz von raubkopierter Software in Unternehmen unter Strafe gestellt.[803] Vergleicht man die für 1999 von der *SIIA* ermittelten Raubkopieraten von Großbritannien (26%) und Deutschland (27%)[804], zeigt sich, dass die zusätzliche Strafandrohung für den privaten Bereich in Deutschland keine nennenswerte Wirkung entfalten konnte.

---

796 Wandtke/Bullinger-*Lüft*, § 53 UrhG, Rdnr. 7; Schricker-*Loewenheim*, § 53 UrhG, Rdnr. 23 i.V.m. § 16 UrhG, Rdnrn. 17 und 18 (jeweils m.w.N.).
797 Urheberrechtsnovelle vom 24.06.1993, **BGBl. I** 1993, S. 910 ff.
798 *Franzheim*, Strafrechtliche Konsequenzen der Urheberrechtsnovelle, **NJW-CoR** 1994, S. 161
799 *Franzheim*, Überkriminalisierung durch Urheberrechtsnovelle, **CR** 1993, S. 102. Zum Ultima-ratio-Grundsatz siehe auch das Urteil „Schwangerschaftsabbruch II" des *BVerfG* vom 28.05.1993 (Az. 2 BvF 2/90 und 4, 5/92), **BVerfGE** 88, S. 203, 258; darin heißt es: „Das Strafrecht ist zwar nicht das primäre Mittel rechtlichen Schutzes, schon wegen seines am stärksten eingreifenden Charakters; seine Verwendung unterliegt daher den Anforderungen der Verhältnismäßigkeit. Aber es wird als "ultima ratio" dieses Schutzes eingesetzt, wenn ein bestimmtes Verhalten über sein Verbotensein hinaus in besonderer Weise sozialschädlich und für das geordnete Zusammenleben der Menschen unerträglich, seine Verhinderung daher besonders dringlich ist."
800 *Schultz*, S. 124.
801 Siehe Fn. 794.
802 So dargestellt von *Dannecker*, **BB** 1996, S. 1290.
803 Vgl. *Franzheim*, Strafrechtliche Konsequenzen der Urheberrechtsnovelle, **NJW-CoR** 1994, S. 161.
804 Siehe oben Teil 2, B. I. 2.

Schließlich ist zu bedenken, dass eine Einbeziehung von Software in den Anwendungsbereich von § 53 UrhG dazu führen würde, dass die Rechtsinhaber über § 54 UrhG – in entsprechend angepasster Form – einen Kompensationsanspruch erhielten. Dieser ließe sich u.a. über die Einführung einer Leermedien- bzw. Geräteabgabe (CD-ROMs, Festplatten, CD-Brenner) realisieren.[805] Zur Zeit gibt es keinerlei Kompensation für das massenhafte private Kopieren von Software, weshalb eine entsprechende Gesetzesänderung für die Rechtsinhaber positive wirtschaftliche Effekte hätte.

Es bleibt festzuhalten, dass – abgesehen von den bestehenden Diskrepanzen zwischen Verfolgungspraxis und Rechtslage – die geltenden strafrechtlichen Gesetze der Situation gerecht werden. Die anstehende Novellierung des UrhG wird keine einschneidenden Änderungen mit sich bringen, sofern es bei dem vorliegenden Regierungsentwurf bleibt.[806] Begrüßenswert sind die Klarstellungen im Bereich der Providerhaftung. Mit der Anpassung an die Verantwortlichkeitsregelungen des TDG dürften wesentliche Zweifel an der bisherigen Gesetzesauslegung ausgeräumt sein.

3. Weitere Schlussfolgerungen und Anregungen

Der verantwortungsvolle Umgang mit Informationen ist ein zentraler Punkt im Kampf gegen das Raubkopieproblem im Internet. Ziel muss sein, den schwer kontrollierbaren Untergrund möglichst klein zu halten, weshalb Informationen über die Warez-Szene nicht weitläufig und vor allem nicht auf zweifelhafte Art und Weise verbreitet werden sollten. In diesem Kontext spielen vor allem die Printmedien eine bedeutende Rolle. Nicht selten findet man in Computerzeitschriften reißerisch aufgemachte Berichte, die zwar auf die Illegalität des Raubkopierens hinweisen, jedoch die Szene und die Abläufe derart detailliert darstellen, dass sie gleichzeitig als Anleitungen zu unerlaubten Verwertungshandlungen fungieren können.

Abbildung 90 – Schlagzeile einer Computerzeitschrift

Gerade hinsichtlich des allgemein bekannten, geringen Unrechtsbewusstseins beim unerlaubten Vervielfältigen von Software ist dies ein äußerst sorgloser Umgang mit dem Thema. Das folgende Beispiel zeigt deutlich, wie die Gratwanderung zwischen moralischer Verantwortung und

---

[805] So bereits *Meier*, **JZ** 1992, S. 665, der allerdings von einer Leerdiskettenabgabe spricht. Da Leerdisketten mittlerweile zu den aussterbenden Speichermedien gehören, empfiehlt es sich, eine Abgabe an zeitgemäße Datenträger zu koppeln.
[806] Siehe hierzu die Nachträge in den Fn. 342 und 433.

Orientierung an der Auflagenstärke misslingen kann: In der Januar-Ausgabe 1999 einer deutschen Computerzeitschrift erschien ein Artikel über die Internet-Raubkopiererszene, in dem der Autor es ausdrücklich vermied, Schlüsselbegriffe wie „Warez“ etc. zu erwähnen. Dieser löbliche Ansatz wurde jedoch von den Grafikern der Titelseite zunichte gemacht. Letztere titelten in großen Lettern: „Warez, Hackz und Crackz im Internet“.

Abbildung 91 – Schlagzeile einer Computerzeitschrift

Waren solche reißerischen Titel 1999 noch die Ausnahme, hat sich die Situation mittlerweile dramatisch verändert. Ein Großteil der Zeitschriften bricht gewohnheitsmäßig das Tabu und verspricht dem Leser auf den Titelseiten Hilfestellung bei allen Kopier- und Downloadfragen. Solche Maßnahmen, die einzig und allein der Auflagensteigerung dienen sollen, bescheren der Szene mit Sicherheit zusätzlichen Zulauf. Autoren von Computerzeitschriften sollten immer im Hinterkopf haben, dass ihre Leser als „Computerfreaks“ in der Regel sehr neugierige Menschen sind und ein geringes Unrechtsbewusstsein haben, was das nichtlizenzierte Kopieren von Software anbelangt.

Der verantwortungsvolle Umgang mit Informationen ist nicht nur den Medien anzuraten, auch die Webhosting-Provider können zur Sensibilisierung und Aufklärung der Internetnutzer beitragen. Wenn eine Homepage aufgrund entdeckter rechtswidriger Inhalte vom Netz genommen wurde, werden die Daten im Normalfall vom Provider gelöscht. Will ein Internetnutzer die Seite unter der ihm bekannten Adresse aufrufen, erhält er im Regelfall eine Meldung des Providers, dass sich die angeforderten Inhalte nicht mehr auf dem Server befinden. Diese Meldungen reichen von „404 – file not found” oder „ooops – sorry, we can’t find the page you are looking for“ bis „the site you are looking for was taken down due to violation of our membership policies”. Meist sind diese Aussagen allgemein gehalten, der konkrete Grund für die Löschung der Inhalte wird nicht genannt. Hier wäre es angebracht, die Zuwiderhandlung beim Namen zu nennen und eventuell weiterführende Aufklärung zu betreiben. Denkbar wären beispielsweise Informationen über die Rechtslage oder über die rechtlichen Konsequenzen, die der ehemalige Betreiber der Seite im konkreten Fall zu tragen hat (Einleitung eines Strafverfahrens etc.). Da der Host-Service-Provider erkennen kann, von wo aus der Nutzer auf seine Seite zugreift, wäre es sogar möglich, entsprechende Informationen in der Landessprache des jeweiligen Surfers zu übermitteln. Auch Hinweise darauf, dass der Provider sämtliche Aktivitäten auf seinen Seiten in Logfiles schreibt und diese für einen gewissen Zeitraum speichert, hätten sicher eine abschreckende Wirkung.

Bei den Adressaten solcher Aufklärungsseiten wird es sich fast ausschließlich um Nutzer handeln, die gerade im Begriff sind, rechtswidrige Inhalte abzurufen. Eine präzisere Adressierung ist somit kaum denkbar. Jemand, der häufig auf diese Seiten stößt und regelmäßig erfährt, dass die Ermittlungsbehörden mit dem Fall beschäftigt sind, wird es sich mehr als einmal überlegen, ob er selbst eine Homepage mit Raubkopien ins Netz stellt. Die Erfahrung hat gezeigt, dass sich Nachrichten über „Busts" wie Lauffeuer verbreiten. Die Folge sind erhöhte Vorsichtsmaßnahmen der Untergrund-Szene, was den Zugang neuer Szenemitglieder drastisch erschwert. Fraglich ist allerdings, ob die Provider freiwillig zu dieser Aufklärungsarbeit bereit sind. Eine Theorie besagt, das Internet und seine Dienste seien nicht zuletzt wegen der leichten Verfügbarkeit von zweifelhaften Inhalten populär geworden. Sex und Raubkopien werden nicht zu Unrecht als Motor des Internet vermutet:[807] Tatsächlich ist es so, dass der Marktwert eines Webhosting-Providers mit der Anzahl der eingerichteten Homepages und der Anzahl der darauf zugreifenden Nutzer steigt. Es ist kein Geheimnis, dass auf einem Großteil der Homepages, die ihm die ersehnten „Hits" bringen, Pornographie oder Raubkopien angeboten werden. Dass diese Inhalte zu den meistgesuchten Inhalten im WWW zählen, lässt sich unter anderem mit den Suchwortstatistiken der großen Suchmaschinen belegen. Seit Jahren haben die Begriffe „sex" und „warez" einen Stammplatz in den Top Ten aller Suchbegriffe.

Sollte der geschilderte Interessenkonflikt zu einer Verweigerungshaltung der Provider führen, ist eine Einigung auf entsprechende Codes of Conduct erstrebenswert. Erst wenn diese fehlschlägt, sollten gesetzliche Regelungen in Erwägung gezogen werden.

Insgesamt gilt es, bei den Nutzern ein Bewusstsein zu schaffen, dass Software nicht vergütungsfrei über das Internet der Öffentlichkeit zugänglich gemacht werden darf und dass Computerprogramme nicht ohne Lizenz genutzt werden dürfen, sofern sie in Unternehmen oder zu sonstigen Erwerbszwecken eingesetzt werden.

Exkurs - Free Software und Open Source – das Ende der Softwarepiraterie?

Bedingt durch den großen Erfolg des freien Betriebssystems *Linux*[808] erlangte die sogenannte Free-Software-Bewegung einen hohen Bekanntheitsgrad. Viele Anhänger dieser Bewegung lehnen einen urheberrechtlichen Schutz für Computerprogramme sowie für andere geistige Werke gänzlich ab. Eine freie Software soll grundsätzlich ohne Zahlung eines Entgelts und in erster Linie an Privatkunden weitergegeben werden. Derzeit verdienen Unternehmen, die beispielsweise *Linux* distribuieren, am Verkauf von Begleitmaterial sowie an Dienstleistungen für die Kunden (Systempflege, Support, individuelle Anpassungen etc.). Dies ist insofern durchaus lukrativ, als dass auch die großen Hersteller kommerzieller Betriebssysteme den Großteil ihres Umsatzes mit Support und Service erzielen[809]. Hinzu kommt eine strategische Überlegung: Da sich freie Software aufgrund der wegfallenden Anschaffungskosten schnell verbreitet, lassen sich mit einem qualitativ hochwertigen Produkt leicht große Marktanteile gewinnen. Kommt es dann zu Entscheidungs-

---

807 Vgl. *Glaser*, So hat der Sex das Netz gemacht, **konr@d** 5/1999 (Okt./Nov.), S. 26 ff.
808 Der Name *Linux* geht auf den finnischen Informatiker *Linus Thorvalds* zurück, der 1991 begann, den Kern (Kernel) eines freien Betriebssystems zu entwickeln.
809 Vgl. das Interview mit *Young*, bei *Menge*, **c't** 22/1999, S. 46.

prozessen innerhalb von Unternehmungen, bauen die Anhänger der Free-Software-Bewegung darauf, dass zahlreiche Entscheider auf freie Software setzen und in der Folge eine Vielzahl von Softwarepflegeverträgen abschließen.

Die Ideologie der Free-Software-Bewegung wurde entscheidend von dem amerikanischen Programmierer *Richard Stallman* geprägt[810]. *Stallman* war unter anderem federführend an der Entwicklung des alternativen Betriebssystems *GNU*[811] und *EMACS*, einem erweiterbaren Texteditor für *UNIX*, beteiligt. Die bereits angesprochenen *Linux*-Distributionen basieren auf *GNU*, und auch *EMACS* entwickelte sich Anfang der 90er Jahre zu einem erfolgreichen Produkt.[812] *Stallmans* Stellungnahme zum Problem der Softwarepiraterie fällt simpel aus: „You can't pirate something that's free". Er geht davon aus, dass bei den Schadensberechnungen der Softwareindustrie und ihrer Verbände übertrieben wird und vertritt die Ansicht, dass nicht jeder, der raubkopiert, die Software auch gekauft hätte.[813] Die Arbeit der *SPA* (jetzt *SIIA*) vergleicht er gerne mit Praktiken des früheren sowjetischen Regimes. Ausdrücke wie „Piracy" und „Theft" empfindet er als manipulatorisch und der Situation nicht angemessen. Nach Meinung von *Stallman* sind Gesetze generell vergänglich und lediglich ein temporärer Ausdruck von moralischen Ansichten.[814] Eine Anpassung von Urheberrechtsgesetzen an die „digitale Realität" hält er für ausgeschlossen, die derzeit vieldiskutierte Patentierung von Software lehnt Stallman als fortschrittshemmend ab.

Um seine Vision einer Welt freier Software zu verwirklichen, gründete *Stallman* 1984 die *Free Software Foundation (FSF)*[815], eine nicht-gewinnorientierte Organisation mit der Mission, freie Software zu entwickeln.[816] In Verbindung mit *Stallmans GNU*-Projekt kann die *FSF* als eine der ersten Anti-Copyright-Organisationen des digitalen Zeitalters angesehen werden.[817] Im sogenannten *GNU*-Manifest von 1983 erklärt *Stallman* unter anderem: „Ich glaube, dass es das Gebot der Nächstenliebe verlangt, dass ich ein Programm, das mir gefällt, mit anderen teile, denen es ebenfalls gefällt. Software-Anbieter hingegen wollen die Anwender isolieren und beherrschen, wobei sie jeden Anwender dazu verpflichten, nicht mit anderen zu teilen. Ich weigere mich, die Solidarität mit anderen Anwendern in dieser Weise zu brechen. Ich kann nicht mit gutem Gewissen einen Nichtoffenbarungsvertrag oder einen Software-Lizenzvertrag unterzeichnen. Damit ich ehrlich bleiben und trotzdem weiterhin Computer benutzen kann, habe ich mich entschlossen, eine genügend große Sammlung von freier Software zusammenzustellen, so dass ich in der Lage sein werde, ohne jegliche nicht freie Software auszukommen. Ich habe meinen Beruf im *AI Lab* aufgegeben, um dem *MIT* keinen rechtlichen Vorwand zu bieten, mich daran zu hindern, *GNU* weiterzugeben".[818]

---

[810] *Stallman* gilt als einer der angesehensten lebenden Programmierer, vgl. *Garfinkel*, Is Stallman Stalled?, **Wired Magazine** 1.01 – März/April 1993.
[811] *GNU* ist ein *UNIX*-ähnliches Betriebssystem, das 1984 veröffentlicht wurde.
[812] *Garfinkel*, Is Stallman Stalled?, **Wired Magazine** 1.01 – März/April 1993.
[813] Vgl. oben Teil 2, A. VIII. 3.
[814] Vgl. *Stallman*, Why Software Should Not Have Owners, FSF.org.
[815] http://www.fsf.org bzw. http://www.fsfeurope.org *(Free Software Foundation Europe).*
[816] *Garfinkel*, Is Stallman Stalled?, **Wired Magazine** 1.01 – März/April 1993.
[817] Vgl. *Rink*, **c't** 6/1999, S. 194.
[818] *Stallman,* GNU Manifest, FSF.org.

Die *FSF* finanziert sich hauptsächlich durch freiwillige Zahlungen von den Nutzern der entwickelten Software und von verschiedenen Computerunternehmen. Da diese Zuwendungen seit jeher äußerst dürftig ausfielen, geriet die *FSF* zwischenzeitlich in finanzielle Schwierigkeiten.[819] Die eigentlichen Gewinner des alternativen Softwarekonzeptes waren solche Unternehmen, die ihre Dienstleistungen zum Support von *GNU*-Software an große Kunden verkaufen konnten. Mittlerweile versucht die *FSF*, sich zusätzlich über den Verkauf von Software und Merchandising-Artikeln zu finanzieren. Paradoxerweise resultiert der größte Teil der Einnahmen der *FSF* aus Verkäufen von Produkten, die jedermann frei kopieren darf.[820]

Untrennbar mit der Free-Software-Bewegung ist das Prinzip der Open Source verknüpft. In den letzten Jahren hat sich besonders in Europa unter *Linux*-Freunden die Zielvorstellung der Open Source oder Open Software (OS) gebildet. Hierunter versteht man in erster Linie einen offenen Programmcode, d.h. jeder interessierte Nutzer dieser Software darf in den Quellcode hineinschauen und ohne Erlaubnis Weiterentwicklungen selbst vornehmen.[821] Dies ist durchaus nicht selbstverständlich, da der Quellcode einer Software normalerweise von den Herstellern geheimgehalten wird.

Open Source ermöglicht somit einer unbegrenzten Anzahl von potentiellen Softwareentwicklern den freien Zugang zu einem Produkt. Bei *Linux* gibt es bereits eine große und internationale Entwicklergemeinde, die ständig darum bemüht ist, das Betriebssystem zu verbessern. Jeder, der eine Verbesserung oder Erweiterung vorgenommen hat, muss diese bei einem Gremium („Komitee“) vorstellen, welches die Neuerung prüft und schließlich darüber entscheidet, ob sie in der nächsten *Linux*-Version enthalten sein wird. Auf diese Weise ist gewährleistet, dass nur sinnvolle und erprobte Veränderungen Einzug in das Betriebssystem finden. Ein weiterer großer Vorteil von Open-Source-Software besteht darin, dass Sicherheitslücken und Programmfehler erfahrungsgemäß schneller aufgedeckt und behoben werden als bei herkömmlichen Lizenzmodellen. Auch lassen sich keine dem Anwender verborgenen Funktionen in eine Software einbauen.[822]

Das große Einsparungspotenzial bei den Anschaffungskosten und die beschriebenen Sicherheitseffekte sind ausschlaggebend dafür, dass in Zukunft verstärkt Open-Source-Software in der deutschen Bundesverwaltung zum Einsatz kommen wird.[823] Die Bundesregierung unterstützt außerdem das Open-Source-Projekt *GNU Privacy Guard* (*GPG*) mit finanziellen Mitteln. Man erhofft

---

819 *Garfinkel*, Is Stallman Stalled?, **Wired Magazine** 1.01 – März/April 1993.
820 http://www.fsf.org/help/help.html.
821 Grundlage für die Abgrenzung von OS-Software zu herkömmlicher Software ist die Open-Source-Definition (OSD, http://www.opensource.org/docs/definition_plain.php). An der OSD orientieren sich verschiedene OS-Lizenzmodelle, unter anderem die nachfolgend beschriebene *GNU*-GPL.
822 *Schmidt/Hüttermann*, c't 16/1999, S. 114.
823 So wird auf den rund 150 Servern des *Bundestags* die vorhandene *Microsoft*-Software durch das freie Betriebssystem *Linux* ersetzt. Allerdings werden die Arbeitsplatzrechner der Abgeordneten mit dem aktuellen *Microsoft*-Betriebssystem *Windows XP* ausgestattet, vgl. **Heise Online News** vom 14.03.2002, http://www.heise.de/newsticker/meldung/25701.

sich vor allem im Sicherheitsbereich (z.B. Verschlüsselung) eine größere Verlässlichkeit und Transparenz von den Software-Produkten.[824]

Das Open-Source-Prinzip hat dazu geführt, dass die Qualität der Softwareprodukte einen sehr hohen technischen Standard erreicht hat. Experten zufolge kann die Qualität und Komplexität freier Software inzwischen mit kommerziellen Produkten mithalten. Beispiele für erfolgreiche Open-Source-Software sind neben *Linux* die Programme *Apache, Bind, Perl* und *Sendmail*[825]. Aufgrund der außerordentlichen Stabilität von *Linux* ist die Vorreiterstellung von *Microsofts Windows NT* auf dem Markt für Serverbetriebssysteme bereits ins Wanken geraten.[826] Denn die derzeitigen Schwächen freier Software, vor allem die mangelnde Benutzerfreundlichkeit, spielen in diesem Bereich keine nennenswerte Rolle.[827] Der Erfolg von Open Source veranlasst immer mehr Softwarehersteller (u.a. *Apple, SAP, Microsoft* und *Sun Microsystems*) dazu, jedermann die Quellcodes ihrer Programme zugänglich zu machen. Hierbei werden allerdings unterschiedliche Konzepte verfolgt. Manche Entwickler erlauben lediglich einen Blick in die Quellen, ein freies Arbeiten mit den Quelltexten ist jedoch nur nach individueller Erlaubniserteilung gestattet. Während es für einige Vertreter der Open-Source-Bewegung ausschließlich darauf ankommt, dass man den Quelltext uneingeschränkt modifizieren darf, um das Programm eigenen Bedürfnissen anzupassen, zu erweitern oder um Fehler zu beheben und dass man das veränderte Programm unter denselben Bedingungen wie die ursprüngliche Software weitergeben kann, liegt für die Vertreter der Free-Software-Bewegung das Gewicht vor allem auf der „Freiheit" der Software.[828]

Die *GNU*-Pioniere schufen für den Vertrieb ihrer freien Software ein spezielles Lizenzmodell, das die freie Weitergabe und die Offenlegung aller Quellen über sämtliche Generationen eventueller Weiterentwicklung hinweg garantiert bzw. erzwingt – die *GNU* General Public Licence (*GNU*-GPL oder GPL). Deren vielleicht eigentümlichste Eigenschaft ist der sogenannte Virus-Effekt: Ein Softwareprodukt, das der GPL unterworfen ist, darf verkauft, verschenkt, verändert, genutzt und in eigene Projekte eingebaut werden. Diese eigenen Projekte fallen damit allerdings automatisch auch unter die GPL und müssen entsprechend freigegeben werden. Dieses Prinzip wird von den *GNU*-Entwicklern mit dem Begriff „Copyleft" bezeichnet.[829] Im juristischen Sinne nutzt die GPL das Urheberrecht zum Schutz des Open-Source-Prinzips. Zwar dient sie nicht mehr der ursprünglichen Intention des UrhG, dem Urheber die kommerzielle Verwertung seines Werkes zu ermöglichen, sondern die GPL nutzt das klassische Urheberrecht dazu, Software jedermann zugänglich zu machen, indem sie die vermögensrechtliche Verwertung von Programmen verbietet. Die persönlichkeitsrechtlichen Bestandteile des Urheberrechts (z.B. Namensnennung des Schöpfers) verbleiben allerdings beim Urheber.[830] Am 01.07.2002 erlangte die sogenannte *Linux*-Klausel Wirksamkeit im deutschen Urheberrecht, um die bestehenden Wertungswidersprüche zu vermeiden. Im neuen § 32

---

[824] **c't** 25/1999, S. 36.
[825] Informationen zu Verbreitung und Marktanteilen von OS-Software finden sich unter http://www.dwheeler.com/oss_fs_why.html.
[826] Nach einer Studie der *International Data Corporation* (*IDC,* http://www.idc.com) vom Februar 2000 belegt *Linux* mit einem Anteil von 25% den zweiten Platz in der Rangliste der am häufigsten verkauften Server-Betriebssysteme hinter *Windows NT* (38%), **Heise Online News** vom 10.02.2000, http://www.heise.de/newsticker/meldung/7935.
[827] *Diedrich*, **c't** 24/1998, S. 52.
[828] *Feuerbach/Schmitz*, **c't** 16/1999, S. 80.
[829] *Feuerbach/Schmitz*, **c't** 16/1999, S. 79.
[830] *T. Jaeger*, Zwang zur Freiheit, **c't** 8/2000, S. 122.

Abs. 3 S. 3 UrhG wird geregelt, dass ein Urheber jedem Dritten ein einfaches Nutzungsrecht kostenlos einräumen kann.

Neben der *GNU*-GPL gibt es auch die sogenannte *BSD*-Lizenz[831], die wesentlich liberaler ausgestaltet ist. Hier kann der Nutzer nach dem Grundsatz „mach mit der Software, was du willst" verfahren, ohne rechtliche Konsequenzen befürchten zu müssen.[832]

Zweifelsohne ist die Idee einer freien Software-Tauschgesellschaft ein ehrwürdiges Anliegen, das von bewundernswertem Idealismus zeugt. Neben der Schaffung von qualitativ hochwertigen Produkten wäre das Piraterieproblem gelöst. Es ist allerdings stark zu bezweifeln, dass das Free-Software-Modell auch in wirtschaftlicher Hinsicht zu befriedigenden Ergebnissen führt, rüttelt es doch an wesentlichen Grundfesten der marktwirtschaftlichen Ordnung wie geistigem Eigentum, Leistungsprinzip und freiem Wettbewerb - jenen Rahmenbedingungen also, die den westlichen Industrienationen einen enormen Wohlstand beschert haben. Der Vorschlag *Stallmans*, Lücken in der Finanzierung über eine Software-Steuer zu decken[833], erscheint in diesem Zusammenhang wie ein überkommener, interventionistischer Rettungsversuch. Auch die fortwährenden finanziellen Schwierigkeiten seiner *Free Software Foundation* lassen wenig Hoffnung aufkommen. Der große Erfolg von *Linux* wird sich nicht beliebig wiederholen lassen, da hier persönliche, technische und marktspezifische Momente im richtigen Zeitpunkt zusammenspielten; *Linux* profitierte nicht zuletzt von der unbehaglichen Stimmung in der IT-Branche und Computerszene bezüglich des *Microsoft*-Monopols[834].

Wer seine geistigen Schöpfungen schützen möchte, soll dies tun können, wer sie freigeben möchte, ebenso. Die Position eines Produkts am Markt sollte ausschließlich von Qualität und Preis entschieden werden. Dies zu gewährleisten, ist Aufgabe der Kartellwächter, denn vor allem im Bereich der Betriebssysteme besteht die Gefahr der Monopolbildung. Die Quelltexte auch bei kommerziellen Programmen freizugeben, ist sicherlich der richtige Weg, um die Qualität der Produkte zu erhöhen. Dies haben bereits zahlreiche Unternehmen erkannt. Insofern hat zumindest die Open-Source-Bewegung einen nachhaltigen und positiven Einfluss auf die Branche.

---

831 *BSD* steht für *Berkeley Software Design* und ist ein UNIX-Projekt, das an der Universität von Berkeley in den USA entstanden ist, siehe auch http://www.bsd.org.
832 http://www.openbsd.org/policy.html; einen Überblick über die wichtigsten Open-Source-Lizenzen geben *Roehrl/Schmiedl*, **c't** 1/2002, S. 170 ff.
833 Vgl. *Stallman*, Why Software Should Not Have Owners, FSF.org.
834 *F. A. Koch*, Urheber- und kartellrechtliche Aspekte der Nutzung von Open-Source-Software -Teil 1, **CR** 2000, S. 281.

Teil 3 – Internet-Musikpiraterie

A. Beschreibung und Struktur der MP3-Szene

I. Einführung in die kurze Geschichte der Online-Musikpiraterie

Die Geschichte der Online-Musikpiraterie beginnt erst in der zweiten Hälfte der 90er Jahre mit der freien Verfügbarkeit eines sogenannten MP3-Codecs[835]. Hierbei handelt es sich um einen in eine Software implementierten Algorithmus, der aus einer großen Audiodatei, wie sie sich beispielsweise auf einer Audio-CD befindet, eine wesentlich kleinere Datei errechnen kann. Bis zu diesem Zeitpunkt gab es bereits mehrere Verfahren der Audiokomprimierung bzw. –reduktion, allerdings waren diese stark verlustbehaftet. Mit der Einführung des MP3-Formates konnten erstmals große Dateigrößenverminderungen ohne merklichen Qualitätsverlust erreicht werden.

MP3 ist die Kurzform vom MPEG-1 Layer-3[836] und nicht mit MPEG-3 zu verwechseln[837]. MPEG steht für *Motion Picture Experts Group* und bezeichnet ein Komitee von Experten, das Kodierungsverfahren für Video- und Audioanwendungen standardisiert. Innerhalb des MPEG-Komitees gibt es eine Untergruppe, die sich ausschließlich mit Audio-Kodierungsverfahren beschäftigt.[838] Die erste MP3-Encoding-Technologie geht auf das *Fraunhofer-Institut für Integrierte Schaltungen (IIS-A)* mit Sitz in Erlangen zurück. Gemeinsam mit *Thomson*, einem der größten Hersteller von Unterhaltungselektronik, entwickelte das *IIS-A* die patentierte MP3-Technologie und wurde federführend im MPEG-Komitee. Als Vater des Verfahrens gilt *Karlheinz Brandenburg*[839], derzeit Abteilungsleiter des Bereichs Audiotechnik und Multimedia beim *IIS-A*.

Das kleine und qualitativ hochwertige Format sorgte dafür, dass sich im Internet binnen kurzer Zeit eine große MP3-Gemeinde zusammenfand, in der rege Musikdateien ausgetauscht wurden. Zunächst trafen sich die MP3-Fans in IRC-Channels und im UseNet, später gab es verstärkt Download-angebote auf Webseiten und schließlich bewirkte das MP3-Phänomen den weltweiten Siegeszug der sogenannten Peer-to-Peer-Filesharing-Systeme[840]. Der freie Musiktausch über das Internet entwickelte sich zum Schreckgespenst der Musikindustrie, denn bei MP3 handelt es sich um ein Format, das nicht kopiergeschützt ist, und dessen Verbreitung deshalb jeglicher Kontrolle entzogen ist.

Erstmals in der Geschichte hat Massenpiraterie bewirkt, dass ein neuer de-facto-Standard geschaffen wurde, weshalb es nicht verfehlt ist, von einer digitalen Revolution zu sprechen. Während professionelle Anwender immer höhere Auflösungen und Samplingraten favorisieren, „stimmt das Volk mit

---

835 Zusammengesetzt aus den Worten Coder und Decoder; Coder werden auch als Encoder bezeichnet.
836 Layer steht hierbei für Algorithmus.
837 Der Name MPEG-3 war ursprünglich als Videokodierungsformat für die hochauflösende Fernsehnorm HDTV reserviert. Da diese Aktivitäten aber zumindest in Europa komplett gestoppt worden sind, ist MPEG-3 hinfällig geworden. Diesen Standard gibt es nicht und es wird ihn wohl auch in Zukunft nicht geben, vgl. *Erne*, **KEYS** 2/1999, S. 36.
838 In den MPEG-Audio-Standards werden immer nur der Decoder und die Bitstrom-Syntax definiert, nicht jedoch der Encoder.
839 Als Miterfinder des MP3-Formats musste er sich bisweilen herbe Kritik gefallen lassen. So wurde ihm aus Kreisen der Plattenbranche vorgeworfen, er hätte „eine Atombombe“ auf sie „herab geworfen“, vgl. *Schweickhardt/Henke*, **FOCUS**, 37/1998, S. 152.
840 Teil 3, A. VII. 1.

den Füßen ab“ und präsentiert der Musikbranche – zumindest vorübergehend – den neuen Standard für digitale Musik.[841]

Die Nachfrage der Nutzer nach MP3-Dateien wurde so stark, dass sich andere Industrien dem von der Musikindustrie ungeliebten Format nicht entziehen wollten. Zahlreiche Hersteller brachten mobile MP3-Player auf den Markt, und mittlerweile gibt es kaum einen DVD-Player zu kaufen, der nicht in der Lage ist, selbstgebrannte MP3-CDs abzuspielen.

Auch im IT-Bereich hat MP3 einen festen Platz gefunden: Software, mit der man MP3-Dateien auf dem heimischen PC erstellen und abspielen kann, ist für beinahe alle gängigen Betriebssysteme erhältlich, und zahlreiche Standardanwendungen nutzen das MP3-Format aufgrund seiner geringen Größe für Online-Multimediapräsentationen (z.B. *Macromedias Shockwave* und *Flash*). Für Online-Anwendungen ist MP3 außerdem interessant, da es Streaming erlaubt. Beim Streaming wird eine Musikdatei, die auf einem Server bereitliegt, bereits auf dem heimischen Rechner abgespielt, während sie noch übertragen wird. Es vergeht dadurch kaum Zeit zwischen der Anforderung der Datei per Mausklick und dem eigentlichen Abspielen. Damit ist es auch möglich, Radiosender im Internet zu betreiben, bei denen die „Sendeverzögerung“ nur wenige Sekunden beträgt. Ein Streamingformat, das jedem Surfer ein Begriff sein dürfte, ist *RealAudio* von *RealNetworks*. Für Streaming von MP3-Dateien in annehmbarer Qualität stellt eine ISDN-Verbindung das Minimum dar.

II. Die technischen Grundlagen der MP3-Herstellung

Zunächst muss man bei den Möglichkeiten, eine Datei zu verkleinern, zwischen zwei grundlegenden Verfahren unterscheiden: Reduktion und Kompression. Bei der Datenreduktion wird der ursprüngliche Informationsgehalt tatsächlich verringert und lässt sich auch nach einer Dekodierung nicht wieder exakt rekonstruieren. Bei der Datenkompression hingegen bleibt der Informationsgehalt nach Kodieren und Dekodieren voll erhalten. Bei der MP3-Kodierung kommt – entgegen dem mittlerweile üblichen Sprachgebrauch – ein Reduktionsverfahren zum Einsatz.

Die Grundlage für die Audiodatenreduktion liegt in der Psychoakustik. Diese Wissenschaftsdisziplin beschäftigt sich mit akustischen Phänomenen, die sich nicht ohne weiteres mit physikalischen Meßmethoden erfassen lassen. Dazu zählt auch die Lautheit, deren subjektives Empfinden in den seltensten Fällen mit einer reinen Schallpegelmessung korrespondiert. In der Psychoakustik arbeitet man fast ausschließlich mit streng geschulten und selektierten Testhörern, um zu gewährleisten, dass der Durchschnittshörer beim Abspielen komprimierter Dateien keine störenden Effekte wahrnimmt. Die Ergebnisse aufwändiger Hörtests bilden somit die Grundlage für allgemeingültige Methoden, um die Schwächen der menschlichen Akustikwahrnehmung auszunutzen.[842]

Beim gezielten Weglassen von Daten werden in erster Linie psychoakustische Verdeckungseffekte ausgenutzt. Diese entstehen zum Beispiel, wenn ein leiser Ton mit einem lauteren Signal ähnlicher Frequenz zusammentrifft. Ab einer bestimmten Schallgrenze wird er verdeckt und somit unhörbar: „Der Wecker tickt weiter, während er klingelt“[843]; dennoch wird das Ticken während des Klingelns nicht wahrgenommen.

---

841 Vgl. *Carstens*, **c't** 21/1998, S. 242.
842 Vgl. *Carstens*, **c't** 21/1998, S. 244.
843 So das Beispiel von *Meyer*, **c't** 6/2000, S. 93.

Die Psychoakustiker fanden neben dieser sogenannten simultanen Maskierung heraus, dass auch eine zeitliche Verdeckung stattfindet: Das Gehör benötigt bei lauten wie bei leisen Geräuschen eine Erholungsphase (Recovery Time), bis es wieder voll funktionstüchtig ist. In diesen Zeiträumen können zusätzliche Datenreduktionen erfolgen. Allein mit dem Maskierungsansatz kann eine Reduktion der Daten, wie sie auf Audio-CD vorliegen, auf ein Fünftel erreicht werden (entspricht einer MP3-Bitrate von 256 KBit/s[844]). Für eine stärkere Verringerung der Datenrate auf die mittlerweile gängigen 128 bzw. 192 KBit/s sind zusätzliche Verfahren erforderlich: Bei Stereosignalen liegt ein weiteres Verkleinerungspotential in der (unhörbaren) Reduzierung von Stereoinformationen[845].

Bei MP3s, die mit einer Bitrate von 128 KBit/s kodiert wurden, und deren Dateigröße nur rund ein Elftel der Quelldateien ausmacht, ist die Audioqualität bereits hervorragend.[846] Ungeübte Hörer können den Unterschied zur Audio-CD nicht mehr wahrnehmen. In einem großangelegten Blindtest der IT-Fachzeitschrift *c't* konnten trainierte Testhörer MP3s mit einer Qualität von 128 KBit/s zwar noch recht treffsicher erkennen, zwischen CD-Titel und einem 256 KBit/s-MP3 hingegen ließ sich kein Unterschied mehr ausmachen. Zahlreiche Testpersonen empfanden den Klang einzelner 128 KBit/s-MP3s sogar als angenehmer als den Klang der Referenz-CD.[847]

Um ein MP3 aus einem CD-Titel herzustellen, müssen die Audiodaten zunächst vom Tonträger auf die Festplatte kopiert werden. Hierfür gibt es zahlreiche Programme, die auf das CD-ROM-Laufwerk des Rechners zugreifen und die Audio-CD-Daten in WAV-Dateien umwandeln, sogenannte Grabber oder Ripper. In einem zweiten Schritt müssen die großen WAV-Dateien – 5 Minuten CD-Musik benötigen ca. 51 Megabyte Speicherplatz – mittels eines MP3-Codecs in das MP3-Format umgewandelt werden. In der Regel sind die Codecs in Programme eingebunden, die dem Nutzer komfortable Einstellungsmöglichkeiten auf einer grafischen Benutzeroberfläche bieten. Bei den meisten dieser Encoder kann der Nutzer auswählen, in welcher Bitrate (meist zwischen 56 und 320 KBit/s) er ein MP3 erstellen will, und ob es eine Mono- oder eine Stereodatei werden soll.[848]

Das MP3-Format bietet über das sogenannte ID3-Tag die Möglichkeit, in der Datei Textinformationen abzulegen, die sich von jedermann auslesen lassen. Häufig werden im ID3-Tag Angaben zum Album des Künstlers oder zum Erscheinungsjahr des Werkes hinterlegt.

---

844 Zum Vergleich: Nach neueren biophysikalischen Erkenntnissen fließen beim Hören zwischen Ohr und Gehirn lediglich 2–3 Kbit/s an Daten, was rund einem Zwanzigstel der Bandbreite entspricht, die man heute noch zur Übertragung digitalisierter Audiodaten benötigt. Allerdings ist das System, nach dem der „Datenaustausch" im Kopf erfolgt, noch nicht endgültig erforscht, vgl. *Fremerey*, Gefahren und Chancen, **c't** 2/1999, S. 28.

845 Vgl. *Carstens*, **c't** 21/1998, S. 244.

846 Das Herunterladen einer solchen Datei dauert mit einer vollausgelasteten ISDN-Leitung kaum mehr als zehn Minuten. Mit einer ADSL-Verbindung lässt sich ein entsprechendes Musikstück innerhalb einer Minute übertragen.

847 *Meyer*, **c't** 6/2000, S. 94.

848 Verschiedene Codecs ermöglichen außerdem das Kodieren in unterschiedlichen Qualitätsstufen oder im variablen Bitraten-Modus (Variable Bitrate – VBR). VBR macht die verwendete Bitrate von der Komplexität des zu kodierenden Signals abhängig und kann so – im Gegensatz zur konstanten Bitratenkodierung (Constant Bitrate – CBR) – noch kleinere Dateigrößen erzielen.
Beim Kodiervorgang handelt es sich zwar um einen rechenintensiven Vorgang, allerdings braucht ein heutiger Standard-PC nur wenige Minuten, um ein komplettes Album ins MP3-Format zu überführen. Noch leichter fällt dem Rechner das Dekodieren einer MP3-Datei. Obwohl die Filterung des ursprünglichen Signals rückgängig gemacht werden muss, entfällt eine Suche nach einer passenden Maskierungsmethode komplett. Auf heutigen Rechnern läuft das Dekodieren ohne sonderliche CPU-Belastung im Hintergrund ab. Bekannteste Abspielsoftware für MP3-Dateien auf der PC-Plattform ist das Programm *WinAmp*. Mit diesem kann aus einem MP3-File auch wieder ein großes WAV-File erzeugt werden.

Neben dem MP3-Format gibt es mehrere Konkurrenzformate wie *WMA*, *RealAudio*, *Qdesign, ePAC, VQF (TwinVQ), AAC, MP+* oder *Ogg Vorbis,* die ebenfalls auf psychoakustischen Reduktionsverfahren basieren[849]. Für die massenhafte Verbreitung von nichtlizenzierter digitaler Musik im Internet sind diese zur Zeit jedoch kaum von Bedeutung.

III. Tätigkeit der MP3-Gruppen

Nach dem Vorbild der Warez-Gruppen haben sich in den letzten Jahren zahlreiche MP3-Gruppen formiert, die Tonträger und Radiosendungen im MP3-Format veröffentlichen, wobei der größte Teil der MP3-Releases auf komplette Alben aus dem Bereich der Populärmusik entfällt. Dennoch reicht die Bandbreite der Releases von Kinderhörspielen über Konzertmitschnitte zu Klassik-Kopplungen. Denn auch zwischen den MP3-Gruppen gibt es einen Wettstreit darum, wer als erster ein Musik- bzw. Sprachwerk für die Szene bereitstellt. Insgesamt kann man feststellen, dass die MP3-Gruppen die meisten innerhalb der Warez-Szene geltenden Regeln übernommen haben. Direkte Berührungspunkte beider Szenen sind zahlreiche FTP-Server, auf denen neben Warez-Releases auch MP3- und Moviez-Releases[850] bereitgestellt werden.

Im Gegensatz zu der wesentlich größeren Gruppe der Tauschbörsennutzer sind die Mitglieder der MP3-Gruppen darauf bedacht, höchstmögliche Aktualität und Audioqualität ihrer Releases zu gewährleisten. Daher kommt innerhalb der Gruppen dem Supplier und dem Ripper (bzw. Encoder) die größte Bedeutung zu.

IV. Die Mitglieder der Gruppen

1. Supplier

Um möglichst vor dem offiziellen Verkaufsdatum einer Musikproduktion (sogenanntes Street Date) an die entsprechenden Tonträger zu gelangen, suchen die MP3-Gruppen gezielt nach Mitgliedern, die beruflich mit der Musikbranche in Berührung kommen. Hierbei handelt es sich in erster Linie um Mitarbeiter von Plattenfirmen, Mastering-Studios, Presswerken und Plattenläden. Letztere haben Zugang zu Vorabveröffentlichungen, da die Plattenfirmen bzw. ihre Vertriebe den Handel bereits einige Wochen vor dem offiziellen Verkaufsstart zu Promotionzwecken mit den aktuellen Produktionen bemustern.

„Promo-Copies" oder „Promos" werden ebenfalls an Radiostationen, TV-Sender und Musikzeitschriften geschickt, weshalb auch deren Mitarbeiter als Supplier in Frage kommen.

Bedingt durch die weite Verbreitung von Promo-Kopien sind die meisten aktuellen Musikproduktionen einige Wochen vor dem „Street Date" in der MP3-Szene zu finden. Allerdings gibt es kleinere Unterschiede zum finalen Produkt, der sogenannten Retail-Version. Häufig fehlt das endgültige Cover und das Material wurde von dem Tonträgerunternehmen auf einen handelsüblichen Rohling gebrannt. Auch kommt es vor, dass die Titel klanglich noch nicht den letzten Schliff erhalten haben.

---

849 Zum Vergleich der verschiedenen Formate siehe *Zota/Buschmann*, **c't** 23/2000, S. 152 ff.
850 Moviez (Szenesprache) = Filme; siehe oben Teil 1, E. III.

Sofern MP3-Gruppen Promo-Kopien veröffentlichen, werden die Releases entsprechend gekennzeichnet. So tragen Szene-Veröffentlichungen von Promo-Kopien, die nicht die kompletten Stücke, sondern nur Teile derselben enthalten, beispielsweise die Bezeichnung „Snippet-Promo Copy“.

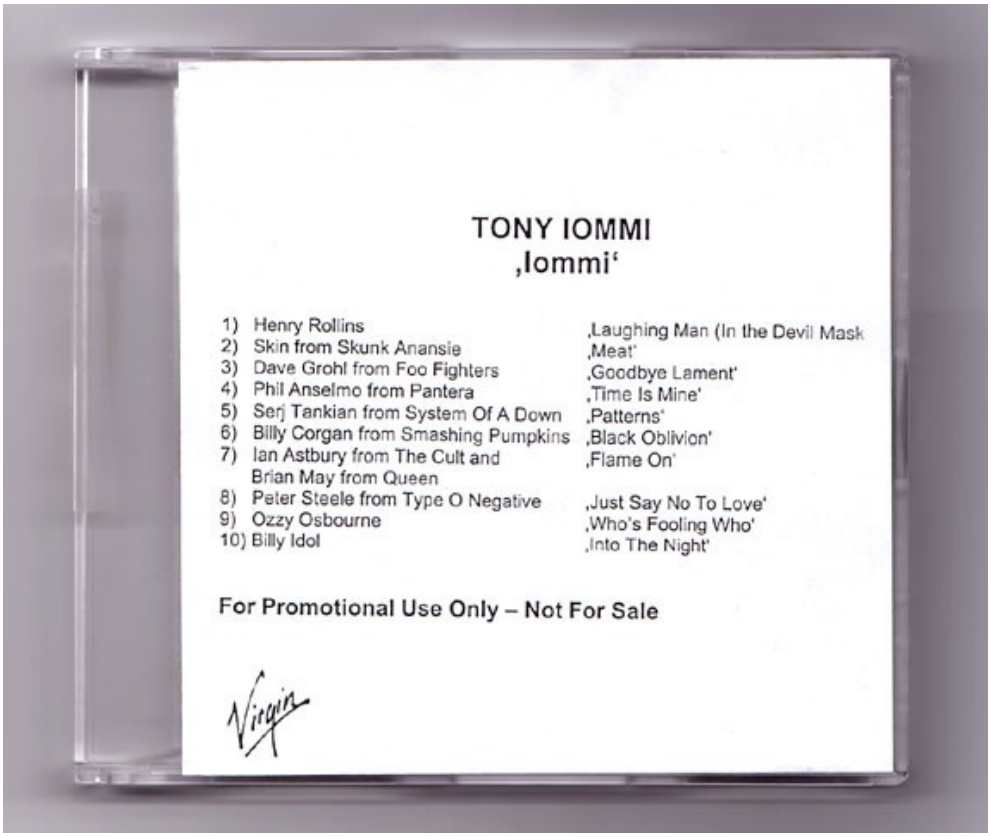


Abbildung 93 – Promo- Kopie eines CD-Albums

Abbildung 94 – MP3-Release einer Promo-CD

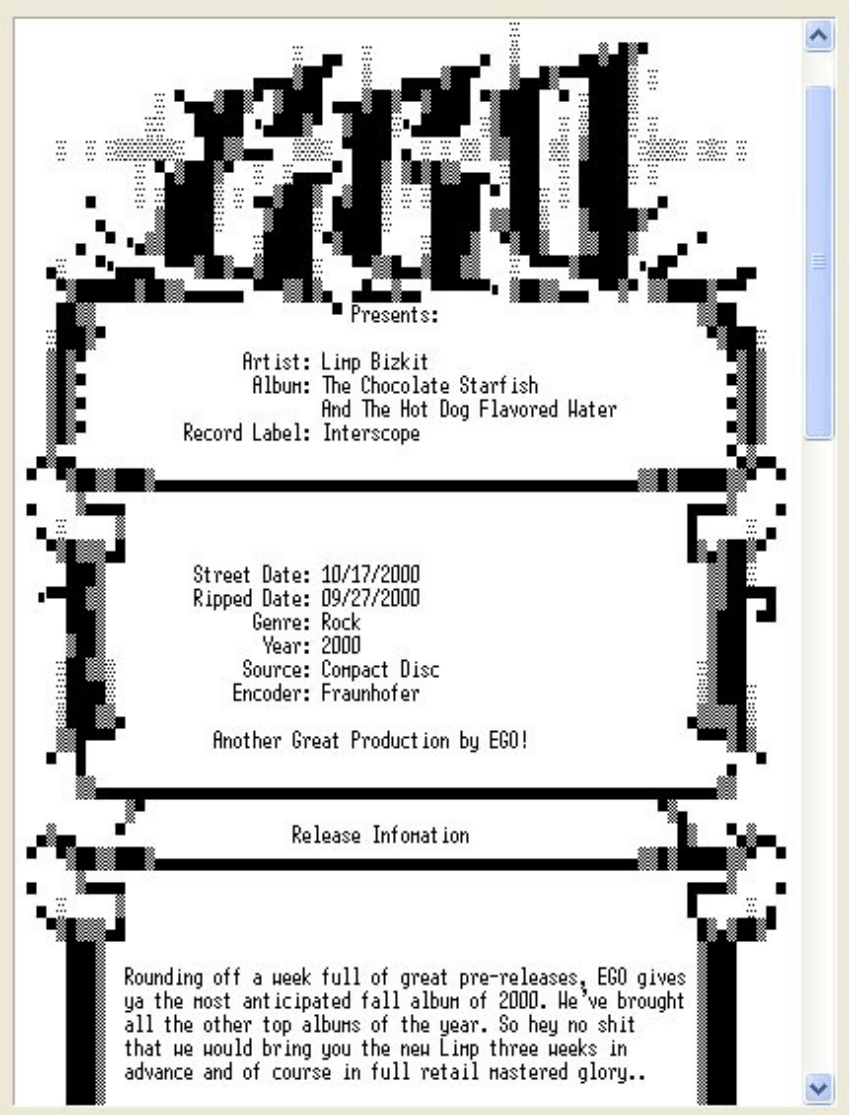


Abbildung 92 – Auszug aus einer NFO-Datei („Street Date“)

2. Ripper / Encoder

Hat der Supplier eine CD besorgt, müssen deren Titel zunächst in WAV-Dateien umgewandelt und auf die Festplatte geschrieben werden. Hierfür ist der Ripper zuständig. Mittels spezieller Programme wie *Audiograbber* oder *Exact Audio Copy (EAC)* versucht er, die Daten möglichst 1:1 auf seinen Rechner zu kopieren. Dies ist trotz der bei der Audio-CD verwendeten Digitaltechnik nicht ohne weiteres gewährleistet, denn der Red-Book-Standard, der die Audio-CD-Spezifikation beschreibt[851], sieht für das Format keine so aufwändige Fehlerkorrektur vor, wie man sie beispielsweise von der Daten-CD-ROM (Yellow-Book-Standard) kennt. Das bedeutet, dass ein Auslesevorgang durchaus als erfolgreich quittiert werden kann, obwohl – z.B. aufgrund von Kratzern oder Verunreinigungen

[851] Das Red Book enthält eine Spezifikation des CD-Patentinhabers *Philips*, die mittlerweile als deutsche Norm übernommen wurde. Unter anderem wird darin festgelegt, dass die Daten auf einer Audio-CD eine Samplingrate von 44,1 kHz sowie eine Auflösung von 16 Bit haben und stereokompatibel sein müssen.

auf der CD-Oberfläche – nicht alle vorhandenen Daten übertragen wurden. Auch schnelles Auslesen bedeutet häufig eine hohe Fehlerquote.

Ist es dem Ripper gelungen, ein fehlerfreies Abbild der CD-Daten zu erstellen, müssen die WAV-Dateien in möglichst guter Qualität ins MP3-Format überführt werden. Um den bestmöglichen Kompromiss zwischen Dateigröße und Qualität zu erzielen, hat man sich in der MP3-Szene auf die Herstellung von MP3s mit einer Bitrate von 192 KBit/s geeinigt. Hier liegt das Verkleinerungsverhältnis immerhin noch bei 7:1 und die Audioqualität ist über jeden Zweifel erhaben.

Welches Codec der Encoder einer Gruppe zum Kodieren der WAV-Dateien benutzen darf, ist ebenfalls innerhalb der Szene festgeschrieben. Sehr beliebt ist neben dem Original-Codec des *Fraunhofer-Instituts* das Freeware-Codec *LAME*. Zuvor nutzten viele Gruppen das sogenannte *Radium*-Codec, ein von der mittlerweile aufgelösten Audiowarez-Gruppe *Radium* modifzierter *Fraunhofer*-Algorithmus. Einem Cracker der Gruppe war es gelungen, die Encoding-Routine so zu optimieren, dass das Codec je nach Signal und Prozessor bis zu 12% schneller arbeitete.

Im Gegensatz zu den Warez-Gruppen ist die strenge Arbeitsteilung innerhalb der MP3-Gruppen nicht mehr erforderlich, da das Herstellen eines Releases kein besonderes Fachwissen mehr erfordert. Ein gewisses Geschick im Umgang mit Soft- und Hardware ist nur dann erforderlich, wenn die zu „rippenden" Audio-CDs mit Kopierschutzsystemen versehen sind, oder wenn Aufnahmen kodiert werden sollen, die auf Vinyl vorliegen oder im Radio gesendet werden. Moderne Kopierschutzsysteme für Audio-CDs sollen in erster Linie das Abspielen auf einem PC verhindern, weshalb das „Rippen" einzelner Stücke über ein CD-ROM-Laufwerk häufig fehlschlägt.[852] Da sich die CDs jedoch auf herkömmlichen Audio-CD-Playern abspielen lassen, benötigt der Ripper lediglich einen CD-Spieler mit Digitalausgang, eine Soundkarte mit Digitaleingang und eine WAV-Aufnahmesoftware, um eine 1:1 Kopie der geschützten Musikdaten zu erstellen. Denkbar ist auch eine analoge Überspielung der Musikstücke. Hierbei verbindet der Ripper den Analogausgang des CD-Spielers mit dem Analogeingang seiner Soundkarte und nimmt das anliegende Signal mit einer entsprechenden Software auf. Allerdings ist dabei die Qualität abhängig von der Güte der verwendeten Hardware. Bei Soundkarten oberhalb der 200-€-Grenze sind die Analog/Digital-Wandler und die klangverarbeitenden Bauteile jedoch so hochwertig, dass kaum hörbare Unterschiede zur reinen Digitalkopie bestehen.

Wie bei der Erstellung einer analogen CD-Kopie wird verfahren, wenn Aufnahmen von Vinyl oder aus dem nicht-digitalen Rundfunk kodiert werden sollen. Entscheidend für den Klang des Endprodukts ist hier die Qualität des Plattenspielers bzw. des Tuners[853]. Aufnahmen aus dem Digitalradio, wie es mittlerweile flächendeckend über Satellit zu empfangen ist, können ohne den Zwischenschritt der analogen Wandlung über eine Soundkarte mit Digitaleingang direkt in den Rechner transportiert werden. Noch einfacher ist das Abspeichern von Musikstücken, die über Web-Radios[854] gesendet

---

852 Ausführlich zu den gängigen Audio-CD-Kopierschutzverfahren siehe unten Teil 3, C. II. 2. a).
853 Tuner (engl.) = Rundfunkempfänger.
854 Zu nennen sind die in der MP3-Szene beliebten *Shoutcast*-Streams (http://www.shoutcast.com), mittels derer Musik in annähernder CD-Qualität über das Internet an die MP3-Abspielsoftware *WinAmp* gesendet wird.

werden. Mit speziellen Programmen[855] lässt sich der „Stream“ auf die Festplatte umleiten und wird dort in eine WAV-Datei geschrieben.

3. Packer

Sind sämtliche Titel einer Produktion fertig kodiert, müssen sie zunächst mit korrekten ID3-Tags versehen werden. Wie bereits erwähnt, enthalten diese Anhängsel Zusatzinformationen zu den Dateien; besonders wichtig für die Gruppen ist es, sich im Feld „Comment“ mit dem Gruppennamen zu verewigen. Eine Kurzform des Gruppennamens – meist aus drei Buchstaben bestehend – befindet sich außerdem am Ende des Namens jeder Datei, die dem Release zugehört („Group Initials“).

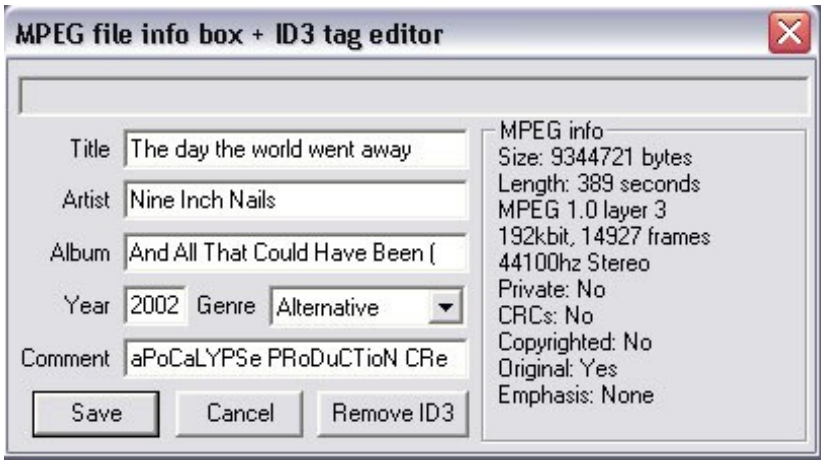


Abbildung 95 – Inhalt eines typischen ID3-Tags (*WinAmp*)

Des Weiteren müssen den MP3-Dateien einige Dateien beigefügt werden, bevor sie veröffentlich werden dürfen. Hierzu gehört auch eine NFO-Datei, wie sie in der Warez-Szene üblich ist.

Zu jedem MP3-Release gehört darüber hinaus eine M3U-Datei. Hierbei handelt es sich um eine sogenannte Playlist, die durch Doppelklicken bewirkt, dass sämtliche MP3-Dateien des Releases in der richtigen Reihenfolge in die MP3-Abspielsoftware *WinAmp* geladen werden. Das M3U-File dient somit der Bequemlichkeit der Nutzer.

Schließlich wird eine SFV-Datei erstellt, wenn das Release komplett zusammengestellt ist. Wie bei den Warez-Releases soll es gewährleisten, dass der Nutzer per Doppelklick überprüfen kann, ob er das Release komplett heruntergeladen hat, oder ob ihm noch Teile fehlen.

Manchmal entschließen sich die Gruppen, zusätzlich eingescannte Cover bzw. Booklets zu veröffentlichen. Diese werden den anderen Dateien meist im JPG-Format beigefügt und ermöglichen es dem Nutzer, sich das entsprechende Cover auszudrucken.

---

[855] Eine Beschreibung findet sich in Teil 3, C. II. 3.

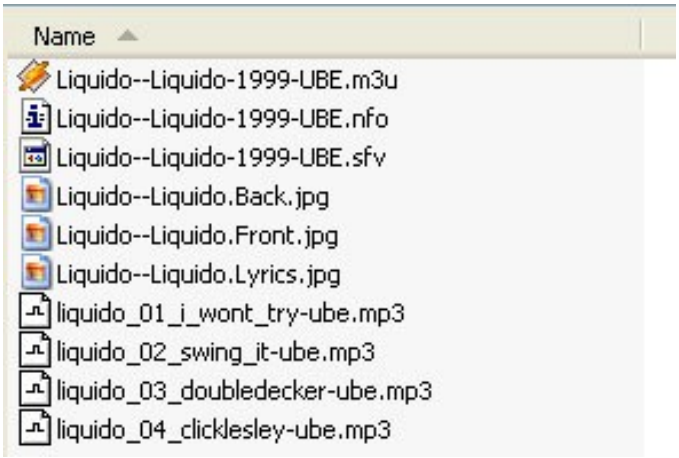


Abbildung 96 – komplettes MP3-Release

4. Andere Gruppenmitglieder

Auch in MP3-Gruppen gibt es Leader, die koordinative Aufgaben übernehmen, Kuriere, die die Releases auf möglichst vielen FTP-Servern verteilen und Serveradministratoren (Siteops), die den Betrieb gruppeneigener FTP-Server gewährleisten. Unterschiede zu den Warez-Gruppen lassen sich – abgesehen von der Art der digitalen Ware – nicht ausmachen.

V. Szenemitglieder ohne Gruppenzugehörigkeit

1. Nutzer von Peer-to-Peer-Filesharing-Systemen (P2P-Systeme)

Obwohl sie mit der eigentlichen Szene – den MP3-Gruppen – kaum in Berührung kommen, stellen die Nutzer von Online-Tauschbörsen die bei weitem größte Gruppe der MP3-Downloader dar. Mittels spezieller Programme schließen sich täglich Millionen von Internetnutzern über Kontinente hinweg zusammen, um MP3-Dateien zu tauschen, die sich auf der Festplatte des jeweils eigenen Rechners befinden.

Je nachdem wie das verwendete Tauschprogramm konfiguriert bzw. konstruiert ist, bietet der Herunterladende gleichzeitig auch Dateien für die anderen Nutzer des Netzwerkes zum Tausch an. Auf die am weitesten verbreiteten P2P-Systeme wird im Abschnitt VII. dieses Teils ausführlich eingegangen.

2. Leecher und Trader

Unzählige illegale MP3-Downloadangebote auf WWW-Seiten bedienen eine Schar von Nutzern, die entweder nicht bereit oder in der Lage sind, spezielle Tauschsoftware einzusetzen. Somit kommen sie in den Genuss von nichtlizenzierter Musik, ohne eine Gegenleistung dafür zu erbringen.

Anderes gilt für die relativ kleine Gruppe von MP3-Tradern, die sich hauptsächlich in IRC-Channels aufhalten. Dort knüpfen sie Kontakte mit anderen Tradern, um dann über eigene FTP-Server Dateien auszutauschen.

3. Profit-Pirates

Piraten, die aus ihrem Tun finanziellen Profit ziehen, nutzen hauptsächlich das WWW. In den meisten Fällen richten sie Downloadseiten ein, die mit Bannerwerbung finanziert werden. Hierbei kann es sich je nach Besucherzahl der Seiten um eine äußerst lukrative Tätigkeit handeln: Nach Schätzungen der *IFPI* verdienten die Betreiber der größten deutschen illegalen MP3-Seite im Jahr 2000 bereits 1.500 US-Dollar pro Tag.[856]

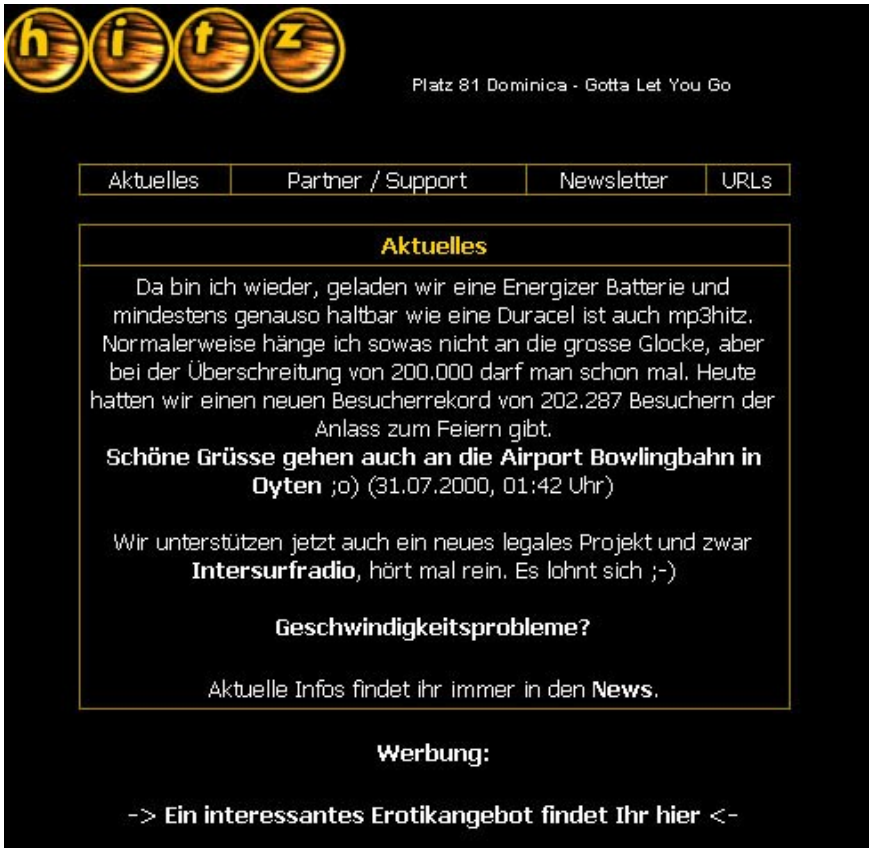


Abbildung 97 – große deutschsprachige MP3-Downloadseite

Seltener findet man Kaufangebote über selbstgebrannte MP3-Compilation-CDs oder Angebote bei Online-Auktionshäusern.

WELCOME TO FSG – FTP SERVER GROUP

TERMS AND CONDITIONS:

A)I) FTP SERVER (operated by yourself)
HARD DRIVE SPACE FROM 3 GIGA OR MORE IS ACCEPTABLE
INTERNET CONNECTION MUST BE "UPSTREAM MORE THAN 20Kb/S"
MIRC OR ICQ AVAILABILITY TO CHAT PERSON TO PERSON

II) AVAILABILITY TO SERVE WITH YOUR SERVER OUR USERS(WE HAVE LOT OF
USERS 200.000 – 500.000 PEOPLE DAILY WANT TO CONNECT SO TRAFFIC ISN'T
PROBLEM AND SO IS CASH THEN ;) IMPRESSIONS AND CLICKS

---

856 Gemäß einer Wortmeldung des ehemaligen *IFPI*-Justitiars *Rasch* auf der Informationsveranstaltung des *BKA* "Bekämpfung der Kriminalität im Internet" am 15. und 16.02.2000 in Wiesbaden.

|FSG| MEMBERS === YOUR WORKING : MAKING AND CHANGING ACCOUNT DAILY OR PER 2 DAYS. THAT'S WHY U NEED MIRC OR ICQ THAT WE CHAT(UPDATE)ABOUT PASSES.
MINIMUM ACCOUNTS THAT U WILL HAVE TO MAKE IS 3 and speed per user 5kb/s
More accounts u provide more cash and hits to your site u can gain
More HARD DRIVE FILLED and more ACCOUNTS(people will visit u often) (we will directly send them to U)

U WILL MAKE ONE DIRECTORY – EXAMPLE: "FSG MEMBERS" AND U WILL PUT ADRESSES OF FTP'S THERE. YOU MUST HAVE ALL THINGS IN THIS POINT TO GET IN OUR TEAM

B)I) WANNA EARN MONEY FROM "FSG"
U MUST KNOW HOW TO MAKE PAGES
AND U WILL GET ACCESS SOON ON OUR DOMAIN .COM NAME WHICH WILL COME SOON
THERE U WILL HAVE TO MAKE LEGAL PAGE AND PUT BANNERS UP
SO U WILL EARN MONEY THROUGH YOUR SERVER AND U WILL EXPAND
ALL ADVICES PUTING ON OUR PAGE IS FREE U WILL GET YOUR LINK IN OUR PAGE
WE HAVE NOW DAILY 10.000 HITS AND MORE ....AND U WILL BE ORIENTED AS A LINK IN OUR BIG PAGE WHEN WE GET "COM" """ LEGAL PAGES """" ONLY

!! IF U CAN'T MAKE PAGE WE CAN DO IT FOR YOU !! FREE ALSO
ALL ADVICES ARE FREE AND ALL IS FREE

U WILL JUST NEED TO MAKE ACCOUNTS DAILY OR IN 2 DAYS(CHANGING THEM)
ALL MUST BE LEECH = FREE; NO RATIO SITES ALLOWED
MAKE PAGES WE WILL PUT YOU UP AND TELL U HOW TO EARN CASH
AND WE WILL SEND OUR USERS TO YOUR PLACES WHICH WILL GET YOU YOUR CASH

ANY QUESTIONS AND JOINING : E-MAIL TO lestad@iname.com

INCOMING!! 1 MIRRORING IN LATE JANUARY AND 2 COMPUTERS AND 2 LINKS FROM ME
SO WE WILL NOW HOST IN MARCH 3 OUR COMPUTERS = 45 GIGA HARD DRIVES MIRRORING
1 IN JANUARY 10 GIGA AND SOME OTHER STUFF OF HIS OWN

REGARDS AND HOPE THAT WE EXPAND AND EARN SOME EXTRA MONEY FOR OUR HOBBY

Hool|FSG| – General Administrator Manager of FSG

Abbildung 98 – Werbung für eine Profit-Pirate-Group

VI. Kommunikationswege

Die Kommunikation innerhalb der MP3-Gruppen findet auf den gleichen Wegen statt wie in der Warez-Szene. Folglich kommt dem IRC die größte Bedeutung für die Verständigung und Koordination der Gruppenmitglieder zu. Allerdings werden aufgrund des latenten Verfolgungsdrucks, der von der Warez-Szene auf die MP3-Szene ausstrahlt, bevorzugt private IRC-Server genutzt, die kaum aufzuspüren sind.

Für die Kommunikation der Nutzer ohne Gruppenzugehörigkeit werden alle verfügbaren Dienste genutzt, zu nennen sind vorrangig öffentliche IRC-Server, Instant-Messaging-Systeme und die in Tauschsoftware integrierten Chat-Clients.

VII. Wege der illegalen Musikdistribution

1. Peer-to-Peer-Filesharing-Systeme (P2P-Systeme)

Mit der enormen Popularität des Musiktauschprogramms *Napster* wurde die Weltöffentlichkeit erstmals auf ein P2P-System aufmerksam. Die Geschichte von *Napster* begann 1999, als der US-Student *Shawn Fanning* ein Programm schrieb, um innerhalb des Netzwerkes seiner Universität komfortabel MP3-Dateien auszutauschen.

Das Prinzip hinter dem ursprünglichen *Napster* ist so einfach wie genial: Jeder Nutzer, der am Tausch teilnehmen möchte, installiert sich den *Napster*-Client, eine FTP-ähnliche Software mit integrierter

Suchfunktion, und gibt den Zugriff auf eine gewisse Anzahl seiner MP3-Dateien frei. Der Betreiber des Netzwerkes richtet schließlich einen zentralen *Napster*-Server ein, mit dem sich die Clients automatisch verbinden. Sobald sich ein Client beim Server anmeldet, wird eine Liste der bereitgestellten MP3-Dateien zum Server übermittelt, wo sie für die Verweildauer des Nutzers im Netzwerk in einer großen Datenbank abgelegt wird. Diese Datenbank kann von jedem anderen Nutzer des Netzwerkes anhand der Suchfunktion seines Clients komplett nach den Namen von MP3-Dateien durchsucht werden. In einer Trefferliste kann er dann auswählen, welches Musikstück er herunterladen möchte.

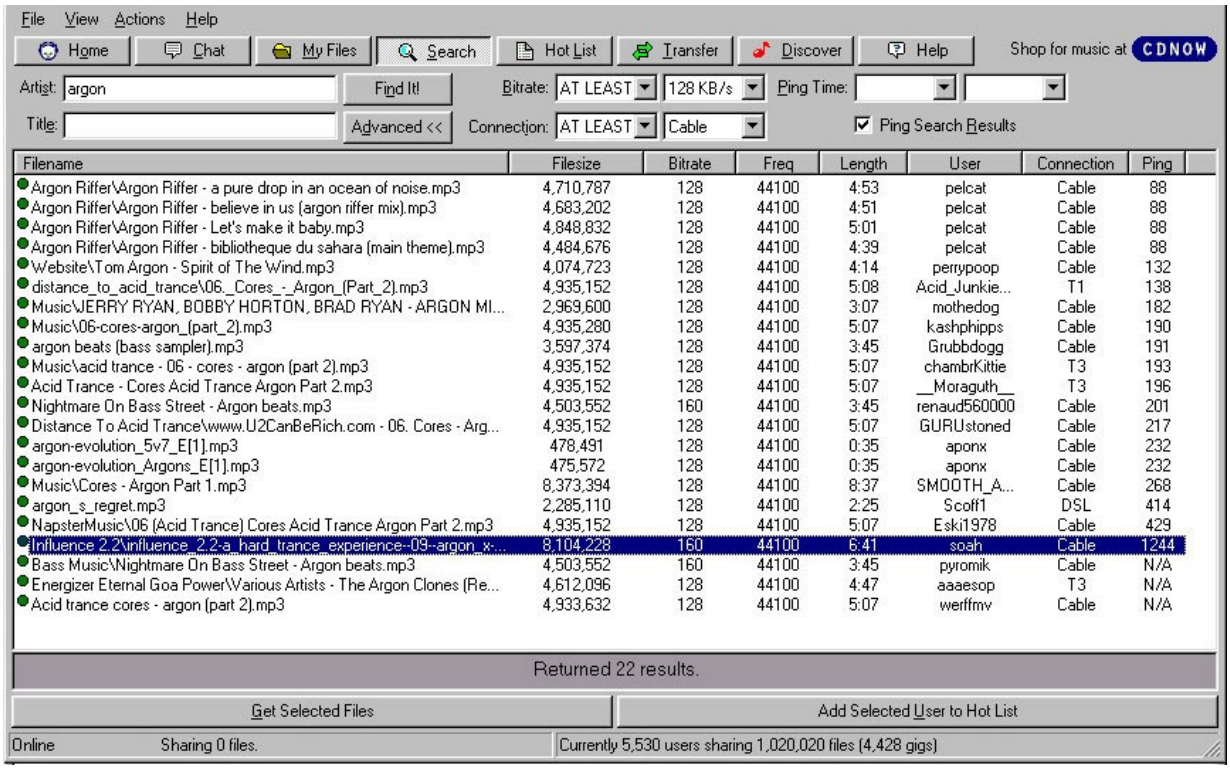


Abbildung 99 – Trefferliste bei *Napster*

Die Datenübertragung erfolgt dann nicht mehr über den Server, sondern „Peer-to-Peer", d.h. direkt von Nutzer zu Nutzer. Der Server übernimmt somit eine reine Vermittlungs- bzw. Verwaltungsfunktion („Vermittlungsstelle"), er ist nicht in die Datenübertragung involviert. Netzwerktopologien ohne dedizierte Client-Server-Architektur werden als Peer-to-Peer-Netze bezeichnet[857].

Neben dem enormen Angebot an Dateien liegt einer der größten Vorteile des P2P-Filesharing darin, dass die Dateien nicht mehr zentral und kostenintensiv von einem Webhosting-Provider bereitgestellt werden müssen, sondern nur Speicherplatz auf den Festplatten der Teilnehmer in Anspruch nehmen.

---

[857] Zu den verschiedenen P2P-Topologien siehe *Minar*, **O'Reilly Network,** 14.12.2001.

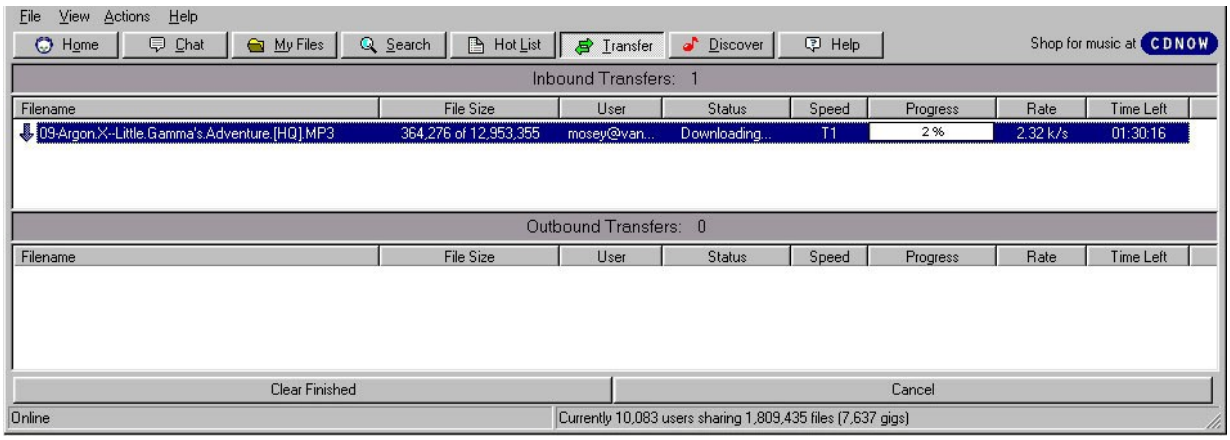


Abbildung 100 – Transfer-Fenster von *Napster*

Napster wurde zu einem enormen Erfolg. Das Programm verbreitete sich rasend schnell im Netz und mit der Gründung von *Napster.com* sowie der Einrichtung von zahlreichen leistungsfähigen *Napster*-Servern wurden weitere Schritte unternommen, die dem Musiktausch im Internet zu neuen Höhen verhalfen. Im Herbst 2000 war die Software auf fast jedem dritten ans Internet angeschlossenen PC installiert und laut Unternehmensangaben griffen auf *Napster* bis zu einer Million User gleichzeitig zu. Zum Vergleich: Auch *AOL* als größter ISP der Welt hat in Spitzenzeiten kaum mehr als 1,5 Millionen User gleichzeitig im Netz.[858] Im Herbst 2000 – nach der Einführung eines *Napster*-Clients für das *Apple Macintosh* Betriebssystem – hatte man als *Napster*-User Zugriff auf ca. 1,5 Millionen Musikdateien.

Mittlerweile gibt es *Napster* in seiner bisherigen Form nicht mehr. Nach mehreren einstweiligen Verfügungs- und Hauptsacheverfahren der Recording Industry Association of America (*RIAA*) gegen *Napster* haben sich die Betreiber Anfang 2001 entschieden, die Server abzuschalten.

Mit dem Verschwinden des ursprünglichen *Napster* ging der Online-Musiktausch mittels P2P-Systemen keineswegs zuende. Neue P2P-Clients breiteten sich ebenso schnell aus wie *Napster* seinerzeit, und erstmals kamen auch dezentrale P2P-Systeme auf den Plan, die nicht mehr auf einen zentralen Vermittlungsserver angewiesen sind. Die Suchabfragen funktionieren hier nach dem Schneeballsystem: Jeder Client nimmt Verbindung zu einer bestimmten Anzahl anderer Clients auf und richtet seine Suchanfrage an diese. Diese wiederum beantworten die Suchanfrage und leiten sie direkt an die mit ihnen verbundenen Clients weiter. Jeder Client, der eine Suchanfrage erhält, sendet seine Antwort zum Ursprung der Abfrage zurück. Um zu verhindern, dass jedes Frage- bzw. Antwortpaket endlos im Netz umherirrt, wird sie mit einem sogenannten TTL-Wert (Time to Live) versehen, den jeder Verbindungspartner um 1 vermindert.[859]

Die P2P-Systeme der zweiten Generation warten darüber hinaus mit neuen Funktionen auf, die den Dateitausch noch komfortabler und vielseitiger machen: Beinahe alle neuen Tauschsysteme sind

---

[858] *Gunther*, **Telepolis** vom 24.09.2001.
[859] So im *Gnutella*-Netz, vgl. *Möller*, Kopieren ohne Grenzen, **c't** 6/2001, S. 151.

nicht mehr auf den Tausch von MP3-Dateien beschränkt, sondern ermöglichen auch den Download von Filmen, Texten, Software etc.. Mittels detaillierter Suchmasken können die Nutzer ihre Anfragen eingrenzen, um wertlose Treffer zu vermeiden. In den Trefferlisten selbst finden sich nicht mehr nur die Dateinamen der gefundenen Stücke, sondern auch Angaben über die beim Kodieren verwendete Bitrate, Länge des Musikstücks, Größe der Datei sowie die Einträge aus dem ID3-Tag des MP3s. Vereinzelt erhält man sogar Informationen über die Bandbreite der Internetzugänge der Nutzer, deren Dateien in der Trefferliste erscheinen.

Die meisten Systeme bieten darüber hinaus die Möglichkeit, mit anderen Nutzern der Tauschbörse zu chatten und den Bestand der von ihnen freigegebenen Dateien zu durchsuchen. Die am stärksten für den MP3-Tausch genutzten P2P-Systeme der zweiten Generation werden nachfolgend kurz dargestellt.

a) *FastTrack*-Netz

Das *FastTrack*-Filesharing-System, das bei den beliebten Clients *KaZaA* (bzw. *KaZaA Lite*) und *Grokster* zum Einsatz kommt, basiert auf einer Hybrid-Topologie aus zentralen und dezentralen Bestandteilen: Die meisten angeschlossenen Clients stehen in einer zentralisierten Beziehung zu einer sogenannten Supernode, also einem Server, der Suchanfragen entgegennimmt und weiterleitet. Allerdings handelt es sich hierbei im Gegensatz zum *Napster*-Prinzip nicht um dezidierte Server, sondern die Supernodes sind wiederum in einem dezentralisierten Netzwerk miteinander verbunden, in dem Suchanfragen weiter-geleitet werden. Welcher Rechner als Supernode fungiert, ist abhängig von seiner Anbindung. Schnell angebundene Rechner werden automatisch zu Supernodes, es sei denn, der Besitzer des Rechners unterbindet dies in der Konfiguration seines Clients.

Der Tausch im *FastTrack*-Netz ist nicht auf MP3-Files beschränkt, die Suchabteilung gliedert sich in die Bereiche „Audio, Video, Images, Documents“ und „Software“ auf.

Die *FastTrack*-Clients unterstützen das gleichzeitige Herunterladen einer Datei von mehreren Nutzern. Beim sogenannten Multi-Source-Download werden Dateifragmente aus verschiedenen Quellen simultan heruntergeladen und am Zielort in der richtigen Reihenfolge zusammengesetzt, was gegenüber der herkömmlichen Downloadmethode für einen beträchtlichen Geschwindigkeitsgewinn sorgt, sofern die gleiche Datei bei vielen Nutzern bereitliegt. Ebenso unterstützen die *FastTrack*-Clients die Funktion Download-Resume, können also mit dem Download unverändert fortfahren, falls dieser unterbrochen wurde, weil beispielsweise der bereitstellende Nutzer das *FastTrack*-Netz verlassen hat, oder die Internetverbindung des Herunterladenden getrennt wurde.

In die Clients integriert sind darüber hinaus eine Chat-Funktion und eine universelle Medienvorschau, mit der sich der Nutzer die Dateien ansehen bzw. anhören kann, während diese noch heruntergeladen werden.

b) *Gnutella*-Netz

Beim *Gnutella*-Netz handelt es sich um das bekannteste rein dezentrale P2P-Netz. Wie bereits beschrieben, fungiert jeder angeschlossene Rechner gleichzeitig als Client und als Server. Programme

wie *Bearshare, Gnotella, Gnucleus* oder *LimeWire* basieren auf dem *Gnutella*-Protokoll und sind weit verbreitet. Durch die Unabhängigkeit von zentralen Servern ist das gesamte Netzwerk zwar schwer verwundbar, allerdings dauern die Anmeldung an das Netzwerk und das Stellen von Suchanfragen im Vergleich zu zentralen Netzwerken und Hybridnetzwerken um ein Vielfaches länger.

Auch im *Gnutella*-Netz lassen sich alle Arten von Dateien tauschen. Die meisten Clients unterstützen außerdem Multi-Source-Download sowie Download-Resume und haben eine Chat-Funktion implementiert.

Das Angebot an Dateien ist deutlich geringer als im *FastTrack*-Netzwerk. Da dessen Zukunft jedoch aus wirtschaftlichen und rechtlichen Gründen ungewiss ist, und der freie Dateitausch über dieses Netz möglicherweise bald ein Ende hat, kann dem *Gnutella*-Netz in Zukunft eine noch größere Bedeutung zukommen.

c) *eDonkey2000*

Populär geworden als Programm für den Download von ganzen Kinofilmen[860], wird *eDonkey2000* mittlerweile auch für den Tausch von MP3-Dateien genutzt. Neben einzelnen MP3-Titeln werden über *eDonkey2000* bevorzugt ganze Alben in gepackter Form getauscht. Die Netzwerktopologie ähnelt in Grundzügen der des *FastTrack*-Netzwerkes. Allerdings werden hier keine leistungsfähigen Clients automatisch zu Supernodes erklärt, sondern es gibt eine spezielle Serversoftware, den *eDonkey*-Server, der von jedermann betrieben werden kann. Somit ist das *eDonkey*-Netzwerk davon abhängig, dass möglichst viele Freiwillige einen Server betreiben. Die Server sind nicht miteinander verbunden, und ein einzelner Server dient in der Regel als Verbindungspunkt für mehrere tausend Clients.

Suchanfragen eines Clients richten sich daher zunächst nur an den mit ihm verbundenen Server. Dieser stellt anhand der bei ihm verwalteten Dateilisten der restlichen verbundenen Clients eine Trefferliste zusammen, die als Antwort zurückgesendet wird. Um eine Suchanfrage auszuweiten, kann der Nutzer diese auf andere Server ausdehnen. Auf welche Server die Anfrage ausgedehnt wird, hängt von einer lokalen Liste ab, die der Nutzer in seinen Client einspeisen muss. Ständig aktualisierte *eDonkey*-Serverlisten gibt es auf zahlreichen WWW-Seiten zum Download.

Wie die meisten anderen P2P-Clients der zweiten Generation unterstützt auch *eDonkey2000* Multi-Source-Downloading, allerdings mit einer Besonderheit: Der herunterladende Anwender wird gezwungenermaßen zum Anbieter der Dateifragmente, die er bereits auf seine Festplatte laden konnte. Diese als Partial Sharing bezeichnete Funktion basiert auf dem Multisource File Transfer Protokoll (MFTP) und lässt sich nicht ohne Eingriffe in den Programmcode abschalten.[861]

---

[860] Vgl. *Zota*, Moviez in Hülle und Fülle, **c't** 6/2002, S. 158 ff.

[861] Eine weitere Besonderheit schließt die Lücke zwischen WWW und P2P. Es besteht die Möglichkeit, über das Klicken eines Hyperlinks auf einer Webseite einen Download per eDonkey2000 zu starten. Vorausgesetzt, der *eDonkey*-Client ist installiert und aufgerufen, muss der Link lediglich mit „e2dk://|file|“ beginnen und mit dem Namen der verknüpften Datei sowie einem mehrstelligen Zuordnungswert - sogenannter Hashwert - enden (z.B.: ed2k://|file|test.avi|734334516|720dbd678334534b225a610e03445435ffad|/); zur Funktionsweise siehe http://magnet-uri.sourceforge.net/magnet-draft-overview.txt.

d) Andere P2P-Systeme

Bei Clients wie *WinMX, AudioGnome* und *Rapigator* handelt es sich um *Napster*-Klone. Die Programme, die auf einem weiterentwickelten *Napster*-Protokoll basieren, greifen auf sogenannte *OpenNap*-Server zu, die hauptsächlich von Privatleuten betrieben werden. Die Beschränkung auf MP3-Dateien wurde weitgehend aufgehoben, auch können sich die *OpenNap*-Server untereinander verbinden.

Direct Connect ist ein P2P-System, das sehr stark an den Dateitausch mittels Ratio-FTP-Servern erinnert. Eine Struktur erhält der Tausch durch sogenannte Hubs, die sich anhand der unterschiedlichen Interessen der Tauschwilligen unterscheiden. *Direct Connect* Hubs gewähren in der meisten Fällen nur solchen Nutzern Einlass, die auf ihrer Festplatte eine mehrere Gigabyte umfassende Menge Tauschmaterial freigegeben haben. Über integrierte Interaktionsmodule können die Nutzer miteinander chatten und Einsicht in die angebotenen Dateien des virtuellen Gegenübers nehmen.

Da die IP-Adressen der Tauschpartner bei fast allen Tauschbörsen nicht offen einsehbar sind, muss man sich anderer Programme bedienen, um diese ausfindig zu machen. So ermöglicht die in *Windows* integrierte netstat.exe das Ausführen des TCP/IP Netstat-Befehls[862], der bewirkt, dass alle aktuellen Verbindungen eines Rechners mitsamt IP-Adresse und Port aufgelistet werden. Downloads von anderen *FastTrack* Clients laufen über Port 1214, bei *Gnutella* ist es in den meisten Fällen Port 6346, und bei *eDonkey2000* Port 4662. Bei letzterem kann man die IP-Adressen der Tauschpartner auch innerhalb des *eDonkey*-Clients herausfinden, indem man den entsprechenden User zu seiner „Friendlist" hinzufügt. Allerdings erscheint die IP-Adresse in der Friendlist als Hexadezimal-Wert (z.B. 954C0C04); dieser lässt sich jedoch leicht in das gebräuchlichere dezimale Format (z.B. 149.76.12.4) umwandeln.

Die Vorläufer der nächsten Generation von P2P-Applikationen sind verschlüsselte Systeme wie *Filetopia* und *Freenet*. Während bei allen anderen P2P-Systemen die IP-Adressen der Tauschenden offen liegen, ermöglichen sie erstmals einen weitgehend anonymen Datenaustausch, was den Copyright-Wächtern in Zukunft die Suche erschweren dürfte. Allerdings sind die Systeme im jetzigen Stadium noch sehr träge und teilweise unkomfortabel in der Bedienung.

Beim zentralen P2P-Filesharing-System *Filetopia* wird die Kommunikation zwischen den Usern verschlüsselt, und für die Authentifizierung kommt Public-Key-Kryptographie zum Einsatz. Um die IP-Adressen zu verschleiern, wird die Verwendung von Stellvertreter-Rechnern (sogenannten Bouncern) unterstützt, die die Datenpakete auf Umwegen zum Empfänger leiten. Zusätzlich kann der Nutzer verschlüsselt chatten, E-Mails versenden und Instant Messaging betreiben. Das dezentral organisierte *Freenet* setzt ebenfalls auf starke Verschlüsselung und eine komplexe Routingmethode für die Datenpakete über mehrere Relaisstationen, die eine Verfolgung beinahe unmöglich machen.

---

[862] Es genügt, in einem DOS-Fenster den Befehl „netstat –a" einzugeben.

Abschließend ist zu erwähnen, dass MP3-Gruppen ihre Releases nicht in Tauschbörsen einspeisen. Finden sich dort Dateien, die Rückschlüsse auf Gruppen zulassen, wurden sie mit großer Wahrscheinlichkeit von Nutzern bereitgestellt, die auch Zugang zu den FTP-Servern oder IRC-Channels der Gruppen hatten.

2. WWW

Vor der massenhaften Nutzung von Tauschbörsen kam dem WWW die bedeutendste Rolle bei der nichtlizenzierten Verbreitung von Musikdateien zu. Auch heute noch gibt es unzählige Webseiten von Privatleuten und Profit-Pirates über die MP3-Dateien zum freien Download angeboten werden. Da von Seiten der Anti-Piraterie-Verbände und der Provider verstärkt gegen diese Angebote vorgegangen wird, entwickeln die Betreiber der Piratenseiten immer raffiniertere Methoden, um unentdeckt zu bleiben. In der Regel liegen die MP3-Dateien auf einem anderen Server als die Webseiten, und über Hyperlinks werden die Besucher der Webseiten zu den Dateien weitergeleitet. Um zu verhindern, dass Suchprogramme der Webhosting-Provider die Dateien aufspüren und löschen, tarnen die Piraten die Dateien auf unterschiedliche Arten. Die Bandweite reicht vom reinen Umbenennen[863] über das Zerstückeln in zahlreiche Einzelteile bis zum Verschlüsseln in gepackte oder proprietäre Formate.

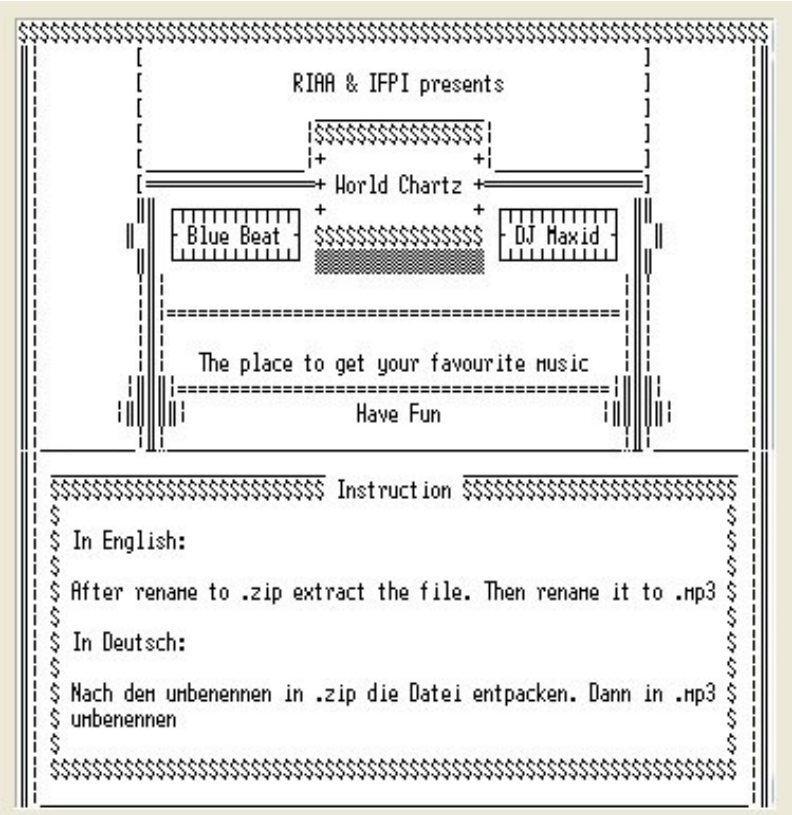


Abbildung 101 – Anleitung zum Entpacken und Umbenennen von Dateien

[863] Besonders beliebt sind die Formate DOC, PDF oder XLS.

Zum Ablegen der Dateien werden neben den normalen Webhosting-Providern auch Provider in Anspruch genommen, die ihren Kunden virtuelle Festplatten im Internet anbieten. Bei diesen Unternehmen wird kein Speicherplatz für die Einrichtung einer eigenen Webseite bereitgestellt, sondern ein universeller Ablageort für persönliche Dateien, der in der Regel über eine Passwortabfrage zu erreichen ist. Im Gegensatz zu den herkömmlichen Webhosting-Angeboten stehen dem Kunden hier häufig 50 Megabyte Speicherplatz zur Verfügung, so dass ein ganzes MP3-Album pro Account bereitgestellt werden kann. Werden solche Angebote von MP3-Piraten ausgenutzt, melden sie sich unter falschen Namen und mit der E-Mail-Adresse eines Freemailers an. Oft werden auch die Besucher einer MP3-Seite aufgefordert, Accounts bei Providern zu erstellen und Dateien hochzuladen. Das Aktualisieren der Links auf den Webseiten übernimmt dann meist der Betreiber der Piratenseite, es sei denn, die Vorgänge sind komplett automatisiert.

Ach noch was, in der Woche, bevor ich hier nach Hamburg fuhr, hab ich ein Programm entwickelt (ist aber noch nicht ganz fertig), daß Euch (beim Uppen) und mir (beim Update) die Arbeit erleichtert und Updates zügiger ablaufen läßt.
Und zwar lädt sich das Programm automatisch aus dem Internet die aktuelle Request-Liste runter und ihr braucht zum Uppen nur noch angeben, wo auf Eurer Platte das (allerdings schon in .doc o.ä. getarnte) MP3 liegt und das Programm lädt dann automatisch die Datei hoch und schickt mir eine Mail in dem von meinem Alben-Verwaltungsprogramm benötigten Format, so daß diese automatisch ausgelesen werden kann. Ich arbeite auch daran, daß einfach eine große Menge MP3s zum Upload angewiesen werden können und das dann ohne Euer Zutun geschieht, sprich: ihr könnt schlafen oder sonstwas machen, während das Programm uppt. Ich denke mal in ein bis zwei Wochen ist es verfügbar. Ich hoffe, es wird dann auch von vielen genutzt :-) Als Anreiz wird es wohl eine Uploader-Statistik für alle, die das Programm benutzen geben ;-).

Abbildung 102 – Text von einer großen deutschen MP3-Piratenseite

Der Aufbau der großen Piratenseiten ist immer ähnlich: Das Angebot an Musikdateien ist in Sektionen wie „Charts, Alben, Singles, HipHop etc." unterteilt. Üblich ist auch die Angabe mehrer URLs, über man die Seite erreichen kann. Bei den meisten URLs handelt es sich um sogenannte Redirectors, also Adressen, die von URL-Weiterleitungsdiensten bereitgestellt werden. Unternehmen wie *kickme.to* verschaffen ihren Kunden eingängige Web-Adressen, falls ihre Homepages nur unter langen oder schlecht einprägsamen Adressen zu erreichen sind. Eine Subdomain namens

http://www.freierplattenplatz.de/kunden/0012546/mp3seite.htm

könnte nach entsprechender Konfiguration auch über den Redirector

http://kickme.to/mp3seite

aufzurufen sein. URL-Weiterleitungsdienste erfreuen sich wegen ihrer Anonymität und Flexibilität – der User kann seine Subdomain über ein einfaches Web-Interface jederzeit auf eine neue Seite umlenken – insbesondere in der Warez- und MP3-Szene großer Beliebtheit.[864]

Schließlich sind Werbebanner ein fester Bestandteil der meisten MP3-Seiten im WWW. Wie bereits geschildert wurde, kann der Betrieb einer großen MP3-Webseite äußerst lukrativ sein.[865]

---

[864] Vgl. **Heise Online News** vom 18.02.2002, http://www.heise.de/newsticker/meldung/24934.
[865] Siehe oben Teil 3, A. V. 3.

Von den MP3-Groups wird das WWW nicht zur Verbreitung von Musikstücken genutzt. Wie bei den Warez-Gruppen ist es als „lame“ verpönt, andere Dienste als FTP und IRC für die Distribution der Releases zu nutzen.

3. FTP

FTP ist der bevorzugte Dienst für die MP3-Gruppen, um ihre Releases zu verbreiten. Zum Einsatz kommen sowohl Server von Privatleuten als auch Server von Unternehmen und Behörden, zu denen sich die Gruppen illegal Zugang verschafft haben. Die Distributionsabläufe ähneln sehr stark denen der Warez-Szene, häufig nutzen Gruppen aus beiden Szenen dieselben Server.

Von Profit-Pirates und anderen Mitgliedern der MP3-Szene werden FTP-Server nur selten genutzt.

4. IRC

Als Distributionsweg für Musikdateien kommt dem IRC eine eher geringe Bedeutung zu. Nur vereinzelt gibt es MP3-Gruppen, die Public Channels unterhalten, in denen DCC-Bots die aktuellen Releases für die anwesenden Chatter bereithalten.

DCC zwischen privaten MP3-Tradern ist eher die Ausnahme. Wurde im IRC ein Tauschkontakt geknüpft, findet der Dateitransfer in den meisten Fällen über private FTP-Server der Chatter statt.

5. Andere Dienste

E-Mail, UseNet oder Instant Messaging Systeme werden seit der Hochkonjunktur der Tauschbörsen kaum noch zur Verbreitung vom Musikdateien genutzt. Lediglich im UseNet gibt es noch einige Binaries-Newsgroups, in denen MP3-Dateien bereitgestellt werden. Dort finden sich schon seit Jahren die etwas exotischeren Musikangebote, z.B. unveröffentlichte und illegal erstellte Konzertmitschnitte („Bootlegs“)[866].

VIII. Phänomenologische Betrachtung der MP3-Szene

1. Subkulturelle Besonderheiten

An dieser Stelle ist auf die Ausführungen zur Warez-Szene zu verweisen. Die MP3-Gruppen orientieren sich beinahe vollständig an den Vorgaben aus der organisierten Software-Raubkopierer-szene.

Auch bei den MP3-Gruppen handelt es sich um eine geschlossene Gesellschaft, die die Elite der gesamten MP3-Szene darstellt. Allerdings mutet sie weniger ideologisch geprägt an als die Warez-

---

[866] Vgl. *Steinberg*, **Wired Magazine** 5.01 – Januar 1997.

Elite. Zwar arbeiten die MP3-Gruppen allesamt ohne Gewinnorientierung, doch entsprechende Hinweise sind in den NFO-Dateien weniger häufig vorzufinden[867].

In der MP3-Szene gibt es ebenfalls strenge Regeln, denen sich die meisten Gruppen unterworfen haben:

```
Much has changed in the mp3 "scene" lately, but Let's skip the intro and history of
the music/mp3scene of the internet. Those of u who have been here since it all started
in 1995/96 know that there has been much chaos, and there still is. Any previous
attempts (mp3spa) at bringing in some organization and guidelines into the scene have
failed. The scene has always worked as every group by it self. That might have worked
fine, but we now want to move on and start appreciating other groups releases/rip, and
save our own time for ripping more. This means we have to be able to trust each other
rips. For this purpose, and nothing else, a council was set up and a name was chosen:
RIAA. The participants agreed on some easy to understand rules about how to release
music on the internet! This was done by a few big mp3 release groups, but it is the
hope of everyone that all groups and independent suppliers will use them as well. We
expect top groups like MGC, UBE, NBD, BF, TFA, WLWMP3, MS, IMPG, IDM (and others we
forgot) to be joining this council soon!

The program is as follows:
The scene will benefit from this effort, and we will respect the agreed rules.
The council name is RIAA.
The members are councils of the chosen groups and a few more selected people.
New members of this council can join on Invite / Vote-in.
Rippers/groups must produce .SFV files for crc'ing every release.
Rippers/groups must produce .NFO files for every release, and the .nfo file must
feature at least:

ARTIST NAME - TITLE - GROUP RELEASE DATE - GROUPNAME; A release without proper .nfo
AND .sfv file is a nuke on all big sites.
Files and directories must only contain a-z A-Z 0-9 _ - () and no other characters.
Underscores will be used for spaces, and double dots won't be used. i.e.
The length of filenames and directorynames must not exceed 64 chars.
Directory names must at minimum include "Artist-Album-GROUPINITIALS"
Filenames must at minimum include "Tracknumber-Songtitle-GROUPINITIALS"
The music format is MP3 until MP4 format is out, and AAC and VFQ are ignored.
The following encoders are banned because of their inability to produce good sounding
mp3s: Xing Encoder, BladeEnc, AudioActive Po -lq mode; These encoders are banned at
the moment, but it might change soon. Stay tuned.

We Also Agreed That These Changes Will Be In Effect No Later Than FEBRUARY 1ST 1999.
So Pls Be Ready With Your Sfv/Nfo Tools.. And The Characters. Happy Mp3'Ing To Us
All.. Let`s Make 1999 A Better Year!

This Document Was Signed & Approved On December 17Th, 1998 By The Following
Individuals, Representing Their Respective Groups:

Vega[aPC] Aeonizer(Kain)[ATM] AlCapone[RnS] EXx[UMA] Fido[AMOK]
```

Abbildung 103 – „Riprules“ für MP3-Gruppen

2. Täterkreis

Was die Alters- und Geschlechtsstruktur anbelangt, dürften bei den Mitgliedern von MP3-Gruppen kaum signifikante Unterschiede zu den Mitgliedern von Warez-Gruppen bestehen. Schätzungsweise ist der Altersdurchschnitt etwas geringer, und der soziale Status dürfte im Mittel auch nicht ganz so hoch sein wie bei den häufig in der IT-Branche beschäftigten Softwarepiraten.

---

[867] Von 48 vom Verfasser untersuchten Gruppen ließen 8 Gruppen in ihren NFO-Dateien explizit verlauten, dass sie den Kauf von Originalprodukten befürworten; zur Methodik siehe Teil 1, F.

Allerdings liegen mangels stattgefundener Verfahren gegen Internet-Musikpiraten keine gesicherten Erkenntnisse über die personelle Struktur der MP3-Gruppen vor.

Anders sieht es bezüglich der Nutzer von MP3-Webangeboten und P2P-Musiktausch-börsen aus: Eine Umfrage von Soziologen der Universitäten Frankfurt/Oder und Leipzig bei 4.340 Internet-nutzern ergab ein recht klares Bild des durchschnittlichen (deutschen) MP3-Konsumenten:[868] Der typische MP3-Hörer ist mit 96%iger Wahrscheinlichkeit ein Mann und durchschnittlich 26 Jahre alt. Mehr als die Hälfte aller Befragten haben Abitur (56%), und fast jeder vierte hat einen Hochschulabschluss (23%). Ein Drittel studiert (36%) und knapp die Hälfte ist berufstätig.

Auch über das Kauf-, Download- und Tauschverhalten der Nutzer liefert die Umfrage Aufschluss: Danach kaufen 62% der Teilnehmer regelmäßig CDs und nutzen parallel dazu MP3-Dateien. 5% der Teilnehmer kaufen ausschließlich CDs, und 32% sind reine MP3-Konsumenten. Von dem Gros der Tauschbörsennutzer werden im Durchschnitt etwa 14 Musikdateien pro Monat heruntergeladen. Die Extremnutzer, die nur einen Anteil von 10% ausmachen, erhöhen den Durchschnitt auf 91 Downloads pro Monat. 17,45% der Tauschbörsennutzer geben keine Dateien auf ihren Festplatten frei, 82,55% zeigen aktive Bereitschaft zum Tauschen. Im Schnitt haben typische MP3-Nutzer in den vergangenen drei Monaten ca. vier CDs gekauft, ebenso viele wurden verliehen oder ausgeliehen. Insgesamt – so das Ergebnis der Umfrage – lässt sich kein Zusammenhang zwischen der Zahl der gekauften CDs und der Download-Aktivität aufzeigen.

3. Tätermotivation

Im Rahmen der zuvor zitierten Umfrage wurden auch Informationen zur Motivation der typischen MP3-Nutzer gesammelt: Praktisch alle Teilnehmer gingen davon aus, dass MP3-Tauschbörsen nicht illegal sind.[869] Es sei so gut wie kein Unrechtsempfinden vorhanden, die Interessen der Rechtsinhaber hätten hier keine Bedeutung. Als Motivation für die Nutzung von Tauschbörsen gäben die Tauschwilligen vor allem die Informationsleistung der Börsen sowie den Gemeinschaftsaspekt des Tausches bei P2P-Systemen an.[870] 77% der Befragten hätten sich außerdem über die mangelnden Möglichkeiten beklagt, preisgünstig einzelne Stücke kaufen zu können.[871]

Neben der Ersparnis hoher CD-Kosten gibt es weitere Gründe für den Download von MP3-Dateien aus dem Internet: Da die Plattenfirmen einen Großteil ihrer Produktionen nur für einen begrenzten Zeitraum anbieten, passiert es, dass weniger nachgefragte Stücke vom legalen Markt verschwinden. Der MP3-Tausch ist dann die einzige Möglichkeit, noch an diese Stücke heranzukommen. Ähnliches gilt für Bootlegs, also unautorisierte Aufnahmen eines Live-Konzerts oder einer unveröffentlichten Studio-Session, da diese niemals auf dem legalen Markt erhältlich waren. Auch indizierte Musik wird verstärkt über P2P-Systeme getauscht; dies gilt insbesondere für die Lieder der in Deutschland verbotenen Skinhead-Bands.

---

868 *Weber/Haug*, **c't** 17/2001, S. 36 f.
869 Vgl. das Interview mit *Weber*, bei *Lehmkuhl*, **FOCUS** 34/2001, S. 132.
870 *Weber/Haug*, **c't** 17/2001, S. 37.
871 Vgl. das Interview mit *Weber*, bei *Lehmkuhl*, **FOCUS** 34/2001, S. 132.

Wie bei den Softwarepiraten gibt es innerhalb der MP3-Szene gewisse psychologische Neutralisierungsmechanismen, anhand derer die MP3-Piraten ihr Handeln vor sich und der Gesellschaft rechtfertigen: Weit verbreitet ist die Ansicht, dass die Plattenindustrie die Fans mit ihren überzogenen Preisen zur Piraterie treibe. Es sei lächerlich, 16 US-Dollar für eine ganze CD auszugeben, wenn man nur einen bestimmten Song haben möchte. Die Industrie „sahne richtig ab". Schließlich sei die gleiche Musik in Radio und Fernsehen ja auch umsonst. Ein Student der Universität von Wisconsin, dessen FTP-Server aufgrund einer Aktion des Tonträgerunternehmens *Geffen* vom Netz genommen wurde, sah die Sache ähnlich: „Ich habe ihre Künstler promoted wie jede normale Radiostation. Das ist wie wenn man an jeden herantritt, der ein Lied aus dem Radio aufgenommen hat".[872] Andere feiern die MP3-Bewegung als eine Revolution, weil sie mittlerweile selbst darüber entscheiden können, was sie hören und nicht mehr den selektierten bzw. oktroyierten Musikgeschmack der Labels und TV-Sender vorgesetzt bekommen.

Bei den Mitgliedern von MP3-Gruppen kommt eine gruppenspezifische Motivation hinzu, wie man sie von den Warez-Gruppen kennt: Jeder genießt die Anerkennung und die Exklusivität, die er mit dem Status eines „Groupmembers" erreicht. Da den meisten Gruppenmitgliedern nicht nur Zugang zu reinen MP3-Servern gewährt wird, sondern viele Server die ganze Bandbreite an „heißer digitaler Ware" abdecken, ist eine Mitgliedschaft auch für jene erstrebenswert, die Teil der gesamten Raubkopiererszene sein möchten.

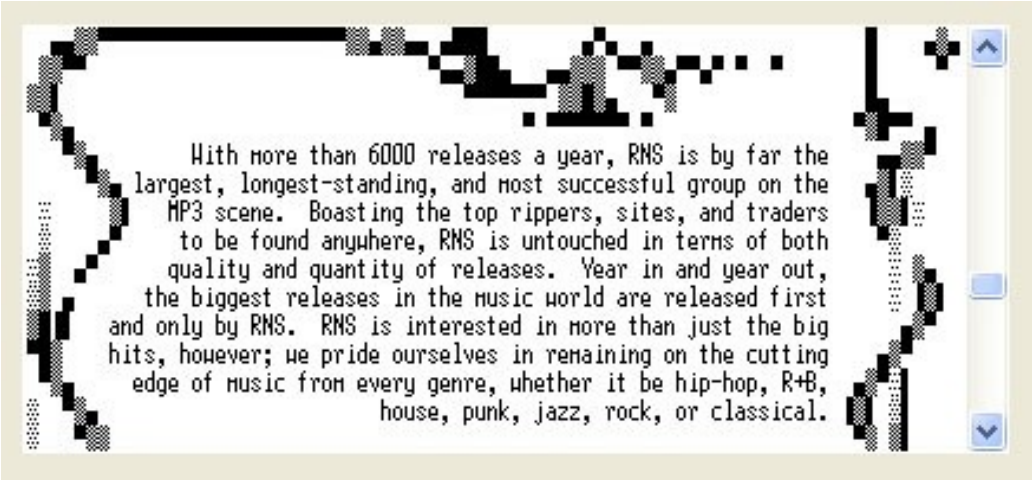


Abbildung 104 – Auszug aus einer NFO-Datei

[872] **Wired News** vom 12.02.1998, http://www.wired.com/news/culture/0,1284,10234,00.html.

B. Bedeutung und Schaden

I. Angaben über Fälle von Online-Musikpiraterie und über den Schaden

1. Angaben der *International Federation of the Phonographic Industry (IFPI)*

Die deutsche Landesgruppe der *IFPI*[873] beklagt für die von der Verbandsstatistik erfassten Unternehmen einen Umsatzrückgang um 10,2% im Jahr 2001 gegenüber dem Vorjahr und führt dies neben der traditionellen gewerblichen Tonträgerpiraterie (Raubpressungen etc.) und privatem CD-Brennen auf die Online-Musikpiraterie zurück. 2001 hätten rund 5 Millionen Personen 492 Millionen Stücke von "meist illegalen Angeboten" aus dem Internet geladen, so ein Sprecher der *IFPI*, der seine Aussage auf eine Studie der *GfK* stützt.[874] Im Rahmen der sogenannten Brenner-Studie[875] der *GfK* wurden 10.000 Deutsche über zehn Jahre von April 2000 bis Februar 2002 schriftlich zu ihrem Kopier- und Download-verhalten von digitaler Musik befragt. Danach kopierten allein im Jahr 2001 17,1 Millionen Bundesbürger Musik, die unter anderem aus dem Internet stamme, auf 182 Millionen CD-Rohlinge. Wäre die Musik gekauft worden, so ein *IFPI*-Sprecher, wäre ein Umsatz von 3,2 Milliarden € erzielt worden. Zu den 3,2 Milliarden müssten noch rund 50 Millionen € illegaler Umsatz für traditionelle gewerbliche Piraterie und 220 Millionen € für die sogenannte Schulhofpiraterie hinzugerechnet werden.[876]

Zum absoluten Schaden, der alleine durch Online-Musikpiraterie entsteht, liefert die *GfK*-Studie keine Angaben, allerdings schätzt die deutsche Landesgruppe der *IFPI* in ihrem Jahreswirtschaftsbericht 2001[877], dass der Umsatzwert für Onlinepiraterie ca. 740 Millionen € beträgt, wäre die aus dem Netz geladene Musik auch gekauft worden. Die Verluste durch Onlinepiraterie hätten sich dabei gegenüber dem Vorjahr verdoppelt.

Der Music Piracy Report der *IFPI* vom Juni 2002[878] liefert Angaben zur weltweiten Situation: Schätzungen zufolge würden ca. 99% aller über das Internet erhältlichen Musikstücke unautorisiert angeboten. Im Mai 2002 sollen sich in P2P-Systemen durchschnittlich 3 Millionen Nutzer aufgehalten und 500 Millionen Musikstücke zum Download bereitgestellt haben. Des Weiteren wird von geschätzten 200.000 WWW-Seiten und FTP-Servern ausgegangen, die 100 Millionen Musikdateien bereithalten.

2. Angaben der *Recording Industry Association of America* (*RIAA*)[879]

Der größte Verband der US-amerikanischen Musikindustrie kommt aufgrund eigener Untersuchungen zu der Feststellung, dass CD-Brennen und kostenlose Raubkopien im Internet den US-Plattenfirmen im Jahr 2001 ein Umsatzminus von 4,1% beschert haben. In Zusammenarbeit mit dem Marktforschungsinstitut *Peter D. Hart Research Associates* hatte die *RIAA* 2.225 Musikliebhaber im

---

873 http://www.ifpi.de.
874 **Heise Online News** vom 21.03.2002, http://www.heise.de/newsticker/meldung/25930.
875 Veröffentlicht bei der deutschen Landesgruppe der *IFPI*: http://www.ifpi.de/news/192/index-Dateien/frame.htm.
876 **Heise Online News** vom 21.03.2002, http://www.heise.de/newsticker/meldung/25930.
877 Veröffentlicht unter http://www.ifpi.de/jb/2002/22-25.pdf.
878 Veröffentlicht unter http://www.ifpi.org/site-content/library/piracy2002.pdf.
879 http://www.riaa.com.

Alter zwischen 12 und 54 Jahren nach ihrem Kaufverhalten befragt. Demnach haben 23% der Befragten 2001 überhaupt keine CDs mehr gekauft, da sie die meisten Songs entweder kopiert oder aus dem Internet bezogen hätten. Hinzu komme, dass rund die Hälfte von ihnen weitere Kopien der illegal bezogenen Songs anfertigten. Zwei Jahre zuvor (1999) seien es nur 13% gewesen.[880]

Im Auftrag der *RIAA* befragten die Marktforscher von *Peter D. Hart Research Associates* im Mai 2002 erneut 860 Internetnutzer im Alter zwischen 12 und 54 Jahren nach ihren Kaufgewohnheiten: Danach gaben 41% der Befragten an, Downloads heute stärker zu nutzen als vor einem halben Jahr und gleichzeitig weniger CDs zu kaufen. Nur 19% sollen erklärt haben, trotz angestiegener Downloads mehr CDs zu kaufen. Insgesamt hätten 52% aller Befragten heruntergeladene Dateien auf CD gebrannt oder auf tragbare Player kopiert[881].

3. Andere Angaben

Die *Gesellschaft für Musikalische Aufführungs- und Vervielfältigungsrechte (GEMA)*[882] verzeichnete für das Jahr 2001 im Bereich der Tonträger-Vervielfältigungsrechte gegenüber dem Ergebnis des Vorjahres einen Rückgang um 3,43%. Als Ursache werden rückläufige Erträge aus der Tonträgerlizenzierung insbesondere im Inlandsmarkt angegeben.[883]

Analysten des US-Marktforschungsunternehmens *Webnoize*[884] wollen herausgefunden haben, dass allein im August 2001 weltweit 3,05 Milliarden Musikdateien über die größten Internet-Tauschbörsen transferiert wurden. Damit sei das Tauschvolumen des Monats Februar 2001 übertroffen worden, in dem die beliebte *Napster*-Software noch ohne Einschränkungen arbeitete. Die Untersuchung bezieht nach Angaben von *Webnoize* die vier beliebtesten Tauschdienste ein. Angeführt wird die Liste von den *FastTrack*-Clients (970 Millionen getauschte Dateien), auf den weiteren Plätzen folgen *Audiogalaxy* (910 Millionen), *iMesh* (640 Millionen) und *Gnutella* (530 Millionen).[885]

In Westeuropa soll sich gemäß einer Studie der US-Marktforscher von *Jupiter Media Metrix*[886] von Februar bis August 2001 die Zahl der Nutzer von Musiktauschbörsen im Internet fast halbiert haben. Die Studie, in deren Rahmen rund 50.000 Internetnutzer in neun westeuropäischen Ländern befragt wurden, kommt weiter zu dem Ergebnis, dass sich im Februar 2001 noch rund 8,2 Millionen Westeuropäer in Tauschbörsen aufhielten, davon rund sechs Millionen bei *Napster*. Im August des selben Jahres soll die Nutzerzahl auf 4,6 Millionen gesunken sein. Offensichtlich seien die

---

880 **Heise Online News** vom 26.02.2002, http://www.heise.de/newsticker/meldung/25153.
881 **musikwoche.de Online News** vom 27.08.2002, http://www.musikwoche.de; **Heise Online News** vom 27.98.2002, http://www.heise.de/newsticker/meldung/30262.
882 http://www.gema.de.
883 **GEMA-Brief**, Ausgabe 42/Mai 2002, S. 1.
884 http://www.webnoize.com.
885 **Heise Online News** vom 07.09.2001, http://www.heise.de/newsticker/meldung/20895.
886 http://www.jmm.com; Informationen zu den von *Jupiter Media Metrix* verwendeten Erhebungsmethoden finden sich unter http://www.jupiterresearch.com/bin/item.pl/data:methodology.

Nachfolger *Napsters* im Gegensatz zu den USA in Europa nicht so beliebt. In Nordamerika hätten sich die Tauschaktivitäten im Untersuchungszeitraum verfünffacht.[887]

Eine Prognose für die nächsten Jahre wagen die Analysten der *Yankee Group*[888]: Gemäß einer Studie der US-Marktforscher wird die Anzahl der Musik-Stücke, die im Internet getauscht werden und nicht bei den Plattenfirmen lizenziert wurden, von 5,16 Milliarden im Jahr 2001 auf 7,44 Milliarden im Jahr 2005 steigen. Im Jahr 2006 soll es dann erstmalig einen Rückgang auf 6,33 Milliarden getauschte Musikstücke geben. 2007 würden nur noch 3,9 Milliarden Musikdateien getauscht.[889] Den Rückgang in der Tauschbörsennutzung erwartet die *Yankee Group*, da zunehmend legale Download-Angebote auf den Markt kommen würden, derer sich die musikbegeisterten Internetnutzer bedienen könnten.

II. Interpretation der Angaben

Musikpiraterie ist nur teilweise für den von der Musikindustrie ermittelten Umsatzrückgang verantwortlich.[890] Branchenkenner – auch aus den eigenen Reihen – führen die Entwicklung darüber hinaus auf überhöhte CD-Preise[891], mangelnde künstlerische Qualität innerhalb der Produktpaletten[892] und die schwache Gesamtkonjunktur[893] zurück.

Hinzu kommt eine Veränderung im Konsumverhalten eines großen Teils der Zielgruppe, die nicht vernachlässigt werden darf: Die Kinder und Jugendlichen von heute geben ihr Taschengeld für andere Dinge aus als in den Jahren zuvor. Ausgaben für Mobiltelefone, Markenbekleidung, Kosmetika, Personal-Computer bzw. Spielekonsolen und Computerspiele haben in letzter Zeit massiv zugenommen.[894] Vor allem die Konkurrenz durch andere Entertainment-Produkte dürfte sich deutlich auf die CD-Verkaufszahlen auswirken. Diese Beobachtung deckt sich mit den Meldungen aus der Videospielbranche, wonach auf dem US-amerikanischen Markt in 2001 der Umsatz bei der Konsolenhardware um 43% und bei Computerspielen um 4,4% gestiegen sei.[895] Ebenfalls gestiegen sind die Absatzzahlen bei DVD-Musikvideos: Die *RIAA* vermeldete für 2001 eine Steigerung gegenüber dem Vorjahr von 138%.[896]

---

887 **Heise Online News** vom 29.10.2001, http://www.heise.de/newsticker/meldung/22249.
888 http://www.yankeegroup.com.
889 **Heise Online News** vom 15.08.2002, http://www.heise.de/newsticker/meldung/29972.
890 Obwohl eine Umfrage bei verschiedenen Vertretern des Tonträgerhandels ergeben hat, dass für 2002 in vielen Fällen das Vorjahresergebnis erreicht wurde, vgl. **musikwoche** 1-2/2002, S. 12, wird unterstellt, dass tatsächlich ein Umsatzrückgang stattgefunden hat, der auf rückläufige Tonträgerverkaufszahlen zurückzuführen ist.
891 So z.B. *Huchthausen* vom *Fachverband Tonträger* in **musikwoche** 46/2001, S. 21 oder *Mikulski*, geschäftsführende Gesellschafterin des Tonträgerunternehmens *ZYX Music,* bei *Theurer*, **FAZ** vom 22.10.2001, S. 20. *Mikulski* wörtlich: "Dass *Napster* und das Raubkopieren schuld an der Branchenkrise sein sollen, ist Unsinn [...]. Wenn neue CDs im Schnitt 35 Mark (entspricht ca. 18 €) kosten, ist das zu viel".
892 So z.B. *Renner*, Geschäftsführer von *Universal Music* Deutschland, in den **Heise Online News** vom 02.09.2001, http://www.heise.de/newsticker/meldung/20762.
893 So *Rosen*, ehemalige Präsidentin und CEO der *RIAA*, in den **Heise Online News** vom 26.02.2002, http://www.heise.de/newsticker/meldung/25153.
894 Siehe hierzu die Ergebnisse der Kids Verbraucher Analyse 2001 der *Verlagsgruppe Lübbe*, der *Bauer Verlagsgruppe* und des *Axel Springer Verlags*, zu finden unter http://www.mediapilot.de oder http://www.bauermedia.com/studien/zielgruppen/kids_verbraucheranalyse/kids_verbraucheranalyse.php.
895 Vgl. **Heise Online News** vom 07.02.2002, http://www.heise.de/newsticker/meldung/24678.
896 **Heise Online News** vom 26.02.2002, http://www.heise.de/newsticker/meldung/25153.

Sofern Verkaufszahlen von CD-Rohlingen herangezogen werden, um die Größenordnung des Raubkopieproblems zu beschreiben, handelt es sich um keine zuverlässige Methode. Kritiker bemängeln, dass bei einem Vergleich von verkauften CD-Rohlingen mit den Verkaufszahlen von Tonträgern „ganz nebenbei Raubkopien, legale Kopien und Daten-Backups in einen Topf" geworfen würden[897]. Zwar unterscheidet beispielsweise die Brenner-Studie der *GfK* nach dem Inhalt von bespielten Rohlingen und kommt zu dem Ergebnis, dass im Jahr 2001 55% aller gebrannten Rohlinge Musik enthielten[898], allerdings wird innerhalb der Gruppe der mit Musik bespielten CD-Rohlinge nicht weiter differenziert, ob es sich um legale Privatkopien lizenzpflichtiger Musik[899], Kopien lizenzfreier Musik oder um Raubkopien handelt. Indem aber die Gesamtzahl von 182 Millionen Rohlingen (55%) im Zusammenhang mit dem Piraterieproblem genannt und zur fiktiven Schadensberechnung herangezogen wird, entsteht ein verzerrtes Bild.[900] Dass die Verkaufszahlen von CD-Rohlingen in den letzten Jahren stetig gestiegen sind, liegt auch darin begründet, dass die analoge Musikkassette langsam vom Markt verschwindet. In den letzten Jahren ist deren Anteil an den verkauften Leermedien um jeweils rund 40% zurückgegangen.[901]

Fragwürdig ist auch die Methode, von den reinen Nutzerzahlen von P2P-Systemen auf die Dimension des illegalen Musiktausches zu schließen. Im Gegensatz zu den ersten *Napster*-Versionen ermöglichen die Tauschbörsen von heute den Tausch beinahe aller Dateiformate. Sachverständige, die im Auftrag der demokratischen Abgeordneten im US-Kongress die bekanntesten Filesharing-Dienste untersucht hatten, kamen zu dem Ergebnis, dass mittlerweile mehr pornographisches Material über Tauschbörsen gehandelt würde als Musiktitel.[902]

Während man getrost davon ausgehen kann, dass das „Schwarzbrennen" von CDs für die Umsatzeinbußen der Musikindustrie mitverantwortlich ist, sind die Auswirkungen der Online-Musikpiraterie auf das Musikgeschäft besonders schwer zu beurteilen. Eine interessante Beobachtung machten Analysten während des rasanten Aufstiegs von *Napster*: Beim Vergleich der Nutzerzahlen von *Napster* und den Tonträger-Verkaufsstatistiken ließ sich ein Zusammenhang erkennen, der als „*Napster*-Boomerang" bezeichnet wurde. Denn parallel zum Wachstum von *Napster* stiegen in den USA die Verkaufszahlen von CDs, und nach dem Verschwinden von *Napster* konnte ein Rückgang der Verkaufszahlen um 5,4% beobachtet werden.[903]

Ob Programme wie *Napster* tatsächlich als eine Art der kostenlosen Werbung für Musik zu verstehen sind und ähnlich wie seinerzeit Radio- und Tonbandgeräte das Wachstum der Musikindustrie begünstigen können, ist nach wie vor heftig umstritten. In diesem Zusammenhang sorgte Mitte 2002

---

897 So z.B. *Himmelein*, Sind wir alle kriminell?, **c't** 2/2002, S. 80.
898 http://www.ifpi.de/news/192/index-Dateien/frame.htm (Folie 11).
899 Legale Privatkopien werden nicht nur zur Weitergabe an Familienmitglieder und enge Freunde hergestellt, sondern viele Käufer machen sich unter anderem Kopien für ihre Musikanlage im Auto, weil sie schlechte Erfahrungen mit Einbrüchen oder den unvermeidlichen Gebrauchsspuren gemacht haben; ausführlich zur Privatkopie siehe unten Teil 3, C. I. 2. d) (1).
900 Zu beachten ist in diesem Zusammenhang, dass die Brennerstudie der *GfK* mit den ermittelten 55% deutlich höher liegt als eine Studie des großen Brennsoftware-Herstellers *Roxio*, wonach in 2001 nur 32% der mit *Roxio*-Software gebrannten CD-Rohlinge Musikdaten enthielten, vgl. *Howard-Spink*, **Music Business International**, October 2001, S. 55.
901 **Heise Online News** vom 26.02.2002, http://www.heise.de/newsticker/meldung/25153.
902 **Heise Online News** vom 29.07.2001, http://www.heise.de/newsticker/meldung/19707.
903 *Rötzer*, Mit dem Niedergang von Napster sinken auch die CD-Verkäufe, **Telepolis** vom 14.08.2001.

eine Studie des US-Marktforschungsunternehmens *Jupiter Media Metrix* für Aufruhr in der Tonträgerbranche: Die Marktforscher wollen herausgefunden haben, dass die Nutzung von Musiktauschbörsen tatsächlich förderlich für den Tonträgerabsatz ist. In der Studie hätten 29% der Befragten gesagt, die Teilnahme an Musiktauschbörsen habe ihr Kaufverhalten verändert, 10% kauften jetzt weniger Musik als zuvor, aber 19% würden verstärkt kaufen.[904] Die *RIAA* kritisierte nach Veröffentlichung der Studie zu Recht, dass bei der Befragung nur Erwachsene herangezogen wurden. Teenager, so der Verband, seien die aktivsten Online-Musikfans. Sie würden massenhaft Lieder aus dem Netz „saugen" und diese auf selbstgebrannten CDs auf dem Schulhof verkaufen.[905]

Jupiters Forschungsergebnis wurde jedoch unlängst von einer unabhängigen Studie des Marktforschungsunternehmens *Ipsos/Reid*[906] bestätigt, bei der 1.113 Nutzer im Alter von 12 bis 55 Jahren befragt wurden. Danach sei die Kaufbereitschaft bei 81% der Musik-Downloader gleich geblieben oder sogar gestiegen.[907]

Zu einem ähnlichen Ergebnis kam bereits im Jahr 2000 eine Studie der *Digital Media Association (DiMA)*[908]. Im Rahmen der Untersuchung, in der 16.000 Amerikaner im Alter zwischen 13 und 39 Jahren online befragt wurden, gaben 59% der befragten Surfer an, eine CD gekauft zu haben, weil sie zuvor die Musik im Internet gehört hätten. 48% gaben an, das Internet zu nutzen, um Musik zu hören, die nicht im Radio gespielt würde. Vertreter der *DiMA* sahen in der Studie den Beweis dafür, dass der Vertrieb über das Internet sowohl das Online- als auch das Offline-Geschäft ankurbelt.[909]

Die Ergebnisse einer aktuellen Studie aus den USA deuten jetzt ebenfalls darauf hin, dass Tauschbörsen keine Schuld an der Branchenkrise der Musikindustrie haben. Eine Befragung unter 1.000 Online-Konsumenten durch das Marktforschungsinstitut *Forrester Research*[910] konnte keinerlei Anhaltspunkte dafür liefern, dass Kunden, die häufig digitale Musikangebote nutzten, weniger CDs kaufen würden. Eine ganze Reihe anderer Ursachen sei für die Umsatzeinbußen verantwortlich, unter anderem die allgemeine wirtschaftliche Rezession.[911]

Dass sich die freie Online-Verfügbarkeit von Musikstücken nicht zwingend schädlich auf den Absatz physikalischer Tonträger auswirkt, ließ sich in der Vergangenheit mehrfach beobachten: Das Lied „Hol' mir mal 'ne Flasche Bier", mit dem der deutsche TV-Moderator *Stefan Raab* den *SPD*-Politiker *Gerhard Schröder* verulkte, wurde von *Raab* auf der Homepage seiner Sendung *TV-Total* zum freien Download angeboten. Erst nachdem sich die Forderungen der Fans nach einer käuflichen Audio-CD mehrten, entschloss sich *Raab* zwei Wochen später, die Platte in den Handel zu bringen. Obwohl das kostenfreie Downloadangebot parallel bestehen blieb, schaffte es die Blödelnummer bis auf Platz 1

---

904 **Heise Online News** vom 05.05.2002, http://www.heise.de/newsticker/meldung/27168. Informationen zu der von *Jupiter Media Metrix* verwendeten Erhebungsmethode finden sich unter http://www.jupiterresearch.com/bin/item.pl/data:methodology.
905 **Heise Online News** vom 10.05.2002, http://www.heise.de/newsticker/meldung/27301.
906 http://www.ipsos-reid.com.
907 Die gesamte Studie findet sich unter http://www.ipsos-reid.com/media/dsp_displaypr_us.cfm?id_to_view=1542; Informationen zu der verwendeten Erhebungsmethode finden sich unter http://www.ipsos-insight.com/pdf/ipsos-insight_tempo.pdf.
908 http://www.digmedia.org.
909 **Heise Online News** vom 19.06.2000, http://www.heise.de/newsticker/meldung/10112.
910 http://www.forrester.com.
911 **Heise Online News** vom 14.08.2002, http://www.heise.de/newsticker/meldung/29960; zur Erhebungsmethode siehe http://www.forrester.com/Technographics.

der deutschen Verkaufscharts und hielt sich über mehrere Wochen in den Top 10. Eine ähnliche Beobachtung konnte man bezüglich des Lieds *„Only Time"* der irischen Sängerin *Enya* machen: Das Lied, das nach den Terroranschlägen auf das *World Trade Center* zur tragischen Hymne des 11. September avancierte, nachdem es in der US-Berichterstattung als Hintergrundmusik für einen Zusammenschnitt der Ereignisse zum Einsatz kam, kletterte weltweit in den Charts auf die Spitzenpositionen und wurde zu einer der erfolgreichsten Singles aller Zeit. Und das, obwohl die Plattenindustrie öffentlich bekannt gab, dass eine Verfolgung von Personen, die das Lied per Internet verbreiten oder downloaden, nicht stattfinden werde. Es ist davon auszugehen, dass *„Only Time"* auch einer der am meisten heruntergeladenen Titel in dieser Zeit war.

Abschließend kann man sagen, dass der Download eines Musiktitels in den meisten Fällen kein vollständiges Substitut für den Erwerb einer Audio-CD ist. Millionen Nutzer laden sich Musik herunter, die sie niemals gekauft hätten, weil es so einfach und komfortabel geworden ist. Ein Stück, das nicht gefällt, wird einfach wieder gelöscht oder verschwindet ungenutzt auf einem Backup-Medium.

Offenbar bietet das körperliche Originalprodukt Vorteile, die ein großer Teil der Konsumenten nicht missen will. Hierzu mögen zum einen das gefühlsmäßige Erleben einer Kauf-CD zählen, zum anderen das Begleitmaterial (Booklet, Cover) und seine künstlerische Gestaltung. Nicht zu vergessen ist außerdem, dass nur eine Original-CD als Geschenk oder Sammelobjekt taugt, weil sie im Gegensatz zur Kopie einen gewissen Wert verkörpert. Die Situation erinnert an die Einführung des sogenannten Home-Taping mittels Tape-Decks und Kassettenrekordern. Auch damals befürchtete man einen drastischen Rückgang bei den bespielten Tonträgern, der dann allerdings nicht eintrat.[912]

Das weit verbreitete Argument, Tauschbörsen schadeten in erster Linie den unbekannteren Künstlern, ist nicht zu bestätigen. Vielmehr ist es so, dass sich in den Tauschbörsen vorrangig die aktuellen Veröffentlichungen von Interpreten finden, die bereits berühmt sind. Da sich eine größere Bekanntheit nur mit großem Marketingaufwand erreichen lässt, wie er der Musikindustrie zur Verfügung steht, schaden die Tauschbörsen unbekannten Musikern genauso wenig, wie sie ihnen nutzen. Tauschbörsen machen also bekannte Künstler noch bekannter; ob sie die Verkaufszahlen beeinträchtigen, ist bislang nicht mit Sicherheit nachzuweisen.

Dennoch muss man davon ausgehen, dass beinahe jedes Musikstück als Raubkopie im Internet erhältlich ist. Allerdings finden sich die exotischeren Werke nicht in den Tauschbörsen, sondern eher auf privaten FTP-Servern der MP3-Gruppen bzw. in deren Peripherie. Wie viele Seiten es im WWW gibt, auf denen nichtlizenzierte Musikdateien zum Download angeboten werden, ist nicht feststellbar.

Eine Ahnung bezüglich der Größenordnung mag eine eigene, turnusmäßig durchgeführte Stichwortsuche zu den Begriffen „mp3" und „mp3z" vermitteln, wobei vor allem die Ergebnisse zum letztgenannten Suchbegriff mit illegalen Downloadangeboten in Verbindung stehen dürften.

---

[912] Vgl. *Theurich,* Leiter der Presseabteilung bei *EastWest Records*, bei *Ziebarth*, **KEYS** 2/1999, S. 44.

Denn der Begriff „mp3“ befindet sich auf Millionen von Webseiten, die sich legal mit dem Thema beschäftigen – zu nennen sind beispielhaft zahllose Webseiten von Bands ohne Plattenvertrag, die eigene Lieder im MP3-Format zum Download ins Netz stellen.

	„mp3“	*„mp3z“*
10/1999	3.649.840*	100.010
01/2000	2.391.484	47.995
04/2000	3.033.925	62.580
07/2000	6.606.630	69.270
10/2000	5.444.640	62.605
01/2001	4.129.570	62.870
04/2001	11.342.410	98.073
07/2001	11.191.892	85.926
10/2001	11.308.480	85.371
01/2002	15.422.607	120.564
04/2002	5.500.221	31.508
07/2002	9.300.155	76.131
10/2002	6.026.454	90.585
01/2003	6.788.544	863.457
04/2003	7.563.895	340.807

Abbildung 105 – Stichwortsuche bei *Altavista.com;* *Anzahl der gefundenen Dokumente (Webseiten und Unterseiten).

	„mp3“	*„mp3z“*
10/2001	13.200.000*	71.300
01/2002	14.300.000	69.200
04/2002	17.400.000	215.000
07/2002	21.700.000	743.000
10/2002	23.600.000	923.000
01/2003	28.000.000	1.440.000
04/2003	30.300.000	1.040.000

Abbildung 106 – Stichwortsuche bei *Google.de;* *Anzahl der gefundenen Dokumente (Webseiten und Unterseiten).

C. Bekämpfung und Überwachung von Online-Musikpiraterie

I. Rechtslage in Deutschland

1. Der (urheber-)rechtliche Schutz von digitalen Musikwerken

Gemäß § 2 Abs. 1 Nr. 2 UrhG zählen „Werke der Musik" zu den vom Urheberrecht geschützten Werken. Hierunter fallen alle Erzeugnisse, die sich der Töne als Ausdrucksmittel bedienen, z.B. Opern, Operetten, Symphonien, Klavierstücke, Lieder sowie Stücke aus dem Bereich der Unterhaltungsmusik.[913] § 2 Abs. 2 UrhG verlangt auch für diese, dass sie eine persönliche geistige Schöpfung darstellen. Dies ist nur dann der Fall, wenn eine individuelle Komposition vorliegt.[914] Individualität kann sich bei Musikwerken nach der Rechtsprechung des *BGH*[915] aus der Gestaltung der Melodie, dem Aufbau der Tonfolgen, der Rhythmisierung, der Instrumentierung und der Orchestrierung ergeben.

Auf die künstlerische Bedeutung des Musikstückes ist bei der Beurteilung der Schutzfähigkeit nicht abzustellen;[916] vielmehr gilt im Bereich des musikalischen Schaffens ebenfalls der Schutz der sogenannten kleinen Münze, wonach neben komplexen Schöpfungen auch solche Leistungen vom Urheberschutz erfasst werden, die lediglich einen gewissen Grad an individueller Prägung aufweisen.[917] Als ausschlaggebend wird dabei der Gesamteindruck des Musikstücks angesehen[918], wobei sich die Individualität eines Musikstücks aus einer Kombination der genannten Elemente oder aber aus einzelnen Gestaltungsmitteln ergeben kann[919]. Demnach kann die Schutzfähigkeit z.B. allein auf der Individualität eines Rhythmus' basieren.[920] Vom Schutz erfasst sind regelmäßig das Thema oder das musikalische Motiv eines Musikwerkes;[921] ausgeschlossen sind dagegen einzelne Töne oder Mehrklänge (Akkorde).[922]

Bei der Verbindung von Musik und Text (i.d.R. Gesang, Sprache oder Sprechgesang) handelt es sich nicht um ein einheitliches Werk, sondern um die Kombination eines Musikwerkes mit einem Sprachwerk, die rechtlich als sogenannte Werkverbindung gemäß § 9 UrhG zu qualifizieren ist.[923]

---

913 Vgl. *Münker*, S. 41.
914 Wandtke/Bullinger-*Bullinger*, § 2 UrhG, Rdnr. 69.
915 Urteil des *BGH* vom 24.01.1991 (Az. I ZR 72/89 – „Brown Girl II"), **GRUR** 1991, S. 533, 535; Urteil des *BGH* vom 26.09.1980 (Az. I ZR 17/78 – „Dirlada"), **GRUR** 1981, S. 267, 268; im Ansatz: Urteil des *BGH* vom 03.11.1967 (Az. Ib ZR 123/65), **GRUR** 1968, S. 321, 324.
916 Urteil des *BGH* vom 24.01.1991 (Az. I ZR 72/89 – „Brown Girl II"), **GRUR** 1991, S. 533; Urteil des *BGH* vom 03.02.1988 (Az. I ZR 143/86), **GRUR** 1988, S. 810, 811; Urteil des *BGH* vom 03.02.1988 (Az. I ZR 142/86 – „Ein bisschen Frieden"), **GRUR** 1988, S. 812, 814; Urteil des *BGH* vom 26.09.1980 (Az. I ZR 17/78 – „Dirlada"), **GRUR** 1981, S. 267, 268; Urteil des *BGH* vom 03.11.1967 (Az. Ib ZR 123/65), **GRUR** 1968, S. 321, 325.
917 Vgl. Urteil des *BGH* vom 22.06.1995 (Az. I ZR 119/93 – „Silberdistel"), **GRUR** 1995, S. 581, 582; Urteil des *BGH* vom 26.09.1980 (Az. I ZR 17/78 – „Dirlada"), **GRUR** 1981, S. 267, 268; Urteil des *BGH* vom 03.11.1967 (Az. Ib ZR 123/65), **GRUR** 1968, S. 321, 324; *Münker*, S. 43 f.; *Kornmeier*, 1.2.
918 Als Beurteilungsmaßstab ist die Auffassung der mit Musik vertrauten und hierfür aufgeschlossenen Verkehrskreise heranzuziehen, Urteil des *BGH* vom 26.09.1980 (Az. I ZR 17/78 – „Dirlada"), **GRUR** 1981, S. 267, 268.
919 Wandtke/Bullinger-*Bullinger*, § 2 UrhG, Rdnr. 70.
920 Urteil des *BGH* vom 24.01.1991 (Az. I ZR 72/89 – „Brown Girl II"), **GRUR** 1991, S. 533, 535; Urteil des *BGH* vom 26.09.1980 (Az. I ZR 17/78 - „Dirlada"), **GRUR** 1981, S. 267, 268.
921 Schricker-*Loewenheim*, § 2 UrhG, Rdnr. 122.
922 Zur urheberrechtlichen Schutzfähigkeit einzelner Werkkomponenten siehe ausführlich *Münker*, S. 45 ff., der das Freihaltebedürfnis der Allgemeinheit an Einzeltönen und –klängen u.a. mit ihrer „musikalischen Bausteinfunktion" begründet (S. 260).
923 Urteil des *BGH* vom 09.06.1982 (Az. I ZR 5/80), **GRUR** 1982, S. 743, 744; Urteil des *BGH* vom 02.10.1981 (Az. I ZR 81/79 – „Musikverleger III"), **GRUR** 1982, S. 41, 42; Schricker-*Loewenheim*, § 9 UrhG, Rdnr. 5.

Der ganz überwiegende Teil aller Musikstücke, die sich auf im Handel erhältlichen Tonträgern befinden, genießt demnach urheberrechtlichen Schutz. Dies gilt vor allem für aktuelle Werke aus dem Bereich der Unterhaltungsmusik, da bei diesen die Schutzfrist des § 64 UrhG[924] – anders als bei zahlreichen Werken der Klassischen Musik – noch nicht abgelaufen ist.

Neben Urheberrechten können „verwandte Schutzrechte" (auch Leistungsschutzrechte genannt) gemäß §§ 70 ff. UrhG an Musikwerken bestehen bzw. in Verbindung mit diesen stehen. Leistungsschutzrechte schützen keine Werke, also persönliche geistige Schöpfungen i.S.d. § 2 Abs. 2 UrhG, sondern künstlerische Leistungen anderer Art und unternehmerische Leistungen auf organisatorisch-technischem Gebiet.[925] Zu nennen sind vor allem das Recht des ausübenden Künstlers gemäß § 73 UrhG und das Recht des Tonträgerherstellers gemäß § 85 UrhG. Nach der Legaldefinition gewährt ersteres demjenigen Schutz, der ein Werk vorträgt oder aufführt oder bei einem Vortrag oder einer Aufführung eines Werkes künstlerisch mitwirkt. Instrumental- oder Vokaleinspielungen von Studio- und Live-Musikern zählen regelmäßig zu den Darbietungen i.S.d. § 73 UrhG[926], so dass die an einer CD-Produktion mitwirkenden Künstler Leistungsschutzrechte erwerben können[927]. § 85 UrhG gibt dem Hersteller eines Tonträgers ausschließliche, wirtschaftliche Verwertungsbefugnisse.[928] Dieses Recht wird ihm aufgrund der organisatorisch-technischen und wirtschaftlichen Leistung zuerkannt, die erforderlich ist, um Tonträger zu produzieren.[929] Eine solche Leistung gilt nur bei der erstmaligen Herstellung des Tonträgers als erbracht, § 85 Abs. 1 S. 3 UrhG.

Nur Berechtigte dürfen mit Musik bespielte Tonträger vervielfältigen und verbreiten bzw. deren Vervielfältigung oder Verbreitung zustimmen. Dazu zählen grundsätzlich der eigentliche Schöpfer (Komponist) nach §§ 7, 15 UrhG, der ausübende Künstler nach §§ 73, 75 UrhG sowie der Hersteller des Tonträgers nach § 85 UrhG.[930] Unter den Begriff der Tonträger fallen auch MP3-Files und andere digitale Musikdateien; Aufnahmetechnik und Format sind für das Vorliegen eines Tonträgers ohne Bedeutung. So hat das *OLG München* in seinem Grundsatzurteil vom 08.03.2001 ausgeführt, dass MIDI-Dateien Tonträger im Sinne von §§ 85 Abs. 1, 16 Abs. 2 UrhG sind.[931]

---

924 Danach erlischt das Urheberrecht 70 Jahre nach dem Tod des Urhebers (post mortem auctoris).

925 Vgl. Schricker-*Krüger*, Vor §§ 73 ff. UrhG, Rdnr. 2, § 73 UrhG, Rdnrn. 15-18 (zum Begriff der Darbietung), § 85 UrhG, Rdnr. 1.

926 Vgl. *Münker*, S. 180. Bei seiner Darbietung darf der Künstler nicht nur den Inhalt des Werkes wiedergeben, sondern er muss gleichzeitig ein Mindestmaß an künstlerischer Interpretation aufbringen, Schricker-*Krüger*, § 73 UrhG, Rdnr. 25; Urteil des *BGH* vom 14.11.1980 (Az. I ZR 73/78), **GRUR** 1981, S. 419, 421; siehe auch Wandtke/Bullinger-*Büscher*, § 73 UrhG, Rdnr. 2, wonach „maßgeblich ist, ob andere Personen diese Leistung in gleicher Weise reproduzieren können". Erfasst werden folglich individuelle Leistungen, die man neudeutsch als „künstlerische Performances" bezeichnet.

927 Diese geben den Inhabern verschiedene verwertungsrechtliche und persönlichkeitsrechtliche Befugnisse, die in den §§ 74 ff. UrhG festgeschrieben sind. Hervorzuheben ist § 75 Abs. 2 UrhG, wonach dem ausübenden Künstler das ausschließliche Recht zukommt, den Tonträger, auf dem seine Darbietung enthalten ist, zu vervielfältigen und zu verbreiten.

928 Anders als der ausübende Künstler erwirbt er (mit der Herstellung des Tonträgers) keine persönlichkeitsrechtlichen, sondern nur verwertungsrechtliche Befugnisse.

929 Schricker-*Vogel*, § 85 UrhG, Rdnr. 1 ff.

930 Des Weiteren sind die Rechte der Wortautoren berührt, wenn Musik mit Texten ohne Zustimmung vervielfältigt wird. Werden eingescannte CD-Cover beigelegt, sind außerdem die Urheberrechte der Grafiker und Designer betroffen.

931 Urteil des *OLG München* vom 08.03.2001 (Az. 29 U 3282/00) – veröffentlicht auf der Webseite des *MIDI File Hersteller Verbands Deutschland e.V.* unter http://www.mhv-online.de/olg_urteil.html.

Im Zusammenhang mit dem Internet ist außerdem von Interesse, wem das Recht zur öffentlichen Wiedergabe von Musikwerken zusteht. Denn das Verbreitungsrecht des § 17 UrhG bezieht sich nur auf körperliche Werkstücke, wozu Dateien nicht gehören.[932] § 15 Abs. 2 UrhG gibt nur dem Urheber das Recht zur öffentlichen Wiedergabe sowie ein Verbotsrecht für den Fall, dass ein anderer sein Werk ohne Zustimmung öffentlich wiedergibt. Ausübende Künstler und Tonträgerhersteller sind auf kompensatorische Vergütungsansprüche beschränkt (vgl. §§ 76 Abs. 2 und 86 UrhG), ein gesetzliches Verbotsrecht steht ihnen nicht zu.

Wann immer also MP3-Dateien vervielfältigt oder öffentlich wiedergegeben werden und keine Erlaubnis des bzw. der Berechtigten vorliegt, ist an sich eine Strafbarkeit aus § 106 UrhG gegeben.[933] Da von § 106 UrhG nur Nutzungen erfasst werden, die „in anderen als den erlaubten Fällen" vorgenommen werden, entfällt der Tatbestand jedoch beim Vorliegen einer nach dem Urheberrechtsgesetz erlaubten Nutzung.[934] Die sogenannten Schranken des Urheberrechts sind in den §§ 45 ff. UrhG geregelt und sehen – vor allem aus Gründen des Gemeinwohls – gesetzliche Ausnahmen von der strafrechtlichen Haftung vor.[935]

Die wichtigste Schranke findet sich in § 53 UrhG[936]: Dieser erklärt Vervielfältigungen zum privaten Gebrauch („Privatkopien") unter gewissen Voraussetzungen für zulässig. Der zur Vervielfältigung Befugte darf die Vervielfältigungsstücke auch durch einen anderen herstellen lassen, doch gilt dies für die Übertragung von Werken auf Bild- oder Tonträger nur, wenn es unentgeltlich geschieht. Gemäß § 53 Abs. 6 UrhG dürfen diese privat hergestellten Vervielfältigungsstücke grundsätzlich weder verbreitet noch zu öffentlichen Wiedergaben benutzt werden. Zur Kompensation für die Privatkopien sieht § 54 UrhG einen Anspruch des Rechtsinhabers auf eine angemessene Vergütung vor, dessen Durchsetzung über die Verwertungsgesellschaften (z.B. die *GEMA*) erreicht wird.[937]

Die Regelung des § 53 UrhG ist vor dem Hintergrund verfassungsrechtlicher Bestimmungen zu sehen. Gemeinsam mit den §§ 54-54h UrhG soll sie die Interessen der Allgemeinheit an einer beschränkten erlaubnisfreien Benutzung urheberrechtlich geschützter Werke (vgl. Art. 5 Abs. 1, 2 GG) mit den Interessen der Urheber (vgl. Art. 14 Abs. 1 UrhG) in Einklang bringen. Da es sich bei den vermögenswerten Befugnissen des Urhebers an seinem Werk um Eigentum i.S.d. Art. 14 GG handelt, ergibt sich für den Gesetzgeber die grundsätzliche Verpflichtung, dem Urheber das vermögenswerte Ergebnis seiner Leistungen zuzuordnen.[938] Die wirtschaftlichen Interessen der

---

[932] Siehe Fn. 391.

[933] Daneben ergibt sich regelmäßig eine Strafbarkeit wegen unerlaubter Eingriffe in verwandte Schutzrechte gemäß § 108 Abs. 1 Nr. 4 und Nr. 5 UrhG, der eine Freiheitsstrafe von bis zu drei Jahren oder eine Geldstrafe vorsieht. Da § 108 UrhG im Vergleich zu § 106 UrhG für den untersuchten Bereich eine untergeordnete Bedeutung zukommt, wird nachfolgend vorrangig auf die unerlaubte Verwertung urheberrechtlich geschützter Werke i.S.d. § 106 UrhG eingegangen.

[934] Hoeren/Sieber-*Sieber*, 19, Rdnr. 455.

[935] Wandtke/Bullinger-*Hildebrandt*, § 106 UrhG, Rdnr. 21.

[936] Wie bereits erwähnt, gilt die Schranke des § 53 UrhG nicht für Software, siehe oben Teil 2, C. I. 1.

[937] Gemäß § 54h UrhG ist die Abgabe verwertungsgesellschaftspflichtig. Sie wird von den Verwertungsgesellschaften eingezogen und an die Urheber verteilt.

[938] Beschluss des *BVerfG* vom 11.10.1988 (Az. 1 BvR 777, 882, 1239/85), **BVerfGE** 79, S. 1, 25; siehe auch den Beschluss des *BVerfG* vom 07.07.1971 (Az. 1 BvR 765/66), **BVerfGE** 31, S. 229, 240 f.: „Zu den konstituierenden Merkmalen des Urheberrechts als Eigentum im Sinne der Verfassung gehört die grundsätzliche Zuordnung des vermögenswerten Ergebnisses der schöpferischen Leistung an den Urheber im Wege privatrechtlicher Normierung und

Urheber werden wesentlich dadurch gewahrt, dass der Urheber das ausschließliche Recht zur Vervielfältigung und Verbreitung seiner Werke hat und Dritten Nutzungsrechte gegen Zahlung einer Vergütung einräumen kann.[939] Die Rechte des Urhebers erfahren jedoch eine Einschränkung durch die Sozialbindung des Eigentums gemäß Art. 14 Abs. 2 GG.[940]

Den Verwertungsinteressen der Urheber steht unter anderem das "Interesse der Allgemeinheit gegenüber, im Rahmen der Entwicklung der modernen Industriegesellschaft zu vorhandenen Informationen und Dokumentationen einen unkomplizierten Zugang haben zu müssen"[941]. Aufgabe des Urheberrechts soll es deshalb auch sein, die widerstreitenden Interessen angemessen auszugleichen.[942]

Der durch die §§ 53, 54 UrhG angestrebte Interessenausgleich basiert auf dem Gedanken monetärer Kompensation. Für die Einschränkung des dem Urheber grundsätzlich zustehenden Ausschließlichkeitsrechts an der Vervielfältigung seines Werkes zugunsten erlaubnisfreier Vervielfältigung im privaten Bereich erhält er einen gesetzlichen Vergütungsanspruch gemäß § 54 UrhG.[943] Die Informations- und Kommunikationserfordernisse der Allgemeinheit gebieten keineswegs, dass eine Vervielfältigung stets vergütungsfrei erfolgen muss.[944]

Der Vergütungsanspruch knüpft nicht an den einzelnen Vervielfältigungsvorgang an, sondern besteht in einer Abgabe, die u.a. die Hersteller von Vervielfältigungsgeräten und von Bild- und Tonträgern zu leisten haben und die sie über den Preis auf die Nutzer der dadurch eröffneten Vervielfältigungsmöglichkeiten abwälzen können.[945]

---

seine Freiheit, in eigener Verantwortung darüber verfügen zu können. Das macht den grundgesetzlich geschützten Kern des Urheberrechts aus". Auch nach der Rechtsprechung des *Europäischen Gerichtshofs (EuGH)* haben die Mitgliedstaaten dafür Sorge zu tragen, den „spezifischen Gegenstand" des Urheberrechts zu gewährleisten, Urteil des *EuGH* vom 17.05.1988 (Rs. 158/86 – *Warner Brothers ./. Christiansen*), **EuGH Slg.** 1988, S. 2605, 2629; Urteil des *EuGH* vom 04.11.1997 (Rs. C-337/95 – *Dior ./. Evora*), **GRUR Int.** 1998, S. 140, 144. Das Urheberrecht soll dem Rechtsinhaber einerseits eine Einkommensquelle sichern und ihm andererseits eine Form der Vertriebskontrolle ermöglichen, vgl. das Urteil des *EuGH* vom 20.01.1981 (verb. Rs. 55 und 57/80 – *Musik-Vertrieb membran ./. GEMA*), **EuGH Slg.** 1981, S. 147, 162.

939 Schricker-*Loewenheim*, § 53 UrhG, Rdnr. 1; Amtl. Begr., **BT-Drucks.** 10/837, S. 9: „Das Urheberrecht ordnet dem Schöpfer eines Werkes der Literatur, Wissenschaft oder Kunst die wirtschaftlichen Ergebnisse seiner schöpferischen Leistung zu und schützt ihn gegen die Verletzung seiner ideellen Interessen an seinem Werk. Die Vermögensinteressen des Urhebers an seinem Werk werden dadurch gewahrt, dass das Gesetz ihm die Verwertung des Werkes vorbehält".

940 Amtl. Begr. **BT-Drucks.** 10/837, S. 9: „Denn wie jedes absolute Recht ist auch das Urheberrecht sozialgebunden und unterliegt im Interesse der Gemeinschaft gewissen Schranken […] der Urheber entfaltet seine schöpferische Tätigkeit nicht losgelöst von seiner Umwelt, sondern eingebunden in seinen Kulturkreis und auf der Grundlage des Kulturschaffens vorangegangener Generationen. Andererseits ist der Urheber auf die Annahme und Aufnahme seines Werkes durch seine Zeitgenossen angewiesen. Kulturelle Schöpfung bedarf deshalb stets eines gegenseitigen Austauschs, eines Gebens und Nehmens. Dem Recht des Urhebers an der Nutzung seines Werkes steht daher das Recht der Allgemeinheit an dem ungehinderten Zugang zu den Kulturgütern gegenüber". Siehe hierzu auch das Urteil des *BGH* vom 16.01.1997 (Az. I ZR 9/95 – „CB-Infobank I"), **BGHZ** 134, S. 250, 263, wonach § 53 UrhG berücksichtigt, „dass der Urheber mit seinem materiellen geistigen Eigentum in die Sozialpflichtigkeit der Eigentumsordnung gemäß Art. 14 Abs. 1 GG eingebunden ist".

941 Urteil des *BGH* vom 16.01.1997 (Az. I ZR 9/95 – „CB-Infobank I"), **BGHZ** 134, S. 250, 263.

942 Beschluss des *BVerfG* vom 07.07.1971 (Az. 1 BvR 765/66), **BVerfGE** 31, S. 229, 242; Amtl. Begr., **BT-Drucks.** 10/837, S. 9.

943 Die Regelung in § 53 Abs. 1 S. 1 UrhG ist als Einräumung einer „gesetzlichen Lizenz" zu qualifizieren.

944 Eine kompensationslose Einräumung von Nutzungsrechten riefe gar verfassungsrechtliche Bedenken hervor, vgl. den Beschluss des *BVerfG* vom 07.07.1971 (Az. 1 BvR 765/66) **BVerfGE** 31, S. 229, 243; danach kann ein gesteigertes öffentliches Interesse zwar einen Vorrang vor den Belangen des Urhebers bewirken, allerdings sei ihm in diesen Fällen eine (kompensatorische) Vergütung zuzubilligen.

945 Schricker-*Loewenheim*, § 53 UrhG, Rdnr. 2; siehe hierzu auch den Beschluss des *BVerfG* vom 11.10.1988 (Az. 1 BvR 777, 882, 1239/85), **BVerfGE** 79, S. 1, 26: „In der verfassungsgerichtlichen Rechtsprechung ist geklärt, dass es zulässig

Dass der Vergütungsanspruch nicht an einzelne Vervielfältigungsvorgänge anknüpft, folgt aus praktischen und rechtlichen Erwägungen. Zum einen gilt es als unmöglich, sämtliche Vervielfältigungsvorgänge im privaten Bereich zu erfassen[946], zum anderen wäre hierzu ein Eindringen in die Privatsphäre der Benutzer erforderlich, was letztendlich auf unverhältnismäßige Eingriffe in Grundrechte hinauslaufen könnte.[947]

2. Strafbarkeit von „Online-Musikpiraten" nach geltendem Recht[948]

a) Mitglieder von MP3-Gruppen

Mangels erlaubter Nutzung können sich die Mitglieder von MP3-Gruppen nicht auf die Ausnahmeregelungen der §§ 45 ff. UrhG berufen. Bei sämtlichen Up- und Downloadvorgängen entstehen illegale Vervielfältigungsstücke der geschützten Musikwerke, weshalb sich eine Strafbarkeit der Handelnden aus § 106 Abs. 1, 1. Handlungsalternative UrhG ergibt.

Beim „Rippen" von CD-Titeln auf die Festplatte entstehen ebenfalls Vervielfältigungsstücke. Gleiches gilt für das Kodieren der WAV-Dateien in das MP3-Format. Selbst wenn der Coder die Original-CD gekauft hat, kann er sich nicht auf das Recht zur Privatkopie berufen, denn die gesetzliche Lizenz aus § 53 UrhG umfasst keine Vervielfältigungen zum Zwecke der Verbreitung. Daher liegen auch im „Rippen" von Audio-CDs und im Encoden von WAV-Dateien durch Gruppenmitglieder strafbare Handlungen i.S.v. § 106 UrhG.

Sofern Kopierschutzsysteme umgangen werden, um das „Rippen" von CD-Titeln zu ermöglichen, muss zwischen den Umgehungsmethoden der Ripper unterschieden werden: Wird manipulativ in die auf dem Ursprungsdatenträger befindlichen Daten eingegriffen, kommt eine Strafbarkeit des Handelnden aus den §§ 202a, 303a StGB und § 17 UWG in Betracht.[949] Dies gilt vor allem für die Fälle, in denen der Ripper Musikdateien aus verschlüsselten Medien (z.B. DVDs oder Computerspiele-CD-ROMs) extrahiert, um diese im MP3-Format zu veröffentlichen. Andere Umgehungsmethoden, wie z.B. das Herstellen einer „rippfähigen" CD-Kopie[950] oder digitale bzw. analoge

---

ist, den unmittelbar nur schwer zu erfassenden privaten Nutzer fremder Urheberleistung mittelbar dadurch zu belasten, dass die zur Herstellung privater Kopien erforderlichen Industrieprodukte mit (abzuwälzenden) Abgaben belegt werden".

946 Siehe hierzu das Urteil des *BGH* vom 16.01.1997 (Az. I ZR 9/95 – „CB-Infobank I"), **BGHZ** 134, S. 250, 263: „Diese Vorschrift (Anm. des Verfassers: Gemeint ist § 53 UrhG) trägt zunächst der Tatsache Rechnung, dass ein Verbot von Vervielfältigungen im privaten Bereich praktisch kaum durchsetzbar ist".

947 Vgl. die Ausführungen von *Flechsig*, **GRUR** 1993, S. 532: „Der Gesetzgeber hatte erkannt, dass demgemäß auch ein Verbot der privaten Vervielfältigung in der Praxis nicht durchgesetzt werden könnte, wenn nicht die Wohnung eines jeden Staatsbürgers daraufhin überprüft werden dürfte, ob er ein Vervielfältigungsgerät besitzt, mit diesem urheberrechtlich geschützte Werke aufnimmt und hierfür die Genehmigung des Urhebers nachweisen kann"; **BT-Drucks.** 4/270, S. 71: "Eine solche Kontrolle würde jedoch dem in Art. 13 GG ausgesprochenen Grundsatz der Unverletzlichkeit der Wohnung widersprechen. Übertretungen einen solchen Verbots könnten daher nur durch Zufall oder Denunziation bekannt werden".

948 Nachtrag: Die vorliegende Arbeit wurde am 26.05.2003 als Dissertation eingereicht. Dieses Datum markiert folglich den Stand der Bearbeitung. Am 10.09.2003 ist das Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft (**BGBl.** I 2003, S. 1774-1788) in Kraft getreten, weshalb die Überschrift nunmehr folgendermaßen zu verstehen ist: „Strafbarkeit von Online-Musikpiraten nach bis zum 10.09.2003 geltendem Recht". Zur Relevanz der UrhG-Änderungen für die nachfolgende Darstellung siehe den Nachtrag in Fn. 997.

949 So auch die Einschätzung von *Czirnich* in **PC Direkt**, 2/2001, S. 54, für softwaremäßig realisierte Kopierschutzmechanismen.

950 Mittels bestimmter CD-Brennprogramme lässt sich ein Teil der kopiergeschützten Audio-CDs dergestalt kopieren, dass die gebrannte CD keinen Kopierschutz mehr aufweist und deshalb von CD-ROM-Laufwerken ausgelesen werden kann.

Überspielungen, begründen keine besondere Strafbarkeit; allerdings beinhalten sie in der Regel strafbare Vervielfältigungshandlungen gemäß § 106 UrhG.

Indem die Kuriere der Gruppen die MP3-Releases auf zahlreichen Servern ablegen, machen sie sich auch nach der 3. Handlungsalternative des § 106 Abs. 1 UrhG strafbar, sofern eine Vielzahl von ihnen unbekannten Personen Zugriff auf die Dateien erhält. Denn die Verbreitung in unkörperlicher Form fällt unter die in § 15 Abs. 2 UrhG (Recht der öffentlichen Wiedergabe) geregelten Fälle und muss ebenso wie die Vervielfältigung und die körperliche Verbreitung vom Rechtsinhaber erlaubt werden.

Eine Strafbarkeit der Gruppenmitglieder gemäß § 129 StGB ist aus den bereits dargelegten Gründen abzulehnen.[951]

b) Betreiber von Webseiten und permanenten FTP-Servern

Wer Webseiten oder FTP-Server einrichtet bzw. betreibt, von denen Musikdateien heruntergeladen werden können, ist als Content Provider gemäß § 8 Abs. 1 TDG für die angebotenen Informationen voll verantwortlich.[952] Sind die Seiten öffentlich zugänglich und unterhält der Betreiber keine persönliche Beziehung zu den Herunterladenden, stellt das Bereithalten urheberrechtlich geschützter Musikstücke auf einem Server eine unbenannte Wiedergabe i.S.v. § 15 Abs. 2 UrhG dar. Sofern dem Betreiber diese nicht gestattet ist, macht er sich gemäß § 106 Abs. 1, 3. Handlungsalternative UrhG strafbar.

§ 53 UrhG wäre nur einschlägig, wenn man Werke auf einen Server stellte, ohne dabei Dritten den Zugriff zu gestatten. Bereits die Weitergabe der URL oder der Zugangsdaten wären als Entfernung aus der Schutzzone des privaten Bereichs zu bewerten.[953]

Gleiches gilt für das Setzen von Links, die bewirken, dass ein geöffneter P2P-Client mit einem Download beginnt, nachdem man auf den Link geklickt hat.[954] Sofern der Link auf eine urheberrechtlich geschützte Datei verweist, die unmittelbar über das P2P-System wieder anderen Nutzern angeboten wird, liegt eine Beihilfe des Linksetzers an der unerlaubten öffentlichen Wiedergabe des Nutzers vor.

c) Profit-Pirates

Personen, die den Tatbestand des § 106 Abs. 1 UrhG verwirklichen und dabei mit Gewinnabsicht handeln, machen sich gemäß § 108a UrhG der gewerbsmäßigen unerlaubten Verwertung von urheberrechtlich geschützten Werken strafbar.[955] § 108a UrhG sieht eine Freiheitsstrafe von bis zu 5 Jahren vor und ist bereits dann einschlägig, wenn jemand sein Web-Downloadangebot mit Bannerwerbung finanziert.

---

951 Siehe oben Teil 2, C. I. 3. b) (1) (c).
952 Hinsichtlich der Haftung der Webseiten-Betreiber für Hyperlinks ist auf die Ausführungen bei Teil 2, C. I. 2. c) (5) zu verweisen.
953 *Scheja*, **c't** 6/2002, S. 171.
954 Siehe Teil 3, A. VII. 1. c).
955 Siehe dazu oben Teil 2, C. I. 3. b) (1) (b).

d) „Endnutzer" von MP3-Dateien

(1) Herunterladen von Musikdateien

Ganz gleich, von wo sich ein Internetnutzer ein MP3-File herunterlädt, ob aus einer Tauschbörse, von einer Webseite, aus einer Newsgroup oder von einem FTP-Server, immer findet eine urheberrechtlich relevante Vervielfältigung statt.[956] Unklar ist in diesem Zusammenhang, ob sich der Nutzer auf sein Recht zur privaten Vervielfältigung aus § 53 UrhG berufen kann, was eine Strafbarkeit gemäß § 106 UrhG entfallen ließe. Vorab sei daran erinnert, dass § 53 UrhG auch digitale Vervielfältigungshandlungen erfasst.[957] Angesichts der Unkontrollierbarkeit der Vervielfältigung im privaten Umfeld ist das Ausdehnen der Schranke auf den digitalen Bereich sinngerecht und rechtspolitisch zu befürworten.[958]

Unterschiedliche Auffassungen gibt es hinsichtlich der Anforderungen an die Kopiervorlage bzw. an die Besitzerlangung derselben: Während weitgehend Einigkeit darüber besteht, dass der Nutzer nur dann in den Genuss der Privilegierung aus § 53 UrhG kommen kann, wenn er rechtmäßig in den Besitz der Kopiervorlage gekommen ist (ungeschriebenes Merkmal des § 53 UrhG)[959], wird von einem Teil der Literatur[960] gefordert, die Vorlage müsse darüber hinaus ein rechtmäßig erstelltes Original – also urheberrechtlich korrekt lizenziert – sein. Die Frage, ob ein Internetnutzer rechtmäßig in den Besitz einer Kopiervorlage kommt, wenn er eine fremde MP3-Datei herunterlädt, wird in der Literatur mehrheitlich bejaht.[961] Argumentiert wird unter anderem mit einer *KG*-Entscheidung[962], in deren Vorfeld sich ein Kopierer durch eigenes rechtswidriges Verhalten in den Besitz des Kopierstücks versetzt hatte. Er begründete fehlerhaften Besitz durch unberechtigtes Ansichnehmen der Kopiervorlage. Das *KG* führte sinngemäß aus, dass es dem Rechtsgedanken des § 53 Abs. 1 UrhG zuwiderliefe, wenn einer Person, die das Werkstück widerrechtlich an sich gebracht hat, das Recht eingeräumt würde, zur Erinnerung an sein rechtswidriges Tun ein Vervielfältigungsstück herzustellen[963]. Es kommt folglich nur darauf an, wie die Besitzverschaffung stattgefunden hat. Wer mit dem Einverständnis des Download-Anbieters eine MP3-Datei aus dem Netz lädt und keine gewerbliche Verwertung, sondern reine Privatnutzung anstrebt, begeht weder Diebstahl noch Unter-

---

956 Das Vervielfältigungsrecht der §§ 15 Abs. 1 Nr. 1, 16 Abs. 1 UrhG ist bereits berührt, wenn der Nutzer das digitale Musikwerk in den Arbeitsspeicher des Computers lädt, vgl. *Bosak*, **CR** 2001, S. 176 f.. Eine (sukzessive) Teilvervielfältigung ist erst dann strafbar, wenn der heruntergeladene Werkteil für sich genommen die Voraussetzungen des § 2 Abs. 2 UrhG erfüllt, Wandtke/Bullinger-*Hildebrandt*, § 106 UrhG, Rdnrn. 12 und 14.

957 Siehe Fn. 796.

958 So auch *Dreier* in *Schricker*, Urheberrecht auf dem Weg in die Informationsgesellschaft, S. 166; *Kreutzer*, Napster, Gnutella & Co. – Teil 1, **GRUR** 2001, S. 199. Siehe hierzu auch das Urteil des *BGH* vom 16.01.1997 (Az. I ZR 9/95 – „CB-Infobank I"), **BGHZ** 134, S. 250, 263: „Diese Vorschrift (Anm. des Verfassers: Gemeint ist § 53 UrhG) trägt zunächst der Tatsache Rechnung, dass ein Verbot von Vervielfältigungen im privaten Bereich praktisch kaum durchsetzbar ist.".

959 So *Harke*, **c't** 5/2000, S. 114; *Kreutzer*, Napster, Gnutella & Co. – Teil 1, **GRUR** 2001, S. 200.

960 *Hamann*, in **FOCUS** 5/2000, S. 248; *Braun*, Vertreter der Rechtsabteilung der *IFPI*, bei *Harke*, **c't** 5/2000, S. 113: Etwas, das illegal angeboten würde, könne nicht rechtmäßig kopiert werden, denn § 53 Abs. 1 UrhG setze immer eine rechtmäßige Kopiervorlage voraus; ähnlich auch *Strömer*, in **PC Direkt**, 2/2001, S. 54.

961 Z.B. von *Harke*, **c't** 5/2000, S. 114; *Mönkemöller*, **GRUR** 2000, S. 667; *Kreutzer*, Napster, Gnutella & Co. – Teil 1, **GRUR** 2001, S. 200.

962 Urteil des *Kammergerichts (KG) Berlin* vom 05.03.1991 (Az. 5 U 4433/91), **GRUR** 1992, S. 168 f.

963 Vgl. *Mönkemöller*, **GRUR** 2000, S. 667.

schlagung noch Hehlerei, so dass von einer rechtmäßigen Besitzerlangung ausgegangen werden kann.[964]

Dass es sich zusätzlich bei der Vorlage für die eigene Kopie um ein rechtmäßig erstelltes Original handeln muss, lässt sich weder dem Gesetz entnehmen, noch wird es von der Rechtsprechung verlangt.[965] § 53 UrhG enthält eine gesetzliche Lizenz, eine vertragliche muss nicht erworben werden. Da kein rechtsgeschäftlicher Erwerb von Rechten nötig ist, spielt es keine Rolle, dass es im Urheberrecht keinen gutgläubigen Rechtserwerb gibt. Die Rechtsbeziehungen zwischen Anbieter und privatem Nutzer sind unerheblich.[966] Erklärte man das Verhältnis von Berechtigtem und Anbieter für relevant, wäre dem privaten Nutzer eine Prüfungspflicht der Rechtslage auferlegt, die er unmöglich erfüllen könnte.[967] Hier muss dasselbe gelten, wie wenn der Nutzer eine rechtmäßige Privatkopie einer ausgeliehenen CD oder Videokassette erstellt; denn in diesen Fällen wird ihm auch keine Prüfung der lizenzrechtlichen Situation zwischen Tonträgerunternehmen (bzw. Filmvertrieb) und Verleiher abverlangt. Sofern sich also der Nutzer Musik herunterlädt, ist dies unabhängig davon, ob das Angebot derselben rechtmäßig war, nach § 53 Abs. 1 UrhG zustimmungsfrei zulässig.[968]

Etwas anderes mag gelten, wenn er konkrete Kenntnis hatte, dass die Dateien nur hergestellt wurden, um unerlaubt verbreitet zu werden. Hinweise hierauf wären die typischen Beigaben zu MP3-Gruppen-Releases wie NFO-, SFV- oder M3U-Dateien, die Art der Dateinamen oder der Inhalt des ID3-Tags. Auch wenn Kopien gleichen Ursprungs massenhaft in einer Tauschbörse auftauchen, ist fraglich, ob dem Downloader noch die Privilegierung des § 53 UrhG zugute kommen kann. Denn in diesen Fällen ist für die meisten Internetnutzer offenkundig, dass nichtlizenzierte Kopiervorlagen angeboten werden. Das Argument mit den überhöhten Anforderungen an eine Prüfungspflicht der Rechtslage greift in diesen Fällen nicht mehr.

Ebenso könnte eine Berufung auf § 53 UrhG ausscheiden, wenn der Nutzer weiß, dass er Promo-Kopien oder andere Vorabveröffentlichungen von Musikwerken herunterlädt. Denn Hauptzweck des § 53 UrhG ist es, die Interessen der Allgemeinheit an einer beschränkten erlaubnisfreien Benutzung urheberrechtlich geschützter Werke mit den Interessen der Urheber in Einklang zu bringen[969]. Promo-Kopien und Vorabveröffentlichungen sind gerade nicht für die Allgemeinheit bestimmt, sondern für einen kleinen Kreis ausgewählter Rezipienten, weshalb in Einklang mit der ratio legis des § 53 UrhG eine Berufung auf diesen versagt werden kann.

Die Nutzung einer Privatkopie ist auf den rein privaten Gebrauch beschränkt. Hierunter ist der „Gebrauch in der Privatsphäre zur Befriedigung rein persönlicher Bedürfnisse durch die eigene Person oder die mit ihr durch ein persönliches Band verbundenen Personen“ zu verstehen.[970] Wann ein solcher privater Gebrauch vorliegt, ist grundsätzlich anhand des Einzelfalls zu überprüfen. Ist

---

964 *Harke*, **c't** 5/2000, S. 114; *Malpricht*, **NJW-CoR** 2000, S. 234.
965 Beachte hierzu den Nachtrag in Fn. 997.
966 *Harke*, **c't** 5/2000, S. 114; *Kreutzer*, Napster, Gnutella & Co. – Teil 1, **GRUR** 2001, S. 200; a.A.: *Scheja*, **c't** 6/2002, S. 172.
967 *Kreutzer*, Napster, Gnutella & Co. – Teil 1, **GRUR** 2001, S. 200.
968 *Kreutzer*, Napster, Gnutella & Co. – Teil 1, **GRUR** 2001, S. 200.
969 Vgl. Schricker-*Loewenheim*, § 53 UrhG, Rdnr. 1.
970 Urteil des *BGH* vom 14.04.1978 (Az. I ZR 111/76 – „Vervielfältigungsstücke“), **GRUR** 1978, S. 474, 475; Wandtke/Bullinger-*Lüft*, § 53 UrhG, Rdnrn. 13 und 14; Schricker-*Loewenheim*, § 53 UrhG, Rdnrn. 11 und 12.

Öffentlichkeit i.S.v. § 15 UrhG gegeben, liegt kein Privatgebrauch vor. Eine Familienfeier ist nicht öffentlich; das Betriebsfest eines größeren Betriebes dagegen schon.[971] Alles, was man für sich und die in seinem Haushalt lebenden Personen kopiert, dürfte jedoch unter die Ausnahme des § 53 Abs. 1 UrhG fallen. Die private Weitergabe an Dritte, zu denen eine persönliche Beziehung besteht, ist nämlich keine Verbreitung im Sinne des UrhG. Unzulässig ist nur das Verschenken an Personen, zu denen keine persönliche Beziehung besteht.[972]

Nicht von § 53 Abs. 1 UrhG privilegiert ist außerdem eine Vervielfältigung, die der Nutzer in erster Linie zum Tausch mit anderen über ein Filesharing-Netz anfertigt, da die Bestimmung des Vervielfältigungsstückes hier von vornherein in der Entäußerung desselben in den außerprivaten Bereich liegt[973].

Die Schranke gestattet die Anfertigung „einzelner Vervielfältigungsstücke", worunter nach der zuvor zitierten *BGH*-Entscheidung, abhängig von der individuellen Bedürfnislage des Vervielfältigenden, bis zu sieben Kopien zu verstehen sind[974]. Allerdings ist zu beachten, dass das *BGH*-Urteil zu Papierkopien erging und aus einer Zeit stammt, in der das digitale Kopieren von geschützten Inhalten nicht an der Tagesordnung war. Dennoch kann man davon ausgehen, dass das Gesetz mehr als eine Privatkopie von Musikwerken gestattet.[975]

Privatkopien dürfen weder verbreitet noch zu öffentlichen Wiedergaben benutzt werden, § 53 Abs. 6 S. 1 UrhG. Der Verkauf einer Privatkopie ist ebenso wenig erlaubt wie das Behalten und Weiterverwenden einer solchen Kopie, nachdem man das Original veräußert hat.[976]

(2) Bereitstellen bzw. Anbieten von Musikdateien

Auch der „private Endnutzer" kann – mehr oder weniger freiwillig – zum Anbieter von geschützten Musikwerken werden, wenn er beispielsweise eine Tauschbörsensoftware benutzt, und ein Verzeichnis mit MP3-Dateien auf seiner Festplatte für die anderen Nutzer des Filesharing-Netzes freigegeben ist.

Die Frage, ob das Bereitstellen bzw. Anbieten von Musikdateien über ein P2P-System eine strafrechtlich relevante unerlaubte Verwertungshandlung darstellt, wird überwiegend bejaht.[977] Dies liegt insofern nahe, als § 53 Abs. 6 UrhG ausdrücklich regelt, dass private Vervielfältigungsstücke nicht verbreitet oder zu öffentlichen Wiedergaben genutzt werden dürfen. Dass ein Fall der öffentlichen Wiedergabe i.S.v. § 15 Abs. 2 UrhG vorliegt, wenn ein Nutzer Musikdateien für zumeist unbe-

---

971 Fromm/Nordemann-*Nordemann*, § 15, Rdnr. 4.
972 *Harke*, **c't** 5/2000, S. 114.
973 *Kreutzer*, Napster, Gnutella & Co. – Teil 1, **GRUR** 2001, S. 200.
974 Urteil des *BGH* vom 14.04.1978 (Az. I ZR 111/76 – „Vervielfältigungsstücke"), **GRUR** 1978, S. 476.
975 Vgl. *Harke*, **c't** 5/2000, S. 114.
976 *Himmelein/Schmitz*, **c't** 2/2002, S. 83.
977 Schwerdtfeger-*Kreuzer*, S. 231; *Harke*, **c't** 5/2000, S. 114; *Mönkemöller*, **GRUR** 2000, S. 669; *Hamann*, in **FOCUS** 5/2000, S. 248.

kannte Dritte zum Download bereitstellt, wurde bereits dargelegt[978]. Öffentliche Wiedergaben von geschützten Werken über das Internet bedürfen grundsätzlich der Zustimmung aller Rechtsinhaber und werden – wenn überhaupt – nur in engen Grenzen von der Schranke des § 52 UrhG erfasst.[979]

Somit macht sich ein Anbieter von MP3-Dateien über ein P2P-System gemäß § 106 Abs. 1, 3. Handlungsalternative UrhG strafbar. Eine strafbare Beihilfe zur unerlaubten Vervielfältigung der Herunterladenden durch Freigeben des – danach öffentlich zugänglichen – Verzeichnisses auf der Festplatte des Nutzers kommt nur dann in Betracht, wenn im Herunterladen eine vorsätzliche rechtswidrige Haupttat zu erblicken ist. Dies ist nicht der Fall, wenn beim Herunterladenden die Voraussetzungen des zulässigen privaten Gebrauchs gemäß § 53 Abs. 1 S. 1 UrhG vorliegen; dann würde eine Strafbarkeit gemäß § 106 UrhG entfallen, es fehlte somit an einer teilnahmefähigen Haupttat.

Fraglich ist die urheberrechtliche Beurteilung, wenn über ein P2P-System, das Multi-Source-Downloading[980] unterstützt, keine kompletten Dateien bereitgestellt werden, sondern lediglich Fragmente derselben. Grundsätzlich können auch kleinste Teile eines Werkes urheberrechtlichen Schutz genießen[981], allerdings muss der Teil für sich genommen schutzfähig sein. Ob dies zutrifft, muss in jedem einzelnen Fall entschieden werden. Häufig werden rein abstrakte Datenpakete angeboten, die für sich genommen keine Nutzung ermöglichen. Fehlt z.B. der Header einer Datei, liegt nutzloser „Datenmüll" vor, mit dem kein Nutzer etwas anfangen kann. Urheberrechtlich relevant dürfte somit nur das Angebot von kompletten Dateien oder Fragmenten sein, die – für sich genommen – Werkqualität besitzen bzw. überhaupt nutzbar sind.[982]

Wird Personen der Zugang zu einem privaten FTP-Server mit Musikdateien ermöglicht, zu denen der Betreiber eine persönliche Beziehung unterhält, ist dies zulässig. Die individuelle Weiterübertragung eines fremden, heruntergeladenen Werkes als Attachment einer E-Mail ist weder als öffentliche Wiedergabe noch als Verbreitung zu qualifizieren und damit ebenfalls gestattet, soweit auch der Empfänger das Privileg des § 53 UrhG genießt.[983]

---

978 A.A. zum Anbieten von Musikdateien in Online-Tauschbörsen: *Scheja*, **c't** 6/2002, S. 171, nach deren Auffassung die elektronische Bereitstellung urheberrechtlich geschützter Werke derzeit nicht vom deutschen Urheberrecht erfasst wird.
979 Vgl. *Kreutzer*, Napster, Gnutella & Co. – Teil 1, **GRUR** 2001, S. 201, der davon ausgeht, dass das Angebot von Dateien über ein Filesharing-Netz gemäß § 52 Abs. 1 S. 1 UrhG ohne Zustimmung der Berechtigten zulässig ist. Dabei sei es unerheblich, ob der Nutzer eigene, vom Berechtigten direkt erworbene Dateien öffentlich wiedergibt, oder ob er private Vervielfältigungsstücke i.S.v. § 53 UrhG bereitstellt, die auch unbekannten Ursprungs sein können. *Kreutzer* begründet dieses Ergebnis damit, dass § 53 Abs. 6 UrhG in den Grenzen des § 52 UrhG Anwendung finde. Dieses Verständnis der Gesetzessystematik sei keineswegs interessenwidrig, da die Nutzungsentschädigung gemäß § 52 Abs. 1 S. 2 UrhG auch dann an den Berechtigten gezahlt werden müsse, wenn eine Privatkopie zur öffentlichen Wiedergabe verwendet würde.
980 Siehe Teil 3, A. VII. 1. a).
981 Schricker-*Loewenheim*, § 16 UrhG, Rdnr. 14.
982 Siehe hierzu auch Wandtke/Bullinger-*Hildebrandt*, § 106 UrhG, Rdnrn. 12 und 14 - zur (sukzessiven) Teilvervielfältigung; nach *Hildebrandt* ist diese erst dann strafbar, wenn der fertiggestellte Werkteil die Voraussetzungen des § 2 Abs. 2 UrhG erfüllt. Aus den dargelegten Gründen sollte dies auch für „Teilangebote" gelten.
983 Schwerdtfeger-*Kreuzer*, S. 231.

Exkurs – Kompensationsansprüche für private Online-Verwertung von Musikwerken

Wie bereits erwähnt, haben Schöpfer einen Anspruch aus § 54 UrhG auf angemessenen Ausgleich für entgangene Tantiemen wegen des Heimkopierens. Der Anspruch richtet sich gegen die Hersteller und Importeure von bespielten Tonträgern, Leermedien und Aufnahmegeräten und ist gegenüber den Verwertungsgesellschaften geltend zu machen.[984] Eine wichtige Überlegung, die zu § 54 geführt hat, war, dass ein Verbot des Heimkopierens nicht zu überwachen sei.[985] Daher wurde eine pauschale Urheberrechtsabgabe eingeführt, die seitdem von der für den Musikbereich zuständigen *GEMA* auf Tonträger, Leermedien und Aufnahmegeräte erhoben wird.[986] In der Regel werden die Kosten für die Vergütungspflicht über den Kaufpreis auf den Konsumenten umgelegt. Zu den Leermedien zählen auch CD-Rohlinge, jedoch nur solche, die speziell für das Brennen von Musikdaten vorgesehen sind[987]. Auf Daten-Rohlinge, Festplatten, die meisten Arten von Wechselmedien und auf Brennsoftware erhebt die *GEMA* derzeit (noch) keine Abgabe[988]. Allerdings handelt es sich bei CD-Brennern um vergütungspflichtige Geräte i.S.v. § 54 Abs. 1 S. 1 UrhG. Diese Auffassung der *GEMA* hat das *Landgericht Stuttgart* mit seinem Urteil vom 21.06.2001[989] im Prozess der in der *Zentralstelle für private Überspielungsrechte* (*ZPÜ*) zusammengeschlossenen Verwertungsgesellschaften gegen den CD-Brennerhersteller *Hewlett-Packard* bestätigt[990].

In der Schwebe befindet sich ein Streit um Abgaben auf Komplett-PCs. Die von der *ZPÜ* vertretenen Verwertungsgesellschaften möchten eine Urheberrechtsabgabe – im Gespräch sind 30 € pro PC[991] – durchsetzen, stoßen bei ihrem Vorhaben jedoch auf Widerstand der Computerhersteller, die im IT-Branchenverband *BITKOM*[992] zusammengeschlossen sind. Die Vertreter von *BITKOM* verweisen auf die Möglichkeiten des Digital Rights Management (DRM)[993] und bezeichnen pauschale Vergütungen als „Anachronismus im digitalen Zeitalter". DRM-Technologien seien nach Aussage der *BITKOM*-Vertreter geeignet, um individuelle Privatnutzungsvorgänge zu erfassen und exakt abzurechnen. Kompensationsabgaben könnten somit vom Anwender selbst eingezogen werden, die Hersteller von Vervielfältigungsgeräten könnten endlich von der Pauschale befreit werden. *BITKOM* hatte sich in Gesprächen bereit erklärt, während einer Übergangsfrist zusätzliche Abgaben auf Drucker, CD-Brenner etc. zu zahlen. Mit Ablauf der Frist sollten die pauschalen Vergütungssysteme durch individuelle Vergütungsmodelle abgelöst werden. Hiermit war die *ZPÜ* jedoch nicht einverstanden, das Recht auf private Kopien dürfe nicht aufs Spiel gesetzt werden.[994] Es bleibt

---

984 *Himmelein/Schmitz*, **c't** 2/2002, S. 83; zu beachten ist die Rechtsprechung des *Bundesverfassungsgerichts*, wonach die Vergütungspflicht nicht an die tatsächliche urheberrechtliche Inanspruchnahme des Geräts bzw. Bild-/Tonträgers anknüpft, sondern an die Möglichkeit hierzu – **BVerfGE** 31, S. 255.

985 Siehe bereits die Ausführungen zu Teil 3, C. I. 1.

986 Die Einziehung der Vergütung erfolgt durch die *Zentralstelle für private Überspielungsrechte (ZPÜ)*, die auch für andere Verwertungsgesellschaften tätig ist. Nach Aussage des *IFPI*-Vertreters *Zombik* betrügen die Einnahmen aus der Pauschale nicht einmal 4% des tatsächlichen Marktwertes der geschützten Rechte, vgl. *Krempl*, Content an der Kette, **c't** 4/2002, S. 32.

987 Die *GEMA*-Abgabe beträgt ca. 6,14 Cent pro Stunde Spieldauer.

988 Vgl. *Hellmich*, **c't** 21/1998, S. 136.

989 Urteil des *LG Stuttgart* vom 21.06.2001 (Az. 17 O 519/00), veröffentlicht auf der Webseite der *GEMA* unter http://www.gema.de/urheberrecht/rechtsprechung/lg_stuttgart_21062001.shtml.

990 Mittlerweile haben sich die Parteien auf eine Urheberabgabe i.H.v. 7,50 € (bzw. 6 € für Mitglieder des Branchenverbands *BITKOM*) pro verkauftem CD-Brenner geeinigt, vgl. **c't** 17/2002, S. 50.

991 *Wilkens/Zota*, **c't** 6/2002, S. 17.

992 http://www.bitkom.org.

993 Siehe unten Teil 3, C. II. 3.

994 *Wilkens/Zota*, **c't** 6/2002, S. 17.

abzuwarten, wie sich der Interessenkonflikt entwickelt. Beachtung verdient in diesem Zusammenhang, dass die Unterhaltungsindustrie verstärkt kopiergeschützte Tonträger auf den Markt bringt. Da somit das Anfertigen einer Privatkopie für die meisten Anwender unmöglich gemacht wird, wird die Berechtigung pauschaler Vergütungsmodelle zusätzlich in Frage gestellt, was den derzeitigen Status der Verwertungsgesellschaften gefährden könnte.

Für die Privilegierungen im Online-Bereich gibt es zur Zeit keine Kompensationsmodelle. Vereinzelt wird die Einführung pauschaler Vergütungsmodelle vorgeschlagen, da die Erfassung einzelner Nutzungshandlungen technisch noch nicht zu realisieren sei.[995] Vorübergehend – bis eine Vergütung für Online-Verwertungen gesetzlich geregelt ist – bleibt es bei der erlaubten privaten Nutzung fremden geistigen Eigentums, auch wenn eine Vergütung gemäß § 54 UrhG nicht entrichtet wird.[996]

3. Strafbarkeit von „Online-Musikpiraten" nach zu erlassendem Recht[997] (Betrachtung de lege ferenda)[998]

Wie bereits erwähnt, sind die Mitgliedstaaten der EU angewiesen, in die nationalen Gesetze ein zusätzliches Verwertungsrecht für den Rechtsinhaber aufzunehmen, welches die Online-Nutzungen urheberrechtlich geschützter Werke umfasst. Das Recht der öffentlichen Zugänglichmachung (Right of Making Available) ist in § 19a UrhG des Entwurfs zur Neuregelung des Urheberrechts in der Informationsgesellschaft der *Bundesregierung* vom 6.11.2002[999] vorgesehen und wird nach der Umsetzung in geltendes Recht bewirken, dass Filesharing ohne Zustimmung des Rechtsinhabers unstreitig rechtswidrig und somit strafbar ist[1000]; das Angebot zum Download von Musikstücken über P2P-Systeme durch den aktiven Teilnehmer wird problemlos vom Recht der öffentlichen Zugänglichmachung erfasst.[1001]

Eine Berufung auf § 52 UrhG wird dem aktiven Teilnehmer in einem Filesharing-Netz ebenso versagt sein wie jedem anderen Online-Anbieter geschützter Werke, sofern der Gesetzesvorschlag realisiert wird:[1002] Der Regierungsentwurf enthält eine Neufassung des § 52 UrhG, nach dessen

---

995 *Kreutzer*, Napster, Gnutella & Co. – Teil 1, **GRUR** 2001, S. 204.
996 *Mönkemöller*, **GRUR** 2000, S. 669.
997 Nachtrag: Die vorliegende Arbeit wurde am 26.05.2003 als Dissertation eingereicht. Dieses Datum markiert folglich den Stand der Bearbeitung. Am 10.09.2003 ist das Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft (**BGBl.** I 2003, S. 1774-1788) in Kraft getreten. Die nachfolgend skizzierten, geplanten Änderungen des Urheberrechtsgesetzes sind seitdem allesamt geltendes Recht. Abgesehen von einer Neufassung des § 53 Abs. 1 UrhG, die auf einer Beschlussempfehlung des Vermittlungsausschusses vom 02.07.2003 (**BT-Drucks.** 15/1353, veröffentlicht auf der Internet-Präsenz des *Deutschen Bundestages* unter http://dip.bundestag.de/btd/15/013/1501353.pdf) beruhte, haben sich keine Abweichungen vom letzten Regierungsentwurf (vgl. Fn. 999) ergeben, die für die Darstellung von Bedeutung sind. In § 53 Abs. 1 S. 1 UrhG n.F. heißt es nunmehr: „Zulässig sind einzelne Vervielfältigungen eines Werkes durch eine natürliche Person zum privaten Gebrauch auf beliebigen Trägern, sofern sie weder unmittelbar noch mittelbar Erwerbszwecken dienen, *soweit nicht zur Vervielfältigung eine offensichtlich rechtswidrig hergestellte Vorlage verwendet wird*". Das Merkmal der „offensichtlich rechtswidrig hergestellten Vorlage" wurde offenbar in das Gesetz aufgenommen, um u.a. die passive Teilnahme an Online-Tauschbörsen und das Herunterladen urheberrechtlich geschützter Werke aus dem Internet von der gesetzlichen Lizenz des § 53 UrhG auszunehmen. Da die Novelle keine weiteren Anhaltspunkte dafür liefert, was unter einer „offensichtlich rechtswidrig hergestellten Vorlage" zu verstehen ist, werden letztlich die Gerichte hierüber entscheiden müssen. Zur „Vorlagenproblematik" siehe auch Teil 3, C. I. 2. d) (1).
998 Zu den Grundlagen der geplanten Urheberrechtsnovellierung siehe oben Teil 2, C. I. 4.
999 **BT-Drucks.** 15/38; auch veröffentlicht beim *Institut für Urheber- und Medienrecht e.V.*, http://www.urheberrecht.org/topic/Info-RiLi/ent/1500038.pdf.
1000 *Scheja*, **c't** 6/2002, S. 172.
1001 *Kreutzer*, Napster, Gnutella & Co. – Teil 1, **GRUR** 2001, S. 199; *Scheja*, **c't** 6/2002, S. 171.
1002 Vgl. *Kreutzer*, Napster, Gnutella & Co. – Teil 1, **GRUR** 2001, S. 202.

Absatz 3 öffentliche bühnenmäßige Darstellungen, öffentliche Zugänglichmachungen und Funksendungen eines Werkes sowie öffentliche Vorführungen eines Filmwerks stets nur mit Einwilligung des Berechtigten zulässig sind. Da das Angebot von Musikdateien innerhalb einer Tauschbörse an einen unbestimmten Kreis von Angehörigen der Öffentlichkeit gerichtet ist, müsste somit die Einwilligung des Rechtsinhabers vorliegen.

Die passive Teilnahme an P2P-Tauschbörsen und das reine Herunterladen von geschützten Werken über die anderen Dienste des Internet werden voraussichtlich auch nach Umsetzung der EU-Richtlinie weiterhin unter die Erlaubnis der Privatkopie gemäß § 53 UrhG fallen.[1003]

Mit der Ergänzung durch den Passus „zum privaten Gebrauch auf beliebigen Trägern" wird in der geplanten Neufassung des § 53 Abs. 1 S. 1 UrhG endgültig klargestellt, dass digitale Vervielfältigungen zum Privatgebrauch erfasst werden.

Der Entwurf eines neuen § 16 UrhG ergänzt die bestehende Vorschrift hinter „gleichviel" um den Zusatz „ob vorübergehend oder dauerhaft" und stellt damit klar, dass auch die ephemere Vervielfältigung unter das Vervielfältigungsrecht des Urhebers fällt.

In diesen Punkten sind somit keine gravierenden Änderungen der Rechtslage zu erwarten. Dennoch ist zu beachten, dass sich einige Tauschsysteme nicht rein passiv nutzen lassen, weshalb ihre Nutzung nach dem Inkrafttreten des 5. Urheberrechtsänderungsgesetzes stets strafrechtlich relevant sein wird.

Einen neuen Straftatbestand für das Urheberrecht sieht der Regierungsentwurf in § 108b vor. Gemäß Absatz 1 der Norm sollen Personen mit einer Freiheitsstrafe bis zu einem Jahr oder mit einer Geldstrafe bestraft werden, wenn sie eine technische Schutzmaßnahme (jegliche Art von technischem Kopier- und Zugangsschutz – vgl. § 95a Abs. 2 des Regierungsentwurfs) umgehen, eine Information für die Rechtewahrnehmung entfernen oder verändern (Informationen, die der Verwaltung von Nutzungsrechten dienen oder Rechtsinhaber bzw. Werke identifizieren[1004] – vgl. § 95c Abs. 1 des Regierungsentwurfs) oder einen Schutzgegenstand einführen, verwerten oder öffentlich wiedergeben, bei dem elektronische Informationen zur Rechtewahrnehmung unbefugt entfernt oder geändert wurden (vgl. § 95c Abs. 3 des Regierungsentwurfs).

Die Strafbarkeit ist jedoch ausgeschlossen, wenn der Täter zum eigenen privaten Gebrauch oder für den privaten Gebrauch persönlich mit ihm verbundener Personen handelt oder sich die Tat auf einen derartigen Gebrauch bezieht. Mit dieser (Ausnahme)Regelung reagiert die *Bundesregierung* mit einem Kompromiss auf die Vorgabe aus Brüssel, wonach die Umgehung von Schutzmechanismen unter Strafe zu stellen ist, es jedoch im Ermessen der Mitgliedstaaten verbleibt, private Kopien weiterhin

---

[1003] Siehe hierzu auch den Nachtrag in Fn. 997.

[1004] Ein Beispiel für solche Informationen ist der sogenannte International Standard Recording Code (ISRC). Dabei handelt es sich um eine zwölfstellige digitale Kennung von Tonaufnahmen, die im Subcode digitaler Aufnahmen unhörbar mitgeführt wird. Durch permanente Wiederholung im Datenstrom kann die Nutzung einer digitalen Aufnahme jederzeit identifiziert werden. Der Code enthält Informationen über das Herkunftsland der Aufnahme, den Erstinhaber der Rechte, das Jahr der Herstellung und einen fünfstelligen Aufnahmeschlüssel, der individuell von den Tonträgerherstellern vergeben werden kann. Der sogenannte Erstinhaberschlüssel muss bei der deutschen Landesgruppe der *IFPI* beantragt werden. Die Vergabe des ISRC und die Codierung auf den Tonträger erfolgt während des Premastering. Ein einmal vergebener ISRC bleibt mit einer Aufnahme über deren gesamten Lebenszyklus verbunden und ändert sich nicht. Wird eine gekennzeichnete Aufnahme beispielsweise illegal gesendet, können Überwachungseinrichtungen, die mit speziellen Decodern ausgestattet sind, den Piraten auf die Schliche kommen und den Rechtsinhabern bzw. den Verwertungsgesellschaften Meldung erstatten – vgl. http://www.ifpi.de/recht/isrc.shtml.

zuzulassen[1005]. Würde man das Umgehen von Kopierschutzsystemen auch für den privaten Nutzer unter Strafe stellen, wäre es ihm nicht mehr erlaubt, Privatkopien von einem großen Teil der aktuellen Musikveröffentlichungen herzustellen, da die Tonträgerhersteller Audio-CDs immer häufiger mit einem Kopierschutz versehen.[1006]

Eindeutig vom neuen § 108b Abs. 1 erfasst werden Ripper von MP3-Gruppen, wenn sie bei der Vorbereitung eines Releases Kopierschutzsysteme von Audio-CDs umgehen (Abs. 1 Nr. 1)[1007] oder Wasserzeichen aus Dateien entfernen (Abs.1 Nr. 2).

Handelt der Täter in den Fällen des § 108b Abs. 1 (Regierungsentwurf) gewerbsmäßig, erhöht sich gemäß Abs. 3 der Strafrahmen auf eine Freiheitsstrafe von bis zu drei Jahren oder eine Geldstrafe.

Im zweiten Absatz des geplanten § 108b ist eine Freiheitsstrafe von einem Jahr oder eine Geldstrafe für den Fall vorgesehen, dass jemand „entgegen § 95a Abs. 3“ des Regierungsentwurfs eine Vorrichtung, ein Erzeugnis oder einen Bestandteil zu gewerblichen Zwecken herstellt, einführt, verbreitet, verkauft oder vermietet. Nach § 95a Abs. 3 sind solche Vorrichtungen, Erzeugnisse und Bestandteile betroffen, die Gegenstand einer Verkaufsförderung, Werbung oder Vermarktung mit dem Ziel der Umgehung wirksamer technischer Maßnahmen sind (§ 95a Abs. 3 Nr. 1) oder abgesehen von der Umgehung wirksamer technischer Maßnahmen nur einen begrenzten wirtschaftlichen Zweck oder Nutzen haben (§ 95a Abs. 3 Nr. 2) oder hauptsächlich entworfen, hergestellt oder angepasst werden, um die Umgehung wirksamer technischer Maßnahmen zu ermöglichen oder zu erleichtern (§ 95a Abs. 2 Nr. 3). Somit wäre nicht nur der technische Vorgang des „Knackens“ von Kopierschutzmechanismen unter Strafe gestellt, sondern auch die Herstellung oder Einfuhr von Werkzeugen, die Kopiersperren aushebeln.[1008] Betroffen wären unter anderem die Hersteller von CD-Emulatoren[1009] und Brennprogrammen, die in erster Linie dazu bestimmt sind, Kopien von geschützten CDs anzufertigen.[1010]

Die EU-Richtlinie und ihre geplante Umsetzung in Form des Regierungsentwurfs stehen in der Kritik von Vertretern aus Wissenschaft und Politik. Insbesondere wird davor gewarnt, mit der

---

1005 Vgl. *Krempl*, Content an der Kette, **c't** 4/2002, S. 32.

1006 Zu beachten ist, dass zivilrechtliche Ansprüche – etwa auf Schadensersatz und Unterlassung – unabhängig von der strafrechtlichen Ausnahmeregelung bestehen und unberührt bleiben, „um einen folgen- oder sanktionslosen Zustand“ zu verhindern – vgl. bereits die Begründung des Regierungsentwurfs vom 16.08.2002 (siehe Fn. 439), S. 68.

1007 Der Begriff der Umgehung ist so bedenklich weit gefasst, dass eine Strafbarkeit möglicherweise auch dann gegeben sein wird, wenn der Kopierschutz ohne Datenveränderung (vgl. § 303a StGB) oder Entschlüsselung von Daten (vgl. §§ 202a StGB, 17 UWG) überwunden wird – z.B. beim Einsatz von speziellen CD-Brennprogrammen oder bei Digital-Analog/Analog-Digital-Wandlungen.

1008 Vgl. *Himmelein/Schmitz*, **c't** 2/2002, S. 83.

1009 Hierbei handelt es sich um Programme, die ein Abbild (Image) einer CD-ROM auf der Festplatte des Nutzers erstellen. Dabei täuschen sie dem Betriebssystem vor, die entsprechende CD befände sich tatsächlich im Laufwerk und simulieren somit den Kopierschutz. Weiterführende Informationen finden sich bei *Himmelein/Vahldiek,* **c't** 17/2002, S. 122 ff.

1010 Nicht unter Strafe gestellt, aber als Ordnungswidrigkeit mit eine Geldbuße bis 50.000 € geahndet, ist die Erbringung von Dienstleistungen, die hauptsächlich erbracht werden, um die Umgehung von Kopierschutzsystemen zu ermöglichen oder zu erleichtern (vgl. §§ 111a Abs. 1 Nr. 1 b) i.V.m. 95a Abs. 3 Nr. 3 des Regierungsentwurfs). Auch das Bewerben von Hilfsprogrammen (Tools) zur Kopierschutzumgehung wird von der Vorschrift des geplanten § 111a UrhG erfasst, so dass der Veröffentlichung von detaillierten Umgehungsanleitungen in Fachzeitschriften ein ordnungsrechtlicher Riegel vorgeschoben wird.

Neuregelung den Status der Privatkopie i.S.v. § 53 Abs. 1 S. 1 UrhG und somit ein verfassungsmäßig abgesichertes Recht zu gefährden:

§ 95b des Entwurfs („Durchsetzung von Schrankenbestimmungen“) verpflichtet Rechtsinhaber von kopiergeschützten Werken, technische Mittel zur Verfügung zu stellen, damit die Werke unentgeltlich von Behinderten, in Bibliotheken und Museen oder für wissenschaftliche Zwecke genutzt werden können. Zum Erlass einer solchen Eingriffsregelung zur Durchsetzung von Schrankenbestimmungen wurden die Mitgliedstaaten durch die Richtlinie verpflichtet, um die Möglichkeit der Erstellung sogenannter Sozialkopien sicherzustellen. Allerdings sind sie nicht zu einem derartigen Eingriff verpflichtet, wenn es um die Möglichkeit der Erstellung von „normalen“ Privatkopien geht[1011]. Hier bleibt es im gesetzgeberischen Ermessen der Mitgliedstaaten, gegen zu weit gehende Kopierschutzmaßnahmen vorzugehen. Bislang ist jedoch im Regierungsentwurf keine Regelung vorgesehen, die für die Begünstigten der Privatkopieschranke deren tatsächliche Nutzung sicherstellt. Bereits in der Begründung des ersten Regierungsentwurfs heißt es hierzu: „Der Entwurf enthält keine Regelung zur Ausfüllung der Kann-Vorschriften der Richtlinie [...] zur Durchsetzung der Privatkopieschranke bei der Anwendung technischer Schutzmaßnahmen. Diese Fragen bedürfen weiterer Prüfung und sollen gesondert mit allen Betroffenen, den Ländern, der Rechtswissenschaft sowie der Rechtspraxis weiter intensiv und ohne Zeitdruck erörtert werden. Sie sollen [...] erst danach abschließend beantwortet und erforderlichenfalls Gegenstand eines weiteren Gesetzentwurfs werden“[1012].

Für die zögerliche Haltung des Ministeriums haben die Kritiker des Entwurfs wenig Verständnis. Gefordert wird eine „Neuordnung des Urheberrechts ohne Tabus“, bei der der Gesetzgeber von dem in Art. 5 GG verankerten Grundrecht auf Informationsfreiheit ausgehen müsse[1013]. Die als Ausnahmen bzw. Schranken im deutschen Urheberrechtsgesetz sowie in der von den Mitgliedstaaten noch umzusetzenden EU-Richtlinie aufgeführten Rechte seien verfassungsmäßig abgesichert. Daher sei es falsch, dass die EU-Urheberrechtrichtlinie die Schranken als fakultativ darstellt. Indem es Kopierschutztechniken über die fundamentalen Rechte der Allgemeinheit zum Informationszugang stelle, verstoße das Gesetzgebungsverfahren „eklatant gegen völkerrechtliche Vorgaben“, denn die der Richtlinie zugrundeliegenden Verträge der *WIPO* von 1996 (WCT und WPPT)[1014] sähen keinen pauschalen rechtlichen Schutz von Kopiersperren vor.[1015] Die Zulässigkeit der Privatkopie sei nicht nur aus Pragmatismus geschaffen worden. Hinter der Überlegung stehe vielmehr das Recht auf Zugang zum verfügbaren Wissen. Ausschließlichkeitsrechte an Informationen, wie sie Verwertungsindustrie und Inhalteanbieter einfordern, bedürften demgegenüber einer gesonderten Rechtfertigung.[1016]

Indem die Musikindustrie einerseits Vergütungspauschalen auf Leermedien für privates Kopieren erhebe und andererseits die Privatkopie zunehmend durch digitales Rechtemanagement (Kopier-

---

1011 Ein Teil der Privatkopien soll jedoch weiterhin ermöglicht werden, vgl. § 95 b Abs. 1 Nr. 6 des Regierungsentwurfs, wonach z.B. sogenannte Papierkopien zum privaten Gebrauch garantiert werden müssen (Nr. 6 a.).
1012 Regierungsentwurf vom 16.08.2002 (siehe Fn. 439), S. 33; im Regierungsentwurf vom 6.11.2002 (siehe Fn. 999) wird auf S. 15 die gleiche Begründung angeführt.
1013 So *Hoeren* in einem Vortrag auf dem Kongress „Digital Rights Management“ am 29.01.2002 in Berlin, vgl. **Heise Online News** vom 29.01.2002, http://www.heise.de/newsticker/meldung/24399.
1014 Siehe oben Teil 2, C. I. 4.
1015 So *Hoeren* auf der Konferenz "Digitales Urheberrecht zwischen Information Sharing und Information Control" am 26.04.2002 in Berlin, vgl. **Heise Online News** vom 26.04.2002, http://www.heise.de/newsticker/meldung/26960.
1016 *Hoeren*, bei *Krempl*, Content an der Kette, **c't** 4/2002, S. 33.

schutzsysteme) verhindere, spiele sie ein doppeltes Spiel. Die Content-Industrie halte längst nicht mehr das Urheberrecht hoch, es gehe ihr vielmehr allein um das "Recht auf Zugang" und die Schaffung und Durchsetzung eines "virtuellen Hausrechts".[1017] Solange die Verbraucher beim Erwerb von Geräten oder Leermedien nach dem nationalen Gesetz Abgaben für Privatkopien entrichteten, seien die Gesetzgeber in den Mitgliedstaaten verpflichtet, die Möglichkeit der Anfertigung dieser Kopien auch zu garantieren. Es könne nicht sein, dass der Verbraucher Abgaben für Kopien bezahle, die er wegen der technischen Schutzmaßnahmen gar nicht anfertigen könne. Darin läge ein grober Verstoß gegen das Gesetz der Fairness und den Verbraucherschutz.[1018]

Es bleibt abzuwarten, in welcher Form die EU-Richtlinie in innerdeutsches Recht umgesetzt wird.[1019] Während zumindest Hoffnung besteht, dass die beschriebenen Kollisionen von Privatkopien und Kopierschutzsystemen in Zukunft vermieden werden[1020], führt die Novelle zu einer „Massenkriminalisierung“ von Tauschbörsennutzern und wird mit einer großen Wahrscheinlichkeit die erhofften generalpräventiven Wirkungen verfehlen. Der Gesetzentwurf verkennt diesbezüglich die Autonomie und Dynamik des Internet. Es ist fraglich, ob sich das geringe oder nicht vorhandene Unrechtsbewusstsein der Nutzer aufgrund der geplanten Gesetzesänderung ändern lässt. Was privates P2P-Filesharing betrifft, hat das *Napster*-Phänomen bei Millionen von Nutzern bereits ein normatives Bewusstsein geschaffen.[1021] Angebracht und überfällig ist vielmehr die Entwicklung von Vergütungsmodellen für die Tauschbörsennutzung, so dass die Rechtsinhaber endlich Kompensation für privaten Online-Tausch erhalten.

II. Betrachtung der Maßnahmen, die offiziell von privater und staatlicher Seite eingesetzt werden bzw. eingesetzt werden sollen

1. Arbeit der Musikindustrie-Verbände

Ähnlich wie in der Softwarebranche gibt es auch in der Musikbranche Industrieverbände und Anwälte, die im Interesse ihrer Mitglieder und Mandanten Maßnahmen gegen Online-Piraterie ergreifen.

a) Maßnahmen der *International Federation of the Phonographic Industry (IFPI)*[1022]

Bei der *IFPI* handelt es sich um den größten internationalen Verband der Tonträgerindustrie. Zu seinen Mitgliedern zählen ca. 1.400 Tonträgerhersteller und -vertriebe aus 76 Ländern. Die Zentrale der *IFPI* befindet sich in London, des Weiteren gibt es 46 angeschlossene Ländergruppen, die eigene Einrichtungen unterhalten. Für Deutschland ist dies der *Bundesverband der phonographischen Industrie*, die

---

1017 So *Hoeren* in einem Vortrag auf dem Kongress „Digital Rights Management“ am 29.01.2002 in Berlin, vgl. **Heise Online News** vom 29.01.2002, http://www.heise.de/newsticker/meldung/24399.
1018 *Wuermeling*, 3. e).
1019 Siehe hierzu die Nachträge in Fn. 948 und 997.
1020 Entsprechende Gestaltungs- bzw. Lösungsvorschläge finden sich bei *Metzger/Kreutzer*, **MMR** 2002, S. 139 ff.
1021 Vgl. *Kuhlen* auf der Konferenz "Digitales Urheberrecht zwischen Information Sharing und Information Control" am 26.04.2002 in Berlin, vgl. **Heise Online News** vom 26.04.2002, http://www.heise.de/newsticker/meldung/26960.
1022 http://www.ifpi.org.

Deutsche Landesgruppe der IFPI und die *Deutsche Phono-Akademie*[1023]. 28 der 46 Ländergruppen beschäftigen eigene Anti-Piraterie-Divisionen, die in den letzten Jahren auch im Kampf gegen die Internet-Musikpiraterie aktiv sind. Neben der Pirateriebekämpfung übernimmt die *IFPI* die Vertretung der Interessen der Musikindustrie in politischen und wirtschaftlichen Belangen.

Zu den wichtigsten Maßnahmen der *IFPI* zur Eindämmung von Online-Musikpiraterie gehört das Entfernen von nichtlizenzierten Musikfiles von öffentlich zugänglichen WWW- und FTP-Seiten. Unverzichtbare Voraussetzung für die schnelle Abwicklung von „Notice and Take Down Procedures" ist eine enge Zusammenarbeit mit den Providern, die die unerwünschten Informationen auf ihren Servern bereithalten. Wenn im Rahmen einer Überprüfung der Informationen auf einer verdächtigen Seite festgestellt wird, dass mit dem Angebot der Dateien Urheber- oder Leistungsschutzrechte verletzt werden, erfolgt zunächst eine Identifikation des Providers, wenn möglich auch des Seitenbetreibers. Daraufhin ergeht eines Abmahnung an den Provider mit der Aufforderung, die Seite zu schließen, bzw. Dateien zu löschen. Außerdem wird er aufgefordert, die Adresse des Seitenbetreibers zu nennen, falls dieser im Vorfeld nicht ermittelt werden konnte.[1024] Den Betreibern droht nach Aussagen einer Verbandssprecherin eine Abmahnung mit Kosten bis zu 1.000 €.[1025]

Abbildung 107 – Nachricht der *IFPI* auf einer geschlossenen MP3-Downloadseite

Die geschilderte Vorgehensweise findet ihre Legitimation in den Verantwortlichkeitsregelungen des TDG. Gemäß § 11 S. 1 Nr. 2 TDG können sich Provider einer straf- und zivilrechtlichen Haftung entziehen, wenn sie unverzüglich tätig geworden sind, um eine Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie Kenntnis von der Rechtswidrigkeit der Information erlangt haben. Die Erfahrung hat gezeigt, dass in den meisten Fällen die rechtswidrigen Informationen binnen 24 Stunden vom Netz genommen sind, weshalb die „Notice and Take Down Procedure" ein wirksames Verfahren zur sofortigen Entfernung verletzender Inhalte darstellt.[1026] Gemäß dem Piracy

---

[1023] http://www.ifpi.de.
[1024] *Bortloff*, **GRUR Int.** 2000, S. 666.
[1025] **Heise Online News** vom 27.10.1999, http://www.heise.de/newsticker/meldung/6689.
[1026] *Bortloff*, **GRUR Int.** 2000, S. 666, der darüber hinaus rät, rechtsgeschäftliche Vereinbarungen mit Providern zu treffen, in denen festgelegt wird, wie mit urheberrechtlich geschützten Files auf den Servern des Providers umgegangen werden soll. Letzterer soll sich zur Kooperation, Aufklärung der Nutzer etc. verpflichten – im Gegenzug solle die *IFPI*

Report der *IFPI* von 2002[1027] gelang es den Anti-Piraterie-Divisionen alleine im Jahr 2001, 28.000 illegale Seiten aus dem Netz zu entfernen, die rund 5,5 Millionen nichtlizenzierte Musikdateien enthielten.

Zum Abschalten von Tauschbörsenservern weist der Report ebenfalls beeindruckende Zahlen aus: In 2001 seien aufgrund Initiative der *IFPI* 997 *OpenNap*-Server in 12 verschiedenen Ländern abgeschaltet worden, die schätzungsweise 1,2 Millionen Nutzer gleichzeitig miteinander verbanden und ein Tauschvolumen von 350 Millionen Musikdateien ermöglichten.

Um die Interessen der Rechtsinhaber zu stärken und abzusichern, bemüht sich die *IFPI* stets, auch Einfluss auf die urheberrechtliche Gesetzgebung zu nehmen. Gerade im Vorfeld der Verabschiedung der EU-Richtlinie zur Harmonisierung des Urheberrechts in der Informationsgesellschaft[1028] waren zahlreiche, weltweit renommierte Künstler für die *IFPI* aktiv. Unter anderem forderten 1.400 Musiker in einer Petition vom 13.07.2000 von den Europaparlamentariern klare und strenge Gesetze für den Gebrauch von urheberrechtlich geschützten Werken und ihren Kopien im Internet.[1029] Diese und andere „Lobby-Aktivitäten ohne Beispiel" haben dazu geführt, dass dem Rechtsausschuss allein 230 Änderungsanträge zum Entwurf der Stellungnahme des Abgeordneten *Enrico Boselli* vorlagen, ein Rekord in dieser Legislaturperiode.[1030] Die enorme Vielzahl der wider-streitenden Interessen ist unter anderem der Grund dafür, dass die Richtlinie wegen ihrer zahlreichen fakultativen Ausgestaltungsvorgaben in der Kritik steht.

Einen außergewöhnlichen Vorstoß wagte die deutsche Landesgruppe der *IFPI* Ende der 90er Jahre mit dem von ihr entwickelten Rights Protection System (RPS), mit dessen Hilfe es möglich sein soll, den Zugriff deutscher Nutzer auf ausländische MP3-Angebote zu unterbinden und somit nationales Recht im Internet durchzusetzen. Das System basiert auf der Idee der Grenzbeschlagnahme, überwacht den Grenz(daten)verkehr und soll den „Import" illegaler Inhalte verhindern.[1031] Hierzu bedient es sich einer schwarzen Liste (Negativliste) von Hyperlinks, die auf illegale Musikdateien verweisen. Diese soll bei Providern unmittelbar vor jenen Routern zum Einsatz kommen, die über eine Verbindung ins Ausland verfügen. Jede Anfrage der Kunden des Providers an den Router-Table wird mit der Liste abgeglichen. Bei einem Treffer wird die Verbindung verweigert, so dass der Nutzer nur noch an die Dateien herankommt, wenn er einen Provider findet, der kein RPS betreibt. Nach den Vorstellungen der *IFPI* sollte die Liste stündlich aktualisiert werden und nach Möglichkeit von offizieller staatlicher Seite, etwa den Zollbehörden, betreut werden.[1032]

---

für die Richtigkeit ihrer Angaben haften und dem ISP jeden direkten wirtschaftlichen Schaden ersetzen, wenn er aufgrund einer fehlerhaften Mitteilung ungerechtfertigterweise eine Musikdatei gelöscht hat (S. 667 f.).

1027 http://www.ifpi.org/site-content/library/piracy2002.pdf.

1028 Richtlinie des Europäischen Parlaments und des Rates zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, Richtlinie 2001/29/EG, **ABl. EG** L 167/11 vom 22.06.2001, S. 10 ff.

1029 *Rötzer*, Europäische Musiker überreichen Petition an das EU-Parlament, **Telepolis** vom 14.07.2000.

1030 *Wuermeling*, 4.

1031 Vgl. *Bortloff*, **GRUR Int.** 2000, S. 669.

1032 *Goltzsch*, **Telepolis** vom 24.02.2000.

In rechtlicher Hinsicht stützte der Verband sein Vorhaben auf § 5 TDG a.F., wonach Diensteanbieter, die fremde Inhalte zur Nutzung bereithalten, nur dann verantwortlich sind, wenn sie von diesen Inhalten Kenntnis haben und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern. Hieraus leiteten die Vertreter der *IFPI* eine Pflicht der deutschen Provider zum Einsatz von RPS her, da die Einrichtung des Systems wirtschaftlich zumutbar sei und eine Nutzungsverhinderung möglich mache. Mit der Neuregelung des TDG wurde dieser Argumentation jedoch der Boden entzogen, denn die neuen Regelungen zur Verantwortlichkeit orientieren sich nicht mehr an den Begriffen „technisch möglich" und „zumutbar". Die veränderte Rechtssystematik des TDG führt zu dem Ergebnis, dass die Diensteanbieter außer im Fall von gerichtlichen und verwaltungsbehördlichen Verfügungen keine Verantwortung für fremde Inhalte tragen. Erst wenn eine Verfügung in Kraft tritt, muss der Anbieter solche Inhalte sperren oder entfernen.[1033] In den meisten Fällen wird also ein Richter die Zumutbarkeit und Verhältnismäßigkeit von Sperrungen feststellen müssen.[1034] Eine Kooperationspflicht von Providern lässt sich somit nicht mehr aus deutschem Recht ableiten, weshalb der Einsatz von RPS nur noch auf freiwilliger Basis stattfinden kann.

Ob dies allerdings geschehen wird, ist zu bezweifeln. Geschmäht als „Zensur-Infrastruktur" sorgte RPS für Empörung und stand in der Kritik zahlreicher Internet-Aktivisten, Politiker und Wissenschaftler: Maßnahmen wie Zensur oder eine generelle Überwachung elektronischer Kommunikation dürften für alle demokratischen Staaten grundsätzlich nicht in Frage kommen. Derartige Systeme könnten auch missbraucht werden, was fatale Folgen für die freie Meinungsäußerung hätte.[1035] Darüber hinaus sei das Vorhaben der *IFPI* bedenklich, da es gegen die Rezipientenfreiheit verstoße.[1036]

Hinzu kommen die üblichen Schwächen von Filtermaßnahmen[1037], so ist auch RPS machtlos gegen das simple Verschieben von Inhalten und immer nur so gut, wie die Liste, mit der es betrieben wird.

Nach wie vor ist es die bessere Lösung, die Zieldateien löschen zu lassen, anstatt zu versuchen, den Zugriff darauf zu kontrollieren.

b) Maßnahmen der *Recording Industry Association of America* (*RIAA*)

Eng mit der *IFPI* zusammen arbeitet die *RIAA*. Die *RIAA* ist der bedeutendste Verband für die US-amerikanische Musikindustrie und somit verantwortlich für den größten Tonträgermarkt der Welt. Die Organisation repräsentiert 250 Mitgliedsunternehmen, zu denen auch die fünf Major Com-

---

1033 *Sieber*, bei *Schulzki-Haddouti*, Trümpfe für den E-Commerce, **c't** 11/2000, S. 46; nach Aussagen eines Insiders hatten Vertreter der *IFPI* in Brüssel bis zuletzt darauf gedrängt, den Passus „technisch möglich" und „zumutbar" auch in die EU-Regelung zu übernehmen, vgl. *Schulzki-Haddouti,* Trümpfe für den E-Commerce, **c't** 11/2000, S. 46.
1034 *Schulzki-Haddouti*, Trümpfe für den E-Commerce, **c't** 11/2000, S. 46.
1035 *Tauss*, medienpolitischer Sprecher der *SPD*, bei *Schulzki-Haddouti*, Kein MP3 für deutsche Surfer?, **SPIEGEL Online** vom 24.02.2000.
1036 Vgl. *Wenning*, *Förderverein Informationstechnik und Gesellschaft (FITUG)*, bei *Schulzki-Haddouti*, Kein MP3 für deutsche Surfer?, **SPIEGEL Online** vom 24.02.2000.
1037 Siehe oben Teil 2, C. III. 8. a) (2) (b).

panies[1038] *BMG, EMI, SONY Music, Vivendi Universal* und *AOL Time Warner* gehören. Die Mitglieder der *RIAA* produzieren rund 90% aller Musikaufnahmen, die in den USA veröffentlicht werden.

Im Bezug auf Online-Musikpiraterie ist die *RIAA* der aktivste Verband, was juristische Maßnahmen gegen Urheberrechtsverstöße anbelangt. Keine zweite Organisation leitete bislang so viele Rechtsstreitigkeiten gegen Unternehmen und Betreiber von Internet-Diensten ein wie die *RIAA*.

Einen der ersten Prozesse im Zusammenhang mit Online-Piraterie – allerdings im weiteren Sinne – führte die *RIAA* 1998 zusammen mit der *IFPI*, der britischen *Mechanical Copyright Protection Society (MCPS)* und der *British Phonographic Industry (BPI)* gegen das Unternehmen *Diamond Multimedia*[1039], Hersteller eines portablen MP3-Players namens *RIO PMP 300*. Die *RIAA* wollte die Auslieferung der Geräte per Gerichtsurteil stoppen, da sie der Ansicht war, dass Hersteller solcher Player die illegale Weitergabe von Musikstücken per Internet unterstützen und somit die Künstler bzw. Verwertungsberechtigten um ihre Tantiemen bringen. Man müsse davon ausgehen, dass die Mehrheit der Player-Benutzer illegale Webseiten aufsuchen würde, um den Speicher mit Musikdateien zu bestücken.[1040] Nach *RIAA*-Argumentation verstoße der Player außerdem gegen den US-amerikanischen Audio Home Recording Act (AHRA) von 1992, der vorsieht, dass Hersteller oder Importeure von „digitalen Rekordern" eine Verwertungsgebühr an die Musikindustrie abführen müssen.[1041]

Für zehn Tage erwirkte die *RIAA* einen Auslieferungsstopp per einstweiliger Verfügung für den US-amerikanischen Markt. Am 26.10.1998 entschied das zuständige Gericht jedoch gegen die Aufrechterhaltung der einstweiligen Verfügung, woraufhin die *RIAA* sogar 500.000 US-Dollar Entschädigung an *Diamond Multimedia* zahlen musste. In der Urteilsbegründung heißt es, dass das Gerät nicht in der Lage sei, serielle Kopien zu fertigen. Er falle daher nicht unter die Regelungen des AHRA, und *Diamond Multimedia* müsse somit auch keine Abgaben leisten.[1042] In Deutschland gab es diese Probleme nicht, da das Gerät bereits frühzeitig der *GEMA* vorgestellt und als Tonaufzeichnungsgerät i.S.v. § 54 UrhG lizenziert wurde.[1043] Der Hersteller zahlt eine Geräteabgabe i.H.v. 2,50 € und darf das Gerät ohne weitere Einschränkungen verkaufen.[1044]

Mit dem sogenannten *Napster*-Prozess erregte die *RIAA* weltweite Aufmerksamkeit. Gemeinsam mit einzelnen Plattenfirmen ging sie im Dezember 1999 juristisch gegen die Betreiber der Musiktauschbörse *Napster* vor, um das Tauschen nichtlizenzierter Musikstücke über den Dienst zu unterbinden. In einer ersten einstweiligen Verfügung des zuständigen kalifornischen Bezirksgerichts wurde *Napster* zunächst verpflichtet, sein Angebot vollständig vom Netz zu nehmen. Die Überprüfung dieser Entscheidung führte Anfang 2001 zu einer zweiten einstweiligen Verfügung, wonach die Tauschbörse zwar am Netz bleiben durfte, allerdings dafür Sorge zu tragen hatte, dass keine urheber-

---

[1038] Unter dem Begriff der Major Companies versteht man solche Unternehmen, die über eigene weltweite Vertriebsstrukturen für Tonträger verfügen. Tonträgerunternehmen ohne diese Strukturen bezeichnet man als Independent-Companies oder Independent-Labels.
[1039] Mittlerweile *SONICblue Inc.*
[1040] Vgl. **c't** 22/1998, S. 18.
[1041] Vgl. *Krempl*, Kampf um die Ohrmuscheln, **Telepolis** vom 17.12.1998.
[1042] Vgl. *Krempl*, Kampf um die Ohrmuscheln, **Telepolis** vom 17.12.1998.
[1043] *Wiedenhoff*, **c't** 23/1998, S. 20.
[1044] Vgl. *Krempl*, Kampf um die Ohrmuscheln, **Telepolis** vom 17.12.1998.

rechtlich geschützten Dateien ohne Zustimmung der Rechtsinhaber getauscht werden können. *Napster* könne für Verstöße gegen das Urheberrecht nur in dem Maße verantwortlich gemacht werden, wie seine Betreiber von den illegalen Kopien Kenntnis erhielten. Somit dürfe man den Dienst nicht einfach komplett schließen, da über die *Napster*- auch legale Kopien ausgetauscht werden könnten.[1045] Um den Tausch nichtlizenzierter Dateien zu unterbinden, entschied man sich für die Installation eines textsensitiven Filtersystems, das nur noch solche Suchanfragen beantwortete, die keine Interpreten- bzw. Songnamen beinhalteten, welche sich auf einer schwarzen Liste der *RIAA*-Mitglieder befanden.

Das Hauptsacheverfahren im *Napster*-Prozess ist noch nicht beendet, allerdings hat sein Ausgang durch das freiwillige Abschalten der *Napster*-Server an Bedeutung verloren.[1046]

Ebenfalls in der Schwebe befindet sich ein Prozess der *RIAA* gegen die auf *FastTrack*-Technologie basierenden Internet-Tauschbörsen KaZaA, *StreamCast* (*Morpheus*)[1047] und *Grokster*. Im Oktober 2001 haben die *RIAA* und die *Motion Picture Association of America (MPAA)* Klage gegen die „Betreiber" dieser P2P-Systeme eingereicht. In einer Vorverhandlung am 04.03.2002 kündigte der vorsitzende Richter an, dass zunächst geprüft werden müsse, ob die Tauschbörsenbetreiber unerlaubter Verwertung von Filmen und Musik Vorschub leisten, bevor man auf weitere Argumente der Parteien eingehen könne.[1048] Die Prozessvertreter der Tauschbörsensoftwarehersteller gehen davon aus, dass die umstrittenen Dienste in die gleiche Kategorie fallen wie Videorekorder und verweisen – wie auch die Beklagtenseite im *Napster*-Prozess – auf das sogenannte *Betamax*-Urteil des *US Supreme Court* aus dem Jahr 1984, in dem festgestellt wurde, dass die Hersteller von Videorekordern nicht für Verstöße gegen das Urheberrecht verantwortlich seien, die von den Endkunden verübt werden. Die Anwälte der Gegenseite verweisen darauf, dass sich das *FastTrack*-Netz nicht so einfach kontrollieren ließe wie *Napster*. Da es keinen zentralen Index-Server gäbe, habe der Betreiber keine Möglichkeit, gegen Urheberrechtsverstöße vorzugehen.[1049]

Außerhalb der USA fand bereits in den Niederlanden ein Verfahren gegen die Betreiber von *KaZaA* statt[1050]. In der Berufungsinstanz wurde Ende März 2002 ein Urteil vom November 2001 aufgehoben, wonach *KaZaA* den Download seiner Software zu sperren hatte, solange die Kunden sie zum Tausch urheberrechtlich geschützter Inhalte nutzten. Das Amsterdamer Berufungsgericht gestattete es den Betreibern, den Vertrieb von den Niederlanden aus wieder aufnehmen. *KaZaA* sei für das Kundenverhalten nicht verantwortlich und könnte die Software demnach weiter vertreiben.[1051] Somit folgt es der bereits dargestellten Argumentation aus dem *Betamax*-Urteil des *US Supreme Court*, auf die der niederländische Anwalt *KaZaAs* seine Berufung stützte.

[1045] **Heise Online News** vom 12.02.2001, http://www.heise.de/newsticker/meldung/15223.
[1046] Siehe oben Teil 3, A. VII. 1.
[1047] *Morpheus* basiert mittlerweile nicht mehr auf *FastTrack*-Technologie, sondern nutzt ein *Gnutella*-kompatibles Protokoll.
[1048] **Heise Online News** vom 05.03.2002, http://www.heise.de/newsticker/meldung/25363.
[1049] **Heise Online News** vom 05.03.2002, http://www.heise.de/newsticker/meldung/25363.
[1050] Vor dem Verkauf an das australische Unternehmen *Sharman Networks* gehörte *KaZaA* der niederländischen Betreibergesellschaft *KaZaA BV*.
[1051] **Heise Online News** vom 28.03.2002, http://www.heise.de/newsticker/meldung/26120.

Neben der Vertretung ihrer Mitglieder vor Gericht bei der Ergreifung juristischer Maßnahmen engagiert sich die *RIAA* auch in Sachen Aufklärung: Mit der groß angelegten „Soundbyting"-Kampagne[1052] möchte die *RIAA* bei Schülern, Studenten und Administratoren von Universitätsnetzwerken ein Bewusstsein für den legalen Umgang mit urheber-rechtlich geschützten Musikwerken schaffen. Auf einer eigens zu diesem Zweck errichteten Webseite finden sich unter anderem juristische Informationen und Stimmen von bekannten Musikern zum Thema Online-Musikpiraterie.

Wie die *IFPI* geht auch die *RIAA* gegen Betreiber von Webseiten vor, die nichtlizenzierte Werke zum Download anbieten. Hierbei nimmt sie unter anderem Privatpersonen ins Visier, die MP3-Dateien online stellen. Können diese nicht direkt ermittelt werden, wird das Problem über den Provider angegangen. Wurde eine verdächtige Seite aufgespürt – was auch durch den Einsatz von speziellen Suchmaschinen geschehen kann – versendet die *RIAA* Abmahnungen (Cease and Desist Letters) an die Webseitenbetreiber, als deren Folge die meisten Seiten sofort geschlossen werden.[1053]

Wie die meisten Verbände versucht die *RIAA*, Einfluss auf die Gesetzgebung zu nehmen. Für besondere Empörung hat das Engagement der *RIAA* im Vorfeld eines US-amerikanischen Gesetzentwurfs[1054] gesorgt, der es den Rechtsinhabern geschützter Werke unter anderem erlauben soll, in die Verzeichnisse der Rechner von Tauschbörsennutzern einzudringen, die Audio- und Videodaten enthalten. Des Weiteren soll ihnen gestattet sein, (Hacking-)Attacken gegen diese Rechner auszuführen, um sie vom Netz zu trennen. Der vom demokratischen Abgeordneten *Howard Berman* in das US-Repräsentantenhaus eingebrachte Gesetzentwurf sieht vor, dass ein geplanter Eingriff seitens der Rechtsinhaber eine Woche vor seiner Ausführung beim Staatsanwalt mit Nennung der technischen Mittel, die benutzt werden sollen, angegeben werden muss. Für die Angegriffenen ist vorgesehen, dass sie auf Anfrage den Grund des Angriffs erfahren müssen. Sie sollen allerdings bei einem ungerechtfertigten Angriff eine Schadensersatzforderung nur dann stellen können, wenn der Schaden mehr als 250 US-Dollar beträgt.[1055] Angesichts der massiven Kritik an diesem Gesetzentwurf steht zu bezweifeln, ob das Vorhaben jemals umgesetzt wird.

Dass die Maßnahmen der *RIAA* in der MP3-Szene nicht besonders populär sind, ist nachvollziehbar. Daher wird die Organisation zuweilen Opfer von humoristischen Attacken oder Angriffen auf die eigene Webseite. So drangen im August 2002 unbekannte Täter in den Webserver der *RIAA* ein und verfälschten die Hypertexte des Verbandes dergestalt, dass man von der offiziellen Homepage der *RIAA* unlizenzierte MP3-Dateien herunterladen konnte und veränderte Textbotschaften zu lesen bekam.[1056]

1052 http://www.soundbyting.com.
1053 Vgl. **c't** 22/1998, S. 18.
1054 http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR05211:@@@L&summ2=m& (Zusammenfassung).
1055 **Heise Online News** vom 26.07.2002, http://www.heise.de/newsticker/meldung/29456.
1056 **Wired News** vom 28.08.2002, http://www.wired.com/news/politics/0,1283,54812,00.html.

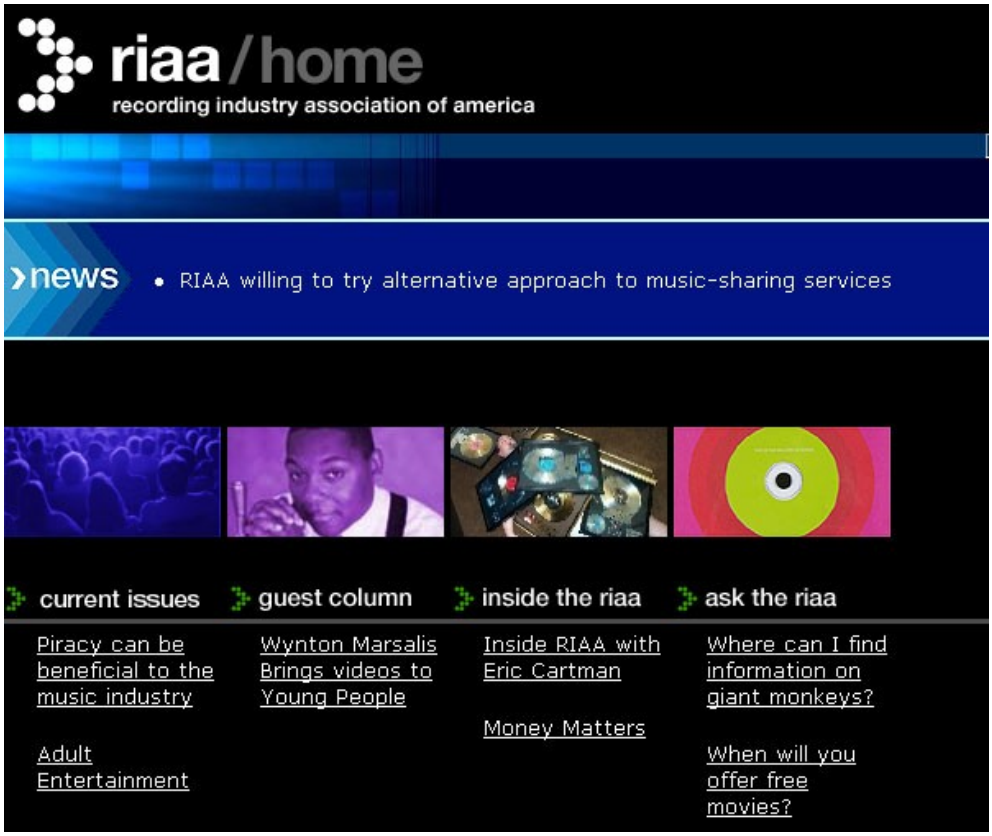


Abbildung 108 – Verfälschte Webseite der *RIAA*

Abbildung 109 – Szene-Grafik (erfundene *RIAA*-Werbeanzeige)

c) Maßnahmen anderer Verbände und von sogenannten Solution Providern

Neben *IFPI* und *RIAA* fahndet auch die deutsche *GEMA* nach illegalen Musikangeboten im Internet. Von Januar bis Oktober 2001 seien rund 2.000 Verstöße gegen das Urheberrecht festgestellt worden, woraufhin die Betreiber der entsprechenden Seiten aufgefordert wurden, die Titel sofort von ihrer Homepage zu entfernen.[1057]

Da über Online-Tauschbörsen nicht nur geschützte Musikwerke sondern auch die neuesten Hollywood-Blockbuster und DVD-Kopien getauscht werden, fürchtet die Filmindustrie eine Beeinträchtigung ihres Geschäfts. Um das Problem in den Griff zu bekommen, ging der US-amerikanische Verband *MPAA* erstmals gegen die Tauschbörsennutzer selbst vor. Mitarbeiter der Industrievertretung klinkten sich in Tauschbörsen ein und notierten IP-Adressen, Datum, Uhrzeit sowie die Namen der angebotenen Dateien. Mit den ermittelten Daten trat die *MPAA* an Provider heran, denen die entsprechenden IP-Adressen zuzuordnen waren, und bat sie um Unterstützung im Kampf gegen Urheberrechtsverstöße.[1058] Allein in 2001 hat die *MPAA* als Interessenvertretung der Filmindustrie weltweit ca. 54.000 Schreiben an 1.680 Internet-Provider versandt; inzwischen sind es über 100.000. Darin werden die Provider gebeten, einzelne User aufzufordern, urheberrechtlich geschützte Inhalte aus dem Netz zu nehmen.[1059] Auch der deutsche ISP *T-Online* wandte sich Mitte Januar 2001 mit einem Brief an einzelne (*T-DSL*-)Kunden: Sie hätten geschützte Inhalte angeboten und sollten dafür Sorge tragen, dass dies nicht wieder vorkomme. Nach Aussage eines Vertreters der *GVU*, einem deutschen Partnerverband der *MPAA*, werde der Einzelanbieter in Filesharing-Netzen zwar noch nicht strafrechtlich verfolgt, aber es müsse überlegt werden, ob nicht ein Exempel an einem „notorischen Vieltauscher" statuiert werden solle.[1060]

Datenschutzexperten halten das Vorgehen der *MPAA* und der Provider für bedenklich. Sie bezweifeln, ob die Provider überhaupt die IP-Adressen speichern dürfen, die sie ihren Nutzern beim Einwählen ins Internet zuweisen.[1061] Nach den Vorgaben des TDDSG darf ein Diensteanbieter personenbezogene Daten eines Nutzers - zu denen auch die zugeordnete IP-Adresse gehört – ausnahmsweise und nur in dem Umfang speichern, soweit es erforderlich ist, um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen. Ob einzelne IP-Adressen zur Abrechnung einer DSL-Flatrate tatsächlich gebraucht würden, sei unklar, wie *Ralf Menger* vom *Regierungspräsidium Darmstadt*, das den Datenschutz bei *T-Online* überwacht, in einer Stellungnahme zu den Abmahnungen ausführte.[1062]

Werden die Strafverfolgungsbehörden eingeschaltet, kommt eine weitere juristische Unklarheit hinzu: Gemäß § 5 S. 2 TDDSG dürfen Provider Auskünfte an Strafverfolgungsbehörden und Gerichte nur für Zwecke der Strafverfolgung erteilen. Wie bereits dargelegt, sind reine Downloader nur zivilrechtlich verantwortlich, und die Anbieter von Dateien über Tauschbörsen begehen derzeit

---

1057 *Dambeck*, Teurer Spaß – Homepage und Urheberrecht, **c't** 25/2001, S. 238.
1058 *Dambeck*, Tausch-Angst – Filmbranche nimmt File-Sharing-Nutzer ins Visier, **c't** 4/2002, S. 42.
1059 **Heise Online News** von 23.07.2002, http://www.heise.de/newsticker/meldung/29308; ein entsprechender Brief der *MPAA* an die *Universität Münster* ist abgedruckt in den **Heise Online News** vom 06.02.2002, http://www.heise.de/newsticker/meldung/24628.
1060 *Dambeck*, Tausch-Angst – Filmbranche nimmt File-Sharing-Nutzer ins Visier, **c't** 4/2002, S. 42.
1061 **Heise Online News** vom 07.02.2002, http://www.heise.de/newsticker/meldung/24689.
1062 **Heise Online News** vom 07.02.2002, http://www.heise.de/newsticker/meldung/24689.

nur nach Auffassung der h.M. strafrechtlich relevante Verwertungshandlungen gemäß § 106 UrhG[1063], so dass nicht bezüglich aller Tauschbörsennutzer Auskünfte eingeholt werden dürfen. Um endgültige Rechtsklarheit zu erlangen, ist die Umsetzung der Urheberrechtsnovelle abzuwarten.[1064]

Das Vorgehen der *MPAA* ist jedoch nicht nur aus datenschutzrechtlichen Gesichtspunkten bedenklich. Indem die Industrie ihre Maßnahmen gegen die eigene Klientel (Film- bzw. Musikinteressierte) richtet, hat sie negative Konsequenzen für ihr Image zu befürchten.

Lösungen für das „Tauschbörsenproblem" versprechen seit Anfang des Jahres 2002 einige privatwirtschaftliche Dienste, die im Auftrag der Musik- bzw. Filmindustrie tätig werden. Selbsternannte „Solution Provider" wie *Vidius*[1065], *MediaDefender*[1066] oder *Overpeer Inc.*[1067] wollen die Attraktivität von P2P-Netzwerken vermindern, indem sie diese mit sogenannten Fake-Files fluten. Dabei handelt es sich um manipulierte Dateien, die aufgrund ihres Namens und ihrer Dateigröße den Anschein erwecken, es handle sich um die begehrten MP3-Files.[1068] Der tatsächliche Inhalt der Dateien variiert jedoch von verstümmelten Versionen der versprochenen Lieder bis zu erzieherischen Wortbotschaften. So berichteten User von einem vermeintlichen MP3 der Gruppe *No Doubt*, nach dessen Starten nur eine Männerstimme zu hören gewesen sei, die minutenlang monoton des Satz "You shouldn't do this" wiederholte.[1069] Auch Fake-Titel des *Eminem*-Albums *„The Eminem Show"* waren schon Wochen vor der offiziellen Veröffentlichung in den Tauschnetzwerken zu finden. Offenbar handelte es sich um speziell für diesen Zweck angefertigte Versionen.[1070]

Wer genau für diese Aktionen verantwortlich zeichnet, ist bislang unklar.[1071] Bestätigt ist jedoch, dass die Gründer von *Overpeer Inc.* Ende Juni 2002 in den USA ein Patent für eine "Methode zur Verhinderung sinkender Plattenverkäufe durch die illegale Verbreitung von Musikdateien in Kommunikationsnetzwerken" angemeldet haben. Darin wird beschrieben, wie man gezielt MP3s manipulieren und dann in Tauschnetzwerke einspeisen kann. Als mögliche Veränderungen werden das Einfügen einer Stimme, das Herabsetzen der Samplequalität oder auch gezielter Einsatz von Verzerrungseffekten genannt. Durch solche Manipulationen werde "bei den Nutzern ein Misstrauen gegenüber der Sound-Qualität und Verlässlichkeit illegaler Musikdateien" erzeugt, was letztlich die Plattenverkäufe steigere.[1072]

Dies gilt es zu bezweifeln, denn die „Fake-Problematik" wohnt den P2P-Netzen schon seit Anbeginn inne und hat nicht zu einer mangelnden Attraktivität derselben geführt. Es gibt viele User, die aus Schadenfreude oder Geltungsdrang falsche Dateinamen vergeben. Eines der ersten bekannteren Fake-Files war eine Datei, die den Namen des ersten *Harry Potter*-Films trug, hinter der sich jedoch ein pornographischer Film verbarg.

1063 Siehe Fn. 977.
1064 Siehe hierzu die Nachträge in Fn. 948 und Fn. 997.
1065 http://www.vidius.com.
1066 http://www.mediadefender.com.
1067 http://www.overpeer.com.
1068 **Heise Online News** vom 26.04.2002, http://www.heise.de/newsticker/meldung/26942.
1069 *Röttgers*, Die Fake-Fluter, **Telepolis** vom 12.07.2002.
1070 *Röttgers*, Die Fake-Fluter, **Telepolis** vom 12.07.2002.
1071 Befragt zum Thema Fake-Files äußerte sich *RIAA*-Präsident *Sherman* folgendermaßen: „Die Studios wären verrückt, wenn sie nicht zu diesen Maßnahmen greifen würden", **FOCUS** 26/2002, S. 132.
1072 *Röttgers*, Die Fake-Fluter, **Telepolis** vom 12.07.2002.

Um sich vor vergeblichen Downloads zu schützen, haben die Nutzer Methoden entwickelt, sich gegenseitig zu warnen. So ist es üblich, dass entsprechende Textdateien erstellt werden, die mit den gleichen Worten wie das Fake-File beginnen, damit sie bei einer alphabetischen Sortierung der Trefferliste einer P2P-Software in unmittelbarer Nähe der Files erscheinen. Andere Nutzer kennzeichnen das betreffende File direkt, indem sie es umbenennen und den Zusatz „Fake!“ oder „Attention Fake!“ einfügen. Schließlich gibt es zunehmend Webseiten, die nur eingerichtet werden, um Listen mit „faulen“ Dateien oder Listen mit korrekt benannten Dateien veröffentlichen.

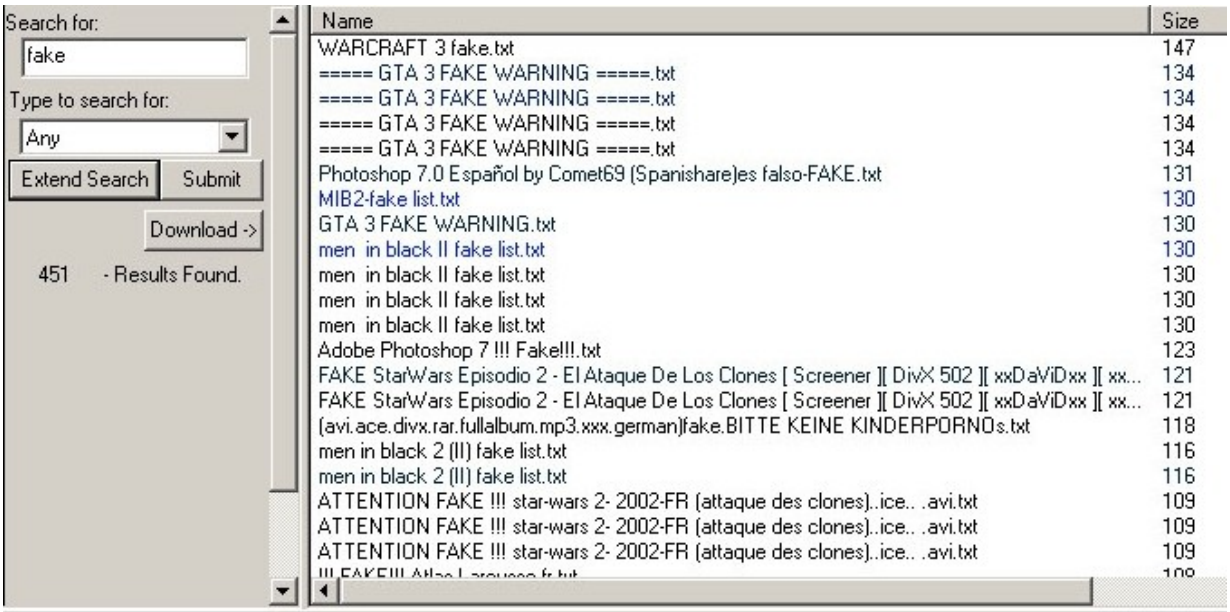


Abbildung 110 – Fake-Warnungen *in eDonkey2000*

Bei MP3s sind Fake-Files noch weniger sinnvoll als bei Filmen, denn das Herunterladen geht so schnell vonstatten, dass es den User nicht davon abhält, sich mehrere Versionen der Stücke herunterzuladen.

Es ist davon auszugehen, dass die beschriebene „Guerilla-Taktik“ der Musikindustrie bzw. der in ihrem Auftrag tätig werdenden Unternehmen bei einem Großteil der Tauschbörsennutzer eine „Jetzt-Erst-Recht-Haltung“ provozieren wird. Denn diese fühlen sich zu großen Teilen von der Musikindustrie bevormundet, was CD-Preise und Auswahl des Repertoires anbelangt. Des Weiteren provozieren derartige Maßnahmen im P2P-Lager auch Reaktionen auf technologischer Ebene. Angekündigt ist bereits die flächendeckende Einrichtung von Online-Datenbanken, in denen sich jedermann detailliert über Dateien informieren kann, die in Tauschnetzwerken kursieren. Hierzu bekommt jede Datei eine eindeutige und unverwechselbare Kennung (einen sogenannten Hashwert) zugeteilt, sofern dies nicht bereits durch das jeweilige P2P-System geschehen ist. Anhand dieses Wertes lässt sich unabhängig vom Dateinamen ermitteln, ob es sich tatsächlich um die begehrte Datei handelt, oder ob es ein Fake-File ist. Geplant ist sogar, die Datenbankfunktion in die P2P-Clients zu integrieren, was den Abgleich wesentlich komfortabler macht.[1073]

[1073] Vgl. *Zota*, Tauschangriff, **c't** 16/2002, S. 68.

Ob sich die Tauschbörsennutzer jemals von Fake-Files entmutigen lassen und kampflos das Feld räumen werden, ist zu bezweifeln. Auf die Entwicklung neuartiger Tauschbörsen, bei denen die IP-Adressen der Nutzer gänzlich verschleiert werden, wurde bereits hingewiesen. Die Lösung des Problems ist eher darin zu suchen, Vergütungsmodelle zu schaffen, die zu einer Kompensation für die bislang freie Online-Verwertung von Musikwerken führen.

2. Maßnahmen von Tonträgerherstellern

a) Kopierschutzmaßnahmen bei Audio-CDs[1074]

Mit der zunehmenden Verwendung von Kopierschutzsystemen auf Audio-CDs werden gleich zwei Ziele verfolgt. Zum einen sollen die Systeme die „Schwarzbrennerei" erschweren, zum anderen wurden sie eingeführt, um das Ripping von CD-Titeln – als Vorstufe von Online-Musikpiraterie – zu verhindern. Um dies zu erreichen, sind die CDs dergestalt verändert, dass sie sich im Idealfall auf allen gebräuchlichen CD-Playern abspielen lassen, nur nicht auf CD-ROM-, CD-R(W), DVD-ROM und DVD-R-Laufwerken von Personal-Computern (kurz: PC-Laufwerke). Formal gesehen sind CDs mit Kopierschutz keine CDs, die dem Red-Book, also dem Standard für Compact Disc Digital Audio (CDDA) entsprechen. Der Standard wurde von *Philips* und *SONY* eingeführt und sollte die Kompatibilität zu bestimmten Abspielgeräten sicherstellen.[1075] Durch die Einführung manipulierter Audio-CDs sorgt sich *Philips* nicht nur um den eigenen Ruf, sondern sieht auch Eigentumsrechte verletzt.[1076]

Deutschland hat den Tonträgermarkt, auf dem bislang prozentual die meisten Audio-CDs mit Kopierschutz veröffentlicht wurden. Je nach Tonträgerhersteller kommen verschiedene Kopierschutzverfahren zum Einsatz, von denen die wichtigsten drei nachfolgend kurz beschrieben werden:

(1) *Key2Audio*

Das von der *SONY DADC AG*[1077] entwickelte System *Key2Audio* gehört zu den am häufigsten verwendeten Kopierschutzverfahren. Bis März 2002 fertigte *SONY* in seinem Salzburger Presswerk nach eigenen Angaben mehr als 11 Millionen *Key2Audio*-geschützte CDs für verschiedene Kunden.[1078]

Das Verfahren nutzt einen Unterschied im Leseverhalten von reinen Audio-CD-Playern und PC-Laufwerken aus. Letztere haben die Angewohnheit, die auf einer CD befindliche Table Of Contents (TOC) – eine Art Inhaltsverzeichnis, in dem unter anderem die Anzahl der Lieder sowie Start- und Endzeiten derselben vermerkt sind – auszulesen, bevor sie mit dem Lesen des eigentlichen Inhalts der CD beginnen. Der Aufbau des TOC hat einer bestimmten Spezifikation[1079] zu folgen, und wenn diese nicht eingehalten wird, kommt es in der Regel zu Irritationen bei Laufwerk und Betriebssystem,

---

1074 Auf die Kopierschutzverfahren der DVD-Audio und Super Audio CD (SACD) wird an dieser Stelle nicht eingegangen. Diese recht jungen Formate sollen die Audio-CD ablösen, sind jedoch derzeit so wenig verbreitet, dass sie als Vorlage zur Erstellung von MP3-Dateien (noch) nicht von Bedeutung sind.
1075 Vgl. das Interview mit *Petri* in **PC Pr@xis** 3/2002, S. 22.
1076 **Heise Online News** vom 04.03.2002, http://www.heise.de/newsticker/meldung/25312.
1077 http://www.sonydadc.com.
1078 **Heise Online News** vom 25.03.2002, http://www.heise.de/newsticker/meldung/26024.
1079 Dem sogenannten Red-Book-Standard, siehe oben Teil 3, A. IV. 2.

die ein korrektes Auslesen unmöglich machen. Aus diesem Grund befinden sich auf *Key2Audio*-geschützten CDs „illegale TOC-Einträge". Reine Audio-CD-Player lassen sich davon in der Regel nicht beeindrucken; entweder lesen sie die TOC nicht aus, oder eine fehlerhafte TOC kann das ordentliche Abspielen der CD-Titel nicht verhindern.

Darüber hinaus handelt es sich bei *Key2Audio*-geschützten CDs um sogenannte Multisession-CDs, was ebenfalls nicht der Spezifikation für Audio-CDs entspricht. Multisession-CDs enthalten mehrere, voneinander unabhängige Teilbereiche (Sessions), die unterschiedlichen Spezifikationen unterliegen können. Typische Multisession-CDs besitzen einen Daten- und einen Audioteil und können sowohl von PC-Laufwerken als auch von Audio-CD-Playern gelesen werden. Allerdings können letztere nur den Audioteil lesen, da es sich typischerweise um Singlesession-Geräte handelt. PC-Laufwerke können hingegen als Multisession-Geräte sämtliche Teile der CD lesen. Sind die Sessions jedoch fehlerhaft miteinander verknüpft, was Vermutungen von Experten zufolge bei *Key2Audio* der Fall sein soll, führt dies zu Fehlfunktionen bei PC-Laufwerken und kann sogar Programmabstürze herbeiführen.

Um zu verhindern, dass Kopien über die Digitalschnittstellen von Audio-CD-Playern und Soundkarten erstellt werden, hat *SONY DADC* bei den CDs das sogenannte Copy-Bit gesetzt. Das zugrundeliegende Verfahren nennt sich Serial Copy Management System (SCMS) und wurde Anfang der 90er Jahre im Consumer-Bereich für digitale Aufnahmegeräte – zum Beispiel für DAT-Rekorder[1080] – eingeführt. Im Datenstrom zwischen SCMS-kompatiblen Geräten werden zwei Zusatz-Bits (Protection-Bit und Generation-Bit) transportiert, die in einem wiederkehrenden Rhythmus signalisieren, ob und wenn ja, wie oft die Informationen kopiert werden dürfen. Mit einem Protection-Bit des Wertes 1 und einem Generation-Bit des Wertes 0 signalisiert das wiedergebende Gerät, dass Kopien generell untersagt sind, jedoch eine einmalige Ausnahme zugelassen wird. Nach der Überspielung setzt das Aufnahmegerät das Generation-Bit der Aufnahme auf 1, wodurch für die Zukunft signalisiert wird, dass bereits eine Kopie vorliegt, deren erneute Vervielfältigung nicht gestattet ist. Indem nun bei *Key2Audio* das Generation-Bit von vornherein gesetzt ist, erkennen andere Geräte mit Digitalschnittstelle die CD als Kopie und verweigern eine vermeintliche Kopie zweiter Generation.

Im Unterschied zu anderen Verfahren werden bei *Key2Audio* die Audiodaten nicht verändert, weshalb die Wiedergabequalität erhalten bleibt.[1081] *Key2Audio* wurde bisher von *SONY Music* und *Zomba Records* eingesetzt.

(2) *SafeAudio*

SafeAudio von *Macrovision*[1082] verfolgt einen anderen Ansatz. Es macht sich einen Unterschied von Audio-CD-Player und PC-Laufwerk zunutze, der ursprünglich dazu gedacht war, die Lauffähigkeit von CDs trotz kleinerer Beschädigungen der Oberfläche zu erhalten: Die Fehlerkorrektur von Audio-CD-Spielern vergleicht die Bereiche vor und nach einem unlesbaren Stück der CD-Spur miteinander und schließt die Lücke mit einem interpolierten Wert oder blendet den fehlerhaften

---

[1080] DAT steht für Digital Audio Tape. Das Format konnte sich im Consumer-Bereich nicht durchsetzen und ist mittlerweile nur noch in der professionellen Tontechnik von Bedeutung.
[1081] *Harbonn*, **ZDNet.de**.
[1082] http://www.macrovision.com.

Bereich sanft aus (Muting); kleinere Kratzer können auf diese Weise kaum hörbar „ausgebügelt" werden. Während das menschliche Ohr diese Korrekturvorgänge kaum wahrnimmt, eignen sich die Interpolations- bzw. Mutingmethoden in der Regel nicht zum Überführen in ein anderes digitales Format. Werden also, wie bei *SafeAudio* der Fall, absichtlich zahlreiche Fehler in den CD-Informationen untergebracht, schafft es das PC-Laufwerk in Verbindung mit der Ripping-Software nicht mehr, sauber klingende WAV-Dateien zu erzeugen. Die im Vergleich zum Audio-CD-Player schwächere bzw. ungeeignetere Fehlerkorrektur des PCs kann die künstlichen Fehler nicht unhörbar korrigieren.[1083]

Zusätzlich zur Manipulation an den Audiodaten ist die neuste Version von *SafeAudio* in der Lage, ähnlich wie bei *Key2Audio* die Zeitdaten zu stören und den Audioteil einer CD für einen PC unsichtbar zu machen.[1084]

SafeAudio wurde bislang hauptsächlich von *Universal Music* für den US-amerikanischen Markt verwendet.

(3) *Cactus Data Shield*

Das *Cactus Data Shield (CDS)* des israelischen Herstellers *Midbar Tech*[1085] war der erste Audio-CD-Kopierschutz, der auf dem deutschen Tonträgermarkt eingesetzt wurde[1086]. Bis Februar 2002 wurden nach Angaben von *Midbar Tech* bereits über zehn Millionen CDs für den amerikanischen und europäischen Markt mit dem *CDS* ausgestattet.[1087] Im August 2002 waren es bereits über 30 Millionen CDs weltweit.[1088]

Midbar Tech bietet seinen Kopierschutz in drei Versionen an: *CDS-100, CDS-200* und künftig *CDS-300*. Während das *CDS-100* das Abspielen auf PC-Laufwerken verhindern soll, ist es bei *CDS-200*-geschützten CDs möglich, den Inhalt auch auf einem PC wiederzugeben. Beide Systeme bedienen sich illegaler TOCs und Multisessions, *CDS-200* streut zusätzlich fehlerhafte Informationen in den Audiostrom ein, die beim „Rippen" zu Kopierfehlern führen. Um zu gewährleisten, dass die Titel einer CD mit *CDS-200* auf einem PC-Laufwerk abspielbar sind, enthält die CD neben dem Audioteil einen Datenteil, in dem die Stücke zusätzlich in einem geschützten und reduzierten Format abgelegt sind. Diese Dateien können nur von der Original-CD mit einem mitgelieferten, speziellen Software-Player wiedergegeben werden, ein Kopieren der reduzierten Dateien ist ebenso nicht möglich wie das „Rippen" der Audiodaten auf die Festplatte.

CDS-300 soll den Transfer der geschützten Audiodaten auf den PC oder einen MP3-Player zulassen, dabei jedoch digitales Rechtemanagement (DRM) unterstützen, d.h. eine vom Rechtsinhaber kontrollierte Weiterverwendung ermöglichen.[1089]

1083 Vgl. *Zota*, Klonverbot, **c't** 2/2002, S. 90.
1084 *Harbonn*, **ZDNet.de**.
1085 http://www.midbartech.com.
1086 Das bei der CD *„Razorblade Romance"* der finnischen Rockgruppe *H.I.M.* eingesetzte Verfahren änderte die TOC-Einträge der CD derart rigoros, dass neben PC-Laufwerken auch zahlreichen Musik-CD-Player den Dienst versagten. Der Kopierschutz wurde daraufhin bei der Folgeauflage wieder entfernt, *Peeck*, **c't** 15/2001, S. 16. Mittlerweile wurde das *CDS* weiterentwickelt und in „verträglicherer" Form ausgeliefert.
1087 **Heise Online News** vom 13.02.2002, http://www.heise.de/newsticker/meldung/24813.
1088 **musikwoche.de Online News** vom 27.08.2002, http://www.musikwoche.de.
1089 *Harbonn*, **ZDNet.de**; zu DRM siehe unten Teil 3, C. II. 3.

CDS-Kopierschutzverfahren werden von den Labels der *BMG* (*CDS-100* und *200*), *EMI* (*CDS-100*), *Warner Music* (*CDS-200*) und *Universal Music* (*CDS-200*) verwendet.

Die technische Umgehung der auf dem Markt befindlichen Kopierschutzsysteme für Audio-CDs gelingt den meisten Hobby-Kopierern. Dank ausführlicher Anleitungen in Internetforen und Computerzeitschriften erhalten sie die notwendigen Tipps zur Auswahl der richtigen Brenn-Software und –Hardware. Denn mit den meisten herkömmlichen CD-Brennprogrammen lassen sich kopiergeschützte Audio-CDs nicht vervielfältigen. Spezielle Software-Tools wie *Blindwrite Suite, CloneCD* oder *CD Mate* sind jedoch in Kombination mit entsprechenden Brennern in der Lage, den überwiegenden Teil geschützter CDs zu kopieren.[1090] Die Anforderungen an die Hardware sind nicht allzu hoch und werden von einem Großteil der aktuellen CD-Brenner erfüllt; unerlässlich ist beispielsweise, dass das Gerät neben den Nutzdaten auch die zur Fehlerkorrektur vorgesehenen Bytes unverändert auslesen und schreiben kann (sogenannter RAW-Modus).[1091] Vereinzelt gibt es sogar Laufwerke, die sich gänzlich unbeeindruckt von einem Teil der Kopierschutzverfahren zeigen. Entsprechende „Kompatibilitätslisten“ finden sich ebenfalls im Internet und in Computerzeitschriften.

Abbildung 112 – Schlagzeile einer Computerzeitschrift

[1090] *Zota*, Klonverbot, **c't** 2/2002, S. 90.
[1091] *Zota*, Klonverbot, **c't** 2/2002, S. 90.

Abbildung 111 – Schlagzeile einer Computerzeitschrift

Mit besonderer Häme wurde ein Bericht der Nachrichtenagentur *Reuters* in der Kopierer-Szene vernommen, wonach sich der Kopierschutz *Key2Audio* mittels eines simplen Filzstiftstrichs auf der Unterseite der geschützten Audio-CD deaktivieren ließ. Mit der Markierung wurde jene Session erfolgreich verdeckt, welche die PC-Laufwerke irritieren sollte.[1092]

Gelingt das Erstellen einer gebrannten Kopie, lässt sich diese in beinahe allen Fällen in PC-Laufwerken abspielen und auslesen.[1093] Selbst wenn sich der Inhalt einer CD über diesem Umweg nicht „rippen" lässt, ist die Bedeutung der Kopierschutzsysteme für die Online-Musikpiraterie zu vernachlässigen. Wie bereits erwähnt wurde, gehört es zu den Besonderheiten der Online-Kriminalität, dass kriminelle Automatismen bei unbegrenzter Multiplikation der Tatobjekte in Gang gesetzt werden können.[1094] Es bedarf somit nur einer einzigen gelungenen Kopie eines Liedes, um in Windeseile weitere Kopien über den ganzen Globus zu verteilen. Abgesehen von der Umgehung mittels Brennutensilien ist es bei allen vorgestellten Kopierschutzverfahren möglich, qualitativ hochwertige Kopien durch Analog- oder Digitalüberspielungen anzufertigen. Über das notwendige Know-how und die entsprechenden Gerätschaften verfügen alle MP3-Gruppen sowie zahlreiche Einzeltäter, so dass die P2P-Netze und FTP-Server der MP3-Gruppen immer mit den aktuellsten Veröffentlichungen der Plattenfirmen gefüllt sein werden. Nicht zu vernachlässigen ist in diesem Kontext auch die Anzahl der MP3s in Tauschnetzwerken, die nicht von Audio-CDs sondern aus anderen Quellen stammen; besonders weit verbreitet sind „Radio-Rips", die von den meisten Konsumenten als qualitativ ausreichend empfunden werden.

Die Kopierschutzmaßnahmen werden zudem kritisiert, da sie die legale Verwendung gekaufter CDs behindern: Außer dem erwünschten Effekt, dass die manipulierten CDs nicht auf PC-Laufwerken

---

1092 Vgl. **Heise Online News** vom 24.05.2002, http://www.heise.de/newsticker/meldung/27634.
1093 Vgl. *Harbonn*, **ZDNet.de**.
1094 Vgl. *Kube*, **Kriminalistik** 1996, S. 622.

abspielbar sind, tritt der höchst unerwünschte Nebeneffekt auf, dass auch einige ältere Audio-CD-Player, DVD-Player oder CD-Autoradios das Abspielen der kopiergeschützten CDs verweigern.[1095] Für die CD-Käufer, die solche Geräte ihr Eigen nennen, sind die CDs nutzlos bzw. in ihrer Nutzung drastisch eingeschränkt, so dass es häufig zu Reklamationen im Tonträgereinzelhandel kommt. Vor allem in Großbritannien soll es derart viele Reklamationen gegeben haben, dass der Audio-CD-Kopierschutz dort schon „kein Thema mehr" sei. Die Händler hätten sich irgendwann geweigert, solche CDs zu verkaufen.[1096] Die Stimmung in Deutschland ist ähnlich, in der öffentlichen Meinung wird der Kopierschutz als kontraproduktive Maßnahme angesehen und häufig als „Abspielschutz" oder „Wiedergabeverhinderer" bezeichnet. Ein besonderes Ärgernis erlebten Besitzer eines *iMac* Rechners, wenn sie die CD *„A New Day Has Come"* von *Celine Dion* abspielen wollten: Nach dem Einlegen der CD ließ sich der CD-Schacht nicht mehr öffnen, der Rechner konnte auch nicht mehr neu gestartet werden. Den Betroffenen blieb nichts anderes übrig als der Gang zum nächsten *Apple*-Händler, der dann das Gehäuse öffnen musste.[1097]

Der Umstand, dass viele Händler in Deutschland die CDs anstandslos umtauschen, wird – sofern man den zahlreichen Beiträgen in Internetforen Glauben schenkt – rege ausgenutzt. Unter dem Vorwand, die erworbene CD laufe nicht im Auto, verlangen die Scheinkunden ihr Geld zurück, nachdem sie zu Hause eine Kopie der CD angefertigt haben. Dieses Vorgehen sei „billiger als im CD-Verleih der nächsten Videothek", heißt es bei einem Forumsteilnehmer, der sich höchstwahrscheinlich nicht darüber im Klaren ist, dass sein Handeln im strafrechtlich relevanten Bereich liegt.

Ein weiteres Problem mit einigen Kopierschutzsystemen ergibt sich in klanglicher Hinsicht: Das HiFi-Fachmagazin *Audio* kam im Januar 2002 bei einem Test zu dem Ergebnis, dass ein Teil der eingesetzten Kopierschutzverfahren die Klangqualität von Audio-CDs verringert.[1098] Mit Spezialgeräten konnten die Tester kurze Aussetzer und kleine Geräusch-Artefakte nachweisen, die beim Abspielen der geschützten CDs auftraten. Betroffen sind vor allem Verfahren, die auf der Ausnutzung der Fehlerkorrektur der CD-Player basieren. Was in diesem Zusammenhang selten bedacht wird, ist, dass die Fehlerkorrektur entwickelt wurde, um Beschädigungen (meist kleine Kratzer) auf der Unterseite der CD unhörbar zu korrigieren. Kommen solche Fehler zu den künstlich produzierten Fehlern hinzu – was bei normalem Gebrauch einer Audio-CD über einen gewissen Zeitraum der Fall ist – werden zahlreiche Audio-CD-Player es nicht mehr schaffen, die CD ordnungsgemäß wiederzugeben.

Dass sich ein Teil der legal erworbenen CDs nicht mehr am PC abspielen lässt, empfinden viele Kunden als ärgerliche Einschränkung ihrer gewohnten Nutzungsmöglichkeiten. Auf den Unmut der Verbraucher reagierte die Industrie unter anderem mit dem Kopierschutzsystem *CDS-200*, das zusätzlich ein auf dem Computer abhörbares MP3-File enthält.[1099] Einen anderen Weg geht *SONY*

1095 Vgl. **Heise Online News** vom 13.02.2002, http://www.heise.de/newsticker/meldung/24813 zu *CDS*-geschützten CDs; *Zota/Hansen/Himmelein*, **c't** 22/2001, S. 52 zu CDs mit *Key2Audio*-Kopierschutz.
1096 So *Philips*-Sprecher *Petri* in den **ZDNet News** vom 09.01.2002, http://www.zdnet.de/news/hardware/0,39023109,2102238,00.htm.
1097 Vgl. **ZDNet News** vom 14.05.2002, http://www.zdnet.de/news/hardware/0,39023109,2110156,00.htm.
1098 **ZDNet News** vom 18.01.2002, http://www.zdnet.de/news/software/0,39023144,2102814,00.htm.
1099 Vgl. das Interview mit *Spiesecke*, Sprecher der deutschen *IFPI*, **c't** 2/2002, S. 84.

Music mit seinem Web-Portal *Esquare4u*[1100]. Käufer einer *Key2Audio*-geschützten CD können dort nach Eingabe eines neunstelligen Schlüssels die Titel der CD im *WMA*-Format auf ihre Computer herunterladen oder sich per *RealAudio*-Stream anhören.[1101] Beide Formate unterstützen digitales Rechtemanagement (DRM)[1102] und sind so konfiguriert, dass die Titel nur auf dem Rechner abgespielt werden können, von dem aus sich der Nutzer legitimiert hat.[1103]

Zwar handelt es sich bei diesen Maßnahmen um löbliche Ansätze, doch ist zu bezweifeln, dass sie den Unmut der Kunden in Wohlgefallen auflösen können. Ein Großteil der musikbegeisterten PC-Nutzer will seine CDs ins MP3-Format (in der Regel in einer Qualität von 192 KBit/s) überführen, seine Lieblingslieder auf der Festplatte lassen bzw. auf einen mobilen MP3-Player transferieren und den Rest auf CD-R archivieren. All das wird weder durch Systeme wie *CDS-200* noch durch Download-Portale wie *Esquare4u* gewährleistet. Hinzu kommt, dass letzteres für den Verbraucher ohne Internet-Zugang völlig nutzlos ist.

Die geschilderten Umstände bewirken nicht zuletzt, dass es sich beim Audio-CD-Kopierschutz um eine extrem unpopuläre Maßnahme handelt. Es ist zu befürchten, dass er nicht nur zu vermehrten Reklamationen führen, sondern auch die Nachfrage nach Raubkopien der betreffenden Alben steigern wird[1104]. Jemand, der nach wie vor ein frei nutzbares MP3-File eines Liedes haben möchte, wird in Zukunft gar nicht mehr daran denken, sich eine Original-CD zu kaufen, sondern gleich eine Tauschbörse nutzen.

Auf das Spannungsfeld zwischen pauschaler Vergütung auf der einen Seite und technischer Verhinderung der Privatkopie auf der anderen Seite wurde bereits hingewiesen.[1105] Die damit zusammenhängende Problematik wird in der Audio-Kopierschutzdebatte am deutlichsten, wenn man bedenkt, dass es kein Land gibt, in dem die Gerätehersteller so viele Urheberrechtsabgaben bezogen auf das Gesamtmarktvolumen bezahlen müssen wie in Deutschland.[1106] Eine de-facto-Verhinderung der Privatkopie würde diesen Abgabenleistungen jegliche Rechtfertigung entziehen.

b) Unternehmensstrategische Maßnahmen

(1) Herstellung spezieller Promo-Kopien

Um zu verhindern, dass Raubkopien von Musikwerken vor dem „Street Date", also dem offiziellen Veröffentlichungstermin, im Internet kursieren, haben sich einige Plattenfirmen dazu entschlossen, für die Bemusterung zu Promotionzwecken Spezialversionen der Tonträger herzustellen. In der Regel werden die Lieder in ihrer Qualität vermindert, oder es werden nur Auszüge der Lieder auf die Promo-CDs gebrannt. Dies hindert die MP3-Gruppen jedoch nicht daran, den Inhalt als „Promo-

---

1100 http://www.esquare4u.com.
1101 Aus Kostengründen bieten jedoch nicht alle Labels, die *Key2Audio* einsetzen, einen Service wie *Esquare4u* an.
1102 Siehe unten Teil 3, C. II. 3.
1103 **Heise Online News** vom 25.03.2002, http://www.heise.de/newsticker/meldung/26024.
1104 Vgl. *Zota/Hansen/Himmelein*, **c't** 22/2001, S. 52.
1105 Siehe oben Teil 3, C. I. 2. d) (2) (Exkurs).
1106 So *Kamp*, Deutschland-Chef der Sparte Konsumenten-Elektronik bei *Philips* in den **Heise Online News** vom 04.03.2002, http://www.heise.de/newsticker/meldung/25312. Der Abgabenanteil auf einzelne Geräte an die Inhalteanbieter habe sich in den vergangenen zehn Jahren um das Vier- bis Fünffache erhöht.

Rip“ oder „Advance Copy“ zu veröffentlichen. Sobald das finale Produkt auf den Markt geworfen wird, bringen es die Gruppen als „Retail Version“ heraus.

(2) Senkung der CD-Preise

Heftige Auseinandersetzungen innerhalb der deutschen Tonträgerbranche gibt es im Rahmen der sogenannten CD-Preisdiskussion. Ein Teil der Branche macht nicht nur das mangelnde Qualitätsbewusstsein im A&R-Bereich[1107], Online-Tauschbörsen und Schwarzbrennerei für die Branchenkrise verantwortlich, sondern auch überhöhte CD-Preise[1108]. Trotz des rückläufigen Absatzes ist ein Trend zu stetig steigenden CD-Preisen zu beobachten. Ende 2001 hatten alle großen Hersteller die Preise angehoben, was zu Unmut auf Seiten der Verbraucher und bei den Handelsunternehmen geführt hat.[1109] Die Vertreter der Tonträgerhersteller wollen an den Preisen festhalten und erwägen sogar weitere Erhöhungen; nicht selten hört man den Vergleich, dass „ein gutes Buch auch um die 25 € koste“ und dass der Spielraum nach oben noch nicht ausgeschöpft sei.

Leider entbehrt diese Überlegung jeder betriebswirtschaftlichen Vernunft. Es ist kontraproduktiv, sinkenden Verkaufszahlen mit Preiserhöhungen entgegenzutreten, denn es ist damit zu rechnen, dass mit steigenden Preisen die Verkäufe weiter zurückgehen werden. Bestätigt wird diese Erkenntnis vom US-amerikanischen Finanz- und Consulting-Unternehmen *Merrill Lynch*, das Anfang 2002 den Tonträgerunternehmen geraten hat, künftig einen Standardpreis von zehn US-Dollar (rund 10 €) für CD-Neuveröffentlichungen anzusetzen, um den Umsatz wieder anzukurbeln. Amerikanische Handelsketten wie die *Virgin Megastores* hätten bereits im Weihnachtsgeschäft 2001 sehr gute Erfahrungen mit niedrigen CD-Preisen gemacht.[1110]

(3) Schaffung legaler Download-Angebote

Um die hochmotivierten Musikkonsumenten von den kostenlosen Tauschbörsen zu bezahlpflichtigen Angeboten zu bewegen, ist es nicht sinnvoll, die Gruppe der Downloader als potenzielle Internetpiraten zu brandmarken. Für die Musikindustrie gilt es vielmehr, reizvolle Alternativen zu schaffen, was gleich aus mehreren Gründen geboten ist:

Wie verschiedene Studien ergeben haben, zeigt ein beachtlicher Teil der an Musikdownloads interessierten Nutzer eine erhöhte Zahlungsbereitschaft für das Herunterladen von digitalen Musikstücken.[1111] Dies mag unter anderem darin begründet liegen, dass im Netz nicht alle Lieder auf Anhieb und in der gewünschten Qualität aufgetrieben werden können. Diese Nachteile der „illegalen Angebote“ kann sich die Musikindustrie mit der Bereitstellung eines großen Repertoires qualitativ hochwertiger Dateien zunutze machen. Mit einer Strategie, die allein auf die juristische Verfolgung

---

[1107] A&R steht für Artist & Repertoire. Die A&R-Manager der Plattenfirmen sind in erster Linie für die Akquise neuer Künstler und Produkte verantwortlich.
[1108] Siehe Fn. 891.
[1109] *Köhn/Theurer*, **FAZ** vom 20.11.2001, S. 30.
[1110] **musikwoche** 1-2/2002, S. 3.
[1111] Vgl. *Wiedmann/Frenzel/Walsh*, Musik im Internet – Teil 2, **musikmarkt** 50/2001, S. 18, wonach 30% der befragten Downloader angaben, dass sie für Musik aus dem Internet bezahlen würden. Für ein Abonnement-Modell (unbegrenzte Zahl von Songs gegen Gebühr) entschieden sich knapp 60% der Zahlungswilligen, wobei wiederum 54% von ihnen eine Gebühr von 2,50-5 € /Monat vorschwebt. Die Pay-per-Song-Variante wird entsprechend von ca. 40% der Downloader favorisiert (S. 19).

setzt, läuft die Musikwirtschaft Gefahr, ihr Image zu beschädigen und damit den Trend zur kostenlosen Beschaffung von Musik weiter zu verschärfen.[1112] Das Image der Industrie ist innerhalb der Internetgemeinde bereits angekratzt. In kostenlosen Downloads sieht ein großer Teil der Nutzer eine Art ausgleichende Gerechtigkeit für Preisabsprachen und das „Monopolgehabe der Musikindustrie". Freies Herunterladen von MP3-Dateien ist für viele Downloader Ausdruck von Verbraucherprotest.

Darüber hinaus hat die Web-Vermarktung von Musik enorme wirtschaftliche Vorteile gegenüber dem physikalischen Tonträgerhandel, denn die Kosten für CD, Hülle, Artwork, Distribution, Lagerhaltung etc. entfallen komplett.

Unbedingt zu berücksichtigen ist bei der Schaffung bezahlpflichtiger Angebote die Nachfragesituation. Kaum ein Kunde wird sich mit Formaten zufrieden geben, die einen geringeren Nutzungsumfang oder schlechtere Klangqualität bieten als das MP3-Format. Als wichtiges Kriterium für den Kauf von Musikfiles über das Internet gilt des Weiteren die Möglichkeit der individuellen Zusammenstellung von Titeln.[1113] Auch ist zu beachten, dass Anmeldung und Abrechnung benutzerfreundlich und unkompliziert gestaltet werden müssen. Kreditkartenzahlungen werden in Deutschland noch weitgehend mit großer Skepsis betrachtet; anbieten würde sich eine Abrechnung über die Telefonrechnung der Surfer.

Die Angebote der großen Plattenfirmen orientieren sich kaum an der Nachfrage der Musik-Downloader, sondern sind wesentlich restriktiver ausgestaltet. Zur bisherigen Online-Strategie der meisten Unternehmen gehörten kopiergeschützte Formate, die sich weder auf CD brennen noch auf andere Rechner bzw. mobile Player transferieren lassen.[1114] Besonders weit verbreitet sind die folgenden zwei Formate, die wie das MP3-Format auf der Reduktion unhörbarer Artefakte beruhen und sowohl Download als auch Streaming erlauben:

(a) *Windows Media Audio (WMA)*

Das von *Microsoft* entwickelte *WMA*-Format unterstützt im Gegensatz zu MP3 digitales Rechtemanagement, weshalb es sich für die geschützte Distribution von digitaler Musik eignet. Beim Erstellen eines *WMA*-Files kann der Rechtsinhaber beispielsweise festlegen, ob und wenn ja, wie oft das File weiterkopiert werden darf und in welchem Zeitraum es abspielbar ist. Nach Aussagen von *Microsoft* ermöglicht es bei besserem Klang noch kleinere Dateigrößen als MP3, was sowohl die Downloadzeiten für die Kunden verkürze als auch Bandbreite und Speicherplatz für Provider spare.[1115]

Experten räumen dem Format gute Chancen ein, der Nachfolger von MP3 zu werden, denn allein auf Grund seiner exponierten Marktstellung ist *Microsoft* in der Lage, Standards zu etablieren. Um dies voranzutreiben, vergibt *Microsoft* kostenlose Lizenzen zur Nutzung von *WMA* an Hersteller von

---

1112 *Wiedmann/Frenzel/Walsh*, Musik im Internet – Teil 2, **musikmarkt** 50/2001, S. 18.
1113 *Wiedmann/Frenzel/Walsh*, Musik im Internet – Teil 2, **musikmarkt** 50/2001, S. 18.
1114 Einen umfassenden Überblick zu den Angeboten gibt *Hansen*, **c't** 16/2002, S. 70 ff.
1115 http://www.microsoft.com/windows/windowsmedia/music/default.aspx.

HiFi-Produkten.[1116] *WMA* wird derzeit von allen Major Companies[1117] genutzt, und zahlreiche portable Audio-Player unterstützen mittlerweile das *Microsoft*-Format.

(b) *Liquid Audio*[1118]

Auch *Liquid Audio* des gleichnamigen Unternehmens unterstützt digitales Rechtemanagement. Zu den wählbaren Parametern („Permission Sets") gehören unter anderem territoriale Beschränkungen, Festlegung zeitlicher Nutzungsperioden oder die Erlaubnis bzw. das Verbot, ein File auf CD zu brennen. In klanglicher Hinsicht ist *Liquid Audio* nicht auf eine Encoding-Technologie festgelegt, es unterstützt verschiedene Codecs wie z.B. MP3, *AAC, ATRAC3* oder *WMA*.

Im Gegensatz zu *WMA* wird bei der Kodierung einer *Liquid Audio* Datei ein digitales Wasserzeichen eingewoben. Hierbei werden mit steganographischen Methoden Bereiche redundanter Informationen dergestalt modifiziert, dass darin zusätzliche Informationen gespeichert werden können. Die Markierung soll im Idealfall vom Benutzer weder erkannt noch entfernt oder verändert werden können, ohne die Datei zu zerstören oder zumindest erhebliche Qualitätsverluste zu erreichen.[1119] Die eingewobenen Informationen bleiben sogar bei analogen Überspielungen erhalten.

Liquid-Audio-Dateien lassen sich nur mit dem *Liquid Player* (oder über ein entsprechendes Plug-In für *WinAmp*) wiedergeben, einem speziellen Programm, das überprüft, ob es sich um lizenzierte Files handelt.

Nicht nur wegen der genannten Nutzungsbeschränkungen sondern auch wegen der Preisgestaltung sind die meisten Bezahl-Angebote unattraktiv für die Musik-Downloader. Bisweilen ist es sogar vorgekommen, dass heruntergeladene Titel eines Albums den Surfer mehr gekostet haben als eine Original-CD mit Artwork, besserer Klangqualität und vollen Nutzungsmöglichkeiten.[1120] Erst seit kurzem ist ein Trend zu beobachten, dass die Download-Angebote günstiger werden[1121]. Bei einem Preis von 0,50 € pro Lied wäre die Musik so günstig, dass sich für viele Nutzer das „Stehlen" nicht mehr lohnt. Der Anreiz, nach einem nichtlizenzierten Lied mehrere Stunden lang zu suchen, fehlt, wenn man es für 0,50 € sofort, legal und in guter Qualität haben kann. Letztlich geht es beim E-Commerce um Komfort.

Insgesamt ist die Schaffung legaler Download-Alternativen eine wirksame und seit Jahren überfällige Maßnahme, um die nichtlizenzierte Musiknutzung zu reduzieren – vorausgesetzt, die Musikindustrie orientiert sich an der Nachfrage der Interessierten. Gestaltet man die Preise attraktiv und gibt den Kunden ausreichend Flexibilität im Umgang mit der Musik, werden die meisten von ihnen zufrieden sein und weniger Tauschbörsen oder andere illegale Web-Angebote nutzen. Der Schutz von Musik

---

1116 **Heise Online News** vom 13.04.2001, http://www.heise.de/newsticker/meldung/17069.
1117 Siehe Fn. 1038.
1118 http://www.liquidaudio.com.
1119 Vgl. Hoeren/Sieber-*Bechtold*, 7.11, Rdnr. 11,
1120 Vgl. *Schult*, **c't** 14/2001, S. 106 (*mod* der *Deutschen Telekom*).
1121 Vgl. *Hansen*, **c't** 16/2002, S. 73. Besondere Beachtung verdient das Downloadportal von *Universal Music „Popfile"* (http://www.popfile.de); für 0,99 € pro Titel können sich Nutzer dort DRM-kompatible Musik (im *WMA*-Format) herunterladen, die sich weiterkopieren und auf CD brennen lässt.

mittels technologischer Maßnahmen hat stets Einschränkungen in der Nutzung zur Folge, weshalb zu erwägen ist, auf DRM-Systeme zu verzichten. Die Angst, dass sich ungeschützte Files in Tauschbörsen wiederfinden werden, ist zwar berechtigt, allerdings kursieren die gleichen Stücke bereits aus anderen Quellen im Netz. Hingewiesen wurde in diesem Zusammenhang auf die Tätigkeit der MP3-Gruppen[1122] und die Möglichkeit von Mitschnitten aus digitalem Radio und Web-Radio[1123].

3. Entwicklung von DRM-Systemen

„DRM" hat sich in den letzten Jahren zu einem Zauberwort für die Content-Industrie entwickelt. Digital Rights Management steht für eine Technologie, die es ermöglichen soll, einzelne Nutzungsvorgänge geschützter Werke unter anderem zu Abrechnungszwecken zu erfassen und die Verbreitung derselben zu kontrollieren – selbst wenn sich die Werke bereits in der Sphäre des Anwenders befinden.

Das Prinzip hinter DRM beruht bei fast allen Systemen auf der Einrichtung eines sicheren Bereichs auf dem Rechner des Nutzers (DRM-Container). In diesem Container werden die Werke verschlüsselt abgelegt und sind nur demjenigen zugänglich, der über einen speziellen Schlüssel verfügt. Bei jedem einzelnen Nutzungsvorgang muss der aufgerufene Inhalt des Containers von der Abspiel- oder Export-Software des DRM-Systems entschlüsselt werden. Zu einem DRM-System können darüber hinaus Module gehören, die die folgenden Optionen bieten:[1124]

- Benutzeridentifizierung
- Authentizitätsprüfung
- Zugangskontrolle
- Verschlüsselung (in der Regel asymmetrisch)
- Verwendung digitaler Wasserzeichen
- Verwendung digitaler Fingerabdrücke (nutzerbezogene individuelle Markierung von Inhalten) – ermöglicht die Überführung des Täters eines Urheberrechtsdelikts, sogenanntes Traitor-Tracing.
- Festlegung von Nutzungsbedingungen (u.a. Kopiersperre, Kopierkontrolle, Wiedergabekontrolle) – technisch gesehen ist es ohne weiteres möglich, verschiedene Stufen der Nutzerrechte festzulegen. Von „nur hören" über „einmal kopieren ist erlaubt" bis zur uneingeschränkten Kopiererlaubnis[1125].
- Integration eines Zahlungssystems

1122 Siehe oben Teil 3, A. III. und IV.
1123 Siehe oben Teil 3, A. IV. 2. a.E.
1124 Vgl. *Günnewig/Hauser*, **c't** 16/2002, S. 182 ff.
1125 Vgl. das Interview mit *Petri* in **PC Pr@xis** 3/2002, S. 22.

Grundsätzlich ist bei DRM-Systemen zwischen reinen Softwarelösungen und Kombinationen aus Hard- und Software zu unterscheiden. Letzteren wird eine höhere Sicherheit gegen Umgehungsversuche attestiert, allerdings wird es noch dauern, bis die Konsumenten mit entsprechender DRM-kompatibler Hardware ausgestattet sind. Geht es nach dem Willen der Entwickler, sollen künftige PCs bereits mit speziellen DRM-Chips[1126] ausgeliefert werden, die als Verschlüsselungs-Coprozessoren arbeiten und Benutzerauthentifizierung und –identifikation ermöglichen.[1127] In einem ersten Schritt sollen solche Chips auf das Motherboard gelötet, aber auch in PDAs[1128], Mobiltelefone und Unterhaltungselektronik-Komponenten integriert werden. Schließlich sollen die Funktionen des Chips direkt im Prozessor des Rechners implementiert werden, was das System noch sicherer gegenüber Umgehungsversuchen machen wird.[1129]

Sogar Festplatten könnten in Zukunft nur noch in DRM-kompatibler Form ausgeliefert werden, sofern es dem Herstellerkonsortium *4C Entity (4C)*[1130] gelingen sollte, ein selbstentwickeltes Schutzverfahren für digitale Medien in den ATA-Standard[1131] einfließen zu lassen: Die Content Protection for Recordable Media (CPRM) sieht vor, dass sich urheberrechtlich geschütztes Material künftig nur noch in verschlüsselter Form und auf CPRM-konformen Medien speichern lässt. Jede Festplatte bekommt vom Hersteller einen sogenannten Media Key Block aufgespielt, den dieser in Lizenz von dem Unternehmen *4C* erwirbt und der einmalig ist. Eine Software, die geschütztes Material abspeichern will, muss einen von *4C* vergebenen Schlüssel besitzen. Mit diesem authentifiziert sie sich in einem kryptographischen Challenge-Response-Verfahren und erhält daraufhin einen Schlüssel, mit dem sie das Material kodiert und als gewöhnliche Datei abspeichert. Zur Wiedergabe fordert die Software auf demselben Wege den Dekodierschlüssel vom Laufwerk an, wobei sich die ausgetauschten Schlüssel bei jedem Kopiervorgang ändern.[1132]

Die derzeit auf dem Markt befindlichen DRM-Systeme sind zueinander inkompatibel, was einer der Gründe ist, warum sie für die Distribution geschützter Inhalte noch keine allzu bedeutende Rolle spielen. Bislang wurden komplexere DRM-Systeme von der deutschen Musikindustrie eher selten verwendet. Eines der ersten softwarebasierten DRM-Systeme wurde 2001 eingesetzt, um Fans der französischen Gruppe *Daft Punk* in den Genuss exklusiver Web-Inhalte kommen zu lassen:[1133] Jeder Käufer einer Original-CD der Gruppe erhielt mit der CD-Hülle einen individuellen und einmalig nutzbaren Zugangscode für einen geschützten Bereich der Band-Homepage. Nach Eingabe des Codes auf der Webseite überträgt der Server eine sieben Megabyte große Datei auf den heimischen Rechner, die den *InterRights Point* des Unternehmens *InterTrust* installiert und das DRM einrichtet. Beim ersten Aufruf aktiviert sich die Software über eine Verbindung zum *InterTrust*-Server. Nach erneuter Eingabe des Codes kann man schließlich das Musikfile herunterladen. Dabei handelt es sich

---

1126 Auch Trusted Platform Module (TPM) oder „Fritz Chip" – benannt nach dem US-Senator *Ernest „Fritz" Hollings*, der sich politisch für die Einführung von DRM-Systemen einsetzt.
1127 *Himmelein*, Der digitale Knebel, **c't** 15/2002, S. 18.
1128 PDA steht für Personal Digital Assistant und bezeichnet tragbare Kleincomputer, die vornehmlich zur Terminplanung und Adressverwaltung verwendet werden.
1129 Vgl. *Himmelein*, Der digitale Knebel, **c't** 15/2002, S. 18.
1130 http://www.4centity.com. Die *4C Entitiy, LLC* wurde gegründet von den Firmen *IBM, Intel, Toshiba* und *Matsushita*.
1131 Beim ATA/ATAPI-Standard handelt es sich um die derzeit bedeutendste IDE-Schnittstellenspezifikation.
1132 *Bögeholz*, **c't** 2/2001, S. 24.
1133 Vgl. *Himmelein*, Geschenk mit Pferdefuß, **c't** 13/2001, S. 39.

nicht um ungeschützte MP3-Dateien sondern um proprietäre SAF-Dateien, die sich nur auf einem System mit aktiviertem *InterRights Point* wiedergeben lassen.

Die heutigen DRM-Systeme sind zudem noch nicht ausreichend gegen Umgehungsmaßnahmen gefeit. Es ist zu beachten, dass an den analogen Ausgängen eines PC immer noch ein ungeschütztes Signal anliegt, das mit entsprechenden A/D-Wandlern in hervorragender Qualität kopiert werden kann[1134]. Mit entsprechenden Tools gelingt es sogar, den Datenstrom noch vor dem Verlassen der Soundkarte abzugreifen und auf die Festplatte umzulenken. Solche Programme klinken sich als Soundkartentreiber in das Betriebssystem ein und schreiben die entschlüsselten digitalen Daten in eine WAV-Datei. Das von sämtlichen Nutzungsbeschränkungen befreite Ergebnis kann der Nutzer in eine MP3-Datei umwandeln oder auf eine Audio-CD brennen.[1135] Gegen diese Art der Umgehung helfen weder Wasserzeichen noch digitale Fingerabdrücke, denn diese enthalten nur Urheber- bzw. Nutzerinformationen. Erst wenn DRM-Systeme fest ins Betriebssystem verankert und Digital-Rekorder und PCs mit entsprechenden Erkennungsschaltkreisen ausgestattet sind, kann nach Erkennung eines Wasserzeichens ein Kopiervorgang erfolgreich unterbunden werden.[1136]

Der erste, breit angelegte Versuch, die großen Plattenfirmen mit Endgeräteherstellern und DRM-Anbietern an einen Tisch zu bringen, um eine Spezifikation für ein sicheres Übermittlungsverfahren für digitale Musik zu entwickeln, war die *Secure Digital Music Initiative (SDMI)*. Im Dezember 1998 gab die *RIAA* die Gründung der *SDMI* bekannt, der sich unter anderem *BMG Entertainment, SONY Music, Warner, IBM, Intel* und *AT&T* anschlossen. Zu den geplanten Schutzmaßnahmen gehörte auch die Entwicklung verschiedener kopiergeschützter Formate.

Um die Formate „auf Herz und Nieren zu prüfen", schrieb die *SDMI* im Herbst 2000 einen Wettbewerb aus (die sogenannte *SDMI*-Challenge), bei dem jedermann versuchen konnte, innerhalb von drei Wochen aus sechs verschiedenartig kopiergeschützten Musikdateien sämtliche Schutzvorkehrungen zu entfernen. Einem Team um *Princeton*-Professor *Edward Felten* gelang es, vier Wasserzeichen zu entfernen und Fehler in den restlichen beiden Versuchsanordnungen zu finden.[1137] *Feltens* Schlussfolgerungen fielen eindeutig aus: „Wenn es einem Konsumenten möglich ist, geschütztes Material zu hören oder zu sehen, wird es dem Konsumenten auch möglich sein, das Material zu kopieren".[1138] „Ob wir glauben, dass man jeden Kopierschutz für Audiodaten knacken kann? Sicherlich [...] – insbesondere glauben wir, dass keine wasserzeichenbasierte Methode Aussicht auf Erfolg hat".[1139] Als *Felten* die Ergebnisse seiner Arbeit auf einem Kongress vorstellen wollte, wurde er im Vorfeld von einem Vertreter der *SDMI* aufgefordert, auf die Veröffentlichung seines Manuskripts zu verzichten. Man verstehe zwar, dass er die Forschungsergebnisse anlässlich der Tagung präsentieren wolle, bitte ihn aber eindringlich, von diesem Vorhaben abzusehen. Die vor der *SDMI*-Challenge getroffene Vereinbarung erlaube es nicht, die Informationen der Öffentlichkeit

---

1134 *Laue/Zota*, **c't** 2/2002, S. 86 ff.
1135 Vgl. *Himmelein*, Geschenk mit Pferdefuß, **c't** 13/2001, S. 39.
1136 Vgl. *Himmelein*, Sind wir alle kriminell?, **c't** 2/2002, S. 81; digitale Wasserzeichen alleine stellen noch keine technische Schutzmaßnahme dar. Es handelt sich lediglich um eine Möglichkeit, Informationen jeglicher Art mit einem Werk nahezu untrennbar zu verbinden, Hoeren/Sieber-*Bechtold*, 7.11, Rdnr. 12.
1137 *Boutin*, **Wired Magazine**, 9-07 – Juli 2001.
1138 „There's no such thing as a pirate-proof distribution system", vgl. *Boutin*, **Wired Magazine**, 9-07 – Juli 2001.
1139 *Zota*, Wasserzeichen-Blamage, **c't** 10/2001, S. 54.

zugänglich zu machen. Die *SDMI* drohte *Felten* außerdem mit Konsequenzen wegen Verletzung des DMCA.[1140]

Die erfolgreiche Umgehung durch *Felten* und sein Team hat dazu geführt, dass die Aktivitäten der *SDMI* vorerst auf Eis gelegt wurden. MP3-Miterfinder *Karlheinz Brandenburg* bezeichnete die *SDMI* im Winter 2001/2002 gar als „tot".[1141]

Die *SDMI*-Formate sind nicht die einzigen Formate, die bisher „geknackt" wurden. Derzeit gibt es kein digitales Audioformat, das nicht kopiert werden kann. So ist *Microsofts WMA* einem anonymen Programmierer mit dem Decknamen *„Beale Screamer"* zum Opfer gefallen. Mit einem selbstgeschriebenen Programm namens *FreeMe* konnte er jegliche Restriktionen von einer *WMA*-Datei entfernen. Einzige Voraussetzung war der Besitz einer gültigen Nutzungslizenz.[1142] Bereits zwei Jahre zuvor war es gelungen, geschützte *WMA*-Dateien mit einem der oben beschriebenen Tools (Soundkartentreiber-Emulator) zu kopieren.[1143]

DRM-Systeme werden nicht nur aufgrund der verhältnismäßig einfachen Umgehungsmöglichkeiten kritisiert.[1144] Auch bei Datenschützern rufen sie Bedenken hervor. *Alexander Dix*, Datenschutzbeauftragter des Landes Brandenburg, befürchtet, dass mit individuellen Abrechnungsverfahren Nutzerprofile bei den Content-Anbietern gesammelt würden, was einer Einladung zum Missbrauch gleichkäme. Die Medienreferentin des *Deutschen Industrie- und Handelskammertags (DIHK) Ina Pernice* warnt: „Wir dürfen nicht politisch den gläsernen Bürger bekämpfen, während wir gleichzeitig den gläsernen Konsumenten ermöglichen".[1145]

Sofern DRM-Systeme großflächig zum Einsatz kommen, spitzt sich ein weiterer Konflikt zu, auf den bereits hingewiesen wurde[1146]: Die integrierten Kopierschutzsysteme unterwandern die Schrankenregelungen des Urheberrechts, indem sie die digitale Privatkopie unmöglich machen. Gefordert wird daher, dass der Gesetzgeber die bestehenden Schrankenregelungen zugunsten des Anwenders schützt, in dem er beispielsweise die Content-Anbieter zur Duldung von Privatkopien verpflichtet.[1147]

Ein anderer Schwachpunkt von DRM-Systemen resultiert aus den beschränkten Nutzungsmöglichkeiten für digitale Inhalte. Ist das Weiterkopieren untersagt, muss der Nutzer beispielsweise dann all seine erworbenen Werke erneut erwerben, wenn er sich einen neuen Computer anschafft.[1148] Angesichts der freien Angebote, die volle Flexibilität im Umgang mit den Musikdateien bieten, muten die nutzungsbeschränkenden Alternativen als „Provokation der Bezahlwilligen" an[1149].

1140 Vgl. **Heise Online News** vom 22.04.2001, http://www.heise.de/newsticker/meldung/17248.
1141 Vgl. **musikwoche** vom 5.11.2001, S. 5.
1142 *Gleich*, **c't** 23/2001, S. 62.
1143 **Wired News** vom 18.08.1999, http://www.wired.com/news/technology/0,1282,21325,00.html.
1144 Vgl. *Federrath*, bei *Krempl*, Content an der Kette, **c't** 4/2002, S. 32.
1145 *Krempl*, Content an der Kette, **c't** 4/2002, S. 33.
1146 Siehe oben Teil 3, C. I. 2. d) (2) (Exkurs).
1147 Vgl. *Günnewig/Hauser/Himmelein*, **c't** 17/2002, S. 20.
1148 Vgl. *Himmelein*, Volle Kontrolle, Editorial **c't** 14/2001, S. 3.
1149 *Himmelein*, Volle Kontrolle, Editorial **c't** 14/2001, S. 3.

4. Maßnahmen von Hardwareherstellern

Die Hersteller der meisten portablen MP3-Player haben ihre Geräte so konzipiert, dass ein Zurückspielen von Dateien aus dem Player in den Computer unmöglich ist. Auf diese Weise wird verhindert, dass das Gerät bei Freunden oder Bekannten an den Rechner angeschlossen wird, um Dateien auf deren Festplatte zu kopieren.

Geht es nach dem Willen der Content-Industrie, werden Abspielgeräte für digitale Musikstücke in Zukunft mit DRM-Chips ausgestattet, um „Piratenformate" wie MP3 vom Markt zu verdrängen. Tatsächlich unterstützt bereits ein Teil der heutigen Geräte DRM. Es ist jedoch ein Gegentrend aus Fernost zu beobachten: Das Gros der in Deutschland erhältlichen Standalone-DVD-Player ist in der Lage, eine Vielzahl unterschiedlicher Audio- und Videoformate von CD oder DVD wiederzugeben, zu denen auch das MP3-Format gehört.

Solange es nicht gelingt, DRM-kompatible Musik flächendeckend einzuführen, wird MP3-fähige Hardware aufgrund der enormen Nachfrage produziert werden und nicht nur bei den Musik-Downloadern reißenden Absatz finden. Es ist zu bezweifeln, dass es die Content-Industrie auf anderem Wege erreichen wird, dass die Hersteller von freien Formaten abrücken. Denn Verbote für MP3-fähige Geräte finden keine rechtliche Grundlage. MP3 ist lediglich ein Dateiformat wie jedes andere auch. Urteile wie die *Betamax*-Entscheidung[1150] und die bereits erwähnte *RIO*-Entscheidung[1151] bestätigen diese Einschätzung.

5. Andere Maßnahmen

Es ist nicht bekannt, dass die Strafverfolgungsbehörden anlassunabhängig tätig werden, um Online-Musikpiraten das Handwerk zu legen. Etwas anderes gilt nur für Fälle von professioneller Tonträgerpiraterie, deren Täter sich mittlerweile auch des Internet bedienen, um Kunden für ihre Raubpressungen zu gewinnen.

Webhosting- und Service-Provider werden in der Regel nur dann tätig, wenn der von ihnen bereitgestellte Speicherplatz massenhaft von Betreibern von MP3-Webseiten missbraucht wird, was kostenintensiven Traffic (Bandbreitennutzung) erzeugt. Provider wie *Geocities* löschen regelmäßig mehrere hundert Gigabyte an illegal angebotenen MP3-Files von den eigenen Servern. Problematisch ist hierbei häufig die Identifikation der entsprechenden Dateien, da sie zumeist umbenannt oder in verschlüsselter Form abgelegt werden, um sie möglichst lange für die Downloader bereitzustellen.

Bezüglich der freiwilligen Maßnahmen von Public-FTP-Administratoren ist auf die Ausführungen im zweiten Kapitel der Arbeit zu verweisen.[1152] Gleiches gilt für juristische Maßnahmen im Kampf gegen die Online-Piraterie.[1153]

[1150] Mit dieser wurde es *SONY* im Jahr 1981 vom *US Supreme Court* erlaubt, gegen den Willen der Hollywood-Studios einen Videorekorder auf den Markt zu bringen.
[1151] Siehe oben Teil 3, C. II. 1. b).
[1152] Siehe oben Teil 2, C. III. 7.
[1153] Siehe oben Teil 2, C. III. 8.

III. Betrachtung der Maßnahmen, über deren Einsatz spekuliert wird

1. Datenausspähung über Multimedia-Player

Für Unruhe in der Netzgemeinde sorgen seit einiger Zeit Meldungen, wonach die beiden populärsten Wiedergabeprogramme für Mediendateien, der *RealPlayer* von *RealNetworks* und der *Mediaplayer* von *Microsoft*, individuelle Nutzerdaten an alle Server übermitteln, von denen Mediendateien zum Rechner des Anwenders transferiert werden[1154]. So sollen nicht nur die MAC-Adresse[1155] der Netzwerkkarte übertragen worden sein, sondern auch Informationen über die Hör- bzw. Konsumgewohnheiten des Nutzers.[1156]

Nach Aussage eines Sprechers von *Microsoft* plant der Konzern nicht, gesammelte Daten über die medialen Konsumgewohnheiten von Kunden zu vermarkten, man wolle dies aber für die Zukunft nicht ausschließen.[1157] *Keela Robinson*, Produktmanagerin für Consumer Devices bei *RealNetworks*, stellt für ihr Unternehmen klar, dass die Daten definitiv nicht benutzt würden, „um Raubkopien aufzuspüren oder Benutzer zu identifizieren".[1158]

Angesichts der Tatsache, dass aufgrund der privatwirtschaftlich gesammelten Daten bislang keine Maßnahmen gegen Online-Musikpiraten unternommen wurden, ist davon auszugehen, dass die genannten Unternehmen mit den Datenerhebungen eher Marktforschungsinteressen verfolgen als die Bekämpfung der Online-Musikpiraterie.

2. „Virenattacken" gegen Tauschbörsennutzer

Schenkt man dem neuesten Gerücht in der MP3-Szene Glauben, verbreitet die Musikindustrie Dateien über P2P-Tauschbörsen, die ähnlich Viren andere Dateien auf den Rechnern der Tauschbörsennutzer löschen. Angeblich sollen diese Files gleichlautende Dateien auf der Festplatte zerstören.[1159]

Dass über Tauschbörsen auch Viren verbreitet werden, ist unbestritten; ob jedoch die Musikindustrie Urheber solcher Aktionen ist, wird wohl nie geklärt werden. Ihre Mitarbeiter innerhalb der Gruppe der „Script-Kiddies"[1160] und Hobby-Hacker zu identifizieren, dürfte beinahe unmöglich sein. Sicher ist nur, dass derartige Maßnahmen nach deutschem Recht im strafrechtlich relevanten Bereich anzusiedeln sind.[1161]

1154 Vgl. *Schmidt*, **c't** 23/1999, S. 20 f.
1155 Siehe Fn. 554.
1156 Vgl. **c't** 24/1999, S. 42 (*RealJukebox*) und **Heise Online News** vom 21.02.2002, http://www.heise.de/newsticker/meldung/25044 (*Mediaplayer* von *Windows XP*).
1157 **Heise Online News** vom 21.02.2002, http://www.heise.de/newsticker/meldung/25044.
1158 *Schmidt*, **c't** 23/1999, S. 21.
1159 Vgl. *Patalong*, **SPIEGEL Online** vom 26.07.2002.
1160 So werden - meist jugendliche - Internetnutzer bezeichnet, die mit Programmen und Skripten (Scripts) i.d.R. fremder Programmierer Schaden anrichten bzw. anzurichten versuchen; sie können nicht selbst programmieren, und ihnen fehlt regelmäßig das Verständnis für die grundlegenden technischen Zusammenhänge ihrer Aktivitäten.
1161 In Betracht kommen vor allem die Straftatbestände der §§ 202a und 303a StGB.

IV. Fazit / Eigener Ansatz

1. Zusammenfassung der effektivsten Maßnahmen

Das Entfernen nichtlizenzierter Musikfiles und der Angebote gewerbsmäßig handelnder Tonträgerpiraten von öffentlich zugänglichen WWW- und FTP-Seiten („Notice and Take Down Procedure") gehört zu den wichtigsten Maßnahmen, die von den Verbänden der Musikindustrie ergriffen werden. Versuche, von vornherein den Zugriff der Surfer auf unerwünschte Dateien technisch zu unterbinden, sind praktisch kaum zu realisieren, finden derzeit keine rechtliche Grundlage und sind bereits aus rechtspolitischen Erwägungen abzulehnen.[1162]

Um das Löschen der Zieldateien schnell zu erreichen, ist eine enge Zusammenarbeit mit den Webhosting-Providern über die Ländergrenzen hinweg erforderlich. Entsprechende Vereinbarungen zwischen Verbänden und Providern (Codes of Conduct) sind anzuraten.

Um dem Problem der Musiktauschbörsen zu begegnen, sollte die Musikindustrie legale Alternativen schaffen, anstatt der Verfolgung von Einzeltätern nachzugehen. Denn bei diesen handelt es sich fast ausnahmslos um musikbegeisterte Internetnutzer mit – wenn überhaupt – geringer krimineller Energie, deren Verfolgung eine weitergehende Schädigung des bereits angekratzten Images der Musikindustrie bewirken würde.

Zudem ist nicht zweifelsfrei erwiesen, dass die massenhafte Nutzung der P2P-Systeme zum Umsatzrückgang in der Musikbranche beigetragen hat. Daher gilt es vorrangig, die Nutzer der Tauschbörsen dazu zu bewegen, Geld für legale Angebote auszugeben. Dies kann auf zwei Wegen erreicht werden: Zum einen müssen die Preise für Audio-CDs entsprechend der Nachfragesituation gesenkt werden, zum anderen müssen legale Download-Angebote etabliert werden, die dem Nutzer die Flexibilität im Umgang mit digitaler Musik ermöglichen, die er vom MP3-Format gewohnt ist. Bei der Preisgestaltung ist zu berücksichtigen, dass der Kunde das Gefühl haben muss, ein vernünftiges Geschäft getätigt zu haben. Dies wird nur dann der Fall sein, wenn die legalen Angebote im Vergleich zu den freien Angeboten einen Mehrwert (z.B. durchgängig hohe Klangqualität, breites Angebot etc.) verkörpern.

2. Juristische Schlussfolgerungen

Das deutsche Recht bietet bereits jetzt genügend Möglichkeiten, um gegen jegliche Art von Online-Musikpiraterie vorzugehen. Mit der Novellierung des Urheberrechtsgesetzes werden voraussichtlich einige Klarstellungen vorgenommen, die zum Großteil die derzeit überwiegenden Auffassungen bestätigen.[1163]

Problematisch ist nach wie vor die Diskrepanz zwischen Rechtslage und Verfolgungspraxis bezüglich der Nutzung von Online-Musiktauschbörsen. Wie bereits dargelegt wurde, fällt der Download unter die sogenannte Privatkopie und ist somit straflos, während das – bei einigen Tauschbörsen zwangsläufige – Bereitstellen zum Download eine unerlaubte öffentliche Wiedergabe darstellt und gemäß § 106 UrhG strafbar ist. Da in Deutschland bislang keine strafrechtlichen Sanktionen gegen einzelne

---

1162 Siehe hierzu die Ausführungen zum Rights Protection System (RPS) der *IFPI*, Teil 3, C. II. 1. a).
1163 Siehe hierzu die Nachträge in Fn. 948 und 997.

Tauschbörsennutzer verhängt wurden[1164], und dies aufgrund der Vielzahl der Nutzer und des recht hohen Verfolgungsaufwands auch nicht in großem Umfang zu erwarten ist, wäre es aus kriminologischer und rechtspolitischer Sicht konsequent, die private Tauschbörsennutzung straflos zu stellen. Andernfalls führt das Missverhältnis zwischen Sanktionsdrohung und Sanktionspraxis dazu, dass die neu gefassten Strafnormen keine generalpräventiven Wirkungen entfalten können, und somit ein anerkannter Strafzweck entfällt.

Dass diese Konsequenzen mit der Novellierung des Urheberrechts nicht gezogen werden, steht bereits fest. Es bleibt bei der Strafdrohung für das unerlaubte öffentliche Zugänglichmachen von digitalen Musikstücken, eine Schranke – gekoppelt mit einem Kompensationsanspruch der Rechtsinhaber – ist nicht vorgesehen. Somit fehlt es bedauerlicherweise an der rechtlichen Grundlage für die Schaffung eines Vergütungsmodells für die Tauschbörsennutzung.

3. Weitere Schlussfolgerungen und Anregungen

Nicht nur bezüglich der Softwarepiraterie sondern auch bezüglich illegaler Downloadmöglichkeiten für Musikdateien ist ein verantwortungsvollerer Umgang mit entsprechenden Informationen von den Printmedien zu wünschen. Zwar wird mit der Novellierung des Urheberrechts unterbunden werden, dass Berichte über die Umgehung von Kopierschutzmaßnahmen von Audio-CDs veröffentlicht werden; Artikel, die sich mit der Nutzung von Tauschbörsen oder anderen Downloadquellen beschäftigen, werden jedoch weiterhin unter dem Hinweis auf die Zulässigkeit von Privatkopien erscheinen dürfen.

Informationsmanagement ist ebenfalls das Stichwort, das die Musikindustrie aufgreifen sollte, wenn es darum geht, eigene Download-Portale als Alternative zu den zahlreichen Online-Tauschbörsen zu etablieren. Da es gilt, sich von den nichtlizenzierten Angeboten abzuheben und einen Mehrwert zu versprechen, sollten die Anbieter der Bezahl-Angebote ihre Dienste geschickter bewerben, als es zur Zeit der Fall ist. Hierbei könnten sie unter anderem die folgenden Nachteile bzw. Makel der freien Angebote aufgreifen:

Die Tauschbörsennutzung ist bei allen P2P-Systemen mit gewissen Sicherheitsrisiken verbunden[1165]. Da jeder Nutzer Content in den Tausch-Pool einbringen kann, finden sich dort Unmengen von falsch benannten Dateien, die Viren, Würmer oder Trojaner enthalten.[1166] Unbedarfte Nutzer, die sich mit den entsprechenden Dateiendungen nicht auskennen oder keinen aktuellen Virus-Schild aktiviert haben, können nach dem Download solcher Dateien äußerst unangenehme Erfahrungen sammeln. Weitere Risiken ergeben sich aus der fehlerhaften Programmierung einiger Tausch-Clients. So sorgte unlängst eine Sicherheitslücke auf Port 1214 in den *FastTrack*-Clients für Aufregung, da sie

---

1164 Die Angaben beruhen auf einer Expertenbefragung des Verfassers am *Amtsgericht Frankfurt am Main* (Stand: 07/2002) und Recherchen in den Online-Archiven der deutschen Landesgruppe der *IFPI* und des Branchenportals *musikwoche.de*. Im Rahmen der Expertenbefragung wurden zwei Jugendstrafrichter und der für die Geschäftsverteilung der Frankfurter Strafgerichte zuständige Richter hinsichtlich entsprechender Strafprozesse sowie ein Oberstaatsanwalt und ein Mitarbeiter der Jugendgerichtshilfe Frankfurt am Main hinsichtlich entsprechender Ermittlungsverfahren (einschließlich eventueller Verfahrenseinstellungen gemäß §§ 153 ff. StPO) befragt.

1165 Allgemein zu den Risiken in P2P-Filesharing-Netzen siehe *Möller*, Sicherheit in Peer-to-Peer-Netzen, **Telepolis** vom 29.06.2001.

1166 Vgl. **Heise Online News** vom 19.05.2002, http://www.heise.de/newsticker/meldung/27489.

es jedermann ermöglichte, lokale Dateien auszulesen, ohne dass anderslautende Einstellungen in der Client-Software berücksichtigt wurden.[1167] Persönliche Daten von Tauschbörsennutzern sind auch regelmäßig durch sogenannte Adware oder Spyware in Gefahr. Hierbei handelt es sich um Programmmodule, die in einige P2P-Clients integriert sind und meist für wechselnde Werbeeinblendungen in die Benutzoberfläche des Clients oder in separate Pop-Up-Fenster sorgen. Häufig versenden diese Module persönliche Daten des jeweiligen Anwenders an fremde Server, wovon der betroffene Nutzer nichts mitbekommt.[1168]

Neben den dargestellten Sicherheitsrisiken haften den Tauschbörsen auch sittlich-moralische Makel an. Da sie seit jeher zum Tausch von (verbotener) Pornographie und rechtsradikalem Liedgut verwendet werden[1169], besteht bei den meisten Eltern sicher der dringende Wunsch, ihre Kinder von entsprechenden Angeboten fernzuhalten.

Zu den größten Nachteilen der freien Musiktauschbörsen gehört die inkonsistente Qualität der angebotenen Dateien, die Fülle an Fake-Files sowie die mangelnde Verfügbarkeit älterer Werke oder der Werke weniger bekannter Künstler. Sofern die legalen Angebote diese Nachfragelücken ausfüllen, sollten nicht versäumt werden, explizit darauf hinzuweisen.

Um dem Kundenwunsch weiter entgegenzukommen, sollte in Erwägung gezogen werden, Dateien anzubieten, die nicht nur annähernde CD-Qualität bieten. Geeignet wären hierzu Bitraten oberhalb von 128 KBit/s (192, 256 oder 320 KBit/s).

Da die Plattenfirmen in der Regel auch die Rechte an Bildmaterial und Künstlerinformationen besitzen, wäre es unproblematisch, den Kunden entsprechende Dateien als Bonus zur Verfügung zu stellen.

Insgesamt gilt es, dem Kunden ein ruhiges Gewissen zu vermitteln, wenn er die legalen Downloadangebote nutzt („Peace of Mind“). Hierzu könnte neben Hinweisen darauf, dass die Künstler direkt von den Bezahl-Downloads profitieren, gezielte Aufklärung über die rechtliche Situation beitragen.

Falls sich ein Unternehmen scheuen sollte, die Werke seiner Künstler gänzlich ungeschützt zum Download anzubieten, besteht die Möglichkeit, in die zu übertragende Datei eine individuelle Signatur einzufügen, die Rückschlüsse auf den Kunden zulässt. Beim Kauf müsste sich der Anbieter die datenschutzrechtliche Zustimmung des Kunden einholen und Letzterer könnte sich zu einer pauschalen Vertragsstrafe (z.B. 100 €) für den Fall verpflichten, dass sich das File in einer Tauschbörse oder auf einer öffentlich zugänglichen Internetseite wiederfindet. Das Einbringen der Signatur ließe sich so gestalten, dass sie jede digitale Weitergabe überdauert, jedoch beim analogen Kopieren oder Brennen auf eine Audio-CD verloren geht. Auf diese Weise würde ein unkalkulierbares Risiko für den Verbraucher eliminiert, falls er beispielsweise eine CD an Freunde verleiht. Da diese Gestal-

---

1167 **Heise Online News** vom 04.02.2002, http://www.heise.de/newsticker/meldung/24550.
1168 Vgl. **Heise Online News** vom 03.01.2002, http://www.heise.de/newsticker/meldung/23733 für Spyware in den Filesharing-Clients *Grokster* und *LimeWire*.
1169 **Heise Online News** vom 10.01.2001, http://www.heise.de/newsticker/meldung/14387; **Heise Online News** vom 19.12.2000, http://www.heise.de/newsticker/meldung/13994.

tung wesentlich weniger aufwändig ist als das Einweben eines Wasserzeichens und zudem keine Lizenz des Wasserzeichen-Entwicklers benötigt, ist sie auch aus wirtschaftlichen Gründen attraktiv.

Letztlich geht es darum, einen fairen Handel abzuwickeln, bei dem sich beide Parteien bewusst sind, worauf sie sich einlassen. Der Kunde erhält zu einem vernünftigen Preis maximale Flexibilität im Umgang mit der von ihm erworbenen Musik und weiß auf der anderen Seite genau, dass er sie nicht über das Internet bereitstellen oder in ihrer ursprünglichen Form weitergeben darf.

Parallel zur Schaffung legaler Download-Angebote sollte die Musikindustrie weitere alternative Einnahmequellen ausschöpfen, die sich durch die massenhafte Internetnutzung von Musikliebhabern auftun. Zu denken ist unter anderem an sogenannte Subscription Sites, auf denen gegen Zahlung einer monatlichen oder jährlichen Gebühr exklusive Inhalte (z.B. Musikvideos oder Remixe) für Fans angeboten werden, oder an die Einrichtung von Online-Shops für den Verkauf von Merchandising-Artikeln. Sämtliche Online-Angebote können – sofern sie rege frequentiert werden – durch die Einbindung von Werbebannern zusätzlichen Profit generieren.

Gesamtfazit

Sich ständig verändernde Situationen erfordern ein fortwährendes Anpassen der rechtlichen und wirtschaftlichen Strategien. Dazu bedarf es in erster Linie einer genauen Analyse von Under- und Overground der „Piratenszene" sowie des Verständnisses der technischen Grundlagen der Internetkommunikation. Die vorliegende Arbeit zeigt exemplarisch, wie vielschichtig die illegale Reproduktion und Distribution von urheberrechtlich geschützten Werken erfolgt. Dementsprechend gibt es auch kein universelles Rezept gegen das Problem der „Cyberpiraterie", sondern eine Vielzahl von Ansatzpunkten[1170].

Letztlich wird sich nie vollständig verhindern lassen, dass nichtlizenzierte Werke per Internet den Besitzer wechseln. Solange die Nutzer E-Mails mit Attachments versenden und empfangen können, werden sie unbemerkt illegale Inhalte austauschen. Das gilt vor allem für die Zukunft, in der die Anbindungen an das Netz für jedermann noch schneller und komfortabler werden.

In diesem Zusammenhang muss man sich stets vor Augen halten, dass Reproduktion und Verbreitung zu den wesentlichen Eigenschaften von (digitaler) Information gehören.[1171] Eine freie Informationsgesellschaft ohne Risiken wird es niemals geben. Dies verlangt nach einer Balance zwischen Totalüberwachung und Untätigkeit (Stichwort: Risikominimierung), die sich stets an den rechtsstaatlichen Grundprinzipien orientieren muss.

Bis Kopierschutzmechanismen in der Lage sind, das Erstellen von Kopien wirksam zu verhindern, werden aller Voraussicht nach noch einige Jahre vergehen. Derzeit ist bei fast allen verwendeten Kopierschutzverfahren eine Umgehung möglich, selbst die jüngsten Systeme zur digitalen Rechteverwaltung (DRM-Systeme) weisen noch zahlreiche Schwachstellen auf. Besonders schwierig gestaltet sich der technische Schutz von audiovisuell wahrnehmbaren Werken, da sie unverschlüsselt konsumiert werden müssen („Auge und Ohr bleiben analog"). Selbst wenn es – womöglich durch den Einsatz starker Kryptographie – gelingen sollte, digitale Kopien dieser Werkarten zu verhindern, ist davon auszugehen, dass weiterhin analoge Kopien angefertigt und in „re-digitalisierter" Form über das Internet verbreitet werden.

Moderne Auguren der Informationsgesellschaft prophezeien seit einigen Jahren einschneidende und nachhaltige Veränderungen für den Umgang mit geistigem Eigentum. So stellte *Nicholas Negroponte*, Professor am *MIT*[1172] *Media Lab*, 1995 die These auf, dass das Urheberrecht vom Erdboden verschwinden werde, noch ehe es die digitale Realität überhaupt zur Kenntnis habe nehmen können.[1173] Auch *John Perry Barlow*, Mitbegründer der *Electronic Frontier Foundation (EFF)*[1174], zog

---

1170 Siehe oben Teil 2, C. V. und Teil 3, C. IV.
1171 So auch *Barlow*, **Wired Magazine** 2.03 – März 1994, der folgendes Beispiel gebraucht: „Der Versuch, die Verbreitung einer substantiellen Information zu verhindern, kommt dem Versuch gleich, einen Schwarm Killerbienen vom Überschreiten einer Landesgrenze abzuhalten" (übersetzt aus dem Englischen).
1172 *Massachusetts Institute Of Technology* (Boston).
1173 *Negroponte*, S. 58 - „copyright law is totally out of date"; übersetzt aus dem Englischen von *Dreier*, Urheberrecht an der Schwelle des 3. Jahrtausends, **CR** 2000, S. 45.
1174 http://www.eff.org.

frühzeitig einen Kollaps des heutigen Urheberrechtssystems, wie wir es in der westlichen Welt seit *Gutenberg* kennen, in Betracht.[1175]

Die Frage, ob sich die digitale Realität durch das Internet bereits so stark verändert hat, dass unser Urheberrecht ausgedient hat, ist jedoch zu verneinen.[1176] Zwar bekommt die Content-Industrie spätestens seit *Napster* täglich zu spüren, was es bedeutet, die Kontrolle über digitale Informationen zu verlieren, die Zeit, das Feld kampflos den „modernen Freibeutern" zu überlassen, ist jedoch noch nicht gekommen.

Vielmehr geht es darum, das bestehende Recht an die digitale Realität anzupassen. Hier muss der Wahlspruch der Verwertungsgesellschaften gelten: „Das Schützbare schützen, das Nicht-Schützbare vergüten"[1177].

Da zum jetzigen Zeitpunkt keinerlei Einigkeit darüber besteht, welche Inhalte in welchem Medium schützbar sind, ignorieren die Vertreter der Content-Industrie die eigene Dynamik des Internet und erklären alle digitalen Werke für schützbar. Obwohl sich ein solcher Schutz bislang kaum realisieren ließ, halten die Rechtsinhaber an der Pönalisierung der Dateitauscher fest, anstatt alternative Vergütungsmodelle in Erwägung zu ziehen.

Die vorliegende Arbeit hat an mehreren Punkten gezeigt, dass ein wesentlicher Teil der bestehenden und bevorstehenden urheberrechtlichen Regelungen die digitale Realität nur unzureichend berücksichtigt. So sind Gründe für eine urheberstrafrechtliche Ungleichbehandlung von Computerprogrammen und anderen Werken nicht mehr ersichtlich. Heutzutage liegen alle Arten von Werken digital vor und sind in gleichem Maße Piraterie bzw. privatem Kopieren ausgesetzt[1178], so dass konsequenterweise auch Computerprogramme in den Anwendungsbereich von § 53 UrhG einbezogen werden müssten, sofern ein entsprechendes Vergütungsmodell zugunsten der betroffenen Rechtsinhaber entwickelt würde. Ebenso konsequent wäre es, die digitale Privatkopie aller Werkarten zu verbieten, was allerdings aus generalpräventiver Sicht nur dann Wirkung zeigen kann, wenn der Sanktionsdrohung eine Sanktionspraxis gegenübersteht, die zu einer Abschreckung potentieller Rechtsbrecher geeignet ist. Da eine entsprechende Verfolgungspraxis bereits aus Kapazitätsgründen nicht zu realisieren ist, erscheint ein generelles Verbot der Privatkopie aus kriminologischer Sicht wenig erfolgversprechend.[1179]

Hinzu kommen verfassungsrechtliche Bedenken: Die Zulässigkeit der Privatkopie muss vor dem Hintergrund der Art. 2, 5 Abs. 1 und 14 Abs. 2 GG betrachtet werden. Als (geistiges) Eigentum

---

1175 *Barlow*, **Wired Magazine** 2.03 – März 1994. *Barlow* spricht sich unter anderem für technische Schutzmaßnahmen anstelle von rechtlichen Schutzmaßnahmen aus.
1176 So auch *Grzeszick*, **MMR** 2000, S. 417 und *Dreier*, Urheberrecht an der Schwelle des 3. Jahrtausends, **CR** 2000, S. 45.
1177 Vgl. die Stellungnahme des „Forums der Rechteinhaber" zur Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (siehe Fn. 434), veröffentlicht auf der Webseite der *GEMA*, http://www.gema.de/kommunikation/pressemitteilungen/eu_info_richtlinie_pm.shtml.
1178 In den großen Online-Tauschnetzwerken finden sich neben Musikstücken und Filmen auch zahlreiche Computerprogramme.
1179 Oder um es mit *Kohler*, S. 171, zu sagen: Ein vollkommen unbeschränktes Urheberrecht würde „die menschlichen Verhältnisse knechten und die Freiheit der Persönlichkeit zerstören"; uneingeschränkter Urheberschutz stünde mit dem Satz im Widerspruch, dass „Gedanken zollfrei sind und niemals bestraft werden können"; vgl. auch *Flechsig*, **GRUR** 1993, S. 532.

unterliegt auch das Urheberrecht der Sozialbindung gem. Art. 14 Abs. 2 GG[1180], so dass es Aufgabe des Gesetzgebers ist, im Interesse der Allgemeinheit am unkomplizierten Zugang zu vorhandenen Informationen und Dokumentationen die – zwar nicht unbedingt vergütungsfreie, jedoch zumindest – erlaubnisfreie Vervielfältigung im privaten Bereich zu gewährleisten.[1181] Die Schranke des § 53 UrhG ist somit nicht nur als grundlegende Voraussetzung für die ungehinderte Ausbreitung kultureller Errungenschaften und Identifikationsfaktoren, sondern auch als Garantie für einen freien Informationsfluss in der modernen Wissensgesellschaft anzusehen.

Die digitale Realität schafft ihre eigenen Fakten: Jeden Tag vervielfältigen und tauschen Millionen von Nutzern Abermillionen urheberrechtlich geschützter Dateien, ohne dass die Rechtsinhaber irgendeine geldwerte Kompensation dafür erhalten. Die größte Herausforderung für den Gesetzgeber ist in diesem Zusammenhang, dem Problem der Online-Tauschbörsen in angemessener Weise zu begegnen. Selbst wenn sich bislang nicht mit Sicherheit nachweisen ließ, dass die Nutzung von P2P-Systemen den Umsatz von Unternehmen der Content- und Softwareindustrie negativ beeinträchtigt[1182], ist davon auszugehen, dass den Rechtsinhabern digitaler Werke Tantiemen entgehen, weshalb ein Einschreiten des Staates geboten ist. Dies ergibt sich vor allem aus der in Art. 14 Abs. 1 S. 1 GG normierten Eigentumsgarantie, die auch das geistige Eigentum – und damit Urheber- und Leistungsschutzrechte – umfasst[1183]. Hierbei muss eine schwierige Gratwanderung zwischen strafrechtlicher Sanktionsdrohung und der Gestattung angemessener erlaubnisfreier Benutzung urheberrechtlich geschützter Werke unternommen werden.

Die momentane Strategie des Gesetzgebers zielt darauf ab, des freien Tauschs mittels strafrechtlicher und zivilrechlichter Sanktionen Herr zu werden. Ob die Rechtsinhaber mit Sanktionen, digitaler Rechteverwaltung (DRM) und Verschlüsselung die Kontrolle über ihre Werke zurückerlangen können, oder ob die „anarchische Parallelwelt“ neben dem „neuen und sicheren Marktplatz“ bestehen bleibt, ist abzuwarten.

Eine breite Öffentlichkeit so umzuerziehen, dass beispielsweise das Herunterladen einzelner Musiktitel als verwerflich empfunden wird, ist ein sehr langwieriger Prozess und dürfte nur bezüglich eines Teils der Bevölkerung möglich sein. Denn zu den tragenden Charakteristika der sogenannten Netzkultur, wie sie heute existiert, gehört das (kosten-)freie Beziehen von Informationen aller Art. Eine Anerkennung entgegenstehender Normen sowie die Einübung von Normvertrauen und Rechtstreue scheinen nur dann erreichbar, wenn die bereits erwähnte Diskrepanz zwischen Sanktionsdrohung und Sanktionspraxis deutlich verringert würde. Dies ist jedoch angesichts geschätzter Nutzerzahlen von mehreren Millionen – allein 70 Millionen Menschen sollen Mitte 2002 in den USA Tauschbörsen genutzt haben[1184] – nicht in absehbarer Zeit zu erwarten. Denn zum einen ist eine konsequente strafrechtliche Verfolgung aufgrund mangelnder Ressourcen so gut wie ausgeschlossen,

---

1180 Siehe oben Fn. 940.
1181 Vgl. das Urteil des *BGH* vom 16.01.1997 (Az. I ZR 9/95 – „CB-Infobank I“), **BGHZ** 134, S. 250, 263; Beschluss des *BVerfG* vom 07.07.1971 (Az. 1 BvR 765/66), **BVerfGE** 31, S. 229, 242; Amtl. Begr. **BT-Drucks.** 10/837, S. 9
1182 Dies mag vor allem daran liegen, dass nur wenige interessenungebundene Gutachten zu diesem Sachverhalt erstellt wurden.
1183 Siehe Fn. 938.
1184 **Heise Online News** vom 21.08.2002, http://www.heise.de/newsticker/meldung/30132.

zum anderen würde sie dazu führen, dass Millionen grundsätzlich rechtstreuer Bürger kriminalisiert würden.

Gelingt es daher nicht, dem Problem mittels strafrechtlicher Drohung und Verfolgung zu begegnen, müssen alternative Wege gesucht werden, die auf eine Vergütung der betroffenen Rechtsinhaber hinauslaufen.[1185]

Denkbar wäre die Schaffung eines Gesetzes, das die Hersteller bzw. Distributoren von Tauschbörsensoftware zur Kooperation bei der Errichtung eines Vergütungsmodells verpflichtet, weil offenkundig ist, dass ihre Software zur massenhaften unerlaubten Verwertung von urheberrechtlich geschützten Werken eingesetzt wird.[1186]

Das Vergütungsmodell selbst würde auf der Idee basieren, Tauschbörsennutzern gegen Zahlung einer monatlichen Pauschale legalen Zugang zu einem P2P-Netz zu ermöglichen.[1187] Einzelne Tauschvorgänge zu Abrechnungszwecken zu erfassen, widerspräche dem Wesen des Online-Tausches, bei dem jeder Nutzer nur das bereitstellt, was ihm beliebt, und bei dem sich Leistung und Gegenleistung gerade nicht in einem angemessenen Verhältnis befinden müssen. Zudem wäre das Erfassen einzelner Tauschvorgänge unter datenschutzrechtlichen Aspekten bedenklich, denn die Erhebung und Zuordnung der entsprechenden Daten würde gemäß § 3 TDDSG die Einwilligung des betroffenen Nutzers voraussetzen. Ob diese in Anbetracht des Umstandes, dass die Zuordnung von Inhaltsdaten (getauschte Dateien) und Bestandsdaten (Daten zur Identität des Nutzers) ein Quasi-Nutzungsprofil bildet, ohne weiteres erteilt würde, steht zu bezweifeln. Denn die – zum Teil intimen – Daten befänden sich möglicherweise in den Händen privatwirtschaftlicher Unternehmen, was berechtigte Sorgen bezüglich der sich daraus ergebenden Missbrauchsmöglichkeiten begründen würde. Es ist somit davon auszugehen, dass sich der überwiegende Teil der Nutzer anonymisierte Tauschvorgänge wünscht, was überdies dem gesetzlichen Gebot des § 4 Abs. 6 TDDSG entspräche.

Um zu gewährleisten, dass eine gerechte Ausschüttung an die Rechtsinhaber erfolgt, müsste ein zentraler Server eine Liste mit den Dateien erstellen, die erfolgreich getauscht wurden.[1188] Ein großer

---

[1185] In weiser Voraussicht hat der Gesetzgeber bereits in den 60er Jahren den Weg der gesetzlichen Lizenz (i.V.m. einer korrespondierenden Vergütungsregelung) gewählt, siehe oben Teil 3, C. I. 1. Er hatte erkannt, dass ein Verbot der privaten Vervielfältigung praktisch nicht durchsetzbar ist. Diese Erkenntnis hat ihre Gültigkeit im digitalen Zeitalter nicht verloren, sie hat sogar an Bedeutung gewonnen.

[1186] Selbst wenn sich zunehmend legale und preisgünstige Download-Alternativen zu den P2P-Netzwerken etablieren sollten, ist nicht davon auszugehen, dass sich die Nutzerzahlen der letztgenannten dramatisch verringern werden. Denn ein großer Teil der Nutzer schätzt den „anarchischen, spielwiesenartigen Charakter" von Tauschbörsen. Zu nennen sind vor allem das unvergleichlich breite Angebot an unterschiedlichen Medientypen (die zudem nicht redaktionell selektiert oder zensiert werden) sowie die pragmatische Erwägung, dass man sich nicht bei verschiedenen Download-Portalen registrieren muss, um unterschiedliche Arten von Werken zu nutzen.

[1187] Ein ähnliches Abonnement-Modell wurde zur Zeit des *Napster*-Prozesses diskutiert, konnte aber nie etabliert werden, da sich die betroffenen Rechtsinhaber nicht einig wurden. So hat man es über Jahre versäumt, an der Nutzung von *Napster* mitzuverdienen. Zwar wurde per Gerichtsbeschluss erreicht, dass der Dienst eingestellt wurde, aber die zahlreichen – zum Teil schwerer zu bekämpfenden – Nachfolger *Napsters* sind immer noch aktiv. Rechtlich ließe sich das Modell über die Einräumung gesetzlicher Lizenzen zur Vervielfältigung zum privaten Gebrauch und zur öffentlichen Zugänglichmachung im Rahmen von P2P-Netzwerken gestalten.

[1188] Hierzu ist erforderlich, dass die bei den Nutzern aktiven P2P-Clients bei jedem komplettierten Download eine (anonymisierte) Mitteilung, die auch den unverwechselbaren Hashwert (siehe oben Teil 3, C. II. 1. c) und Fn. 861) der jeweiligen Datei enthält, an den Erfassungs-Server senden. Um zu verhindern, dass zugunsten einzelner Rechtsinhaber gefälschte Komplettierungsmitteilungen gesendet werden, sind kryptographische Authentifizierungsverfahren zu erwägen.

Vorteil dieses Modells bestünde zum einen darin, dass im Vorfeld der Verteilung nicht mehr der vielfach als ungerecht empfundene *GEMA*-Verteilungsschlüssel herangezogen werden müsste, sondern erstmalig an einzelne Vervielfältigungsvorgänge im privaten Bereich angeknüpft werden könnte.[1189] Zum anderen kämen erstmals auch Softwarehersteller in den Genuss von Vergütungen für nichtlizenziertes Kopieren ihrer Produkte.

Falsch benannte Dateien ließen sich mittels entsprechender Datenbanken leicht identifizieren. Die notwendigen Änderungen in der Client-Software könnten mit der Verbreitung einer neuen Programmversion eingeführt werden. Parallel müsste darauf hingewiesen werden, dass das vorhandene Tauschnetzwerk nur noch mit den aktuellen Clients legal nutzbar ist. In Betracht kommt in einer möglichen zweiten Migrationsstufe die Änderung des verwendeten Netzwerkprotokolls oder der Ports, was zu einer technischen Inkompatibilität der alten und neuen Clients führen würde.

Damit das legale Angebot nicht nur von rechtstreuen bzw. normanerkennenden Bürgern Zulauf erhält, ist es ratsam, gegen Nutzer ohne Zugangsberechtigung oder Nutzer anderer („nichtvergütender") Tauschbörsen rechtlich vorzugehen. Hierbei sollte in erster Linie gezielt gegen private Serverbetreiber vorgegangen werden, die mit ihren Rechnern aktiv zum Erhalt serverbasierter Tauschnetzwerke - wie z.B. *OpenNap* - beitragen. In serverlosen Tauschnetzwerken sollten sich die rechtlichen Maßnahmen gegen „notorische Vieltauscher" richten, d.h. gegen solche Personen, die permanent große Datenmengen in Tauschbörsen bereitstellen.

Entsprechende Maßnahmen wären nicht zuletzt unter dem Gesichtspunkt positiver Generalprävention unbedingt publik zu machen. Die Gesamtheit der Tauschbörsennutzer müsste darüber informiert werden, dass man sich gegen Entrichtung der Vergütungspauschale ein ruhiges Gewissen („Peace of Mind") kaufen kann und dass es einen rechtlichen Unterschied macht, ob man mit oder ohne Zugangsberechtigung in Tauschnetzwerken aktiv ist.

Anbieter von P2P-Software, die nicht bereit sind, das von ihnen geförderte Tauschnetz dem Vergütungsmodell zu unterwerfen, müssten damit rechnen, dass die Nutzer ihrer Software weiterhin straf- und zivilrechtlicher Verfolgung ausgesetzt sind und dass die eigene Verweigerungshaltung rechtliche Konsequenzen haben kann. Eine entsprechende Grundlage für die haftungsrechtliche Inanspruchnahme der Anbieter könnte in dem zu schaffenden Gesetz verankert werden. Ausgelöst würde die Haftung bereits dann, wenn beobachtet wird, dass mit Hilfe der angebotenen Software ein Tauschnetzwerk erweitert wird und urheberrechtlich geschützte Daten ohne Einverständnis der Rechtsinhaber getauscht werden[1190].

[1189] Um an der Ausschüttung teilzunehmen, müssten sich die Rechtsinhaber bei einer Verwertungsgesellschaft anmelden und dort die Werke (mitsamt den entsprechenden Hashwerten der jeweiligen P2P-Netze) angeben, für die sie Rechtsinhaberschaft beanspruchen bzw. belegen können.

[1190] Übergangsweise bzw. alternativ zu dem hier skizzierten Vorschlag ist ein stark vereinfachtes Modell („reines Peace-of-Mind-Modell") denkbar, bei dem auf eine vergütungsrelevante Anknüpfung an einzelne Tauschvorgänge verzichtet wird. Jedem potentiellen Tauschbörsennutzer müsste gegen Zahlung einer monatlichen Vergütungspauschale gestattet werden, P2P-Netzwerke aktiv und passiv zu nutzen. Kann ein Nutzer im Rahmen einer Stichprobe nachweisen, dass er die Vergütung entrichtet hat, wird von einer zivil– und strafrechtlichen Verfolgung abgesehen. Nutzer, die zum Zeitpunkt der Ermittlung ohne Erlaubnis am Onlinetausch teilgenommen haben, müssen dagegen mit rechtlichen Sanktionen rechnen. Zur Ausschüttung der eingenommenen Gelder müssten u.a. die bislang verwendeten Verteilungsschlüssel herangezogen werden; um die Verteilung so gerecht wie möglich zu gestalten, bietet sich zusätzlich eine regelmäßige Analyse der Angebotsstruktur in P2P-Netzwerken an.

In der vom Verfasser als geboten erachteten Errichtung eines Vergütungsmodells für Tauschbörsennutzung ist kein Freibrief für Raubkopierer oder eine Bankrotterklärung des Urheberrechtssystems zu erblicken, sondern der möglicherweise einzige Weg, geldwerte Kompensation für die Verwertung urheberrechtlicher Werke in den großen P2P-Netzwerken zu erlangen. Sollte es wider Erwarten nicht gelingen, mit dem entworfenen Konzept Geld an der Tauschbörsennutzung zu verdienen, bleiben noch immer zivilrechtliche Sanktionen und die „Keule des Strafrechts" als ultima ratio gegen die Nutzer von P2P-Systemen.

Es ist jedoch Eile geboten, denn mit wachsendem Verfolgungsdruck auf einzelne Tauschbörsennutzer besteht die Gefahr, dass sich zunehmend P2P-Systeme etablieren, in denen die Nutzer bzw. die getauschten Inhalte nicht mehr ohne Weiteres zu identifizieren sind.

Unabhängig davon, was die zukünftigen Gesetze zum Schutz von Urheberrechten vorsehen, ist es unabdingbar, dass sie weltweit gelten und dass die befassten Behörden supranational zusammenarbeiten[1191]. Nur so kann der Grenzenlosigkeit des „Cyberspace" Rechnung getragen werden. Inhaltlich wäre wünschenswert, dass die Regelungen klar zwischen kommerziellen Interessen und privatem bzw. persönlichem Vergnügen der Nutzer geschützter Werke differenzieren, wobei nur ein Handeln vor kommerziellem Hintergrund und das öffentliche Anbieten durch Privatpersonen strafrechtlich relevant sein sollte[1192]. Eine weitergehende strafrechtliche Verantwortlichkeit ist bereits aus den zum Thema Privatkopie dargelegten Gründen abzulehnen; der Strafzweck entsprechender Normen erscheint vor allem im Hinblick auf die unüberbrückbare Diskrepanz zwischen Sanktionsdrohung und Sanktionspraxis zweifelhaft. Angesichts der unüberschaubaren Zahl der privaten Dateitauscher und der vergleichsweise verschwindend geringen Strafverfolgungsressourcen sind keine negativ-generalpräventiven Wirkungen zu erwarten. Ob es langfristig gelingt, positiv-generalpräventive Wirkungen zu erzielen, also Normanerkennung und Rechtstreue einzuüben, hängt entscheidend davon ab, ob den Nutzern legale Download- bzw. Tauschmöglichkeiten geboten werden, die von diesen als wirkliche Alternativen akzeptiert werden.[1193]

Das Urheberrecht selbst darf aus zweierlei Gründen nicht in Frage gestellt werden: Zum einen schützt es den Schöpfer eines Werkes der Literatur, Wissenschaft oder Kunst vor der Verletzung eigener ideeller Interessen an seinem Werk[1194], indem es ihm persönlichkeitsrechtliche Befugnisse einräumt[1195]. Es handelt sich um höchstpersönliche, unveräußerliche Rechte von Menschen (Urheberpersönlichkeitsrechte), die die geistigen und persönlichen Beziehungen des Urhebers zu seinem Werk vor Beeinträchtigungen Dritter bewahren. Vor allem in Zeiten zunehmend unkontrollierbarer Distribution von urheberrechtlich geschützten Werken und einer aufkeimenden

---

1191 Vgl. *Sieber*, Missbrauch der Informationstechnik, Teil 3, IV.; siehe hierzu oben - Teil 2, C. III. 5. c) - die Beschreibung eines vorzugswürdigen Modells internationaler behördlicher Zusammenarbeit (G8-Arbeitsgruppe *High-Tech Crime*).
1192 Unter dem öffentlichen Anbieten durch Privatpersonen ist das Anbieten außerhalb „legalisierter" Tauschnetzwerke zu verstehen, sei es im WWW oder in anderen Diensten des Internet.
1193 Siehe hierzu die Anregungen unter Teil 3, C. IV. 3.
1194 Vgl. **BT-Drucks.** 10/837, S. 9.
1195 Vgl. §§ 12-14 UrhG. Beispielhaft ist § 13 UrhG zu nennen, wonach der Urheber u.a. das unveräußerliche Recht auf Anerkennung seiner Urheberschaft am Werk hat.

Aufmerksamkeits-Ökonomie[1196] wird deutlich, wie wichtig der Erhalt der persönlichkeitsrechtlichen Komponente des Urheberschutzes ist.

Des Weiteren behält das Urheberrecht dem Urheber die wirtschaftliche Verwertung seines Werkes vor und wahrt somit dessen unmittelbare Vermögensinteressen. Der Lohn für die schöpferische Tätigkeit ist ein wichtiger „Motor" für die Schöpfer aller Werkarten. Leistung muss sich weiterhin lohnen – auch im kreativ-kulturellen Bereich.

In einer Rede vor dem US-Kongress im Sommer 2000 sprach der *Disney*-Geschäftsführer *Michael Eisner* aus, was viele Vertreter der Content-Industrie so nervös macht: „So wie Computer in der Lage sind, Bilder von wundervoller Qualität zu erzeugen, sind sie auch in der Lage, Kopien von wundervoller Qualität zu erzeugen".[1197] Das Gesagte mag paradox erscheinen, aber die Personal-Computer von heute sind bekanntermaßen Allround-Maschinen, deren Fähigkeiten stetig wachsen. Ob es in absehbarer Zeit gelingt, den Konsumenten Geräte zu verkaufen, die in ihrem Funktionsumfang beschränkt und noch dazu mit DRM-Hardware ausgestattet sind[1198], steht zu bezweifeln.

Dennoch ist nicht zwingend davon auszugehen, dass die Content-Industrie dem Problem auf lange Sicht schutzlos gegenüberstehen wird. Die Entwicklung von Thin Clients, Online-Dongles, Web-Shops oder starker Verschlüsselung zeigt beispielhaft, dass die Möglichkeiten der Computertechnik in Verbindung mit dem Internet dazu beitragen können, dem Missbrauch erfolgreich zu begegnen.

1196 Siehe Fn. 205.
1197 Bei *Godwin*, Cryptome.org (übersetzt aus dem Englischen).
1198 Vgl. die Ausführungen unter Teil 3, C. II. 3.