



Lars Rau (Autor)

Phänomenologie und Bekämpfung von 'Cyberpiraterie' Eine kriminologische und kriminalpolitische Analyse

Lars Rau

Phänomenologie und Bekämpfung von 'Cyberpiraterie'

Eine kriminologische und kriminalpolitische Analyse



Cuvillier Verlag Göttingen

<https://cuvillier.de/de/shop/publications/2799>

Copyright:

Cuvillier Verlag, Inhaberin Annette Jentsch-Cuvillier, Nonnenstieg 8, 37075 Göttingen,
Germany

Telefon: +49 (0)551 54724-0, E-Mail: info@cuvillier.de, Website: <https://cuvillier.de>

Inhaltsverzeichnis

Seitenzahl

Literaturverzeichnis.....	IX
Abkürzungsverzeichnis.....	XXXIII
Teil 1 - Einführung	001
A. Bedeutung und Einordnung des Forschungsgegenstands.....	001
B. Die Geschichte des Internet.....	002
C. Die technischen und organisatorischen Grundlagen des Internet.....	004
I. Die Datenübertragung im Internet.....	004
1. Die Netzstruktur.....	004
2. Die Regeln der Datenübertragung – TCP/IP als wichtigstes Protokoll.....	005
3. Das Domain Name System (DNS).....	007
II. Zugang des privaten Nutzers zum Internet.....	009
D. Die wichtigsten Bereiche / Dienste des Internet.....	011
I. World Wide Web (WWW).....	011
II. E-Mail.....	015
III. File Transfer Protocol (FTP).....	016
IV. Newsgroups / UseNet.....	018
V. Internet Relay Chat (IRC).....	021
VI. Instant Messaging (am Beispiel von <i>ICQ</i>).....	025
E. Überblick über die verschiedenen Daten, die Gegenstand von strafbaren Handlungen i.S.d. §§ 106 ff. UrhG sind.....	026
I. Software.....	026
II. Musik in CD-Qualität.....	026
III. Kinofilme / Videofilme.....	026
IV. (Licht-)Bilder.....	027
V. Schriftwerke.....	027
VI. Fonts.....	028
VII. Ton- bzw. Klangdateien („Sounds“ oder „Samples“.....)	028
VIII. Kompositionen.....	028
IX. Sonstige Daten mit Werkcharakter.....	028
F. Methodik.....	029
I. Dokumenten-Inhaltsanalyse.....	029
II. Distanzierte, verdeckte Beobachtung.....	030
III. Befragungen.....	030

Teil 2 - Internet-Softwarepiraterie	031
A. Beschreibung und Struktur der sogenannten Warez-Szene.....	031
I. Welche Software wird über das Internet verbreitet?.....	031
Exkurs – Software und Lizenzmodelle:	031
Kostenpflichtige Software	031
Shareware	032
Freeware	032
Public Domain Software.....	033
II. Historische Betrachtung.....	033
III. Tätigkeit von Warez-Gruppen.....	035
IV. Die Mitglieder der Gruppen / Arbeitsteilung innerhalb der Gruppen.....	036
1. Supplier.....	036
2. Cracker.....	037
Exkurs – Der Begriff des Hackers:	037
a) Haupttätigkeit des Crackers	038
b) Verschiedene Arten des Kopierschutzes und ihre Umgehung.....	039
(1) Seriennummern.....	039
(2) RegistrierungsCodes („RegCodes“ oder „Keys“)	039
(3) Trial-Versionen mit zeitlicher Nutzungsbeschränkung	041
(4) Trial-Versionen mit Einschränkung der Funktionen	041
(5) CD-Abfragen.....	041
(6) Dongles („Hardware Locks“ oder „Keys“)	043
(7) Online-Registrierung und Online-Updates.....	045
(8) Mischformen (z.B. „Online-Dongles“)	046
(9) Hardwaregestützte Software	047
c) Weitere Tätigkeiten des Crackers	047
(1) Debugging.....	047
(2) Implementieren von neuen Programmoptionen (Features).....	048
(3) Schreiben von Cracking-Programmen, Tutorials und “Crackmes”	049
3. (Beta-)Tester	051
4. Packager.....	051
5. Leader	053
6. Kuriere.....	055
7. Serveradministratoren (Siteops).....	056
8. Coder.....	057
V. Szenemitglieder ohne Gruppenzugehörigkeit	059
1. Leecher	059

2. Trader.....	059
3. Profit-Pirates (Warez-Sellers)	059
4. Betreiber von Release-Info-Seiten („Dupecheck-Sites“)	061
VI. Kommunikationswege der Warez-Szene.....	062
1. IRC.....	062
2. Instant Messaging Systeme	062
3. E-Mail	062
4. UseNet.....	063
5. WWW	063
VII. Wege der illegalen Softwaredistribution.....	065
1. WWW	065
2. FTP.....	068
3. UseNet.....	069
4. IRC	070
5. E-Mail	070
6. Instant Messaging Systeme	071
7. Peer-to-Peer-Filesharing-Systeme (P2P-Systeme).....	071
VIII. Phänomenologische Betrachtung der Warez-Szene	071
1. Subkulturelle Besonderheiten.....	071
2. Täterkreis.....	076
3. Tätermotivation.....	079
B. Bedeutung und Schaden.....	085
I. Angaben über Fälle von (Internet-)Softwarepiraterie und über den Schaden	085
1. Angaben der <i>Business Software Alliance (BSA)</i>	085
2. Angaben der <i>Software Publishers Association (SPA)</i>	087
3. Angaben von <i>Microsoft</i> Deutschland	088
4. Angaben aus der Polizeilichen Kriminalstatistik (PKS)	088
II. Interpretation der Angaben.....	092
C. Bekämpfung und Überwachung von Online-Softwarepiraterie.....	097
I. Rechtslage in Deutschland.....	097
1. Der urheberrechtliche Schutz von Computerprogrammen.....	097
2. Strafrechtsschutz von Computerprogrammen außerhalb des Urheberrechts.....	101
a) Patentrechtlicher Schutz	102
b) Markenrechtlicher Schutz.....	104
c) Wettbewerbsrechtlicher Schutz	105
3. Strafbarkeit von „Online-Softwarepiraten“ nach geltendem Recht	106
a) Anwendbarkeit deutschen Strafrechts	106

b) Handlungen der Mitglieder von Cracker-Gruppen.....	108
(1) Alle Mitglieder.....	108
(a) § 106 Abs. 1 UrhG	108
(b) § 108a UrhG.....	109
(c) § 129 StGB.....	109
(2) Cracker	110
(a) § 106 Abs. 1 UrhG	110
(b) § 202a StGB.....	110
(c) § 303a StGB.....	112
(d) § 17 UWG	113
(3) Packager / Ripper.....	114
(4) Kuriere.....	114
c) Handlungen der Betreiber von Webseiten und permanenten FTP-Servern.....	116
(1) Strafrechtliche Verantwortlichkeit.....	116
(2) Anbieten von Raubkopien.....	118
(3) Anbieten von Umgehungsprogrammen und Registrierungsinformationen.....	118
(4) Bereitstellen von Release-Informationen	119
(5) Haftung für (Hyper-)Links	120
d) Handlungen der Endnutzer von Raubkopien („Leecher“ und „Trader“).....	122
(1) Herunterladen oder Hochladen von Raubkopien.....	122
(2) Herunterladen und Benutzen vom Umgehungsprogrammen	122
(3) Herunterladen und Verwenden von illegalen Registrierungsinformationen.....	123
4. Strafbarkeit von „Online-Softwarepiraten“ nach zu erlassendem Recht (Betrachtung de lege ferenda).....	124
5. Rechtsprechung in Deutschland	126
II. Allgemeine Voraussetzungen einer effektiven Bekämpfung.....	126
1. Besonderheiten der Online-Kriminalität / Zukunftsprognose	126
2. Welche Spuren hinterlässt ein Online-Täter?.....	130
3. Einordnung der Bekämpfungsmaßnahmen / Arten der Kriminalitätsvorbeugung.....	136
III. Betrachtung der Maßnahmen, die offiziell von privater und staatlicher Seite eingesetzt werden bzw. eingesetzt werden sollen.....	137
1. Arbeit der Verbände und Anwälte von Softwareherstellern.....	137
a) Maßnahmen der <i>Software & Information Industry Association (SIIA)</i> bzw. <i>Software Publishers Association (SPA)</i>	137
b) Maßnahmen der <i>Business Software Alliance (BSA)</i> und von <i>Microsoft</i>	139
(1) Eigene Ermittlungen	139
(2) Internationale Zusammenarbeit mit Behörden und Providern / Schulungen	142
(3) Aufklärungsarbeit / Öffentlichkeitsarbeit.....	142

(4) Einflussnahme auf die Gesetzgebung.....	144
c) Maßnahmen anderer Verbände bzw. Unternehmen und von Anwälten	144
(1) <i>Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU)</i>	144
(2) <i>Verband der Unterhaltungssoftware Deutschland (VUD)</i>	145
(3) <i>Interactive Digital Software Association (IDSA)</i>	145
(4) Anwälte.....	146
(5) Private Copyright-Überwachungsdienste.....	147
2. Entwicklungsstrategische Maßnahmen von Softwareherstellern.....	149
a) Kopierschutzmaßnahmen	149
b) Zwangsaktivierung	149
c) Piracy Reminder, Schadroutinen etc.....	152
d) Softwaremiete - insbesondere Application Service Providing.....	155
e) Softwaredesign.....	156
3. Maßnahmen der <i>Internet Engineering Task Force (IETF)</i>	157
Exkurs – „Recht auf Anonymität“?	159
4. Maßnahmen von Hardwareherstellern.....	160
a) Internettaugliche Hardware nach der PC-Ära.....	160
b) Implementierung individueller Hardwarekennungen	161
5. Maßnahmen der Strafverfolgungsbehörden.....	163
a) Anlassabhängige Ermittlungen	163
b) Anlassunabhängige Ermittlungen	169
c) Internationale polizeiliche Zusammenarbeit	170
d) Zusammenarbeit mit der Providerindustrie	172
Exkurs – Selbstkontrolle und Codes of Conduct	172
6. Freiwillige Maßnahmen von Providern	173
7. Freiwillige Maßnahmen von Public-FTP-Administratoren	175
8. Rechtliche Maßnahmen zur Bekämpfung unerlaubter Verwertung von urheberrechtlich geschützten Werken per Internet	175
a) Verpflichtung von Providern zur Sperrung oder Filterung des Online- Angebots / Verantwortlichkeit der Diensteanbieter.....	175
(1) Haftung der Diensteanbieter für fremde rechtswidrige Informationen, die auf den eigenen Servern liegen	176
(2) Haftung für die Zugangsvermittlung zu fremden Inhalten.....	179
(a) Kontrollmöglichkeiten von Network-Providern	180
(b) Kontrollmöglichkeiten von Access-Providern	180

b) Kryptographie-Regulierung	184
9. Weitere Maßnahmen.....	188
a) Softwarefilter oder Rating Systeme beim Anwender.....	188
(1) Softwarefilter	188
(2) Rating-Systeme.....	189
b) Einrichtung von Hotlines	193
IV. Betrachtung der Maßnahmen, über deren Einsatz spekuliert wird	194
1. Datenausspähung über Applets bzw. Controls in Webbrowsern.....	194
2. Datenausspähung bei der Windows-Registrierung	195
3. Datenausspähung über Abstrahlungen von Computerhardware.....	198
4. Eingriffe in die IRC-Kommunikation.....	198
V. Fazit / Eigener Ansatz.....	200
1. Zusammenfassung der effektivsten Maßnahmen.....	200
2. Juristische Schlussfolgerungen	202
3. Weitere Schlussfolgerungen und Anregungen.....	207
Exkurs - Free Software und Open Source – das Ende der Softwarepiraterie?	209
Teil 3 - Internet-Musikpiraterie.....	214
A. Beschreibung und Struktur der MP3-Szene.....	214
I. Einführung in die kurze Geschichte der Online-Musikpiraterie.....	214
II. Die technischen Grundlagen der MP3-Herstellung	215
III. Tätigkeit der MP3-Gruppen.....	217
IV. Die Mitglieder der Gruppen.....	217
1. Supplier.....	217
2. Ripper / Encoder.....	219
3. Packer.....	221
4. Andere Gruppenmitglieder.....	222
V. Szenemitglieder ohne Gruppenzugehörigkeit	222
1. Nutzer von Peer-to-Peer-Filesharing-Systemen (P2P-Systeme)	222
2. Leecher und Trader.....	222
3. Profit-Pirates.....	223
VI. Kommunikationswege.....	224
VII. Wege der illegalen Musikdistribution	224
1. Peer-to-Peer-Filesharing-Systeme (P2P-Systeme)	224
a) <i>FastTrack</i> -Netz.....	227
b) <i>Gnutella</i> -Netz.....	227

c) <i>eDonkey2000</i>	228
d) Andere P2P-Systeme.....	229
2. WWW	230
3. FTP.....	232
4. IRC.....	232
5. Andere Dienste.....	232
VIII. Phänomenologische Betrachtung der MP3-Szene.....	232
1. Subkulturelle Besonderheiten.....	232
2. Täterkreis.....	233
3. Tätermotivation.....	234
B. Bedeutung und Schaden.....	236
I. Angaben über Fälle von Online-Musikpiraterie und über den Schaden.....	236
1. Angaben der <i>International Federation of the Phonographic Industry (IFPI)</i>	236
2. Angaben der <i>Recording Industry Association of America (RIAA)</i>	236
3. Andere Angaben.....	237
II. Interpretation der Angaben.....	238
C. Bekämpfung und Überwachung von Online-Musikpiraterie	243
I. Rechtslage in Deutschland.....	243
1. Der (urheber-)rechtliche Schutz von digitalen Musikwerken.....	243
2. Strafbarkeit von „Online-Musikpiraten“ nach geltendem Recht.....	247
a) Mitglieder von MP3-Gruppen	247
b) Betreiber von Webseiten und permanenten FTP-Servern.....	248
c) Profit Pirates.....	248
d) „Endnutzer“ von MP3-Dateien.....	249
(1) Herunterladen von Musikdateien	249
(2) Bereitstellen bzw. Anbieten von Musikdateien	251
Exkurs - Kompensationsansprüche für private Online-Verwertung von Musikwerken	253
3. Strafbarkeit von „Online-Musikpiraten“ nach zu erlassendem Recht (Betrachtung de lege ferenda).....	254
II. Betrachtung der Maßnahmen, die offiziell von privater und staatlicher Seite eingesetzt werden bzw. eingesetzt werden sollen.....	258
1. Arbeit der Musikindustrie-Verbände	258
a) Maßnahmen der <i>International Federation of the Phonographic Industry (IFPI)</i>	258
b) Maßnahmen der <i>Recording Industry Association of America (RIAA)</i>	261
c) Maßnahmen anderer Verbände und von sogenannten Solution Providern	266
2. Maßnahmen von Tonträgerherstellern	269
a) Kopierschutzmaßnahmen bei Audio-CDs	269

(1) <i>Key2Audio</i>	269
(2) <i>SafeAudio</i>	270
(3) <i>Cactus Data Shield</i>	271
b) Unternehmensstrategische Maßnahmen.....	275
(1) Herstellung spezieller Promo-Kopien	275
(2) Senkung der CD-Preise.....	276
(3) Schaffung legaler Download-Angebote.....	276
(a) <i>Windows Media Audio (WMA)</i>	277
(b) <i>Liquid Audio</i>	278
3. Entwicklung von DRM-Systemen.....	279
4. Maßnahmen von Hardwareherstellern.....	283
5. Andere Maßnahmen	283
III. Betrachtung der Maßnahmen, über deren Einsatz spekuliert wird	284
1. Datenausspähung über Multimedia-Player.....	284
2. „Virenattacken“ gegen Tauschbörsennutzer.....	284
IV. Fazit / Eigener Ansatz	285
1. Zusammenfassung der effektivsten Maßnahmen.....	285
2. Juristische Schlussfolgerungen	285
3. Weitere Schlussfolgerungen und Anregungen.....	286
Gesamtfazit	289