

Vergleichende Studie über Modelle zur Versendung von Warnhinweisen durch Internet-Zugangsanbieter an Nutzer bei Urheberrechtsverletzungen

im Auftrag des Bundesministeriums für Wirtschaft und Technologie
I C 4-02 08 15-29/11

vorgelegt von

Professor Dr. iur. habil. Rolf Schwartmann

unter Mitwirkung von

Caspar Bunke, Ass. iur.; Marie-Anne Buron, Avocat, Izabela Dumistracel, LL.M.; Professor
Klaus Gennen; Laureline Kergueris; Rechtsanwältin Nicola Lamprecht-Weißenborn LL.M.
Eur.; Gila Polzin, Ass. jur.; Rechtsanwältin Petra Silberkuhl.

Januar 2012

1. Teil: Rechtsvergleichende Untersuchung zu Warnhinweismodellen bei Urheberrechtsverletzungen im Internet

A.	Auftrag/Vorgehensweise	19
I.	Anlass der Untersuchung	19
II.	Rechtspolitische Ausgangssituation.....	21
1.	Positionen der Bundesregierung zu Warnhinweisen	21
2.	Der Wirtschaftsdialog	24
III.	Auftrag, Ziel und Vorgehensweise der Studie.....	26
1.	Vorgehensweise.....	28
a.	Datenerhebung.....	28
b.	Rechtsvergleich	29
c.	Methode der Rechtsvergleichung.....	29
IV.	Aufbau der Studie	30
1.	Ausgangslage und Status quo (1. Teil, A und B)	31
2.	Warnhinweismodelle in anderen EU-Mitgliedstaaten (1. Teil C).....	31
3.	Evaluation der Wirksamkeit vorhandener Warnhinweisregelungen (1. Teil D).....	32
4.	Erfordernis der Einführung eines Warnhinweismodells vor dem Hintergrund des aktuellen Urheberrechts (1. Teil E.).....	32
5.	Erwägungen zu einem innerstaatlichen Ansatz (2. Teil).....	33
B.	Status quo	34
I.	Vorbemerkung zur Methodik im Rahmen der Untersuchung	34
II.	Erscheinungsformen urheberrechtlich relevanter Handlungen im Internet	34
1.	Usenet.....	35
2.	P2P-Filesharing.....	36
3.	Sharehosting	37
4.	Streamhosting und Filmportale.....	38
5.	Recording Software und Online-Recording	38
6.	Fazit.....	39
III.	Ursachen für Urheberrechtsverletzungen im Internet.....	40
1.	Technologischer Fortschritt	41

2.	Mangelndes Rechts- bzw. Unrechtsbewusstsein	43
a.	Unkenntnis der Rechtslage	44
aa.	Unkenntnis des Rechts	45
bb.	Unkenntnis der tatsächlichen Umstände	46
b.	Fehlende Akzeptanz und Respektierung des Urheberrechts: Bewusste Normüberschreitung	47
aa.	Geltungsgründe von Recht	47
bb.	Versagen ethisch-moralischer Verhaltenskorrektur	48
cc.	Rechtsdurchsetzungsdefizit	50
IV.	Überblick zu Urheberrechtsverletzungen im Internet	51
1.	Allgemeines	51
2.	Einzelne Branchen	52
a.	Musik	53
b.	Film- und Fernsehbranche	55
c.	Software	57
e.	Bücher	58
f.	Zeitungen und Zeitschriften	59
3.	Zwischenergebnis	60
V.	Wirtschaftliche Auswirkungen von Urheberrechtsverletzungen	60
1.	Auswirkungen auf die Gesamtwirtschaft	60
2.	Auswirkungen auf die Umsatzentwicklung der betroffenen Branchen	61
3.	Auswirkungen auf die Kreativwirtschaft	65
a.	Methodische Schwierigkeiten bei der Ermittlung der Auswirkungen	66
b.	Konkrete Ansätze zur Feststellung wirtschaftlicher Auswirkungen	66
aa)	Ermittlungen im Rahmen des „Impact Assessment“ im Vereinigten Königreich	66
bb)	Auswirkungen auf das wirtschaftliche Wachstum in der Europäischen Union	67
cc)	Onlinepiraterie als Hemmnis bei der Schaffung kreativer Werke	70
dd)	Urheberrechtsverletzungen und neue Geschäftsmodelle in der digitalen Welt	71
VI.	Entwicklungstendenzen für die künftige Entwicklung von Onlinepiraterie	73

1.	Ausweitung des Zugangs zu Breitbandanschlüssen und Wandel zu mobilen Technologien.....	73
2.	Diversifizierung der technischen Möglichkeiten zur Rechtsverletzung.....	74
3.	Fortschreitende Digitalisierung kreativer Erzeugnisse	75
VII.	Zusammenfassung	75
C.	Warnhinweisemodelle in anderen EU Staaten.....	76
I.	Frankreich.....	76
1.	Ausgangslage (Überblick)	76
a.	Bedeutung von Kultur	76
b.	Urheberrechtliche Rahmenbedingungen und verfassungsrechtliche Grundlagen des Schutzes Geistigen Eigentums	76
aa.	Verfassungsrechtliche Perspektive	76
bb.	Gesetzliche Verankerung des Schutzes von Urheberrechten	77
2.	Stand der Gesetzgebung.....	79
a.	Historischer Kontext des Warnhinweisverfahrens	80
aa.	Novelle von 2006	80
bb.	Mission Olivennes.....	81
cc.	Novelle von 2009/2010.....	83
b.	Status quo.....	83
3.	Das französische Modell	85
a.	Schwierigkeiten der Ausgangslage	85
b.	Ausgestaltung des neuen Schutzsystems.....	85
aa.	Regelungsziel (Schutzzweck) und wesentliche Neuerungen.....	86
bb.	Systematische Verortung der Warnhinweis-Regelung	88
cc.	Anwendungsbereich der Hadopi-Gesetze.....	90
dd.	Regelungsinhalt des neuen Schutzsystems	91
1)	Die Einrichtung der Hadopi	91
a)	Struktur der Hadopi	91
b)	Aufgabe der Hadopi.....	92
aa)	Veröffentlichungen	92
bb)	Zertifizierung.....	93

cc)	Kennzeichnungs- und Filtertechniken	93
dd)	DRM	93
2)	Das Warnhinweisverfahren	94
a)	Tatbestandlicher Anknüpfungspunkt	94
b)	Antragsberechtigung	96
aa)	Inhalt des Antrags	96
bb)	Ablauf des Verfahrens	97
(1)	Erste Verwarnung	97
(2)	Zweite Verwarnung	98
(3)	Aufforderung zur Stellungnahme und Übermittlung an die Staatsanwaltschaft	98
cc)	Entscheidungsrahmen der Hadopi	99
3)	Gerichtliche Schritte	99
a)	Tatbestandliche Grundlagen - Ahndung von Urheberrechtsverstößen	99
aa)	Straftatbestand der Raubkopie	100
bb)	Fahrlässigkeitstatbestand	100
b)	Rechtsfolgen	102
4)	Weitere rechtliche Rahmenbedingungen	103
a)	Auskunftsansprüche gegen Internet-Zugangsanbieter	103
b)	Zivilrechtliche Durchsetzung von Urheberrechten	103
c.	Technische/organisatorische Umsetzung des Warnhinweismodells	104
4.	Datenschutzrechtliche Fragen von Warnhinweismodellen	107
5.	Zusammenfassung	109
II.	Vereinigtes Königreich	110
1.	Ausgangslage (Überblick)	110
a.	Rechtliche Rahmenbedingungen	110
aa.	Gesetzliche Verankerung des Schutzes von Urheberrechten	110
bb.	Auskunftsanspruch	111
b.	Akzeptanz des Urheberrechts in der Bevölkerung	112
2.	Stand der Gesetzgebung	113
a.	Historischer Kontext des Warnhinweisverfahrens	113

aa.	Digital Britain.....	113
bb.	Der Digital Economy Act 2010.....	114
b.	Status Quo.....	114
3.	Das britische Modell.....	115
a.	Erfasste Erscheinungsformen von Internetpiraterie.....	115
b.	Ausgestaltung des Schutzsystems nach dem DEA.....	116
aa.	Regelungsziel (Schutzzweck).....	116
bb.	Systematische Verortung der Warnhinweis-Regelung.....	117
1)	Initial Obligations Code.....	117
2)	Technical Obligations Code.....	117
cc.	Die Rolle der OFCOM.....	118
1)	Erlass des Initial Obligations Code.....	118
2)	Erlass des Technical Obligations Code.....	118
3)	Überwachung.....	118
dd.	Anwendungsbereich des DEA.....	119
1)	Vorgabe des DEA.....	119
2)	Umsetzung durch den Entwurf des Initial Obligations Code.....	119
3)	Gerichtliche Überprüfung.....	120
ee.	Regelungsinhalt des neuen Schutzsystems.....	120
1)	Prävention vor Sanktion.....	120
2)	Aufklärung durch Versendung von Warnhinweisen (Art. 124 A – 124 F DEA).....	121
a)	Ermittlung des Rechtsverstoßes nach DEA.....	121
b)	Der Warnhinweis.....	122
aa)	DEA.....	122
bb)	OFCOM-Entwurf des Initial Obligations Code.....	123
c)	Liste der gemeldeten Urheberrechtsverstöße als Grundlage des Auskunftsanspruchs (Verstoßliste).....	124
aa)	Hintergrund der Verstoßliste.....	124
bb)	Verstoßliste nach DEA.....	124
cc)	OFCOM-Entwurf des Initial Obligations Code.....	125

3)	Sanktion - Technische Verpflichtungen (Art. 124 G – J DEA)	125
4)	Rechtsschutzverfahren	126
a)	Widerspruchsrecht gegen Maßnahmen im Rahmen der Warnhinweisversendung (Art. 124 K DEA).....	126
b)	Rechtsschutz gegen technische Sanktionen (Art. 124 K DEA).....	127
aa)	Widerspruchsverfahren.....	127
bb)	Anfechtung von Maßnahmen vor dem First-tier Tribunal (Art. 124 K DEA) 128	
c.	Technische/organisatorische Umsetzung des Warnhinweismodells, hier Kostenverteilung	128
aa.	Qualifizierungskosten	128
1)	Ursprünglich 25 Prozent der Kosten bei Diensteanbieter.....	128
2)	Überprüfung durch den High Administrative Court.....	128
3)	Korrektur durch den Gesetzgeber.....	129
bb.	Relevante Kosten	129
cc.	Kosten des Rechtsschutzverfahrens.....	129
4.	Überprüfung des DEA durch den High Administrative Court.....	130
a.	Verhältnismäßigkeit der Regelungen des DEA	131
aa.	Geeignetheit/legitimer Zweck.....	131
bb.	Erforderlichkeit der angegriffenen Regelungen	132
cc.	Angemessenheit der angegriffenen Regelungen.....	133
1)	Abschreckungswirkung.....	133
2)	Direktes Vorgehen gegen Nutzer unverhältnismäßig?.....	134
3)	Gemeinschädlichkeit des Regelungsansatzes	134
4)	Unzutreffende Zahlen von Seiten der betroffenen Branchen?	134
5)	Kostenverteilung.....	135
6)	Zwischenergebnis	135
b.	Berufung gegen die Entscheidung des High Court (Administrative Court)	135
5.	Impact Assessment zum Warnhinweismodell (Kosten-Nutzen-Analyse).....	137
a.	Kosten	138
aa.	Kosten der Internetzugangsdiensteanbieter	138

1) Kosten der Warnhinweisversendung	138
2) Qualifizierungskosten	140
3) Kosten für Kundenhotline	140
4) Kapitalkosten der Diensteanbieter	140
5) Kosten mobiler Netzwerkanbieter	142
bb. Kosten auf Verbraucherseite	142
cc. Kosten auf Seiten der Rechteinhaber.....	143
dd. Kosten auf Seiten des Staates	144
b. Nutzen.....	144
aa. Nutzen für Rechteinhaber	144
bb. Nutzen für Verbraucher.....	144
cc. Nutzen für den Staat.....	145
c. Ergebnis der Kosten-Nutzen-Analyse	145
aa. Kosten - £290 - 500 Mio.....	145
bb. Nutzen - £1.7 Mrd	145
d. Gesamt Netto-Nutzen £1,2 Mrd.....	145
6. Zusammenfassung	145
III. Republik Irland	146
1. Ausgangslage (Überblick)	146
a. Bedeutung von Kultur	146
b. Urheberrechtliche Rahmenbedingungen und verfassungsrechtliche Grundlagen des Schutzes Geistigen Eigentums	147
aa. Verfassungsrechtliche Perspektive	147
bb. Gesetzliche Verankerung des Schutzes von Urheberrechten	147
1) Copyright and Related Rights Act 2000	147
2) Auskunftsanspruch	149
a) Offenlegung der Identität.....	149
b) Weitere Auskunftsklagen.....	150
c) Sonstige Verfahren	151
2. Stand der Gesetzgebung/ Vergleichsregelung.....	151
3. Vergleich und Protokoll zur Warnhinweisregelung	152

4.	Das Warnhinweis-Modell in der Republik Irland	154
a.	Ausgestaltung.....	154
aa.	Regelungsziel (Schutzzweck)	154
bb.	Systematische Verortung der Warnhinweis-Regelung	155
cc.	Anwendungsbereich	155
dd.	Regelungsinhalt.....	155
1)	Schematische Prüfung	155
a)	Level 1 („First Warning“)	156
b)	Level 2 („Second Warning“).	157
c)	Level 3 („Termination Notice“ und Anschlussunterbrechung).....	158
d)	Level 4 (Wiederanschluss).....	158
e)	Level 5 (Einjährige Anschluss Sperre)	158
2)	Beschwerderecht des Anschlussinhabers	159
b.	Organisatorische Umsetzung des Warnhinweismodells.....	160
aa.	Aufgabe der Rechteinhaber	160
bb.	Aufgabe der Provider	161
5.	Entscheidungen des <i>High Court</i> mit Bezug zur Vergleichsregelung	162
a.	Vereinbarkeit der Warnhinweis-Regelung mit irischem Datenschutz- und Verfassungsrecht	162
aa.	IP-Adresse als personenbezogenes Datum	162
bb.	Verfassungsrechtliche Bewertung des „ <i>Graduated Response</i> “- Verfahrens ...	162
cc.	Weitere datenschutzrechtliche Aspekte.....	163
b.	Sperrung von Pirate Bay.....	164
c.	Anordnungen zur Sperrung auf gesetzlicher Grundlage.....	164
aa.	Keine gesetzliche Grundlage im irischen Recht.....	165
bb.	Bestätigung der Entscheidung zum Eircom-Vergleich.....	166
6.	Zusammenfassung	166
IV.	Finnland	168
1.	Ausgangslage (Überblick)	168
a.	Urheberrecht in Finnland	168
b.	Rechtsdurchsetzung.....	168

c.	Rechtsprechung.....	169
aa.	Zugangssperren.....	169
bb.	Schadensersatz.....	169
2.	Gescheiterter Entwurf eines Warnhinweismodells.....	169
a.	Entwicklung bis Frühjahr 2011.....	170
b.	Inhalt des gescheiterten Entwurfs.....	170
c.	Diskussion des Vorschlags in Finnland.....	171
3.	Weitere Entwicklung.....	172
a.	Politische Entwicklung.....	172
b.	Rechtsprechung.....	172
4.	Zusammenfassung.....	172
V.	Belgien.....	174
1.	Die Gesetzesentwürfe.....	174
a.	Das abgestufte Warnhinweisverfahren.....	174
aa.	Ausgangspunkt des Verfahrens.....	175
bb.	Ablauf des Verfahrens.....	175
b.	Weitere Maßnahmen.....	176
aa.	Maßnahmen gegen sog. Piraten-Seiten (Artt. 3, 4).....	176
bb.	Förderung legaler Angebote im Internet und Aufklärung der Internetnutzer (Artt. 5, 6, 25).....	176
cc.	Zurverfügungstellung urheberrechtlich geschützter Werke und Leistungen in Datenbanken (Artt. 7 ff.).....	176
dd.	Austausch urheberrechtlich geschützter Werke und Leistungen durch Zugangsdiensteanbieter (Artt. 12, 13).....	177
2.	Stand des Gesetzgebungsverfahrens.....	177
3.	Die Entscheidung in der Rechtssache Scarlet Extended/SABAM.....	177
4.	Zusammenfassung.....	179
VI.	Schweden.....	180
1.	Ausgangssituation.....	180
2.	Urheberrecht.....	180
a.	Auskunftsanspruch.....	181

b.	Durchsetzung des Auskunftsanspruchs	184
aa.	Speicherungspflicht der Zugangsanbieter	184
bb.	Überprüfung des Auskunftsanspruchs durch den EuGH (Bonnier Audio AB/ePhone)	185
cc.	Effizienz des Auskunftsanspruchs	186
1)	Rückgang von Datenverkehr	186
2)	Positive Auswirkungen auf das Piraterieverhalten	186
3)	Nachlassen der Wirkung	187
4)	Ursachen für Nachlassen der Wirkung	188
c.	Strafrechtliche Verfolgung von Urheberrechtsverletzungen	188
3.	Lösungsansatz des Justizministeriums unter Einbindung der Zugangsanbieter 188	
4.	Zusammenfassung	189
VII.	Warnhinweisemodelle außerhalb der Europäischen Union	190
1.	Vereinigte Staaten von Amerika	190
2.	Chile	192
3.	Republik Korea (Südkorea)	192
4.	Taiwan	193
5.	Neuseeland	193
6.	Kanada	194
D.	Effizienz/ Wirksamkeit	195
I.	Rechtsvergleichende Bewertung von Warnhinweisemodellen	195
1.	Technische Perspektive	195
a.	Identifikation des Verantwortlichen	195
b.	Identifikation der Rechtsverletzung	197
aa.	Identifikation in Peer-to-Peer-Netzen (Vorgehen und Unsicherheiten)	197
bb.	Dauer der Speicherung von Daten	200
c.	Bewertung	201
2.	Pädagogische Perspektive	202
a.	Generelle Bedeutung der Rechtsdurchsetzung	203
b.	Ausweichen auf andere Techniken wegen technischen Anwendungsrahmens 204	

c.	Verhaltenssteuerung.....	205
aa.	Abkehr von Peer-to-Peer-Nutzung - Änderung des Nutzerverhaltens hin zur Legalisierung.....	206
1)	Zielgruppe	206
2)	Besonders betroffene Bereiche	207
3)	Gerechtigkeitsempfinden und Verständnis für Interessen der Urheber ..	208
4)	Erkennbare Verhaltensänderungen	208
a)	Auswirkung von Warnhinweisen auf Nutzerverhalten	208
b)	Bedeutung von Sanktionen	218
bb.	Veränderung des Konsumverhaltens: Gibt es Indikatoren dafür, dass die Nutzer zur Legalisierung ihres Verhaltens angehalten werden?	219
d.	Zwischenfazit	220
3.	Informationelle Perspektive	220
a.	Unterscheidung rechtmäßig - unrechtmäßig	220
b.	Aufklärungsarbeit allgemein.....	222
c.	Zwischenfazit	223
4.	Effizienz und wirtschaftliche Perspektive.....	224
E.	Rechtsdurchsetzung	226
I.	Grundzüge nationaler urheberrechtlicher Vorgaben im einfachen Recht	226
II.	Einzelheiten zu den Voraussetzungen zivilrechtlicher Durchsetzung von Urheberrechten	227
1.	Rechtswidrigkeit der Verletzung	227
2.	Verschulden.....	229
3.	Anspruchsberechtigte	229
4.	Anspruchsverpflichtete.....	230
a.	Haftung als Täter/Teilnehmer, telemedienrechtliche Haftungsprivilegierung 230	
b.	Mögliche Haftung als Störer.....	231
aa.	Allgemeine Voraussetzungen der Störerhaftung	231
bb.	Bestehen einer Prüfungspflicht als Voraussetzung für die Störerhaftung ..	232
1)	Prüfungspflichten von Host-Providern	232
2)	Zuganganbieter (Access-Provider) als Störer.....	235

3) Haftung bzw. Störerhaftung des Anschlussinhabers.....	238
5. Voraussetzungen für einen Unterlassungsanspruch, Erstbegehungs- bzw. Wiederholungsgefahr.....	241
6. Schadensersatzanspruch.....	242
a. Verschulden.....	242
b. Höhe des Schadensersatzes, Berechnungsmethoden.....	243
7. Abmahnung.....	245
a. Anforderungen an die Abmahnung.....	246
b. Rechtsmissbräuchlichkeit der Abmahnung.....	246
c. Reaktionsmöglichkeiten des Abgemahnten.....	248
d. Ersatz von Abmahnkosten.....	250
III. Auskunftsanspruch nach deutschem Recht.....	252
1. Ausgangslage.....	252
2. Voraussetzungen des Auskunftsanspruchs gegen Zugangsanbieter.....	253
a. Offensichtliche Rechtsverletzung und gewerbliches Ausmaß der Zugangsvermittlung.....	254
b. Gewerbliches Ausmaß der Rechtsverletzung.....	255
c. Auskunftsverfahren gegen Zugangsanbieter gemäß § 101 Abs. 9 UrhG.....	257
aa. Grundlagen.....	257
bb. Verkehrsdaten.....	258
cc. Richtervorbehalt bei Verkehrsdaten.....	259
dd. Probleme in der Praxis.....	260
3. Eignung des Auskunftsanspruchs zur Rechtsdurchsetzung.....	265
IV. Rechtsvergleichender Blick auf Auskunftsansprüche.....	266
2. Teil: Erwägungen zu einem innerstaatlichen Ansatz.....	268
A. Vorgerichtliches Mitwirkungsmodell.....	268
I. Ausgangsüberlegung.....	268
II. Parameter eines denkbaren Ansatzes.....	269
B. Internationale Rahmenvorgaben für ein vorgerichtliches Mitwirkungsmodell.....	269
I. Urheberrecht.....	270
1. Völkerrechtliche Grundlagen.....	270

a.	Vereinte Nationen	270
b.	Weltorganisation für geistiges Eigentum (WIPO).....	271
c.	Welturheberrechtsabkommen.....	272
d.	Rom-Abkommen	272
e.	Welthandelsorganisation (WTO).....	272
f.	Anti-Counterfeiting Trade Agreement (ACTA).....	273
g.	Europarat	276
2.	Recht der Europäischen Union.....	276
a.	Charta der Grundrechte der europäischen Union (EU-Grundrechtecharta)....	276
b.	InfoSoc-Richtlinie (2001/29/EG)	276
c.	Enforcement-Richtlinie (2004/48/EG).....	277
d.	Telekom-Paket.....	277
e.	Art. 8 Abs. 1 Rom II-VO.....	279
f.	Rechtsprechung des EuGH – Scarlet Extended.....	279
3.	Rechtspolitische Initiativen der Europäischen Union.....	280
a.	Mitteilung zur „Verbesserung der Durchsetzung von Rechten des geistigen Eigentums im Binnenmarkt“	280
b.	Grünbuch „Erschließung des Potenzials der Kultur- und Kreativindustrien“ ..	280
c.	Eine digitale Agenda für Europa.....	281
d.	Gallo-Bericht.....	281
II.	Datenschutzrecht	282
1.	Völkerrecht.....	282
a.	Vereinte Nationen und OECD	282
b.	Europarat	282
2.	Recht der Europäischen Union.....	283
a.	Primärrecht	283
b.	Sekundärrecht.....	283
aa.	Allgemeine Datenschutzrichtlinie (95/46/EG)	283
bb.	Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG)	285
cc.	Vorratsdatenspeicherungsrichtlinie (2006/24/EG)	285
c.	Rechtsprechung des Europäischen Gerichtshofs zum Auskunftsanspruch.....	286

aa. <i>Promusicae</i>	286
bb. <i>Bonnier Audio AB</i>	287
C. Nationale Vorgaben für ein Warnhinweismodell	287
I. Rechteinhaber	288
1. Verfassung.....	288
2. Einfaches Recht	288
II. Nutzer	288
1. Art. 5 GG	288
2. Art. 10 GG und Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG	289
a. Verfassungsrechtliche Parameter.....	289
aa. Recht auf informationelle Selbstbestimmung.....	289
bb. Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	291
cc. Fernmeldegeheimnis	291
1) Allgemeine Fragen	291
2) Anlasslose Speicherung im Hinblick auf das vorgerichtliche Mitwirkungsmodell.....	292
b. Einfachgesetzliche Ausgestaltung	293
aa. Fernmeldegeheimnis	293
bb. Datenschutzrecht	294
c. Datenschutzrechtlich relevante Aspekte von Warnhinweismodellen.....	295
aa. IP-Adresse als personenbezogenes Datum	295
1) Exkurs zum internationalen Recht.....	295
a) Europäische Union	296
b) Vereinigtes Königreich.....	297
c) Irland.....	297
2) National	298
a) Personenbezug von IP-Adressen für Internetzugangsanbieter.....	299
b) Personenbezug von IP-Adressen für andere Stellen	299
c) Personenbezug von IP-Adressen für Rechteinhaber.....	299
bb. Datenschutzrechtlich relevantes Handeln.....	300

1) Ermittlung von IP-Adressen durch die Rechteinhaber	300
2) Verwendung der IP-Adresse durch Zugangsdiensteanbieter	300
III. Zugangsanbieter	302
1. Art. 12 GG.....	302
2. Art. 14 GG.....	302
D. Vorschlag und Prüfung eines vorgerichtlichen Mitwirkungsmodells in Deutschland	303
I. Regelungsziel und Mittel des vorgerichtlichen Mitwirkungsmodells.....	303
1. Regelungsziel: Urheberrechtsschutz	303
2. Mittel: Kombination von erklärenden Warnhinweisen und gerichtlichen Auskunftsanspruch unter Mitwirkung der Zugangsanbieter	304
a. Aufklärung und Warnung.....	304
b. Auskunft zur Ermöglichung des zivilrechtlichen Ausgleichs.....	304
c. Mitwirkung der Zugangsanbieter	304
aa. Mitwirkung nach derzeitigem Recht.....	305
bb. Mitwirkung nach dem vorgerichtlichen Mitwirkungsmodell.....	305
cc. Datenschutzrechtliche Bedachtnahme.....	306
3. Verfassungsrechtliche Fragen einer Inpflichtnahme der Zugangsanbieter	306
a. Ausgangslage.....	306
b. Die widerstreitenden Grundrechtspositionen	307
c. Ausgestaltung der Eigentumsfreiheit der Rechteinhaber	308
d. Inpflichtnahme und Berufsfreiheit der Zugangsanbieter nach Art. 12 GG	310
aa. Eingriff in den Schutzbereich von Art. 12 Abs. 1 GG	310
bb. Verfassungsrechtliche Rechtfertigung	310
1) Regelung der Berufsausübung.....	310
2) Verhältnismäßigkeit einer Inpflichtnahme der Zugangsanbieter	311
a) Legitimer Zweck.....	311
b) Eignung des vorgerichtlichen Mitwirkungsmodells	312
aa) Einschätzungsspielraum des Gesetzgebers bei Beurteilung der Eignung	312
bb) Effizienz von Warnhinweisen.....	313
(1) Frankreich.....	313

(2) Irland	314
(3) Vereinigtes Königreich	316
cc) Beschränkung auf P2P	316
dd) Zwischenergebnis	317
c) Erforderlichkeit des vorgerichtlichen Mitwirkungsmodells	318
aa) Vorgehen ohne Mitwirkung der Zugangsanbieter	318
bb) Vorgehen nur im Rahmen des Auskunftsanspruchs.....	318
(1) Probleme bei der Geltendmachung des Auskunftsanspruchs.....	318
(2) Auskunftsanspruch als milderes Mittel.....	318
cc) Sanktionslose Versendung von Warnhinweisen	320
dd) Anlasslose Warnhinweise	320
ee) Netzsperrern	320
d) Angemessenheit des vorgerichtlichen Mitwirkungsmodells	322
aa) Nähe zur Rechtsverletzung.....	322
bb) Vertragliche Befugnisse des Zugangsanbieters bei Rechtsmissbrauch.....	322
cc. Zwischenergebnis	326
E. Ergebnis	326
3. Teil Kurzfassung	327
A. 1. Teil: Rechtsvergleichende Untersuchung zu Warnhinweismodellen bei Urheberrechtsverletzungen im Internet	327
I. Ausgangssituation	327
1. Erscheinungsformen von Rechtsverletzungen im Internet	327
2. Betroffene Branchen	328
3. Umsatzrückgänge	328
4. Zusammenhang zwischen Umsatz und illegaler Nutzung.....	328
5. Auswirkungen.....	329
6. P2P.....	329
II. Rechtsvergleichende Untersuchung	329
1. Frankreich.....	330
2. Vereinigtes Königreich	331

3.	Republik Irland.....	332
4.	Ausgewählte weitere Europäische Staaten.....	333
III.	Effizienz von Warnhinweismodellen.....	333
1.	Technische Perspektive.....	333
2.	Pädagogische Perspektive.....	334
3.	Informationelle Perspektive.....	335
4.	Wirtschaftliche Perspektive.....	335
IV.	Rechtsdurchsetzung nach deutschem Urheberrecht.....	336
B.	2. Teil: Erwägungen zu einem innerstaatlichen Ansatz.....	336
I.	Vorgerichtliches Mitwirkungsmodell.....	337
II.	Verfahrensablauf.....	337
III.	Vorteil des Modells.....	338
IV.	Erfordernis rechtlicher Konsequenzen bei mehrfachen Verstößen.....	338
V.	Unterschied gegenüber dem reinen Auskunftsanspruch.....	338
VI.	Rechtlicher Rahmen.....	339
1.	Internationaler urheber- und datenschutzrechtlicher Rahmen.....	339
2.	Nationaler Rechtsrahmen.....	339
a.	Datenschutzrecht.....	340
b.	Verfassungsrechtliche Vorgaben.....	341
C.	Fazit.....	344
	Anhang (Gesetzestexte und Quellen).....	346

A. Auftrag/Vorgehensweise

I. Anlass der Untersuchung

Digitalisierung und Internet haben erheblichen Einfluss¹ auf die wirtschaftliche, kulturelle und gesellschaftliche Entwicklung der letzten beiden Jahrzehnte. Der Markt für Internet-Anschlussdienste hat sich nach Daten der Europäischen Kommission in den vergangenen 15 Jahren zu einem Sektor mit Milliardenumsatz entwickelt.² Der aktuellen ARD/ZDF-Onlinestudie zufolge nutzen 73,3 Prozent der Deutschen das Internet.³ Danach hat sich die Zahl der Internetnutzer in den letzten 15 Jahren nahezu verdoppelt.⁴ Der größte Anteil der Nutzung entfällt dabei auf Kommunikation. Mit einem Drittel Anteil an der Kommunikation schlagen hierbei soziale Netzwerke zu Buche, mit zwei Dritteln der Emailverkehr und die Nutzung von Gesprächsforen.⁵ In der Rangliste der häufigsten Tätigkeit steht die Suche nach Informationen hinter der Kommunikation auf dem zweiten Platz, danach folgen Online-Spiele, Unterhaltung und Online-Geschäfte (Shopping, Banking, Auktionen).⁶ Elektronische Kommunikation ist damit zu einem wesentlichen Bestandteil des geschäftlichen und auch des privaten Lebens geworden.

Im und mit dem Internet hat sich eine Vielzahl neuer Geschäftsmodelle von enormem wirtschaftlichem Potential entwickelt.⁷ Die Gesellschaft macht sich die neuen Möglichkeiten zunutze und entwickelt sich mit ihnen weiter. Sichtbar wird dies in der kaum mehr ersetzbaren Nutzung neuer Kommunikationsmöglichkeiten für soziale Interaktion, für Bildung und Kultur, in der Nutzbarmachung des Internets für den Vertrieb und Einkauf, für Unternehmenskommunikation und Online-Bürgerservices, zugleich auch in den Fortschritten von Wissenschaft und Technik.

¹ Bisweilen wird der Vergleich mit der Erfindung der Dampfmaschine als Grundstein der Industrialisierung gezogen, vgl. *Schirmacher*, Was passiert, wenn der Kopf nicht mehr mitkommt, in: *Schwartzmann*, Leben im Schwarm – Wie das Internet uns verändert, 2010, S. 13 f.

² Offenes Internet und Netzneutralität in Europa, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen v. 19.4.2011, KOM(2011) 222 endgültig.

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0222:FIN:DE:PDF>.

³ Nach dem elften Berichtsband des (N)ONLINE Atlas sind es im Jahr 2011 sogar 74,7 Prozent der deutschen Bevölkerung ab 14 Jahren, die das Internet nutzen. (N)ONLINER Atlas, Studie der Initiative D21 in Zusammenarbeit mit TNS Infratest, S. 12.

⁴ *van Eimeren/Frees*, Drei von vier Deutschen im Netz – ein Ende des digitalen Grabens in Sicht?, Ergebnisse der ARD/ZDF-Onlinestudie 2011, Media Perspektiven 7-7/2011, S. 334.

⁵ *van Eimeren/Frees*, a.a.O., S. 334, 341.

⁶ *van Eimeren/Frees*, a.a.O., S. 334, 341.

⁷ Allein die Bedeutung der Informations- und Kommunikationswirtschaft (IKT) selbst wird über ihren Anteil von fünf Prozent an der Bruttowertschöpfung der europäischen Wirtschaft hinaus als wesentlicher Innovationsmotor und Umsatzbringer in vielen Anwenderbranchen gesehen. Vgl. Monitoring-Report Deutschland Digital, Der IKT-Standort im internationalen Vergleich 2010, Bundesministerium für Wirtschaft und Technologie (BMWi)/TNS Infratest Business Intelligence, S. 9.

Die großflächige, zeitnahe und vergleichsweise simple Verfügbarkeit von Inhalten und Informationen⁸ macht das Internet zu einem unvergleichlichen Massenmedium. Es steht für Meinungsaustausch, für Kreativität und Innovation. Zugleich birgt es auch Phänomene, die an die Grenzen der bisherigen Rechtsordnung stoßen und mitunter darüber hinaus gehen. Als ein solches Massenphänomen dürfen **Urheberrechtsverletzungen im Internet** gelten. Es ist unbestritten, dass laufend urheberrechtlich geschützte Inhalte illegal veröffentlicht, verändert und/oder kopiert werden. Der Rechtsbruch erfolgt in unterschiedlicher Form. Die technischen Möglichkeiten sind vielfältig. Wege der Rechtsverletzung sind beispielsweise der Gebrauch von Downloadplattformen oder Internettauschbörsen/Peer-to-Peer-Filesharingsystemen, über die Content unautorisiert angeboten und/oder abgerufen werden kann. Daneben existieren Geschäftsmodelle, wie Streaming-Portale, die auf illegale Weise den Konsum aktueller Filme, TV-Serien und/oder Sportereignisse ermöglichen. Vergleichbar sind Host-Services (sog. Cyberlocker oder ShareHoster), die dem Nutzer die Ablage von Dateien auf einem virtuellen Speicherplatz (Cloud) ermöglichen und auf die Dritte über eine Verlinkung Zugriff haben.⁹

Betroffen von unberechtigtem Gebrauch urheberrechtlich geschützter Werke sind insbesondere Inhalte aus den Bereichen Musik, Film und Software.¹⁰ Das Recht verbietet unlicenziertes Gebrauchmachen ohne Einwilligung des berechtigten Urhebers oder Lizenzinhabers.¹¹ Auch sieht das Urheberrechtsgesetz strafrechtliche Sanktionierungen vor. Die Rechtsdurchsetzung folgt dem Recht jedoch gerade im Internet nur behäbig¹². Dem Rechteinhaber ist die Identität des Rechteverletzers nicht bekannt, seine Nutzerdaten sind für ihn nicht verfügbar bzw. nur schwierig ermittelbar. Das Internet ist weitgehend anonym und technische Raffinessen erlauben es, diese Anonymität bis zur absoluten Unkenntlichkeit des Nutzers für jeden an der Datenübertragung beteiligten Dienst, d.h. selbst für den Internetprovider, zu steigern.¹³ Soweit eine Verfolgung von Urheberrechtsverletzungen überhaupt praktisch durchführbar ist, kann sie stets nur im Einzelfall ermittelt und die Rechtsverfolgung nur individuell betrieben werden. Dies ist mit erheblichem finanziellem und personellem Aufwand bei nur bedingter Effizienz verbunden.

⁸ Eine Versorgung mit Breitband von mindestens 1 Mbit/s war 2010 für 98,3 Prozent der deutschen Haushalte möglich. Vgl. Bericht zum Breitbandatlas 2010 des Bundesministeriums für Wirtschaft und Technologie, Teil 1, S. 5. Abrufbar unter:

<http://www.zukunft-breitband.de/Dateien/BBA/PDF/breitbandatlas-bericht-2010-teil-1,property=pdf,bereich=bba,sprache=de,rwb=true.pdf> (letzte Zugriff: 29.8.2011).

⁹ Dazu *Schwartmann*, Sharehosting, Filesharing & Co, K&R Beihefter 2/2011.

¹⁰ Siehe unten, S. 52.

¹¹ *Schwartmann*, Sharehosting, Filesharing & Co, K&R Beihefter 2/2011.

¹² *Schwartmann*, Leben im Schwarm, S. 99, 101 f.

¹³ Im Netz werden bspw. sog. „Anonymizer“ angeboten. Gängig sind etwa Proxy-Server, die mit Verschlüsselungen arbeiten. Beispiele hierfür sind: <http://hujiko.com>; <http://www.behidden.com/>; <http://www.megaproxy.com/freesurf/>; <http://www.the-cloak.com/login.html>; <http://anonymouse.org/anonwww.html>; <http://proxify.com/>; <http://www.anonymousinet.com/index2.php>; http://www.guardster.com/subscription/proxy_free.php; <http://proxy.org/>; <http://proxy.guardster.com/proxy.php>; <http://browseatwork.com/>.

Aufgrund des Vorwurfs einer massenhaften, letztlich – wie behauptet wird - mangels Rechtsdurchsetzung faktisch nicht sanktionierten Missachtung von Urheber- und Verwertungsrechten¹⁴ werden immense wirtschaftliche und kulturelle Schäden reklamiert. Ermöglicht werden die Rechtsverletzungen im Internet durch die neuen Techniken zur raschen Herstellung und Übermittlung von Kopien. Dass und die Fülle, in der sie stattfinden, kann Hinweis auf ein sich wandelndes Werteverständnis und Rechtsbewusstsein sein.¹⁵ Gründe dafür werden in der fehlenden effektiven Sanktionierung gesehen¹⁶. Ein Teil der Rechtsüberschreitungen wird gerade bei privaten Nutzern aber auf mangelnde Aufklärung zurückgeführt. Hinzu kommt, dass gesetzlich aufgezeigte Grenzen den steten technischen Entwicklungen kaum Rechnung tragen können und dabei zu Bewertungsspielräumen beim Nutzer führen. Als Beispiel sei hier die auch in der Fachliteratur diskutierte Frage der rechtlichen Bewertung des Konsums illegaler Angebote auf Plattformen wie des stillgelegten Portals kino.to angeführt.¹⁷ Rechtliche Grenzen werden ausgeschöpft und bisweilen übertreten.

Angesichts der Rechtsverletzungen, ihren Auswirkungen und den Schwierigkeiten, die sich bei der Rechtsdurchsetzung im Verhältnis zwischen Rechteinhaber und Rechteinverletzer stellen, werden neue Möglichkeiten diskutiert, das Problem in Angriff zu nehmen. Dabei ist die Einbeziehung der Internet-Service-Provider bzw. Internet-Zugangsanbieter („Zugangsanbieter“) in die Durchsetzung urheberrechtliche Ansprüche ebenso naheliegend wie umstritten¹⁸.

II. Rechtspolitische Ausgangssituation

1. Positionen der Bundesregierung zu Warnhinweisen

Diese Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie setzt – soweit Rahmenbedingungen für das innerstaatliche Recht aufgezeigt werden sollen - bei den Vorgaben des Koalitionsvertrages zwischen CDU, CSU und FDP für die 17. Legislaturperiode vom 26.10.2009 an. In den Ausführungen zum Urheberrecht¹⁹ heißt es auf Seite 103 f.:

„Das Urheberrecht hat in der modernsten Medien- und Informationsgesellschaft eine Schlüsselfunktion. Wir werden das Urheberrecht deshalb entschlossen weiterentwickeln, mit dem **Ziel ein hohes Schutzniveau und eine wirksame Durchsetzbarkeit des Urheberrechts zu gewährleisten**. Um dieses Ziel zu erreichen,

¹⁴ Vgl. zur Haltbarkeit dieses Vorwurfs S. 204.

¹⁵ Siehe im Einzelnen unten, S. 40.

¹⁶ *Schwartmann*, *Leben im Schwarm*. 99, 101f.

¹⁷ Vgl. *Schwartmann*, *Sharehosting, Filesharing & Co*, K&R Beihefter 2/2011, S. 15 ff.

¹⁸ Siehe dazu unten, S. 226 ff.

¹⁹ Dazu *Paal/Hennemann*, ZRP 2010. 40, 41.

werden wir zügig die Arbeit an einem Dritten Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft („Dritter Korb“) aufnehmen. (...)

Das Internet darf kein urheberrechtsfreier Raum sein. Wir werden deshalb unter Wahrung des Datenschutzes bessere und wirksame Instrumente zur konsequenten Bekämpfung von Urheberrechtsverletzungen im Internet schaffen. Dabei wollen wir Möglichkeiten der **Selbstregulierung unter Beteiligung von Rechteinhabern und Internetserviceprovidern fördern. Wir werden keine Initiativen für gesetzliche Internetsperren bei Urheberrechtsverletzungen** ergreifen.

Der Schutz durch das Urheberrecht ist eine notwendige Voraussetzung für die Schaffung und für die Verwertung kreativer Leistungen. Wir wollen deshalb Maßnahmen unterstützen, die das gesellschaftliche Verständnis für die Bedeutung des Urheberrechts und den Respekt vor fremdem geistigem Eigentum fördern.“ (Hervorhebungen diesseits).

Der Monatsbericht des BMWi zu Schlaglichtern der Wirtschaftspolitik aus dem Oktober 2009 fasste unter dem Punkt „Fortentwicklung des Rechtsrahmens für digitalen Urheberrechtsschutz“ die Fortführung des Ansatzes und der Ziele der Bundesregierung wie folgt zusammen:

„In der Kultur- und Kreativwirtschaft kommt den Schöpfern von Inhalten eine besondere Bedeutung zu. Sie legen erst die Grundlage für eine Vielzahl sich anschließender ökonomischer Aktivitäten. Wichtig ist daher, dass die kreativen Schöpfer auch wirtschaftlich eine Zukunft haben. Die Balance zwischen Urhebern und Nutzern ist durch die Digitalisierung aus dem Gleichgewicht geraten und es muss versucht werden, die Waage wieder stärker auszubalancieren. Insbesondere die Fortentwicklung des Rechtsrahmens für digitalen Urheberrechtsschutz bleibt daher langfristig eine wichtige Aufgabe. Kurz und mittelfristig sind neue Formen der **wirtschaftlichen und technischen Kooperation von Rechteinhabern und Diensteanbietern notwendig**, z. B. Aufklärung und **Warnhinweise**, technische Schutzmaßnahmen oder neue Geschäftsmodelle. Rechteinhaber und Diensteanbieter müssen stärker als bisher und unvoreingenommen über die Vor- und Nachteile der jeweiligen Maßnahmen reden. Der Ende des letzten Jahres begonnene und beim Bundesministerium für Wirtschaft und Technologie eingerichteten **Wirtschaftsdialog** für mehr Kooperation zur Bekämpfung der Internetpiraterie wird deshalb mit dem Ziel fortgeführt, gemeinsam mit allen Beteiligten zu ersten Lösungsansätzen in einem überschaubaren Zeitraum zu kommen.“²⁰ (Hervorhebungen diesseits).

²⁰ <http://www.bmwi.de/BMWi/Navigation/Wirtschaft/Branchenfokus/kultur-kreativwirtschaft,did=315898.html?view=renderPrint>.

Unterdessen wurde das rechtspolitische Ziel der Koalition in **der Berliner Rede zum Urheberrecht** der Bundesjustizministerin vom 14. Juni 2010²¹ präzisiert. Dort heißt es:

„Eine Alternative, die gerade unsere Nachbarn in Frankreich beschlossen haben, halte ich allerdings für einen falschen Weg. Nach der Devise "Three strikes and you are out" wird dort nun nach der dritten Urheberrechtsverletzung der Internet-Zugang eines Users für einen bestimmten Zeitraum gesperrt. Das ist keine Alternative, denn das ist ein tiefer Eingriff in die Kommunikationsfreiheit und kann angesichts der großen Bedeutung des Internets im Alltag eine harte Strafe sein. Das Kappen des Internet-Anschlusses ist zudem keine zielgenaue Sanktion. Bei einem Familienanschluss, den mehrere nutzen, würden alle für das Fehlverhalten eines Familienmitgliedes bestraft. Der Rechteverletzer könnte dagegen über jeden anderen Anschluss weiterhin ins Netz gehen. Netzsperrern setzen also an der falschen Stelle an. Die Bundesregierung wird daher keine Initiativen für Netzsperrern ergreifen, und es wird auch keine Bandbreitenbeschränkungen geben. Das will ich weder in Deutschland noch verpflichtend in der EU oder in internationalen Abkommen. Deshalb war es mir auch so wichtig, Transparenz in die Verhandlungen über das ACTA-Abkommen, das Abkommen gegen Fälscher und Raubkopierer, zu bringen. Das ist jetzt geschehen, die EU-Kommission hat die Dokumente offengelegt. Nun kann jeder sehen, in welche Richtung die Verhandlungen laufen, und für mich ist in einem Punkt klar: Netzsperrern wären die falsche Richtung.“

Weiter heißt es:

„Deshalb gibt es noch andere Vorschläge, dem Problem beizukommen. Ein Vorschlag zielt darauf ab, diejenigen, die eine Urheberrechtsverletzung begehen, frühzeitig zu warnen. Da würde dann etwa ein User den automatischen Hinweis auf seinen Bildschirm bekommen: "Hallo, was Du da gerade tust, ist illegal und verletzt das Urheberrecht".

Die Content-Industrie verspricht sich viel von einem solchen Ansatz und die Erfahrungen, die man in den USA damit gemacht hat, scheinen dies zu belegen. Wenn jemandem vor Augen geführt wird, dass er rechtswidrig handelt und welche Sanktionen ihm drohen, dann kann das durchaus eine erzieherische Wirkung haben. Wäre es da nicht besser, der Schüler, der den neuen Kinofilm aus dem Netz illegal herunter laden will, bekommt einen automatischen Warnhinweis statt eine Abmahnung mit Kostennote des Anwalts? Diese Frage muss man durchaus stellen.

Allerdings ist für mich eines ganz klar: Eine gesetzlich angeordnete Kontrolle des individuellen Surfverhaltens kann es nicht geben. Aus gutem Grund habe ich als Abgeordnete gegen die Vorratsdatenspeicherung beim Bundesverfassungsgericht geklagt. Das Warnhinweis-Modell kann deshalb nur dann in Betracht kommen,

²¹ http://www.bmj.de/SharedDocs/Reden/DE/2010/20100614_Berliner_Rede_zum_Urheberrecht.html.

wenn sich dies **technisch ohne eine Inhaltskontrolle und Datenerfassung** realisieren ließe.“ (Hervorhebungen diesseits).

Im weiteren Verlauf wurde unter dem Titel „**Ohne Urheber keine kulturelle Vielfalt**“ durch den Staatsminister für Kultur und Medien am 26. November 2010 ein Positionspapier zum Schutz des geistigen Eigentums im digitalen Zeitalter vorgelegt. Er äußerte und sich darin wie folgt zu einem Warnhinweismodell:

„Zur weiteren Verbesserung der Durchsetzung geistiger Eigentumsrechte in der digitalen Welt sollte der bestehende rechtliche Rahmen um ein effizientes System ergänzt werden, das es ermöglicht, einem (potentiellen) Verletzer einen Warnhinweis zu senden. Dann könnte dieser ohne juristische und finanzielle Konsequenzen sein illegales Handeln einstellen. Dabei muss jedoch sichergestellt sein, dass der verwarnete Nutzer bei wiederholter Rechtsverletzung mit einer **ernstzunehmenden Reaktion** zu rechnen hat (z. B. der kostenträchtigen **Abmahnung**).

Ein solches System hätte als **Ergänzung** zu den existierenden Möglichkeiten der zivilrechtlichen und gegebenenfalls strafrechtlichen Verfolgung den Vorzug, dass es den rechtswidrigen Nutzer zunächst über den Unrechtsgehalt seiner Tat aufklärt, ohne dass ihm sofort Sanktionen drohen. Insbesondere kann seitens der Rechteinhaber zunächst auf Abmahnungen verzichtet werden. Durch die Warnung wird der **Nutzer** beispielsweise über konkreten Missbrauch von drahtlosen Internetanschlüssen (W-LAN), aber auch die Sicherung der Verbindung, **aufgeklärt**. Darüber hinaus trägt die direkte Ansprache der Nutzer unmittelbar zur **Bewusstseinsbildung** über den Wert des geistigen Eigentums bei und fördert die Akzeptanz der Rechtsdurchsetzung in der Bevölkerung. Zuletzt könnte ein solches sanktioniertes Warnsystem durch einen standardisierten Ablauf unter Wahrung datenschutzrechtlicher Belange massentauglich ausgestaltet werden, ohne dabei Gerichte und Staatsanwaltschaften stärker zu belasten.“ (Hervorhebungen diesseits).

Im Oktober 2011 wurde zudem ein durch den CDU-Politiker *Siegfried Kauder*, dem Vorsitzenden des Rechtsausschusses im Deutschen Bundestag, für Ende November 2011 ein Gesetzesentwurf zu einem Warnhinweismodell, allerdings mit der Konsequenz von zeitlich begrenzten Zugangssperren, angekündigt.²²

2. Der Wirtschaftsdialog

Ausgehend von einem erheblichen Ausmaß an Urheberrechtsverletzungen im Internet und dadurch entstehenden wirtschaftlichen Schäden, rief das Bundesministerium für Wirtschaft und Technologie Ende 2008 im Rahmen der Initiative Kultur- und Kreativwirtschaft

²² Interview in Promedia Heft 11, 2011, S. 5. <http://www.promedia-berlin.de/fileadmin/Archiv/2011/11/promedia201111-online01.pdf>.

der Bundesregierung einen Wirtschaftsdialog „für mehr Kooperation bei der Bekämpfung der Internetpiraterie“ ins Leben. Unter Beteiligung von Rechteinhabern und Internetzugangsanbietern werden im Rahmen dieses Dialogs Möglichkeiten der Zusammenarbeit bei der Bekämpfung von Internetpiraterie diskutiert.

Von Seiten der Rechteinhaber wird u.a. die Schaffung eines Warnhinweismodells gefordert.²³ Nach einem solchen Modell würden Internet-Zugangsanbieter auf Veranlassung der Rechteinhaber Warnhinweise an diejenigen ihrer Kunden versenden, deren IP-Adresse von den Rechteinhabern zuvor im Zusammenhang mit Rechtsverletzungen ermittelt wurde. Der unter dem **3. Mai 2011** veröffentlichte Vorschlag für ein „sanktioniertes Aufklärungs- und Warnhinweismodell“ lautet wie folgt:

„Schließlich setzen sich die Rechteinhaber für eine alternative Rechtsverfolgung von Urheberrechtsverletzungen durch Nutzer ein und haben im Rahmen des Wirtschaftsdialogs für mehr Kooperation bei der Bekämpfung der Internetpiraterie ein dem technischen Umfeld des jeweiligen illegalen Angebots angepasstes, sanktioniertes Aufklärungs- und Warnhinweismodell als eine kooperative Maßnahme mit der Internetwirtschaft diskutiert. Dieses steht **selbstständig neben** dem gerichtlichen Verfahren nach § 101 UrhG (**Auskunftsanspruch**).

Ein solches Warn- und Hinweismodell kann fair und effizient unter Berücksichtigung datenschutzrechtlicher Belange technologieneutral ausgestaltet werden – und damit **neben den Tauschbörsen auch andere Formen der Internetpiraterie** erfassen. Es kann die Medienkompetenz fördern und trägt zu einem aktiven Verbraucherschutz bei. Ein solches Verfahren kann eine direkte Beziehung zwischen Internetservice Providern und Rechteinhabern oder ein Drei-Parteien-System vorsehen, bei dem zwischen Internetservice Providern und Rechteinhabern eine **unabhängige zentrale Stelle** geschaltet ist.

Im Falle eines **wiederholten Rechtsverstoßes** erfolgt dabei eine **ernstzunehmende Sanktion** gegen den Nutzer, die **auch technischer Art** sein kann. Nachfolgend wird das Modell einer unabhängigen zentralen Stelle dargestellt, das zahlreiche Vorteile bietet. Konkrete Fragen der Organisationsstruktur sind dabei noch zu klären.

- Eine unabhängige zentrale Stelle bildet die Schnittstelle zwischen Rechteinhaber und Telekommunikationsunternehmen und legt Standards für die Legitimation der Rechteinhaber und die Ermittlung der Urheberrechtsverletzung fest.
- Der Rechteinhaber hat sich bei der zentralen Stelle zu registrieren.

²³ Vorschläge der Rechteinhaber im Rahmen des Wirtschaftsdialogs für mehr Kooperation bei der Bekämpfung der Internetpiraterie im BMWi, Kurzfassung v. 3.5.2011, S. 6 f., abrufbar unter: https://www.gema.de/fileadmin/user_upload/Presse/Publikationen/Kurzfassung_Dialogpapier.pdf (letzter Zugriff: 15.8.2011).

- Der Rechteinhaber dokumentiert die Rechtsverletzung nach den etablierten Grundsätzen.
- Die zentrale Stelle prüft den Antrag und nimmt die Angaben in eine Datenbank auf.“²⁴

Die Rechteinhaber erhoffen sich von einem solchen Vorgehen, Urheberrechtsverletzungen im Internet signifikant eindämmen zu können. Ihr erster – im Rahmen des Wirtschaftsdialogs vorgelegter – **Modellvorschlag** für ein „sanktioniertes Aufklärungs- und Warnhinweismodell“ sieht also zusammengefasst ein Antragsverfahren vor einer einzurichtenden zentralen Stelle vor. Die Aufgabe dieser Einrichtung wäre es, nach den von ihr festgesetzten Standards die Legimitation der Rechteinhaber und die behauptete Urheberrechtsverletzung zu prüfen und die entsprechenden Daten in einer Datenbank zu sammeln. Von den Telekommunikationsunternehmen würden die betroffenen Anschlussinhaber ermittelt und diesen eine Aufklärungs- und Hinweis-Nachricht übersandt. Soweit sich aus der Datenbank eine Mehrzahl von Verstößen desselben Anschlussinhabers ergibt, soll durch die zentrale Stelle auch eine Information an den Rechteinhaber erfolgen. Bei wiederholten Rechtsverstößen sollen Sanktionen gegen den Nutzer möglich sein.

Auf freiwilliger Basis wird ein solches oder ähnliches anlassbezogenes Warnhinweismodell von den Telekommunikationsdiensteanbietern abgelehnt.²⁵

III. Auftrag, Ziel und Vorgehensweise der Studie

Das Bundesministerium für Wirtschaft und Technologie nennt in der Projektbeschreibung zur Ausschreibung der Studie folgende Aufgaben und Ziele der Untersuchung:

„Aufgaben/ Ziele:

Überlegungen in Hinblick auf etwaige gesetzgeberische Maßnahmen müssen Erkenntnisse über die Erfahrungen in den anderen EU- Mitgliedstaaten berücksichtigen. Die Verbesserung des Urheberrechtsschutzes im Internet ist Gegenstand des Koalitionsvertrages für die laufende Legislaturperiode. Dabei stellen Internetsperren aus Sicht des Bundesministeriums für Wirtschaft und Technologie kein adäquates Mittel dar. Zugleich gilt es auch, die Belange des Datenschutzes und des Fernmeldegeheimnisses angemessen zu berücksichtigen.

Ziel des Vorhabens ist die Gewinnung von Erkenntnissen über gesetzliche Regelungen zur Bekämpfung der Internetpiraterie im Netz mittels der Versendung von Warnhinweisen in anderen EU- Mitgliedstaaten und ihre Auswirkungen. Dazu

²⁴ https://www.gema.de/fileadmin/user_upload/Presse/Publikationen/Kurzfassung_Dialogpapier.pdf. Hervorhebungen diesseits.

²⁵ Vgl. etwa jüngst *Süme*, <http://www.lto.de/de/html/nachrichten/5062/pro-und-contra-warnhinweismodell-ein-streit-ueber-den-umgang-mit-fileshearn/>.

- soll dargestellt werden , wie sich in Europa das Piraterieverhalten im Netz in den letzten zwei Jahren entwickelt hat, welche Entwicklungstendenzen absehbar sind, welche wirtschaftlichen Auswirkungen bestehen und welche Branchen hiervon besonders betroffen sind;
- sollen die in den EU- Mitgliedstaaten geregelten bzw. geplanten Modelle zu Warnhinweisverfahren dargestellt und miteinander verglichen werden, wobei die datenschutzrechtlichen Sicherungen besonders herausgestellt werden sollen (die Gesetze bzw. Gesetzesentwürfe sind in deutscher Übersetzung beizufügen);
- sollen die bisherigen Praxiserfahrungen ausgewertet werden - insbesondere im Hinblick auf die Anzahl der versendeten Warnhinweise, ihre Auswirkung auf den Umfang der Urheberrechtsverletzungen und die ggf. damit verbundenen Auswirkungen auf die Umsätze der betroffenen Medienindustrie, die mit den Maßnahmen verbunden finanziellen Belastungen der Internet- Zugangsvermittler sowie der Rechteinhaber, die Verteilung der Kosten und die Art und den Umfang der gegen Nutzer ergriffenen technischen Sanktionen;
- soll die praktische Relevanz von Auskunftsansprüchen gegen Vermittler sowie die zivilrechtliche Durchsetzung von Urheberrechten im außergerichtlichen Verfahren bei der Bekämpfung von Urheberrechtsverletzungen im Internet (auch im Vergleich zu Deutschland) dargestellt sowie untersucht werden, ob und inwieweit Warnhinweismodelle einen zusätzlichen und maßgeblichen Beitrag zur Bekämpfung zu Internetpiraterie leisten;
- soll untersucht werden, ob und inwieweit Warnhinweismodelle mit Blick auf das sich ändernde Nutzerverhalten ein zukunftsgerichtetes Instrument zur Bekämpfung von Urheberrechtsverletzungen im Internet darstellen.“

Die vorliegende Studie untersucht und evaluiert daher bereits vorhandene Modelle zur Versendung von Warnhinweisen durch Zugangsanbieter. Berücksichtigt werden solche Warnhinweisregelungen, die in anderen EU-Mitgliedstaaten bereits in Kraft getreten sind, verabschiedet oder auf Ebene des nationalen Gesetzgebers konkret geplant sind. Dies ist namentlich das bereits existente Verfahren in Frankreich. Im Vereinigten Königreich ist ein Modell verabschiedet, aber noch nicht in Kraft. In anderen EU-Mitgliedstaaten (Finnland und Belgien) existieren Gesetzesentwürfe, die aber nicht umgesetzt wurden. In Irland werden Warnhinweise mit der Folge von Sanktionen durch den größten Provider auf freiwilliger Basis versandt. Die Analyse gibt Aufschluss über die Ausgestaltung und die Implementierung der Modelle im jeweils nationalen Recht. Betreffend die Modelle, die bereits umgesetzt sind, sind zudem deren Wirkweise sowie deren mögliche Auswirkungen näher untersucht.

Diese Studie befasst sich auftragsgemäß ausdrücklich **nicht** mit der Option der **Sperrung** von Internetinhalten oder Internetzugängen. Die hier auftretenden Rechtsfragen werden

aber zum Teil zur Abgrenzung mit behandelt und weil Rechtsfragen betroffen sind, die auch bei Sperrungen tangiert wären, zum Beispiel die Speicherung einer IP-Adresse.

1. Vorgehensweise

Methodisch wurde zunächst die Ausgangslage in den Blick genommen. Es wurden Hintergründe, Ursachen und Auswirkungen von Urheberrechtsverletzungen analysiert sowie gängige Sachverhalte der Urheberrechtsverletzungen im Internet technisch beleuchtet und rechtlich bewertet. Hieran anschließend erfolgte die vergleichende Analyse im europäischen Ausland bereits vorhandener bzw. konkret diskutierter gesetzlicher Regelungen und Entwürfe zu Warnhinweismodellen. Der Untersuchung wurde eine Auswertung vorliegender Daten über die Wirkung der bereits umgesetzten Modelle angeschlossen. Der Evaluation gewonnener praktischer Erfahrungen wurde insofern primär das französische Modell zugrunde gelegt, weil dort eine entsprechende gesetzliche Regelung bereits in Kraft ist und insoweit bereits Erkenntnisse über die Wirksamkeit des Modells gewonnen werden konnten. Weiterhin von besonderer Bedeutung war Irland. Hier wird ein Modell praktiziert, das zwar gesetzlich nicht implementiert ist, aber dennoch vom wichtigsten Zugangsanbieter als Ergebnis eines Vergleichs angewendet wird. Auch auf dieser Basis liegen erste Erfahrungen über Wirkung und Akzeptanz von Warnhinweisen vor. Neben der Effektivität (Wirksamkeit) und Effizienz der Modelle wurde besonderes Augenmerk auch auf wirtschaftliche Implikationen gelegt. Zudem wurde der Frage nachgegangen, ob und inwieweit sich positive Auswirkungen für das kreative Schaffen in Form von Rechtssicherheit und Akzeptanz des Modells abzeichnen. In einer abschließenden Bewertung im Rahmen einer Verhältnismäßigkeitsprüfung wurden schließlich auch zu den Warnhinweismodellen alternative Rechtsschutzinstrumente berücksichtigt.

a. Datenerhebung

Grundlage der Datenauswertungen bildete das vorhandene und bis zum Ablauf der Studie vorliegende öffentlich zugängliche Datenmaterial. Primärdatenerhebung wurde nicht vorgenommen. Datenquellen sind namentlich veröffentlichte Erhebungen von staatlichen und anderen Stellen. Einbezogen in die Datenerhebung wurden insbesondere auch von den Beteiligten (Rechteinhaber, Contentanbieter, Zugangsanbieter, Nutzer) und ihren Interessenverbänden erstellte oder in Auftrag gegebene Studien sowie Stellungnahmen und weitere Informationen und Auskünfte, etwa aus einem Telefoninterview mit der Präsidentin der Hadopi vom 23. November 2011. Hierbei ist zu berücksichtigen, dass die Datenlage zur jüngsten Vergangenheit begrenzt ist. Auch aktuelle Studien basieren weitgehend auf der Erhebung von Daten aus den Jahren 2008 und davor liegenden Zeiträumen. Eine Einschätzung auch der Tendenzen lässt sich den vorliegenden Daten jedoch bereits entnehmen. Von Seiten des Auftraggebers wurden die Teilnehmer des Wirtschaftsdialogs vor Be-

ginn der Bearbeitung der Studie auf die Möglichkeit hingewiesen, Datenmaterial zur Verfügung stellen zu können.

b. Rechtsvergleich

Die rechtlichen Regelungen zu den vorgefundenen Warnhinweismodellen wurden zunächst jeweils für sich untersucht und dargestellt. Schwerpunkt bildete hier das geltende französische Recht und die Entwürfe im Vereinigten Königreich sowie in Finnland und Belgien, sowie das Modell in Irland. Ergänzend zu den rechtlichen Vorgaben für das jeweilige Warnhinweismodell wurde eine Einordnung der jeweiligen rechtlichen Vorgaben in den rechtlichen Gesamtkontext des nationalen Rechts vorgenommen. Dabei fand neben einer Einordnung der verfassungsrechtlichen Implikationen insbesondere das jeweilige nationale Datenschutzrecht im Hinblick auf die jeweils mit dem Modell einhergehende Datennutzung Berücksichtigung. Die Funktionsweise der Warnhinweisregelungen wurde miteinander verglichen und erste Erkenntnisse für einen denkbaren Ansatz im deutschen Recht gewonnen.

c. Methode der Rechtsvergleichung

Ausgangspunkt der vorliegenden Studie ist die Frage, ob und inwieweit die Warnhinweismodelle in anderen europäischen Ländern der Verfolgung bzw. Verhinderung von Urheberrechtsverletzungen im Internet und somit einer verbesserten Durchsetzung von Urheberrechten in der digitalen Welt Rechnung tragen²⁶.

Die rechtsvergleichende Perspektive zielt auf Erkenntnisse über die Funktionsweise der Warnhinweismodelle in verschiedenen Rechtsordnungen. Die Betrachtung des fremden Rechtssystems lässt dessen Eigenheiten, aber auch Vor- und Nachteile der Herangehensweise der jeweiligen Rechtsordnung an die Frage der Bekämpfung von Urheberrechtsverletzungen im Internet sichtbar werden. Die Analyse hat eine mögliche Verwendung von Teilen vorgefundener Lösungen in die eigene nationale Rechtsordnung zum Ziel. Durch die vergleichende Analyse sollen Erkenntnisse zu einer möglichen Implementierung eines Warnhinweismodells in das deutsche Recht gewonnen werden²⁷.

Die Auswahl der Rechtsordnungen, die in den Rechtsvergleich einbezogen werden, richtet sich an dem konkret verfolgten Ziel des Vergleichs aus²⁸, nämlich der Gewinnung von Erkenntnissen für eine mögliche gesetzliche Regelung in Deutschland. Vor diesem Hinter-

²⁶ Bei rechtsvergleichenden Arbeiten ist die Fragestellung anhand des Prinzips der Funktionalität zu formulieren. Es besagt, dass solche Rechtsinstitute vergleichbar sind, die funktionsverwandt sind, weil sie dasselbe Problem ansprechen. Ansatzpunkt jeder Rechtsvergleichung ist also ein konkretes Sachproblem (hier: Urheberrechtsverletzungen in Internet). Dazu: *Zweigert/Kötz* § 3 II, S. 33 ff.; *Rösler JuS* 1999, S.1186 ff.; *Brand JuS* 2003, S.1086; *Rheinstein* S. 31 ff.

²⁷ Zu den Zielen der Rechtsvergleichung *Sommermann DÖV* 1999, S. 1019 ff.; *Sacco* § 1, S. 13 ff.; *Constantinesco* Band II, S. 331 ff.

²⁸ So *Constantinesco* Band II, S. 49 ff. Vgl. auch *Zweigert/Kötz* § 3 IV, S. 40 ff.

grund bieten sich für den Rechtsvergleich vor allem Frankreich, England, Irland, bedingt auch Belgien und Finnland sowie in gewisser Weise Schweden an. Zwar gehören diese Länder zu unterschiedlichen Rechtskreisen²⁹. Der Grund für deren Einbeziehung in den Vergleich liegt darin, dass in einem dieser EU-Mitgliedstaaten bereits ein Gesetz in Kraft ist (Frankreich) bzw. bevorsteht (England). In anderen existieren entsprechende Gesetzesentwürfe zur Bekämpfung der Urheberrechtsverletzungen im Internet durch Versendung von Warnhinweisen, die aber nicht weiter verfolgt wurden bzw. werden. In Irland wird ein Warnhinweismodell zwar nicht gesetzlich geregelt, wird aber von den Zugangsanbietern angewendet. Zudem wird kurz auf außereuropäische Staaten eingegangen.

In einem ersten Schritt befasst sich die Studie mit der Auswertung von Studien und Untersuchungen zu den Ursachen und Auswirkungen von Internetpiraterie. Im nächsten Schritt werden die ausländischen Lösungsansätze bzw. die Warnhinweis-Regelungen in ihrem jeweiligen Kontext dargestellt und analysiert. Der vergleichende Teil setzt sich sodann im Hinblick auf die Effizienz von Warnhinweisen mit den Auswirkungen der untersuchten Regelungen für der Piraterieverhalten auseinander. Das Herausarbeiten von Unterschieden und Gemeinsamkeiten erfolgt, indem Betrachtungen zu Einzelaspekten aus technischer, pädagogischer, informationeller und wirtschaftlicher Perspektive angestellt werden. Die herausgearbeiteten Unterschiede und Gemeinsamkeiten werden analysiert und die wesentlichen Gründe hierfür werden offen gelegt und bewertet³⁰. Rechtsvergleichende Aspekte finden sich darüber hinaus in weiteren Teilen der Studie, soweit dies der Sache nach geboten war. Im nächsten Schritt werden die innerstaatliche Durchsetzung des Urheberrechts in Deutschland einschließlich des Auskunftsanspruchs untersucht. Im abschließenden 2. Teil der Studie wird ein mögliches Modell der Warnhinweisversendung vorgestellt und einer ersten rechtlichen Begutachtung unterzogen.

IV. Aufbau der Studie

Die Studie gliedert sich in zwei Teile. Teil 1 befasst sich mit vorhandenen Grundlagen, also der Ausgangslage, dem Rechtsvergleich und den aktuellen Möglichkeiten zur Bekämpfung von Urheberrechtsverletzungen im Internet. Teil 2 ist befasst sich mit einer möglichen Handlungsoption und ordnet diese in den Kontext des internationalen und innerstaatlichen Rechts ein.

²⁹ Zu den Rechtskreisen vgl. *Zweigert/Kötz* § 3 IV, S. 40 ff.; *Rösler JuS* 1999, S.1187 ff.; *Brand JuS* 2003, S. 1088 ff.

³⁰ Zu den Gründen ausführlich *Constantinesco* Band II, S. 292 ff., der feststellt, dass die Gründe nicht immer im rechtlichen Bereich liegen müssen, sie können vielmehr historischer, wissenschaftlicher, politischer oder gesellschaftlicher Art sein.

1. Ausgangslage und Status quo (1. Teil, A und B)

Den Ausgangspunkt der Studie bildet nach der Beschreibung der Ausgangslage in Teil A die gegenwärtige tatsächliche Situation der Urheberrechtsverletzungen im Internet. Im Einzelnen wird unter Teil B der Studie beschrieben und analysiert, wie sich die rechtswidrige Nutzung geschützter Inhalte im Internet im Untersuchungszeitraum entwickelt hat und in welcher Form Rechtsverletzungen im Netz in Erscheinung treten. So können Urheberrechte, etwa bei der Nutzung von Tauschbösen/Peer-to-Peer Filesharing (P2P), Cyberlockern/Sharehostern, Streaming-Portalen etc., verletzt werden. Die Beschreibung dieser unterschiedlichen Phänomene stellte sich als erforderlich dar, weil dargelegt werden muss, welche Erscheinungsformen von Rechtsverletzungen durch Warnhinweis-Regelungen erfasst bzw. nicht erfasst werden. Mit Blick auf die im Rahmen der Studie später zu erläuternde Frage der Effektivität einer Regelung werden zudem die möglichen Ursachen für das rechtswidrige Verhalten der Nutzer analysiert. Ferner werden die wirtschaftlichen Auswirkungen der Rechtsverletzungen sowie die Branchen dargestellt, die von Rechtsverletzungen besonders betroffen sind. In einem weiteren Schritt werden absehbare Entwicklungstendenzen beschrieben, die sich in Bezug auf das Verhalten der Nutzer, das Angebot rechtswidrig nutzbarer Dienste und das Spektrum der digitalen Verwertung urheberrechtlich geschützter Inhalte abzeichnen.

2. Warnhinweismodelle in anderen EU-Mitgliedstaaten (1. Teil C)

Im Teil C werden anlassbezogene Warnhinweisregelungen beschrieben und miteinander verglichen. Im Fokus stehen dabei die in Frankreich umgesetzten Regelungen. Berücksichtigt sind aber auch das britische Gesetz sowie Gesetzesentwürfe, wie sie in einigen EU-Mitgliedstaaten diskutiert werden oder wurden sowie das in Irland praktizierte Modell, welches auf einem Kompromiss innerhalb der Privatwirtschaft basiert. Die jeweiligen Regelungen werden im wesentlichen nach der systematischen Verortung der Warnhinweis-Regelung, dem Regelungsziel, dem Anwendungsbereich sowie dem Inhalt der jeweiligen Regelung im Detail dargestellt und erläutert. In diesem Zusammenhang untersucht die Studie auch Aspekte der praktischen Umsetzung des jeweiligen Warnhinweismodells. Dies betrifft insbesondere die Tatbestandsvoraussetzungen für das Eingreifen der Regelung, den Ablauf des Meldeverfahrens und der Warnhinweiserteilung; außerdem werden Sanktionen und Rechtsschutzmöglichkeiten in den Blick genommen. Weiterhin geht es um die Regelungen zur Kostenverteilung. Die relevanten datenschutzrechtlichen Anforderungen in den EU-Referenzstaaten werden dabei nicht gesondert erörtert, sondern im Verlauf des Textes zum jeweiligen Staat abgehandelt.

3. Evaluation der Wirksamkeit vorhandener Warnhinweisregelungen (1. Teil D)

In einem weiteren Schritt schließt sich der Gesetzesanalyse die Evaluation der anlassbezogenen gesetzlichen Warnhinweis-Regelungen als Mittel zur Bekämpfung von Rechtsverletzungen an. Grundlage bilden die bisherigen Erfahrungen in der Praxis der jeweiligen EU-Mitgliedstaaten mit entsprechenden Vorschriften. Besonderes Augenmerk wird daher auch hier auf das bereits geltende gesetzliche Modell in Frankreich gelegt, wo erste Praxiserfahrungen vorliegen. Erfahrungswerte liefert zudem das in Irland freiwillig praktizierte Warnhinweismodell. Erkenntnisse im Vereinigten Königreich, die aus Vorabbefragungen mit Bezug auf eine etwa kommende Warnhinweis-Regelung resultieren, werden ebenfalls berücksichtigt. Auf dieser Grundlage werden die Auswirkungen der Gesetzesbestimmungen für die einzelnen Bezugsgruppen (Rechteinhaber, Content-Anbieter, Internetzugangsanbieter und Nutzer) sowie die gesamtwirtschaftlichen und gesellschaftlichen Auswirkungen der Vorschriften in Bezug genommen. Dargestellt wird, ob und inwieweit das jeweilige nationale Modell zu einem Rückgang von Urheberrechtsverletzungen im Netz geführt hat und welche Ursachen hierfür als maßgebend zu betrachten sind. Als wesentlicher Aspekt für die Bewertung des jeweiligen Warnhinweismodells unter dem Gesichtspunkt der Wirksamkeit werden die mit ihm verbundenen tatsächlichen finanziellen Belastungen für Internet-Zugangsanbieter, Rechteinhaber und Content-Anbieter erörtert. Zudem finden namentlich für Frankreich die Fragen Erörterung, wie häufig im Anschluss an die Versendung Warnhinweisen noch gerichtliche Verfahren gegen Nutzer eingeleitet wurden und wie häufig ein Gerichtsverfahren mit Sanktionen gegen Nutzer endete.

4. Erfordernis der Einführung eines Warnhinweismodells vor dem Hintergrund des aktuellen Urheberrechts (1. Teil E.)

Im Rahmen von Teil E wird untersucht, ob und inwieweit durch Auskunftsverlangen und zivilrechtliche Durchsetzung von Urheberrechten gegenwärtig ein hinreichender Schutz gegen Urheberrechtsverletzungen im Netz besteht. Hieraus können Schlüsse darauf gezogen werden, ob und inwieweit gesetzlich verankerte Warnhinweismodelle einen zusätzlichen und maßgeblichen Beitrag (Mehrwert) zur Aufklärung über Urheberrechtsverletzungen im Internet und die Bekämpfung von rechtswidrigem Nutzerverhalten im Internet sowie zur Schaffung von Rechtsfrieden und Rechtssicherheit leisten können. Die Studie untersucht daher eingehend die vorhandenen Durchsetzungsmöglichkeiten zum Schutz von urheberrechtlich geschützten Inhalten im Netz. Dazu zählen insbesondere die rechtlichen Grundlagen und praktischen Auswirkungen von Auskunftsansprüchen gegen Internet-Zugangsanbieter sowie die zivilrechtliche Durchsetzung von Urheberrechten im außegerichtlichen Verfahren.

5. Erwägungen zu einem innerstaatlichen Ansatz (2. Teil)

In einem zweiten Teil der Studie werden unter Berücksichtigung der gefundenen Ergebnisse grundlegende rechtliche Parameter benannt, die bei Implementierung eines Warnhinweismodells in Deutschland berücksichtigt werden müssten und Gedanken zu einem entsprechenden Ansatz vorgestellt. Hierbei werden die Rechtspositionen der von einer derartigen Regel betroffenen, nämlich der Rechteinhaber, der Zugangsanbieter und der Nutzer soweit sie für den Ansatz relevant sind berücksichtigt. In diesem Zusammenhang wird der Ansatz ausgehend von einer Darstellung des völker- und europarechtlichen Rahmens des Urheber- und Datenschutzrechts und einfachgesetzlichen innerstaatlichen Parameter einer kursorischen verfassungsrechtlichen Prüfung unterzogen. Zudem werden die Fragen der Verhältnismäßigkeit des Warnhinweissystems unter Berücksichtigung von Legitimität, Eignung, Erforderlichkeit und Angemessenheit untersucht.

ENTWURF/ VERTRAULICH

B. Status quo

I. Vorbemerkung zur Methodik im Rahmen der Untersuchung

Diese Studie basiert in tatsächlicher Hinsicht auf Ergebnissen öffentlich zugänglicher Studien, die unterschiedlich ausgerichtet sind und verschiedene Aspekte in den Fokus nehmen. Teilweise sind sie von staatlicher Stelle³¹, größtenteils aber im Auftrag von Interessengruppen erstellt worden. Sie legen zum Teil repräsentative Teilnehmerbefragungen zugrunde und werten zudem statistische Wirtschaftsdaten aus. Bei der Auswertung war zu berücksichtigen, dass im Internet begangene Rechtsverstöße keine physisch mess- und auswertbaren Spuren hinterlassen. Zum Teil messen die Studien zur Ermittlung des illegalen Nutzungsverhaltens das Aufkommen des Internetverkehrs. Allerdings können Messergebnisse, etwa im Hinblick auf erhöhten Datendurchsatz³², auch Gründe haben, die nicht auf illegale Nutzung zurückzuführen sind.³³ Darüber hinaus sind methodische Besonderheiten zu berücksichtigen. So werden in den Studien teilweise unzureichende Angaben zu Methodik bzw. Datenbasis gemacht. Dabei geht man methodisch unterschiedlich vor, teilweise ohne die Bewertungsmethoden offen zu legen. Zu berücksichtigen ist auch, dass Recherchen zu der Thematik von der betroffenen Industrie bzw. interessierter Seite finanziert wurden.³⁴

II. Erscheinungsformen urheberrechtlich relevanter Handlungen im Internet

Urheberrechtsrelevante Handlungen erfolgen auf verschiedene Weise. Am meisten werden das sog. Usenet, P2P-Filesharing-Börsen, Sharehostingangebote, Streamhostingangebote im Zusammenhang mit nicht autorisierten Filmportalen sowie moderne Aufnahmemöglichkeiten im Internet genutzt. Im Folgenden sei die Funktionsweise dieser

³¹ Im Vereinigten Königreich wurden im Rahmen eines staatlichen *Impact Assessment* die wirtschaftlichen Auswirkungen des gesetzgeberischen Unterlassens der Pirateriebekämpfung erhoben. In einer unabhängigen vom britischen Premierminister in Auftrag gegebenen Studie zum gesetzlichen Rahmen des geistigen Eigentums im Vereinigten Königreich wurden bereits vorhandene Studien zur Online-Piraterie analysiert und bemängelt, dass verlässliche Zahlen lediglich in überraschend geringer Anzahl vorhanden seien. *Hargreaves*, S.69.

³² Bspw. die Studie von *Adermon/Liang*, welche etwa einen Rückgang des Internetverkehrs in Schweden mit einer Gesetzesänderung im Hinblick auf die Rechtsverfolgung von Urheberrechtsverstößen im Internet erklärt.

³³ So auch *Hargreaves*, S. 69.

³⁴ *Karaganis*, S. 1.

Dienste erläutert.³⁵ Dabei ist zu berücksichtigen, dass die Nutzung der Dienste sowohl zu legalen, als auch zu illegalen Zwecken möglich ist und auch erfolgt.

1. Usenet

Das weltweite Kommunikationsnetzwerk Usenet setzt sich aus zahlreichen miteinander verbundenen Newsservern zusammen. In einem automatisierten Verfahren wird der Datenbestand ständig gespiegelt und redundant auf den Servern vorgehalten. Nachrichten zu diversen Themen können wie auf einem „schwarzen Brett“ in hierarchisch untergliederten Newsgroups gespeichert werden. Der prinzipiell jedem offenstehende Zugang zu einer Newsgroup erfolgt über einen der Newsserver mittels eines sog. Newsreaders. Es handelt sich dabei um ein auf dem Rechner des Nutzers installiertes Programm, das über das Internet zu dem adressierten Newsserver Kontakt aufnimmt. Auf diesem listet es die dort gespeicherten Newsgroups auf. Dadurch können die Nutzer der Newsgroups Beiträge Dritter abrufen und eigene Beiträge einstellen. Es kann auf veröffentlichte Artikel geantwortet und es können eigene Nachrichten verfasst werden. Postings mit Dateianhängen³⁶ können in sog. Binary Newsgroups bereit gestellt werden. Dabei handelt es sich meist um (Audio-, Video- oder Bilddateien). Ein Usenet-Download ist in der Regel kostenpflichtig, wobei man nach Dateigröße und Download oder pauschal zahlt.³⁷

Binary Newsserver werden teilweise von Providern selbst betrieben. Zum Teil wird auch lediglich der Zugang hierzu vermittelt, indem Newsreadersoftware zur Verfügung³⁸ gestellt wird. Die Suche nach bestimmten Inhalten, z.B. einem Musiktitel, wird über Kopfzeilen (Header) mit Informationen über die Inhalte des Postings ermöglicht.³⁹ Wenn ein Nutzer einen Beitrag sendet, wird dieser zunächst nur auf dem kontaktierten Newsserver in der dortigen Newsgroup bereit gestellt. Das Spiegeln der Daten ermöglicht es, die Nachricht schnell von den weltweit vorhandenen Newsservern abzurufen.⁴⁰ Bis Inhalt und Anhänge

³⁵ Dazu eingehend *Schwartzmann*, Sharehosting, Filesharing & Co, K&R Beihefter 2/2011.

³⁶ Die Übertragung der Daten erfolgt anhand des *Network News Transfer Protocol* (NNTP). Größere Dateien müssen dabei in mehrere Teilnachrichten aufgespalten werden. Nach Umwandlung in der Art eines Textdokuments – und damit in einer als Musik- oder Bilddatei nicht wiedergabefähigem Format – werden sie transportiert und auch entsprechend auf den Servern gespeichert. Die Wiedergabe dieser Dateien ist erst möglich, wenn sie in das Ausgangsformat rückumgewandelt worden sind. Dies geschieht automatisch; vgl. *OLG Hamburg* Ur. v. 28.1.2009 – 5 U 255/07 (Alphaload / Usenet II) Rn.5; vgl. *Auch High Court of Justice Twentieth Century Fox Film Corp. et al. v. British Telecommunications PLC* [2011] EWHC 1981 (Ch) Rn. 27 ff., 32.

³⁷ Vgl. <http://www.usenet.de/server.cfm>.

³⁸ Vgl. *OLG Hamburg* Ur. v. 14.01.2009 - 5 U 113/07, MMR 2009, 631 (Spring nicht / Usenet I) und *OLG Hamburg* Ur. v. 28.1.2009 – 5 U 255/07 (Alphaload / Usenet II).

³⁹ Vgl. *OLG Hamburg* Ur. v. 28.1.2009 – 5 U 255/07 (Alphaload / Usenet II) Rn.7; siehe auch *Ritterhoff/Neubert*, in: *Widmaier*, *Anwaltshandbuch Strafverteidigung*, Kap. 80, Rn. 120 ff.

⁴⁰ Vgl. *OLG Hamburg* Ur. v. 28.1.2009 – 5 U 255/07 (Alphaload / Usenet II) Rn.5; *Sieber*, in: *Hoeren/Sieber*, *Handbuch Multimediarecht*, Teil 1, Rn. 150; *Ritterhoff/Neubert*, in: *Widmaier*, *Anwaltshandbuch Strafverteidigung*, Kap. 80, Rn. 119.

erst nach einer Nutzeranforderung geladen und für einen begrenzten Zeitraum gespeichert werden, ist nur ein Header auf den anderen Newsservern abgelegt.⁴¹ Diensteanbieter können Daten auf ihren Servern löschen oder sperren, sie können aber keine Datenbestände aus dem Usenet eliminieren⁴². Diese bleiben auf Newsservern anderenorts verfügbar.⁴³ Allein auf dem Server, auf dem sie ursprünglich gespeichert wurden, können sie nachhaltig entfernt werden.⁴⁴ Über eine entsprechende Angabe im Header des Postings ist der Betreiber des Ausgangsservers ermittelbar. Bis hin zum ersten Speicherort im Usenet werden dort alle Newsserver aufgelistet, die der Beitrag durchlaufen hat.⁴⁵ Die Dateien können vom Betreiber des Ausgangsservers per sog. Cancel-Anweisung auch auf anderen Servern gelöscht werden⁴⁶, wenn die Newsserver entsprechend konfiguriert sind.⁴⁷ Wenn der Beitrag über einen Remailer⁴⁸ zur Entpersonalisierung eingespeist wurde, kann der ursprüngliche „Uploader“ eines rechtsverletzenden Usenet-Beitrags auch über die Angaben im Header nicht festgestellt werden.⁴⁹

2. P2P-Filesharing

Unter illegalem Filesharing versteht man das „Tauschen“ – oder technisch richtig „Kopieren“ – von urheberrechtlich geschützten Werken, wie Musik, Filme, Spiele oder Computerprogramme ohne Zustimmung der Rechteinhaber in sogenannten „Internettauschbörsen“. Die ersten Filesharing-Netzwerke ermöglichten Suchanfragen noch über einen zentralen Server⁵⁰. Moderne Filesharing-Netzwerke nutzen ein dezentrales Peer-to-Peer-Netzwerk (P2P-Netzwerk).⁵¹ Hier schließen sich Nutzer mit ihren Rechnern zu einem Netzwerk zusammen, in dem Daten zum Kopieren zur Verfügung gestellt werden.⁵² Wer einen Inhalt herunterlädt, stellt ihn i.d.R. zugleich auch zur Verfügung. Damit sind die Nutzer mit ihren

⁴¹ Vgl. *OLG Düsseldorf* Ur. v. 20.5.2008 – I- 20 U 196/07, K&R 2008, 183 (im entschiedenen Fall ist die Nachricht 32 Stunden gespeichert gewesen); *LG München I* Ur. v. 19.04.2007 – 7 O 3950/07, MMR 2007, 453, 454 (Vorhaltezeit 30 Tage).

⁴² Vgl. *OLG Düsseldorf* Ur. v. 20.5.2008 – I- 20 U 196/07, K&R 2008, 183.

⁴³ *Sieber*, in: *Hoeren/Sieber*, Handbuch Multimediarecht, Teil 1, Rn.151; *OLG Düsseldorf* Ur. v. 20.05.2008 – I- 20 U 196/07, K&R 2008, 183.

⁴⁴ Vgl. *OLG Hamburg* Ur. v. 28.1.2009 – 5 U 255/07 (Alphaload / Usenet II) Rn. 8; *OLG Hamburg* Ur. v. 14.01.2009 – 5 U 113/07, MMR 2009, 631, 632 (Spring nicht / Usenet I).

⁴⁵ Siehe dazu auch *Ritterhoff/Neubert*, in: *Widmaier*, Anwaltshandbuch Strafverteidigung, Kap. 80, Rn. 124 ff.

⁴⁶ Vgl. *OLG Hamburg* Ur. v. 28.1.2009 – 5 U 255/07 (Alphaload / Usenet II) Rn. 8; *OLG Hamburg* Ur. v. 14.01.2009 – 5 U 113/07, MMR 2009, 631, 632 (Spring nicht / Usenet I).

⁴⁷ Vgl. *OLG Düsseldorf* Ur. v. 20.05.2008 – I- 20 U 196/07, K&R 2008, 183.

⁴⁸ Ein Remailer ist ein pseudonymisierender und/oder anonymisierender Internet-Dienst. Die Software entpersonalisiert insoweit, dass Rückschlüsse auf den ursprünglichen Absender nicht möglich sind.

⁴⁹ Vgl. *Ritterhoff/Neubert*, in: *Widmaier*, Anwaltshandbuch Strafverteidigung, Kap. 80, Rn.126.

⁵⁰ So z.B. „Napster“, welches die erste Musikauschbörse war, die zur Zugänglichmachung von MP3-Files programmiert wurde. Heute wird unter dem Namen Napster und dem Logo der ehemaligen Tauschbörse in Deutschland, den USA, Kanada und Großbritannien ein vollständig lizenziertes Kauf- und Abo-Modell zur Musiknutzung betrieben.

⁵¹ *Möllmann/Bießmann* in *Schwartzmann*, Praxishandbuch Medienrecht, Kap. 32, Rn. 87.

⁵² *Ritterhoff/Neubert* in *Widmaier*, Münchener Anwaltshandbuch Strafverteidigung, Teil L, Rn.128.

Rechnern gleichzeitig sog. Clients⁵³ und Server und darüber hinaus ist der Nutzer auch zugleich Anbieter.⁵⁴ Er gibt Daten frei, die von anderen Nutzern aufgefunden und heruntergeladen werden können, wobei die gesuchte Datei per Download auf einen Datenträger des zugreifenden Benutzers übertragen wird. Sog. kollaborative Filesharing-Protokolle ermöglichen es, die gesuchte Datei von mehreren verfügbaren Quellen zu beziehen und immer nur ein Datei-Fragment (Bit) zu kopieren, das auf dem empfangenden Datenträger zu einer vollständigen, identischen Kopie zusammengesetzt wird.⁵⁵ Aus technischen Gründen ist ein solches dezentral organisiertes Netzwerk kaum zu überwachen. Es ist auch nicht stillzulegen, indem ein Server abgeschaltet wird.⁵⁶ Beim P2P-Filesharing nimmt der Nutzer durch das Anbieten und das Herunterladen von geschützten Werken zwei urheberrechtlich relevante Nutzungshandlungen vor. Obwohl es dem P2P-Filesharer nur auf das Herunterladen zur eigenen Verwendung ankommt, ermöglicht das dazu erforderliche Computerprogramm zugleich den Zugriff Dritter auf die gespeicherten Daten des am P2P-Netzwerk angemeldeten Benutzers zu „Tauschzwecken“. Es stellt sich hier die Frage, ob Dritte, wie der Betreiber eines Vermittlungsservers oder der Anbieter der Filesharing-Software, für Rechtsverletzungen anderer haften.

3. Sharehosting

Auch über sog. Sharehosting-Dienste finden Urheberrechtsverletzungen statt. Diese Dienste sind, wie das Usenet, für sich genommen legal. Gleichwohl ermöglichen sie es, große Dateien zu speichern und sie über Links anderen Nutzern zum Download zur Verfügung zu stellen. Auf diese Weise wird, je nachdem was zum Download bereit gestellt wird, Missbrauch ermöglicht.⁵⁷ Reine Sharehoster⁵⁸-Dienste bieten allein Speicherplatz auf Servern für Datenupload an.⁵⁹ Werden sie etwa auf Portalseiten über eine URL für Dritte auffindbar gemacht,⁶⁰ können sie grundsätzlich kostenlos heruntergeladen werden. Wer sich bei einem Sharehosting-Dienst registriert, muss zumeist keine personenbezogenen Daten preisgeben und kann einen beliebigen Benutzernamen verwenden. Auch die IP-Adressen werden sowohl beim Up- als auch beim Download nicht gespeichert. Kostenpflichtige Zu-

⁵³ Ein Client ist ein Computer oder ein Programm, welches Kontakt zu einem anderen Computer oder Programm aufnimmt und von diesem einen Dienst oder ein Programm anfordert, vgl. *Werner/Jaeger*, *AnwaltFormulare EDV- und Internetrecht*, S. 37.

⁵⁴ Andere Modelle nutzen nicht nur einen, sondern zahlreiche verteilte Server zur Verwaltung von Suchanfragen. Wird ein Server abgeschaltet, fangen andere seine Funktion auf und das Netzwerk bleibt bestehen.

⁵⁵ *Ritterhof/Neubert in Widmaier*, *Münchener Anwaltshandbuch Strafverteidigung*, Teil L, Rn. 128.

⁵⁶ *Solmecke*, *K&R* 2007, 138, 139.

⁵⁷ *Härting*, *Internetrecht*, Kap. H., IV., Rn. 1775.

⁵⁸ Auch Filehoster oder One-Klick-Hoster genannt.

⁵⁹ *Möllmann/Bießmann in Schwartmann*, *Praxishandbuch Medienrecht*, Kap.32 Rn.88.

⁶⁰ *Härting* *Internetrecht*, Kap. H., IV., Rn. 1775.

satzleistungen, etwa für erhöhten Datendurchsatz, finanzieren einen Teil des Dienstes. Urheberrechtlich problematisch kann die Nutzung von Sharehosting-Diensten dadurch werden, dass Nutzer geschützte Inhalte auf Server laden und die URL, etwa zu einem aktuellen Kinofilm, in Foren öffentlich zugänglich gemacht wird, die ihrerseits über Suchmaschinen gefunden werden können. Portalseiten, die auf das Auffinden solcher URLs spezialisiert sind sowie Linksammlungen zu bei Sharehostern gespeicherten geschützten Werken, sind ein besonderes Problem.

4. Streamhosting und Filmportale

Eine Erscheinungsform von Internetkriminalität sind Portalseiten, die, geordnet nach inhaltlichen Kriterien, Links zu Servern anbieten, die unter anderem aktuelle Kinofilme zum Abspielen bereit halten, welche weltweit illegal kopiert werden. Die Kopien werden auf die Server von Streamhostern gestellt, wo dann über die Portalseiten auf einen bestimmten Inhalt, etwa einen Film zugegriffen werden kann. Auf diesen werden URLs gesammelt, katalogisiert, beschrieben und bewertet.⁶¹ Die Übertragung zum Konsumenten erfolgt technisch per Streaming, bei dem eine kontinuierliche Datenübertragung per Push-Dienst⁶² zwischen Server und Empfangsgerät des Nutzers stattfindet. Der Datenstrom wird währenddessen am Bildschirm wiedergegeben.⁶³ Für die Dauer des Streamingvorganges werden die Daten im Empfangsgerät zwischengespeichert und nach der Nutzung in der Regel automatisch gelöscht. Urheberrechtlich relevant beim Streaming sind das Erstellen der Kopie, ihr Bereitstellen, das Verlinken auf diesen Inhalt sowie das Anschauen.⁶⁴

5. Recording Software und Online-Recording

Auch das Mitschneiden von Rundfunksendungen per Internetverbindung ist über Internetdienste möglich und grundsätzlich nicht unzulässig. Auch dabei wird auf urheberrechtlich geschütztes Material zugegriffen. Im Internet ist dafür zum einen intelligente Aufnahme-Software zur digitalen Vervielfältigung von Daten kostenlos⁶⁵ erhältlich. Diese ermöglicht es, Webradios gezielt und automatisiert nach Inhalten, wie einem gewünschten Lied,

⁶¹ Kino.to verdiente u.a. an einem pornographischen Werbebanner auf der Startseite, das monatlich 80.000 € gekostet haben soll und mit weiteren Bannern, Fenstern und „Kostenfallen“ Bei letzteren führt ein Mausclick in einen kostenpflichtigen Bereich, ohne dass der Anbieter darauf hinweist. Durch ein kostenloses Oberflächenangebot oder etwa ein Gewinnspiel wird das Interesse des Nutzers geweckt, auf der Webseite muss er sich dann aber für weitere Inhalte weiterklicken, etwa in einem „Member-Bereich“. Unauffällig in einer Fußnote oder sonst unscheinbar ist auf der Webseite in kleiner Schrift vermerkt, dass dieser Klick einen Vertrag mit Kostenpflicht auslöst. So: *Kitz* in *Hoeren/Sieber*, Multimedia-Recht, Teil 13.1 Rn. 9a.

⁶² *Sieber* in *Hoeren/Sieber*, Multimedia-Recht, Teil 1, Rn. 134.

⁶³ *Möllmann/Bießmann* in *Schwartzmann*, Praxishandbuch Medienrecht, Kap. 32, Rn. 89.

⁶⁴ Dazu *Schwartzmann*, Filesharing, Sharehosting & Co in *K&R Beihefter 2/2011*, S. 15 ff.

⁶⁵ Die kostenlose Nutzung ist hier jedoch z.T. beschränkt (z.B. auf 20 Stücke aus einem bestimmten Bereich).

zu durchsuchen.⁶⁶ Inhalte können dort eingegeben werden und werden dann aufgefunden, mitgeschnitten und auf einem Datenträger des Nutzers in einem hochkomprimierten Format gespeichert. Die Vielzahl von Onlineangeboten macht auch aktuelle Stücke schnell verfügbar, auf seltener gespielte Inhalte muss man warten.

Eine andere Möglichkeit bieten Online-Recording-Dienste, die mit digitalen Festplattenrekordern vergleichbar sind. Über derartige internetbasierte Personal Video Recorder (iPVR) können bestimmte Radio-⁶⁷ oder Fernsehprogramme⁶⁸ „aufgenommen“ werden. Diese werden dann auf dem Server des Anbieters zum späteren Download oder zum Konsum per Stream bereitgehalten. Im Unterschied zu herkömmlichen digitalen Festplattenrekordern wird ein Rechner zwischengeschaltet, der Programme in einen binären Code umwandelt bevor er diesen auf dem Datenträger speichert.⁶⁹ Das Programmieren der Sendung erfolgt auf der Internetseite des Anbieters.⁷⁰

6. Fazit

Urheberrechtsverletzungen im Internet können auf vielfältige Weise begangen werden. Auch wenn das Fortschreiten der Technik neue Variationen hervorbringen wird, sind die wiederkehrenden Handlungen der Up- und Download von Inhalten, das Verlinken sowie das Anbieten eines Dienstes. Die wesentlichen Rechtsfragen in diesem Zusammenhang befassen sich damit, ob Vervielfältigungen von den Schranken des Urheberrechts gedeckt sind, ob Dritte auf fremde Inhalte hinweisen dürfen, wenn sie wissen, dass dieser Hinweis zu Rechtsverletzungen führt und ob man haften muss, weil man die technischen Mittel für die Rechtsverletzungen Dritter bereit stellt.⁷¹ Urheberrechtlich handelt es sich dabei um Vervielfältigungen oder öffentliche Zugänglichmachung. Bei Nutzung dieser Dienste können legale und illegale Verhaltensweisen teilweise nur schwer unterschieden werden, weil technisch gleich Funktionierendes rechtlich unterschiedlich zu bewerten sein kann und

⁶⁶ Erkannt wird das gewünschte Lied anhand von z.B. sog. ID3-Tags. Dazu v. *Zimmermann* MMR 2007, 553, 554.

⁶⁷ Z.B. der „OnlineMusicRecorder“. Das bis 2007 aktive Angebot von mp3flat.com. schnitt automatisiert die Programme von Internetradios mit und bot die einzelnen Lieder seinen Nutzern zum Download im mp3-Format an. Nach zwei einstweiligen Verfügungen des *LG Köln*, durch die das Gericht den Betreibern die Vervielfältigung geschützter Musikwerke ohne Zustimmung der GEMA untersagte, wurde der Dienst abgeschaltet. <http://www.heise.de/newsticker/meldung/MP3flat-com-ist-offline-148913.html>.

⁶⁸ So etwa „shift.tv“, „save.tv“, oder „onlinetvrecorder.com“.

⁶⁹ *Hofmann* MMR 2006, 793, 793.

⁷⁰ *Hofmann* MMR 2006, 793, 793f.

⁷¹ Dazu *Schwartzman*, Filesharing, Sharehosting & Co. In K&R Beihefter 2/2011, S. 1 ff.

umgekehrt.⁷² Je nach Erscheinungsform und Ausübung ist ein Verhalten etwa wegen § 53 UrhG nicht zu beanstanden.⁷³

III. Ursachen für Urheberrechtsverletzungen im Internet

Warum werden im Internet massenhaft urheberrechtswidrig fremde Werke veröffentlicht, verändert, kopiert und konsumiert? Die Ursachen für Urheberrechtsverletzungen im Netz sind vielschichtig. Ihnen ist im Folgenden nachzugehen. Dabei wird die Analyse in mehrfacher Hinsicht eingegrenzt. Erstens konzentriert sie sich auf die Beweggründe bei **massenhaften Rechtsverletzungen**. Diese treten im Rahmen von Geschäftsmodellen in Erscheinung, die auf die netzbasierte Massenverbreitung und -beschaffung von fremden Inhalten ausgerichtet sind. Zweitens steht im Zentrum der Untersuchung das Verhalten der **individuellen Internet-Nutzer bzw. deren Motivation**. Denn diese sind die Adressaten von Warnhinweisen. Ausgeblendet sind damit die Betreiber der besagten Geschäftsmodelle und solche weiteren Akteure, die in dem System eines illegalen Geschäftsmodells notwendig mitwirken.⁷⁴ Drittens konnten im Rahmen dieser Studie **keine eigenen Daten** erhoben, sondern es musste auf bereits vorhandenes aktuelles Datenmaterial zurückgegriffen werden. Dieses liefert zu Teilaspekten wichtige Erkenntnisse. Ein umfassendes Gesamtbild der Ursachen erschließt sich daraus aber nicht. Einzelne Annahmen dieser Studie müssen deshalb ebenso empirisch unbelegt bleiben und mögliche weitere, aber allenfalls untergeordnete Gründe unberücksichtigt. Insbesondere wird nicht beantwortet, inwieweit – im Sinne einer ungefähren Größenangabe oder Prozentzahl – die im Folgenden beschriebenen Ursachen oder einzelne ihrer Aspekte kausal für die Verletzungen von Urheberrechten im Internet sind. Hierzu sind die Ursachen zu wenig belastbar erforscht und zu multikausal.

Urheberrechtsverletzungen im Netz lassen sich danach **im Kern auf zwei Gründe** zurückführen, die verschiedentlich in Zusammenhang miteinander stehen und zusammenwirken. Sie sind zum einen Folge der **technologischen Entwicklung**, die gemeinsam mit anderen Faktoren der breiten Masse der Bevölkerung den Zugang zum Internet ermöglicht und dabei den illegalen Zugriff auf urheberrechtlich geschützte Werke für den einzelnen Nutzer attraktiv macht (unten 1.). Zum anderen beruhen Urheberrechtsverletzungen im Inter-

⁷² Dazu *Schwartmann*, Filesharing, Sharehosting & Co. In K&R Beihefter 2/2011, S. 1ff.

⁷³ Dazu *Schwartmann*, Filesharing, Sharehosting & Co in K&R Beihefter 2/2011, S. 19 ff.

⁷⁴ Siehe näher zu den Akteuren illegaler Geschäftsmodelle und ihrer Motivation: GVU, Jahresbericht 2009, S. 7 ff. Danach wird grundsätzlich zwischen vier Kategorien von Raubkopierern unterschieden: „Am Beginn der illegalen Verwertung stehen die Release-Gruppen, welche die frühesten illegalen Kopien herstellen und auf nicht-öffentlichen Servern, den Top Sites, verbreiten. In der Regel verfolgen sie keine finanziellen Interessen. Vielmehr stehen die Release-Gruppen im Wettkampf darum, als erstes eine illegale Kopie in bestmöglicher Qualität auf die Top Sites hochzuladen bzw. dort am schnellsten zu verbreiten. Diese illegalen Kopien werden dann sowohl von digitalen Dealern als auch von digitalen Hehlern weiterverwertet. Zumeist mit monetären Interessen verknüpft, ermöglichen, steuern und organisieren diese Raubkopierer die illegale Massenverbreitung durch Internetnutzer. Die vierte Kategorie bilden Raubkopier-Nutzer. Infolge der durch digitale Dealer und digitale Hehler geschaffenen Voraussetzungen und Infrastruktur benötigen sie zum Auffinden und illegalen Konsum urheberrechtlich geschützter Filme, TV-Serien und Games keine tiefgehenden technischen Kenntnisse.“

net auf einem **Mangel an Rechts- bzw. Unrechtsbewusstsein** (unten 2.). Rechts- bzw. Unrechtsbewusstsein kann schlicht fehlen, wenn der Nutzer nicht weiß, dass er sich unrecht verhält. Mangelndes Rechts- bzw. Unrechtsbewusstsein ist Ursache für Urheberrechtsverletzungen auch in dem Fall, dass der Nutzer weiß oder zumindest für möglich hält, dass sein Verhalten im Netz rechtswidrig ist. Der Nutzer handelt dann eigennützig motiviert rechtsverletzend, weil er die urheberrechtlichen Bestimmungen – in der konkreten Situation für sich oder generell – nicht gelten lässt.

Unter den Ursachen für Urheberrechtsverstöße im Internet ist der Mangel an Rechts- bzw. Unrechtsbewusstsein bei den Nutzern besonders in den Blick zu nehmen. Denn hier setzen Warnhinweise an. Die Untersuchung ihrer Wirkrichtung und Effektivität ist daran auszurichten. Entsprechend muss sich die Ausgestaltung einer etwaigen Warnhinweis-Regelung sowie von Warnhinweisen als solchen hieran orientieren.

1. Technologischer Fortschritt

Die technologische Entwicklung, die für die massenhaften Urheberrechtsverletzungen im Internet mitursächlich ist, betrifft zwei Aspekte. Zum einen bezieht sie sich auf das urheberrechtlich geschützte Werk selbst, d.h. dessen Umsetzung in einen Binärcode (Digitalisierung). So gut wie jedes Werk liegt heute bereits in digitaler Form vor oder kann zumindest digitalisiert werden. Dadurch ist es praktisch unbegrenzt verfügb- und reproduzierbar. Mit der Digitalisierung lassen sich namentlich alle Werke „ins Netz“ stellen. Sie können dann im Prinzip zu allen Zeiten und von allen Orten der Welt abgerufen und beliebig aus dem Internet kopiert werden.

Zum anderen bezieht sich der technologische Fortschritt als Mitursache für das Massenphänomen der Urheberrechtsverletzungen im Internet auf die Medien einschließlich Software, die der Datenspeicherung und -übertragung sowie dem Empfang, der Aufnahme und Wiedergabe der Daten dienen, sowie auf deren und auf der Verbreitung des Internet in der Bevölkerung.

Als Speichermedien existieren heute neben PC- oder externen Festplatten, CDs, DVDs, USB-Sticks, Chips und virtuelle Speicherplätze (Clouds). Dabei nehmen sowohl die Speicherkapazitäten der einzelnen Medien als auch die Möglichkeiten der Datenkomprimierung zu, so dass für die Speicherung von Daten kaum physische Grenzen zu bestehen scheinen. Nutzer können dadurch ganze digitale Bibliotheken mit urheberrechtlich geschützten Werken anlegen. Im Hinblick auf den Datentransport sind ein fortschreitender Ausbau der Übertragungswege (Netzausbau) sowie deutliche Steigerungen der Übertragungsraten bzw. –geschwindigkeiten zu verzeichnen.⁷⁵ So ist etwa das Kopieren eines Mu-

⁷⁵ Erhöhtes Datenaufkommen – bis zum Jahr 2014 soll, so wird prognostiziert, die Menge der global übertragenden Daten auf mehr als 40.401 Petabyte pro Monat wachsen, was über 1400 Petabytes pro Tag entspricht oder täglich der 3500 fachen Information aller Bücher, die je geschrieben wurden (siehe

sikstücks aus dem Internet auf die Festplatte des heimischen PC eine Angelegenheit von Sekunden. Empfangs-, Aufnahme- und Wiedergabemedien sind dabei längst nicht mehr nur der PC, das Laptop oder Notebook. Urheberrechtlich geschützte Werke bzw. deren Daten können mittlerweile von vielen weiteren mobilen internettauglichen Geräten empfangen, aufgenommen (kopiert) und / oder wiedergegeben werden. Neben CD- und DVD-Brennern sowie MP3-Playern sind das etwa Tablet-Computer und Smart-Phones. Dabei ist entscheidend, dass die Kopie als Ergebnis des Kopiervorgangs fast nie in der Qualität hinter dem Original zurücksteht.⁷⁶

Die technologische Entwicklung bewirkt zusammen mit der dadurch möglichen Massenproduktion und dem hierdurch entfachten Wettbewerb der Anbieter zudem eine ansteigende Verbreitung dieser Medien wie überhaupt der Nutzung des Internet in der Bevölkerung. Aus Sicht des Verbrauchers ist damit nämlich eine günstige Kostenentwicklung verbunden, die für ihn sowohl den Erwerb der Hard- und Software zum Empfang-, zur Aufnahme und Wiedergabe der Mediendaten als auch die Nutzung des Internet erschwinglich macht. Dies wiederum führt zu einem Anstieg der Rechner- und Nutzerzahlen sowie der Nutzungsdauer und -häufigkeit.⁷⁷ Schließlich führt die Kostenreduktion in Folge dieser Entwicklung insbesondere auch dazu, dass Werke im Netz verbreitet unentgeltlich oder gegen Zahlung nur eines geringen Entgelts bezogen werden können.

Im Ergebnis bewirkt der technologische Fortschritt daher zum einen, dass der einzelne Nutzer nahezu alle Werke bzw. deren Daten im Internet ohne nennenswerten Qualitätsverlust kopieren kann. Das Auffinden und Kopieren von Daten ist auch in großen Mengen bemerkenswert einfach („benutzerfreundlich“), schnell und kostenlos oder kostengünstig.

http://de.wikipedia.org/wiki/Internet#cite_note-22 . Aufruf vom 9.9.2011) –, aber auch gezielte Eingriffe in den Datenverkehr führen freilich auch immer wieder zu „Datenstaus“.

⁷⁶ Letzteres ist offenbar anders bei Software: Der *Eighth Annual BSA Global Software Piracy Study* (Mai 2011), S. 1, 7 zu Folge ist verbreitete Erkenntnis, dass lizenzierte Software besser ist als raubkopierte Software; sie wird als sicherer und verlässlicher eingeschätzt als diese. Siehe auch *ICC BASCAP / StrategyOne, Research Report on Consumer Attitudes and Perceptions on Counterfeiting and Piracy* (www.iccwbo.org/bascap), November 2009, S. 81, Table 34. Bezogen auf Risiken, die mit Piraterie- oder Fälschungssoftware in Verbindung gebracht werden, gaben im U.K. 48 Prozent der Befragten an, dass sie glauben, dass solche Software definitiv Computer ernsthaft beschädigen kann; 37 Prozent meinten, dass solche Software manchmal geringfügige Probleme verursacht; 12 Prozent der Befragten äußerten, dass schlimmstenfalls solche Software nicht richtig funktioniert, während nur 3 Prozent der Meinung waren, dass solche Software sich insoweit nicht von der Originalware unterscheidet.

⁷⁷ So können nach der *DCN-Studie 2011* (Presseversion), Chart Nr. 9) 52 Prozent der deutschen Bevölkerung in Privathaushalten auf CD-Brenner und 32 Prozent auf DVD-Brenner zugreifen (Basis: 63, 7 Mio. priv. Deutsche ab 10 Jahren), was auf der Grundlage der erhobenen Daten einer Zahl von 32,9 bzw. 20,6 Mio. Personen entspricht. 45 Prozent haben dieser Studie zu Folge MP3-Player und 51 Prozent MP3-Handies in ihrem persönlichen Besitz (= 28,7 bzw. 32,5 Mio. Personen).⁷⁷ Laut *ARD/ZDF-Onlinestudie 2011* (<http://www.ard-zdf-onlinestudie.de/index.php?id=onlinenutzung00> , mit Angaben zur Entwicklung seit 1997). sind mittlerweile 73,3 Prozent der (deutschsprachigen) Bevölkerung (2010: 69,4 Prozent) online. In absoluten Zahlen bedeutet dies, dass 51,7 Millionen Erwachsene in Deutschland (ab 14 Jahren) zumindest gelegentlich das Internet nutzen (im Vorjahr: 49,0). Dabei verwenden 75 Prozent PCs / Computer als Zugang zum Internet, 53 Prozent Laptops, 16 Prozent das Handy (davon: 6 Prozent iPhone, 8 Prozent anderes Smartphone, 2 Prozent „normales“ Handy), 3 Prozent Spielkonsolen, 1 Prozent MP3-Player, 3 Prozent Fernseher und 2 Prozent Tablet-PCs (<http://www.ard-zdf-onlinestudie.de/index.php?id=314>). Die durchschnittliche Verweildauer bei der Online-Nutzung beträgt nach dieser Studie 137 Minuten am Tag (<http://www.ard-zdf-onlinestudie.de/index.php?id=319> , mit Angaben zur Entwicklung seit 1997).

Für den Einzelnen ist damit der Zugriff auf Daten urheberrechtlich geschützter Werke un-
gemein **attraktiv und verlockend**.⁷⁸ Das gilt umso mehr, wenn man den Kopiervorgang
aus dem Netz mit einem Erwerb des entsprechenden körperlichen Werks als Alternative
vergleicht. Zum anderen führt die technologische Entwicklung (zusammen mit anderen
Faktoren) zu einer Zunahme der Anzahl empfangs-, aufnahme- und / oder wiedergabe-
tauglichen Rechner wie auch zu einer Zunahme der Nutzung des Internet. Damit sind im-
mer mehr Menschen immer häufiger und andauernder in der Lage, Werkdaten im Netz
hoch- und herunterzuladen und zu konsumieren.⁷⁹ Dadurch steigt auch potentiell die Zahl
von Urheberrechtsverletzungen im Internet. Schließlich leisten Technik und technologi-
sche Entwicklung insofern einen Beitrag zum massenhaften Urheberrechtsverstoß, als
Nutzer vermeintlich oder tatsächlich anonym, d. h. unter Verschleierung ihrer wahren Iden-
tität im Internet agieren können und damit das Risiko, wegen eines Verstoßes belangt zu
werden, minimieren.

2. Mangelndes Rechts- bzw. Unrechtsbewusstsein

Rechtsbewusstsein bezeichnet die (ethisch-moralische) Einstellung des Einzelnen zum
Recht. Es wird beschrieben als

„jener Zustand, worin der Mensch sich als solidarischer Teil einer Kultur begreift, die
dem Einzelnen als Rechtsperson Autonomie, dem sozialen Ganzen als Rechtssystem
aber obersten Orientierungswert für das gesellschaftliche Handeln zuweist.“⁸⁰

Dies verlangt zum einen, dass die Person als Normadressat Kenntnis oder zumindest eine
juristisch-laienhafte Vorstellung davon hat, wie sie sich rechtlich verhalten *soll* bzw. was
rechtlich erlaubt und verboten ist (**Norm-Kennntnis**). Davon umfasst sind nach hiesigem
Verständnis nicht nur die Regelungen als solche, sondern auch die tatsächlichen Umstände
und deren Bedeutung hinsichtlich der Rechtsanwendung im Einzelfall.⁸¹ Dementspre-
chend mangelt es einem Internet-Nutzer an Rechts- bzw. Unrechtsbewusstsein, wenn er
sich entweder über die Reichweite oder Voraussetzungen einer urheberrechtlichen Ver-
bots- oder Erlaubnisnorm irrt oder über die Tatumstände oder deren Bedeutung im Hin-
blick auf die Rechtsverletzung (unten a.). Der Irrtum erweist sich dabei als (mit-)ursächlich
für den Verstoß gegen das Urheberrecht, wenn anzunehmen ist, dass sich der Nutzer bei
zutreffender Rechtskenntnis rechtmäßig verhalten hätte bzw. würde. Zum anderen setzt
Rechtsbewusstsein voraus, dass der Adressat der Verhaltensanforderungen diese als „rich-

⁷⁸ Siehe auch *“Estimating the global economic and social impacts of counterfeiting and piracy -
A report commissioned by business action to stop counterfeiting and piracy (BASCAP)”*, February 2011, p. 23 f.

⁷⁹ Siehe auch *“Estimating the global economic and social impacts of counterfeiting and piracy -
A report commissioned by business action to stop counterfeiting and piracy (BASCAP)”*, February 2011, p. 23 f.

⁸⁰ Lampe, in: Lampe (Hrsg.), *Zur Entwicklung von Rechtsbewusstsein*. Einleitung, S. 7, 15.

⁸¹ Abweichend die strafrechtliche Doktrin, wonach das Unrechtsbewusstsein (= Bewusstsein der Rechtswid-
rigkeit) als Element der Schuld zu trennen ist von der Tatumstands- und Bedeutungskennntnis als Bestandteile
des Vorsatzes.

tig“ anerkennt (**Norm-Akzeptanz**) und entsprechend beachtet (**Norm-Respektierung oder Norm-Treue**). Daher kann es sein, dass der Nutzer weiß oder zumindest für möglich hält, dass ein bestimmtes Verhalten im Internet illegal ist. Dann liegt der Mangel an Rechts- bzw. Unrechtsbewusstsein darin, dass der Nutzer die Geltung urheberrechtlicher Regelungen im Internet in der konkreten Situation bewusst missachtet oder generell nicht anerkennt (unten b.). Gleichsam dazwischen liegt der Fall, dass die Rechtslage unklar ist und die juristische „Grauzone“ bzw. Regelungslücke von dem User (aus-)genutzt wird.

a. Unkenntnis der Rechtslage

Laut der sog. Digital Content Nutzung-Studie (DCN-Studie) 2011, die im Auftrag der Musikindustrie erstellt wurde, wissen 80 Prozent der Bevölkerung, dass das Herunterladen oder Anbieten von urheberrechtlich geschützten Medieninhalten im Internet erhebliche rechtliche Folgen nach sich ziehen kann.⁸² 98 % der Bevölkerung sollen sich darüber im Klaren sein, dass die Verbreitung von urheberrechtlich geschützten Werken nicht erlaubt ist.⁸³

Erhöht ist dieser Anteil bei den aktiven „Downloadern“. Hier wissen 96 Prozent, dass das Herunterladen oder Anbieten von urheberrechtlich geschützten Medieninhalten im Internet rechtliche Folgen haben kann.⁸⁴ 15 Prozent der Deutschen (ab 10 Jahren) sind der Ansicht, dass der Download aus Peer-to-Peer-Netzwerken legal ist.⁸⁵ Unter denjenigen, die das Internet zum Download benutzen, sind es 17 Prozent.⁸⁶ 8 Prozent dieser Nutzer halten das Hochladen von urheberrechtlich geschützten Materialien, an dem sie keine Rechte haben, auf Server von Sharehostern wie bspw. Rapidshare für rechtmäßig.⁸⁷ Den **Software-Download** in Peer-to-Peer-Netzwerken halten nach einer Untersuchung zur PC-Software-Piraterie demgegenüber **21 Prozent** der PC-Nutzer in entwickelten Volkswirtschaften weltweit für „**wahrscheinlich legal**“.⁸⁸

Im Vereinigten Königreich sind sich 73 Prozent der Verbraucher nicht darüber im Klaren, was zulässigerweise kopiert oder aus dem Rundfunk aufgenommen werden darf.⁸⁹ 44 Prozent der Verbraucher dort halten Filesharing in P2P-Netzwerken sogar für legal.⁹⁰

Letztlich lässt sich diesem Zahlenmaterial nicht eindeutig entnehmen, ob und inwieweit Nutzer in Deutschland im Zeitpunkt der Verletzungshandlung aktuelles Unrechtsbewusstsein haben, d. h. in der konkreten Situation tatsächlich wissen, dass das eigene Verhalten urheberrechtswidrig ist. Der Beitrag unzureichender Rechtskenntnis der Nutzer zu Rechts-

⁸² DCN-Studie 2011 (Presseversion) Chart 34. Basis: 63, 7 Mio. priv. Deutsche ab 10 Jahren

⁸³ Pressemitteilung von BVMI, Börsenverein und GfK zur Vorstellung der DCN-Studie 2011, http://www.boersenverein.de/sixcms/media.php/976/110830_DCN_PM_FINAL.pdf.

⁸⁴ Vgl. DCN-Studie 2011 (Vollversion), S. 39.

⁸⁵ Vgl. DCN-Studie 2011 (Vollversion), S. 40.

⁸⁶ Vgl. DCN-Studie 2011 (Vollversion), S. 43.

⁸⁷ Vgl. DCN-Studie 2011 (Vollversion), S. 44.

⁸⁸ Eighth Annual BSA Global Software Piracy Study (Mai 2011), S. 7.

⁸⁹ Consumer Focus, Outdated copyright law confuses consumers, 24.02.2010, Link: <http://www.consumerfocus.org.uk/news/outdated-copyright-law-confuses-consumers>, zuletzt aufgerufen am 19.08.2011.

⁹⁰ Harris Interactive/BPI, Digital Music Survey, 2010.

verstößen im Internet ist hieraus nicht klar ablesbar. Immerhin scheint nach den Daten hinreichend Grund zu der Annahme zu bestehen, dass nicht wenigen Nutzern die Rechtswidrigkeit ihres Tuns nicht bewusst ist.

aa. Unkenntnis des Rechts

Es gibt Nutzer, die weder eine genaue **Kenntnis** noch eine hinreichende juristisch-laienhafte Vorstellung davon haben, **welches Verhalten unter welchen Bedingungen im Internet überhaupt urheberrechtlich verboten oder ausnahmsweise erlaubt** ist.

Eine Ursache dafür ist grundsätzlicher Natur. Sie liegt darin, dass das Urheberrecht geistiges Eigentum schützt, das weder als solches noch dessen Beeinträchtigung physisch fassbar ist. Dies gilt gerade dort, wo die geistige Schöpfung des Urhebers (vgl. § 2 Abs. 2 UrhG), wie im Internet, allein als Datei digital existiert und in keiner Weise gegenständlich in Erscheinung tritt. Während Verletzungen des körperlichen Eigentums sich als Zerstörung, Beschädigung, Entzug oder Vorenthaltung darstellen, werden „nur“ unsichtbare Verwertungsrechte des Urhebers verletzt.⁹¹ Dementsprechend lassen sich die wirtschaftlichen Nachteile einzelner Urheberrechtsverletzungen auch nicht unmittelbar wahrnehmen. Die Daten geschützter Werke, die illegal im Internet hoch- oder heruntergeladen werden, bleiben unversehrt erhalten, Reproduktions- oder Wiederbeschaffungskosten entstehen nicht. Möglicherweise sind deshalb die Anerkennung der Leistung des Urhebers und deren wirtschaftliche Verwertung durch den Urheber im öffentlichen Bewusstsein nicht etabliert.

Hinzu kommt, dass die Rechtslage in Teilbereichen tatsächlich unklar ist. Eindeutige Verstöße gegen das Urheberrecht hingegen werden nicht sanktioniert, weil einerseits die Rechteinhaber sich zu einer effizienten Rechtsverfolgung nicht in der Lage sehen und andererseits Internet-Service-Provider untätig bleiben, selbst wenn sie nach bestehenden Vertragsbedingungen durchaus berechtigt sind, den Internet-Anschluss ihrer Kunden zu sperren oder den Vertrag zu kündigen.⁹² Darüber hinaus wird in der Öffentlichkeit von Aktivisten das Netz zum „urheberrechtsfreien Raum“ erklärt oder eine „Freiheit im Netz“ propagiert, die es der Allgemeinheit erlaube, im Internet kostenfrei unter urheberrechtlichem Schutz stehende Werke zu nutzen. Weniger weitgehend sind rechts- und gesellschaftspolitische Bestrebungen zur Fortentwicklung des Urheberrechts im Zeitalter von Internet und Informationsgesellschaft, die den Nutzer mit seinen Interessen in das Zentrum urheberrechtlicher Regelungen rücken und dementsprechend den bestehenden urheberrechtlichen Schutz der geistigen Leistung abschwächen wollen. Betreiber dubioser Geschäftsmodelle behaupten schließlich, ihre Dienste und deren Nutzung seien mit dem Urheberrecht vereinbar. Vor diesem Hintergrund herrscht in der Bevölkerung augenscheinlich ein diffuses Gefühl der Rechtsunsicherheit oder es sind unzutreffende Rechtsansichten darü-

⁹¹ Unter Umständen wird allerdings der Urheber auch in seinem Urheberpersönlichkeitsrecht verletzt (vgl. §§ 12 ff. UrhG).

⁹² Vgl. z. B. die Allgemeinen Geschäftsbedingungen Internet-Zugangstarife der Telekom Deutschland GmbH Ziff. 4.1 b) und 4.2, Ziff. 11.4 (<http://www.telekom.de/dlp/agb/pdf/39303.pdf>).

ber verbreitet, was im Internet urheberrechtlich legal ist und was nicht. Vielen erscheint das, was man technisch machen kann, auch erlaubt bzw. nicht verboten zu sein. Das alles kann dazu führen, dass Internet-Nutzer mitunter den Umfang des Schutzes der Urheberrechte im Netz nicht nur nicht kennen, sondern auch in seiner Wertung nicht nachvollziehen. Das Hochladen und Abspeichern von Daten im Netz etwa wird ein Nutzer womöglich nicht als Unrecht ansehen, wenn das betreffende Werk bereits anderweitig veröffentlicht ist. Andere Nutzer werden den Download aus dem Netz allein zu Privatzwecken stets für zulässig halten und etwa nicht nachvollziehen, dass eine rechtmäßig produzierte CD zum privaten Gebrauch „gebrannt“ werden darf, während eine Privatkopie derselben CD-Titel aus dem Internet grundsätzlich unzulässig ist.⁹³

bb. Unkenntnis der tatsächlichen Umstände

Vielen Nutzern werden im Einzelfall **die tatsächlichen Umstände** und / oder deren rechtliche Bedeutung für den Tatbestand einer Urheberrechtsverletzung und die Geltung der Urheberrechtsschranken **unklar** sein und es wird ihnen insoweit Rechts- bzw. Unrechtsbewusstsein fehlen. Solche Unkenntnis kann darin bestehen, dass die technischen Abläufe für nicht versierte Nutzer intransparent sind. So werden womöglich nicht alle Nutzer eines P2P-Netzwerkes wissen, dass die Daten nach dem Download in der Regel automatisch wieder im Netzwerk angeboten und das Herunterladen dadurch mit einem rechtswidrigen öffentlichen Zugänglichmachen verbunden ist.⁹⁴ In Anbetracht zahlreicher legaler kostenfreier Download- oder Streamingangebote im Internet wird es zudem vorkommen, dass Nutzer irrtümlich annehmen, der Urheber bzw. Rechteinhaber habe einer privaten Vervielfältigung zugestimmt oder diese stamme von einer rechtmäßig hergestellten und öffentlich zugänglich gemachte Vorlage (vgl. § 53 Abs. 1 UrhG).⁹⁵ So mag ein Nutzer zwar das Angebot eines aktuell im Kino gezeigten Filmes auf einer Filmportalseite für verboten halten, die Veröffentlichung eines Top-10-Musikclips bei YouTube aber für erlaubt. Ein Irrtum über die tatsächlichen Umstände und ihre urheberrechtliche Bedeutung liegt schließlich insbesondere auch dort vor, wo der Inhaber des Internetanschlusses (z. B. Wirtschaftsunternehmen, Eltern) als vermeintlicher Nutzer nicht weiß, dass über seinen Anschluss illegal Daten im Netz verbreitet und/oder heruntergeladen werden.

⁹³ Etwas anderes gilt nur ausnahmsweise dann, wenn entweder auch die Vorlage rechtmäßig öffentlich zugänglich oder wenn die Vorlage nicht offensichtlich rechtswidrig öffentlich zugänglich gemacht worden ist (vgl. § 53 Abs. 1 UrhG).

⁹⁴ Vgl. *Schwartmann*, Sharehosting, Filesharing & Co, K&R Beihefter 2/2011, S. 9 ff.

⁹⁵ Vgl. insoweit auch *Röhl/Bosch* NJOZ 2008, 1197, 1204. Zur umstrittenen Frage, ob die „Offensichtlichkeit“ der Rechtswidrigkeit der Vorlage i. S. v. § 53 Abs. 1 UrhG aus objektiver Nutzersicht zu beurteilen ist oder aus subjektiver Sicht des Nutzers mit der Folge, dass eine zulässige Privatkopie und bereits keine Urheberrechtsverletzung vorliegt, siehe oben *Schwartman*, K & R Beihefter 2/2011 S. 9.

b. Fehlende Akzeptanz und Respektierung des Urheberrechts: Bewusste Norm-überschreitung

Ein Mangel an Rechts- bzw. Unrechtsbewusstsein ist auch dort (Mit-)Ursache für Urheberrechtsverletzungen im Internet, wo Nutzer zwar die Illegalität ihres Netzverhaltens kennen oder für möglich halten, sich aber eigennützig darüber hinwegsetzen und urheberrechtswidrig handeln, also Urheberrecht nicht gelten lassen wollen. Das ist etwa der Fall, wenn ein Nutzer bewusst ohne die Zustimmung des Rechteinhabers ein Musikstück in einem P2P-Netzwerk herunterlädt, um damit die Kosten zu sparen, die er sonst für den Erwerb aufbringen müsste. Der Nutzer respektiert dann entweder in der konkreten Situation die urheberrechtlichen Vorschriften nicht oder lehnt deren Geltung im Internet generell ab und lässt sich auch von den rechtlichen Konsequenzen einer Rechtsverletzung (Schadensersatz / Strafbarkeit) nicht abhalten. Damit stellt sich im Hinblick auf die Wirkung und Wirksamkeit einer Warnhinweis-Regelung die Frage, worauf ein solcher Mangel beruht bzw. weshalb Nutzer Urheberrecht missachten und eigene Interessen vorziehen.

aa. Geltungsgründe von Recht

Grundlegend ist dabei zunächst die in der Rechtswissenschaft verbreitete rechtstheoretische Erkenntnis, dass Recht einen juristischen, einen moralischen und einen faktischen Geltungsgrund kennt.⁹⁶ **Juristische Geltung** meint die Anerkennung von Recht aufgrund eines durchsetzbaren staatlichen Rechtssetzungsakts. Man beachtet ein gesetzliches Verbot, auch wenn man es persönlich nicht für nötig erachtet. Es genügt, dass der Staat die Einhaltung des Gebots bzw. dessen Sanktionierung durchsetzen kann und in der Regel auch durchsetzt.⁹⁷ Unter **moralischer Geltung** lässt sich verstehen, dass rechtliche Verhaltensnormen anerkannt und befolgt werden, weil der Betreffende nach seinen Werten und Wertmaßstäben ihnen mit einem Gefühl der inneren Verpflichtung verbunden ist und sie selbst für „richtig“ hält. **Faktische Geltung** schließlich meint, dass Recht gilt, weil es tatsächlich befolgt wird.

Dort, wo – zumindest in der Wahrnehmung des Einzelnen – ein Rechtsdurchsetzungs- bzw. –verfolgungs- und Sanktionsdefizit besteht, also Recht juristisch nicht in vollem Umfang

⁹⁶ Rütters, Rechtstheorie, Rn. 334 ff.; für den vorliegenden Zusammenhang Schwartmann, in: Schwartmann (Hrsg.), Das Leben im Schwarm, S. 99, 101 ff.; ders., Entwicklung des Urheberrechts in der digitalen Gesellschaft, Enquete-Kommission Internet und digitale Gesellschaft – Stellungnahme zu den rechtlichen Aspekten der Fragen der Fraktionen zur öffentlichen Anhörung Urheberrecht der Enquete-Kommission Internet und digitale Gesellschaft am 29. November 2010, S. 6 f. m. w. N. (abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Sitzungen/20101129/A-Drs__17_24_009_H-_Stellungnahme_Prof__Schwartmann.pdf).

⁹⁷ Schwartmann, Entwicklung des Urheberrechts in der digitalen Gesellschaft, Enquete-Kommission Internet und digitale Gesellschaft – Stellungnahme zu den rechtlichen Aspekten der Fragen der Fraktionen zur öffentlichen Anhörung Urheberrecht der Enquete-Kommission Internet und digitale Gesellschaft am 29. November 2010, S. 7 (abrufbar unter: http://www.bundestag.de/internetenquete/dokumentation/Sitzungen/20101129/A-Drs__17_24_009_H-_Stellungnahme_Prof__Schwartmann.pdf); siehe auch dens., in: Schwartmann (Hrsg.), Das Leben im Schwarm, S. 99, 102.

gilt, kann der Mensch aus Eigennutz zu rechtswidrigem Handeln verleitet sein. Als wirtschaftlich denkender Mensch ist ein Individuum nämlich in der Regel bestrebt, für das von ihm nachgefragte Gut den geringstmöglichen Preis zu zahlen.⁹⁸ Ohne ethisch-moralischen Wertmaßstab verhält sich die Einzelperson als *homo oeconomicus* ökonomisch rational, d. h. sie entscheidet sich für die Handlungsvariante, die ihr den größten Nutzwert verschafft. Ein solches Verhalten setzt eine Kosten-Nutzen-Abwägung hinsichtlich der gegebenen Handlungsmöglichkeiten voraus.

Diese Überlegungen sind zunächst entscheidend für den Nutzer, der zwar generell den Schutz geistiger Leistungen nach dem UrhG (im Internet) akzeptiert, aber in der konkreten Situation Urheberrecht (auch wiederholt) nicht respektiert und File-Sharing betreibt. Der Nutzer lädt nämlich deshalb illegal urheberrechtlich geschütztes Material in P2P-Netzwerken hoch und herunter, weil dieses Verhalten ökonomisch rational ist, ihm also mehr nützt als schadet. Denn er erhält einen Vorteil, etwa kostenlos und auf sehr einfachem Wege ein Musikstück, bei – so seine Wahrnehmung – vergleichsweise geringem Risiko bzw. geringer Wahrscheinlichkeit des Eintritts einer Sanktion und bei gegebenenfalls vergleichsweise geringer Schadenshöhe. Der Rechtsbruch im Netz ist technisch einfach, man fühlt sich unbeobachtet und die Rechtsdurchsetzung bzw. Rechtsverfolgung bei Verstößen ist oftmals nicht möglich oder führt zu einer geringen Sanktion. Der einzelne Nutzer entscheidet sich insofern also für illegales Up- und Downloading, weil er keine oder nur eine unerhebliche Sanktion befürchtet.

bb. Versagen ethisch-moralischer Verhaltenskorrektur

Weshalb nun dieses ökonomisch rationale Verhalten nicht wenigstens durch ethisch-moralische Vorstellungen bzw. Moral als Geltungsgrund für Recht gleichsam korrigiert wird, bleibt fraglich.⁹⁹ Offenbar gelten „in der Welt des Internet“ mit seiner Dank des technologischen Fortschritts schier unerschöpflichen, vermeintlich kostenlosen Verfügbarkeit urheberrechtlich geschützter Inhalte andere Wertmaßstäbe als in der „körperlichen Welt“. Ein Nutzer, der niemals eine CD oder DVD in einem Geschäft stehlen würde, hat häufig kein Unrechtsempfinden, wenn er denselben Inhalt aus dem Internetangebot herunterlädt. Nur wenige würden eine „Schwarz-DVD“ mit einem neuen Kinofilm noch am Tag seines Anlaufens reinen Gewissens von einem Unbekannten annehmen und dies als rechtlich und moralisch in Ordnung werten, während im Netz über Plattformen massenhaft solche Filme offenbar ohne Unrechtsempfinden gestreamt werden. Warum aber herrschen im Internet anscheinend andere ethisch-moralische Wertvorstellungen? Die Ursachen sind vielschichtig.

⁹⁸ Vgl. auch *Liebowitz*, Testing File-Sharing's Impact by Examining Record Sales in Cities, CAPRI Publication 05-02.

⁹⁹ Vgl. dazu auch *Karaganis (Ed.)*, Media piracy in emerging economies (<http://piracy.ssrc.org>), 2011, S. 33 f. (abrufbar unter: <http://piracy.ssrc.org>), sowie *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 233.

- Ein Grund liegt in der **fehlenden Körperlichkeit**: Der Nutzer hat nicht das Gefühl, Recht zu verletzen, weil die kopierten Werke unversehrt erhalten bleiben und keine Reproduktions- oder Wiederbeschaffungskosten entstehen.¹⁰⁰
- Hinzu kommt, dass eine einzelne Verletzungshandlung im konkreten Fall in der Tat keine gravierenden Schäden verursacht. Erst die **massenhafte Begehung** führt zu einer **nachhaltigen Schädigung**, die oder deren Dimension von dem Einzelnen aber nicht wahrgenommen wird.
- **Geschädigt** wird in der Wahrnehmung des Nutzers zudem keine Einzelpersonen, sondern nur ein anonymes Gebilde wie die Musik- oder **Kreativindustrie**. Dem Nutzer erscheint deshalb die leicht durchführbare, minimale Einzeltat nicht als verwerflich und sanktionswürdig, zumindest aber die bestehende Sanktion als unverhältnismäßig.
- Weiterhin ist illegales File-Sharing in P2P-Netzwerken offenbar von der Vorstellung eines „Das-machen-doch-alle“ oder eines „Das-macht-doch-jeder-mal“ getragen. Urheberrechtsverletzungen im Internet werden deshalb nicht als gravierendes Rechtsproblem, sondern bestenfalls als „**Kavaliersdelikt**“ empfunden.
- Mehr noch erscheint die gelegentliche Rechtsverletzung zu privaten Zwecken wenn auch nicht rechtlich, so doch als „**sozial akzeptiert**“ und insoweit auf der Grundlage eines eher basisdemokratischen Verständnisses als legitimiert. Ein Blick in aktuelle Parteiprogramme, die die Rechtslage dem Nutzerverhalten angleichen wollen, dürfte das Unrechtsbewusstsein in diesem Zusammenhang weiter relativieren.¹⁰¹ Damit entfällt auch die tatsächliche Befolgung des Urheberrechts als Geltungsgrund für Recht und schlussendlich als „Korrektiv“ für eigennütziges Handeln des Menschen als *homo oeconomicus*.
- Schließlich wird die vermeintliche **Anonymität** der Handlung am Rechner und das sich nicht beobachtet werden, ein Grund für den Rechtsverstoß sein.

¹⁰⁰ Siehe bereits oben S. 45.

¹⁰¹ So heißt es etwa im Programm der Piraten Partei unter der Überschrift **Freies Kopieren und freie Nutzung** „:Da sich die Kopierbarkeit von digital vorliegenden Werken technisch nicht sinnvoll einschränken lässt und die flächendeckende Durchsetzbarkeit von Verboten im privaten Lebensbereich als gescheitert betrachtet werden muss, sollten die Chancen der allgemeinen Verfügbarkeit von Werken erkannt und genutzt werden. Wir sind der Überzeugung, dass die nichtkommerzielle Vervielfältigung und Nutzung von Werken als natürlich betrachtet werden sollte und die Interessen der meisten Urheber entgegen anders lautender Behauptungen von bestimmten Interessengruppen nicht negativ tangiert. Es konnte in der Vergangenheit kein solcher Zusammenhang schlüssig belegt werden. In der Tat existiert eine Vielzahl von innovativen Geschäftskonzepten, welche die freie Verfügbarkeit bewusst zu ihrem Vorteil nutzen und Urheber unabhängiger von bestehenden Marktstrukturen machen können. Daher fordern wir, das nichtkommerzielle Kopieren, Zugänglichmachen, Speichern und Nutzen von Werken nicht nur zu legalisieren, sondern explizit zu fördern, um die allgemeine Verfügbarkeit von Information, Wissen und Kultur zu verbessern, denn dies stellt eine essentielle Grundvoraussetzung für die soziale, technische und wirtschaftliche Weiterentwicklung unserer Gesellschaft dar.“ http://wiki.piratenpartei.de/Parteiprogramm#Freies_Kopieren_und_freie_Nutzung.

cc. Rechtsdurchsetzungsdefizit

Blickt man abschließend auf den Nutzer, der Urheberrecht in seiner bestehenden Fassung im Internet generell nicht akzeptiert und sich bei seinem rechtswidrigen Handeln auch nicht von Sanktionen abschrecken lässt, dann ist auch für diese fehlerhafte Einstellung zum Recht ein empfundenes Rechtsdurchsetzungs- bzw. -verfolgungs- und Sanktionsdefizit mitursächlich. Denn Recht gilt juristisch nur dort, wo es im Allgemeinen auch tatsächlich angewandt und durchgesetzt wird bzw. werden kann. In der Wahrnehmung solcher Nutzer ist das aber bei dem bestehenden Urheberrecht im Internet nicht der Fall. Vielmehr werden „Tauschbörsen“ als urheberrechtlich nicht kontrollierbar, die Rechtsanwendung und -durchsetzung als nicht realistisch oder zumindest nicht praktikabel angesehen. Hinzu kommt, dass das gegenwärtige Urheberrecht jedenfalls im Hinblick auf seine Anwendung im Internet als unverständlich oder unklar und kompliziert angesehen wird. Damit hat es aus der Sicht dieser Nutzer keinen juristischen Geltungsanspruch. Auch unter ethisch-moralischem Blickwinkel halten diese Nutzer das Urheberrecht in seiner derzeitigen Fassung bzw. dessen Geltung im Internet nicht für legitim bzw. für überholt. Sie rücken – zumindest im Netz – nicht die Schöpfer der geistigen Leistung, sondern die Nutzer und deren Interessen in den Vordergrund und reden einer Kostenfreiheit im Internet das Wort. Schließlich wird das gegenwärtige Urheberrecht aus der Sicht dieser Nutzer auch tatsächlich nicht befolgt und hat deshalb auch keine faktische Geltung.

Ein Problem ist auch, dass Aussagen von Vertretern des Staates Rechtsverletzungen im Internet teilweise bagatellisieren. Teile der Politik fordern etwa zumeist mit Blick auf ein mit der Rechtslage nicht übereinstimmendes Nutzerverhalten, eine Legalisierung von Urheberrechtsverstößen. Till Steffen, ehemaliger Hamburger Justizsenator der GAL forderte etwa 2010 im Hinblick auf private Vervielfältigungen eine Legalisierung von als geringfügig eingestuften Urheberrechtsverletzungen:

„Wenn das, was allgemein üblich ist, auch erlaubt ist – dann haben wir eine Chance, die Fälle, wo jemand in großem Stil und mit Gewinnerzielungsabsicht handelt, die Verbote auch durchzusetzen“¹⁰².

Die Üblichkeit von Rechtsverletzungen ist aber im Rechtsstaat kein legitimer Grund für ihre Legalisierung. Sollten der Staat und Parteien sich in den Aussagen zu Urheberrechtsverlet-

¹⁰² Zitiert nach epd medien Nr. 69 v. 4.9.2010, S. 24.

zungen im Netz insoweit nicht eindeutig festlegen¹⁰³, bleibt die Orientierung für den Bürger schwierig.

IV. Überblick zu Urheberrechtsverletzungen im Internet

1. Allgemeines

Von Urheberrechtsverletzungen im Internet sind verschiedene Branchen der Kultur- und Kreativwirtschaft betroffen. Vor einer branchenspezifischen Betrachtung sollen einleitend die Ergebnisse einer aktuellen umfassenden Untersuchung vorgestellt werden. Für Deutschland führt die Gesellschaft für Konsumforschung (GfK) jährlich eine repräsentative Befragung von 10.000 Personen¹⁰⁴ im Auftrag des Bundesverbandes der Musikindustrie durch. Im Jahr 2011 wurde in der sog. Studie zur Digitalen Content Nutzung (DCN-Studie)¹⁰⁵ für 2010 neben Musik auch die Nutzung anderer Medieninhalte wie Bücher, Filme und TV-Serien für die Bundesrepublik Deutschland analysiert. Neben dem Bundesverband der Musikindustrie zählen nun auch der Börsenverein des Deutschen Buchhandels und die Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e.V. zu den Auftraggebern.

Nach den Ergebnissen dieser Untersuchung sollen in Deutschland 19,9 Mio. Menschen im Jahr 2010 Medieninhalte online genutzt haben. 15,6 Mio. haben Musik, 5,8 Mio. TV-Serien, 4,3 Mio. Filme, 3,6 Mio. Spiele, 3,3 Mio. Hörbücher und 2,0 Mio. eBooks im Internet genutzt.¹⁰⁶ Ein Fünftel der Nutzer (3,7 Mio.) soll sich die Inhalte ausschließlich illegal¹⁰⁷, das heißt unter Nutzung „unlizenzierter“ und nicht gemeinfreier Angebote, verschafft haben. 73 Prozent der Personen auf dem deutschen Markt, die ausschließlich unlicenzierte Quellen für den Musikdownload benutzen, sollen danach gar nicht für Musik zahlen¹⁰⁸, sodass ein Nebeneinander von legaler und illegaler Nutzung in dieser Gruppe die Ausnahme ist.¹⁰⁹

¹⁰³ Vgl. etwa den zitierten damals amtierenden Hamburgischen Justizminister Till Steffens.

¹⁰⁴ DCN-Studie, S. 4, (früher Brenner-Studie).

¹⁰⁵ Die bis 2010 verwendete Bezeichnung „Brenner-Studie“ geht zurück auf den ursprünglichen Gegenstand der Studie, das Nutzerverhalten im Hinblick auf das Brennen von CD's zu untersuchen. Da aber die massenhafte Verbreitung unlizenzierter Inhalte über das Internet in den vergangenen Jahren zu einem wesentlich bedeutenderem Problem für die Branche geworden ist, wurde die Studie 2011 konsequenterweise umbenannt, in „Studie zur digitalen Content-Nutzung“.

¹⁰⁶ DCN-Studie, S. 10.

¹⁰⁷ Unter „illegal“ fallen dabei Angaben von Personen, die mitgeteilt haben, Downloads von Tauschbörsen, Sharehostern, privaten Websites, Blogs, Foren, ftp-Servern oder Newsgroups getätigt zu haben. Der Begriff „illegal“ ist aber insoweit unpräzise, als deren Rechtswidrigkeit teilweise nach geltender Rechtslage in Deutschland nicht abschließend geklärt ist. Zudem kann aus der Art des genutzten Dienstes bzw. Angebots nicht zwingend auf die Rechtswidrigkeit geschlossen werden, da manche Dienste bzw. Angebote sowohl rechtswidrigen wie auch rechtmäßigen Nutzungen zugänglich sind. Dazu ausführlich *Schwartzmann*, K&R 2011, Beihefter 2.

¹⁰⁸ GfK, DCN-Studie, S. 7.

¹⁰⁹ Dieses Ergebnis spricht gegen die Erkenntnisse von *Ipsos*, abrufbar unter: <http://knowledgecenter.ipsos.de/docdetail.aspx?c=1043&did=2df20c44-f4c4-4e37-a746-e785070a02da>, zuletzt aufgerufen am 17.10.2011.

Zwar überwiegt die lizenzierte Nutzung im Internet in Deutschland die illegale. 74 Prozent der Medieninhalte insgesamt wurden legal genutzt. Es gaben 14 Prozent der Nutzer an, sowohl lizenzierte als auch unlizenzierte Angebote genutzt zu haben, 12 Prozent nutzten ausschließlich unlizenziert, wobei der höchste Anteil ausschließlich lizenzierter Nutzung mit 78 Prozent bei den Hörbüchern und Hörspielen liegt, gefolgt von Musik mit 75 Prozent. Unlizenziert wurden am häufigsten Filme mit 49 Prozent, gefolgt von TV-Serien mit 39 Prozent und eBooks mit 35 Prozent genutzt.¹¹⁰

Die Erhebungen beleuchten Erscheinungsformen von Verletzungshandlungen gesondert und ermitteln innerhalb dessen eine Rangfolge im Verhältnis der Gesamtdownloads aller Nutzungsarten. Die Nutzung von Medieninhalten im Internet war 2010 im Bereich Musik am höchsten (15,6 Mio), gefolgt von Fernseh- und TV-Serien (5,8 Mio.) und Spiel- und Kinofilmen (4,3 Mio.) sowie Hörbüchern und Hörspielen (3,3 Mio.) und eBooks (2,0 Mio.).¹¹¹ Über **Sharehostingdienste** wurden in Deutschland 2010 23 Prozent aller eBooks, 19 Prozent aller Filme, 12 Prozent aller Hörbücher und acht Prozent aller TV-Serien unlizenziert geladen.¹¹²

Über **P2P-Filesharing** wurden sieben Prozent aller Filme, -, vier Prozent der Hörbüchern und TV-Serien sowie jeweils drei Prozent der eBooks und Musik¹¹³ geladen.

Die Nutzung unlizenzierter **Streams**, die über Portale aufgefunden werden, lag bei Filmen bei 19 Prozent und bei TV-Serien bei zehn Prozent.¹¹⁴ Bei Musik, Hörbüchern und eBooks spielten Streams eine eher untergeordnete Rolle.¹¹⁵

In der DCN-Studie wurde der Trend bestätigt, dass die Zahl der illegalen Downloads abnimmt. Während sich 2009 noch 4,5 Mio. Menschen¹¹⁶ unlizenzierte Inhalte verschafften, waren es 2010 noch 3,7 Mio.¹¹⁷ Im Vergleich dazu stieg die Anzahl der Personen die kostenpflichtig Musik herunterladen von vier Mio. im Jahr 2006 auf 5,6 Mio im Jahr 2009.¹¹⁸ 2010 nutzen 6,6 Mio. kostenpflichtige Downloadplattformen.¹¹⁹

2. Einzelne Branchen

Im Vordergrund steht derzeit die unlizenzierte Nutzung von Musik, Film, Rundfunkinhalten, Büchern, Presseerzeugnissen, Computer- und Videospielesoftware sowie anderer Soft-

¹¹⁰ GfK, DCN-Studie, S. 13.

¹¹¹ GfK, DCN-Studie, S. 18.

¹¹² GfK, DCN-Studie, S. 18.

¹¹³ Die absoluten Zahlen sind bei Musik aufgrund der Vielzahl der Downloads aber hoch.

¹¹⁴ GfK, DCN-Studie, S. 18.

¹¹⁵ GfK, DCN-Studie, S. 18.

¹¹⁶ GfK, Brennerstudie 2010, S. 10.

¹¹⁷ GfK, DCN-Studie, S. 6.

¹¹⁸ GfK, Brennerstudie 2010, S. 25.

¹¹⁹ GfK, DCN-Studie, S. 19.

ware.¹²⁰ Wie stark Inhalte illegal genutzt werden, hängt von unterschiedlichen Faktoren ab, etwa der Verbreitung im Internet und dem Interesse der Nutzer. Filme und TV-Serien, gefolgt von Musik, sind weltweit am häufigsten betroffen.¹²¹

a. Musik

Musik wurde bereits früh unlizenziert unter Nutzern geteilt bzw. kopiert.¹²² Musikdateien eignen sich, im Vergleich zu audiovisuellen Inhalten, wegen ihres geringen Datenumfangs zur schnellen Verbreitung.

Der als „Krise der Musikindustrie“ apostrophierte Rückgang bestimmter Arten von Musiknutzung über Tonträger, wird als eigentliche Krise des CD-Geschäfts und damit der sog. „Major Labels“¹²³ bezeichnet.¹²⁴ Allerdings sind vom Rückgang der Verkaufszahlen ganz besonders auch die Künstler selbst und kleinere unabhängige Produktionsunternehmen betroffen, die die Auswirkungen zum Teil stärker spüren als die marktführenden Unternehmen.¹²⁵

Bei einer repräsentativen Befragung von 26.644 Online-Verbrauchern aus 53 Märkten weltweit, die vom internationalen Marktforschungsunternehmen *Nielsen* im Auftrag der weltgrößten Musikmesse *Midem*¹²⁶ im März 2011 durchgeführt wurde, gaben knapp über 20 Prozent der Europäer an, innerhalb der letzten drei Monate Musik über ein Filesharing-Programm illegal getauscht oder über ein Portal kostenfrei heruntergeladen zu haben.¹²⁷

In Deutschland waren unlizenzierte Musikdownloads statistischen Erhebungen zufolge in den Jahren 2002 und 2003 am stärksten verbreitet. Im Jahr 2002 fanden 622 Mio. unlizenzierte Musikdownloads statt, 2003 waren es 602 Mio.¹²⁸ Legale Angebote zum Download im Internet waren in diesen Jahren nicht vorhanden. Im Vergleich dazu waren es 2010 414 Mio. Musikdownloads aus sowohl lizenzierten wie unlizenzierten Quellen.¹²⁹ 185 Mio. einzelne Stücke und 46 Mio. Musikalben stammten dabei aus unlizenzierten Quellen. Im Jahr 2004 startete der Dienst iTunes als erster mit dem Vertrieb digitaler Musik über das Inter-

¹²⁰ Zur Kultur- und Kreativwirtschaft zählen neben den genannten noch die Teilmärkte Kunstmarkt, Markt für darstellende Künste, Designwirtschaft, Architekturmarkt und Werbemarkt, siehe BMWi, Forschungsbericht Nr. 577, S. 3.

¹²¹ *Envisional*, S.10 und 18.

¹²² *TERA Consultants*, S. 30.

¹²³ EMI, Sony Music Entertainment, Universal Music Group und Warner Music Group. Ein Musiklabel, Plattenlabel oder Label im eigentlichen Sinne ist in der Musikindustrie die eigenständig geführte Abteilung eines Tonträgerunternehmens, die Interpreten unter einem bestimmten Markennamen vertreibt. Bisweilen wird – so auch hier – mit einer gewissen begrifflichen Unschärfe unter „Label“ jedoch (auch) das Tonträger produzierende Unternehmen im Ganzen verstanden.

¹²⁴ *Karaganis*, S. 41.

¹²⁵ *IFPI*, DMR 2011, S. 22ff.

¹²⁶ *Midem (Marché international de l'édition musicale)* ist die weltgrößte Musikmesse, die als Plattform zur Ankündigung neuer Produkte, Musiker oder Branchenstrategien dient. Sie findet jährlich in Cannes statt.

¹²⁷ *Nielsen*, S. 8.

¹²⁸ *GfK*, Brenner-Studie, S. 23.

¹²⁹ *GfK*, DCN-Studie, S. 15.

net. Im selben Jahr stammten in Deutschland 91 Prozent aller Album-Downloads aus Filesharing-Quellen, im Jahr 2010 sind immerhin noch 74 Prozent.¹³⁰

Die **legale digitale Musikknutzung** im Internet hat also in den letzten Jahren stetig zugenommen. Digitale Verkäufe konnten im Jahr 2010 den Gesamtumsatzrückgang um 4,6 Prozent im Vergleich zum Vorjahr, der überwiegend durch Rückgänge im Bereich des Verkaufs physischer Tonträger verursacht wurde, zwar nicht kompensieren, aber zumindest abschwächen.¹³¹ 2011 soll das Umsatzvolumen des deutschen Musikmarkts erstmalig seit 1997 nicht zurückgegangen sein.¹³² In Deutschland stieg die Anzahl der Personen, die Musik aus dem Internet laden, von 12 Mio. im Jahr 2009 auf 15,6 Mio. im Jahr 2010.¹³³ Die Zahl der Nutzer in Deutschland, die Musik unlizenziert nutzen, sank,¹³⁴ während die Zahl derjenigen, die schon einmal legal Musik im Download im Netz erworben haben, um über eine Million Personen anstieg.¹³⁵

Beliebtestes Angebot für Online-Musikknutzung war in Deutschland 2010 das Streaming von Musikvideos¹³⁶; 6,9 Mio. Menschen haben davon Gebrauch gemacht.¹³⁷ An zweiter Stelle stehen kostenpflichtige Downloadplattformen¹³⁸, die von 6,6 Mio. Menschen genutzt wurden. Trotz der zunehmenden Anzahl lizenzierter Musikknutzer überwiegt die unlizenzierte Musikknutzung insgesamt. Denn Personen, die Musik unlizenziert aus dem Internet laden, betreiben dies mit hoher Intensität. So haben in 2010 1,8 Mio. Menschen etwa 103 Mio. Musikstücke heruntergeladen.¹³⁹ Zur unlizenzierten Nutzung wurden am häufigsten Sharehosting verwendet. 1,8 Mio. Menschen haben sich auf diese Weise Musik verschafft. 1,5 Mio. luden Musik aus P2P-Netzwerken.¹⁴⁰

Zur Musikknutzung im Internet existieren mittlerweile eine Reihe von Angeboten, die ähnlich wie die unlizenzierten Angebote dem Nutzerinteresse auf Zugang zu kostengünstigen und unbegrenzten digitalen Inhalten genügen. Neben den bekannten kostenpflichtigen Downloadplattformen und lizenzierten Videoplattformen bringt der Markt zunehmend sogenannte Abo- oder Freemium¹⁴¹-Modelle hervor. Den 258 Mio. unlizenzierten Musikkdownloads im Jahr 2008 stehen 111 Mio. Musikkdownloads aus legaler kostenloser oder kostenpflichtiger Quelle gegenüber.¹⁴²

¹³⁰ GfK, DCN-Studie, S. 60.

¹³¹ Bundesverband der Musikindustrie, Musikindustrie in Zahlen 2010, S. 12.

¹³² Heise Online: <http://www.heise.de/newsticker/meldung/Deutscher-Musikmarkt-hat-sich-stabilisiert-1414373.html>.

¹³³ GfK, Brenner-Studie 2010, S.21 und DCN-Studie, S. 12.

¹³⁴ GfK, Brenner-Studie, S. 21, von 3,8 auf 2,9 Mio.

¹³⁵ GfK, Brenner-Studie, S. 21, von 4,5 auf 5,6 Millionen.

¹³⁶ Z.B. MyVideo, YouTube.

¹³⁷ GfK, DCN-Studie, S. 66.

¹³⁸ Z.B. Musicload, iTunes.

¹³⁹ GfK, DCN-Studie, S. 15.

¹⁴⁰ GfK, DCN-Studie, S. 66.

¹⁴¹ Modelle, bei welchen der Nutzer zwischen kostenloser, werbeunterstützter Nutzung (Free) und kostenpflichtiger, werbefreier Nutzung (Premium) wählen kann.

¹⁴² GfK, Brenner-Studie, S. 23.

Insgesamt lässt sich also feststellen, dass sich, obwohl Musik im Internet weiterhin massenhaft illegal genutzt wird, ein positiver Trend der legalen, digitalen Musikknutzung abzeichnet.

b. Film- und Fernsehbranche

Im Vergleich zur Musikbranche war der Bereich Film und Fernsehen zunächst weniger stark von illegaler Nutzung betroffen. Zurückgeführt wird dies auf die für hohe Datenmengen ungeeigneten geringen Übertragungsraten im Internet in der Vergangenheit und auf die zunächst mangelnde Eignung der Endgeräte für die Nutzung größerer Videodateien.¹⁴³ Mit der technischen Weiterentwicklung von Breitbandnetzen und leistungsfähigeren Endgeräten, treten technische Hemmnisse zunehmend zurück.¹⁴⁴

Die Film- und Fernsehbranche weist gegenüber der Musik- und Buchbranche strukturelle Besonderheiten auf.¹⁴⁵ Zum einen unterscheiden sich Filmhersteller und Filmverwerter. Zum anderen sind die Kosten für die Herstellung eines Filmwerks und seine Verwertung deutlich höher als bei Musikstücken. Sie belaufen sich bei Kinofilmen aktuell auf durchschnittlich 3 bis 5 Mio. Euro und bei Fernsehfilmen auf 1,3 bis 1,8 Mio. Euro. Serien à 60 Minuten kosten 350.000 bis 800.000 Euro.¹⁴⁶

Die Verwertung eines Kinofilmes erfolgt in zeitlichen Abschnitten vom Kinostart, über DVD/Blu-Ray Auswertung zu VOD/EST (*Electronic Sell Through*) über Pay-TV zum Free-TV.¹⁴⁷ Diese zeitlichen Abschnitte überspannen gemeinsam einen Zeitraum von über 18 Monaten. Insofern besteht ein komplexes Geflecht exklusiver Rechtevergabe zur umfassenden und auskömmlichen Verwertung.¹⁴⁸

Die Filmindustrie ist schon länger von „physischer Piraterie“, etwa durch den Verkauf von unzulässigen DVD-Kopien, betroffen. Mittlerweile werden Werke vermehrt in digitaler Form im Internet unlizenziiert genutzt. Die Unternehmen reagieren darauf, indem sie zunehmend Lizenzen für Online-Geschäftsmodelle vergeben. Kostenpflichtige legale Geschäftsmodelle können sich aber nicht gegen kostenlose illegale Angebote behaupten.¹⁴⁹ Vor allem wird die o. a. zeitliche Verwertungsabstufung durch die sofortige Verfügbarkeit von Film- und TV-Inhalten auf unlizenziierten Plattformen, teilweise schon vor Kinostart, konterkariert. Bei Kinofilmen entspricht der Konsum der unlizenziiert genutzten Inhalte

¹⁴³ Hargreaves, S. 28.

¹⁴⁴ Hargreaves, S. 28.

¹⁴⁵ Produzentenallianz, S. 2.

¹⁴⁶ Produzentenallianz, S. 2.

¹⁴⁷ Produzentenallianz, S. 3.

¹⁴⁸ Produzentenallianz, S. 4.

¹⁴⁹ IFPI, S. 23.

dem Rang in den Kinocharts.¹⁵⁰ Bei den TV-Serien dominieren US-amerikanische Serien die unlicenzierten Kanäle.¹⁵¹

Illegale Nutzung von Kinofilm- und Fernsehangeboten über das Internet haben sich innerhalb der letzten zwei Jahre stark ausgeweitet. Im Jahr 2010 sollen im Vereinigten Königreich 14 Prozent der Internetnutzer sowohl Filme als auch TV-Programme aus P2P-Netzwerken heruntergeladen haben. Daneben wird Video-Streaming, als das weltweit am schnellsten wachsende Segment¹⁵², zunehmend zur illegalen öffentlichen Zugänglichmachung urheberrechtlich geschützter Inhalte verwendet. Bei der Verwendung von Streaming-Technologie kann der gewünschte Film innerhalb weniger Sekunden gestartet werden, da kein Download abgewartet werden muss. Die optische Qualität (Auflösung) bleibt aber oftmals hinter derjenigen aus P2P-Quellen zurück. Beliebte Streaming-Portale weisen monatliche Nutzerzahlen in Millionenhöhe auf.¹⁵³ Nach den Ergebnissen der britischen Analysefirma Envisional stellt P2P-Filesharing aber immer noch die meistgenutzte Technologie zur illegalen Nutzung geschützter Inhalte dar, mit weltweit viermal so vielen Nutzern wie illegales Video-Streaming.¹⁵⁴ Kinofilme und Fernsehserien sind nach deren Erhebungen, vor Musik, der am meisten illegal genutzte Inhalt. Auf den „Top 10.000 Torrent¹⁵⁵-Seiten“ sind nach diesen Erhebungen 35,3% Prozent der Inhalte Kinofilme und 12,7 Prozent TV-Serien, während nur 2,9 Prozent auf Musik entfallen sollen. Auf Sharehosting-Angebote sollen 35,8 Prozent geschützte Kinofilme, 8,5 Prozent ebensolche TV-Inhalte und 10,1 Prozent Musik entfallen.¹⁵⁶

Dieses Ergebnis spiegeln die Erkenntnisse der DCN-Studie auch für den deutschen Markt wieder. **Kinofilme** im Internet werden danach überwiegend, nämlich von 49 Prozent, unlicenziert genutzt. 44 Prozent der Nutzer gaben an, ausschließlich Filme aus lizenzierten Quellen zu konsumieren. Nur sechs Prozent greifen gelegentlich auf beide Quellen zurück.¹⁵⁷ TV-Serien konsumieren 54 Prozent ausschließlich legal, während 39 Prozent unlicenzierte Angebote und acht Prozent beides nutzen.¹⁵⁸ Kinofilme werden zumeist über Videostreaming-Plattformen¹⁵⁹, gleichauf mit unlicenzierten Streaming-Portalen¹⁶⁰ konsumiert, die jeweils 1,3 Mio. Nutzer verzeichnen.¹⁶¹ Sharehostingangebote wurden von 1,2 Mio. Nutzern zum Filmkonsum verwendet, gefolgt von kostenpflichtigen Downloadplatt-

¹⁵⁰ Karaganis, S. 46.

¹⁵¹ Karaganis, S. 46.

¹⁵² *Envisional*, S. 19, unter Berufung auf Sandvine, Cisco und Arbor Networks.

¹⁵³ *Envisional*, S. 20.

¹⁵⁴ *Envisional*, S. 22.

¹⁵⁵ Kollaboratives Filesharing-Protokoll zum P2P-Filesharing.

¹⁵⁶ *Envisional*, S. 10 und S. 18.

¹⁵⁷ *GfK*, DCN-Studie, S. 89.

¹⁵⁸ *GfK*, DCN-Studie, S. 90.

¹⁵⁹ Z.B. MyVideo, YouTube.

¹⁶⁰ Z.B. kino.to.

¹⁶¹ *GfK*, DCN-Studie, S. 91.

formen¹⁶² mit einer Mio. Nutzern, während 0,6 Mio. Nutzer über P2P-Netzwerke auf Film- und Fernsehinhalte zugegriffen.¹⁶³

Rechteinhaber gehen davon aus, dass im Jahr 2010 312 Mio. Kinofilme unlicenziert allein über Sharehoster-Dienste genutzt wurden, während lediglich 226 Mio. Filmkopien legal vermarktet worden sind.¹⁶⁴ Fernsehserien wurden von 2,1 Mio. Nutzern auf Videostreaming-Plattformen und von 2,0 Mio. Nutzern über Online-Mediatheken konsumiert. Eine Mio. Nutzer bedienten sich unlizenzierter Streaming-Portale, gefolgt von 0,8 Mio. Nutzer kostenpflichtiger lizenzierter Downloadplattformen und 0,7 Mio. Nutzern von Sharehostingangeboten. Aus P2P-Netzwerken wurden 0,4 Mio. TV-Serien heruntergeladen.¹⁶⁵

c. Software

Neben Musik, Fernsehen und Film verzeichnet auch der Softwarebereich Einbußen durch illegale Nutzung. Unter sog. „Softwarepiraterie“ versteht die Business Software Alliance (BSA), soweit das Internet als Verbreitungsform betroffen ist, die Zugänglichmachung und den Download von unlizenzierter Software, die Versendung von unlizenzierter Software per Email oder das Anbieten von Technologien zum Knacken von Kopierschutz im Internet.¹⁶⁶ Auch die sog. „Unterlizenzierung“, durch Nutzung einer für einen Computer lizenzierten Software auf mehreren Geräten, zählt zur illegalen Softwarenutzung.¹⁶⁷ Unter illegale Software-Nutzung wird auch Zugänglichmachung und Download von Software in P2P-Netzwerken oder auf Sharehoster-Servern gefasst.

Von der BSA stammen zwar die durchgängigsten Erhebungen zu „Piraterieverhalten“ im Hinblick auf Software. Deren Ergebnisse werden aber auch am stärksten kritisiert.¹⁶⁸ Für 2010 wird der Wert unlizenzierter Softwarenutzung durch die BSA weltweit auf 59 Mrd. US-\$ geschätzt. Dies stellt eine Verdoppelung gegenüber 2003 dar.¹⁶⁹ Ein erheblicher Teil dieses Wachstums wird der in dem entsprechenden Zeitraum erheblichen zunehmenden Verbreitung von Computern zugeschrieben.¹⁷⁰

Die deutlich höheren Zahlen im Vergleich zu anderen Branchen decken sich nicht mit den Erkenntnissen anderer Studien zur Verfügbarkeit von Software in unlizenzierter Kanälen.

¹⁶² Z.B. Maxdome.

¹⁶³ GfK, DCN-Studie, S. 91.

¹⁶⁴ Internet-Report II/2011, S. 1.

¹⁶⁵ GfK, DCN-Studie, S. 92.

¹⁶⁶ TERA Consultants, S. 44.

¹⁶⁷ *Envisional*, S. 10 und S. 18: Der Anteil an Software auf den Top 10.000 Torrent-Seiten soll 2010 4,2 Prozent betragen haben, bei den Sharehostern sollen es 10 Prozent gewesen sein.

¹⁶⁸ Kritisiert wird u.a. eine unterstellte eins-zu-eins Substitution (in der Vergangenheit) entgangener Verkäufe durch Piraterie (was beispielsweise die Möglichkeit eines Ausweichen auf Open-Source-Produkte ausblendet), ungenügende Transparenz zugrundeliegender Methodik und die Nicht-Berücksichtigung positiver Netzwerkeffekte (Lock-In Effekt), etc. hierzu ausführlich *Karaganis*, S. 6 und S. 51.

¹⁶⁹ *Business Software Alliance*, S. 2.

¹⁷⁰ *Karaganis*, S. 12.

Der Anteil an Software auf den „Top 10.000 Torrent-Seiten“ soll im Jahr 2010 4,2 Prozent betragen haben, bei Sharehostingangeboten sollen es 10 Prozent gewesen sein. Im weltweiten Vergleich ist die Softwarepiraterie-Rate in der EU mit 35 Prozent vergleichsweise gering.¹⁷¹ Deutschland liegt mit 27 Prozent an zwölfter Stelle unter den 30 Ländern mit den niedrigsten Piraterieraten weltweit. Die geringsten Probleme haben auf den Plätzen eins bis drei die USA, Japan und Luxemburg.¹⁷²

d. Games (Computer- und Videospielesoftware)

Von illegalem Nutzerverhalten im Internet sind auch Spielehersteller betroffen. Der Umsatz mit Computer- und Videospielesoftware betrug 2010 in Deutschland insgesamt 1,86 Mrd. Euro. Dies entspricht einer Steigerung um 3 Prozent.¹⁷³ In den USA erreichten die Umsatzzahlen 2008 mit 11,7 Mrd. US-, eine Erhöhung von 28 Prozent gegenüber 2007.¹⁷⁴ Konsolenspiele machen dabei mit ca. 39 Prozent den überwiegenden Umsatzanteil aus.¹⁷⁵ Dennoch befürchtet auch die Spielebranche, dass die zunehmende unlizenzierte Nutzung ihrer Produkte negative Auswirkungen auf die Einnahmen haben könnte.¹⁷⁶ Der Bundesverband Interaktiver Unterhaltungssoftware (BIU) geht davon aus, dass in Deutschland zwischen 5 und 10 Prozent aller Nutzer auf illegale Angebote zurückgreifen.¹⁷⁷ Die Anbieter versuchen sich zu schützen, indem sie technische Kopierschutzvorrichtungen nutzen oder das Spielen nur serverbasiert ermöglichen. Sog. Konsolenspiele waren in der Vergangenheit weniger anfällig für Piraterie; wobei die Entwicklung in Richtung leichter Überwindung von Sperren gehen könnte.¹⁷⁸

e. Bücher

Buchverlage sehen sich durch das Internet insgesamt neuen Herausforderungen gegenüber. In den USA waren im Februar 2011 eBooks erstmalig das meistverkaufte Format.¹⁷⁹ Mit der zunehmenden Verbreitung von Hardware zum digitalen Lesen werden neue Märkte für die Buchbranche erschlossen. Gleichzeitig nimmt die Gefahr digitaler Piraterie zu.¹⁸⁰

Insoweit befürchtet man ähnliche Entwicklungen wie in der Musikbranche. Dort sanken die Produktionskosten zunächst, als die CD Marktanteile der Schallplatte übernahm. Mit der Möglichkeit der unautorisierten Verbreitung im Internet, sanken die Verkaufszahlen

¹⁷¹ *Business Software Alliance*, S. 4.

¹⁷² *Business Software Alliance*, S. 3.

¹⁷³ BIU: <http://www.biu-online.de/de/fakten/marktzahlen.html>, zuletzt aufgerufen am 30.8.2011.

¹⁷⁴ Karaganis, S.48 unter Berufung auf ESA.

¹⁷⁵ Karaganis S. 49 unter Berufung auf ISFE 2009.

¹⁷⁶ *Envisional*, S.10 und S.18: Der Anteil an Games auf den Top 10.000 Torrent-Seiten soll 2010 3,9 Prozent PC Games, 2,8 Prozent Konsole Games und 1,5 Prozent Anima betragen haben, bei den Sharehostern sollen es insgesamt 9,4 Prozent gewesen sein.

¹⁷⁷ BIU: <http://www.biu-online.de/de/themen/urheberrecht.html>, zuletzt aufgerufen am 30.8.2011.

¹⁷⁸ Karaganis, S. 48.

¹⁷⁹ *Association of American Publishers*, February 2011 sales report, abrufbar unter: www.publishers.org/press/30, zuletzt aufgerufen am 29.8.2011.

¹⁸⁰ IFPI, S. 23.

der Musikbranche.¹⁸¹ Infolge der zunehmenden Digitalisierung von Büchern und der Einführung digitaler Lesegeräte¹⁸² wachsen die Befürchtungen, dass die Verlagsbranche Ähnliches erwartet.¹⁸³ Im Jahr 2010 sollen Suchanfragen in Internetsuchmaschinen nach unlicenzierten Kopien von eBooks um 50 Prozent gestiegen sein. Seit Einführung des iPads sollen sich unlicenzierte Downloads um 20 Prozent erhöht haben. Der Anteil an eBooks und Hörbüchern auf den „Top 10.000 Torrent-Seiten“ soll 2010 0,2 Prozent betragen haben, bei den Sharehostern sollen es 2,6 Prozent gewesen sein.¹⁸⁴

In Deutschland beziehen Nutzer von Hörbüchern und Hörspielen diese zu 78 Prozent aus legalen Quellen.¹⁸⁵

18 Prozent laden ausschließlich aus unlicenzierten Quellen herunter. Fünf Prozent nutzen sowohl lizenzierte als auch unlicenzierte Angebote.¹⁸⁶ Bei eBooks sind es 60 Prozent der Nutzer die ausschließlich auf lizenzierte, 35 Prozent die ausschließlich auf unlicenzierte Quellen und sechs Prozent die auf beides zurückgreifen.¹⁸⁷ Die weitere Entwicklung in dieser erst relativ neu betroffenen Branche bleibt abzuwarten.

f. Zeitungen und Zeitschriften

Die zunehmende Verbreitung von Tablet-PCs hat auch neue Märkte für Zeitschriften-Verlage eröffnet.¹⁸⁸ Jüngere Generationen sind es bereits gewohnt, fast ausschließlich auf Bildschirmen, statt auf Papier zu lesen.¹⁸⁹ Die marktwirtschaftlichen Chancen, aber auch die Gefahr, dass es zu einer Zunahme unlicenzierter Zugänglichmachung digitaler Produkte kommt, beschränkt sich nicht allein auf die Buchbranche. Viele Magazine und Zeitungen bieten ihre Ausgaben – neben einem Gratisauftritt im Internet mit einem umfangreichen Informationsangebot – auch als ePaper an, welches das Risiko unlicenzierter Kopien birgt. An anderer Stelle werden Ausschnitte von Nutzern gescannt und ohne die Erlaubnis der Herausgeber ins Internet gestellt.¹⁹⁰ Zeitungen- und Zeitschriftenverlage haben in der Vergangenheit bereits stark unter der kostenlosen, legalen Online-Konkurrenz gelitten.¹⁹¹ Es bestehen Befürchtungen, dass manche Verlagshäuser durch eine mögliche weitere Ab-

¹⁸¹ Hargreaves, S. 28.

¹⁸² Harris Interactive, S.41 und 48: Im Vereinigten Königreich besaßen im Oktober 2010 acht Prozent der Gesamtbevölkerung ein iPad und fünf Prozent ein anderes elektronisches Lesegerät.

¹⁸³ Gelles /Edgecliffe-Johnson, Publishers rush to erect defence against piracy, Financial Times vom 15.4.2011.

¹⁸⁴ Envisional, S.10 und S. 18.

¹⁸⁵ GfK, DCN-Studie, S. 79.

¹⁸⁶ GfK, DCN-Studie, S. 79.

¹⁸⁷ GfK, DCN-Studie, S. 80, dies ergibt insgesamt 101 Prozent, Angaben ob es sich um gerundete Werte handelt, fehlen.

¹⁸⁸ Hargreaves, S. 28.

¹⁸⁹ TERA Consultants, S. 55.

¹⁹⁰ TERA Consultants, S. 56.

¹⁹¹ TERA Consultants, S. 56.

nahme ihrer Verkaufszahlen aufgrund unlizenzierter Zugänglichmachung ihrer Produkte in ihrer Existenz bedroht werden.¹⁹²

3. Zwischenergebnis

Die fortschreitende Digitalisierung hat die oben genannten Branchen vor neue Herausforderungen gestellt und das Risiko der unlizenziierten Verbreitung von Kopien ihrer Produkte erhöht. Es gilt nun, den Blick auf die wirtschaftlichen Auswirkungen zu lenken.

V. Wirtschaftliche Auswirkungen von Urheberrechtsverletzungen

In der Kultur- und Kreativwirtschaft existierten im Jahr 2009 nach Schätzungen knapp 237.000 Unternehmen. Mit knapp 787.000 abhängig Beschäftigten erzielten sie zusammen ein Umsatzvolumen von insgesamt mehr als 131 Milliarden Euro.¹⁹³ Dieser Wirtschaftszweig gilt als wichtige Quelle für originäre Innovationsideen.¹⁹⁴ Der Produktionsfaktor „Kreativität“ kann sich aber nur dort entwickeln, wo es ein soziales, kreatives und kulturelles Umfeld gibt, das durch Bildung und Wissen gefördert wird, sowie eine Wirtschaft, die in Kultur und kulturbezogene Kreativität investiert.¹⁹⁵ Daher ist eine Wirtschaftspolitik ohne Kulturpolitik nicht möglich.¹⁹⁶ Ihr Mehrwert gegenüber anderen förderungswürdigen Branchen liegt in der kulturellen Produktion, die nicht nur der Bedürfnisbefriedigung der unmittelbaren Konsumenten dient, sondern der Gesellschaft insgesamt nutzt.¹⁹⁷ Die wirtschaftlichen Auswirkungen von Urheberrechtsverletzungen im Internet sollen daher nachfolgend beleuchtet werden.

1. Auswirkungen auf die Gesamtwirtschaft

In diesem Zusammenhang wird untersucht, ob Onlinepiraterie auf volkswirtschaftlicher Ebene keine oder nur geringfügige negative Folgen zeigt, da Geld, das nicht für Produkte der Kreativwirtschaft ausgegeben wird, von dem Nutzer ggf. in einer anderen Branche – etwa in Konsumgüter – investiert wird.¹⁹⁸ Was sich als Verlust für eine Branche darstellt, könne ein Gewinn für andere oder für die Gesellschaft als Ganze sein.¹⁹⁹ Piraterie, so wird

¹⁹² TERA Consultants, S. 56.

¹⁹³ BMWi 2010, Forschungsbericht Nr. 594, S. 43.

¹⁹⁴ BMWi, Forschungsbericht Nr. 577, S. 3.

¹⁹⁵ Mundelius, S. 4.

¹⁹⁶ Mundelius, S. 4.

¹⁹⁷ Mundelius, S. 4.

¹⁹⁸ Hargreaves, S. 73: Selbst unter Zugrundelegung der durch die Content-Industrie verwendeten Zahlen, die Hargreaves für zu hoch hält, gelangt er zu dem Ergebnis, dass Urheberrechtsverletzung unter 0,1 Prozent aller wirtschaftlicher Aktivität ausmachen.

¹⁹⁹ Karangnis, S. 16.

geltend gemacht, verursache (lediglich) eine Verschiebung der Einnahmen, nicht aber einen Verlust.²⁰⁰ Ausgaben innerhalb anderer Branchen verursachten (dort) Steuerabgaben, neue Arbeitsplätze und Investitionen in Infrastruktur.²⁰¹ Tatsächlich gibt es andere Wirtschaftszweige, die mit einiger Wahrscheinlichkeit von der weltweiten Verbreitung von Online-Piraterie profitieren. Hier kann man, im Hinblick auf die Nachfrage nach Anschlüssen mit höherer Breitband-Geschwindigkeit, an die Diensteanbieter denken, an den Markt für elektronische Endgeräte²⁰² oder auch an Suchmaschinenbetreiber, die vom Internetverkehr profitieren und andere Beteiligte der „Internetwirtschaft“. Auch wer beim Anbieten unlizenzierter Produkte, etwa durch Werbung, verdient, profitiert rein wirtschaftlich betrachtet.²⁰³ Für die Gesamtwirtschaft ist Piraterie daher nicht zwingend schädlich.

2. Auswirkungen auf die Umsatzentwicklung der betroffenen Branchen

Inwieweit sich das Vorkommen von Piraterie auf die Umsatzentwicklung der betroffenen Branchen auswirkt ist fraglich. Betrachtet man die gesamten Umsatzzahlen der betroffenen Industrien in Deutschland in den letzten Jahren, so lassen sich bei dieser Betrachtung jedenfalls keine gravierenden, durch die illegale Nutzung verursachten Umsatzeinbrüche aller Branchen beobachten.

Umsätze Teilmärkte der Kultur- und Kreativwirtschaft in Deutschland

Teilmarkt	2006	2007	2008	2009	2010 (vorläufige Zahlen)
Musikwirtschaft	5.392	5.282	5.596	5.538	6.380
Buchmarkt	14.743	14.623	14.446	14.766	14.390
Filmwirtschaft	7.609	7.044	7.283	7.150	8.950
Rundfunkwirtschaft	9.797	10.232	10.085	9.277	6.820
Pressemarkt	27.312	27.916	28.065	27.160	30.470
Software-/Games-Industrie	24.103	27.465	29.545	28.067	26.41

Umsatz in Mio. €, Quelle: BMWi, Kultur- und Kreativwirtschaft 2003- 2009 nach elf Teilmärkten, Forschungsbericht Nr. 589.

²⁰⁰ Karaganis, S. 16.

²⁰¹ Karaganis, S. 16.

²⁰² Z.B. Laptops, Mp3-Player, u.ä.; so auch Oberholzer-Gee/Strumpf, S. 21.

²⁰³ Handelt es sich um (organisierte) Kriminalität entsteht allerdings insoweit ein volkswirtschaftlicher Schaden, dass diese Einnahmen nicht versteuert werden, siehe auch Hargreaves, Supporting Document CC, S. 5.

Dies ist auch nicht zu erwarten. Die Ursachen für die Entwicklung von Umsätzen sind multikausal und den Einfluss einzelner Faktoren exakt zu bestimmen nur sehr begrenzt möglich. Es ist nicht anzunehmen, dass sich Piraterie auf die Umsatzentwicklung im gesamten Markt einer Branche auswirkt. Anfällig sind allein die Bereiche, in welchen das Piraterieangebot ein hinreichendes Substitut für den Erwerb eines Produktes darstellt. So wird in der Musikwirtschaft der Verkauf von Musikinstrumenten von Online-Piraterie nicht bedroht. Hingegen sollen die Umsätze aus dem Verkauf von Musikaufnahmen in den letzten zehn Jahren stark zurückgegangen sein – in Deutschland von 2,63 Mrd. Euro im Jahr 2000 um über 40 Prozent auf 1,571 Mrd. in 2009.²⁰⁴ In 2011 soll das Umsatzvolumen des deutschen Musikmarkts erstmalig seit 1997 nicht zurückgegangen sein.²⁰⁵ Weltweit sollen nach Angaben der *International Federation of the Phonographic Industry* (IFPI) die Umsatzzahlen aus Musikverkäufen von 33,7 Mrd. US-\$ in 2001 auf 16 Mrd. US-\$ in 2011 gesunken sein.²⁰⁶ Vertreter der Rechteinhaber führen diesen Rückgang auf einen seit 1999 stattfindenden Boom der illegalen Nutzung zurück. Gegner dieser Begründung halten auch andere Ursachen für zumindest mitursächlich;²⁰⁷ verringerte Kosten für die Produktion und den Vertrieb von Musik würden international alternative Geschäftsmodelle ermöglichen.²⁰⁸ Auch in den meisten europäischen Ländern sind die Umsätze aus dem physischen und digitalen Musikverkauf von 2009 auf 2010 gesunken.

Umsatzentwicklung des europäischen Musikverkaufs 2009-2010

(physischer und digitaler Musikverkauf ohne Performance Rights)

Land	Umsatz 2009 in Mio. €	Umsatz 2010 in Mio. €	Verlust/ Zu- wachs
Deutschland	1.546,8	1.528,4	- 1,2 %
Frankreich	993,3	965,5	- 2,8 %
Großbritannien	1.531,8	1.510,4	- 1,4 %
Irland	-	-	-
Schweden	144,9	154,4	+ 6,6 %
Finnland	73,8	73,6	- 0,2 %
Italien	243,5	253,5	+ 4,1 %

²⁰⁴ VUT, S. 15 unter Berufung auf die GfK.

²⁰⁵ Heise Online: <http://www.heise.de/newsticker/meldung/Deutscher-Musikmarkt-hat-sich-stabilisiert-1414373.html>.

²⁰⁶ IFPI, *The Recording Industry in Numbers*, 2001 and 2011.

²⁰⁷ Karagnis, S. 42.

²⁰⁸ Karagnis, S. 44.

Niederlande	263,2	232,3	- 11,7 %
Spanien	229,6	185,1	- 19,4 %
Österreich	179,9	163,2	- 9,3 %
Belgien	153,8	159,6	+ 3,8 %
Polen	91,3	97,6	+ 6,9 %
Dänemark	116,1	114,7	- 1,2 %
Griechenland	81,0	62,8	- 22,4 %
Portugal	53,8	38,3	- 28,8 %
Tschech. Rep.	33,4	25,7	- 23,0 %
Ungarn	22,9	19,6	- 14,5 %

Quelle: Bundesverband Musikindustrie, Musikindustrie in Zahlen 2010, S. 61.

Ein direkter Zusammenhang zwischen der Nutzung illegaler Kopien und dem Rückgang der Umsatzzahlen liegt nahe, ist aber nur sehr schwer nachzuweisen. Hierzu bekannt ist die Untersuchung von *Adermon&Liang: Piracy, Music, and Movies: A Natural Experiment* aus dem Jahr 2010 für Schweden. Sie maß den Internetverkehr vor und nach Einführung einer Gesetzesänderung zur besseren Verfolgung von Urheberrechtsverletzungen im Internet in Schweden über einen Zeitraum von 9 Monaten.²⁰⁹ Nach Inkrafttreten der Gesetzesreform wurde ein Rückgang des Internetverkehrs um 18 Prozent für die folgenden sechs Monate gemessen. In den Vergleichsländern Norwegen und Finnland war im gleichen Zeitraum kein derartiger Rückgang festzustellen. Daraus folgern *Adermon&Liang*, dass es sich bei den eingestellten Internetaktivitäten um illegales Nutzungsverhalten handelte, welches aus Angst vor einer Rechtsverfolgung aufgegeben wurde.²¹⁰ Im selben Zeitraum stieg die Anzahl der physischen Musikverkäufe um 27 Prozent und der digitalen Musikverkäufe um 48 Prozent.²¹¹ Wäre dieser Effekt konstant, so wären physische Musikverkäufe in Schweden um 72 Prozent höher und im Bereich digitaler Musikverkäufe sogar 131 Prozent höher.

Umsatzrückgänge gab es in Europa in den letzten Jahren vor allem im Bereich der physischen Musikverkäufe, eine scheinbar natürliche Entwicklung im Zuge fortschreitender Digitalisierung. Nach den Ergebnissen von *Adermon&Liang* ist die Abnahme physischer Musikverkäufe in Schweden in den Jahren 2000 und 2008 allerdings zu 43 Prozent auf Piraterievorkommen zurückzuführen.²¹² Dies stützt die Behauptung der Tonträgerindustrie

²⁰⁹ Hierzu ausführlich unten S.180.

²¹⁰ *Adermon&Liang*, S. 15.

²¹¹ *Adermon&Liang*, S. 18.

²¹² *Adermon&Liang*, S. 16.

die Umsatzrückgänge der vergangenen Jahre, seien schwerwiegend auf die illegale Konkurrenz zurückzuführen. Tatsächlich ging der Umsatz aus Tonträgerverkäufen auch in den meisten anderen europäischen Ländern in den letzten Jahren zurück. Vergleichbare Erhebungen wie die aus Schweden, die untersuchen inwieweit Piraterie hierfür ursächlich ist, existieren jedoch nicht.

Umsatzentwicklung der europäischen Tonträgermärkte 2007-2008

Land	Umsatz 2007 in Mio. €	Umsatz 2008 in Mio. €	Verlust/ Zu- wachs
Deutschland	1.662,0	1.601,7	- 3,6 %
Frankreich	1.175,0	1.060,5	- 9,7 %
Großbritannien	2.171,5	1.652,4	- 23,9 %
Irland	95,5	-	-
Schweden	162,0	146,7	-9,5 %
Finnland	94,1	93,0	- 1,2 %
Italien	392,0	314,7	- 19,7 %
Niederlande	294,0	254,0	- 13,6 %
Spanien	309,0	278,7	- 9,8 %
Österreich	214,0	185,5	- 13,3 %
Belgien	182,0	182,9	+ 0,5 %
Polen	97,0	113,7	+ 17,2 %
Dänemark	137,9	121,9	- 11,6 %
Griechenland	127,7	95,1	- 25,5 %
Portugal	72,2	64,5	- 10,8 %
Tschech. Rep.	32,1	40,4	+ 25,9 %
Ungarn	39,4	28,0	- 28,9 %

Quelle: Bundesverband Musikindustrie, Musikindustrie in Zahlen 2009, S. 50.

Ein ähnlich konstanter Rückgang der Umsätze lässt sich bei den Produkten anderer Branchen, außerhalb der Musikindustrie nicht erkennen. Dies mag daran liegen, dass wie oben dargestellt, andere Branchen erst seit jüngerer Zeit betroffen sind.

Nach den Erkenntnissen von *Adermon&Liang* hatte der Rückgang des Piraterieverhaltens keine der Musikverkäufe vergleichsweise Substitutionswirkung für den Verkauf von Kinokarten oder DVDs.²¹³ Die Verkaufszahlen für diese nahmen in dem untersuchten Zeitraum nicht spürbar zu. Daraus folgern *Adermon&Liang*, dass der Kinobesuch oder der DVD-Erwerb kein Substitut für die illegale Filmbeschaffung ist. Für diesen Bereich existieren auch weniger gute, legale digitale Geschäftsmodelle, wie im Bereich Musik in Schweden. Zahlen, inwieweit Nutzer auf andere legale Nutzungsformen ausweichen, wie bspw. das Fernsehen, existieren keine.

Die in Schweden festgestellten Effekte der Abnahme des Rückgangs des Piraterieverhaltens verschwanden nach sechs Monaten wieder. Als Ursache wird vermutet, dass es nicht zu einer tatsächlichen Rechtsverfolgung aufgrund der neuen Gesetzeslage kam. Die Nachfrage nach legaler Musik sank dadurch wieder, vor allem bei den physischen Musikverkäufen. Bei digitalen Musikverkäufen blieb die Umsatzsteigerung konstant, was andeutet, dass die Migration zur Legalität in diesem Bereich langfristig war und die Nutzer Geschäftsmodelle der legalen, digitalen Musiknutzung als echtes Substitut für die illegale Nutzung entdeckten.²¹⁴

3. Auswirkungen auf die Kreativwirtschaft

Dass eine massenhafte, unlicenzierte Nutzung der Produkte der Kreativwirtschaft stattfindet, wurde oben dargestellt und ist unbestritten. Daher ist es schwer vorstellbar, dass dort wo keine erheblichen Umsatzeinbrüche zu erkennen sind, die massenhafte illegale Nutzung keinerlei Auswirkungen hat. Wenn Geld aufgrund kostenloser Ersatzprodukte nicht ausgegeben wird, dann stellt sich die Frage, ob die Umsätze der betroffenen Branchen nicht höher ausgefallen wären, wenn die illegalen Produkte nicht verfügbar gewesen wären. Beziffern müsste man also die verlorenen Verkäufe der betroffenen Branchen. Dies bereitet jedoch tatsächliche Schwierigkeiten. Außerdem ist denkbar, dass durch Umsatzrückgänge oder unsicheres zukünftiges Wachstum eine Verunsicherung bei den betroffenen Branchen ausgelöst wird, die Investitionen hemmt. Zuletzt sind die Auswirkungen der illegalen Konkurrenz auf legale digitale Geschäftsmodelle zu betrachten.

²¹³ *Adermon&Liang*, S. 18.

²¹⁴ *Adermon&Liang*, S. 18.

a. Methodische Schwierigkeiten bei der Ermittlung der Auswirkungen

Die vorhandenen Ergebnisse lassen konkrete Angaben über Auswirkungen von Piraterie auf das Wirtschaftswachstum nur begrenzt zu²¹⁵, weil sich die wirtschaftlichen Verluste für die betroffenen Branchen rechnerisch nur schwer exakt feststellen lassen. Vorhandene Studien²¹⁶ versuchen etwa Berechnungen entgangener Umsätze mit Hilfe einer **Substitutionsrate** anzustellen. Dabei wird ein Wert ermittelt bzw. geschätzt, der in etwa den verlorenen entgeltlichen Geschäften entsprechen soll.²¹⁷ Das Problem dieser Methode liegt in der Festlegung einer Substitutionsrate²¹⁸, die sich nur auf hypothetische Annahmen über alternatives rechtliches Kaufverhalten stützen kann. Verlässliche, konkrete Zahlen sind unter solchen Voraussetzungen nur sehr schwer zu ermitteln.

b. Konkrete Ansätze zur Feststellung wirtschaftlicher Auswirkungen

Es lassen sich, wie oben erwähnt, im Wesentlichen drei Punkte ausmachen, die wirtschaftliche Auswirkungen widerspiegeln.

- Zunächst wird über die Frage nach dem Einfluss der Piraterie auf das wirtschaftliche Wachstum durch verlorene entgeltliche Geschäfte diskutiert.
- Zudem ist zu fragen, ob sich Piraterie negativ auf den Anreiz zur Schaffung kreativer Werke auswirkt.²¹⁹
- Schließlich ist zu erwägen, inwieweit Geschäftsmodelle für die Digitale Welt durch illegale und kostenlose Alternativnutzung ausgeschlossen werden.

Im Folgenden soll zu ausgewählten Überlegungen zur Ermittlung wirtschaftlicher Auswirkungen auf die Kreativbranche Stellung genommen werden, darunter das Ergebnis einer staatlichen Untersuchung im Vereinigten Königreich.

aa) Ermittlungen im Rahmen des „Impact Assessment“ im Vereinigten Königreich

Im Vereinigten Königreich wurden die ökonomischen Auswirkungen von Onlinepiraterie ermittelt. Die Analyse wurde durchgeführt, weil ein wesentlicher Grund für die Schaffung des Warnhinweissystems die mutmaßlichen durch Urheberrechtsverletzungen verursachten wirtschaftlichen Schäden waren, die der Gesetzgeber minimieren wollte. Um das Gesetzgebungsverfahren durch eine Kosten-Nutzen-Analyse abzusichern und den ökonomischen Nutzen des neuen Modells zu ermitteln, wurde ein *Impact Assessment* vorgelegt. Dabei handelt es sich um eine besondere Form der Gesetzesbegründung, die Kosten und

²¹⁵ Hargreaves, S. 73.

²¹⁶ Z.B. Tera Consultants.

²¹⁷ Rechenbeispiel: Wird eine Substitutionsrate von zehn Prozent festgelegt, wird unterstellt, dass ohne das kostenfreie, illegale Angebot für jeweils zehn illegale Downloads eine legale kostenpflichtige Nutzung stattgefunden hätte.

²¹⁸ Tatsächlich variieren die Ergebnisse zwischen 0-20 Prozent. Eine Liste mit einem Überblick zu verschiedenen Studien zu dieser Problematik findet sich z.B. in *BIS, dcms, Intellectual Property Office: Impact Assessment*, S. 69.

²¹⁹ So Hargreaves, S. 72.

Nutzen des Vorhabens in ein Verhältnis zueinander setzt. Der Ministerialverwaltung ging es darum, bereits zu Anfang herauszustellen, welche Kosten den am Warnhinweismodell bei Diensteanbietern, Rechteinhabern und Anschlussinhabern auf der einen Seite und beim Staat auf der anderen Seite entstehen.

Die Kosten-Nutzen-Analyse²²⁰ wurde von drei staatlichen Stellen, nämlich dem *Department for Business, Innovation and Skills*, dem *Department for Culture, Media and Sport* und dem *Intellectual Property Office* erstellt.

Nach dem Ergebnis dieser Untersuchung ergäben sich bei einem Verzicht auf ein Warnhinweismodell Verluste der Kreativwirtschaft in Höhe von jährlich **£400 Mio.**²²¹ Unsicherheiten, die daher rühren, dass Langzeitauswirkungen von Urheberrechtsverletzungen im Internet noch unbekannt sind, weil es sich um ein neues Phänomen handelt,²²² werden dabei in Kauf genommen. Grundlage für die Berechnung sind Werte die durch die Musik-, Film- und TV-Industrie und von den drei vorgenannten Behörden erhoben worden sind. Für die Software- und Videospielebranche wurde unterstellt, dass die Auswirkungen mit denen der anderen Branchen vergleichbar sind. Im Einzelnen wurden dabei £152 Mio. für die Film- und TV-Industrie²²³, £160 Mio. für die Musik-Industrie²²⁴ und £80 Mio. für die Software- und Videospiele-Industrie²²⁵ angesetzt. Insgesamt ergeben sich damit **Verluste** in Höhe von £392 Mio., die in der Ergebnisdarstellung des *Impact Assessment* auf **£400 Mio.** aufgerundet wurden.²²⁶

bb) Auswirkungen auf das wirtschaftliche Wachstum in der Europäischen Union

Eine der meistbeachteten Studien zu den Auswirkungen von physischer und digitaler Piraterie auf die Kreativwirtschaft innerhalb der europäischen Union stammt von TERA Consultants. Sie ist die einzige, die in diesem Umfang die wirtschaftlichen Auswirkungen von Piraterie auf die Kreativwirtschaft innerhalb der gesamten EU zu messen versucht und wurde im Auftrag der Internationalen Handelskammer und *Business Action to Stop Counterfeiting and Piracy* (BASCAP) erstellt und im März 2010 veröffentlicht.

Die Studie basiert nicht auf eigenen Erhebungen, sondern wertet Ergebnisse vergangener Untersuchungen und Umfragen aus.²²⁷ Zur Messung des Wertschöpfungsbeitrages der Kreativindustrie zur Wirtschaftsentwicklung der Europäischen Union bedient sie sich Re-

²²⁰ Erstellt auf Grundlage des *Digital Entertainment Survey 2008* und *NERA Economic Consulting, The Costs and Benefits to ISPs of Proposed Measures to Curb Illegal File Sharing*, Dezember 2009.

²²¹ *BIS, dcms, Intellectual Property Office, Impact Assessment*, S. 64.

²²² *BIS, dcms, Intellectual Property Office, Impact Assessment*, S. 67.

²²³ *BIS, dcms, Intellectual Property Office, Impact Assessment*, S.65, unter Berufung auf IPSOS, *Digital & Physical Piracy in GB*, November 2007, abrufbar unter: http://www.ukfilmcouncil.org.uk/media/pdf/g/m/Ipsos_Piracy_UK_2007.pdf.

²²⁴ *BIS, dcms, Intellectual Property Office, Impact Assessment*, S.65, unter Berufung auf Jupiter Research (2007).

²²⁵ *BIS, dcms, Intellectual Property Office, Impact Assessment*, S.65. Der *Digital Entertainment Survey (2008)* kommt zu dem Ergebnis, dass Filesharing von Videospielen und Software niedriger ist als in den anderen Branchen.

²²⁶ Vgl. auch unten S. 110.

²²⁷ *TERA Consultants*, S. 6.

search- und statistischen Daten, die von EU-Mitgliedstaaten, der Europäischen Kommission und der Weltorganisation für geistiges Eigentum (WIPO) ermittelt bzw. in Auftrag gegeben wurden.²²⁸ Sie nimmt die Umfrageergebnisse zu digitaler und physischer Piraterie aus den fünf analysierten Märkten und versucht anhand derer die wirtschaftlichen Auswirkungen zu berechnen. Für die Zukunftsprognose analysiert die Studie Branchenprognosen in Bezug auf die Verbreitung von Breitbandanschlüssen, sowie Prognosen zur Internet-Traffic-Entwicklung. Allerdings werden Zweifel an der korrekten Erhebung der konkreten Zahlen geäußert²²⁹, weil die Berechnungen äußerst schwierig seien und jedenfalls teilweise auf Schätzungen oder Vermutungen beruhen und nicht alle zahlenmäßige Angaben explizit verifizierbar seien.

„Online-Piraterie“ wächst danach rasant und ist die Ursache für wirtschaftliche Verluste der Kreativwirtschaft.²³⁰ Den Wertschöpfungsbeitrag der Kreativwirtschaft bemisst die Studie für das Jahr 2008 mit 6,9 Prozent des Gesamt-Bruttoinlandproduktes in der EU, was einem Betrag von 860 Mrd. Euro entspricht.²³¹ Im Jahr 2008 sollen den Branchen Film, TV, Musik und Software in der EU durch digitale und physische Piraterie insgesamt Umsatzeinbußen in Höhe von 10 Mrd. Euro entstanden und dort über 185.000 Arbeitsplätze verloren gegangen sein.²³² Soweit es nicht zu einer effektiven Bekämpfung von Piraterie kommt, prognostiziert die Studie für die Kreativwirtschaft bis zum Jahr 2015 Umsatzverluste in Höhe von 240 Mrd. Euro und den Verlust von 1,2 Mio. Arbeitsplätzen.²³³

Zur Einschätzung der Auswirkungen von Piraterie auf die Kreativwirtschaft analysiert die Studie die Ergebnisse aus den fünf größten regionalen Märkten Europas²³⁴, d.h. aus dem Vereinigten Königreich, Frankreich, Deutschland, Italien und Spanien²³⁵ Für die Prognose der Piraterieentwicklung bis 2015 werden zwei verschiedene Szenarien beschrieben. Beiden liegt zugrunde, dass keine nennenswerten Versuche zur Eindämmung der Piraterie in Europa unternommen werden.²³⁶ Im ersten Szenario wird davon ausgegangen, dass Onlinenpiraterie parallel zum Ausmaß des Filesharing-Datenverkehrs weiter zunehmen wird.²³⁷ Anhand des bisherigen Verkehrs und der bisherigen Steigerungsraten wird ohne weitere Begründung damit gerechnet, dass der Filesharing-Traffic von 2008 bis 2015 in Europa jährlich um mehr als 18 Prozent zunehmen wird.²³⁸ Das zweite Szenario geht davon aus, dass die digitale Piraterie parallel zum globalen IP-Traffic-Trend der Konsumenten in Euro-

²²⁸ TERA Consultants, S. 6f.

²²⁹ Siehe hierzu ausführlich: Hargreaves, Supporting Document CC, S. 6 ff.

²³⁰ TERA Consultants, S. 5.

²³¹ TERA Consultants, S. 6.

²³² TERA Consultants, S. 6.

²³³ TERA Consultants, S. 6.

²³⁴ TERA Consultants, S. 9 f.: Auf die fünf größten EU-Märkte sollen ca. 75 Prozent des europäischen Bruttoinlandsproduktes entfallen.

²³⁵ TERA Consultants, S.7, bei Märkten in denen digitale Mediennutzung weniger entwickelt ist, spiegeln die ausgewerteten Daten ebenfalls die verbleibende physische Piraterie wieder.

²³⁶ TERA Consultants, S. 11.

²³⁷ TERA Consultants, S. 11.

²³⁸ TERA Consultants, S. 11, unter Berufung auf Cisco.

pa verlaufen wird.²³⁹ Dabei werden im Unterschied zu Szenario Eins, neben dem Filesharing, auch Verletzungshandlungen über Streaming berücksichtigt. Entsprechend der Analyse durch TERA Consultants kommen sie zu dem Ergebnis, dass der IP-Traffic von 2008 bis 2015 um mehr als 24 Prozent zunehmen wird.²⁴⁰ Laut der Studie ging der Umsatz des Einzelhandelsmarkts für Musik zwischen 2004 und 2008 um 26 Prozent zurück, obwohl Umsätze mit digitaler Musik deutlich zunahmen.²⁴¹ In der Kino-Branche gingen die Eintrittszahlen in europäischen Kinos zwischen 2004 und 2008 um 5 Prozent und die Umsätze aus dem Verkauf von DVDs und dem Video-Verleih um 14 Prozent zurück.²⁴² Für Deutschland kommen TERA Consultants zu dem Ergebnis, dass innerhalb des oben genannten Zeitraums die Einzelhandelsausgaben für audiovisuelle Produkte um zehn Prozent zurückgingen.²⁴³ Insgesamt soll die Kreativwirtschaft in Deutschland aufgrund von Piraterie 2008 annähernd 740 Mio. Euro Verlust gemacht haben.²⁴⁴

Die Studie ist begrüßenswert transparent im Hinblick auf ihr methodisches Vorgehen. Dies fördert ihre Nachvollziehbarkeit, führte aber zugleich zu Kritik an den ermittelten Zahlen, deren methodisch belastbare Erhebung hinterfragt wurde. Dies gilt insbesondere für die Bestimmung der gewählten Substitutionsrate²⁴⁵ und die Anzahl der zugrundegelegten²⁴⁶ Urheberrechtsverstöße.²⁴⁷

Ungeachtet der Frage einer bis ins letzten Detail konsistenten Erhebung, lassen sich aus der Studie aber belastbare Tendenzen ableiten. Danach wird man annehmen können, dass, sollte es nicht zu einer spürbaren Eindämmung des Piraterieverhaltens kommen, sich die Umsatzeinbußen der betroffenen Branchen fortsetzen und verschärfen werden. Mit den Umsatzeinbußen der Kreativwirtschaft geht dann ein Verlust von Arbeitsplätzen einher.

Als Fazit lässt sich also festhalten, dass die Ergebnisse und Bewertungen bisher vorliegender Gutachten und Schätzungen bei der Ermittlung des Ausmaßes der wirtschaftlichen Auswirkungen der illegalen Nutzung von geschützten Inhalten im Internet auseinandergehen.²⁴⁸ Urheber und Verwertungswirtschaft hegen indes keinen Zweifel daran, dass Piraterie erhebliche Schäden für die ökonomische Basis für kulturelles Schaffen verursacht.

²³⁹ TERA Consultants, S. 11, d.h. parallel zur Entwicklung der Kommunikation über das Internetprotokoll.

²⁴⁰ TERA Consultants, S. 12, unter Berufung auf Cisco.

²⁴¹ TERA Consultants, S. 31, unter Berufung auf PwC.

²⁴² TERA Consultants, S. 32, unter Berufung auf PwC.

²⁴³ TERA Consultants, S. 36 unter Berufung auf PwC.

²⁴⁴ TERA Consultants, S. 36, davon 121 Mio. im Bereich Musik, 251 Mio. im Bereich Film und 74 Mio. im Bereich TV-Serien.

²⁴⁵ Hargreaves, Supporting Document CC, S. 7; allerdings wird anerkannt, dass manche Studien zu dem Ergebnis gelangen, die Substitutionsrate sei gleich Null. Diese werden aber nicht berücksichtigt, mit der Begründung, dass sie in der Minderheit seien.

²⁴⁶ Die von TERA zugrunde gelegte Zahl von 373 Mio. Urheberrechtsverstößen im Jahr 2008 stimmt etwa nicht mit der der Brennerstudie 2009 für 2008 überein, die 316 Mio. Downloads aus unlicenzierten Quellen in Deutschland zugrunde legt. Brennerstudie 2009, S. 25.

²⁴⁷ Zu weiteren Punkten Hargreaves, Supporting Document CC, S. 10.

²⁴⁸ Siehe Hargreaves, S. 70ff.

Dies wird überwiegend nicht bestritten. Allerdings existieren Erhebungen, die die Schädlichkeit von Onlinepiraterie für die Volkswirtschaft relativieren.²⁴⁹

cc) Onlinepiraterie als Hemmnis bei der Schaffung kreativer Werke

Eine weitere Frage ist, ob illegale Nutzung von Inhalten im Internet Urheber an der Schaffung kreativer Werke hindert.

Das Bedürfnis sich kreativ zu betätigen ist ein inneres Bedürfnis und weitestgehend unabhängig von wirtschaftlichen Anreizen. So ist trotz sinkender Umsatzzahlen bei den Musikverkäufen die Anzahl der Neuerscheinungen von Musikwerken und neuer Künstler in den letzten Jahren stetig gestiegen.²⁵⁰ Um aber mit ihren Produkten auch wirtschaftlich hinreichend erfolgreich zu sein, bedürfen die Künstler in aller Regel professioneller Partner,²⁵¹ auch wenn es ausnahmsweise Fälle geben mag, in denen ein Künstler in Blogs oder auf freien Internetplattformen mit wirtschaftlicher Relevanz auf sich aufmerksam gemacht hat.

Es bestehen aber Anzeichen dafür, dass die Bereitschaft der Kreativbranche, in professionelles kreatives Schaffen zu investieren, abgenommen hat.²⁵² Der Verband unabhängiger Musikunternehmen e.V. (VUT) beobachtet, dass durch rückläufige Vergütungen aus der Nutzung von Musikaufnahmen, die Bereitschaft, Wissen, Geld und Zeit in Musikerkarrieren zu investieren, in Deutschland substantiell gesunken sei.²⁵³ Das wirtschaftliche Risiko sei beim Aufbau neuer Künstler am höchsten. Daher sei es vor allem für junge, bisher unbekannte Musiker zunehmend schwieriger geworden, Partner zu finden, die in die Produktion, Weiterentwicklung, Vermarktung und Distribution von Aufnahmen ihrer Werke investieren. Insofern habe das Internet nicht die Motivation für die Produktion kreativer Güter verändert, die massenhafte unvergütete Nutzung von Musikaufnahmen im Internet zerstöre aber zunehmend die ökonomische Grundlage für Investitionen in Musikaufnahmen, insbesondere für komplexere Werke und junge Künstler.²⁵⁴

Im Vereinigten Königreich stellt die *British Recorded Industry* (BPI) eine vergleichbare Entwicklung fest. Die britische Tonträgerindustrie investiere um die 370 Mio. Pfund in Künstlerakquise²⁵⁵ und Marketing pro Jahr und damit ca. 10 Prozent des weltweiten Gesamtvolumens. Die Bereitschaft der Plattenfirmen in den Aufbau der Karrieren neuer Künstler zu investieren, nehme durch sinkende Verkaufszahlen ab. So hat in den 5 Jahren, für die Zahlen vorliegen, die Anzahl neuer Künstler im Vereinigten Königreich im Jahr 2010, mit nur 17 Einzelkünstlern oder Musikgruppen, welche die Grenze von jeweils 100.000 verkauften

²⁴⁹ Siehe hierzu unter S. 60., siehe auch *Huygen: Ups and Downs: Economic and Cultural Effects of Filesharing on Music, Film, and Games*, 2009.

²⁵⁰ *Waldfoegel*, S.1

²⁵¹ Also ein Verlag, ein Musiklabel, eine Filmgesellschaft, etc.

²⁵² *Hargreaves*, S. 75.

²⁵³ *VUT*, S. 3.

²⁵⁴ *VUT*, S. 3.

²⁵⁵ „Artist und Repertoire“ ist die Abteilung von Musikunternehmen, die für die Akquise von Künstlern zuständig ist. Die branchenübliche Abkürzung lautet A&R.

Platten erstmalig erreicht haben, ihren Tiefpunkt erreicht. In den beiden Vorjahren lag die Anzahl bei jeweils 26 Künstlern. Das BPI sammelte Daten zu Investitionen in Künstlerakquise und fand heraus, dass die Ausgaben in den letzten drei Jahren stetig gefallen sind; von 250 Mio. Pfund in 2006 auf 201 Mio. Pfund in 2009. Das ist ein Rückgang von 20 Prozent innerhalb von vier Jahren.²⁵⁶

Historisch ist Spanien einer der stärksten Exportmärkte für Filme. Der spanische Markt gilt mit 45 Prozent an Nutzern von unlizenziierten Diensten aber auch als europaweit am stärksten von Piraterie betroffen. Der Durchschnitt, gebildet aus den Werten von Deutschland, Frankreich, Italien, Großbritannien und Spanien, liegt hier bei 23 Prozent.²⁵⁷ Während in der Vergangenheit Minimum-Finanzgarantien vom Vertrieb in Höhe von zehn Prozent des Film-Budgets an Künstler gezahlt wurden, ist die Höhe der Vorab-Vertriebszusagen auf in der Regel 3 bis 5 Prozent gesunken, was als Folge von Piraterieverhalten gewertet wird.²⁵⁸ Auch die Verkaufszahlen der spanischen Musikindustrie sollen zwischen 2005 und 2010 um 55 Prozent gesunken sein und das Land hat in jüngerer Vergangenheit keine international renommierten Künstler mehr hervorgebracht.²⁵⁹

Als Fazit lässt sich festhalten, dass infolge von tatsächlichen oder befürchteten Umsatzrückgängen, die auf die massenhafte unlicenzierte Zugänglichmachung von geschützten Werken zurückzuführen sind, eine Verunsicherung bei den betroffenen Branchen ausgelöst wurde, die dazu führt, dass die Bereitschaft zu Investitionen in neue Werke und Künstler gesunken ist.

dd) Urheberrechtsverletzungen und neue Geschäftsmodelle in der digitalen Welt

Für das Internet taugliche Geschäftsmodelle sind eine wichtige Zukunftschance für die Kreativbranche. Im Musikbereich waren im Jahr 2010 legale Downloads die Haupteinnahmequelle im Onlinegeschäft. Digitaler Vertrieb machte 2010 weltweit 29 Prozent der Einnahmen von Plattenfirmen aus; verglichen mit 25 Prozent im Jahr 2009.²⁶⁰ In Europa haben die Einnahmen der Musikbranche über Onlineplattformen 2010 ein Wachstum von beinahe 20 Prozent erreicht²⁶¹, welche aus Onlineshops und Abonnement-Modellen stammen.²⁶² In Europa sind auch physische Tonträger noch bedeutend. Über digitale Vertriebswege wurden im Jahr 2010 weniger als 20 Prozent der Einnahmen der Plattenfirmen erlöst.²⁶³ In den USA hingegen stammten 2010 beinahe die Hälfte aller Einnahmen aus dem Online-

²⁵⁶ Hargreaves, S. 75, unter Berufung auf BPI.

²⁵⁷ Ipsos, <http://knowledgecenter.ipsos.de/docdetail.aspx?c=1043&sid=67F6B1C4-CC4A-4636-A948-1860CB7A00B1&did=2df20c44-f4c4-4e37-a746-e785070a02da>, zuletzt aufgerufen am 7.12.2011.

²⁵⁸ Hargreaves, S.76, unter Berufung auf Independent Film & Television Alliance.

²⁵⁹ IFPI, DMR 2011, S. 14.

²⁶⁰ IFPI, DMR 2011, S. 12.

²⁶¹ IFPI, DMR 2011, S. 12.

²⁶² Spotify entwickelte sich zur zweitgrößten Quelle für Einnahmen aus digitaler Musik für Labels in Europa; in Deutschland ist das Angebot aber zurzeit noch nicht verfügbar, IFPI, DMR 2011, S. 12.

²⁶³ IFPI, DMR 2011, S. 12.

Vertrieb von Musikdateien.²⁶⁴ Seit seinem Markteintritt im Jahr 2004 hat iTunes über zehn Milliarden Downloads verkauft.²⁶⁵ Mit erhöhter Übertragungsbandbreite erfahren (legale) Abonnementmodelle²⁶⁶ weltweit eine immer stärkere Nutzung. Auch auf mobilen Endgeräten sind Musik-Abonnements mittlerweile gebräuchlich.²⁶⁷

Digitale Geschäftsmodelle sind die ökonomische Zukunft der Content-Industrie. Sie entwickeln sich rasant und gewinnen zunehmend an Bedeutung. Eine wirtschaftlich bedeutsame Frage ist, ob Onlinepiraterie Auswirkungen auf den Anreiz zur Schaffung digitaler Geschäftsmodelle haben kann. Für die Musikindustrie stellt die illegale Nutzung den ausschlaggebenden Faktor für eine Erschwerung der weiteren Entwicklung legaler Geschäftsmodelle dar.²⁶⁸ Für Musikunternehmen und legale Musikanbieter ist die stärkste Auswirkung durch Piraterie die schwindende Bereitschaft der Konsumenten für Musik Geld auszugeben.²⁶⁹ Hauptgrund für die Nutzung von Piraterie-Angeboten sei die Kostenfreiheit der Angebote.²⁷⁰ Gute Auswahl, überzeugende Qualität und Service seien nur nachrangige Faktoren.²⁷¹ In Schweden gelangte man zu dem Ergebnis, dass illegale Musik ein starkes Substitut für legale Musik ist. Musikverkäufe in Schweden sollen um 72 Prozent höher sein, wenn es keine illegalen Angebote gäbe. Für den Bereich digitaler Musikverkäufe gehen *Adermon & Liang* sogar von einer Erhöhung um 131 Prozent aus.²⁷²

Eine auf massenhafte legale Nutzung ausgerichtete Lizenzierungsstrategie für legale Online-Musikdienste war nicht geeignet, den stetigen Umsatzrückgang im legalen Musikmarkt im Ganzen zu verhindern.²⁷³ Nach Angaben der IFPI soll der Markt für Onlinemusikhandel von 2004 bis 2010 um 1.000 Prozent gestiegen sein, während die Gesamteinnahmen der Musikindustrie im gleichen Zeitraum um 31 Prozent gesunken seien.²⁷⁴

Es liegt auf der Hand, dass legale Anbieter, deren Wirtschaftsmodell zwangsläufig auf eine Erwirtschaftung von Gewinnen angelegt ist, nicht mit unlizenziierten Angeboten konkurrieren²⁷⁵ können, deren Produktions- und Beschaffungskosten gegen Null gehen. Die fehlenden realistischen Möglichkeiten zur Errichtung einer breiten Palette legaler digitaler Geschäftsmodelle zur Bekämpfung des Rückgangs der physischen Umsätze bildet, aus Sicht der Rechteinhaber, den eigentlichen Kern des Problems, da freier illegaler Inhalt für neue

²⁶⁴ IFPI, DMR 2011, S. 12.

²⁶⁵ IFPI, DMR 2011, S. 6.

²⁶⁶ Wie z.B. Napster, Rhapsody.

²⁶⁷ IFPI, DMR 2011, S. 7.

²⁶⁸ IFPI, DMR 2011, S. 7.

²⁶⁹ IFPI, DMR 2011, S. 14.

²⁷⁰ IFPI, DMR 2011, S. 14, unter Berufung auf GfK (Schweden), CCI Digital Futures (Australien), Harris Interactive (UK) und Nielsen (China).

²⁷¹ IFPI, DMR 2011, S. 14, unter Berufung auf GfK (Schweden), CCI Digital Futures (Australien), Harris Interactive (UK) und Nielsen (China).

²⁷² Siehe hierzu auch schon oben, *Adermon/Liang*, S. 16.

²⁷³ IFPI, DMR 2011, S. 14.

²⁷⁴ IFPI, DMR 2011, S. 14.

²⁷⁵ IFPI, DMR 2011, S. 14.

digitale Musikdienste zu Wettbewerbsverzerrungen führt.²⁷⁶ Das Heranführen der Nutzer an die frühzeitige Verfügbarkeit von kreativen Inhalten, die im Internet teilweise vor dem offiziellen Erscheinen liegt, hat dazu geführt, dass die durch den hohen Kapitaleinsatz bedingten Geschäftsmodelle umgangen werden. Gleichzeitig ist es unerlässlich, neue Geschäftsmodelle zu entwickeln, die sich an neuen technischen Gegebenheiten und Nutzerinteressen orientieren.²⁷⁷ Aufgrund der illegalen Konkurrenz, die ohne wesentliche Investitionskosten auskommt, können die Chancen, die durch Onlinemöglichkeiten entstanden sind, nicht voll ausgeschöpft werden.²⁷⁸

Digitale Geschäftsmodelle zum Vertrieb kreativer Inhalte entwickeln sich und fangen zum Teil Umsatzrückgänge aus dem Verkauf physischer Produkte auf. Es ist aber plausibel anzunehmen, dass die illegale Konkurrenz die optimale Ausschöpfung des Potentials dieses neuen Marktes hemmt. Im Ergebnis ist es daher gut möglich, dass Onlinepiraterie die Entwicklung neuer Geschäftsmodelle insofern bremst, als sich diese, vor dem Hintergrund umfangreicher illegaler Nutzung, letztlich schwieriger etablieren lassen. Mit einer steigenden Kontrolle über die Onlinepiraterie könnten die rechtlichen Rahmenbedingungen für alternative Geschäftsmodelle stabiler werden.

VI. Entwicklungstendenzen für die künftige Entwicklung von Onlinepiraterie

Der technologische Fortschritt wird nicht nur wie dargestellt²⁷⁹ als Ursache für Internetpiraterie ausgemacht. Zugleich wird erwartet, dass technische Neuerungen, den Kontrollverlust über Inhalte erhöhen werden und der Vervielfältigung geschützter Inhalte weitere Dynamik verleihen können²⁸⁰. Im einzelnen wird dies für möglich gehalten durch

- die Ausweitung des Zugangs zu Breitbandanschlüssen und den Umstieg auf mobile Endgeräte;
- die Verbesserung von Rechtsverletzungen ermöglichenden Technologien und
- die zunehmende Digitalisierung kreativer Erzeugnisse.

1. Ausweitung des Zugangs zu Breitbandanschlüssen und Wandel zu mobilen Technologien

Breitbandanschlüsse bieten eine im Vergleich zu den geringen Bandbreiten, die noch vor wenigen Jahren vorherrschten, verbesserte Zugangsqualität bei niedrigeren Tarifen und damit einen schnelleren und kostengünstigeren Zugang zu Inhalten. Es wird erwartet, dass

²⁷⁶ TERA Consultants, S. 31.

²⁷⁷ Produzentenallianz, S. 4.

²⁷⁸ Teilweise werden Mittel wie Aufklärung und Rechtsverfolgung der Nutzer mit eingehender Begründung für gänzlich ineffektiv gehalten. Man sieht legale Geschäftsmodelle, die am unteren Preissegment aktiv mit den Piraterie-Angeboten konkurrieren, als einzig Erfolg versprechend an im Hinblick auf eine Überführung von Nutzern von unlicenzierter zur legalen Nutzung an. Karaganis, S. iv.

²⁷⁹ Siehe oben S. 41.

²⁸⁰ So u.a.: TERA Consultants, S. 49.

der Breitbandzugang bei den privaten Haushalten in der EU bis 2013 85 Prozent erreicht.²⁸¹ In Großbritannien sollen bis Ende 2012 alle Haushalte mit Breitbandanschlüssen versorgt sein.²⁸² Die Ausweitung des Zugangs zum Breitbandnetzwerk wird auf der einen Seite den potenziellen Markt im Internet für die Kreativwirtschaft erweitern, aber zugleich traditionelle Geschäftsmodelle in Frage stellen.²⁸³ Mit der Ausweitung der Internetzugangsbreite dürfte auch das Risiko der Ausweitung von Piraterie einhergehen.²⁸⁴ Ferner nimmt die Anzahl der WLAN-Internetzugänge (WiFi, WiMax) in öffentlichen Räumen zu²⁸⁵ und der Ausbau des mobilen Internets (LTE, LTE-Advanced) ermöglicht Nutzern mit entsprechenden mobilen Endgeräten immer und überall eine Internetverbindung herzustellen, was die Gelegenheiten illegaler Nutzung vermehrt.

2. Diversifizierung der technischen Möglichkeiten zur Rechtsverletzung

Eine von Envisional im Auftrag des US-amerikanischen Medienkonzerns NBC Universal erstellte Studie unternimmt den Versuch, die Verteilung unterschiedlicher Arten illegaler Internetaktivität zu bestimmen. Dazu wurde die Breitbandnutzung des Internets mit dem Ziel untersucht, den Anteil urheberrechtsverletzenden Datenverkehrs im Internet zu ermitteln. Die Datenerhebung fand an nur einem Tag statt, so dass kein über einen bestimmten Zeitraum ermittelter Durchschnittswert vorliegt. Zum Ausgleich wurden vier weitere Untersuchungen zur selben Problematik durchgeführt und die Ergebnisse kombiniert.²⁸⁶ Auch wenn die konkreten Zahlen nicht endgültig belastbar sind, kann der Report Indizien zum Umfang des Anteils von urheberrechtsverletzendem Internetverkehr liefern und einen Eindruck von der möglichen Verteilung innerhalb der verschiedenen Erscheinungsformen illegaler Nutzung verschaffen.

Nach den Ergebnissen von *Envisional* ist knapp ein Viertel des Internetverkehrs weltweit rechtswidrig.²⁸⁷ Die mit Abstand **meisten** unautorisierten Downloads erfolgen danach mit **16,37 Prozent** über die Nutzung von **P2P-Netzwerken**.²⁸⁸ Die Datenverschaffung über Sharehoster nimmt zu.²⁸⁹ 5,12 Prozent des gesamten Internetverkehrs sind rechtsverletzende Downloads von Sharehostern.²⁹⁰ Von den Links, welche zu auf den Servern der Sharehoster gespeicherte Inhalte verweisen, führen beinahe Dreiviertel zu rechtsverletzenden

²⁸¹ *TERA Consultants*, S. 50 unter Berufung auf Forrester.

²⁸² *Digital Britain*, S. 47 ff.

²⁸³ *Leadbeater*, S. 2.

²⁸⁴ *TERA Consultants*, S. 50.

²⁸⁵ *TERA Consultants*, S. 51.

²⁸⁶ *Envisional*, S. 2.

²⁸⁷ *Envisional*, S. 2: 23,76 Prozent, wobei Pornographie außen vor gelassen ist.

²⁸⁸ *Envisional*, S. 51 ff.: 11,39 Prozent des gesamten Internetverkehrs ist rechtsverletzende BitTorrent-Nutzung, 1,56 Prozent Gnutella-, 1,82 Prozent eDonkey- und 1,6 Prozent sonstige P2P-Nutzung. In der Summe ergibt sich daraus die Zahl von 16,37 Prozent P2P-Netzwerknutzung.

²⁸⁹ *IFPI*, DMR 2011, S. 14, unter Berufung auf *Harris Interactive*; *Envisional*, S.16, Die beliebtesten Sharehoster weltweit (4Shared und MegaUpload) sollen jeweils 78 Mio. Nutzer monatlich haben.

²⁹⁰ *Envisional*, S. 51.

Inhalten.²⁹¹ Datenverkehr in Form von Video-Streaming ist die am schnellsten wachsende Erscheinungsform von Onlinepiraterie und macht 25 Prozent des Datenverkehrs aus²⁹² Video-Streaming wird aber überwiegend legal genutzt; lediglich ca. 5,3 Prozent sind urheberrechtswidrig, was 1,4 Prozent des gesamten Internetverkehrs entspricht.²⁹³ Rechtsverletzende Usenet-Nutzung nimmt mit 0,86 Prozent den geringsten Anteil am Gesamtverkehr ein.²⁹⁴

3. Fortschreitende Digitalisierung kreativer Erzeugnisse

Onlinepiraterie ist nur an digitalen Werken möglich. Neue Endgeräte, wie elektronische Lesegeräte und Tablet-PCs, schaffen neue Bedürfnisse nach digitalen Inhalten. Insbesondere in der Buch-, Zeitungs- und Zeitschriftenverlagsbranche nehmen digitale Angebote spürbar zu. Mit der nachhaltigen Digitalisierung sämtlicher kreativer Produkte geht aber nicht nur die Möglichkeit einher, diese leichter zur Verfügung stellen zu können, sondern auch das Erfordernis nach effektivem Schutz vor unbefugter Verwendung urheberrechtlich geschützter digitaler Inhalte.

VII. Zusammenfassung

Ungeachtet ihrer unterschiedlichen Erhebungsmethoden und differierenden Ergebnisse besteht also Einigkeit über die Existenz von Urheberrechtsverletzungen im Internet als Massenphänomen.²⁹⁵ Allerdings sind die Branchen und Teilmärkte der Kultur- und Kreativwirtschaft unterschiedlich stark betroffen. Auswirkungen manifestieren sich teilweise in Umsatzrückgängen der betroffenen Branchen, jedenfalls aber in verlorenen Verkäufen, auch wenn sich diese schwer beziffern lassen. Außerdem sinkt die Bereitschaft der Branchen für Investitionen und es ist wahrscheinlich, dass die illegale Konkurrenz die Etablierung neuer digitaler Geschäftsmodelle hemmt. Als Faktoren für eine Zunahme illegaler Nutzung gelten die Ausweitung des Zugangs zu Breitbandanschlüssen und den Umstieg auf mobile Endgeräte; die Verbesserung von Rechtsverletzungen ermöglichenden Technologien und die zunehmende Digitalisierung kreativer Erzeugnisse.

²⁹¹ *Envisional*, S. 51: 73,15 Prozent dies sagt aber nichts über den Anteil rechtsverletzender Inhalte auf den Servern der Sharehoster aus, da auf rechtmäßige Inhalte typischerweise nicht verlinkt wird.

²⁹² *Envisional*, S. 3.

²⁹³ *Envisional*, S. 3.

²⁹⁴ *Envisional*, S. 53: 0,86 Prozent.

²⁹⁵ *Karaganis*, S. 7.

C. Warnhinweismodelle in anderen EU Staaten

I. Frankreich

1. Ausgangslage (Überblick)

a. Bedeutung von Kultur

Kulturgüter und kulturelles Schaffen nehmen in Frankreich traditionell einen hohen Stellenwert ein. Der explizite Schutz kultureller Güter geht in seinen Ursprüngen zurück in die Zeit der französischen Revolution Ende des 18. Jahrhunderts. Besonderem Schutz unterstellt waren zunächst Gemälde und Skulpturen. Im Mittelpunkt stand dabei nicht der Künstler, sondern der Schutz der Güter im Dienste der Allgemeinheit. Kulturelle Güter, die nicht dem Eigentum eines Einzelnen zugeordnet werden konnten, wurden bewahrt und in den ersten Museen der Öffentlichkeit zugänglich gemacht.

b. Urheberrechtliche Rahmenbedingungen und verfassungsrechtliche Grundlagen des Schutzes Geistigen Eigentums

aa. Verfassungsrechtliche Perspektive

Der Schutz des Geistigen Eigentums ist in Frankreich auf verfassungsrechtlicher Ebene dem Schutz des Rechts auf Eigentum zugeordnet.

Artikel 17 der Erklärung der Menschenrechte (*Déclaration des Droits de l'Homme et du Citoyen*) vom 26. August 1789, welche durch die Präambel der Französischen Verfassung von 1946 ergänzt wurde und noch heute Verfassungsrang hat,²⁹⁶ sieht das Recht des Einzelnen auf Eigentum vor. Wörtlich heißt es:

„La propriété étant un droit inviolable et sacré, nul ne peut en être privé, si ce n'est lorsque la nécessité publique, légalement constatée, l'exige évidemment, et sous la condition d'une juste et préalable indemnité.“

„Das Eigentum ist ein unverletzliches und geheiligtes Recht, niemandem kann es genommen werden, außer wenn dies aus zwingenden Gründen des Allgemeininter-

²⁹⁶ Vgl. Präambel der Verfassung vom 4.10.1958 (*Constitution du 4 octobre 1958*), abrufbar unter: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/constitution/constitution.pdf; deutsche Fassung: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/allemand/constitution_allemand_avril2009.pdf.

resses ausdrücklich durch Gesetz und gegen eine gerechte und vorherige Entschädigung vorgesehen ist.“

Das französische Verfassungsgericht (*Conseil Constitutionnel*) hatte im Rahmen der Überprüfung neuerer Gesetzgebung in den vergangenen Jahren mehrfach zum Schutz des Geistigen Eigentums Stellung zu nehmen. In seiner Entscheidung Nr. 2006-540 vom 27. Juli 2006²⁹⁷ betreffend das Gesetz vom 1. August 2006 „über das Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft“ verwies der *Conseil Constitutionnel* darauf, dass das Geistige Eigentum, insbesondere das Urheberrecht und die Leistungsschutzrechte, dem Recht auf Eigentum zugehören, wie es als Menschenrecht durch Artikel 2 der Erklärung der Menschenrechte von 1789 verbürgt ist.

In seiner Entscheidung Nr. 2009-580 DC vom 10. Juni 2009 betreffend das „Gesetz zur Förderung der Verbreitung und des Schutzes künstlerischen Schaffens im Internet“²⁹⁸ erinnerte der *Conseil Constitutionnel* erneut daran, dass das menschenrechtlich verbürgte Recht auf Eigentum auch das geistige Eigentum umfasse, und machte zugleich deutlich, dass das Recht, Geistiges Eigentum inne zu haben, insofern unmittelbar dem Urheber zugeordnet sei.

Wörtlich heißt es in Absatz 13 der Entscheidung:

„In Erwägung dessen, dass das Eigentumsrecht zu den Menschenrechten gehört, welche in den Artikeln 2 und 17 der Erklärung von 1789 niedergelegt sind; dass der Zweck und die Ausübung des Eigentumsrechts seit 1789 eine Entwicklung durchgemacht haben, welche sich durch eine Ausdehnung des Anwendungsbereichs dieses Rechts auf neue Sachgebiete auszeichnet; dass dazu das Recht der Inhaber von Urheberrechten oder von verwandten Schutzrechten gehört, ihr geistiges Eigentumsrecht innezuhaben und es im Rahmen des Gesetzes und der von Frankreich eingegangenen internationalen Verpflichtungen zu schützen; dass der Kampf gegen unrechtmäßige Kopien, die sich im Internet verbreiten, dem Zweck des Schutzes geistigen Eigentums dient“.²⁹⁹

bb. Gesetzliche Verankerung des Schutzes von Urheberrechten

Der Schutz des Geistigen Eigentums wurde erstmals durch Gesetz vom 11. März 1957 konkret normiert:

²⁹⁷ Entscheidung des *Conseil Constitutionnel* Nr. 2006-540 DC vom 27.7.2006, abrufbar unter: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/cc2006540dcpdf>; deutsche Fassung: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2006540DCde2006_540dcpdf.

²⁹⁸ Entscheidung des *Conseil Constitutionnel* Nr. 2009-580 vom 10.6.2009, abrufbar unter: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/cc-2009580dc.pdf>; deutsche Fassung: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009-580DC-2009580dc.pdf>.

²⁹⁹ Entscheidung des *Conseil Constitutionnel* Nr. 2009-580 DC vom 10.6.2009, a.a.O., Absatz 13.

„l'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous. Ce droit comporte des attributs d'ordre intellectuel et moral ainsi que des attributs d'ordre patrimonial.“

„Der Schöpfer eines geistigen Werkes genießt, alleine aus der Tatsache seines Schaffens heraus, ein exklusives und gegenüber jedermann einwendbares unkörperliches Eigentum an seinem Werk. Dieses Recht umfasst die geistige und moralische ebenso wie die vermögensmäßige Verwertung.“

Das Gesetz von 1957 legte die Prinzipien des Schutzes Geistigen Eigentums nieder, definierte, welche Werke geschützt sein und welche Rechte dem Rechteinhaber zustehen sollten.

Um die Bedeutung des Schutzes des Geistigen Eigentums zu unterstreichen, wurden im Jahr 1992 alle Gesetze und Verordnungen betreffend den Schutz des Geistigen Eigentums in einem einheitlichen Gesetzbuch über das Geistige Eigentum (*Code de la propriété intellectuelle*) kodifiziert.³⁰⁰ In diesem Gesetzbuch sind heute alle Regelungen betreffend den Schutz des Urheberrechts und der gewerblichen Schutzrechte geregelt, namentlich die rechtlichen Grundlagen, die Rechte und Pflichten der Rechteinhaber sowie mögliche Sanktionen bei Verstößen.

Die Grundlagen des Urheberrechts sind im ersten Teil des Gesetzbuchs über das Geistige Eigentum enthalten. Festgelegt werden der Schutzgegenstand des Urheberrechts und verwandter Rechte sowie die Rechte des Urhebers bzw. des Inhabers von Leistungsschutzrechten. Das Urheberrecht selbst ist in Artikel L.111-1 definiert und nahezu wortgleich mit der Definition von 1957.

Als Schutzgegenstand nach dem Gesetzbuch über das Geistige Eigentum gelten alle Arten geistiger Schöpfungen, „unabhängig von ihrer Art, ihrer Darstellungsform, ihrem Wert oder ihrer Bestimmung“ (Artikel L.112-1):

„... toutes les oeuvres de l'esprit, quels qu'en soient le genre, la forme d'expression, le mérite ou la destination.“

Eine nicht abschließende Liste der Schutzgegenstände ist in Artikel L.112-2 des Gesetzbuchs über das Geistige Eigentum enthalten. Hierzu gehören u.a. Schrift- und Sprachwerke, Werke der Tanzkunst und der Musik, Lichtbild- und Filmwerke sowie Werke der bildenden Kunst und Software.

Die Rechteinhaber sind, nach Art der in Betracht kommenden Werke, in den Artikeln L 123-1 bis 9 des Gesetzbuchs über das Geistige Eigentum bestimmt. Ihm stehen, insofern wie im deutschen Urheberrecht, zwei Arten von Rechten zu: das Urheberpersönlichkeitsrecht (Ar-

³⁰⁰ *Loi n°92-597 du 1er juillet 1992.*

tikel L.121-1 ff. Gesetzbuch über das Geistige Eigentum) und das Urhebervermögensrecht (Artikel L.122-1 ff. Gesetzbuch über das Geistige Eigentum).

Neben den grundsätzlich dem Urheber ausschließlich und exklusiv zustehenden Rechten an seinem Werk nennt das Gesetz Schranken des Urheberrechts. In Artikel L.122-5 des Gesetzbuchs über das Geistige Eigentum ist insbesondere das Recht auf Privatkopie verankert. Dieses gewährt dem Nutzer das Recht, eine Vervielfältigung eines Werkes auch ohne Einwilligung des Urheberrechtlichsinhabers anzufertigen. Das Gesetz sieht für diese Art der privaten Nutzung eine pauschale Vergütung des Urhebers vor.³⁰¹ Eine Privatkopie im gesetzlichen Sinne liegt vor, wenn das Werk vom Urheberrechtlichsinhaber bereits verbreitet wurde und die Kopie nur zu privaten Zwecken genutzt wird. In einem Urteil vom 30. Mai 2006 entschied der *Cour de Cassation* als Oberster Gerichtshof der ordentlichen Gerichtsbarkeit im Zusammenhang mit Peer-to-Peer-Netzwerken, dass die Ausnahme der Privatkopie nur dann greife, wenn die Quelle des Werks legal sei und die Rechte des Urheberrechtlichsinhabers nicht bereits verletze.³⁰²

In den Artikeln L.211-1 bis 217-3 Gesetzbuch über das Geistige Eigentum sind die Leistungsschutzrechte, wie zum Beispiel die Rechte der Darsteller oder der Hersteller von Videofilmen und Tonaufzeichnungen, niedergelegt.

Das Gesetzbuch über das Geistige Eigentum enthält über die eigentumsrechtlichen Fragen hinaus Normen des Sonderstrafrechts betreffend Verstöße gegen die gesetzlichen Vorgaben zum Schutz des Geistigen Eigentums. Das Sonderstrafrecht ist im Wesentlichen in den Artikel L.335-1 bis 10 Gesetzbuch über das Geistige Eigentum enthalten.

2. Stand der Gesetzgebung

Angesichts EU-rechtlicher Vorgaben wurde das Urheberrecht in Frankreich erstmals im Jahr 2006 gezielt im Hinblick auf die besonderen Anforderungen des Internetzeitalters angepasst. Es folgten weitere Novellen, mit denen systematisch der Schutz des Urheberrechts im Internet gestärkt werden sollte. Kern dieses Systems ist ein Verfahren zur Versendung von Warnhinweisen an Inhaber von solchen Internetanschlüssen, über die Urheberrechtsverletzungen begangen wurden.

³⁰¹ Artikel L.311-1 ff. *Code de la Propriété Intellectuelle*.

³⁰² *Cour de cassation*, 30.5.2006, Az. 05-83335, abrufbar unter:

<http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007640614&fastReqlid=1807781249&fastPos=1>.

a. Historischer Kontext des Warnhinweisverfahrens

aa. Novelle von 2006

Mit Gesetz vom 1. August 2006 über das Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft (*Loi relative au droit d'auteur et aux droits voisins dans la société de l'information – DADVSI*),³⁰³ waren zunächst die Anforderungen der Europäischen Urheberrechtslinie 2001/29/EG³⁰⁴ in das nationale Recht umgesetzt worden. Gesetzlich abgesichert wurden dabei technische Maßnahmen zum Schutz von Urheberrechten (Digital Rights Management- DRM) und zu deren Überwachung eine neue Behörde, die *Autorité de régulation des mesures techniques* (ARMT), geschaffen. Ihre Aufgabe sollte es sein sicherzustellen, dass die vonseiten der Produktionsbranche ergriffenen DRM-Maßnahmen nicht die Interoperabilität gefährdeten und dass die gesetzlich vorgesehenen Ausnahmen zur freien Nutzung von urheberrechtlich geschützten Inhalten (z.B. das Recht auf Privatkopie) dadurch nicht untergraben würden.

Gegenstand der Diskussion war bereits im Rahmen dieser Urheberrechtsnovelle, wie mit den zunehmenden Fällen illegaler Tauschbörsennutzung im Internet umgegangen werden sollte. Angesichts der massenhaften Urheberrechtsverletzungen über Internettauschbörsen und der nur fragmentarischen Verfolgbarkeit wurde im Rahmen des Gesetzgebungsverfahrens u.a. der Vorschlag diskutiert, derartige Werknutzungen zu legalisieren und pauschal zu vergüten. Vorschläge in dieser Richtung fanden jedoch keinen Eingang in das Gesetz. Zur Eindämmung der Urheberrechtsverletzungen wurde für das Herstellen oder die Verbreitung von Software, die das Herunterladen oder die Zurverfügungstellung von urheberrechtlich geschützten Werken erlaubt, oder Werbung für solche Software ein eigener Straftatbestand eingeführt.³⁰⁵ Demgegenüber hatte der französische Gesetzgeber das unautorisierte Vervielfältigen urheberrechtlich geschützten Materials über Peer-to-Peer-Netzwerke aus dem Strafenkatalog ausklammern und nurmehr als Ordnungswidrigkeit einstufen wollen.³⁰⁶ Mit dieser Abstufung von strafrechtlichen Sanktionen hatte sich auf Anrufung durch Abgeordnete der Regierungsoption im Folgenden der *Conseil Constitutionnel* zu befassen. Dieser sah in der gesetzlichen Begünstigung der Tauschbörsennutzung einen Verstoß gegen den Gleichheitsgrundsatz, da er keinen Unterschied darin erkannte, ob eine Raubkopie im Wege des Peer-to-Peer-Filesharings oder auf anderem Wege erstellt wurde.³⁰⁷ Die entsprechende Vorschrift wurde daher im Gesetz gestrichen.

³⁰³ *Loi n°2006-961 du 1 août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information*, abrufbar unter: <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT00000266350>. Kodifiziert im *Code de la propriété intellectuelle*.

³⁰⁴ Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft.

³⁰⁵ Artikel 21 DADVSI.

³⁰⁶ Artikel 24 DADVSI. Vgl. hierzu *Blocman*, Gesetz über das Urheberrecht und die verwandten Schutzrechte in der Informationsgesellschaft verabschiedet, IRIS 2006/7, S. 11, sowie dies., Verfassungsrat kritisiert Gesetz über Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft, IRIS 2006/8, S. 13.

³⁰⁷ Entscheidung des *Conseil Constitutionnel* Nr. 2006-540 DC vom 27.7.2006, a.a.O.

Auch das illegale Filesharing blieb damit grundsätzlich dem Straftatbestand der Raubkopie unterworfen und ist von daher mit Strafen in Höhe von bis zu 300.000 Euro und drei Jahren Haft belegt.

bb. Mission Olivennes

Die gesetzlich vorgesehenen Strafen bei Urheberrechtsverstößen wurden von der französischen Regierung nicht als befriedigende Lösung für die Behandlung der Internetaustauschbörsen erachtet. Der Sanktionierung von Urheberrechtsverletzung gegenüber stand vielmehr die Überlegung, dass echte Alternativen und Anreize für das legale Downloaden von Werken geschaffen werden müssten, um der illegalen Nutzung von Werken Einhalt gebieten zu können. Es wurde daher von der französischen Regierung im September 2007 eine vierköpfige Kommission unter der Leitung von *Denis Olivennes*, dem ehemaligen Generaldirektor der französischen Medienhandelskette Fnac,³⁰⁸ beauftragt, unter Einbeziehung aller Beteiligten Lösungsvorschläge für die Problematik der illegalen Nutzung urheberrechtlich geschützter Werke im Internet zu erarbeiten - die sog. „*Mission Olivennes*“. Der Auftrag an die Kommission Olivennes zielte vor allem darauf, die kommerziellen, ökonomischen, rechtlichen und technischen Rahmenbedingungen aufzuzeigen, unter denen legale Angebote im Internet für den Nutzer eine attraktive Alternative zu illegalen Angeboten darstellen könnten.³⁰⁹ Wörtlich heißt es zum Ziel des Auftrags:

“... conduire une mission de réflexion et de concertation destinée à favoriser la conclusion d'un accord entre professionnels, permettant le développement d'offres légales attractives d'œuvres en ligne et dissuadant le téléchargement illégal de masse.”

„... einen Auftrag der Reflexion und Verständigung auszuführen, welcher eine Vereinbarung zwischen den Beteiligten Industrien zum Ziel hat, welche attraktive legale Angebote im Internet erlaubt und massenhafte illegale Downloads vermindert.“

Im Rahmen der Durchführung der Mission erfolgten zahlreiche Anhörungen von Vertretern der Rechteinhaber, der Inhalteverwerter, der Internetprovider und der Verbraucher. Dabei zeigte sich im Ergebnis Einigkeit aller Beteiligten darüber, dass ein Warnhinweissystem, welches mögliche weitere Sanktionen bei wiederholtem Urheberrechtsverstoß vorsieht, eingeführt werden sollte. Zudem war einhellige Meinung, dass legale Angebote im Internet gefördert werden müssten. Ansätze hierzu sollten die Gewährleistung von Interoperabilität und eine Verkürzung von Verwertungsfenstern sein. Zugleich sollte mehr Enga-

³⁰⁸ Weiter Beteiligte waren *Olivier Bomsel*, *Pascal Faure* und *Isabelle Falque-Pierrotin*. Zu den Kommissionsmitgliedern: <http://www.culture.gouv.fr/culture/actualites/index-olivennes231107.html>.

³⁰⁹ Auftrag der Ministerin für Kultur und Kommunikation an *Denis Olivennes*, abrufbar unter: <http://www.culture.gouv.fr/culture/actualites/index-olivennes231107.html>.

gement in die Entwicklung technischer Maßnahmen zur Identifikation illegaler Angebote im Netz fließen.³¹⁰

Als Ergebnis der den Anhörungen folgenden Verhandlungen konnte am 23. November 2007 als Meilenstein die sog. Elysée-Vereinbarung über die Entwicklung und den Schutz kultureller Werke und Programme in den neuen Netzen (*Accord pour le développement et la protection des œuvres et programmes culturels sur les nouveaux réseaux*) abgeschlossen werden. Die Beteiligten des als „geschichtsträchtig“ bezeichneten³¹¹ Abkommens waren 42, später 45, Einrichtungen bzw. Unternehmen aus dem Bereich Film, Musik, Fernsehen und Internetdiensten.³¹² Es enthielt erstmals konkrete, im Konsens mit den Internet Providern beschlossene Maßnahmen zur Bekämpfung von Urheberrechtsverletzungen.

Die Unterzeichner verpflichteten sich darin, an einer gemeinsamen Lösung im Kampf gegen die Piraterie (*prévention du piratage*) sowie bei der Förderung des Internet als Distributionsweg für kulturelle Inhalte (*favorisation l'offre légale*) mitzuwirken. Bestandteil der Vereinbarung war insbesondere die Einführung und Umsetzung des Warn- und Sanktionssystems gegen den illegalen Download urheberrechtlich geschützter Werke unter Mitwirkung der Internetprovider. Hierzu sollten dem französischen Parlament vonseiten der öffentlichen Hand die erforderlichen gesetzgeberischen Maßnahmen vorgeschlagen werden. Darüber hinaus verpflichteten sich die Internetprovider zusammen mit den Rechteinhabern, Identifikationssysteme zur Kennzeichnung legaler bzw. illegaler Angebote (digitale Fingerprints oder Wasserzeichen) bzw. Filtersysteme zu entwickeln und zur Anwendung zu bringen. Gegenstand der Vereinbarung war u.a. auch eine Verkürzung der Verwertungsfenster für audiovisuelle Inhalte.³¹³ So sollten zukünftig etwa Filme als Video-on-Demand-Angebot zügiger legal online für den Verbraucher verfügbar gemacht werden können.³¹⁴ Die Produktionsfirmen verpflichteten sich im Sinne der Gewährleistung von Interoperabilität außerdem, Musik ohne technische Schutzmaßnahmen anzubieten, so dass legal gekaufte Titel auf allen Endgeräten abspielbar sein könnten.³¹⁵

³¹⁰ Bericht der *Olivennes*-Kommission, abrufbar unter: <http://www.culture.gouv.fr/culture/actualites/index-olivennes231107.htm>.

³¹¹ Vgl. *Projet de Loi favorisant la diffusion et la protection de la création sur internet, Exposé des motifs*, Begründung zum Entwurf eines Gesetzes über die Verbreitung und den Schutz schöpferischer Inhalte im Internet, S. 3, abrufbar unter: <http://www.culture.gouv.fr/culture/actualites/dossiers/internet-creation08/6%20-%20Projet%20de%20loi.pdf>.

³¹² Übersicht über die beteiligten Parteien abrufbar unter: <http://www.culture.gouv.fr/culture/actualites/index-olivennes231107.htm>.

³¹³ Vgl. allgemein zu den europäischen Vorgaben und nationalen Regelungen von Verwertungsfenstern *Kuhr*, Verwertungsfenster im Wandel, IRIS plus 2008/4.

³¹⁴ Eine Verwertung mittels Online-Dienst sollte auf der gleichen Ebene wie DVD-Angebot erfolgen, d.h. sechs Monate nach der Erstausstrahlung des Films im Kino.

³¹⁵ Vereinbarung im Volltext abrufbar unter: <http://www.culture.gouv.fr/culture/actualites/index-olivennes231107.html>.

cc. Novelle von 2009/2010

Die von der *Olivennes*-Kommission erarbeiteten Rahmenbedingungen, insbesondere das Warnhinweisverfahren, wurde 2008 von der französischen Regierung aufgegriffen und dem Ministerrat ein entsprechender Gesetzentwurf vorgestellt. In der Gesetzesbegründung wurde insbesondere auf die präventive Wirkung von Warnhinweisen verwiesen. Danach wurde unter Verweis auf verschiedene Studienergebnisse davon ausgegangen, dass mit einer ersten Warnung mehr als zwei Drittel aller Internetnutzer abgehalten werden könnten, weitere Verstöße gegen das Urheberrecht zu begehen. Mit einem zweiten und ggf. dritten Warnhinweis könne diese Wirkung bei 90 und mehr Prozent der Internetnutzer erzielt werden.³¹⁶

Das vorgeschlagene Warnhinweis-Modell ergänzt damit letztlich die schon mit dem DADVSI von 2006 eingeführten Regulierungsmaßnahmen durch einen repressiven, stark erzieherischen Ansatz. Der Internetnutzer soll aufgeklärt werden und Sanktionierungen von Taten aus Unkenntnis der rechtlichen Sachlage außerhalb regulärer Gerichtsverfahren erfolgen.³¹⁷

b. Status quo

Die Grundlagen des zum Schutz der Urheberrechte eingeführten mehrstufigen Warnhinweis-Systems wurden zunächst mit Gesetz vom 12. Juni 2009 zur Förderung der Verbreitung und zum Schutz von Werken im Internet (*Loi favorisant la diffusion et la protection de la création sur Internet* – Hadopi I)³¹⁸ gelegt.

Einige Bestimmungen dieses Gesetzes wurden jedoch auf Klage von 60 Abgeordneten durch das französische Verfassungsgericht (*Conseil Constitutionnel*) nachfolgend für nicht verfassungskonform erklärt.³¹⁹ Im Mittelpunkt standen dabei vor allem die der sog. „Hadopi“ (Abkürzung für *Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet*), einer nach dem Gesetz neu einzurichtenden Behörde zur Durchführung des Warnhinweis-Systems, zugestandenen weitreichenden Kompetenzen. Weiterhin umstritten waren die im Gesetz vorgesehenen Methoden zur Ermittlung des Rechtsverstoßes, da hierin eine Verletzung der Privatsphäre des Betroffenen gesehen wurde. Im Hinblick auf die Vergabe von Gütezertifikaten durch die Hadopi wurde das Fehlen konkreter gesetzlicher Vorgaben gerügt. In der Diskussion waren zudem die Möglichkeit der Sperrung des Internetzugangs und deren Zulässigkeit angesichts einer etwaigen Verletzung der Mei-

³¹⁶ Vgl. *Projet de Loi favorisant la diffusion et la protection de la création sur internet, Exposé des motifs*, a.a.O., S. 4 ; deutsche Fassung: <http://www.culture.gouv.fr/culture/actualites/communiq/albanel/creaallemand.htm> .

³¹⁷ Vgl. *Projet de Loi favorisant la diffusion et la protection de la création sur internet, Exposé des motifs*, a.a.O., S. 2.

³¹⁸ *Loi n°2009-669 du 12.06.2009 favorisant la diffusion et la protection de la création sur Internet*, abrufbar unter <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020735432&fastPos=1&fastReqId=826391324&categorieLien=cid&oldAction=rechTexte>.

³¹⁹ Entscheidung des *Conseil Constitutionnel* Nr. 2009-580 vom 10.6.2009, abrufbar unter <http://www.conseil-constitutionnel.fr/decision/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html> .

nungs- und Redefreiheit. Im Zusammenhang hiermit steht auch die im Gesetz vorgesehene Verpflichtung des Anschlussinhabers zur Fortzahlung des Entgelts für einen Internetanschluss im Fall seiner Sperrung. Die Regelung wurde als versteckte Strafe für den Anschlussinhaber kritisiert.

Der *Conseil Constitutionnel* befasste sich entsprechend in seiner Entscheidung vom 10. Juni 2009³²⁰ u.a. mit der Bedeutung des Zugangs zum Internet und ordnete diesen dem in Artikel 11 der Erklärung der Menschenrechte von 1789 verbürgten Recht auf Meinungsäußerungsfreiheit zu. Wörtlich heißt es:

„... dass aufgrund des gegenwärtigen Stands der Kommunikationsmittel und in Anbetracht der allgemeinen Verbreitung von Online-Kommunikationsmitteln, sowie der Bedeutung, die diese Dienste für die demokratische Mitwirkung und den Ausdruck von Gedanken und Meinungen besitzen, das in Artikel 11 gewährleistete Recht die Freiheit beinhaltet, Zugang zu diesen Diensten zu erhalten.“³²¹

Er beanstandete in Abwägung mit den Eigentumsrechten der Rechteinhaber die Möglichkeit der Internetsperre jedoch nicht generell. Er erklärte aber die der Hadopi als Behörde eingeräumte Befugnis, die Sperrung eines Internetzugangs selbst anzuordnen, für verfassungswidrig. Es bedürfe, insbesondere angesichts der Schwere des Eingriffs, hierfür vielmehr der Anordnung durch ein Gericht.

Die Ermittlung von IP-Adressen durch Private, d.h. Beauftragte der Rechteinhaber, beurteilte der *Conseil Constitutionnel* als verfassungskonform. Dieser Bewertung lag u.a. zugrunde, dass nach den gesetzlichen Vorgaben die IP-Adressen nur an die Rechtsschutzkommission der Hadopi bzw. an die Gerichte weitergeleitet werden dürfen.

Aufgrund der Entscheidung des *Conseil Constitutionnel* folgte ein weiteres Gesetz, mit dem die vom Verfassungsgericht formulierten Anforderungen umgesetzt wurden. Dieses Gesetz vom 28.10.2009 über den strafrechtlichen Schutz des geistigen Eigentums (*Loi relative à la protection pénale de la propriété littéraire et artistique sur Internet – Hadopi II*)³²², legt die Befugnisse der verschiedenen Akteure, die an der Durchführung des Warnhinweismodells beteiligt sind, und die Rolle der Gerichte in diesem System fest.

³²⁰ Entscheidung des *Conseil Constitutionnel* Nr. 2009-580 DC vom 10.6.2009, a.a.O.

³²¹ Entscheidung des *Conseil Constitutionnel* Nr. 2009-580 DC vom 10.6.2009, a.a.O., Absatz 12.

³²² *Loi n°2009-1311 du 28.10.2009 relative à la protection pénale de la propriété littéraire et artistique sur Internet*, abrufbar unter:

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021208046&fastPos=1&fastReqId=2023550673&categorieLien=cid&oldAction=rechTexte>.

3. Das französische Modell

a. Schwierigkeiten der Ausgangslage

Vor der Einführung des neuen Systems zum Schutz von Urheberrechten im Internet konnten Internetnutzer, nahezu ohne rechtliche Konsequenzen fürchten zu müssen, urheberrechtlich geschützte Daten im Internet herunterladen bzw. tauschen.

Dies lag zum einen daran, dass die Ermittlung des Inhabers eines Internetanschlusses mittels der IP-Adresse nur durch die Polizei und die Gendarmerie³²³ zulässig war. Einen eigenen Auskunftsanspruch kann der in seinen Rechten verletzte Urheber oder Lizenznehmer gegenüber dem Internetprovider – auch heute noch – nicht geltend machen. Die Verfolgung von Urheberrechtsverletzungen war daher von den im Rahmen strafrechtlicher Ermittlung erfolgenden Maßnahmen der Ermittlungsbehörden abhängig.

In der Rechtspraxis kam zum anderen hinzu, dass zum damaligen Zeitpunkt die Ermittlung von Urheberrechtsverletzungen nicht im Fokus der Tätigkeit von Polizei und Gendarmerie stand. Als prioritär galt insbesondere die Verfolgung von Delikten im Zusammenhang mit Pädophilie im Internet, so dass Raubkopien zumeist nur zufällig entdeckt und sichergestellt wurden.

Die Sicherstellung von urheberrechtsverletzendem Material durch die Ermittlungsbehörden und auch die aus den Strafverfahren folgenden möglichen Sanktionierungen in Form von Haft- oder Geldstrafen hinderten den Internetnutzer letztlich nicht an etwaigen weiteren Zuwiderhandlungen. Soweit den Inhaber eines Internetanschlusses die zum damaligen Zeitpunkt in Artikel L.335-12 des Gesetzbuchs über das Geistige Eigentum vorgesehene Pflicht zur Überwachung seines Internetzugangs traf, ergaben sich hieraus keine besonderen Konsequenzen. Der Anschlussinhaber hatte danach zwar dafür Sorge zu tragen, dass über seinen Zugang keine Verletzung von Urheberrechten begangen wird. Eine Missachtung dieser Pflicht war indes mit keiner eigenständigen Sanktion verknüpft.

b. Ausgestaltung des neuen Schutzsystems

Die mit der damaligen Rechtslage und Praxis verbundenen Schwächen des Schutzes von Urheberrechten sollten im Rahmen der Einführung des neuen Schutzsystems behoben und ein gerechter Interessenausgleich aller Beteiligten hergestellt werden.

³²³ Die Gendarmerie ist Teil des Militärs und untersteht dem Verteidigungsministerium. Ihre primäre Zuständigkeit liegt in der Aufrechterhaltung der öffentlichen Ordnung in ländlichen Gebieten. Im Übrigen findet sie Einsatz im militärischen Bereich. Soweit die Gendarmerie polizeiliche Funktionen ausübt, ist sie dem Innenministerium unterstellt. Die Polizei untersteht hingegen unmittelbar dem Innenministerium. Betreffend die Verfolgung von Straftaten sind die Funktionen von Polizei und Gendarmerie identisch.

aa. Regelungsziel (Schutzzweck) und wesentliche Neuerungen

Das mit den Hadopi-Gesetzen und den entsprechenden Verordnungen neu eingeführte System bezweckt, wie das vorangegangene DADVSI, den Schutz des Urheberrechts speziell im Internet. Es wurde eingeführt, um das zunehmend illegale Downloaden von urheberrechtlich geschützten Werken stärker zu reglementieren und zu sanktionieren. Während die bis dato ergriffenen Maßnahmen vor allem repressiver Art waren mit dem Ziel, erfolgte Verstöße gegen das Urheberrecht zu ahnden, hat das Warnhinweis-Modell vor allem **präventiven**, zum Teil **edukatorischen Charakter**. Das Ziel der Bekämpfung des Piraterieverhaltens im Internet soll damit, in Ergänzung zu den strafrechtlichen Möglichkeiten, über Aufklärung und zugleich über die Förderung legaler Angebote urheberrechtlich geschützter Inhalte im Internet erzielt werden.

Ausgehend von dem Grundrecht der Kulturschaffenden auf Urheberrecht und dem Grundrecht der Internetnutzer auf Beachtung ihres Persönlichkeitsrechts hat der französische Gesetzgeber bei der Errichtung des Schutzsystems zwei Perspektiven eingenommen. Zum einen steht der Internetnutzer selbst im Fokus der Regelung. Der Internetnutzer, der den kriminellen Charakter seines Handelns unter Umständen nicht erkennt, soll vor strafrechtlicher Sanktionierung bewahrt und über die Dimension seines Handelns aufgeklärt werden. Zum anderen lag dem gesetzgeberischen Handeln die kulturelle und gesamtwirtschaftliche Dimension des Phänomens zugrunde. Dabei wurden einerseits Umsatzeinbrüche der Kreativ- bzw. Verwertungsbranche insbesondere im Musikgeschäft, rückläufige Zahlen im Arbeitsmarkt und auch Tendenzen einer Verringerung des kulturellen Schaffens als Folge der Online-Piraterie zugeordnet. Andererseits wurde die Bedeutung des Internet erkannt und dieses vor allem als Chance begriffen, kulturelle Güter und Inhalte zu verbreiten. Die Internetpiraterie wurde insofern jedoch als Hauptgrund dafür angesehen, dass sich legale Geschäftsmodelle bis dato nicht etablieren konnten. Voraussetzung dieses im gesellschaftlichen Interesse liegenden Ziels sei, so das Verständnis des Gesetzgebers, dass Kreative in ihren Urheberrechten ausreichend geschützt würden.³²⁴

Wesentliche Neuerung im Rahmen des Warnhinweissystems war vor diesem Hintergrund die Errichtung einer unabhängigen staatlichen Behörde, der **Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (Hadopi)**.³²⁵ Sie trat die Nachfolge der ARMT an und wurde mit weitreichenden Befugnissen ausgestattet, um Urheberrechtsverletzungen im Internet vorzubeugen, sie zu verfolgen und zu sanktionieren. Besondere Bedeutung hat dabei vor allem die Aufklärung und Verwarnung der Internetnutzer.

³²⁴ Vgl. *Projet de Loi favorisant la diffusion et la protection de la création sur internet, Exposé des motifs*, a.a.O., S. 1 ff.

³²⁵ „*Autorité publique indépendante*“. Es handelt sich hierbei um Behörden, die Kompetenzen des Staates ausüben, aber nicht unter der Schirmherrschaft eines Ministeriums stehen. Auch die französische Datenschutzbehörde, der *Commission nationale de l'informatique et des libertés (CNIL)*, ist ebenfalls eine öffentlich unabhängige Behörde.

Darüber hinaus war einer der entscheidenden weiteren Neuerungen des eingeführten Systems, dass nicht mehr nur die Polizeibehörden für die Strafermittlung zuständig sein sollten. Es wurden vielmehr nun auch Private, d.h. vereidigte und vom Ministerium zugelassene private Bevollmächtigte der Urheberrechtsanspruchsberechtigten, mit dem Recht ausgestattet, die IP-Adressen potentieller Täter von Urheberrechtsverletzungen zu ermitteln. In der Praxis durchsuchen die Bevollmächtigten im Internet ausfindig gemachte Peer-to-Peer-Netzwerke auf urheberrechtlich geschütztes Material und ermitteln dabei die IP-Adressen der möglichen Rechteverletzer.³²⁶

Die Notwendigkeit einer gesetzlichen Ermächtigung der Rechteinhaber für die Erhebung und Speicherung von IP-Adressen ist dem - nicht gänzlich geklärten - Status der IP-Adresse im französischen Recht geschuldet. So galt sie grundsätzlich als personenbezogenes und daher datenschutzrechtlich relevantes Datum. In einigen neueren Urteilen, u.a. des Pariser Berufungsgerichts (*Cour d'Appel de Paris*), wurde dies jedoch anders beurteilt und die bisherige Einstufung damit in Frage gestellt.³²⁷ Bis 2004 durften ausschließlich Gerichte und die an der Rechtspflege Beteiligten personenbezogene Daten betreffend Rechtsverletzungen, Verurteilungen und Sicherungsmaßnahmen nutzen. Durch Gesetz Nr. 2004-801 vom 6. August 2004 über den Schutz personenbezogener Daten³²⁸ wurde Artikel 9 des Gesetzes Nr. 78-17 vom 6. Januar 1978 über Computer, Dateien und Freiheiten (*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*) dahingehend geändert, dass nunmehr auch Vertreter der Urheberrechtsinhaber derartige personenbezogene Daten nutzen dürfen. Dieses Recht wurde durch den *Conseil Constitutionnel* mit zwei Schranken versehen:³²⁹ Das Verfahren zur Ermittlung der IP-Adresse bedürfe der Zustimmung der für den Datenschutz zuständigen *Commission Nationale de l'Informatique et des Libertés*³³⁰ (Nationale Kommission für Informatik und Freiheiten, CNIL) und die Zusammenführung von IP-Adresse und Name des Anschlussinhabers dürfe nur auf der Basis einer richterlichen Entscheidung erfolgen.

Im Jahr 2005 verweigerte die CNIL den vier Verwertungsgesellschaften SACEM, SDRM, SCCP und SPPF die erforderliche Zustimmung zur Ermittlung von IP-Adressen. Die Verwer-

³²⁶ Die Beauftragten geben sich dabei selbst als Peer-to-Peer-Nutzer aus. Die Ermittlung stößt insofern dort an Grenzen, wo Netzwerke auf bestimmte Nutzerkreise begrenzt sind oder nur Personen zulassen, die jeweils wiederum persönlich von Mitgliedern eingeladen wurden.

³²⁷ Z.B. *Cour d'Appel de Paris* (Berufungsgericht), Urteile vom 27. April und 15. Mai 2007. Indem die Qualität der IP-Adresse als personenbezogenes Datum verneint wurde, wurden die Rechteinhaber ermächtigt, diese ohne Ermächtigung der CNIL zu erheben und zu sammeln.

³²⁸ *Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, abrufbar unter:

http://www.legifrance.gouv.fr/affichTexte.do?sessionId=76D88609F1B1AA2CAD91191619871AEB.tpdjo13v_2?cidTexte=LEGITEXT000005821923&dateTexte=20111122.

³²⁹ Entscheidung des *Conseil Constitutionnel* Nr. 2004-499 vom 29. Juli 2004, abrufbar unter:

<http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/cc2004499dcpdf>.

³³⁰ Stellungnahme, abrufbar unter: http://electronlibre.info/IMG/pdf/AVIS_CNIL-HADOPI.pdf.

tungsgesellschaften riefen daraufhin den *Conseil d'Etat* an, der am 23. Mai 2007³³¹ die Entscheidungen der CNIL aufhob. Er nahm keine abschließende Bewertung der Qualität von IP-Adressen als personenbezogenes Datum vor, entschied aber in der Sache, dass Urheberrechtsinhaber berechtigt seien, die IP-Adressen von Rechteverletzern zu ermitteln. Die Entscheidung über die Zuordnung der Namen der Anschlussinhaber zur IP-Adresse sollte hingegen weiterhin Aufgabe des Gerichts bleiben.³³²

Angesichts der Entscheidungen wird in Frankreich weiterhin diskutiert, ob IP-Adressen als personenbezogene Daten anzusehen sind; durch die von der CNIL den Rechteinhabern erteilten Ermächtigungen ist der Streit in der Praxis jedoch nicht von Relevanz.

Weitere bedeutende Neuerung des eingeführten Systems ist, dass als besondere Sanktion im Gesetz die Möglichkeit vorgesehen wurde, Internetzugänge zu sperren, wenn von diesen aus wiederholt Urheberrechtsverletzungen begangen wurden. Damit sollte den Betroffenen die Möglichkeit genommen werden, weiterhin Musik, Film oder Software usw. über die eigene Internetanbindungen illegal via Internet zu verbreiten bzw. herunterzuladen.

bb. Systematische Verortung der Warnhinweis-Regelung

Rechtstechnisch wurden mit den beiden Gesetzen aus den Jahren 2009 und 2010, dem sog. Hadopi I und Hadopi II, Änderungen und Ergänzungen des Dritten Buchs des rechtsetzenden Teils³³³ des französischen Gesetzbuchs über das Geistige Eigentum³³⁴ vorgenommen.

Für die Umsetzung der neuen Gesetzesvorgaben wurden darüber hinaus zehn Verordnungen (*décret*)³³⁵ erlassen:

- Verordnung 2009-1773 vom 29.12.2009 betreffend die Organisation der Hohen Behörde für die Verbreitung der Werke und den Schutz der Rechte im Internet³³⁶ („*Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet*“ - Hadopi).

³³¹ Entscheidung des *Conseil d'État* Nr. 288149 vom 23. Mai 2007, abrufbar unter: <http://arianeinternet.conseil-etat.fr/arianeinternet/ViewRoot.asp?View=Html&DMode=Html&PushDirectUrl=1&Item=3&fond=DCE&textes=cnil+23+mai+2007&Page=1&querytype=simple&NbEltPerPages=4&Pluriels=True>.

³³² Die CNIL hat in der Folge den Rechteinhabern die erforderlichen Ermächtigungen durch Beschluss erteilt: *Décision n° 2007-298 du 11.10.2007; n° 2007-334 du 8.11.2007; n! 2007-348 du 22.11.2007; n° 2008-006 du 8.1.2008.*

³³³ Das Gesetzbuch unterteilt sich in einen rechtsetzenden Teil (*Partie législative*) und einen Anordnungsteil (*Partie réglementaire*). Beide unterscheiden sich durch Ursprung und Qualität der jeweils in ihm enthaltenen Regelungen. Ein Artikel, der durch Gesetz erlassen wurde, wird in den rechtsetzenden Teil eingeführt. Artikel einer Verordnung oder eines Erlasses werden in den Anordnungsteil aufgenommen.

³³⁴ Artikel L.331-1 à L.343-7 *Code de la propriété intellectuelle*.

³³⁵ Drei weitere Verordnungen betrafen Fragen der Nominierung von Mitgliedern der Hadopi.

³³⁶ *Décret n°2009-1773 du 29.12.2009 relatif à l'organisation de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet*, abrufbar unter: <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021573619&fastPos=1&fastReqId=731503649&categorieLien=cid&oldAction=rechTexte>.

Die Verordnung regelt die Zusammensetzung der Hohen Behörde und ihren Betrieb.

- Verordnung 2010-236 vom 5. März 2010 betreffend die automatisierte Verarbeitung personenbezogener Daten.³³⁷ Die Verordnung enthält Regelungen dazu, welche Daten wie lange von wem gespeichert und eingesehen werden dürfen. Die Verordnung erhielt späterhin Ergänzungen und Änderungen durch die Verordnung 2010-1057 vom 3. September 2010 und Verordnung 2011-264 vom 11. März 2011.
- Verordnung 2010-695 vom 25. Juni 2010 betreffend die Einführung eines Fahrlässigkeitstatbestands zum Schutz geistigen Eigentums.³³⁸
Durch die Verordnung wurde ein neuer Fahrlässigkeitstatbestand eingeführt, mit dem die fehlende Sicherung eines Internetanschlusses sanktioniert wird.
- Verordnung 2010-872 vom 26. Juli 2010 betreffend das Verfahren vor der Rechtsschutzkommission (*Commission de protection des droits*) der Hadopi.³³⁹
Im Rahmen der Verordnung werden alle Schritte des Verfahrens betreffend den Rechteinhaber, den Internetnutzer und die Staatsanwaltschaft konkretisiert.
- Verordnung 2010-1202 vom 12. Oktober 2010 betreffend die Pflichten der Internet-Diensteanbieter.³⁴⁰
Diese sog. „Free-Verordnung“ betrifft die Verpflichtung der Internetzugangsdiensteanbieter zur Kooperation mit der Hadopi.
- Verordnung 2010-1366 vom 10. November 2010 betreffend die Sicherheitszertifizierung der Online-Dienstleistungen und die Regulierung der technischen Schutzmaßnahmen sowie der Identifizierung der urheberrechtlichen geschützten Werke und Gegenstände.³⁴¹

³³⁷ Décret n°2010-236 du 5.3.2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L.331-29 du code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur Internet, abrufbar unter:

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021923996&fastPos=1&fastReqId=1732810531&categorieLien=cid&oldAction=rechTexte>.

³³⁸ Décret n°2010-695 du 25.6.2010 instituant une contravention de négligence caractérisée protégeant la propriété littéraire et artistique sur Internet, abrufbar unter:

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022392027&fastPos=1&fastReqId=973713529&categorieLien=cid&oldAction=rechTexte>.

³³⁹ Décret n°2010-872 du 26.7.2010 relatif à la procédure devant la commission de protection des droits de la Haute Autorité pour la diffusion des œuvres et à la protection sur Internet, abrufbar unter:

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022518612&fastPos=1&fastReqId=537061043&categorieLien=cid&oldAction=rechTexte>.

³⁴⁰ Décret n°2010-1202 du 12.10.2010 modifiant l'article R.331-37 du code de la propriété intellectuelle, abrufbar unter:

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022913572&fastPos=1&fastReqId=161056296&categorieLien=cid&oldAction=rechTexte>.

³⁴¹ Décret n° 2010-1366 du 10.11.2010 relatif à la labellisation des offres des services de communication au public en ligne et à la régulation des mesures techniques de protection et d'identification des œuvres et des objets protégés par le droit d'auteur, abrufbar unter:

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023037200&fastPos=1&fastReqId=553343945&categorieLien=cid&oldAction=rechTexte>.

- Verordnung 2010-1630 vom 23. Dezember 2010 betreffend die Bewertung und Zertifizierung der Schutzmaßnahmen.³⁴²
Die Verordnung bestimmt die Voraussetzungen, unter denen Softwareverlage ihre Software von der Hadopi zertifizieren lassen können.
- Verordnung 2011-386 vom 11. April 2011 betreffend die Indikatoren der Hadopi. Durch sie werden Kriterien für die Bewertung der Entwicklungen legaler Angebote und die Nutzung urheberrechtlich geschützter Inhalte Internet festgelegt.

Mit Ausnahme der Verordnung vom 5. März 2011 betreffend die automatisierte Verarbeitung personenbezogener Daten sind diese Verordnungen im Anordnungsteil des Dritten Buch des Gesetzbuchs über das Geistige Eigentum kodifiziert³⁴³.

Die wesentlichen Vorgaben zur Implementierung des Warnhinweis-Systems sind in den Artikeln L.331-21, L.331-21-1, L.331-24 bis -30, R.331-35 bis -46 des Gesetzbuchs über das Geistige Eigentum und in der Verordnung vom 5.3.2011 zur automatisierten Verarbeitung personenbezogener Daten verankert.³⁴⁴

cc. Anwendungsbereich der Hadopi-Gesetze

Das neue System bezieht in den Schutz alle urheberrechtlich relevanten Schöpfungen und Leistungen ein, die über das Internet verbreitet werden können. Im Blickfeld der Hadopi-Gesetze sind Sachverhalte, in denen urheberrechtlich geschütztes Material unter Verstoß gegen die Rechte des Urhebers und der Leistungsschutzrechteinhaber im Internet vervielfältigt, veröffentlicht, zur Verfügung gestellt oder verbreitet, insbesondere also heruntergeladen oder zum Download zur Verfügung gestellt werden.³⁴⁵ Erfasst ist damit jegliche Form der Rechtsverletzung.

Faktischer Ansatzpunkt für die Versendung von Warnhinweisen und die mögliche spätere Sanktionierung von Verstößen gegen das Urheberrecht ist die Ermittlung der vom Rechtsverletzer benutzten IP-Adresse und deren spätere Zuordnung zum jeweiligen Anschluss. Sofern eine derartige Ermittlung bzw. Zuordnung daher nicht erfolgen kann, weil etwa die IP-Adresse verschlüsselt wurde, sind diese vom System nicht erfassbar.

Die Anwendung des Warnhinweis-Modells beschränkt sich zudem auf Nutzer in Frankreich. Dem System unterliegen ausschließlich Nutzer französischer IP-Adressen.

³⁴² *Décret n° 2010-1630 du 23.12.2010 relatif à la procédure d'évaluation et de labellisation des moyens de sécurisation destinés à prévenir l'utilisation illicite de l'accès à un service de communication au public en ligne*, abrufbar unter:

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023295302&fastPos=1&fastReqId=772274486&categorieLien=cid&oldAction=rechTexte> .

³⁴³ Artikel R.331-1 à R.335-5 *Code de la propriété intellectuelle*.

³⁴⁴ Die wesentlichen Paragraphen und deren Übersetzung sind im Anhang enthalten.

³⁴⁵ Vgl. Artt. L.331-25, L.336-3 *Code de la propriété intellectuelle (reproduction, représentation, mise à disposition, communication au public)*.

dd. Regelungsinhalt des neuen Schutzsystems

1) *Die Einrichtung der Hadopi*

Zentral für die Funktionsweise des neuen Schutzsystems ist die Hohe Behörde für die Verbreitung der Werke und den Schutz der Rechte im Internet (*Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet* – Hadopi).³⁴⁶ Mit ihr sollte eine staatliche Einrichtung geschaffen werden, die frei, unabhängig und neutral agiert und zwischen den unterschiedlichen Beteiligten und Interessen vermittelt.

a) *Struktur der Hadopi*

Die Hadopi ist nach Artikel L.331-12 CPI unabhängige Verwaltungsbehörde³⁴⁷ und als solche zum Teil nicht den allgemeinen verwaltungsrechtlichen Regeln unterworfen.³⁴⁸

Hauptentscheidungsgremium der Hadopi ist das neunköpfige sog. *Collège* (Kollegium), dessen Präsident oder Präsidentin zugleich Präsident oder Präsidentin der Hadopi ist.³⁴⁹ Das Kollegium, dessen Mitglieder u.a. den obersten französischen Gerichten angehören, setzt sich wie folgt zusammen:

- ein aktives Mitglied des *Conseil d'Etat* (Oberstes Verwaltungsgericht)³⁵⁰,
- ein aktives Mitglied des *Cour de cassation* (Oberster Gerichtshof der ordentlichen Gerichtsbarkeit),
- ein aktives Mitglied des *Cour des comptes* (Rechnungshof),
- ein Mitglied des *Conseil supérieur de la propriété littéraire et artistique* (Hoher Rat des literarischen und künstlerischen Eigentums),
- drei qualifizierte Personen, die auf gemeinsamen Vorschlag der Minister für elektronische Kommunikation, für Verbraucherschutz und für Kultur ernannt werden sowie
- zwei qualifizierte Personen, jeweils benannt vom Präsidenten des *Assemblée nationale* (Parlament) bzw. des *Sénat* (Senat).

Der Präsident oder die Präsidentin der Hadopi muss ein Richter oder eine Person mit richterlicher Funktion sein. Das dreijährige Mandat der Mitglieder des Kollegiums ist nicht widerruflich und kann grundsätzlich nicht verlängert werden.³⁵¹

³⁴⁶ Artikel L.331-12 ff. *Code de la propriété intellectuelle* sowie *Décret n°2009-1773 du 29.12.2009 relatif à l'organisation de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet*, a.a.O.

³⁴⁷ Sog. *Autorité publique indépendante* – API. Diese Rechtsform wurde auch für andere französische Einrichtungen gewählt, etwa der *Commission nationale de l'informatique et des libertés* (Datenschutzbehörde) oder der *Autorité de régulation des communications électroniques et des postes* (Regulierungsbehörde für den Bereich elektronische Kommunikation und Post).

³⁴⁸ Vgl. *Rapport d'activité 2010*, Tätigkeitsbericht der Hadopi über ihre Aktivitäten in den ersten eineinhalb Jahren ihres Bestehens, September 2011, abrufbar unter: <http://www.hadopi.fr/sites/default/files/page/pdf/rapport-d-activite-hadopi.pdf>, S. 25.

³⁴⁹ Artikel L.331-15, L.331-16 *Code de la propriété intellectuelle*.

³⁵⁰ Der Staatsrat ist die oberste verwaltungsgerichtliche Instanz. Außerdem hat er Beratungsfunktion für die Regierung bei Gesetz- und Verordnungsentwürfen.

Neben dem Kollegium ist die *Commission de protection des droits* (Rechtsschutzkommission) fester Bestandteil der Hadopi.³⁵² Sie hat drei Mitglieder, die alle richterliche Funktion ausüben und für jeweils 6 Jahre berufen sind: Ein Mitglied des *Conseil d'Etat*, ein Mitglied des *Cour de cassation* und ein Mitglied des *Cour des comptes*. Auch ihr Mandat ist weder widerruflich noch verlängerbar.

Die Mitglieder der Entscheidungsgremien sind nicht weisungsgebunden. Um die Unabhängigkeit der Entscheidungen der Hadopi darüber hinaus zu gewährleisten, sieht das Gesetz für die Erteilung der Mandate Regelungen über Inkompatibilitäten vor. So dürfen den der Erteilung des Mandats vorangegangenen drei Jahren keine beruflichen Verbindungen zu einer der betroffenen Branchen bestanden haben.³⁵³

Entscheidungen werden in den Gremien der Hohen Behörde nach Stimmenmehrheit getroffen.³⁵⁴

b) Aufgabe der Hadopi

Die Aufgaben der Hadopi sind in Artikel L.331-13 Gesetzbuch über das Geistige Eigentum verankert und umfassen drei Bereiche:

- den Schutz der Urheberrechte im Internet.
- die Beobachtung der Entwicklung legaler und illegaler Nutzung von urheberrechtlich geschützten Werken im Internet und die Förderung legaler Angebote.
- die Regulierung und Überwachung von technischen Schutzmaßnahmen.

Die Hadopi ist damit bedeutende Schnittstelle zwischen den Rechteinhabern, den Internetzugangsanbietern und den Anschlussinhabern. Als Maßnahme zum Schutz von Urheberrechten im Internet bildet die Durchführung des Warnhinweisverfahrens einen wesentlichen Aspekt der Arbeit der Hadopi. Darüber hinaus sind der Hadopi jedoch weitere Aufgaben zugeordnet, die Aspekte der Regulierung, der Förderung und der Aufklärung umfassen:

aa) Veröffentlichungen

Im Rahmen ihrer Pflicht zur Beobachtung des Marktes veröffentlicht die Hadopi jedes Jahr einen Bericht über die Erfüllung ihrer Aufgaben und die Entwicklung des Piraterieverhaltens im Internet. Ein solcher erster Bericht wurde im September 2011 vorgelegt.³⁵⁵

³⁵¹ Eine Ausnahme gilt, wenn die Amtsdauer nur bis zu zwei Jahre dauerte.

³⁵² Artikel L.331-15, L.331-17 *Code de la propriété intellectuelle*.

³⁵³ Artikel L.331-18 *Code de la propriété intellectuelle*.

³⁵⁴ Artikel L.331-20 *Code de la propriété intellectuelle*.

³⁵⁵ Vgl. *Rapport d'activité 2010*, Tätigkeitsbericht der Hadopi über ihre Aktivitäten in den ersten eineinhalb Jahren ihres Bestehens, September 2011, abrufbar unter:
<http://www.hadopi.fr/sites/default/files/page/pdf/rapport-d-activite-hadopi.pdf>.

bb) Zertifizierung

Zu den Maßnahmen der Hadopi betreffend die Förderung legaler Angebote³⁵⁶ gehört u.a. die Erteilung von Gütezertifikaten für Webseiten und die Einrichtung eines Onlineregisters für entsprechende Angebote. Die Zertifikate werden für die urheberrechtliche Unbedenklichkeit eines Angebots erteilt. Der Betreiber eines Onlinedienstes erhält damit die Berechtigung, ein Logo mit der Beschriftung *Hadopi PUR Promotion des Usages Responsable* (dt.: Förderung verantwortungsvoller Nutzung) auf seiner Webseite anzubringen. Es soll dem Nutzer erleichtern, legale Angebote zu identifizieren.³⁵⁷ Der Antrag auf Erteilung eines solchen Zertifikats muss persönliche Angaben über den Betreiber und den Hostprovider sowie eine Liste der verbreiteten Angebote enthalten.³⁵⁸ Darüber hinaus verlangt die Erteilung eines Zertifikats eine Erklärung des Anbieters, dass nicht gegen Urheberrechte verstoßen wird. Die Abgabe einer falschen Erklärung in diesem Zusammenhang ist unter Strafe gestellt.³⁵⁹

Alle in dieser Form eingegangenen Anträge werden veröffentlicht, so dass jedem Urheber die Möglichkeit gegeben ist, innerhalb von vier Wochen Widerspruch gegen die Erteilung zu erheben. Kann im Fall eines solchen Widerspruchs im Rahmen einer von der Hadopi eingeräumten Zeitspanne keine Einigung zwischen den Parteien erzielt werden, sollen streitgegenständliche Werke aus dem Angebot entfernt werden.

Die Zertifizierung ist jeweils mit neuen Angeboten zu aktualisieren.

Bis Ende Juni 2011 lagen 28 Anfragen, in der Mehrheit vonseiten Musikanbietern, aber auch von Anbietern von Software und Online-Gaming vor. Insgesamt 21 Widersprüche wurden (bei 14 Angeboten) eingelegt, nur 7 waren laut Hadopi begründet.³⁶⁰

cc) Kennzeichnungs- und Filtertechniken

Weiterhin zu den Fördermaßnahmen der Hadopi gehört es, Techniken zu evaluieren, mit denen Angebote im Internet gefiltert oder gekennzeichnet werden könnten. Dabei hat die Hadopi zugleich Untersuchungen dazu durchzuführen, wie, d.h. mittels welcher Techniken, die illegale Nutzung urheberrechtlich geschützter Werke im Internet erfolgt.

dd) DRM

Im Hinblick auf die Regulierung von Systemen des Digital Rights Managements hat die Hadopi u.a. dafür Sorge zu tragen, dass eingesetzte technische Schutzmaßnahmen die

³⁵⁶ Vgl. Artikel L.331-23 *Code de la propriété intellectuelle*.

³⁵⁷ Artikel L.331-23 CPI, R.331-47 ff. *Code de la propriété intellectuelle* bzw. *Décret n° 2010-1366 du 10.11.2010*, a.a.O.

³⁵⁸ Formulare der Hadopi abrufbar unter: <http://www.hadopi.fr/hadopi-pro/labellisation-de-loffre- legale/presentation-de-la-procedure>.

³⁵⁹ Artikel 441-6 *Code pénal*, abrufbar unter: <http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719>.

³⁶⁰ Vgl. *Rapport d'activité 2010*, S. 11, 49.

Nutzung von Werken nicht stärker begrenzen, als dies vom Urheberrechtsinhaber selbst intendiert ist bzw. - angesichts gesetzlich zulässiger Kopien (Recht auf Privatkopie) - das Gesetz dies erfordert.³⁶¹ Damit soll insbesondere sichergestellt werden, dass eine Nutzung legal erworbener Werke nicht auf bestimmte Endgeräte beschränkt ist.

2) Das Warnhinweisverfahren

Eine der wesentlichen Neuerungen des eingeführten Rechtsschutzsystems und zugleich eine der wesentlichen Aufgaben der Hadopi ist die Durchführung des Warnhinweisverfahrens. Zuständig für das Verfahren, welches insgesamt drei Stufen durchläuft, ist innerhalb der Hadopi die Rechtsschutzkommission (*Commission de protection des droits*).³⁶²

Ausgangspunkt für das Verfahren bilden über das Internet begangene Urheberrechtsverletzungen. Dem Warnhinweisverfahren vorgelagert ist insofern zunächst die Ermittlung eines Rechtsverstoßes durch die Polizeibehörden oder die Rechteinhaber und die von ihnen Beauftragten. Die Hadopi wird erst auf Anrufung durch die Rechteinhaber bzw. die Staatsanwaltschaft tätig.³⁶³ Da im Hinblick auf den potentiellen Täter der Urheberrechtsverletzung zunächst nur die IP-Adresse bekannt ist, ist in das Verfahren nur der der IP-Adresse zuzuordnende Anschlussinhaber eingebunden.

Nach Abschluss des Warnhinweisverfahrens kann der Vorgang durch die Rechtsschutzkommission der Hadopi zur strafrechtlichen Weiterverfolgung an die zuständigen Justizbehörden übergeben werden. Insofern stellt sich das von der Hadopi durchgeführte Warnhinweisverfahren als Vorstufe für ein gerichtliches Verfahren dar. Der *Conseil d'Etat* hat in seiner Entscheidung Nr. 2009-580 vom 10. Juni 2009 die Funktion der Rechtsschutzkommission der Hadopi als wesentlich für den Zeitpunkt vor Einleitung eines gerichtlichen Verfahrens angesehen und ihr Tätigwerden aufgrund dessen als gerechtfertigt bewertet, dass ihr Nutzen in einer Reduzierung der Anzahl strafbarer Handlungen liegt, die von den Gerichten behandelt werden müssten.³⁶⁴ Gleichwohl ist das Warnhinweisverfahren von Gesetzes wegen nicht insgesamt zwingend der Anrufung der Strafgerichte vorgelagert, sondern es stellt hierzu für die Rechteinhaber grundsätzlich einen alternativen bzw. ergänzenden Verfahrensweg zur Geltendmachung ihrer Rechte dar.³⁶⁵

a) Tatbestandlicher Anknüpfungspunkt

Das Verfahren vor der Hadopi knüpft tatbestandlich an Artikel L.331-25 Gesetzbuch über das Geistige Eigentum an. Danach müssen geeignete Anhaltspunkte dafür bestehen, dass der Anschlussinhaber seinen, ihm vom Gesetz auferlegten Verpflichtungen zur Sicherung

³⁶¹ Artikel L.331-31 *Code de la propriété intellectuelle*.

³⁶² Artikel L.331-17 *Code de la propriété intellectuelle*.

³⁶³ Vgl. Artikel 331-24, 331-25 *Code de la propriété intellectuelle*.

³⁶⁴ Vgl. Entscheidung des *Conseil Constitutionnel* Nr. 2009-580 vom 10.6.2009, Absatz 28.

³⁶⁵ Anders die strafrechtliche Inanspruchnahme des Anschlussinhabers nach R.335-5 *Code de la propriété intellectuelle*, die an die Durchführung des Warnhinweis-Verfahrens anknüpft.

seines Internetzugangs, Artikel L.336-3 Gesetzbuch über das Geistige Eigentum, nicht nachgekommen ist.

Hiernach muss der Inhaber eines Internet-Zugangs dafür Sorge tragen, dass sein Zugang nicht zur Vervielfältigung, Veröffentlichung, Zurverfügungstellung oder Verbreitung von urheberrechtlich geschützten Werken oder Gegenständen ohne Genehmigung der Urheberrechtsinhaber genutzt wird. Wörtlich heißt es in Absatz 1 des Artikel L.336-3:

„La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise.“

„Der Inhaber eines Zugangs zu Online-Kommunikationsdiensten ist verpflichtet, darüber zu wachen, dass dieser Anschluss nicht zum Zwecke der Vervielfältigung, der Darstellung, der Bereitstellung oder der Mitteilung an die Öffentlichkeit von Werken oder Gegenständen, welche durch Urheberrechte oder verwandte Schutzrechte geschützt sind, verwendet wird, ohne dass die Erlaubnis des Trägers der in Buch I und Buch II vorgesehenen Schutzrechte vorliegt, sofern diese Erlaubnis erforderlich ist.“³⁶⁶

Der Tatbestand war im Hadopi I - Gesetz zunächst mit einer Verschuldensvermutung verknüpft worden, wonach der Anschlussinhaber den Nachweis hätte erbringen müssen, dass der Urheberrechtsverstoß über seinen Anschluss durch einen Dritten erfolgt ist.³⁶⁷ Eine solche Regelung wurde jedoch vom *Conseil Constitutionnel* als verfassungswidrig beurteilt.³⁶⁸ Ebenso hatten die vom Gesetzgeber vorgesehenen Sanktionen, die u.a. die Sperrung des Internetanschlusses vorsahen und auf der Basis eines kontradiktorischen Verfahrens vor der Rechtsschutzkommission hätte verhängt werden können, vor dem obersten Gericht keinen Bestand. Das Verfassungsgericht urteilte hierzu, dass der Gesetzgeber angesichts der Bedeutung der Meinungs- und Kommunikationsfreiheit die Verhängung einer Strafe in Form einer Internetsperre nicht einer Verwaltungsbehörde zuweisen durfte.

Das Gesetzbuch über das Geistige Eigentum erfasst nach dem Wortlaut seiner Regelungen (Artt. L.331-25 und L.336-3) zum einen jegliche Form der Rechteverletzung. Die Verfolgbarkeit ist mithin nicht auf Vervielfältigungshandlungen im Rahmen des illegalen Downloads beschränkt. Zum anderen wird keine Unterscheidung getroffen zwischen den unterschiedlichen Techniken, die zur Begehung von Urheberrechtsverstößen verwendet werden können. Rechteverletzungen über Peer-to-Peer-Netzwerke sind damit ebenso erfasst wie solche mittels Sharehosting oder unter Nutzung von Streaming-Verfahren. Die Ver-

³⁶⁶ Übersetzung aus der Entscheidung des *Conseil Constitutionnel* Nr. 2009-580 vom 10.6.2009 (dt. Fassung).

³⁶⁷ Artikel L.331-38 *Code de la propriété intellectuelle* - Entwurf.

³⁶⁸ Vgl. Entscheidung des *Conseil Constitutionnel* Nr. 2009-580 vom 10.6.2009, Absatz 17 ff.

ordnung vom 5. März 2010 betreffend die automatisierte Verarbeitung personenbezogener Daten beschränkt den Handlungsspielraum der Hadopi indes auf Peer-to-Peer-Dienste. Vorbehaltlich einer Erweiterung des Funktionsbereichs der Behörde durch eine entsprechende Änderung dieser Verordnung, die etwa auch erweiterte Maßnahmen, wie etwa die Filterung von Inhalten einschließen könnte, bleibt daher vorläufig lediglich der Dateitausch via Peer-to-Peer vom Anwendungsbereich des Warnhinweisverfahrens erfasst.

b) Antragsberechtigung

Zur Anrufung der Rechtsschutzkommission berechtigt sind vereidigte und vom Ministerium zugelassene Beauftragte der Rechteinhaber. Diese werden durch die Interessenvertretungsorganisationen, die Verwertungsgesellschaften bzw. das „Centre national de la cinématographie“ (Nationales Filmzentrum) benannt. Die vereidigten und zugelassenen Bevollmächtigten recherchieren anhand von den durch die Rechteinhaber erstellten Listen, in denen urheberrechtlich geschützte Werke aufgeführt sind, nach Urheberrechtsverletzungen im Internet. In der Praxis wurde hierfür seitens der Rechteinhaber ein in Nantes ansässiges Unternehmen, Trident Media Guard (TMG), bevollmächtigt.

Darüber hinaus kann die Kommission auch auf Hinweis der Staatsanwaltschaft tätig werden.³⁶⁹

aa) Inhalt des Antrags

Der Antrag muss, um zulässig zu sein, eine eidesstattliche Erklärung des Bevollmächtigten über seine Berechtigung, für den Rechteinhaber zu handeln, sowie bestimmte weitere Informationen enthalten.³⁷⁰ Diese sind in der Verordnung vom 5. März 2010³⁷¹ über die automatische Verarbeitung personenbezogener Daten näher bestimmt und sind:

- Datum und Uhrzeit der vorgeworfenen Tat,
- die ermittelte IP-Adresse,
- das Peer-to-Peer-Protokoll,
- ggf. das vom Nutzer verwendete Pseudonym,
- die betroffenen Werke,
- Name des Internetzugangsanbieters sowie
- Angaben zur Position und Funktion des Bevollmächtigten.

³⁶⁹ Artikel L.331-24 *Code de la propriété intellectuelle*.

³⁷⁰ Artikel R.331-35 *Code de la propriété intellectuelle*.

³⁷¹ *Décret n°2010-236 du 5.3.2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L.331-29 du code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur Internet*, abrufbar unter:

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021923996&fastPos=1&fastReqId=1732810531&categorieLien=cid&oldAction=rechTexte>.

bb) Ablauf des Verfahrens

Wird die Rechtsschutzkommission mit Handlungen, die unter den Tatbestand des Artikels L.336-3 des Gesetzbuchs über das Geistigen Eigentum fallen, befasst, und beurteilt sie den Antrag als substantiiert, fordert sie zunächst Namen und Kontaktdaten des Anschlussinhabers bei dem betreffenden Internetdiensteanbieter an.

Sie übermittelt dazu dem betreffenden Internetzugangsanbieter die relevante IP-Adresse sowie den Zeitpunkt der Rechtsverletzung. Dem Internetzugangsanbieter kommt gemäß Artikel R.331-37 des Gesetzbuchs über das Geistige Eigentum³⁷² die Pflicht zu, die IP-Adresse mit seinen Bestandsdaten abzugleichen und die Identität des Rechteinhabers zu ermitteln.³⁷³ Er hat

- Familienname und Vorname,
- Postanschrift und Emailadresse sowie
- Telefonnummer(n), d.h. insbesondere die Nummer des vertraglichen Telefonanschlusses

innerhalb einer Frist von acht Tagen an die Rechtsschutzkommission zu übermitteln.³⁷⁴

Im dem Fall, dass der Internetdiensteanbieter nicht selbst Vertragspartner des Anschlussinhabers ist, sondern ein Diensteanbieter dazwischen geschaltet ist, der dem Endkunden den Netzzugang mittels der fremden Netzinfrastruktur vermittelt, hat der Internetdiensteanbieter der Rechtsschutzkommission den Namen dieses Internetanbieters und die zugehörige Aktennummer (*numéro de dossier*) zu benennen, so dass die Rechtsschutzkommission an diesen eine weitere Anfrage stellen kann.³⁷⁵

Erfolgt die Mitteilung durch den Internetdiensteanbieter nicht im Rahmen der gesetzten Frist, drohen ihm Geldbußen in Höhe von bis zu 1.500 Euro.³⁷⁶ Bei Wiederholung erhöht sich die Geldbuße auf bis zu 3.000 Euro.³⁷⁷

Liegen der Rechtsschutzkommission die erforderlichen Daten des Anschlussinhabers vor, beginnt sodann ein dreistufiges Verfahren.

(1) Erste Verwarnung

Im ersten Schritt kann die Rechtsschutzkommission dem betroffenen Anschlussinhaber durch dessen Zugangsanbieter einen Hinweis zukommen lassen.³⁷⁸ Dieser Hinweis erfolgt

³⁷² Kodifizierung der Verordnung Nr. 2010-1202 vom 12.10.2010 (*Décret n°2010-1202 du 12.10.2010*), a.a.O.

³⁷³ Verkehrsdaten, d.h. Daten, die für die Zuordnung der IP-Adresse zum Anschlussinhaber erforderlich sind, dürfen nach Artikel L.34-1 *Code des Postes et des télécommunications* (Gesetzbuch über Post und Telekommunikation) ein Jahr lang vom Diensteanbieter gespeichert werden.

³⁷⁴ *Décret n°2010-236 du 5.3.2010*, a.a.O.

³⁷⁵ *Décret n°2010-236 du 5.3.2010* a.a.O.

³⁷⁶ Artikel R.331-38 *Code de la propriété intellectuelle*.

³⁷⁷ Artikel R.331-38 *Code de la propriété intellectuelle*, Artikel 132-11 *Code pénal*.

³⁷⁸ Der Diensteanbieter hat innerhalb von 24 Stunden der Aufforderung der Rechtsschutzkommission nachzukommen, Artikel R.331-37.

per Email. Der Betroffene wird darin an seine Verantwortung erinnert, die ihm durch Artikel L.336-3 des Gesetzbuchs über das geistige Eigentum auferlegt ist und nach der er als Anschlussinhaber dafür Sorge zu tragen hat, dass sein Internetanschluss nicht zur Begehung von Urheberrechtsverletzungen genutzt wird. Zudem wird er über die Verfolgbarkeit von Straftaten nach Artikel L.335-7 und L.335-7-1 des Gesetzbuchs über das Geistige Eigentum aufgeklärt. Der Hinweis enthält auch Informationen über legale Online-Angebote von Werken, über die Existenz von Sicherheitsmaßnahmen und die Auswirkungen von Urheberrechtsverletzungen für das künstlerische Schaffen und die Wirtschaft des kulturellen Sektors. Im Hinweis wird das genaue Datum und die Uhrzeit der vorgeworfenen Urheberrechtsverletzung angegeben. Aus Gründen des Persönlichkeitsschutzes sieht das Gesetz ausdrücklich vor, dass keine Angaben über den konkreten Inhalt der betroffenen urheberrechtlich geschützten Datei gemacht werden dürfen. Dem Anschlussinhaber werden zugleich jedoch Kontaktdaten der Rechtsschutzkommission übermittelt, um ihm die Möglichkeit einer Stellungnahme einzuräumen. Der Anschlussinhaber kann im Rahmen dessen Informationen über die ihm vorgeworfene Rechtsverletzung von der Hadopi anfordern. Mehrheitlich wurden hier in der Praxis der Hadopi Rückfragen zum Inhalt der Dateien, die illegal genutzt sein sollen, gestellt.³⁷⁹

Die erste Verwarnung hat spätestens zwei Monate nach Anrufung der Rechtsschutzkommission zu erfolgen. Wird sie innerhalb dieses Zeitfensters nicht versendet, müssen die bei der Kommission hierzu vorliegenden Daten gelöscht werden.³⁸⁰

(2) Zweite Verwarnung

Wird dem Anschlussinhaber innerhalb von sechs Monaten nach dem ersten Hinweis ein weiterer Verstoß zur Last gelegt, kann die Rechtsschutzkommission einen zweiten Hinweis, in der Praxis auch per Email, mit gleichem Inhalt übersenden. Bei diesem Hinweis wird, anders als beim vorangegangenen eine Empfangsbestätigung, eingefordert.³⁸¹

(3) Aufforderung zur Stellungnahme und Übermittlung an die Staatsanwaltschaft

Wird die Rechtsschutzkommission innerhalb eines auf den zweiten Hinweis folgenden Jahres erneut wegen Verstößen angerufen, die denselben Anschlussinhaber betreffen, kann die Rechtsschutzkommission die Akte an die Staatsanwaltschaft zum Zweck der Strafverfolgung weiterleiten. Hierzu hat sie zunächst selbst eine Einschätzung vorzunehmen, inwieweit durch die vorliegenden Anhaltspunkte eine strafbare Handlung (gemäß Artikel R. 335-5 bzw. Artt. L.335-2, L.335-3, L.335-4 Gesetzbuch über das Geistige Eigentum) als begründet erscheint. Der Anschlussinhaber wird, entsprechend den Vorgaben des Artikels R.331-40 Gesetzbuch über das Geistige Eigentum, zunächst per Einschreiben darüber informiert, dass gegen ihn der Vorwurf erhoben wird, sich der Begehung einer Rechtsverlet-

³⁷⁹ Vgl. *Rapport d'activité* 2010, S. 36 f.

³⁸⁰ Vgl. Artikel 3 *Décret n° 2010-236 du 5 mars 2010*, a.a.O.

³⁸¹ Artikel L.331-25 *Code de la propriété intellectuelle*.

zung schuldig gemacht zu haben. Der Anschlussinhaber wird aufgefordert, innerhalb von fünfzehn Tagen zu diesem Vorwurf Stellung zu nehmen sowie Angaben zu seiner finanziellen Belastung durch die Familie und seinen Einnahmen zu machen. Der Betroffene kann sich in diesem Verfahrensstadium eines Rechtsbeistandes bedienen. Anstelle des Schriftwechsels kann, wie dies in der Praxis von der Hadopi auch so gehandhabt wird, eine Anhörung von der Rechtsschutzkommission durchgeführt werden.³⁸² Kommt die Rechtsschutzkommission zu dem Ergebnis, dass eine Gesetzesübertretung vorliegt, macht sie Mitteilung hierüber beim Oberstaatsanwalt des zuständigen Landgerichts, und informiert die Rechteinhaber hierüber.³⁸³

cc) Entscheidungsrahmen der Hadopi

Das Gesetz lässt der Hadopi bzw. der Rechtsschutzkommission einen sehr weiten Entscheidungsspielraum darüber, ob ein Warnhinweis versendet bzw. das Verfahren am Ende an die Staatsanwaltschaft übergeben werden soll.³⁸⁴ Die intern erarbeiteten Kriterien für die Ausübung des Ermessens, an denen sich das Handeln der Hadopi bzw. die Entscheidungspraxis der Rechtsschutzkommission ausrichtet, sind nicht in Einzelheiten öffentlich bekannt. Sie richten sich jedoch an dem ihr übertragenen Auftrag aus, den die Hadopi in erster Linie darin sieht, aufzuklären und unter pädagogischen Aspekten auf die Nutzer, die in unrechtmäßiger Weise geschützte Werke nutzen, einzuwirken. In der Praxis wird von der Hadopi bei der mehrfachen Verwirklichung eines Verstoßes daher auch berücksichtigt, inwieweit sich hierin der Unrechtsgehalt der Handlung erhöht. Mehrfache Verstöße eines Internetnutzers werden etwa nicht jeweils mit einem eigenen Warnhinweis belegt, wenn ersichtlich ist, dass diese Verstöße im gleichen Kontext erfolgten (etwa auch wegen wiederholter Internetnutzung bei aktivierter Filesharing-Software, die jeweils einen Zugriff auf Verzeichnisse des Rechners erlaubt).

Die Hadopi steht den betroffenen Anschlussinhabern darüber hinaus für Fragen und Informationen zur Verfügung und nimmt insofern auch beratende Funktion wahr. Dies gilt insbesondere auch für Fragen zur ausreichenden Sicherung des Internetzugangs.

Rechtsmittel der Betroffenen oder Rechteinhaber gegen die Entscheidungen der Hadopi bzw. gegen ein etwaiges behördliches Unterlassen ihrerseits bestehen nicht.

3) Gerichtliche Schritte

a) Tatbestandliche Grundlagen - Ahndung von Urheberrechtsverstößen

Das Verfahren vor der Hadopi kann, wie dargelegt, in die strafgerichtliche Verfolgung von Urheberrechtsverstößen münden.

³⁸² Artikel R.331-40 bis 331-43 *Code de la propriété intellectuelle*.

³⁸³ Artikel R.331-43 *Code de la propriété intellectuelle*.

³⁸⁴ Im Gesetz ist dies an die Formulierung „kann“ geknüpft.

aa) Straftatbestand der Raubkopie

Die zentrale Vorschrift für die Durchsetzung des Schutzes des Urheberrechts ist im französischen Recht der Straftatbestand der Raubkopie (*Contrefaçon*). Dieser wurde bereits 1992 geschaffen und als Artikel L.335-2 in das Gesetzbuch über das Geistige Eigentum eingefügt. Der Straftatbestand ist nicht auf die Begehung von Urheberrechtsverletzungen im analogen oder digitalen Umfeld beschränkt und daher für gewöhnliche Raubkopien ebenso wie auf online gefertigte Raubkopien anwendbar.

Unter Strafe gestellt ist danach jede Vervielfältigung eines urheberrechtlich geschützten Werks im Ganzen oder in Teilen unter Missachtung der Gesetze und sonstigen Regelungen zum Schutz des Urheberrechts. Gleiches gilt für den Verkauf sowie die Ein- oder Ausfuhr von Raubkopien.

„Toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production, imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon et toute contrefaçon est un délit.

La contrefaçon en France d'ouvrages publiés en France ou à l'étranger est punie de trois ans d'emprisonnement et de 300 000 euros d'amende.

Seront punis des mêmes peines le débit, l'exportation et l'importation des ouvrages contrefaisants.

Lorsque les délits prévus par le présent article ont été commis en bande organisée, les peines sont portées à cinq ans d'emprisonnement et à 500 000 euros d'amende.“

Der Tatbestand der Raubkopie selbst wurde seit seiner Einführung nie verändert, allein das Strafmaß wurde in der Vergangenheit mehrfach erhöht. So betrug die zu verhängende Strafe im Jahr 1992 zwischen 3 Monaten und 2 Jahren Haft oder/und eine Geldstrafe von 6.000 bis 120.000 Franc³⁸⁵, im Jahr 2000 waren es 2 Jahre Haft und 1.000.000 Franc³⁸⁶. Seit 2004 sind, wie bereits dargelegt, bis zu 3 Jahre Gefängnis und 300.000 Euro als Strafe vorgesehen.

bb) Fahrlässigkeitstatbestand

Die Novellierung durch die Hadopi-Gesetze 2009 und 2010 enthielten keine Änderungen der Regelungen betreffend die Raubkopie. Durch sie wurden aber weitere Tatbestände eingefügt,³⁸⁷ die insbesondere den Internetanschlussinhaber stärker in die Verantwortung nehmen.

³⁸⁵ Nach derzeitigem Umrechnungskurs wären dies etwa 900 bis 18.000 €.

³⁸⁶ Nach derzeitigem Umrechnungskurs wären dies etwa 150.000 €.

³⁸⁷ Auch das Aufzeichnen von Filmen im Kino (sog. Camcording) wurde als Straftat eingeführt; L.335-3 Gesetzbuch über Geistiges Eigentum.

Einen wesentlichen Tatbestand bildet insofern Artikel L.336-3 des Gesetzbuchs über das Geistige Eigentum, der im Wortlaut seines Absatz 1 dem ehemaligen Artikel L.335-12 Gesetzbuch über das Geistige Eigentum entspricht und, wie dargelegt, Ausgangspunkt für die Einleitung des Verfahrens vor der Hadopi ist.

Die in Artikel L.336-3 in seiner jetzigen Fassung enthaltene Verpflichtung des Anschlussinhabers wird ergänzt durch einen speziellen Fahrlässigkeitstatbestand, der mit Verordnung vom Juni 2010 in den Anordnungsteil des Dritten Buchs des Gesetzbuchs über das Geistige Eigentum, Artikel R. 335-5, aufgenommen wurde.³⁸⁸ Dieser sanktioniert den Inhaber eines Internetanschlusses, wenn er keine Maßnahmen zur Sicherung des Anschlusses getroffen hat oder ihm im Hinblick auf die Ergreifung solcher Maßnahme ein Sorgfaltsverstoß vorzuwerfen ist. Eine Bestrafung setzt jedoch zudem voraus, dass ein Hinweis im Rahmen des Warnhinweisverfahrens an den Anschlussinhaber erfolgt ist, seinen Anschluss zu schützen, und es im Laufe eines Jahres nach der Zustellung dieser Empfehlung erneut zu einer Urheberrechtsverletzung kommt.

Wird über einen Internetzugang daher eine der Tathandlungen der Raubkopie begangen, kann der Inhaber des Internetanschlusses, unabhängig davon, ob ihm die Verletzung der Urheberrechte selbst zur Last gelegt werden kann, aufgrund der Verletzung von Sicherungspflichten strafrechtlich in die Verantwortung genommen werden.

Dabei gilt für Unternehmen grundsätzlich derselbe Maßstab wie für private Anschlussinhaber. Auch die Unternehmen, die ihren Kunden oder Mitarbeitern Internetzugänge zur Verfügung stellen, sind verpflichtet, Maßnahmen zu ergreifen, um die Begehung von Urheberrechtsverletzungen über ihren Internetzugang zu verhindern. Andernfalls kommt auch hier eine strafrechtliche Sanktionierung des Verantwortlichen nach Art. R.335-5 Gesetzbuchs über das Geistige Eigentum in Betracht.

Der Anschlussinhaber hat insofern alle Maßnahmen zu ergreifen, die eine unerlaubte Nutzung des Internet-Zugangs durch Dritte verhindern. Welche Sicherheitsmaßnahmen dies konkret sind, ist nicht im Gesetz geregelt, sondern wird von der Hadopi definiert.³⁸⁹ Hinweise zu technischen Maßnahmen zur Sicherung des Internetzugangs enthalten die von ihr versendeten Warnhinweise. Außerdem nimmt die Hadopi eine beratende Funktion ein und tritt im Einzelfall in Dialog mit den jeweils Betroffenen, so dass hier auf Besonderheiten, etwa bei der Bereitstellung von Internetanschlüssen durch Unternehmen, eingegangen werden kann.

Vorgesehen ist desweiteren auch, dass die Hadopi Gütesiegel für bestimmte Sicherheitsmaßnahmen vergibt.³⁹⁰

³⁸⁸ Art. 1 *Décret n°2010-695 du 25 juin 2010*, a.a.O.

³⁸⁹ Artikel L.331-31 f. *Code de la propriété intellectuelle*.

³⁹⁰ Artikel L.331-26 *Code de la propriété intellectuelle*.

b) Rechtsfolgen

Die strafrechtliche Verfolgung der Rechtsverletzung obliegt der Staatsanwaltschaft. Sie entscheidet nach Mitteilung durch die Rechtsschutzkommission oder der Polizeiorgane über die strafrechtliche Verfolgung des Anschlussinhabers und das anzuwendende Verfahren. Zur Beschleunigung kann die Sanktionierung mittels Strafbefehl³⁹¹ erfolgen. Im Übrigen findet das reguläre gerichtliche Verfahren statt.

Die Staatsanwaltschaft informiert die Rechtsschutzkommission über ihre jeweilige Entscheidung.³⁹²

Die im Rahmen des Strafverfahrens zu verhängenden Hauptstrafen sind grundsätzlich Haft- und Geldstrafen. Das Strafmaß ist nach Art und Umfang der Tat festgelegt. Einige Taten fallen unter die Straftat der Raubkopie, andere sind nur als Ordnungswidrigkeiten eingestuft.³⁹³

Alle Taten, die unter die Straftat der Raubkopie fallen, werden mit bis zu drei Jahren Gefängnisstrafe und 300.000 Euro Geldstrafe bestraft. Die Ordnungswidrigkeiten können generell mit Geldbußen von bis zu 3.750 Euro geahndet werden. Zu den Ordnungswidrigkeiten zählt etwa der Tatbestand der groben Fahrlässigkeit nach Artikel R. 335-5 Gesetzbuch über das Geistige Eigentum, der mit einer Geldbuße von bis zu 1.500 Euro belegt ist.³⁹⁴

Neu eingeführt wurde mit den Hadopi-Gesetzen die zweitweise Sperrung des Internetanschlusses als ergänzende Sanktionsmöglichkeit. Es handelt sich hierbei um eine Zusatzstrafe, die neben den allgemeinen Strafen durch das Gericht angeordnet werden kann. Mit dieser Sperrung wird auch der Abschluss eines neuen Vertrags während der Sperrzeit untersagt. Dem Anschlussinhaber drohen bei Verstoß ein Bußgeld in Höhe von bis zu 3.750 Euro³⁹⁵, dem Internetzugangsdiensteanbieter eine Strafe von bis zu 5.000 Euro. Die Sperrung kann wegen des Haupttatbestands der Raubkopie³⁹⁶ bis zu einem Jahr und wegen des sekundären Tatbestands³⁹⁷ für bis zu einen Monat verhängt werden. Während der Sperrung muss der Zugang zu Telefon- und Fernsehdiensten weiter gewährleistet werden. Die vertraglichen Kosten für den Internetanschluss bleiben von der Sperre unberührt und sind vom Anschlussinhaber weiter zu tragen. Ist die Strafe vollstreckbar, sind die Internet-

³⁹¹ Sogenannte *ordonnance pénale*.

³⁹² Artikel R.331-44 *Code de la propriété intellectuelle*.

³⁹³ Der Unterschied in Frankreich zwischen Straftaten und Ordnungswidrigkeiten betrifft nur das Strafmaß. Die beiden sind strafrechtlich von der Staatsanwaltschaft verfolgt. Bei Ordnungswidrigkeit werden nur Geldstrafen verhängt. Die Straftaten sind in Verbrechen und Vergehen unterteilt. Alle Straftaten, die mit mehr als 10 Jahre Freiheitsstrafe verurteilt sind, sind Verbrechen, die übrigen sind Vergehen.

³⁹⁴ Eine weitere Ordnungswidrigkeit ist etwa die Nutzung von Software zum Zwecke der Umgehung von DRM-Maßnahmen (Artikel R.335-4 *Code de la propriété intellectuelle*).

³⁹⁵ Artikel 335-7-1 *Code de la propriété intellectuelle*.

³⁹⁶ Artikel L.335-7 *Code de la propriété intellectuelle*.

³⁹⁷ Artikel L.335-7-1 und Artikel R.335-5 *Code de la propriété intellectuelle*.

anbieter unter Androhung von Bußgeld verpflichtet, den Internetanschluss innerhalb von 15 Tagen zu sperren.³⁹⁸

4) *Weitere rechtliche Rahmenbedingungen*

a) *Auskunftsansprüche gegen Internet-Zugangsanbieter*

Den Internetzugangsdiensteanbietern obliegt eine Auskunftspflicht gegenüber der Rechtsschutzkommission. So kann die Rechtsschutzkommission im Rahmen der Durchführung des Warnhinweisverfahrens Informationen über die Identität eines Anschlussinhabers verlangen. Gemäß Artikel R. 331-37 des Gesetzbuch über das Geistige Eigentum haben die Diensteanbieter innerhalb von 8 Tagen der Aufforderung der Rechtsschutzkommission zur Mitteilung von Daten über den Anschlussinhaber nachzukommen.

Der Rechteinhaber selbst hat keinen solchen Auskunftsanspruch gegenüber dem Internetdiensteanbieter. Kenntnis über die Identität eines Anschlussinhabers kann er nur über ein strafrechtliches Ermittlungsverfahren erlangen. Leitet die Staatsanwaltschaft gegen den Inhaber des Internetanschlusses ein strafrechtliches Verfahren ein, kann der Anspruchsberechtigte etwa eine Kopie der Akte verlangen und seine Ansprüche bereits im Rahmen des strafrechtlichen Verfahrens geltend machen. Werden die Ermittlungen von der Staatsanwaltschaft eingestellt, darf der Anspruchsberechtigte ebenfalls eine Kopie der Akte fordern, um seinerseits vor dem Zivilgericht zu klagen.

Ein Auskunftsrecht oder ein Recht auf Akteneinsicht gegenüber der Rechtsschutzkommission der Hadopi steht dem Rechteinhaber nicht zu. Der Anspruchsberechtigte erhält jedoch eine Mitteilung der Rechtsschutzkommission, wenn sein Fall an die Staatsanwaltschaft weitergegeben wird.³⁹⁹

b) *Zivilrechtliche Durchsetzung von Urheberrechten*

In Frankreich können die Opfer einer Straftat im Zuge eines strafrechtlichen Verfahrens als Nebenkläger Schadensersatz fordern. Diese Möglichkeit erstreckt sich bislang indes nicht auf Strafbefehlsverfahren, so dass Anspruchsberechtigte insoweit auf den Zivilrechtsweg angewiesen bleiben.⁴⁰⁰ Wiederholungstäter werden grundsätzlich im üblichen Strafverfahren angeklagt, so dass hier die Anspruchsberechtigten regelmäßig im Rahmen des Verfahrens ihre Ansprüche geltend machen können.

³⁹⁸ Artikel L.335-7 *Code de la propriété intellectuelle*.

³⁹⁹ Artikel 4 *Décret n°2010-236 du 5 mars 2010*, a.a.O.

⁴⁰⁰ Derzeit wird ein Gesetzentwurf diskutiert, der die die Geltendmachung von Schadensersatz auch in Strafbefehlsverfahren ermöglichen soll. Dieser Entwurf wurde durch die *Assemblée Nationale* Anfang Juli 2011 angenommen.

Im Übrigen sind Schadensersatzansprüche von den Rechteinhabern vor den Zivilgerichten geltend zu machen. Das Verfahren folgt hierbei den allgemeinen Zivilverfahrensregeln, jedoch wird als Besonderheit die Zuständigkeit bestimmter Landgerichte vorgegeben.⁴⁰¹

Der Unterlassungsanspruch ist im französischen Recht in den Artikeln 1382 ff. des *Code Civil* (Zivilgesetzbuch) verankert. Da er deliktischer Natur ist, setzt er, insofern anders als im deutschen Zivilrecht, immer Verschulden voraus. Ihm kommt daher im Rahmen der Rechtsdurchsetzung von Urheberrechtsverletzungen nur begrenzte Wirkung zu, da auch ihm faktisch die Ermittlung des Täters vorangestellt ist.

c. Technische/organisatorische Umsetzung des Warnhinweismodells

Die Einführung des geltenden französischen Warnhinweis-Modells war mit Hindernissen verbunden und erfolgte daher bis zu seiner jetzigen Ausformung stufenweise im Rahmen von Nachbesserungen und Ergänzungen.

So wurde bereits das erste Gesetz vom 12. Juni 2009 zur Einführung des Modells verfassungsgerichtlich überprüft und für teilweise verfassungswidrig erklärt⁴⁰². Im Oktober 2009 wurde daher per Gesetz nachgebessert, um die beanstandeten Regelungen zur Strafverfolgung und zum Datenschutz zu korrigieren.

Da die Internetzugangsdiensteanbieter, vor allem der Diensteanbieter „Free“, sich weigerten, mit der Rechtsschutzkommission zu kooperieren, wurde zudem ergänzend eine spezielle Verordnung erlassen, um die Kooperation zu erzwingen. Erst die sogenannte „Free-Verordnung“⁴⁰³ verpflichtet die Dienste-Anbieter unter Androhung einer Geldbuße innerhalb vorgegebener Frist die personenbezogenen Daten des Anschlussinhabers zu übermitteln.

Ebenso stellt sich der **Datenschutz** insofern als kritischer Punkt heraus, als es hier in der Umsetzung zu Zwischenfällen kam. Da der Server des in Nantes ansässigen, vonseiten der Rechteinhaber zur Ermittlung von IP-Adressen beauftragten Unternehmens „TMG“ Anfang 2011 für mehrere Stunden ungeschützt war, waren mehrere tausend personenbezogene Daten dem Zugriff Dritter ausgesetzt. Nach einer Überprüfung des Unternehmens durch

⁴⁰¹ Die Liste der zuständigen Landgerichte wird durch eine entsprechende Verordnung bestimmt. Regelungen zur Geltungsmachung zivilrechtlicher Ansprüche der Urheberrechtsinhaber sind in den Artikel L.331-1 bis 4 *Code de la propriété intellectuelle* niedergelegt.

⁴⁰² Das erste Gesetz sah vor, dass die Hadopi selbst die Internet-Sperrung anordnen kann. Diese Tätigkeit sei nur Kompetenz der Gerichte nach dem Verfassungsgericht. Siehe S. 114.

⁴⁰³ Kodifiziert in Artikel R.331-37: *Décret n°2010-1202 du 12.10.2010 modifiant l'article R.331-37 du code de la propriété intellectuelle*, abrufbar unter:
<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022913572&fastPos=1&fastReqId=161056296&categorieLien=cid&oldAction=rechTexte>.

die CNIL im Mai 2011 wurde das Unternehmen angemahnt, innerhalb von drei Monate die Sicherheitslücke zu schließen.⁴⁰⁴

Das Warnhinweisverfahren trat im Sommer 2010 in Kraft. Im August gingen die ersten Verfahrensanträge von Rechteinhabern bei der Hadopi ein.⁴⁰⁵

Insgesamt erhielt die Hadopi im Zeitraum zwischen Oktober 2010 und Juni 2011 knapp **18,5 Millionen** Verfahrensanträge von Rechteinhabern.⁴⁰⁶ Gerechnet als Mittelwert, einschließlich des Monats September 2010, waren es - um die Dimensionen des Umfangs aufzuzeigen - mehr als 71.500 Anträge pro Monat.⁴⁰⁷

Hiervon ausgehend wurden von der Hadopi insgesamt über **eine Million** Anfragen bei den Zugangsdiensteanbietern zur Identifikation von Anschlussinhabern anhand der verwendeten IP-Adressen gestellt.

Die Anzahl der an die Zugangsdiensteanbieter gerichteten Anfragen wurde vor dem Hintergrund der Notwendigkeit einer Etablierung interner Verfahrensabläufe vonseiten der Hadopi phasenweise erhöht. Während im September 2010 noch einige Hundert Anfragen gestellt wurden, erhöhte sich die Zahl der Anfragen bis Mai 2011 auf 11.500 Anfragen pro Tag.⁴⁰⁸

Eine Zuordnung von IP-Adresse und Anschlussinhaber konnte in 89 Prozent der Anfragen vorgenommen werden.⁴⁰⁹

Erste Warnhinweise wurden durch die Zugangsdiensteanbieter - per Email - im September 2010 versandt, die ersten Warnhinweise der zweiten Stufe - versandt per Email mit Rückantwort - folgten im Februar 2011.

Insgesamt waren es bis Ende Juni 2011 **470.935** erste und **20.598** zweite Warnhinweise.⁴¹⁰ Nach aktuellen Zahlen der Hadopi wurden mit Stand vom November 2011 insgesamt 700.000 Warnhinweise der 1. Stufe und 55.000 Warnhinweise der 2. Stufe versandt.

In der dritten Stufe des Warnhinweisverfahrens befinden sich ebenfalls mit Stand von November 2011 insgesamt 111 Anträge in der 3. Phase, in der Anhörungen vor der Rechtsschutzkommission durchgeführt werden. Es ist fraglich, ob die Rechtsschutzkommission, die sich im Wesentlichen in der Rolle eines Präventionsorgans sieht, die Staatsanwaltschaft einschalten wird. Bisher wurde keine der Akten weitergeleitet.

Die Aktivitäten der Hadopi verdeutlicht die nachstehende Grafik:

⁴⁰⁴Pressemitteilung der CNIL vom 6.7.2011, abrufbar unter: <http://www.cnil.fr/la-cnil/actu-cnil/article/article/dispositif-de-reponse-graduee-la-cnil-met-en-demeure-les-societes-de-perception-et-de-repa/>.

⁴⁰⁵ *Rapport d'activité 2010*, a.a.O., S. 11.

⁴⁰⁶ 18.429.234, vgl. *Rapport d'activité 2010*, a.a.O., S. 43.

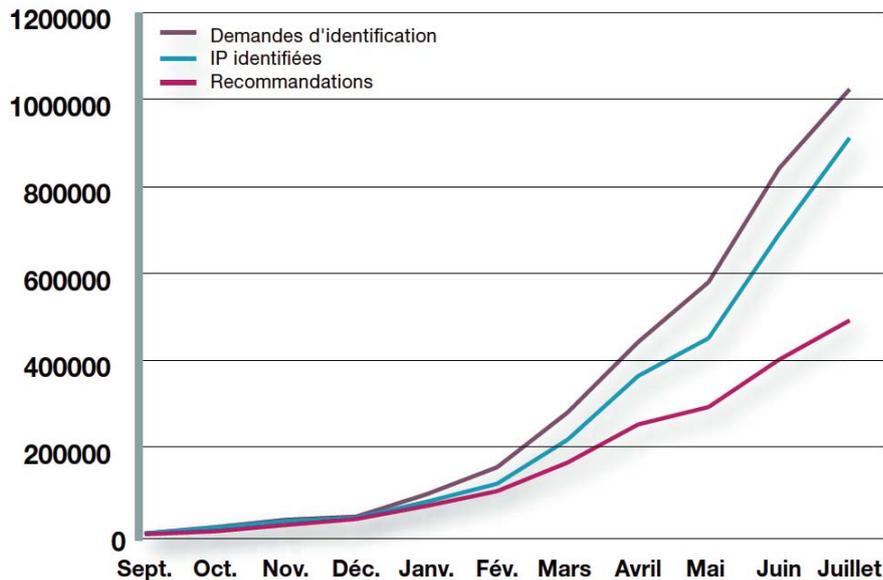
⁴⁰⁷ 71.613, vgl. *Rapport d'activité 2010*, a.a.O., S. 43.

⁴⁰⁸ Vgl. *Rapport d'activité 2010*, a.a.O., S. 43.

⁴⁰⁹ Von insgesamt 1.023.079 Anfragen wurden 911.970 identifiziert, vgl. Bericht, S. 11.

⁴¹⁰ Vgl. *Rapport d'activité 2010*, a.a.O., S. 11, 44.

NOMBRE CUMULÉ D'IDENTIFICATIONS ET DE RECOMMANDATIONS



Grafik Nr. 1: Bericht der Hadopi, S. 43. Der violette Balken weist die Anfragen an die Internetzugangsdiensteanbieter aus, der blaue die Identifizierten Anschlussinhaber und der pinkfarbene die Anzahl der versandten Warnhinweise.

Die erkennbare Differenz zwischen der Anzahl der Anträge von Rechteinhabern und der Anzahl der bei den Internetdiensteanbietern gestellten Anfragen einerseits sowie zwischen der Anzahl dieser Anfragen bei den Diensteanbietern und der Versendung erster Warnhinweise andererseits erklärt sich zum einen aus verfahrenstechnischen Gründen. Die bei der Hadopi eingegangenen Anträge werden schrittweise bearbeitet. Das interne technische Verfahren zur Bearbeitung der Anträge ist derzeit noch in der Einführungsphase und es wird an der Optimierung der technischen Infrastruktur gearbeitet, um die Verfahren noch zügiger durchzuführen.

Zum anderen haben die Differenzen teils auch inhaltliche Gründe. So handelt es sich bei manchen Anträgen um solche, die von verschiedenen Bevollmächtigten in derselben Sache gestellt werden. Zudem werden bestimmte Mehrfachverstöße von der Hadopi als ein einheitlicher Sachverhalt gewertet und entsprechend in einem einzigen Warnhinweis zusammengefasst. So wird verfahrenstechnisch der Antrag eines Rechteinhabers zunächst zwar auf Substantiiertheit geprüft, bevor eine Anfrage an den Internetzugangsdiensteanbieter zur Identifizierung des Anschlussinhabers erfolgt. Da jedoch erst im Zeitpunkt der Mitteilung durch den Internetzugangsdiensteanbieter bekannt ist, ob verschiedene Anträgen denselben Anschlussinhaber betreffen und gegebenenfalls mehrere Tathandlungen - entsprechend der Entscheidungspraxis der Rechtsschutzkom-

mission - als Einheit zusammengefasst werden können, folgt eine weitere Prüfung des Sachverhalts nach Mitteilung durch den Diensteanbieter.

4. Datenschutzrechtliche Fragen von Warnhinweismodellen

Die Hadopi ist zur automatischen Verarbeitung personenbezogener Daten bevollmächtigt,⁴¹¹ sofern und soweit dies erforderlich ist, um die Durchführung des Verfahrens durch die Rechtsschutzkommission zu ermöglichen.

Die Verordnung vom 5. März 2010⁴¹² regelt, welche Daten erhoben und gespeichert werden dürfen, wie lange diese Daten vorgehalten werden dürfen und wer zur Nutzung dieser Daten berechtigt ist.

Eine wesentliche Ergänzung erhielt die Verordnung durch eine weitere Verordnung vom 11.3.2011⁴¹³. Dies war eine Reaktion auf die Stellungnahme der für den Datenschutz zuständigen CNIL. Sie bemängelte zwar nicht die gesammelten Daten an sich, kritisierte aber, dass die Daten nicht unmittelbar gelöscht wurden im Fall, dass die Rechtsschutzkommission das Verfahren nicht der Staatsanwaltschaft übergab. Mit Verordnung vom 11. März 2011 wurde daher für jeden Stand des Verfahrens klargestellt, wann jeweils welche personenbezogenen Daten gelöscht sein müssen.

Erhoben werden dürfen personenbezogene Daten, die die Tat und den Inhaber des Internetanschlusses betreffen. Die Bevollmächtigten der Rechteinhaber sind berechtigt, folgende Daten zu ermitteln und an die Rechtsschutzkommission weiterzugeben:

- Datum und Uhrzeit der Urheberrechtsverletzung,
- IP-Adresse des Nutzers,
- Name des benutzten Peer-to-Peer Protokolls,
- Benutzername des Internetnutzers,
- Informationen über die urheberrechtlich geschützten Werke,
- Name der Datei auf dem Computer des Internetnutzers,
- Name des Internetanbieters.

Darüber hinaus haben sie folgende Angaben zu machen, die die Rechtsschutzkommission speichern darf:

- Familienname und Vorname des Bevollmächtigten,
- Datum und Dauer seiner Zulassung,

⁴¹¹ Artikel L.331-29 *Code de la propriété intellectuelle*.

⁴¹² Siehe oben, S. 88.

⁴¹³ *Décret n°2011-264 du 11.3.2011 modifiant le décret n°2010-236 du 5.03.2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L.331-29 du code de la propriété intellectuelle*, abrufbar un-

ter:<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023690143&fastPos=1&fastReqId=434240394&categorieLien=cid&oldAction=rechTexte>.

- Datum seiner Vereidigung,
- Name der Organisation, die ihn benannt hat.

Vonseiten der Internet-Anbieter sind

- Familiennamen und Vorname,
- Post- und Mailadresse des Inhabers des Internetanschlusses und
- Telefonnummer

an die Rechtsschutzkommission weiterzuleiten.⁴¹⁴

Nach der geltenden Regelung dürfen personenbezogene Daten⁴¹⁵ nur eine begrenzte Zeit gespeichert bzw. gelagert werden.⁴¹⁶ Lässt die Rechtsschutzkommission keinen Hinweis versenden, müssen die Daten zwei Monate nach Erhalt gelöscht werden. Die Löschung muss spätestens 14 Monate nach dem Versand des ersten Hinweises erfolgen, wenn in dieser Frist kein zweiter Hinweis verschickt wurde. Wenn die Akte nicht an den Staatsanwalt weitergeleitet wurde, muss die Löschung 21 Monate nach dem Zugang des zweiten Hinweises erfolgen. Wird innerhalb eines Jahres nach Weiterleitung der Akte von der Staatsanwaltschaft kein Verfahren eingeleitet, müssen die personenbezogenen Daten gelöscht werden. Die Daten müssen auch gelöscht werden, sobald die Rechtsschutzkommission durch die Staatsanwaltschaft informiert ist, dass keine Sperrung des Internetanschlusses durch das Gericht angeordnet wurde. Wird eine Sperrung angeordnet, müssen die Daten gelöscht werden, sobald die Sperrung in das polizeiliche Führungszeugnis eingetragen wird. Spätestens muss die Löschung zwei Jahre nach der gerichtlichen Verurteilung erfolgen.

Unmittelbaren Zugang zu den vorgehaltenen personenbezogenen Daten haben die vereidigten und zugelassenen Bevollmächtigten der Rechteinhaber und die Mitglieder der Rechtsschutzkommission. Den Internet-Anbietern werden nur die technischen Daten zur Ermittlung des Inhabers des Internet-Zugangs, die Hinweise der Rechtsschutzkommission und die notwendigen Informationen für die Sperrung des Internet-Zugangs übermittelt⁴¹⁷. Die Justizbehörden erhalten Feststellungsprotokolle über die ermittelte Urheberrechtsverletzung.⁴¹⁸ Das in Artikel 38 des Gesetzes vom 6. Januar 1978⁴¹⁹ vorgesehene Widerspruchsrecht gegen die Erhebung von Daten ist in diesem Fall nicht anwendbar.

⁴¹⁴ Siehe S. 96.

⁴¹⁵ Liste in Anhang der Verordnung, *Décret n° 2010-236 du 5.3.2010*.

⁴¹⁶ Artikel 3 *Décret n°2010-236 du 5.3.2010*.

⁴¹⁷ Die technischen Daten für die Identifizierung des Zugangsinhabers, die Empfehlungen der Kommission, die notwendigen Informationen für die Internetzugangssperrung.

⁴¹⁸ Artikel 4 *Décret n°2010-236 du 5.3.2010*.

⁴¹⁹ Artikel 38 des Gesetzes Nr. 78-17 vom 6.1.1978 über Informatik, Daten und Freiheiten (*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*) sieht vor, dass jeder ein Einspruchsrecht auf die Verarbeitung und Weiterleitung seiner personenbezogenen Daten hat. Da dieser Artikel hier nicht anwendbar ist, haben die Inhaber der Internet-Zugänge keinen Einspruch über die Sammlung, Verarbeitung, Speicherung und Weiterleitung ihren personenbezogenen Daten. Dieses Gesetz ist abrufbar unter:

5. Zusammenfassung

Mit den Hadopi-Gesetzen vom Juni und Oktober 2009 wurde in Frankreich ein System zum Schutz von Urheberrechten im Internet eingeführt, das als wesentlichen Kern ein mehrstufiges Warnhinweisverfahren beinhaltet. Dieses wird von der Hadopi als neu eingerichtete, unabhängige Behörde durchgeführt und ermöglicht die Versendung von Warnhinweisen an Inhaber von Internetanschlüssen, über die Urheberrechtsverletzungen begangen wurden. Nach zwei Warnhinweisen innerhalb eines Zeitraums von zwei Monaten und einem weiteren Verstoß innerhalb des darauffolgenden Jahres kann die Hadopi den Sachverhalt an die Staatsanwaltschaft abgeben und so in ein strafrechtliches Verfahren überleiten. Der Anschlussinhaber hat, unabhängig davon, ob er selbst die Urheberrechtsverletzungen begangen hat, nach dem Gesetz die Pflicht, für eine ausreichende Sicherung seines Internetanschlusses zu sorgen. Kommt er dem nicht nach, kann im strafrechtlichen Verfahren gegen ihn eine Geldbuße in Höhe von bis zu 1.500 Euro auferlegt und sein Internetanschluss für bis zu einen Monat gesperrt werden.

Die Ermittlung der Urheberrechtsverletzung erfolgt durch Bevollmächtigte der Rechteinhaber. Sie teilen der Hadopi die IP-Adresse des potentiellen Urheberrechtsverletzers mit. Die Zuordnung der IP-Adresse zum jeweiligen Anschlussinhaber erfolgt durch die Internetzugangsdiensteanbieter, welche gegenüber der Hadopi zur Auskunft verpflichtet sind. Verstöße gegen diese Mitteilungspflicht sind mit Geldbußen belegt.

Das Warnhinweissystem stellt sich als Maßnahme dar, die außerhalb des (straf-)gerichtlichen Verfahrens zur Eindämmung von Urheberrechtsverstößen im Internet beitragen und für einen gerechten Interessenausgleich zwischen den Beteiligten unter Beachtung rechtsstaatlicher Maßgaben sorgen soll. Das Warnhinweissystem ist insofern in Zusammenhang mit den weiteren Maßnahmen zu sehen, die durch die Hadopi-Gesetze initiiert wurden und die weitere Aufklärung sowie die Förderung von legalen kulturellen Angeboten im Internet zum Gegenstand haben.

II. Vereinigtes Königreich

1. Ausgangslage (Überblick)

a. *Rechtliche Rahmenbedingungen*

Der Urheberrechtsschutz ist im Vereinigten Königreich umfassend geregelt und kennt seit 1974 einen Auskunftsanspruch der Rechteinhaber gegenüber unbeteiligten Dritten nach Rechtsverletzungen.

aa. Gesetzliche Verankerung des Schutzes von Urheberrechten

Urheberrechtsschutz hat im Vereinigten Königreich traditionell einen hohen Stellenwert. Mit dem Erlass des *Statute of Anne* im Jahr 1710 war Großbritannien das erste Land mit einem gesetzlich geregelten Urheberrecht, welches Künstlern individuelle Rechte einräumte, um gegen unzulässige Kopien ihrer Werke vorzugehen. Darin wurde auch erstmalig das Recht gewährt, finanziell von Werken zu profitieren und über deren Integrität zu bestimmen.

Derzeit ist das Urheberrecht im *Copyright, Designs and Patents Act 1988* geregelt. Teil I und II des Gesetzes enthalten Regelungen zum Urheber- und Leistungsschutzrecht. Teil I unterteilt sich in 10 Kapitel und regelt im ersten Kapitel die Entstehung des Urheberrechts, die Urheberschaft und die Schutzdauer. Das Urheberrecht entsteht nach britischem Recht automatisch mit der Schöpfung des Werkes.⁴²⁰ Bei Filmen und Tonaufnahmen ist Urheber, wer die Vorbereitungen für die Erstellung des Werkes getroffen hat, in der Regel also der Filmproduzent.⁴²¹ Das zweite Kapitel normiert die Rechte des Urhebers, darunter das Recht auf Vervielfältigung, Veröffentlichung und Aufführung des Werkes.

Kapitel 3 regelt die Schranken des Urheberrechts, also Handlungen, die ohne Zustimmung des Urhebers zulässig sind. Dazu zählen vorübergehende Vervielfältigungen, Vervielfältigungen zu Unterrichts- und Recherchezwecken oder das Kopieren in Bibliotheken. Die Schrankenregelungen haben die europäischen Vorgaben zur Beschränkung des Urheberrechts für nicht-kommerzielle Nutzung der Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informati-

⁴²⁰ Durie, GRUR Int 1990, 832.

⁴²¹ Durie, GRUR Int 1990, 832.

ongesellschaft (Urheberrechtsrichtlinie) bislang nicht so weit umgesetzt, wie es die Richtlinie zuließe. So ist die Herstellung einer Kopie zu privaten Zwecken, anders als etwa in Deutschland, nach britischem Recht unzulässig.⁴²² Auch die zulässige Verwendung von Werken im Rahmen von Parodien oder sonstigen künstlerischen Nachahmungen existiert nicht.⁴²³ Damit sind Handlungen der alltäglichen Internetnutzung, wie Sicherungskopien oder Formatumwandlungen von geschützter Musik, von geschützten Filmen und ebooks, verboten.⁴²⁴

Kapitel 4 normiert die Urheberpersönlichkeitsrechte. Dazu zählen unter anderem das Recht auf Anerkennung der Urheberschaft und das Recht, einer Entstellung seines Werkes zu widersprechen. Kapitel 5 betrifft den Umgang mit urheberrechtlich geschützten Werken, also etwa der Übertragung und Lizenzierung von Rechten an einem Werk. Kapitel 6 enthält Ansprüche bei Rechtsverletzungen und Straftatbestände. Kapitel 7 – 10 normieren Verfahrens- und sonstige Vorschriften. Teil 2 regelt das Recht des ausübenden Künstlers in Bezug auf Aufführung und Herstellung von Tonaufnahmen, also eine Art Leistungsschutzrecht.

bb. Auskunftsanspruch

Schon vor seiner Befassung mit einem Warnhinweismodell kannte das britische Recht den Anspruch auf richterliche Anordnung zur Auskunftserteilung (*Norwich Pharmacal order*) im Zusammenhang mit Urheberrechtsverletzungen im Internet. Hier können Rechteinhaber zum Vorgehen gegen Urheberrechtsverletzungen im Internet eine Kooperation der Internetzugangsdiensteanbieter⁴²⁵ in Form der Auskunftserteilung verlangen.

Grundlage für den gerichtlichen Auskunftsanspruch gegenüber dem Diensteanbieter nach britischem Recht ist der Präzedenzfall *Norwich Pharmacal Co. & Others v. Customs and Excise Commissioners*⁴²⁶. Kläger war ein Pharmaunternehmen, welches ein exklusives Patentrecht an einem Medikament hielt. Zwischen 1960 und 1970 wurden unlizenzierte Nachahmungen des Produktes nach Großbritannien eingeschifft. Das Unternehmen konnte die Importeure nicht identifizieren, die entsprechenden Informationen waren aber beim beauftragten Schiffsunternehmen vorhanden, das sich jedoch zur Auskunft weder berechtigt noch verpflichtet sah. Das *House of Lords* befand, dass dann, wenn eine unbeteiligte dritte Partei

⁴²² Hargreaves, S. 68.

⁴²³ Hargreaves, S. 49.

⁴²⁴ Hargreaves, S. 44. Im Vereinigten Königreich handelt also nicht nur rechtswidrig, wer aus illegalen Filesharing-Netzwerken geschütztes Material herunterlädt, sondern auch, wer Musikdateien von einer gekauften CD auf seine Festplatte oder seinen MP3-Player überspielt.

⁴²⁵ Im Folgenden: "Diensteanbieter".

⁴²⁶ 1974] AC 133.

Informationen habe, die sich auf das rechtswidrige Verhalten eines anderen beziehen, eine Auskunftserteilung zur Unterstützung des Betroffenen gerichtlich angeordnet werden kann.⁴²⁷ Der Betroffene muss substantiiert vortragen, dass die Rechtsverletzung stattgefunden hat, dass die Auskunft des Dritten zur Verfolgung seiner Ansprüche notwendig ist, dass der Dritte nicht nur Zeuge, sondern an der Rechtsverletzung in irgendeiner Form beteiligt und in Besitz der Information ist, sowie dass die gerichtliche Anordnung zur Auskunftserteilung im konkreten Fall angebracht ist.

Die Einführung des Warnhinweissystems erfordert im Vereinigten Königreich also insofern keine Modifikation des geltenden Rechts, als die hier im Fokus stehenden Handlungen als rechtswidrig eingestuft waren und ein Auskunftsanspruch zur Verfolgung von Urheberrechtsverletzungen im Internet Rechteinhabern auch nach früherer Rechtslage zustand.

b. Akzeptanz des Urheberrechts in der Bevölkerung

Die britische Bevölkerung ist mit der geschilderten Rechtslage nur unzureichend vertraut oder jedenfalls wird diese dort nicht hinreichend akzeptiert.⁴²⁸ 73 Prozent der Verbraucher sind sich nicht darüber im Klaren, was zulässigerweise kopiert oder aus dem Rundfunk aufgenommen werden darf.⁴²⁹ 44 Prozent der Verbraucher halten Filesharing in P2P-Netzwerken sogar für legal.⁴³⁰ Allerdings lassen sich die Nutzer auch in offensichtlichen Fällen⁴³¹ nicht von illegaler Nutzung abschrecken.⁴³² Diese Umstände waren Anlass, ein Warnhinweismodell mit präventiven und repressiven Elementen⁴³³ zu erwägen.

⁴²⁷ *Norwich Pharmacal Co & Others v Customs and Excise Commissioners* [1974] AC 133.

⁴²⁸ *Hargreaves*, S. 68.

⁴²⁹ *Consumer Focus*, Outdated copyright law confuses consumers, 24.2.2010, abrufbar unter: <http://www.consumerfocus.org.uk/news/outdated-copyright-law-confuses-consumers>, zuletzt aufgerufen am 19.8.2011.

⁴³⁰ *Harris Interactive/BPI*, Digital Music Survey, 2010.

⁴³¹ Im Fall von "The Pirate Bay" etwa weisen die Betreiber mit Piratenschiff und Totenkopf auf der Startseite auf die Illegalität des Angebots hin.

⁴³² *Hargreaves*, S.68. Der im Jahr 2003 errichtete Dienst zählt heute 5 Mio. Nutzer, obwohl seine Gründer im Jahr 2009 zu Gefängnisstrafen verurteilt wurden.

⁴³³ Zu diesem Ansatz aktuell *EuGH*, *Scarlet Extended C 70/10*, v. 24.11.2011; Zif. 31 unter Verweis auf, *L'Oréal u. a.*, vom 12. Juli 2011, C-324/09, Slg. 2011, I-0000, Zif. 131.

2. Stand der Gesetzgebung

a. Historischer Kontext des Warnhinweisverfahrens

aa. Digital Britain

Grundlage für den Erlass der konkreten gesetzlichen Regelungen zur Warnhinweisversendung war die Durchführung eines Pilotversuchs zur Warnhinweisversendung und eine im Anschluss daran ausgesprochene Empfehlung in dem Bericht „*Digital Britain*“.⁴³⁴

Im Juli 2008 verpflichteten sich britische Diensteanbieter in Zusammenarbeit mit der British Recorded Industry (BPI) in einem von der Regierung unterstützten Pilotversuch für drei Monate, auf freiwilliger Basis Warnhinweise zu versenden.⁴³⁵ Das Pilotprojekt ergab, dass etwa **55 Prozent der Nutzer** ihr rechtswidriges Verhalten aufgrund des Erhalts eines Warnhinweises aufgeben würden.⁴³⁶ Im Juni 2009 legten das *Department for Business, Innovation and Skills* (BIS) und das *Department for Culture, Media and Sports* (dcms) den Bericht „*Digital Britain*“ vor. Unter Berücksichtigung der Ergebnisse des Pilotversuchs wurde die Einführung eines Warnhinweismodells empfohlen. Es sollte ein Gesetzesrahmen geschaffen werden, der das **Vereinigte Königreich** zu einem der **führenden Standorte für die Kreativwirtschaft weltweit** macht.⁴³⁷ Die effektive Bekämpfung von Urheberrechtsverletzungen im Internet wird als wichtiger Schritt zur Erreichung dieses Zieles angesehen.

Dies soll über zwei Stufen erreicht werden: Zunächst soll mit Hilfe von Warnhinweisen **Aufklärungsarbeit** hinsichtlich des legalen Zugangs zu kreativen Inhalten geleistet und Rechtsklarheit durch den Gesetzgeber geschaffen werden. Erst auf einer zweiten Stufe sind – falls sich der präventive Ansatz nicht bewährt – effektive **Sanktionen** bei rechtswidrigem Verhalten vorzusehen.

Der Bericht geht dabei davon aus, dass, wer illegal nutzt, auch zu legaler Nutzung bereit ist.⁴³⁸ Daher sollen neue Geschäftsmodelle geschaffen und ausgebaut werden,⁴³⁹ die erschwinglichen und benutzerfreundlichen Zugang zu kreativen Inhalten im Netz bieten

⁴³⁴ *BIS/dcms*, *Digital Britain*, S. 105ff.

⁴³⁵ Vgl. *High Administrative Court*, [2011] EWHC 1021 (Admin).

⁴³⁶ *BIS, dcms, Intellectual Property Office*, *Impact Assessment*, S. 68.

⁴³⁷ *BIS/dcms*, *Digital Britain*, S. 105, Par. 1.

⁴³⁸ *BIS/dcms*, *Digital Britain*, S. 110, Par. 19.

⁴³⁹ Im Vereinigten Königreich sind bereits eine Anzahl führender neuer digitaler Geschäftsmodelle zur Nutzung kreativer Inhalte verfügbar, darunter Hulu, Spotify, Six-To-One und FremantleMedia.

und für das Netz gefördert werden.⁴⁴⁰ Neben staatlichen Aufklärungs- und Sanktionsmaßnahmen sieht der Bericht hier die **Kreativwirtschaft** essentiell in der **Pflicht**.⁴⁴¹

bb. Der Digital Economy Act 2010

Die im Anschluss daran geschaffene gesetzliche Grundlage für die Einführung des Warnhinweismodells im Vereinigten Königreich ist das Gesetz über die digitale Wirtschaft, der **Digital Economy Act 2010 (DEA)** vom 08. April 2010.⁴⁴² Der Gesetzgeber verspricht sich von dem neuen Modell zum einen repressiv Rechtsverstöße im Internet zu bekämpfen und zum anderen präventiv Aufklärung über die Verbote zu erreichen und dadurch den Nutzer zu legalen Angeboten zu führen.⁴⁴³

Der DEA⁴⁴⁴ ändert insbesondere den *Communications Act* (2003). Gegenstand der Neuregelung in **Sections 3-18 DEA** ist die Bekämpfung von Urheberrechtsverletzungen im Internet durch Versendung von Warnhinweisen und gegebenenfalls durch anschließende Sanktionen. Die Regelungen des Gesetzes lassen sich wie folgt zusammenfassen.

- Sec. 3-8 (Art. 124 A – F DEA) regelt die Versendung von Warnhinweisen an Anschlussinhaber und das damit verbundene Verfahren.
- Sec. 9 – 12 (Art. 124 G – J DEA) regelt die bei Ineffizienz des reinen Warnhinweisystems vorgesehene Verhängung von Sanktionen in Form von technischen Maßnahmen, die von den Zugangsanbietern durchzuführen sind (Section 10-12).
- Sec. 13 – 15 (Art. 124 K – M DEA) betreffen Rechtsbehelfe des Anschlussinhabers, die Durchsetzung der Verpflichtungen und die Aufteilung der bei der Warnhinweisversendung anfallenden Kosten.
- Sec. 16 (Art. 124 N) enthält Begriffsbestimmungen.
- Sec. 17 DEA ist eine Verordnungsermächtigung für den *Secretary of State* zu gerichtlichen Sperrverfügungen für Internetseiten mit urheberrechtsverletzenden Inhalten und Sec. 18 DEA enthält Vorschriften für das parlamentarische Verfahren.

b. Status Quo

Da das Warnhinweismodell im Vereinigten Königreich noch nicht umgesetzt ist, liegen keine Erkenntnisse über dessen Effizienz vor. Als nächster Schritt steht die Verabschiedung

⁴⁴⁰ *BIS/dcms*, Digital Britain, S. 109, unter Berufung auf *Adermon/Liang*.

⁴⁴¹ *BIS/dcms*, Digital Britain, S. 110, Par. 22f.

⁴⁴² Der DEA wurde am 08. April 2010 erlassen und ist teilweise am selben Tag und teilweise am 08. Juni 2010 in Kraft getreten.

⁴⁴³ *Dcms*, Next Steps for implementation of the Digital Economy Act, August 2011, S.7. Er liegt insoweit auf einer Linie mit der aktuellen Rechtsprechung des Europäischen Gerichtshofs *EuGH*, *Scarlet Extended C 70/10*, v. 24.11.2011; Zif. 31 unter Verweis auf, *L'Oréal u. a.*, vom 12. Juli 2011, C-324/09, Slg. 2011, I-0000, Zif. 131

⁴⁴⁴ Im Folgenden ist mit „DEA“ oder „Regelungen des DEA“ nicht das gesamte Gesetz gemeint, sondern nur die Sec. 3-18 zur Bekämpfung von Urheberrechtsverletzungen im Internet.

eines *Initial Obligations Code* durch die OFCOM an,⁴⁴⁵ nachdem bereits seit Ende Mai 2010 ein Entwurf (*Draft*) des *Initial Obligations Code* vorliegt.⁴⁴⁶ Nachdem zwei der betroffenen Telekommunikationsunternehmen BT (British Telecommunications plc.) und TalkTalk (TalkTalk Telecom) die gerichtliche Überprüfung des DEA und der Vorschläge des *Draft Initial Obligations Code* vor dem *High Administrative Court*⁴⁴⁷ angestrengt hatten, setzte die OFCOM den Erlass eines endgültigen *Initial Obligations Code* bis zum Abschluss des gerichtlichen Verfahrens aus. Ursprünglich war nach dem Urteil vom April 2011, dass die Nichtzulassung der Berufung⁴⁴⁸ vorsah, geplant, zügig mit der Umsetzung fortzufahren, sodass die ersten Warnhinweise voraussichtlich gegen Ende 2012 hätten versandt werden sollen.⁴⁴⁹ Nach einer zwischenzeitlichen Zurückweisung im Juni 2011⁴⁵⁰ gab der *Court of Appeal* jedoch der Nichtzulassungsbeschwerde der Kläger im Oktober 2011 statt.⁴⁵¹ Es ist zu erwarten, dass die OFCOM vor Erlass eines endgültigen *Initial Obligations Code* die Erschöpfung des Rechtsweges abwartet, sodass eine zeitnahe Aufnahme der Warnhinweisversendung im Vereinigten Königreich derzeit nicht nahe liegt.

3. Das britische Modell

Implementierung und Regelungsansatz des DEA sind mehrstufig. Das Inkrafttreten der Regeln zu Warnhinweisen auf der ersten Stufe setzt zum einen das Inkrafttreten der Änderungsvorschriften des DEA voraus und zum anderen das Inkrafttreten von behördlichen Ausführungsvorschriften zu den grundlegenden Verpflichtungen der Diensteanbieter („**Initial Obligations Code**“). Der Einsatz von technischen Sanktionen auf der zweiten Stufe verlangt ein weiteres regulatorisches Tätigwerden, nämlich den Erlass von weiteren Ausführungsvorschriften zu technischen Maßnahmen („**Technical Obligations Code**“), zu denen Diensteanbieter verpflichtet werden.

a. Erfasste Erscheinungsformen von Internetpiraterie

Das britische Modell setzt derzeit allein bei illegaler P2P-Nutzung an.⁴⁵² Dem Gesetzgeber im Vereinigten Königreich ist bewusst, dass damit nur ein Ausschnitt illegaler Nutzung erfasst wird.⁴⁵³ Über die Hälfte unlizenzierter Inhalte im Vereinigten Königreich stammt aus anderen illegalen Quellen, wie illegalen MP3-Seiten, MP3-Suchmaschinen und Linksamm-

⁴⁴⁵ *Dcms*, Next Steps for implementation of the Digital Economy Act, August 2011, S. 8.

⁴⁴⁶ <http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf>.

⁴⁴⁷ *High Administrative Court*, [2011] EWHC 1021 (Admin).

⁴⁴⁸ Siehe dazu unten, S. 135.

⁴⁴⁹ *Dcms*, Next Steps for implementation of the Digital Economy Act, August 2011, S. 8.

⁴⁵⁰ *Court of Appeal* C1/2011/1437.

⁴⁵¹ *Court of Appeal* [2011] EWCA Civ 1229.

⁴⁵² *Dcms*, Next Steps for implementation of the Digital Economy Act, August 2011, S. 7.

⁴⁵³ Schätzungen der Rechteinhaber zufolge gibt es im Vereinigten Königreich wenigstens 6,5 Mio. rechtswidrig agierende File-Sharer; vgl. BIS, *dcms*, Intellectual Property Office: Impact Assessment, S. 67.

lungen, die zu Sharehoster-Diensten führen.⁴⁵⁴ Diese sollen ebenfalls bekämpft werden, sind aber derzeit nicht Gegenstand der Warnhinweisversendung. Diese Erscheinungen nahm der DEA zunächst dadurch in Bezug, dass er die Möglichkeit vorbehielt, eine Sperrung derartiger Webseiten zu einem späteren Zeitpunkt vorzunehmen,⁴⁵⁵ die dann eine gerichtliche Verfügung voraussetzt. Nach Kritik an den entsprechenden Vorschriften in Sec. 17 und 18 DEA gab die Regierung der OFCOM im Februar 2011 auf, die Praktikabilität der Regelungen des DEA zu überprüfen.⁴⁵⁶ Die OFCOM kam zu dem Ergebnis, dass keine effektive Wirkung zu erwarten sei, da der Erlass einer **gerichtlichen Verfügung zu zeitintensiv** sei, so dass von der Umsetzung dieser Vorschriften Abstand genommen wurde.⁴⁵⁷ Stattdessen soll entsprechend der **Intellectual Property Crime Strategy**⁴⁵⁸ direkt gegen Webseiten mit überwiegend urheberrechtswidrigem Material vorgegangen werden und es sollen Strategien zur Verteilung der internationalen Verantwortung entwickelt werden. Gemeinsam mit Industrie und Rechtsverfolgungsorganen wird nach Mitteln gesucht, mit deren Hilfe Geldzuflüsse an urheberrechtsverletzende Webseiten bzw. an deren Betreiber gestoppt werden können. So soll Werbung auf solchen Seiten untersagt werden und Geldinstitute zur Unterlassung von Transaktionen für derartige Webseiten verpflichtet werden. In Zusammenarbeit mit Suchmaschinenbetreibern soll sichergestellt werden, dass rechtswidrige Quellen nicht vor legalen Angeboten aufgefunden werden können. Zulässige Geschäftsmodelle sollen aber durch solche Maßnahmen nicht unterbunden und der faire Wettbewerb nicht gestört werden.⁴⁵⁹

b. Ausgestaltung des Schutzsystems nach dem DEA

Der Aufbau des Gesetzes und dessen vorgesehene Wirkung gestalten sich wie folgt.

aa. Regelungsziel (Schutzzweck)

Das britische Modell verfolgt das Ziel, die Zahl der Urheberrechtsverletzungen im Internet zu senken, um ökonomische Schäden zu verhindern oder zumindest zu reduzieren. Dazu soll dem im britischen Recht verankerten Auskunftsanspruch als Instrument der direkten Rechtsverfolgung ein Mittel zur Bewusstseins-schaffung und Aufklärung vorangestellt werden, das schonend, schnell, wirksam und kostengünstig ist.

⁴⁵⁴ *Dcms*, Next Steps for implementation of the Digital Economy Act, August 2011, S. 7, unter Berufung auf Harris Interactive.

⁴⁵⁵ *Digital Economy Act 2010*, Section 17 and 18.

⁴⁵⁶ Vgl. http://www.culture.gov.uk/news/media_releases/7756.aspx.

⁴⁵⁷ *Dcms*, Next Steps for implementation of the Digital Economy Act, August 2011, S. 7.

⁴⁵⁸ HM Government (August 2011) *Prevention and cure: The UK IP Crime Strategy 2011*.

⁴⁵⁹ *Dcms*, Next Steps for implementation of the Digital Economy Act, August 2011, S. 7.

bb. Systematische Verortung der Warnhinweis-Regelung

Die Grundsätze zum Erlass von Warnhinweisen und Sanktionen regelt der DEA als gesetzliche Grundlage. Er enthält entsprechende Ermächtigungen und macht inhaltliche **Vorgaben** für zwei Regelwerke zur Festlegung von Details der Durchführung in den Ausführungsvorschriften des **Initial Obligations Code** und des **Technical Obligations Code**.

1) *Initial Obligations Code*

Der *Initial Obligations Code* betrifft Details der Warnhinweisversendung. Er sollte nach dem ursprünglichen Plan von den betroffenen Wirtschaftsbranchen ausgehandelt und anschließend durch die OFCOM anerkannt werden.⁴⁶⁰ Da es nicht zu einer Vereinbarung kam, hat die OFCOM den *Initial Obligations Code* zu erlassen.⁴⁶¹ Am 28. Mai 2010 hat sie einen **Entwurf** mit dem Titel "*Online Infringement of Copyright and the Digital Economy Act 2010 - Draft of Code of Practice to include processes to be followed, rights and obligations of rights owners, ISPs and subscribers*"⁴⁶² vorgelegt.

Nach dem DEA hat der *Initial Obligations Code* folgende Aspekte zu regeln:⁴⁶³

- Meldung von Urheberrechtsverstößen
- Versendung der Warnhinweise an die Anschlussinhaber
- Festlegung einer Mindestgrenze für die Einordnung als sog. „relevanter Anschlussinhaber“
- Speicherung und Dauer der Speicherung von Daten der Anschlussinhaber
- Kostenregelung im Hinblick auf Verwaltungs-, Durchführungs- und Widerspruchsverfahren und Rechtsbehelfsverfahren.

2) *Technical Obligations Code*

Der *Technical Obligations Code* soll die Anordnung technischer Sanktionen nach Verletzungshandlungen regeln. Ob er überhaupt vorgelegt wird, hängt davon ab, ob sich ein Warnhinweismodell ohne Zugangssperren bereits als effizient genug erweist, um das Regelungsziel des DEA zu erreichen. Nach einer mindestens zwölfmonatigen Erfahrung mit dem *Initial Obligations Code* ist der *Technical Obligations Code* auf Anordnung des *Secretary of State*⁴⁶⁴ durch die OFCOM zu erarbeiten, falls entsprechende Voruntersuchungen der Behörde zu dem Ergebnis führen, dass ein reines Warnhinweismodell ineffizient ist.⁴⁶⁵ Im Rahmen der Voruntersuchung soll nach Anhörung von Rechteinhabern, Diensteanbietern und Anschlussinhabern die Erforderlichkeit beleuchtet werden. Die Untersuchungen sollen auch Aufschluss über die zu erwartende Effizienz von Sanktionen im Hinblick auf die jewei-

⁴⁶⁰ *Digital Economy Act 2010*, Section 5 (*Communications Act 2003*, 124C).

⁴⁶¹ *Digital Economy Act 2010*, Section 6 (*Communications Act 2003*, 124D).

⁴⁶² <http://stakeholders.ofcom.org.uk/consultations/copyright-infringement/>.

⁴⁶³ *Digital Economy Act 2010*, Section 7 (*Communications Act 2003*, 124E).

⁴⁶⁴ *Digital Economy Act 2010*, Section 10 (*Communications Act 2003*, 124H), subsection 1.

⁴⁶⁵ *Digital Economy Act 2010*, Section 10 (*Communications Act 2003*, 124H), subsection 2.

lige Art des Internetanschlusses geben⁴⁶⁶ und alle Technologien in den Blick nehmen, die aktuell zur Rechtsverletzung im Internet genutzt werden.⁴⁶⁷

cc. Die Rolle der OFCOM

Das *Office of Communications* (OFCOM) ist die britische Medienaufsichtsbehörde. Sie wurde 2002 durch den *Office of Communications Act* gegründet, um den gattungsübergreifenden Problemen im Medienbereich gerecht zu werden. Die Behörde hat eine ökonomische Gesamtausrichtung und ihre Hauptaufgaben liegen in der Erteilung von Lizenzen, in der Medienforschung und in der Erarbeitung von Regularien. Neben der Medienregulierung dient die OFCOM dem Verbraucherschutz und der Wettbewerbsförderung.

Die **Durchführung** der Maßnahmen des DEA, die Rechte und Pflichten von Rechteinhabern, Diensteanbietern und Anschlussinhabern zu normieren, überträgt der DEA der **OFCOM** und dem *Secretary of State*, als ein Kabinettsmitglied im Ministerrang.

1) *Erlass des Initial Obligations Code*

Weil sich Rechteinhaber und Provider nicht auf ein Warnhinweismodell einigen konnten, obliegt der OFCOM die Erarbeitung des *Initial Obligations Code* zur Regelung der Details zur Ausführung des Warnhinweismodells.⁴⁶⁸ Zunächst wurde dazu im Zuge der Erstellung eines vorläufigen Entwurfs ein Fragenkatalog erarbeitet und Ende Mai 2010 ein Entwurf vorgelegt.⁴⁶⁹

2) *Erlass des Technical Obligations Code*

Nachdem die OFCOM Voruntersuchungen zu der Notwendigkeit der Verhängung von technischen Maßnahmen angestellt hat, muss sie entscheiden, ob auf Basis dieser Untersuchungen zusätzliche technische Sanktionen erforderlich sind. Der *Secretary of State*⁴⁷⁰ kann auf dieser Basis den Erlass des *Technical Obligations Code* durch die OFCOM anordnen.

3) *Überwachung*

Sobald das Warnhinweismodell verankert ist, treffen die OFCOM Überwachungsaufgaben sowie die Überprüfung des Systems auf seine Effizienz. Die Behörde hat nach **Art. 124 F DEA** im Abstand von zwölf Monaten **Fortschrittsberichte** zum Ausmaß von Urheber-

⁴⁶⁶ *Digital Economy Act 2010*, Section 9 (*Communications Act 2003*, 124G), subsection 5(b).

⁴⁶⁷ *Digital Economy Act*, Explanatory Notes, Par.61.

⁴⁶⁸ Diese Regelungen sind sodann vom Parlament anzuerkennen, bevor sie der EU-Kommission zu notifizieren sind. Die Mitteilungspflicht gegenüber der EU-Kommission ergibt sich aus Art. 8 Abs. 1 der Richtlinie 98/34/EG über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften (Notifizierungsrichtlinie). Danach müssen Mitgliedstaaten jeden Entwurf über „technische Vorschriften“ der Kommission vorlegen.

⁴⁶⁹ <http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf>.

⁴⁷⁰ *Digital Economy Act 2010*, Section 11 (*Communications Act 2003*, 124I).

rechtsverletzungen im Internet zu erstellen und zu veröffentlichen,⁴⁷¹ wobei alle drei Monate **Zwischenberichte** zu erfolgen haben.⁴⁷² Sofern dies datenschutzrechtlich geboten ist, kann von einer vollständigen Veröffentlichung abgesehen werden. Die Jahresberichte müssen zur Anzahl der Urheberrechtsverletzungen im Internet und zu den durch Rechteinhaber getroffenen Maßnahmen zur Förderung legaler Alternativangebote Stellung nehmen. Sie müssen sich zudem mit Nachweisen über die Aufklärungsarbeit und Maßnahmen mit Blick auf die Wahrung von Werten in der digitalen Welt befassen und Angaben zur Wirksamkeit der vorgenannten Maßnahmen sowie Hinweise zur Zahl der gemeldeten Rechtsverstöße enthalten. Zudem müssen sie die Anzahl eingeleiteter Verfahren infolge eines gemeldeten Rechtsverstoßes und die Menge der Verfahren gegen Anschlussinhaber erfassen, zu denen in beachtlichem Umfang Rechtsverstöße gemeldet wurden.⁴⁷³ Der *Secretary of State* kann auf die Anordnung von Zwischenberichten verzichten, wenn er diese für entbehrlich hält.⁴⁷⁴

dd. Anwendungsbereich des DEA

1) Vorgabe des DEA

Der DEA berechtigt und verpflichtet Rechteinhaber, Diensteanbieter und Anschlussinhaber. Grundsätzlich sind also auch alle Zugangsanbieter vom Anwendungsbereich erfasst.

2) Umsetzung durch den Entwurf des *Initial Obligations Code*

In der Gesetzesbegründung war erwogen worden, dass Diensteanbieter, die nur ein sehr geringes Aufkommen von Urheberrechtsverletzungen in ihrem Netzwerk zu verzeichnen haben, vom Anwendungsbereich des DEA ausgenommen werden können und sie aus Gründen der Verhältnismäßigkeit⁴⁷⁵ im *Initial Obligations Code* von der Verpflichtung zur Versendung von Warnhinweisen zu befreien.⁴⁷⁶ Auf diese Weise würden kleinere und mittlere Festnetz- sowie mobile Netzwerkanbieter unter dieser Grenze bleiben.⁴⁷⁷ Wenn die Befreiung an die Unterschreitung der Grenze gebunden sei, bestehe für kleinere Diensteanbieter ein Anreiz, Urheberrechtsverletzungen im gesteckten Rahmen zu halten, insbesondere, wenn eine Befreiung nach einem einmaligem Überschreiten der Grenze nicht wieder aufleben könne.⁴⁷⁸ Der OFCOM-Entwurf des *Initial Obligations Code* greift die-

⁴⁷¹ *Digital Economy Act*, Explanatory Notes, Par. 60.

⁴⁷² *Digital Economy Act 2010*, Section 8 (*Communications Act 2003*, 124F), subsection 3.

⁴⁷³ *Digital Economy Act 2010*, Section 8 (*Communications Act 2003*, 124F), subsection 5.

⁴⁷⁴ *Digital Economy Act 2010*, Section 8 (*Communications Act 2003*, 124F), subsection 4.

⁴⁷⁵ *Digital Economy Act*, Explanatory Notes, Par. 51.

⁴⁷⁶ *Digital Economy Act*, Explanatory Notes, Par. 51., vorgeschlagen wird eine Befreiung von Providern mit weniger als 400.000 Anschlussinhabern, S. 12, Par. 3.14.

⁴⁷⁷ *Digital Economy Act*, Explanatory Notes, Par. 51.

⁴⁷⁸ *Digital Economy Act*, Explanatory Notes, Par. 51.

se Idee auf und schlägt eine Grenze von 400.000 Anschlussinhabern⁴⁷⁹ und einen Ausschluss von Mobilfunkanbietern vor.⁴⁸⁰

3) Gerichtliche Überprüfung

Im Verfahren vor dem *High Administrative Court* hatten die Kläger die Ausnahmeregelung als Diskriminierung gemäß Art. 6 der *Richtlinie 2002/20/EG* über die Genehmigung elektronischer Kommunikationsnetze und -dienste (Genehmigungsrichtlinie) begriffen.⁴⁸¹ Eine Ungleichbehandlung wurde darin gesehen, dass die Ausnahmeregelung einen Anreiz biete, zu einem ausgenommenen Diensteanbieter zu wechseln. Das Gericht wies dies zum Entscheidungszeitpunkt als spekulativ zurück und bestätigte die von der OFCOM vorgeschlagene Grenze von **400.000 Anschlussinhabern**.⁴⁸² Da die sechs Provider, die mehr als 400.000 Anschlussinhaber haben, gemeinsam einen Marktanteil von 93,4 Prozent auf dem Breitbandmarkt für häusliche und mittelständische Anschlüsse auf sich vereinten, bestünde eine natürliche Grenze.⁴⁸³ Da der Kleinste der Großanbieter bereits doppelt so groß sei, wie der nächstgrößte Marktteilnehmer, könne der Gesetzgeber Prioritäten setzen und kleine Diensteanbieter erst aufgrund einer einzelfallbezogenen Betrachtung nach vermehrten Rechtsverstößen hinzuzuziehen.⁴⁸⁴ Im Falle **mobiler Netzwerkanbieter** sei die Ausnahme gerechtfertigt, weil sich deren Anschlüsse wegen der Geschwindigkeits- und Kapazitätseinschränkungen und der im Verhältnis zum Festnetz erhöhten Preise entscheidend weniger für Rechtsverletzungen eigneten. Der illegale Datenverkehr über mobile Netzwerk-Anbieter liege unter 5 Prozent, so dass die Anordnung von Warnhinweisen hier per se unverhältnismäßig sei.⁴⁸⁵ Um hier bei Bedarf nachzubessern, ist die OFCOM dazu verpflichtet, die Entwicklung von Urheberrechtsverletzungen im Internet zu überwachen, sodass die Qualifikationskriterien für Netzbetreiber im *Initial Obligations Code* der Entwicklung in zukünftigen Warnhinweis-Versendungszeiträumen angepasst werden können. Dabei soll nicht auf Fest- oder Mobilnetz abgestellt werden, sondern auf die Anzahl der Rechtsverletzungen.⁴⁸⁶

ee. Regelungsinhalt des neuen Schutzsystems

1) Prävention vor Sanktion

Das zweistufige britische Modell lässt sich wie folgt zusammenfassend beschreiben.

⁴⁷⁹ *Draft Initial Obligation Code*, 3.14 ff.

⁴⁸⁰ *Draft Initial Obligation Code*, 3.11 ff.

⁴⁸¹ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 201.

⁴⁸² *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 201.

⁴⁸³ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 201.

⁴⁸⁴ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 201.

⁴⁸⁵ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 202.

⁴⁸⁶ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 202.

Es beginnt mit der Feststellung eines Urheberrechtsverstoßes durch den Rechteinhaber, den dieser einem Diensteanbieter meldet. Auf jede Meldung erfolgt die Versendung eines Warnhinweises an den betreffenden Anschlussinhaber durch den Diensteanbieter, über den dieser Buch zu führen hat (Art. 124 A DEA). Werden Urheberrechtsverstöße über den Internetzugang des Anschlussinhabers fortgesetzt und überschreitet dieser dabei die festgesetzte Mindestgrenze, so legt der Diensteanbieter eine anonymisierte Liste der gemeldeten Rechtsverstöße über ihn an.

Erweist sich dieses reine Warnhinweismodell als effizient genug, um zu einem markanten Rückgang der Onlinepiraterie zu führen, so kann es in dieser Weise fortgeführt werden. Anderenfalls müssen Sanktionen geprüft werden. Sofern sich nämlich innerhalb eines Jahres nach Aufnahme der Warnhinweisversendung dessen hinreichende Effizienz nicht nachweisen lässt, können die OFCOM und der *Secretary of State* zusätzliche Sanktionen in Form der Verhängung von technischen Maßnahmen, wie die Drosselung oder vorübergehende Sperrung des Internetzugangs, erwägen (Art. 124 G DEA).

2) Aufklärung durch Versendung von Warnhinweisen (Art. 124 A – 124 F DEA)

a) Ermittlung des Rechtsverstoßes nach DEA

Die Versendung eines Warnhinweises an einen Anschlussinhaber setzt tatbestandlich die Feststellung eines selbst begangenen oder einem Dritten ermöglichten Rechtsverstoßes über den Dienst eines Diensteanbieters voraus.⁴⁸⁷ Dazu muss der Rechteinhaber unlizenzierte Quellen im Internet identifizieren, die sein Material öffentlich zugänglich machen.⁴⁸⁸ In der Praxis wird durch Download des Materials im P2P-Netzwerk die IP-Adresse des verletzenden Anschlussinhabers ermittelt.⁴⁸⁹ Sodann wird der Urheberrechtsverstoß durch den Rechteinhaber an den betroffenen Diensteanbieter gemeldet.⁴⁹⁰ Die Meldung hat innerhalb eines Monats nach Feststellung der IP-Adresse zu erfolgen.⁴⁹¹ Dabei müssen die Rechtsverletzung durch die Benennung des illegal verfügbar gemachten Inhalts und die Berechtigung des Rechteinhabers hieran sowie der Zeitpunkt des vorgeworfenen Urheberrechtsverstoßes benannt werden.⁴⁹²

⁴⁸⁷ *Digital Economy Act 2010*, Section 3 (*Communications Act 2003*, 124A), subsection 1.

⁴⁸⁸ *Digital Economy Act*, Explanatory Notes, Par. 41.

⁴⁸⁹ *Digital Economy Act*, Explanatory Notes, Par. 41.

⁴⁹⁰ *Digital Economy Act 2010*, Section 3 (*Communications Act 2003*, 124A), subsection 2.

⁴⁹¹ *Digital Economy Act 2010*, Section 3 (*Communications Act 2003*, 124A), subsection 3(d).

⁴⁹² *Digital Economy Act 2010*, Section 3 (*Communications Act 2003*, 124A), subsection 3.

b) *Der Warnhinweis*

aa) *DEA*

Auf Basis dieser Meldung trifft den Diensteanbieter die Pflicht zur Versendung eines Warnhinweises.⁴⁹³ Hierfür kommen nach dem DEA E-Mail oder Brief in Betracht. Die Versendung muss gerechnet vom Tag der Meldung innerhalb eines Monats erfolgen.⁴⁹⁴ Der **Warnhinweis** muss nach Art. 124 A Subsec. 6 DEA folgenden **Inhalt** haben:

- „(a) einen Vermerk, dass die Benachrichtigung gemäß diesem Abschnitt und infolge eines gemeldeten Verstoßes gegen das Urheberrecht erfolgt;
- (b) den Namen des Rechteinhabers, der den Verstoß gemeldet hat;
- (c) eine Beschreibung des offenkundigen Verstoßes;
- (d) einen Beweis für den Verstoß, aus dem die IP-Adresse des Anschlussinhabers hervorgeht sowie Informationen dazu, wann genau der betreffende Beweis gesichert wurde;
- (e) Informationen über das Widerspruchsrecht des Nutzers und die Gründe aus denen ein solcher Widerspruch erhoben werden kann;
- (f) Informationen über das Urheberrecht und seinen Sinn und Zweck;
- (g) Informationen über Möglichkeiten des legalen Zugriffs auf urheberrechtlich geschützte Werke⁴⁹⁵ bzw. einen Hinweis, wo entsprechende Informationen erhältlich sind;
- (h) Informationen über die Möglichkeiten des Anschlussinhabers, seinen Internetzugang vor unberechtigtem Zugriff zu schützen, bzw. einen Hinweis, wo entsprechende Informationen erhältlich sind; und
- (i) alle anderen Angaben, die laut Initial Obligations Code in der Benachrichtigung enthalten sein müssen.“

Der **Initial Obligations Code** kann zu weiteren Hinweisen verpflichten,⁴⁹⁶ zu denen gemäß Art. 124 A Subsec. 8 DEA insbesondere folgende Punkte gehören:

- „(a) der Vermerk, dass der Anbieter des Internetdienstes Informationen über die vorliegende Urheberrechtsverletzung speichern kann;

⁴⁹³ *Digital Economy Act 2010, Section 3 (Communications Act 2003, 124A), subsection 4.*

⁴⁹⁴ *Digital Economy Act 2010, Section 3 (Communications Act 2003, 124A), subsection 5.*

⁴⁹⁵ Die Hinweise variieren je nachdem, ob der Anschluss privat, geschäftlich oder in sonstiger Weise (z.B. Hotel, Internetcafé) genutzt wird. *Digital Economy Act, Explanatory Notes, Par. 42.*

⁴⁹⁶ *Digital Economy Act 2010, Section 3 (Communications Act 2003, 124A), subsection 8.*

- (b) der Vermerk, dass der Rechteinhaber den Anbieter des Internetdienstes dazu auffordern kann offenzulegen, welche der von ihm gemeldeten Urheberrechtsverletzungen von dem Anschlussinhaber begangen wurden;
- (c) der Vermerk, dass der Rechteinhaber nach Offenlegung dieser Informationen die Identität des Anschlussinhabers mithilfe einer gerichtlichen Verfügung ermitteln und eine Klage wegen Verletzung des Urheberrechts gegen den Nutzer anstrengen kann; und
- (d) der Vermerk, dass, falls die Verpflichtung zur Versendung der Benachrichtigung daraus resultiert, dass zuvor bereits ein anderer Verstoß nach Punkt (4) gemeldet wurde, die Anzahl der vom Anschlussinhaber begangenen Urheberrechtsverletzungen herangezogen werden kann für eine Entscheidung über die Anwendung technischer Maßnahmen.“

*bb) OFCOM-Entwurf des Initial Obligations Code*⁴⁹⁷

- **Dreistufiger Verwarnungsprozess**

Der von der OFCOM vorgelegte **Entwurf des Initial Obligations Code** greift dies auf. Von besonderem Interesse ist der dreistufige Verwarnungsprozess („**three-stage notification process**“). Es wird eine Versendung der Meldung durch den meldeberechtigten Rechteinhaber innerhalb von zehn Werktagen vorgeschlagen.⁴⁹⁸ Der weitere Prozess soll wie folgt ablaufen:⁴⁹⁹

- Der **erste Warnhinweis** erfolgt nach der ersten Verstoßmeldung.⁵⁰⁰
- Der **zweite Warnhinweis** erfolgt bei wiederholter Meldung innerhalb eines Monats nach dem ersten Warnhinweis unter Verweis auf die erste Warnung.
- Der **dritte Warnhinweis** erfolgt, wenn innerhalb eines Monats nach dem zweiten Warnhinweis ein weiterer Verstoß gemeldet wird. Er enthält Informationen darüber, warum es zur Warnhinweisversendung kam und verweist auf die vorangegangenen Verwarnungen. Mit dem dritten Warnhinweis soll die Aufnahme in die **Verstoßliste** erfolgen.⁵⁰¹

Im **Anhang 6** des OFCOM-Entwurfs⁵⁰² sind jeweils Mustervorschläge für die Hinweise auf den unterschiedlichen Stufen abgedruckt, welche im Tonfall von

⁴⁹⁷<http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf>.

⁴⁹⁸ 4.8 des Entwurfs des *Initial Obligations Code*.

⁴⁹⁹ 5.11 des Entwurfs des *Initial Obligations Code*.

⁵⁰⁰ Zur Verstoßmeldung („*Copyright Infringement Reports – CIR*“) siehe Section 4 des Entwurfs des *Initial Obligations Code*.

⁵⁰¹ Siehe dazu unten, S. 124.

⁵⁰²<http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf>.

der reinen Aufklärung,⁵⁰³ über die ernstzunehmende Warnung.⁵⁰⁴ bis hin zu der Aufnahme in die Verstoßliste.⁵⁰⁵ schärfer werden.

- **Maßnahmen zur Verifikation der gemeldeten Rechtsverstöße**

Darüber hinaus schlägt der Entwurf der OFCOM einen gegenüber der Behörde zu erbringenden „*Quality Assurance report*“ vor, der Angaben zur Verifizierung der durch die Rechteinhaber festgestellten Verstöße enthält. Dadurch soll gewährleistet werden, dass für die behauptete Urheberrechtsverletzung ein robuster und akkurater Nachweis erbracht wird. Jeder Rechteinhaber, der sich am Verfahren beteiligen will, muss diesen Anforderungen entsprechen („*Qualifying Copyright Owner*“).⁵⁰⁶

- c) *Liste der gemeldeten Urheberrechtsverstöße als Grundlage des Auskunftsanspruchs (Verstoßliste)*

- aa) *Hintergrund der Verstoßliste*

Rechteinhaber haben nach geltendem Recht keine praktikable Möglichkeit, in Erfahrung zu bringen, ob ein Anschlussinhaber regelmäßig Urheberrechte verletzt. Aufgrund hoher Rechtsverfolgungskosten wurden Rechtsverstöße in der Vergangenheit insgesamt zurückhaltend gerichtlich geltend gemacht.⁵⁰⁷

- bb) *Verstoßliste nach DEA*

Um eine effektive Rechtsdurchsetzung zu ermöglichen, müssen Diensteanbieter künftig gem. **Art. 124 B DEA** über die Anzahl der gemeldeten Rechtsverstöße Nachweis führen.⁵⁰⁸ Für auffällige Anschlussinhaber muss der Diensteanbieter bei Überschreiten einer im Initial Obligation Code festzulegenden Mindestgrenze⁵⁰⁹ eine aus Datenschutzgründen anonymisierte Liste über gemeldete Urheberrechtsverstöße anlegen.⁵¹⁰ Diese ist **Grundlage** für das **Auskunftsverlangen** über die Identität des Anschlussinhabers, dem nur aufgrund vorheriger richterlicher Anordnung entsprochen werden darf.⁵¹¹ Hintergrund dieser Regelung ist, dass eine Meldung sich nur auf singuläre Rechtsverstöße bezieht und Einzelfälle nicht von Urheberrechtsverletzungen im großen Stil unterschieden werden können.⁵¹² Berücksichtigt werden die Zahl der gemeldeten Rechtsverstöße und die Zeitspanne von Ver-

⁵⁰³<http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf>, S. 65 f.

⁵⁰⁴<http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf>, S. 67.

⁵⁰⁵<http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf>, S. 68 f.

⁵⁰⁶ Section 4. 4 und 4.5 des Entwurfs des *Initial Obligations Code*.

⁵⁰⁷ *Digital Economy Act*, Explanatory Notes, Par. 45.

⁵⁰⁸ *Digital Economy Act*, Explanatory Notes, Par. 44.

⁵⁰⁹ *Digital Economy Act 2010*, Section 4 (*Communications Act 2003*, 124B), subsection 3.

⁵¹⁰ *Digital Economy Act*, Explanatory Notes, Par. 44ff.

⁵¹¹ *Norwich Pharmacal Co. & Others v Customs and Excise Commissioners [1974] AC 133*.

⁵¹² *Digital Economy Act*, Explanatory Notes, Par. 45.

stößen und Meldungen.⁵¹³ Der Liste muss zu entnehmen sein, welche der gemeldeten Rechtsverstöße sich auf den betroffenen Anschlussinhaber beziehen, ohne dass dieser zu identifizieren ist.⁵¹⁴ Um die Rechtsverfolgung zu ermöglichen, müssen die Provider den Rechteinhabern die Liste auf Verlangen zur Verfügung stellen.⁵¹⁵ Mehr als zwölf Monate zurückliegende Meldungen finden keine Berücksichtigung.⁵¹⁶ Näheres soll der Initial Obligations Code regeln.⁵¹⁷ Hat der Rechteinhaber mit Hilfe dieser Liste im Wege einer *Norwich Pharmacal order* von dem Provider Auskunft über die Identität des Anschlussinhabers erhalten, so muss er den Anschlussinhaber letztmalig abmahnen und ihn unter Androhung rechtlicher Schritte zur Unterlassung auffordern.⁵¹⁸ Danach kann er gerichtliche Hilfe in Anspruch nehmen.⁵¹⁹

*cc) OFCOM-Entwurf des Initial Obligations Code*⁵²⁰

Der OFCOM-Entwurf regelt die Aufnahme in die Verstoßliste.⁵²¹ Während der Betroffene bereits mit der dritten Warnung in die Verstoßliste aufgenommen wird, soll die Liste bei einem erneuten **vierten Verstoß** ohne Anforderung und unmittelbar, aber anonymisiert, innerhalb von fünf Tagen an den Rechteinhaber geschickt werden. Anderenfalls hat dieser keine Möglichkeit, auf die auf der Liste geführten Personen aufmerksam zu werden. Der Rechteinhaber soll auch das Recht haben, Listen anzufordern, dies aber nicht öfter als alle drei Monate.

3) Sanktion - Technische Verpflichtungen (Art. 124 G – J DEA)

Sollte sich das vorstehend erläuterte System als ineffizient erweisen, sind durch den *Secretary of State* auf Basis der OFCOM-Berichte zusätzliche technische Maßnahmen als Sanktionen zu erwägen.⁵²² Das Erfordernis und die Voraussetzungen dieser Maßnahmen regelt der gemäß Art. 124 I DEA von der OFCOM unter Berücksichtigung der Vorgaben von Art. 124 J DEA zu erstellende⁵²³ **Technical Obligations Code**.⁵²⁴ Die Behörde muss dessen Erlass auf Basis der bis zu diesem Zeitpunkt erstellten Berichte befürworten, der Code darf aber nicht vor Ablauf von zwölf Monaten nach der Aufnahme der Warnhinweisversendung erlassen werden.

⁵¹³ *Digital Economy Act 2010*, Section 7 (*Communications Act 2003*, 124E), subsection 5.

⁵¹⁴ *Digital Economy Act 2010*, Section 4 (*Communications Act 2003*, 124B), subsection 2.

⁵¹⁵ *Digital Economy Act 2010*, Section 4 (*Communications Act 2003*, 124B), subsection 1(a).

⁵¹⁶ *Digital Economy Act 2010*, Section 7 (*Communications Act 2003*, 124E), subsection 6.

⁵¹⁷ *Digital Economy Act 2010*, Section 4 (*Communications Act 2003*, 124B), subsection 1(b).

⁵¹⁸ *Digital Economy Act*, Explanatory Notes, Par. 37.

⁵¹⁹ *Digital Economy Act*, Explanatory Notes, Par. 37.

⁵²⁰ <http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf>.

⁵²¹ Siehe Section des *OFCOM-Entwurfs des Initial Obligations Code*.

⁵²² *Digital Economy Act*, Explanatory Notes, Par. 60.

⁵²³ *Digital Economy Act 2010*, Section 11 (*Communications Act 2003*, 124I).

⁵²⁴ Er wird auf Basis einer Anordnung des *Secretary of State* erlassen, wenn die Voraussetzungen dafür vorliegen. Siehe *Digital Economy Act 2010*, Section 10 (*Communications Act 2003*, 124H), subsection 1.

Als technische **Sanktionsmaßnahmen** können nach Art. 124 G Subsec. 3 DEA in Betracht gezogen werden:

- „(a) Herabsetzung der Übertragungsgeschwindigkeit oder anderer Leistungen, die dem Anschlussinhaber zur Verfügung gestellt werden;
- (b) Verweigerung oder Beschränkung der Nutzung des Dienstes für den Zugriff auf bestimmte Inhalte;
- (c) Aussetzung der Dienstleistung für den Anschlussinhaber; oder
- (d) sonstige Beschränkungen der Nutzung des Dienstes.“

Die genannten technischen Sanktionsmaßnahmen sollen zur Reduzierung oder Verhinderung von Urheberrechtsverstößen beitragen, die durch auffällige Anschlussinhaber⁵²⁵ begangen wurden. Ihre Umsetzung wird den Diensteanbietern auferlegt.⁵²⁶

4) Rechtsschutzverfahren

Der DEA gewährt dem Anschlussinhaber im Hinblick auf seine Maßnahmen verschiedene Rechtsschutzmöglichkeiten. Gegen die Maßnahmen im Rahmen der Warnhinweisversendung ist Widerspruch statthaft, gegen technische Sanktionen kann nach erfolglosem Widerspruch weitere Beschwerde bei Gericht eingelegt werden.

a) Widerspruchsrecht gegen Maßnahmen im Rahmen der Warnhinweisversendung (Art. 124 K DEA)

Einzelheiten zu dem Widerspruchsverfahren des Anschlussinhabers gegen Maßnahmen im Rahmen der Warnhinweisversendung sind nach Vorgaben des DEA im *Initial Obligations Code*⁵²⁷ zu regeln. Das Widerspruchsrecht⁵²⁸ des Anschlussinhabers muss vor einer unabhängigen Widerspruchsstelle⁵²⁹ gegen folgende Maßnahmen geltend gemacht werden können:

- die Meldung eines Rechtsverstoßes,⁵³⁰
- die Versendung eines Warnhinweises,⁵³¹
- die Aufnahme oder die Androhung der Aufnahme in die Liste der gemeldeten Urheberrechtsverstöße⁵³² oder
- gegen andere nach dem Initial Obligation Code vorgesehene Handlungen.⁵³³

⁵²⁵ *Digital Economy Act*, Explanatory Notes, Par. 65.

⁵²⁶ *Digital Economy Act 2010*, Section 9 (*Communications Act 2003*, 124G), subsection 2. Einzelheiten in Art. 124 H DEA.

⁵²⁷ Der OFCOM-Entwurf zum *Digital Obligations Code* nimmt in Section 7, S. 28 f. im Wesentlichen auf die entsprechenden Regeln des DEA Bezug.

⁵²⁸ *Digital Economy Act 2010*, Section 13 (*Communications Act 2003*, 124k), subsection 2(a).

⁵²⁹ *Digital Economy Act 2010*, Section 13 (*Communications Act 2003*, 124k), subsection 2(b)(c).

⁵³⁰ *Digital Economy Act 2010*, Section 16 (*Communications Act 2003*, 124N), subsection 1(a)(i).

⁵³¹ *Digital Economy Act 2010*, Section 16 (*Communications Act 2003*, 124N), subsection 1(a)(ii).

⁵³² *Digital Economy Act 2010*, Section 16 (*Communications Act 2003*, 124N), subsection 1(a)(iii).

Das DEA nennt folgende, nicht abschließende Beispiele:

- die irrtümliche Einordnung eines Verhaltens als Rechtsverstoß,⁵³⁴
- die falsche Zuordnung einer IP-Adresse im Zeitpunkt des mutmaßlichen Rechtsverstoßes,⁵³⁵
- ein Verstoß von Rechteinhabern oder Diensteanbietern gegen den Code.⁵³⁶

Der Anschlussinhabers kann sich entlasten, wenn er darlegen kann, den Rechtsverstoß nicht selbst begangen und angemessene Maßnahmen getroffen zu haben, um Rechtsverstöße durch Dritte über den Dienst seines Diensteanbieter zu verhindern.⁵³⁷ Die **Beweislast** tragen Diensteanbieter bzw. Rechteinhaber, je nachdem wer die Maßnahme vorgenommen hat, gegen die sich der Widerspruch richtet.⁵³⁸ Entstehen dem Anschlussinhaber infolge fehlerhafter Ermittlungen Nachteile,⁵³⁹ treffen Rechteinhaber bzw. Diensteanbieter Entschädigungspflichten.⁵⁴⁰ Bei erfolgreichem Widerspruch hat der Anschlussinhaber grundsätzlich⁵⁴¹ einen Anspruch auf Erstattung der Verfahrenskosten gegen Rechteinhaber und Diensteanbieter.⁵⁴²

b) Rechtsschutz gegen technische Sanktionen (Art. 124 K DEA)

Die Rechtsbehelfe gegen technische Sanktionen sind gegebenenfalls im *Technical Obligation Code* zu regeln. Sie können sich gegen die Androhung einer technischen Maßnahme⁵⁴³ oder andere Handlungen im Zusammenhang mit den technischen Verpflichtungen oder dem *Technical Obligation Code* richten.⁵⁴⁴

aa) Widerspruchsverfahren

Sofern der *Technical Obligations Code* erlassen werden sollte, sind dort Regelungen über die Befugnisse der Widerspruchsstelle im Falle des Widerspruchs gegen technische Maßnahmen oder gegen deren Androhung zu regeln. Dies betrifft gem. Art. 124 K DEA

- die Bestätigung einer technischen Maßnahme;⁵⁴⁵
- die Untersagung oder den Abbruch der Durchführung einer technischen Maßnahme;⁵⁴⁶

⁵³³ *Digital Economy Act 2010*, Section 16 (*Communications Act 2003*, 124N), subsection 1(a)(iv).

⁵³⁴ *Digital Economy Act 2010*, Section 13 (*Communications Act 2003*, 124k), subsection 3(a).

⁵³⁵ *Digital Economy Act 2010*, Section 13 (*Communications Act 2003*, 124k), subsection 3(b).

⁵³⁶ *Digital Economy Act 2010*, Section 13 (*Communications Act 2003*, 124k), subsection 4.

⁵³⁷ *Digital Economy Act 2010*, Section 13 (*Communications Act 2003*, 124k), subsection 6(a)(b).

⁵³⁸ *Digital Economy Act 2010*, Section 13 (*Communications Act 2003*, 124k), subsection 5(b).

⁵³⁹ *Digital Economy Act 2010*, Section 13 (*Communications Act 2003*, 124k), subsection 7(a).

⁵⁴⁰ *Digital Economy Act 2010*, Section 13 (*Communications Act 2003*, 124k), subsection 7(b).

⁵⁴¹ *Digital Economy Act 2010*, Section 13 (*Communications Act 2003*, 124k), subsection 8.

⁵⁴² *Digital Economy Act 2010*, Section 13 (*Communications Act 2003*, 124k), subsection 7(c).

⁵⁴³ *Digital Economy Act 2010*, Section 16 (*Communications Act 2003*, 124N), subsection 1(b)(i).

⁵⁴⁴ *Digital Economy Act 2010*, Section 16 (*Communications Act 2003*, 124N), subsection 1(b)(ii).

⁵⁴⁵ *Digital Economy Act 2010*, Section 13 (*Communications Act 2003*, 124k), subsection 9(a)(i).

⁵⁴⁶ *Digital Economy Act 2010*, Section 13 (*Communications Act 2003*, 124k), subsection 9(a)(ii).

- die Ersetzung einer technischen Maßnahme durch eine geeignete Alternativmaßnahme.⁵⁴⁷

Im Hinblick auf die Verhängung technischer Sanktionen muss die Widerspruchsstelle dieselben Befugnisse wie die OFCOM haben,⁵⁴⁸ auf die die Entscheidung über den Widerspruch übertragen werden kann.⁵⁴⁹

bb) Anfechtung von Maßnahmen vor dem First-tier Tribunal (Art. 124 K DEA)

Gegen den Widerspruchsbescheid ist Beschwerde zum *First-tier Tribunal* (britisches Verwaltungsgericht) zulässig. Als Anfechtungsgründe können die sachliche oder rechtliche Fehlerhaftigkeit sowie die Unverhältnismäßigkeit der Anordnung der Maßnahme vorgetragen werden.⁵⁵⁰ Technische Maßnahmen gegen einen Anschlussinhaber dürfen – soweit kein Rechtsmittelverzicht vorliegt – erst nach Rechtskraft erfolgen.⁵⁵¹

c. Technische/organisatorische Umsetzung des Warnhinweismodells, hier Kostenverteilung

Die Aufteilung der Kosten für die Versendung von Warnhinweisen regelt eine Kostenverordnung. Sie unterscheidet zwischen „Qualifizierungskosten“ (Verwaltungskosten), „relevanten Kosten“ (Durchführungskosten) und Kosten des Rechtsschutzverfahrens.

aa. Qualifizierungskosten

Die als Verwaltungskosten zu begreifenden Qualifizierungskosten entstehen bei der OFCOM und den Rechtsbehelfsstellen für die Einrichtung des Warnhinweisystems, einschließlich der Schaffung einer Widerspruchsstelle.

1) Ursprünglich 25 Prozent der Kosten bei Diensteanbieter

Nach einer ursprünglichen Kostenordnung zum DEA sollten die Diensteanbieter der OFCOM 25 Prozent dieser Kosten erstatten müssen.

2) Überprüfung durch den High Administrative Court

Diese Aufteilung wurde vom *High Administrative Court* als unzulässig angesehen.⁵⁵² Die Qualifizierungskosten seien typischerweise als Verwaltungskosten anzusehen und unterfielen dem Anwendungsbereich des Art. 12 Richtlinie 2002/20/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über die Genehmigung elektronischer Kommunikationsnetze und -dienste (Genehmigungsrichtlinie). Danach dürfen Kommunikationsnetzbetreibern keine Verwaltungsgebühren auferlegt werden, da es sich anderenfalls um

⁵⁴⁷ *Digital Economy Act 2010*, Section 13 (*Communications Act 2003*, 124k), subsection 9(a)(iii).

⁵⁴⁸ *Digital Economy Act 2010*, Section 13 (*Communications Act 2003*, 124k), subsection 9(c).

⁵⁴⁹ *Digital Economy Act 2010*, Section 13 (*Communications Act 2003*, 124k), subsection 9(d).

⁵⁵⁰ *Digital Economy Act 2010*, Section 13 (*Communications Act 2003*, 124k), subsection 10(a).

⁵⁵¹ *Digital Economy Act 2010*, Section 13 (*Communications Act 2003*, 124k), subsection 11.

⁵⁵² *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 262.

verschleierte Abgaben oder Steuern handele,⁵⁵³ was dem Sinn und Zweck von Art. 12 Genehmigungsrichtlinie zuwiderliefe.⁵⁵⁴ Die Norm verbiete nach der Rechtsprechung des EuGH Abgaben, Gebühren und Zwangszuschüsse.⁵⁵⁵

3) Korrektur durch den Gesetzgeber

Der Gesetzgeber überarbeitet derzeit die Kostenverordnung im Hinblick auf die Ausgestaltung der Qualifizierungskosten (Verwaltungskosten), die jedenfalls nicht den Diensteanbietern auferlegt werden dürfen.⁵⁵⁶

bb. Relevante Kosten

Relevante Kosten sind solche internen Betriebskosten, die einem fiktiven und wirtschaftlich handelnden Diensteanbieter nach der Berechnung durch die OFCOM in Erfüllung seiner Verpflichtungen nach dem DEA pro Warnhinweis konkret entstehen dürfen.⁵⁵⁷ Der ermittelte Betrag ist in Höhe von 75 Prozent von den Rechteinhabern zu tragen. Die verbleibenden 25 Prozent verbleiben beim Diensteanbieter. Eingerechnet werden

- die Kosten der Entgegennahme der Meldung eines Rechtsverstoßes,
- die Kosten der Zuordnung der IP-Adresse zu einem Anschlussinhaber,
- das Erstellen und Versenden des Warnhinweises,
- das Führen der Liste der Rechtsverstöße und
- die Bereitstellung der Liste für Rechteinhaber.

cc. Kosten des Rechtsschutzverfahrens

Die Widerspruchsstelle hat für jedes durch einen Anschlussinhaber angestrebte Widerspruchsverfahren eine Gebühr zu erheben. Auch diese ist in Höhe von 75 Prozent von den Rechteinhabern und in Höhe von 25 Prozent von den Diensteanbietern zu tragen.⁵⁵⁸ Der

⁵⁵³ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 197.

⁵⁵⁴ Art. 12 Genehmigungsrichtlinie zu Verwaltungsabgaben lautet wie folgt: „(1) Verwaltungsabgaben, die von Unternehmen verlangt werden, die aufgrund einer Allgemeingenehmigung einen Dienst oder ein Netz bereitstellen oder denen ein Nutzungsrecht gewährt wurde, a) dienen insgesamt lediglich zur Deckung der administrativen Kosten für die Verwaltung, Kontrolle und Durchsetzung von Allgemeingenehmigungen und Nutzungsrechten sowie der in Artikel 6 Absatz 2 genannten besonderen Verpflichtungen, die die Kosten für internationale Zusammenarbeit, Harmonisierung und Normung, Marktanalyse, Überwachung der Einhaltung und andere Marktkontrollmechanismen sowie für Regulierungstätigkeiten zur Ausarbeitung und Durchsetzung des abgeleiteten Rechts und von Verwaltungsbeschlüssen, beispielsweise von Beschlüssen über den Zugang und die Zusammenschaltung, einschließen können, und b) werden den einzelnen Unternehmen in einer objektiven, verhältnismäßigen und transparenten Weise auferlegt, bei der die zusätzlichen Verwaltungskosten und zugehörigen Aufwendungen auf ein Mindestmaß reduziert werden. (2) Erheben die nationalen Regulierungsbehörden Verwaltungsabgaben, so veröffentlichen sie einen jährlichen Überblick über ihre Verwaltungskosten und die insgesamt eingenommenen Abgaben. Entsprechend der Differenz der Gesamtsumme der Abgaben und der Verwaltungskosten werden entsprechende Berichtigungen vorgenommen.“ Anhang A enthält die Maximalliste der Bedingungen, die an eine Allgemeingenehmigung geknüpft werden können. Nr. 2 lautet : „Verwaltungsgebühren entsprechend Art. 12 der vorliegenden Richtlinie.“

⁵⁵⁵ *EuGH*, Urt. v. 21.2.2008 - C-296/06 (Telecom Italia).

⁵⁵⁶ *High Administrative Court*, [2011] EWHC 1021 (Admin), par.200.

⁵⁵⁷ *The Online Infringement of Copyright (initial Obligations) (Sharing of Costs) Order 2011*, sec. 1(1).

⁵⁵⁸ *The Online Infringement of Copyright (Initial Obligations) (Sharing of Costs) Order 2011*, sec. 5.

Anschlussinhaber hat an die Widerspruchsstelle eine Gebühr in Höhe von £20 für jede Widerspruchsanzeige zu entrichten. Die Widerspruchsstelle muss dem Anschlussinhaber die Gebühr erstatten, wenn sie den Widerspruch des Anschlussinhabers vollumfänglich zu dessen Gunsten entscheidet.⁵⁵⁹

4. Überprüfung des DEA durch den High Administrative Court

Der DEA und die Vorschläge zur Umsetzung im Entwurf des *Initial Obligations Code* waren im Vereinigten Königreich nicht unumstritten und wurden von zwei der betroffenen Telekommunikationsunternehmen, BT (British Telecommunications plc.) und TalkTalk (TalkTalk Telecom), vor dem *High Administrative Court*⁵⁶⁰ zur Überprüfung gestellt. Der *High Court*, mit Sitz ausschließlich in London, ist in seiner *Administrative Division* mit einem deutschen erstinstanzlichen Verwaltungsgericht vergleichbar. Während des Klageverfahrens wird die weitere Umsetzung durch die OFCOM ausgesetzt. Mit Urteil vom 20. April 2011 wies der *High Court* die Klage im Wesentlichen zurück und gab den klagenden Zugangsanbietern nur im Hinblick auf die Kostentragungspflicht⁵⁶¹ recht.

Hauptpunkte der Klage waren neben den bereits behandelten Punkten der rechtswidrigen Kostentragung⁵⁶² und der Problematik der Ausnahme kleiner Provider vom Anwendungsbereich des *Initial Obligations Code*⁵⁶³ die allgemeine **Verhältnismäßigkeit** der Regelungen des DEA, der **Datenschutz**⁵⁶⁴ und weitere Fragen der **Kostenverteilung**.⁵⁶⁵ Die Auswirkungen der Regelungen auf Verbraucher, Geschäftsanschlussinhaber und Inhaber öffentlicher Anschlüsse (*public intermediaries*) wurden ganz generell als unverhältnismäßig (*disproportionate*) angesehen.⁵⁶⁶ Der DEA verstieße gegen die Grundrechtecharta der Europäischen Union, nämlich Artt. 7 (Privatsphäre), 8 (Datenschutz), 11 (Meinungs- und Informationsfreiheit) und 52. Moniert wurde auch die Missachtung allgemeiner Rechtsgrundsätze des EU-Rechts sowie des Rechts auf freien Zugang zum Internet gemäß dem 4. Erwägungsgrund der Richtlinie 2009/140/EG.⁵⁶⁷ Auch wurden Kollisionen mit dem *Human Rights Act* von 1998, bei dem es sich der Sache nach im Wesentlichen um eine Umsetzung der EMRK in nationales britisches Recht handelt, sowie gegen Art. 8 und Art. 10 EMRK selbst geltend gemacht.⁵⁶⁸ Die Verhältnismäßigkeitsprüfung durch den *High Court* fiel besonders gründlich aus und greift eine Vielzahl von Bedenken auf, die generell gegen

⁵⁵⁹ *The Online Infringement of Copyright (Initial Obligations) (Sharing of Costs) Order 2011*, sec. 6.

⁵⁶⁰ *High Administrative Court*, [2011] EWHC 1021 (Admin).

⁵⁶¹ Hierzu ausführlich unten S. 135.

⁵⁶² Siehe dazu S. 128.

⁵⁶³ Siehe dazu oben S. 120.

⁵⁶⁴ Siehe dazu S. 297.

⁵⁶⁵ Siehe dazu oben S. 135.

⁵⁶⁶ Vgl. *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 203.

⁵⁶⁷ Vgl. *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 203.

⁵⁶⁸ Vgl. *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 203.

Warnhinweisemodelle vorgebracht werden, und ist aus diesem Grund im Rahmen dieser Untersuchung auszuwerten.

a. Verhältnismäßigkeit der Regelungen des DEA

Das Gericht hielt den im DEA vorgenommenen Interessenausgleich für nicht zu beanstanden.⁵⁶⁹ Die Regelungen hätten den entgegenstehenden Wirtschaftsinteressen von Providern und Rechteinhabern sowie den Rechten der Nutzer gerecht zu werden.⁵⁷⁰ Bei der rechtlichen Überprüfung nimmt der *High Court* Aspekte in Bezug, die sich wie folgt in die nach deutschem Recht geläufigen Kategorien der Eignung, Erforderlichkeit und Angemessenheit einordnen lassen.

aa. Geeignetheit/legitimer Zweck

Der DEA eigne sich mit seinen regulatorischen, administrativen und gerichtlichen Durchsetzungsmaßnahmen zunächst generell zu einer Stärkung des Urheberrechtsschutzes.⁵⁷¹

Die Kläger sprachen der Regelung des DEA aber auch insofern konkret die Eignung zur Bekämpfung von Internetpiraterie ab, als BPI-Daten zeigen würden, dass nur 37 Prozent der Urheberrechtsverletzungen im Internet durch illegales P2P-Filesharing verursacht würden. Allein gegen diese Erscheinungsform richteten sich aber die konkreten Maßnahmen des DEA. Es sei deshalb insgesamt zur Bekämpfung der Internetpiraterie ungeeignet.

Für den *High Court* stellt dies die Verhältnismäßigkeit der Maßnahmen nicht in Frage. P2P-Filesharing sei mit einem Anteil von 37 Prozent für sich gesehen die meistgenutzte Technologie für Urheberrechtsverletzungen. Eine deutliche Reduzierung von illegalem P2P-Filesharing würde eine bemerkenswerte Verringerung des gesamten Ausmaßes von Urheberrechtsverletzungen herbeiführen.⁵⁷² Das Gericht verkennt nicht, dass es neben dem Filesharing andere technische Möglichkeiten gibt, Rechtsverletzungen im Internet zu begehen, ohne entdeckt zu werden. Indes basiere das Argument der Migration zu anderen Formen auf Spekulationen in Bezug auf menschliches Verhalten. Es habe Untersuchungen gegeben, Profile typischer Filesharer zu erstellen und die Gründe für das rechtswidrige Verhalten zu ermitteln, um Rückschlüsse auf die Reaktion auf das Regelungssystem des DEA zu ziehen. Maßnahmen, die alle Nutzer erreichen und auf legale Alternativen umschwenken lassen, seien nicht denkbar. Der Erfolg von Maßnahmen sei nicht bestimmbar, da menschliches Verhalten nicht akkurat vorherzusagen sei.⁵⁷³ Die Ergebnisse von Studien, die Ursachen, Verhaltensweisen, alternative Verhaltensweisen, Abschreckungswirkung und Unrechtsbewusstsein der Nutzer im Internet untersuchten, seien bestenfalls vieldeutig. Ins-

⁵⁶⁹ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 210.

⁵⁷⁰ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 213.

⁵⁷¹ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 221.

⁵⁷² *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 230.

⁵⁷³ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 232.

gesamt sei unklar, welche Auswirkungen unterschiedliche Arten von Strafverfolgung oder Androhung von Strafverfolgung oder andere Sanktionen wahrscheinlich haben würden.⁵⁷⁴

Dem DEA liege die Erwägung zugrunde, dass ein beträchtlicher Teil der Rechteverletzer zum gegenwärtigen Zeitpunkt nicht hinreichend aufgeklärt sei. Es fehle das Bewusstsein, dass ein Verhalten rechtliche und moralische Interessen anderer massiv beeinträchtige. Auch wenn das Verhalten des Einzelnen trivial und entschuldigbar erscheinen möge, dürfte der generelle Effekt zu einer erheblichen Schädigung der Kreativindustrie führen. Das Gericht spricht von *“tyranny of small decisions that have ruinous economic consequences”*.⁵⁷⁵ Ein zentrales Anliegen der Regelungen sei daher auf Aufklärung gerichtet: Durch die systematische Versendung von Warnhinweisen werde der Empfänger über die Rechtswidrigkeit seines Verhaltens und die möglichen Konsequenzen für andere informiert und dadurch veranlasst werden, sein Verhalten einzustellen oder sonst zu ändern. Diese Entscheidung sei auch dann möglich, wenn sie seinen unmittelbaren Eigeninteressen zuwiderlaufe. Die Annahme, dass Verbraucher nur zur Verfolgung ihrer eigenen wirtschaftlichen Interessen handelten und nicht rational auf moralische, altruistische oder nachhaltige Aspekte reagieren, sei überholt.

Zudem bestünden Risiken nachhaltiger Rechtsverletzungen. Selbst der selbstsüchtige, entschlossene Rechtsverletzer müsse Entdeckung fürchten und könne nicht sicher sein, ob technische Möglichkeiten bestehen oder entwickelt werden, die ihn überführten. Die Ungewissheit, durch neue Ermittlungsmöglichkeiten überführt zu werden, sei nicht zu vernachlässigen. Auch wenn es schwierig sei, den Effekt der Maßnahmen des DEA zu bestimmen, so gäbe es einige Anhaltspunkte dafür, von positiven Effekten auszugehen.⁵⁷⁶ Im Ergebnis sei nicht feststellbar, dass die Annahme des Parlaments, der DEA werde zu einer signifikanten Reduzierung von illegalem P2P-Filesharing führen, unzutreffend sei und Zweifel an der Eignung und Verhältnismäßigkeit der Regelungen aufwerfe.⁵⁷⁷

bb. Erforderlichkeit der angegriffenen Regelungen

Dem DEA wurde die mangelnde Erforderlichkeit nach einem Gesetz zum Urheberrechtsschutz im Internet entgegen gehalten. Es stünden mildere Handlungsalternativen zur Verfügung, um den Gesetzeszweck zu erreichen. Das Erfordernis einer Zusammenarbeit von Providern und Rechteinhabern wurde von Klägerseite gesehen. Da sich diese auf freiwilliger Basis erreichen lasse, bedürfe es keines Gesetzes.⁵⁷⁸

Der *High Court* begegnet dem insbesondere damit, dass das Warnsystem des DEA zunächst auf Aufklärung setze und erst nach Vorwarnung gerichtliche Schritte nach sich zie-

⁵⁷⁴ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 232.

⁵⁷⁵ „Herrschaft der kleinen Entscheidungen mit verheerenden wirtschaftlichen Auswirkungen.“ Siehe *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 233.

⁵⁷⁶ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 233.

⁵⁷⁷ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 234.

⁵⁷⁸ Vgl. *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 222.

he. Es sei also effektiv und milder als die vorherige Regelung. Das System bis zum Erlass des DEA sei zum einen für den Rechteinhaber beschwerlich gewesen, da mit der Geltendmachung eines Auskunftsanspruchs erhebliche rechtliche und tatsächliche Schwierigkeiten verbunden gewesen seien. Das Regelungssystem des DEA sei aber gerade im Sinne des Anschlussinhabers schonend, weil nur der wiederholte Rechtsverletzer nach einem abgestuften Vorgehen in eine Verstoßliste aufgenommen werde, die präzise das Ausmaß der ihm vorgeworfenen Rechtsverletzungen bestimme. Wenn sich der Rechteinhaber nach Erhalt der Liste zur Rechtsverfolgung entscheide, bedürfe es weiterhin der richterlichen Anordnung zur Auskunftserteilung über die Identität des Anschlussinhabers.⁵⁷⁹ Diesen träfe das gerichtliche Vorgehen aber nicht unvorbereitet. Dementsprechend schaffe der DEA ein im Vergleich zur gegenwärtigen Rechtslage effektiveres, zielgerichteteres und gerechteres System. Zudem sei die Regelung durch ihre vorgerichtliche Komponente kostenschonender für Verwaltung und Justiz.⁵⁸⁰ Im Hinblick auf die Effektivität richterlicher Anordnungen auf Auskunftserteilung stellten die Regelungen des DEA im Ergebnis zumindest ein gleich geeignetes Mittel dar.⁵⁸¹

cc. Angemessenheit der angegriffenen Regelungen

Im Zusammenhang mit der Angemessenheit wiesen die Kläger auf mehrere Punkte hin.

1) Abschreckungswirkung

Die Kläger stellten die Angemessenheit der Warnhinweisregelungen insofern in Abrede, als sie ihnen eine Abschreckungswirkung (*chilling effect*) auf Dritte, nicht rechtsverletzende Nutzer zusprachen.⁵⁸² Dieser Effekt werde möglicherweise in Fällen erzeugt, in denen der Anschlussinhaber zwar nicht der Rechtsverletzer ist, der Warnhinweis aber an ihn als Anschlussinhaber adressiert ist und eine Liste gemeldeter Rechtsverstöße über ihn geführt wird. Dies betreffe vor allem Wi-Fi Spot-Anbieter oder Eltern, deren Kinder einen Anschluss nutzen. Der DEA knüpft deren Exkulpation an das Treffen angemessener Vorkehrungen zur Verhinderung von Rechtsverstößen. Die Abschreckungswirkung durch den DEA – so die Kläger – könne dazu führen, dass überobligatorische Vorkehrungen hinsichtlich der Entlastung getroffen würden. Dies könne zu unnötigen Freiheitseinbußen Dritter führen, insbesondere deren Informationsfreiheit einschränken.⁵⁸³

Insofern weist das Gericht erneut darauf hin, dass sich derartige Auswirkungen auf menschliches Verhalten kaum vorhersagen lassen. Es sei aber unwahrscheinlich, dass negative Effekte der Abschreckungswirkung ein Ausmaß annähmen, das die Vorteile der Regelungen, namentlich den verbesserten Urheberrechtsschutz, derart übersteigen würde,

⁵⁷⁹ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 228.

⁵⁸⁰ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 228.

⁵⁸¹ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 229.

⁵⁸² *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 235.

⁵⁸³ Vgl. *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 235.

dass die Angemessenheit der Regelungen insgesamt in Frage gestellt würde. Für WiFi-Fälle seien im *Initial Obligations Code* angemessene Lösungen zu treffen.⁵⁸⁴

2) Direktes Vorgehen gegen Nutzer unverhältnismäßig?

Seitens der Kläger wurde unter Berufung auf die Enforcement-Richtlinie⁵⁸⁵ auf die Unverhältnismäßigkeit des DEA geschlossen. Ein unmittelbares Vorgehen gegen den nicht gewerbsmäßig handelnden Nutzer sei erst als letztes Mittel angemessen.⁵⁸⁶ Für den *High Court* ist das nicht schlüssig. Die gewählten Maßnahmen seien insbesondere wegen ihres zunächst aufklärenden Charakters angemessen.⁵⁸⁷

3) Gemeenschädlichkeit des Regelungsansatzes

Die Kläger monierten zudem, dass sich der DEA negativ auf das Gemeinwohl auswirke, weil die Bekämpfung von Filesharing die Bereitschaft zur kreativen Nutzung des Internet hemme.⁵⁸⁸ Das Gericht verwirft dies im Wesentlichen mit der Begründung, dass illegale Nutzung insgesamt nicht dem Schutz des Urheberrechts unterstehe.⁵⁸⁹ Zudem sei die hier vorgebrachte Betrachtung, dass das Urheberrecht nur der Sicherung ökonomischer Interessen diene, rechtlich nicht relevant,⁵⁹⁰ weil das anglo-amerikanische Urheberrecht auf das Urheberpersönlichkeitsrecht (*moral rights*) abstelle. Es gewähre etwa Schutzfristen, die ökonomisch möglicherweise nicht notwendig seien.

4) Unzutreffende Zahlen von Seiten der betroffenen Branchen?

Die Kläger verweisen schließlich darauf, dass der seitens der Musikindustrie bezifferte Verlust von 400 Mio. Pfund in Folge von illegalem P2P-Filesharing nicht nachweisbar sei. Für den *High Court* kommt es im Rahmen der Verhältnismäßigkeit der Regelungen nicht auf konkrete Verlustzahlen an. Genannte Zahlen seien nur Indizien dafür, dass P2P-Filesharing erheblichen Einfluss auf den Absatz von Musikinhalten nehme. Auch wenn vieles umstritten sei, spiele illegales Filesharing unstrittig eine negative Rolle, auch in Hinblick auf die Investition in Kultur.⁵⁹¹ Internetpiraterie sei aufgrund ihrer grundsätzlichen Illegalität zu bekämpfen.⁵⁹²

⁵⁸⁴ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 240.

⁵⁸⁵ 2004/48/EG vom 28. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums, OJ [2004] L No 157.

⁵⁸⁶ Vgl. *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 241.

⁵⁸⁷ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 241.

⁵⁸⁸ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 248.

⁵⁸⁹ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 249.

⁵⁹⁰ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 252.15.

⁵⁹¹ Siehe *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 252 mit einer Übersicht zu den relevanten Studien.

⁵⁹² *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 256.

5) Kostenverteilung

Auch die **Kostenaufteilung** war Gegenstand der gerichtlichen Überprüfung und führte nicht zu einer Beanstandung des DEA hinsichtlich der Verhältnismäßigkeit.⁵⁹³ Lediglich die Verpflichtung zur teilweisen Übernahme der sog. Qualifizierungskosten, einer Form von Verwaltungskosten, wurde als rechtswidrig angesehen.⁵⁹⁴

6) Zwischenergebnis

Insgesamt wies das Gericht den klägerischen Vortrag zur Unverhältnismäßigkeit also zurück⁵⁹⁵ und lehnte eine Vorlage zum EuGH ab.⁵⁹⁶

b. Berufung gegen die Entscheidung des High Court (Administrative Court)

Die Berufung zum **Court of Appeal** als Berufungsgericht ließ der *High Court* nicht zu. Hiergegen legten die Kläger Nichtzulassungsbeschwerde ein,⁵⁹⁷ der vom *Court of Appeal* nach einer zwischenzeitlichen Zurückweisung im Juni 2011⁵⁹⁸ im Oktober 2011 stattgegeben wurde.⁵⁹⁹ Das Gericht lässt die Berufung unter verschiedenen Gesichtspunkten zu. Zum einen hält das Berufungsgericht es für genügend aussichtsreich, im Berufungsverfahren davon überzeugt zu werden, dass einzelne Bestimmungen des DEA selbst rechtlich bindende Wirkung (als „technische Vorschriften“) entfalten, so dass sie nicht durchsetzbar sind, weil vor ihrem Erlass keine Notifizierung gegenüber der Europäischen Kommission stattgefunden hat.⁶⁰⁰ Zum anderen lässt das Gericht die Berufung im Hinblick auf die Vereinbarkeit einzelner Bestimmungen des DEA mit unterschiedlichen Europäischen Richtlinien zu. In Frage steht nach Ansicht des Berufungsgerichts, ob Vorschriften des DEA gegen Art. 3 und 12 der E-Commerce Richtlinie,^{601, 602} gegen die Datenschutz-Richtlinie⁶⁰³ und die

⁵⁹³ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 262.

⁵⁹⁴ Siehe dazu oben S. 128.

⁵⁹⁵ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 263.

⁵⁹⁶ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 264.

⁵⁹⁷ *Dcms*: „Next Steps for implementation of the Digital Economy Act“, August 2011, S. 5.

⁵⁹⁸ *Court of Appeal* C1/2011/1437.

⁵⁹⁹ *Court of Appeal* [2011] EWCA Civ 1229. Zum Hintergrund: Berufung gegen ein Urteil des *High Courts* kann entweder beim *High Court* selbst oder beim Berufungsgericht eingelegt werden (Rule 52.3(2) *Civil Procedure Rules* - CPR). Verweigert der *High Court* wie im vorliegenden Fall des Judicial Review des *Digital Economy Act* die Zulassung der Berufung, so kann die Zulassung erneut und zwar direkt beim Berufungsgericht beantragt werden (Rule 52(3) CPR). Dieser Zulassungsantrag wurde am 20. Juni 2011 von dem Richter am *Court of Appeal*, *Sir Richard Buxton*, zurückgewiesen. Da diese Entscheidung ohne mündliche Verhandlung ergangen war, konnten BT und TalkTalk gem. Rule 54.4 CPR die Überprüfung dieser Entscheidung in einer mündlichen Verhandlung beantragen, was zu der Entscheidung vom 7. Oktober 2011 geführt hat.

⁶⁰⁰ *Court of Appeal* [2011] EWCA Civ 1229, par. 1, 6 ff.

⁶⁰¹ Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr").

⁶⁰² *Court of Appeal* [2011] EWCA Civ 1229, par. 11ff.

⁶⁰³ Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

Datenschutz-Richtlinie für elektronische Kommunikation^{604, 605} sowie gegen die Genehmigungs-Richtlinie^{606, 607} verstoßen. Dagegen hat das Gericht der Beschwerde im Hinblick auf die Vereinbarkeit des DEA mit Art. 15 der E-Commerce Richtlinie nicht stattgegeben.⁶⁰⁸ Der *Court of Appeal* hat nun über das Rechtsmittel zu entscheiden. Die mündliche Verhandlung war für den 16. und 17. Januar 2012 angesetzt.

Im Anschluss an die Berufungsentscheidung stünde den Beteiligten die Möglichkeit offen, Revision beim **United Kingdom Supreme Court** einzulegen, der 2009 das *House of Lords* als letzte Instanz abgelöst hat. Die Revision zum *Supreme Court* ist nur bei Entscheidungen mit allgemeiner, grundlegender Bedeutung zulässig.

Ob der Implementierungsprozess des DEA während der gerichtlichen Überprüfung fortgesetzt wird, bleibt abzuwarten. Im britischen Recht ist dabei die Besonderheit zu beachten, dass Parlamentsgesetze einer Aufhebung durch die Gerichte nicht zugänglich sind. Das Vereinigte Königreich hat keine kodifizierte Verfassung und das Recht beruht in weiten Teilen auf ungeschriebenen Verfassungsgrundsätzen. Einer dieser Grundsätze ist die Souveränität des Parlaments.⁶⁰⁹ Bis auf die Bindung eines künftigen Parlaments hat das Parlament uneingeschränkte Befugnisse, und seine Gesetze können gerichtlich nicht aufgehoben werden. Rechtlich sind Gerichte daher grundsätzlich nicht in der Lage, den Vollzug eines Gesetzes auszusetzen.⁶¹⁰ Zu beachten ist in der britischen Rechtspraxis aber, dass eine *declaration of incompatibility* oder eine Feststellung der Unvereinbarkeit eines Gesetzes mit dem Europarecht durch ein nationales Gericht trotz der rechtlichen Unverbindlichkeit faktisch nicht unbeachtet bliebe. Auch wenn formal nicht die Möglichkeit besteht, ein Gesetz zu kassieren, werden die rechtlichen Bedenken eines Richters vom Parlament sehr ernst genommen. Der Richter genießt im Vereinigten Königreich eine wesentlich

⁶⁰⁴ Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (2002/58/EG).

⁶⁰⁵ *Court of Appeal* [2011] EWCA Civ 1229, par. 16 ff.

⁶⁰⁶ Richtlinie 2002/20/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über die Genehmigung elektronischer Kommunikationsnetze und -dienste (Genehmigungsrichtlinie).

⁶⁰⁷ *Court of Appeal* [2011] EWCA Civ 1229, par. 19.

⁶⁰⁸ *Court of Appeal* [2011] EWCA Civ 1229, par. 14.

⁶⁰⁹ Der britische Verfassungstheoretiker *Dicey* hat das Prinzip so zusammengefasst: "*Parliament [...] has, under the English constitution, the right to make or unmake any law whatever: and, further, that no person or body is recognised by the law of England as having a right to override or set aside the legislation of Parliament.*" (A.V. Dicey, Introduction to the Study of the Law of the Constitution (1885).

⁶¹⁰ Eine Ausnahme gilt für den 1998 durch das Parlament verabschiedeten *Human Rights Act* (HRA), der 2000 in Kraft getreten ist. Stellt ein Gericht fest, dass ein Gesetz gegen den HRA verstößt, kann es eine sog. *declaration of incompatibility* abgeben, d.h. eine Erklärung, dass das Gesetz gegen den HRA verstößt (Article 4 *Human Rights Act*). Diese Erklärung führt allerdings nicht dazu, dass das Gesetz aufgehoben wird, weil das gegen die Souveränität des Parlaments verstieße. Der Erklärung kommt lediglich deklaratorische Wirkung zu. In der Praxis befasst sich dann das Parlament bzw. eine Untersuchungskommission mit dem Gesetz. Insgesamt hat das Case Law der britischen Gerichte unter dem *Human Rights Act* ein Konzept zur „Beachtung“ und „Respektierung“ der Entscheidungen und Einschätzungen des Gesetzgebers entwickelt. Dazu *Beatson and Others, Human Rights: Judicial Protection in the Unites Kingdom*, par. 3.182, p.267.

hervorgehobenere und profiliertere Stellung als in Deutschland. Daher kommen informellen Mechanismen wie den so genannten *Committee inquiries* in der englischen Verfassungspraxis große Bedeutung zu. Wird eine Kollision mit Europarecht gesehen, legt das englische Gericht die Sache dem EuGH vor. *Lord Justice Lewison* hat in seinem Annahmebeschluss erkennen lassen, dass dieser Punkt zumindest nicht abwegig ist.⁶¹¹ Vor diesem Hintergrund darf man davon ausgehen, dass die Berufung gegen die gerichtliche Überprüfung des DEA dessen praktische Umsetzung zumindest etwas verzögern wird.

5. Impact Assessment zum Warnhinweismodell (Kosten-Nutzen-Analyse)

Mit dem DEA sollen durch Urheberrechtsverletzungen verursachte wirtschaftliche Schäden minimiert werden. Zugleich greift das Gesetz aber auch erheblich in das Gefüge der Verantwortlichkeiten ein und nimmt insbesondere Zugangsanbieter in die Pflicht. Um das Gesetzgebungsverfahren und die damit verbundenen Eingriffe in die jeweiligen Rechtspositionen abzusichern und zu legitimieren, wurde durch das *Department for Business, Innovation and Skills*, das *Department for Culture, Media and Sport* und das *Intellectual Property Office* eine Kosten-Nutzen-Analyse⁶¹² erstellt. Das sog. „**Impact Assessment**“⁶¹³ legt den ökonomischen Nutzen des neuen Modells dar.⁶¹⁴ Dabei handelt es sich um eine besondere Form der Gesetzesbegründung, die Kosten und Nutzen des Vorhabens in ein Verhältnis zueinander setzt. Konkret wurde unter Zugrundelegung der Preisbasis des Jahres 2008 über einen Zeitraum von zehn Jahren ein **Netto-Nutzen**⁶¹⁵ des Warnhinweismodells **von £1,2 Mrd.**⁶¹⁶ ermittelt. Unsicherheiten, die sich aus den nicht feststellbaren Langzeitauswirkungen von Urheberrechtsverletzungen im Internet als neuem Phänomen ergeben, wurden berücksichtigt.⁶¹⁷

Nach dem Ergebnis der Untersuchung entstünden der Kreativindustrie bei Nichteinführung des Warnhinweismodells Verluste in Höhe von jährlich £400 Mio. durch unterbliebene Verkäufe.⁶¹⁸ Grundlage für die Berechnung sind Werte, die durch die Musik-, Film- und

⁶¹¹Das Gerichtsverfahren in erster Instanz hat bewirkt, dass sich eine parlamentarische Untersuchungskommission mit dem Gesetz befasst. Am 8.11.2010 hat das *Culture, Media and Sport Committee* eine entsprechende Untersuchung angekündigt. Siehe <http://www.parliament.uk/business/committees/committees-a-z/commons-select/culture-media-and-sport-committee/news/committee-announces-new-inquiry/>.

⁶¹²Erstellt auf Grundlage des *Digital Entertainment Survey 2008* und *NERA Economic Consulting, The Costs and Benefits to ISPs of Proposed Measures to Curb Illegal File Sharing*, Dezember 2009.

⁶¹³Im Folgenden wird die Kosten- und Nutzenrechnung im Hinblick auf den ökonomischen Mehrwert eines Warnhinweismodells nachvollzogen. Die Ausführungen der Ministerialverwaltung sind hinsichtlich der Berechnung teilweise inkonsistent, was auf Rundungen zurückzuführen sein muss, deren Notwendigkeit und Motivation sich nicht näher erschließen. Im Rahmen der Studie werden die Zahlen nach Rundung zugrunde gelegt.

⁶¹⁴Bei der Berechnung wird immer die ungünstigste Variante zugrunde gelegt.

⁶¹⁵Der Netto-Nutzen ergibt sich nach Abzug der Kosten (dazu nachfolgend).

⁶¹⁶Die Reichweite des Netto-Nutzen liegt zwischen £1,2 Mrd. bis £1,4 Mrd., als „worst-case-scenario“ wird jedoch der niedrigere Wert zugrunde gelegt; *BIS, dcms, Intellectual Property Office: Impact Assessment*, S.55.

⁶¹⁷*BIS, dcms, Intellectual Property Office: Impact Assessment*, S. 67.

⁶¹⁸*BIS, dcms, Intellectual Property Office: Impact Assessment*, S. 64.

TV-Industrie und von den drei vorgenannten Behörden erhoben worden sind. Für die Software- und Videospiegelbranche wurde unterstellt, dass die Auswirkungen mit denen der anderen Branchen vergleichbar sind. Im Einzelnen wurden dabei £152 Mio. für die Film- und TV-Industrie,⁶¹⁹ £160 Mio. für die Musik-Industrie⁶²⁰ und £80 Mio. für die Software- und Videospiegel-Industrie⁶²¹ angesetzt. Insgesamt ergeben sich damit Verluste in Höhe von £392 Mio., die in der Ergebnisdarstellung des *Impact Assessment* auf £400 Mio. aufgerundet wurden.

a. Kosten

Die Untersuchung ermittelt zunächst die für das Modell anfallenden Kosten für Diensteanbieter, Rechteinhaber und die öffentliche Hand. Sie berechnen sich im Einzelnen wie folgt:

aa. Kosten der Internetzugangsdiensteanbieter

In der Berechnung wurden zunächst die Kosten, die den Diensteanbietern im Rahmen der Umsetzung und Durchführung des Modells entstünden, eingestellt. Hierzu zählen neben den Kosten für die Versendung der Warnhinweise auch Kapitalkosten⁶²² der Diensteanbieter sowie Kosten für die Einrichtung und den Betrieb eines Call-Centers sowie Kapital- und Betriebskosten der mobilen Netzanbieter. Insgesamt wurden hier im ersten Jahr einmalige Kosten in Höhe von **£35 Mio.** erwartet. Die jährlichen Durchschnittskosten sollen zwischen **£30 und £50 Mio.** betragen. Über einen Zeitraum von 10 Jahren sollen sich die abgezinsten Kosten der Diensteanbieter auf **£290 bis £500 Mio.**⁶²³ belaufen. Im Einzelnen stellen sie sich wie folgt dar:

1) *Kosten der Warnhinweisversendung*

Die Kosten der Warnhinweisversendung beim Diensteanbieter werden auf **£3-£10 pro Warnhinweis** beziffert. Dieser Wert wurde gemeinsam mit Diensteanbietern ermittelt⁶²⁴ und umfasst folgende Parameter:

- Identifizierung des Rechteinhabers
- postalische Versendung des Warnhinweises

⁶¹⁹ BIS, dcms, Intellectual Property Office: Impact Assessment, S.65, unter Berufung auf IPSOS, Digital & Physical Piracy in GB, November 2007, abrufbar unter:

http://www.ukfilmcouncil.org.uk/media/pdf/g/m/lpsos_Piracy_UK_2007.pdf.

⁶²⁰ BIS, dcms, Intellectual Property Office: Impact Assessment, S. 65, unter Berufung auf Jupiter Research (2007).

⁶²¹ BIS, dcms, Intellectual Property Office: Impact Assessment, S. 65. Der *Digital Entertainment Survey* (2008) kommt zu dem Ergebnis, dass Filesharing von Videospielen und Software niedriger ist als in den anderen Branchen.

⁶²² Kapitalkosten sind Kosten, die in einem Unternehmen durch Beschaffung von Fremdkapital und Eigenkapital entstehen, welches für Investitionen benötigt wird.

⁶²³ BIS, dcms, Intellectual Property Office: Impact Assessment, S. 70.

⁶²⁴ BIS, dcms, Intellectual Property Office: Impact Assessment, S. 70.

- Inhaltliche Erstellung des Warnbriefes
- Personalschulung und sonstiger Aufwand.

Rechteinhaber schätzen, dass etwa **6,5 Mio.** Menschen im Vereinigten Königreich als rechtswidrige File-Sharer aktiv sind.⁶²⁵ Damit entstünden den Diensteanbietern bei postalischer Versendung eines ersten Warnhinweises an jeden einzelnen dieser Nutzer bei Veranschlagung von mit £3-£10 je Nutzer, insgesamt Kosten zwischen **£20** (aufgerundet von £19,5) **bis £65 Mio.**⁶²⁶

70 Prozent dieser vorgenannten Nutzer würden nach eigenen Angaben **Rechtsverletzungen einstellen**, wenn sie infolge ihres Rechtsverstößes einen Brief oder Anruf ihres Diensteanbieters erhielten.⁶²⁷ Eine tatsächliche Reduzierung der Rechtsverstöße in dieser Größenordnung wird aber erst über einen Zeitraum von zwei Jahren erwartet.⁶²⁸ Bei den verbleibenden 30 Prozent der Nutzer,⁶²⁹ also 1.95 Mio. Personen, geht man davon aus, dass diese auch nach einer ersten Verwarnung ihr rechtswidriges Verhalten fortsetzen und damit weitere Kosten für eine zweite Warnhinweisversendung verursachen würden.⁶³⁰ Bei Kosten von £3-£10 pro Warnhinweis belaufen diese sich auf £6 Mio. (aufgerundet von £5.85 Mio) bis £20 Mio. (aufgerundet von £19.5 Mio.) pro Jahr.⁶³¹ Gerechnet auf einen Zeitraum von zehn Jahren lägen die **durchschnittlichen Jahreskosten** für die **Warnhinweisversendung** insgesamt in etwa im Bereich von **£7,5 bis £24,5 Mio.**⁶³² Diese Kosten treffen in erster Linie die fünf bzw. sechs marktführenden Internet-Zugangsanbieter⁶³³ des Vereinigten Königreichs. Die **einmaligen Kosten** der ersten Warnhinweisversendung (£20 bis £65 Mio.) würden sich danach pro **Diensteanbieter** auf durchschnittlich **£3 Mio.** (abgerundet von £3.3 Mio.) **bis £10 Mio.** (abgerundet von £ 10.83 Mio.) belaufen. Die danach für die weitere Warnhinweisversendung entstehenden **jährlichen Kosten von £6 bis £20 Mio.** lägen somit pro **Diensteanbieter** bei **£1 bis £3 Mio.** (letztere abgerundet von £3.3 Mio.).⁶³⁴

⁶²⁵ BIS, dcms, Intellectual Property Office: Impact Assessment, S. 56.

⁶²⁶ BIS, dcms, Intellectual Property Office: Impact Assessment, S. 71.

⁶²⁷ BIS, dcms, Intellectual Property Office: Impact Assessment, S. 70, unter Berufung auf den Digital Entertainment Survey 2008.

⁶²⁸ BIS, dcms, Intellectual Property Office: Impact Assessment, S. 70.

⁶²⁹ Digital Entertainment Survey 2008.

⁶³⁰ BIS, dcms, Intellectual Property Office: Impact Assessment, S. 71.

⁶³¹ Der Berechnung liegt zugrunde, dass ein Warnhinweis pro Jahr versandt wird. Unberücksichtigt bleibt, dass unter Umständen einzelne Rechteverletzer auch nach einem zweiten Warnhinweis ihr Verhalten nicht ändern und mehr als einen Warnhinweis pro Jahr erhalten.

⁶³² Werte abgezinst über den Zehnjahreszeitraum; BIS, dcms, Intellectual Property Office: Impact Assessment, S. 71.

⁶³³ Während im *Impact Assessment* zunächst von 6 größten ISPs die Rede ist (BT, Virgin, Talk Talk/AOL, Sky, Tiscali und Orange, vgl. BIS, dcms, Intellectual Property Office: Impact Assessment, S.62 Fn. 30), wird später im Text nur von den 5 größten Anbietern gesprochen (vgl. BIS, dcms, Intellectual Property Office: Impact Assessment, S. 71 ff.). Diese Abweichung beruht offenbar darauf, dass im Jahre 2009 ein Zusammenschluss zweier Anbieter stattgefunden hat.

⁶³⁴ BIS, dcms, Intellectual Property Office: Impact Assessment, S. 71.

2) Qualifizierungskosten

Darüber hinaus wurde die Belastung der **Diensteanbieter** mit den Qualifizierungskosten,⁶³⁵ die nach der ursprünglichen Kostenverteilung⁶³⁶ auf sie entfallen wären, auf insgesamt weitere **£6,9 bis £22,6 Mio. pro Jahr** geschätzt.⁶³⁷

3) Kosten für Kundenhotline

Nach Durchführung eines freiwilligen Selbstversuchs hat die OFCOM Daten zur Verfügung gestellt, die den Schluss zulassen, dass 1,5 Prozent der betroffenen Nutzer ihren Diensteanbieter für Nachfragen zu Warnhinweisen per E-Mail oder telefonisch kontaktieren werden.⁶³⁸ Zur Vermeidung von Mehrfachkosten läge ein gemeinsam betriebenes Call-Center der Diensteanbieter nahe.⁶³⁹ Schätzungen der Industrie gehen davon aus, dass einem ISP dabei für die Einstellung von Personal und dessen Schulung einmalige Kosten in Höhe von etwa **£20.000 bis £30.000** entstehen.⁶⁴⁰ Für ein Telefongespräch oder eine E-Mail zur Beantwortung der Frage wird eine zehnminütige Bearbeitungsdauer veranschlagt. Wenn 1,5 Prozent der von der ersten Warnhinweisversendung betroffenen 6,5 Mio. Nutzer, also 97.500 Personen jeweils eine zehnminütige Bearbeitungsdauer in Anspruch nähmen, beliefe sich die Gesamtbearbeitungszeit somit auf etwa 15.000 Stunden (abgerundet von 16.250 Stunden). Bei einem veranschlagten Stundensatz von £13 fielen anfängliche Kosten der Diensteanbieter für die Bearbeitung der Nachfragen bei einer Gesamtbearbeitungszeit von 15.000 Stunden von **£200.000** (aufgerundet von £195.000) an. Es wird aufgrund der erwarteten Reduzierung der Rechtsverletzungen um 70 Prozent nach Versendung der ersten Warnhinweise angenommen, dass sich die Bearbeitungsdauer auf etwa 5.000 Stunden⁶⁴¹ jährlich reduziert und diese Kosten bei dem Stundensatz von £13 in den Folgejahren auf £65.000 jährlich sinken.⁶⁴²

4) Kapitalkosten der Diensteanbieter

Die den Diensteanbietern obliegende Identifikation der Rechteverletzer soll in einem automatisierten Prozess erfolgen. Es wurden drei unterschiedliche Szenarien für die Ermittlung der Kapitalkosten der Diensteanbieter erwogen, bei denen die Buchführungskosten unberücksichtigt blieben.

⁶³⁵ Dazu oben S. 128.

⁶³⁶ Wie oben S. 128 dargelegt, wurde diese Kostenverteilung vom *High Administrative Court* für unzulässig erklärt. Zum Zeitpunkt der Erstellung des *Impact Assessment* war sie jedoch Grundlage für die Berechnung.

⁶³⁷ *BIS, dcms, Intellectual Property Office: Impact Assessment*, S. 71.

⁶³⁸ *BIS, dcms, Intellectual Property Office: Impact Assessment*, S. 72.

⁶³⁹ *BIS, dcms, Intellectual Property Office: Impact Assessment*, S. 72.

⁶⁴⁰ *BIS, dcms, Intellectual Property Office: Impact Assessment*, S. 72.

⁶⁴¹ Der Wert (aufgerundet von 4.875 Stunden) ergibt sich, wenn man davon ausgeht, dass von 6,5 Mio. Rechteverletzern 30 Prozent (1.95 Mio. Personen) die rechtswidrige Nutzung nach Erhalt des ersten Warnhinweises fortsetzen und von diesen sich wiederum 1,5 Prozent (29.250 Personen) an das Call-Center wenden, wobei eine Bearbeitungsdauer von jeweils zehn Minuten pro Anruf veranschlagt wurde.

⁶⁴² *BIS, dcms, Intellectual Property Office: Impact Assessment*, S. 72.

- **Szenario 1** geht davon aus, dass alle Diensteanbieter in Maßnahmen zur Automatisierung des Prozesses der Identifikation der Rechteverletzer und Warnhinweisversendung investieren. Insofern wird hier die kostenintensivste Variante zugrunde gelegt. Es entstehen einmalige Kapitalkosten durch die Investition in die Entwicklung von Software und Systemen zur Automatisierung des Prozesses der Identifikation und Warnhinweisversendung. Erste Angaben der Industrie lassen auf einen Aufwand von etwa **£80,000 pro Diensteanbieter** schließen. Der Markt im Vereinigten Königreich verteilt sich auf etwa 450 Diensteanbieter.⁶⁴³ Es werden hier **einmalige Kosten** in Höhe von insgesamt etwa **£35 Mio.** ($£80.000 \times 450$ Diensteanbieter = £36 Mio., abgerundet £35 Mio.) veranschlagt.⁶⁴⁴
- Bei **Szenario 2** investieren nur die größten fünf Internet-Zugangsanbieter in die Automatisierung, während die übrigen Anbieter die Warnhinweisversendung aus Kostengründen manuell bearbeiten. Entsprechend dem Marktanteil soll jeder der 450 kleineren Diensteanbieter 2.888 Meldungen über einen Verstoß innerhalb der ersten zwei Jahre erhalten. Die nicht automatisierte Identifikation der Rechteverletzer soll dabei Kosten in Höhe von jeweils £ 3,14 verursachen. Für jeden dieser Diensteanbieter ergäben sich Gesamtkosten in Höhe von £9.070 (aufgerundet von £9.068,32) jährlich.⁶⁴⁵ Die kleineren Diensteanbieter kämen insgesamt auf Kosten in Höhe von £4.081.500 (ausgehend von den bereits gerundeten £9.070 x 450 Diensteanbieter) pro Jahr. Für die fünf größten Unternehmen bliebe es jeweils bei den in Szenario 1 dargelegten Kosten in Höhe von £80.000, so dass sich hier Kosten in Höhe von insgesamt £400.000 ergeben würden. Die Gesamtkosten in Szenario 2 betrügen damit insgesamt **£4.481.500.**
- **Szenario 3** liegt die Überlegung zugrunde, dass alle 20 Telekommunikationsnetzbetreiber – dazu zählen auch die 5 größten ISPs – in die Automatisierung investieren, während die kleineren Diensteanbieter von einer Investition absehen, weil eben die Netzbetreiber, deren Netze sie mieten, die Bearbeitung der Warnhinweise für sie als Dienstleistung zur Verfügung stellen.⁶⁴⁶ Bei den 20

⁶⁴³ So *BIS, dcms, Intellectual Property Office: Impact Assessment*, S.73 in Fn. 53. Unklar ist, ob diese Zahl (450.000) die 5 größten ISPs inkludiert. Die Unklarheit entsteht dadurch, dass bei den Berechnungen im Rahmen von Szenario 2 (siehe sogleich) von 450.000 kleineren Diensteanbietern („*niche ISPs*“) und 5 großen ISPs ausgegangen wird (siehe *BIS, dcms, Intellectual Property Office: Impact Assessment*, S. 73 f.).

⁶⁴⁴ *BIS, dcms, Intellectual Property Office: Impact Assessment*, S. 73.

⁶⁴⁵ *BIS, dcms, Intellectual Property Office: Impact Assessment*, S. 74, unter Verweis auf *NERA Economic Consulting, The Costs and Benefits to ISPs of Proposed Measures to Curb Illegal File Sharing*, Dezember 2009.

⁶⁴⁶ *BIS, dcms, Intellectual Property Office: Impact Assessment*, S.74, unter Verweis auf *NERA Economic Consulting, The Costs and Benefits to ISPs of Proposed Measures to Curb Illegal File Sharing*, Dezember 2009.

Telekommunikationsnetzbetreibern entstünden Investitionskosten in Höhe von je £80.000, so dass insgesamt ein Betrag von **£1.600.000** anfiel.⁶⁴⁷

Bei der weiteren Berechnung wurden die Kosten aus Szenario 1 als ungünstigste Variante zugrunde gelegt.

5) *Kosten mobiler Netzwerkanbieter*

Eine Sonderberechnung wurde für die Anbieter mobiler Breitbanddienste angestellt, da die Identifizierung von Rechteinhaltern für Mobilnetzbetreiber technisch komplexer ist und damit zusätzliche Kosten entstehen. Denn anders als im Festnetz nutzt ein einzelner Kunde keine einmalige IP-Adresse. Dies macht es schwierig, den Rechteinhaber aus allen Nutzern der IP-Adresse herauszufiltern. Hinzu kommt, dass der Betreiber eines mobilen Breitbandnetzes zur Identifizierung eines Rechteinhabers alle Datenaktivitäten seiner Kunden überwachen muss. Das produziert notwendig höhere Kosten und ist datenschutzrechtlich bedenklich. Für die Entwicklung und Gestaltung eines Systems zur Zuordnung von IP-Adressen legt das *Impact Assessment* nach Angaben, die auf Schätzung der Industrie beruhen, Kapital- und Betriebskosten in Höhe von **£35 Mio.** für die **fünf Betreiber mobiler Netzwerke**⁶⁴⁸ im ersten Jahr zugrunde. Diese Kosten reduzieren sich ab dem zweiten Jahr auf **£17,5 Mio.** jährlich. Über einen Zeitraum von zehn Jahren entstünden damit jährliche Durchschnittskosten in Höhe von insgesamt **£19 Mio.** (abgerundet von £19,25 Mio.).

bb. Kosten auf Verbraucherseite

Die bei den Diensteanbietern anfallenden Kosten werden im Ergebnis an den Verbraucher weitergegeben. Die Erhebung geht davon aus, dass die jährlichen Kosten zur Nutzung eines Breitbandanschlusses durch die geschilderten Kosten um 0,2 bis 0,6 Prozent steigen werden. Nach Erhebungen der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) lag der durchschnittliche monatliche Preis für einen Breitbandanschluss im Vereinigten Königreich im Jahr 2007 etwa bei £20, also £240 jährlich. Nach Angaben der Anbieter nutzten 2007 etwa 14,5 Mio. Personen einen solchen Anschluss. Nimmt man an, dass sich die jährlichen Kosten der Zugangsanbieter auf Grund der Maßnahmen um £6 bis 20 Mio. pro Jahr erhöhen und dass dieser Betrag an die Verbraucher weitergegeben wird, würde der Preis für einen Privatkundenbreitbandanschluss um £0,40 (gerundet von £0,41) bzw. £1,40 (gerundet von £ 1.38) erhöhen, so dass es zu einer jährlichen Preiserhöhung um 0,2 bis 0,6 Prozent käme. Studien zur Preiselastizität zeigen zwar, dass die Nachfrage für Breitbandanschlüsse nicht sensibel auf Preiserhöhungen reagiert.⁶⁴⁹ Gleichwohl wird mit einem geringen Sinken der Nachfrage nach Breitbandanschlüssen (10.000 bis 40.000)⁶⁵⁰

⁶⁴⁷ BIS, dcms, Intellectual Property Office: Impact Assessment, S. 74.

⁶⁴⁸ Vodafone, O2, T-Mobile, Orange und Hutchinson 3G.

⁶⁴⁹ BIS, dcms, Intellectual Property Office: Impact Assessment, S. 76.

⁶⁵⁰ BIS, dcms, Intellectual Property Office: Impact Assessment, S. 76, unter Berufung auf SPC Network (2008), abrufbar unter: www.spcnetwork.co.uk/uploads/Broadband_Elasticity_Paper_2008.pdf.

und einem daraus resultierenden Einnahmeverlust der Diensteanbieter von £2 bis £9 Mio. pro Jahr gerechnet.⁶⁵¹ In diesem Zusammenhang weist das *Impact Assessment* auch darauf hin, dass sehr einkommensschwache Verbraucher oder solche ohne Zahlungsbereitschaft für digitale Inhalte bei Umsetzung des Warnhinweismodells nicht mehr auf kreative digitale Inhalte zurückgreifen würden.⁶⁵² Die möglichen negativen Auswirkungen für das Gemeinwohl⁶⁵³ ließen sich nicht beziffern.⁶⁵⁴ Allerdings wird darauf hingewiesen, dass der insoweit entfallende Vorteil in der Regel auf rechtswidrigem Verhalten beruhen dürfte, so dass er im Ergebnis keine Berücksichtigung finden könne. Die vom Kunden (unter Umständen endgültig) zu tragenden Gebühren bei Einlegung eines Widerspruchs in Höhe £20⁶⁵⁵ haben im Rahmen des *Impact Assessment* keine Berücksichtigung gefunden.⁶⁵⁶

cc. Kosten auf Seiten der Rechteinhaber

Auch für Rechteinhaber wird das Modell Kosten verursachen, die bei der Feststellung von Rechtsverletzungen, der Zusammenstellung und der Meldung der Rechtsverstöße an den Diensteanbieter sowie durch die Rechtsverfolgung anfallen. Rechteinhabern ist im eigenen Interesse an der konsequenten Verfolgung von Rechtsverstößen gelegen.⁶⁵⁷ Während keine Angaben zu den Kosten der Rechtsverfolgung vorliegen, werden Kosten für die Aufdeckung von Rechtsverstößen und deren Meldung an die Provider nach Schätzungen der Industrie (aber ohne weitere Begründung) wie folgt veranschlagt:⁶⁵⁸

- 2 Mio. Meldungen = £0,8 Mio.
- 4 Mio. Meldungen = £1,6 Mio.
- 6 Mio. Meldungen = £2,8 Mio.

In den beiden ersten Jahren nach Inkrafttreten der Regelungen wird mit ungefähr 21,5 Mio. Meldungen gerechnet.⁶⁵⁹

⁶⁵¹ *BIS, dcms, Intellectual Property Office: Impact Assessment*, S. 76.

⁶⁵² Vgl. dazu kritisch *Consumer Focus*, *Consumer Focus and the Citizens Advice response to notification of Digital Economy Act cost sharing order*, October 2011, abrufbar unter: <http://www.consumerfocus.org.uk/files/2010/10/Consumer-Focus-and-Citizens-Advice-response-to-notification-of-Digital-Economy-Act-cost-sharing-order.pdf>.

⁶⁵³ Belastbare Aussagen hierzu liegen nicht vor. Vgl. etwa *Rob&Waldfoegel; BIS, dcms, Intellectual Property Office: Impact Assessment*, S. 76.

⁶⁵⁴ *BIS, dcms, Intellectual Property Office: Impact Assessment*, S.76.

⁶⁵⁵ Siehe oben S. 129.

⁶⁵⁶ Vgl. dazu wiederum kritisch *Consumer Focus*, *Consumer Focus and the Citizens Advice response to notification of Digital Economy Act cost sharing order*, October 2011, abrufbar unter: <http://www.consumerfocus.org.uk/files/2010/10/Consumer-Focus-and-Citizens-Advice-response-to-notification-of-Digital-Economy-Act-cost-sharing-order.pdf>.

⁶⁵⁷ *BIS, dcms, Intellectual Property Office: Impact Assessment*, S. 77.

⁶⁵⁸ *BIS, dcms, Intellectual Property Office: Impact Assessment*, S. 77, unter Berufung auf Angaben der Rechteinhaber.

⁶⁵⁹ *BIS, dcms, Intellectual Property Office: Impact Assessment*, S. 77, unter Berufung auf NERA Economic Consulting: "The Costs and Benefits to ISPs of Proposed Measures to Curb Illegal File Sharing", Dezember 2009.

dd. Kosten auf Seiten des Staates

Auch für den Staat ist das Modell nicht kostenfrei. Insbesondere schlägt hier der Aufwand bei der OFCOM im Zusammenhang mit der Erstellung, Durchsetzung und Überwachung der Ausführungsvorschriften zu Buche, der vor Inkrafttreten des Codes indes nicht genau beziffert werden kann.⁶⁶⁰ Ein Richtwert ist das in Frankreich für einen ähnlichen Vorschlag zur Bekämpfung von Online-Urheberrechtsverletzungen festgelegte Budget in Höhe von £5 bis £6 Mio. im ersten Jahr, obgleich ein exakter Vergleich nicht möglich ist. Denn HADOPI in Frankreich wird auf anderer rechtlicher Grundlage tätig und nimmt eine zentralere Rolle ein als die, die für OFCOM vorgesehen ist. OFCOM wird im Übrigen in größerem Umfang als Hadopi berichtend tätig. Schließlich wird in Frankreich mit 17 Mio. Rechtsverletzungen jährlich gerechnet und damit im Vergleich zum Vereinigten Königreich mit einer fast dreimal höheren Anzahl (6 bis 7 Mio. Rechtsverletzungen im Jahr).⁶⁶¹

b. Nutzen

Ein Nutzen des Warnhinweismodells wird nicht nur für die Rechteinhaber sondern auch für die Verbraucher und den Staat, nicht aber für Diensteanbieter gesehen.

aa. Nutzen für Rechteinhaber

Das Warnhinweismodell soll den Rechteinhabern verlorene Gewinne in Höhe von etwa £200 Mio. (abgerundet von £220 Mio.) jährlich wiederbringen.⁶⁶² Dem stehen Schäden in Höhe von £400 Mio. Euro bei Verzicht auf ein Warnhinweismodell gegenüber. Dabei wird unterstellt, dass mindestens 55 Prozent der Betroffenen im Rahmen des Warnhinweisverfahrens auf rechtswidriges Verhalten verzichten.⁶⁶³ In den ersten zehn Jahren ergäbe sich somit ein Nutzen in Höhe von £2.000 Mio. (£2 Mrd.), der sich abgezinst auf einen Gesamtnutzen der Rechteinhaber in Höhe von etwa £1700 Mio. (also £1.7 Mrd.) reduziert.⁶⁶⁴

bb. Nutzen für Verbraucher

Die durch das Warnhinweismodell für die Rechteinhaber erreichte Refinanzierung ihrer Investitionen hält die ökonomische Basis für kulturelle Werte aufrecht, so dass künftige Investitionen gesichert und qualitativ für den Verbraucher erhalten bleiben können.⁶⁶⁵ Bei der Berechnung der Kosten blieben diese Effekte unberücksichtigt.

⁶⁶⁰ BIS, dcms, Intellectual Property Office: Impact Assessment, S. 78.

⁶⁶¹ BIS, dcms, Intellectual Property Office: Impact Assessment, S. 78.

⁶⁶² BIS, dcms, Intellectual Property Office: Impact Assessment, S. 68.

⁶⁶³ Dieser Wert ergab sich laut OFCOM bei Auswertung des freiwilligen Selbstversuchs.

⁶⁶⁴ BIS, dcms, Intellectual Property Office: Impact Assessment, S. 55.

⁶⁶⁵ BIS, dcms, Intellectual Property Office: Impact Assessment, S. 69.

cc. Nutzen für den Staat

Der Staat profitiert von der Stabilisierung des Marktes für kulturelle Güter über Mehrwertsteuereinnahmen, die zum Zeitpunkt der Berechnung im Jahre 2010 bereits beginnend mit 2010 auf £35 Mio.⁶⁶⁶ jährlich geschätzt wurden.⁶⁶⁷

c. Ergebnis der Kosten-Nutzen-Analyse

aa. Kosten - £290 - 500 Mio.

Bei der Berechnung des Netto-Nutzens eines Warnhinweismodells wurden auf der Kosten-
seite die Kosten der Diensteanbieter berücksichtigt. Es handelt sich um:

- Einmalige Kosten in Höhe von £35 Mio.
- Jahresdurchschnittskosten in Höhe von £30 -50 Mio.

Somit ergeben sich Gesamtkosten über einen Zeitraum von zehn Jahren in Höhe von £335
– 535 Mio., abgezinst noch **£290 - 500 Mio.**

bb. Nutzen - £1.7 Mrd

Auf der Nutzenseite wurde der Nutzen für die Rechteinhaber auf durchschnittlich £200
Mio. jährlich beziffert. Der Gesamtnutzen beläuft sich über einen Zeitraum von zehn Jah-
ren somit auf £2.000 Mio. (also £2 Mrd.), von dem abgezinst ein Betrag in Höhe von £1.700
Mio. (also £1.7 Mrd.) verbleibt.

d. Gesamt Netto-Nutzen £1,2 Mrd.

Bildet man die Differenz aus Kosten und Nutzen ab, so verbleibt ein Netto-Nutzen in Höhe
von £1,2 bis 1.41 Mrd. (gerundet auf £1,2 bis 1.4 Mrd.). Da das *Impact Assessment* die Werte
des ungünstigsten Ausgangs zugrunde legt, ergibt sich somit insgesamt ein **Netto-Nutzen
eines Warnhinweismodells** über einen Zeitraum von zehn Jahren von **£1,2 Mrd.**

6. Zusammenfassung

Mit dem Digital Economy Act wurde im Vereinigten Königreich ein zweistufiges Warnhin-
weismodell gesetzlich verankert, dessen Umsetzung noch vom Erlass der entsprechenden
Ausführungsvorschriften abhängt. Dieses verbindet auf seiner ersten Stufe ein Warnhin-
weismodell mit dem auch nach britischem Recht möglichen Auskunftsanspruch. Nach
Meldung einer IP-Adresse, die im Zusammenhang mit einer möglichen Rechtsverletzung

⁶⁶⁶ Bei einem Mehrwertsteuersatz von 17,5 Prozent.

⁶⁶⁷ Hier ist das Jahr 2010 ohne weitere Begründung als Beginn der Berechnung veranschlagt, obwohl eine
Aufnahme der Warnhinweisversendung nicht vor Ende des Jahres 2012 erwartet wird. *BIS, dcms, Intellectual
Property Office: Impact Assessment*, S. 70.

seitens des Rechteinhabers an die Zugangsanbieter übermittelt wird, versenden diese Warnhinweise an den betreffenden Kunden und führen zugleich eine Verstoßliste. Nach der dritten Meldung soll die Liste anonymisiert von den Rechteinhabern angefordert werden können. Bei der vierten Meldung eines Rechtsverstößes, bevor die Anforderung erfolgte, soll die Liste automatisch an den Rechteinhaber versandt werden. Die Effizienz dieser ersten Stufe in Hinblick auf die Rechteinhaber soll abgewartet werden. Erst wenn sie sich als ineffektiv erweist, sollen technische Sanktionen, die auf der zweiten Stufe erfolgen können, geprüft werden. Die Implementierung der ersten Stufe steht bevor, allerdings ist das Gesetz derzeit noch Gegenstand einer gerichtlichen Überprüfung.

III. Republik Irland

1. Ausgangslage (Überblick)

a. Bedeutung von Kultur

Kultur und kulturelles Schaffen genießen in Irland einen hohen Stellenwert, der sich insbesondere auch im irischen Recht nieder schlägt. Dies spiegeln die Ausführungen des irischen *High Court* in seinen Entscheidungen zum Urheberrecht im Internet wieder. Der *High Court* hält das *Copyright* für eine Bereicherung der Menschheit, das sich unabhängig von entsprechender Gesetzgebung, also naturrechtlich aus der natürlichen menschlichen Erwartung ergebe, dass ein solches Recht aus Gründen schlichter Fairness existieren müsse.⁶⁶⁸ Die in den Urteilen als „Diebstahl“ bezeichnete Internet-Piraterie vernichte die wirtschaftliche Basis für das Schaffen von Musikproduktionsunternehmen und ruiniere die Fähigkeit einer Generation kreativer Menschen - nicht nur in Irland- mit künstlerischem Schaffen ihren Lebensunterhalt zu verdienen.⁶⁶⁹ Im Hinblick auf das aus Sicht des Gerichts gewaltige Ausmaß der Internet-Piraterie sind die Ermittlung von Rechteverletzern, Warnungen und die Kappung des Internet-Zugangs nach dreimaliger Rechtsverletzung für den *High Court* angemessen.⁶⁷⁰

⁶⁶⁸ EMI Records (Ireland) Ltd., Sony BMG Music Entertainment (Ireland) Ltd., Universal Music (Ireland) Ltd. and Warner Music (Ireland) Ltd. v. Eircom Plc., *Charleton J.*, 24.7.2009 [2009] IEHC 411.

⁶⁶⁹ EMI Records (Ireland) Ltd, Sony Music Entertainment Ireland Ltd, Universal Music Ireland Ltd Warner Music Ireland Ltd and Wea International Inc v UPC Communications Ireland Ltd, *Charleton J.*, *High Court Commercial*, 11.10.2010, [2010] IEHC 377 Rn. 8.

⁶⁷⁰ EMI Records (Ireland) Ltd., Sony B. G. Music Entertainment (Ireland) Ltd., Universal Music Ireland Ltd. and Warner Music Ireland Ltd. v Eircom Ltd., *Charelton J.*, 16.4.2010, [2010] IEHC 108, Rn. 30 sowie EMI Records (Ireland) Ltd, Sony Music Entertainment Ireland Ltd, Universal Music Ireland Ltd Warner Music Ireland Ltd and Wea International Inc v UPC Communications Ireland Ltd, *Charleton J.*, *High Court Commercial*, 11.10.2010, [2010] IEHC 377 Rn. 83.

b. Urheberrechtliche Rahmenbedingungen und verfassungsrechtliche Grundlagen des Schutzes Geistigen Eigentums

aa. Verfassungsrechtliche Perspektive

Das irische Urheberrecht (*Copyright and Related Rights Act 2000*) bezeichnet *Copyright* als Eigentumsrecht (*property right*)⁶⁷¹, das dem Inhaber des Rechts u. a. bestimmte ausschließliche Rechte zur Werkverwertung gewährt. Als Eigentumsrecht steht das *Copyright* unter dem Schutz der irischen Verfassung.⁶⁷² Für den irischen *High Court* ist *Copyright* ein fundamentales Recht nach der irischen Verfassung.⁶⁷³ Die Verfassungsbestimmungen wirken dabei nicht nur gegenüber dem Staat und staatlichen Institutionen, sondern können auch Drittwirkung entfalten.⁶⁷⁴

bb. Gesetzliche Verankerung des Schutzes von Urheberrechten

Das Urheberrecht findet an verschiedenen Stellen des einfachen irischen Rechts seine Verankerung.

1) *Copyright and Related Rights Act 2000*

Nach irischem Urheberrecht (*Copyright and Related Rights Act 2000*) hat der Urheber bzw. der Inhaber des *Copyright*⁶⁷⁵ u. a. das ausschließliche Recht, sein Werk zu kopieren und es der Öffentlichkeit verfügbar zu machen sowie andere hierzu zu autorisieren.⁶⁷⁶ Das Recht des Urhebers, sein Werk zu kopieren und andere dazu zu autorisieren („*reproduction right*“⁶⁷⁷), erfasst etwa dessen Speicherung in jeder Art von Medium.⁶⁷⁸ Die als „*making available right*“ bezeichnete⁶⁷⁹ Befugnis des *Copyright*-Inhabers, sein Werk der Öffentlichkeit zugänglich zu machen und andere zu berechtigen dies zu tun, umfasst u. a. die drahtgebundene und nicht drahtgebundene öffentliche Zugänglichmachung einer Werkkopie in einer Weise, dass Teilnehmer der Öffentlichkeit von einem Ort und zu Zeiten ihrer Wahl Zugang zu dem Werk haben.⁶⁸⁰ Ausdrücklich mit einbezogen ist das Zugänglichmachen einer Werkkopie per Internet.⁶⁸¹

⁶⁷¹ Section 17 (1) *Copyright and Related Rights Act 2000*.

⁶⁷² *Clark/Shúilleabháin*, Intellectual Property Law in Ireland, 2010, S. 75 Rn. 212 mit Hinweis auf *Phonographic Performance (Ireland) v. Cody* [1994] ILRM 241.

⁶⁷³ *High Court* vom 16.4.2010 *EMI Records & Ors v. Eircom Ltd.* [2010] IEHC 108.

⁶⁷⁴ *Clark/Shúilleabháin*, Intellectual Property Law in Ireland, 2010, S. 75 Rn. 212 unter Hinweis auf *Herrity v. Associated Newspapers (Ireland) Ltd.* [2008] IEHC 249.

⁶⁷⁵ Section 17 (1) *Copyright and Related Rights Act 2000*.

⁶⁷⁶ Section 37 (1) (a) (b) *Copyright and Related Rights Act 2000*.

⁶⁷⁷ Section 39 (2) *Copyright and Related Rights Act 2000*.

⁶⁷⁸ Section 39 (1) (a) (i) *Copyright and Related Rights Act 2000*.

⁶⁷⁹ Section 40 (8) *Copyright and Related Rights Act 2000*.

⁶⁸⁰ Vgl. dazu auch *Clark / Shúilleabháin*, Intellectual Property Law in Ireland, 2010, S. 54 Rn. 122.

⁶⁸¹ Section 40 (1) (a) *Copyright and Related Rights Act 2000*.

Wie das deutsche Urheberrecht kennt auch das irische *Copyright Law* eine Reihe von Schranken, die Eingriffe gestatten.⁶⁸² Es sieht aber etwa keine Privatkopie-Regelung vor, die, wie § 53 Abs. 1 UrhG, Vervielfältigungen eines Werkes zum privaten Gebrauch gegen Zahlung einer Vergütung (§§ 54 ff. UrhG) gestattet.⁶⁸³ Das *Copyright* verletzt auch, wer ohne Lizenz des Berechtigten, die nachfolgend genannten Handlungen vornimmt oder andere dazu autorisiert, solche Handlungen vorzunehmen.⁶⁸⁴ Ein Verstoß gegen das „Reproduktions-Recht“ des Urhebers begeht, wer Dateien mit illegalen Werkkopien aus dem Internet herunterlädt.⁶⁸⁵ Illegales P2P-Downloading stellt eine Verletzung des Rechts des Urhebers dar, sein Werk der Öffentlichkeit zugänglich zu machen.⁶⁸⁶ Softwareanbieter, die kommerziell von Filesharing profitieren und die in Kenntnis der Illegalität der meisten Dateien Filesharing Vorschub leisten, „autorisieren“ Verletzungen im Sinne des *Copyright-Act*.⁶⁸⁷

Bei *Copyright*-Verletzung gewährt der *Copyright and Related Rights Act 2000* dem Urheber eine Reihe von Rechtsmitteln,⁶⁸⁸ u. a. einen Anspruch auf Schadensersatz gegen den Verletzer.⁶⁸⁹ Gemäß Section 140 (1) *Copyright and Related Rights Act 2000* sind zudem bestimmte Urheberrechtsverletzungen strafbar, wenn der Betreffende Kenntnis davon oder Grund zu der Annahme hat, dass es sich bei der Kopie, die er herstellt oder nutzt, um eine rechtsverletzende Werkkopie handelt.⁶⁹⁰ Im Hinblick auf das Rechtsmittel einer gerichtlichen Anordnung zur Beendigung von (weiteren) Urheberrechtsverletzungen im Internet hat der *High Court* aber im Oktober 2010 entschieden, dass nach irischem Recht ein Gericht nicht ermächtigt ist, zu verfügen, dass ein Internet-Zugangsanbieter den Zugang zu Internet-Sites blockieren oder abschalten muss. Auch für eine Übertragungsunterbrechung oder Umleitung oder das Trennen des Internet-Zugangs eines Kunden wird keine gesetzli-

⁶⁸² Vgl. Chapter 6 of Part II (Section 49 ff.) of *Copyright and Related Rights Act 2000*. Siehe dazu auch *Clark / Shúilleabháin*, Intellectual Property Law in Ireland, 2010, S. 60 ff. Rn. 149 ff. – Ausnahmen, die im Zusammenhang mit massenhaften Urheberrechtsverletzungen im Internet ggf. relevant sein können, bestehen namentlich für: „Transient and incidental copies“ (Section 87 (1) *Copyright and Related Rights Act 2000*: “The copyright in a work is not infringed by the making of a transient and incidental copy of that work which is technically required for the viewing of or listening to the work by a member of the public to whom a copy of the work is lawfully made available.”), „Recording for purposes of time shifting“ (Section 101 (1) *Copyright and Related Rights Act 2000*: “The making for private and domestic use of a fixation of a broadcast or cable programme solely for the purpose of enabling it to be viewed or listened to at another time or place shall not infringe the copyright in the broadcast or cable programme or in any work included in such a broadcast or cable programme.”).

⁶⁸³ *Clark / Shúilleabháin*, Intellectual Property Law in Ireland, 2010, S. 60 Rn. 149. Ausnahme: Section 50 (1) *Copyright and Related Rights Act 2000*, wonach “Fair dealing [...] for the purpose of [...] private study” keine Urheberrechtsverletzung darstellt; vgl. dazu *Clark / Shúilleabháin*, Intellectual Property Law in Ireland, 2010, S. 61 Rn. 151, 153.

⁶⁸⁴ Section 37 (2) *Copyright and Related Rights Act 2000*. Siehe dazu auch *Clark / Shúilleabháin*, Intellectual Property Law in Ireland, 2010, S. 74 f. Rn. 207 ff.

⁶⁸⁵ *Clark / Shúilleabháin*, Intellectual Property Law in Ireland, 2010, S. 53 Rn. 118 mit Hinweis auf *High Court* [2005] IEHC 233.

⁶⁸⁶ *High Court* vom 16.4.2010 [2010] IEHC 108.

⁶⁸⁷ So *Clark / Shúilleabháin*, Intellectual Property Law in Ireland, 2010, S. 74 Rn. 208 unter Hinweis auf *Universal Music Australia Pty. Ltd. v. Sharman* [2005] FCA 1242.

⁶⁸⁸ Vgl. Section 127 (2) *Copyright and Related Rights Act 2000* sowie die Rechtsmittel im Einzelnen nach Chapter 9 of Part II of *Copyright and Related Rights Act 2000*.

⁶⁸⁹ Dazu ausführlich *Clark / Shúilleabháin*, Intellectual Property Law in Ireland, 2010, S. 77 ff. Rn. 221 ff.

⁶⁹⁰ Siehe dazu auch *Clark / Shúilleabháin*, Intellectual Property Law in Ireland, 2010, S. 79 Rn. 229.

che Grundlage gesehen. Allerdings hält der *High Court* in Anwendung von Section 40 (4) des *Copyright and Related Rights Act 2000* eine Anordnung gegenüber einem Internet-Host-Service für zulässig, urheberrechtlich geschütztes Material von seinen Seiten zu entfernen.⁶⁹¹

2) *Auskunftsanspruch*

Das irische Recht kennt keine gesetzliche Regelung, die einen Internet Service Provider verpflichtet, Rechteinhabern Auskunft über Personen zu erteilen, die über den betreffenden Internetanschluss Urheberrechte verletzt haben.⁶⁹² In ständiger Rechtsprechung des *High Court* ist aber als grundlegendes Rechtsprinzip anerkannt, dass eine Person, die in eine unerlaubte Handlung eines Dritten verwickelt ist, indem sie auch ohne eigenes Verschulden das Fehlverhalten Dritter ermöglicht oder erleichtert hat, dem Verletzten gegenüber zur Auskunft über den Täter verpflichtet ist.⁶⁹³

a) *Offenlegung der Identität*

2005 wurde erstmals ein Anspruch auf Auskunft über die Identität eines Anschlussinhabers gewährt.⁶⁹⁴ Dabei sind grundsätzlich die einem Dritten bekannten Informationen in Bezug auf einen angeblichen Rechteverletzer gegenüber einem Geschädigten offenzulegen.⁶⁹⁵ Diese Pflicht beschränkt sich auf Fälle, in denen ein offenkundiger Beweis einer Verletzungshandlung besteht und in denen es um die namentliche Identität des Verletzers geht,

⁶⁹¹ EMI Records (Ireland) Ltd, Sony Music Entertainment Ireland Ltd, Universal Music Ireland Ltd, Warner Music Ireland Ltd and Wea International Inc v UPC Communications Ireland Ltd, *Charleton J., High Court Commercial*, 11.10.2010, [2010] IEHC 377.

⁶⁹² Vgl. EMI Records (Ireland) Ltd, Sony Music Entertainment Ireland Ltd, Universal Music Ireland Ltd, Warner Music Ireland Ltd and Wea International Inc v UPC Communications Ireland Ltd, *Charleton J., High Court Commercial*, 11.10.2010, [2010] IEHC 377 Rn. 62.

⁶⁹³ Vgl. EMI Records (Ireland) Ltd, Sony BMG Music Entertainment (IRL) Ltd, Universal Music Ireland Ltd, Warner Music Ireland Ltd v Eircom Ltd, BT Communications Ireland Ltd, *Kelly, J., High Court Commercial*, 8. July 2005, [2005] IEHC 233; EMI Records (Ireland) Ltd, Sony Music Entertainment Ireland Ltd, Universal Music Ireland Ltd, Warner Music Ireland Ltd and Wea International Inc v UPC Communications Ireland Ltd, *Charleton J., High Court Commercial*, 11.10.2010, [2010] IEHC 377 Rn. 62. – Grundlage dieses Rechtsprinzips ist eine Entscheidung des *House of Lords* (UK) aus dem Jahr 1973 (*Norwich Pharmacal Company and Others v Customs and Excise Commissioners* [1974] A.C. 133). Es besagt: "If through no fault of his own a person gets mixed up in the tortious acts of others so as to facilitate their wrongdoing, he may incur no personal liability, but he comes under a duty to assist the person who has been wronged by giving him full information and disclosing the identity of the wrongdoers." Gerichtliche Auskunftsanordnungen werden deshalb seither "Norwich Pharmacal Orders" genannt.

⁶⁹⁴ EMI Records (Ireland) Ltd, Sony BMG Music Entertainment (IRL) Ltd, Universal Music Ireland Ltd, Warner Music Ireland Ltd v Eircom Ltd, BT Communications Ireland Ltd, *Kelly, J., High Court Commercial*, 8. July 2005, [2005] IEHC 233. Siehe auch EMI Records (Ireland) Ltd, Sony Music Entertainment Ireland Ltd, Universal Music Ireland Ltd Warner Music Ireland Ltd and Wea International Inc v UPC Communications Ireland Ltd, *Charleton J., High Court Commercial*, 11.10.2010, [2010] IEHC 377 Rn. 58 ff.

⁶⁹⁵ EMI Records (Ireland) Ltd, Sony BMG Music Entertainment (IRL) Ltd, Universal Music Ireland Ltd, Warner Music Ireland Ltd v Eircom Ltd, BT Communications Ireland Ltd, *Kelly, J., High Court Commercial*, 8. July 2005, [2005] IEHC 233 unter Berufung auf die "Norwich Pharmacal"-Entscheidung und das darauf fußende allgemein anerkannte Rechtsprinzip. Siehe auch EMI Records (Ireland) Ltd, Sony Music Entertainment Ireland Ltd, Universal Music Ireland Ltd, Warner Music Ireland Ltd and Wea International Inc v UPC Communications Ireland Ltd, *Charleton J., High Court Commercial*, 11.10.2010, [2010] IEHC 377, Rn. 62 sowie EMI Records (Ireland) Ltd., Sony B.M.G. Music Entertainment (Ireland) Ltd., Universal Music Ireland Ltd. and Warner Music Ireland Ltd. v Eircom Ltd., *Charleton J.*, 16.4.2010, [2010] IEHC 108 Rn. 24.

nicht aber um Modalitäten der Tatbegehung.⁶⁹⁶ Der *High Court* verlangt dabei, zwischen den Rechten der Urheber einerseits und den Verpflichtungen der Internet-Provider gegenüber ihren Abonnenten und den korrespondierenden Rechten dieser Abonnenten andererseits, **abzuwägen**⁶⁹⁷ und dabei auf die bestmögliche Schonung der Persönlichkeitsrechte des Betroffenen zu achten.⁶⁹⁸ Provider sind danach zur Geheimhaltung oder zum Datenschutz gegenüber ihren Kunden rechtlich verpflichtet; eine Anordnung des Gerichts kann aber diese Pflichten außer Kraft setzen. Beim prima facie Beweis einer Rechtsverletzung hat das Recht auf Datenschutz oder Geheimhaltung der Identität zurückzutreten. Wer Urheberrechte verletzt oder derjenige, gegen den sich der Beweis des ersten Anscheins richtet, kann sich nicht auf den Schutz seiner Identität berufen.

Dementsprechend hat das Gericht drei Zugangsanbieter verpflichtet, klagenden Musikproduktionsgesellschaften Namen, Adressen und Telefonnummern von 17 Personen bekanntzugeben. Diese waren Kunden der Provider und hatten nach Angaben der Kläger in großem Umfang illegal Musikstücke in Filesharingnetzen hochgeladen. Der *High Court* hat die Offenlegungsanordnung ("*Norwich Pharmacal Order*")⁶⁹⁹ allerdings mit einer Schutzklausel versehen, um zu gewährleisten, dass die Rechte und Ansprüche der beklagten Provider und der gegenüber den Rechteinhabern identifizierten Kunden angemessen berücksichtigt werden. Danach verlangt die Anordnung die Zusicherung der Kläger, die offengelegten Informationen ausschließlich zu dem Zweck zu gebrauchen, Entschädigung für die verletzten Urheberrechte zu verlangen.

b) Weitere Auskunftsklagen

In einer Anordnung von 2006 hat der *High Court* drei Zugangsanbietern auferlegt, den klagenden Unternehmen die Namen, Adressen und Telefonnummern von 49 Personen bekanntzugeben, die, mutmaßlich im Rahmen von Filesharing, Daten „getauscht“ also kopiert hatten.⁷⁰⁰ Den Personen war vorgeworfen worden, unter Verstoß gegen section 140 des *Copyright and Related Rights Act 2000* zwischen 500 und 5.000 Dateien heruntergeladen zu haben. Der *High Court* sah für die klagenden Unternehmen keinen anderen Weg, an die betreffenden Informationen zu gelangen. Erneut betont das Gericht das Recht auf Privatsphäre und Vertraulichkeit, aber auch die Pflicht, diese Rechtspositionen gegen die vorgeworfenen widerrechtlichen Handlungen abzuwägen. Den Zugangsanbietern wurde

⁶⁹⁶ Unter Bezugnahme auf den *Supreme Court* im Falle von *Megaleasing UK Ltd v Barrett* [1993] IRLM 497, p. 504.

⁶⁹⁷ Vgl. dazu auch *EuGH*, Urt. v. 24. November 2011 (*Scarlet Extended*), Rs. C-70/10, Rn. 44 ff.

⁶⁹⁸ Unter Bezugnahme auf *BMG Canada Inc. and Others v. Doe and Others*.

⁶⁹⁹ Benannt nach dem Fall *Norwich Pharmacal Company and Others v Customs and Excise Commissioners* [1974] A.C. 133).

⁷⁰⁰ *EMI Records (Ireland) Ltd, Sony BMG Entertainment (IRL) Ltd, Universal Music Ireland Ltd und Warner Music Ireland Ltd v Eircom Ltd, BT Communications Ireland Ltd und Irish Broadband Internet Services Ltd, High Court, Kelly J.*, 24. Januar 2006 (unveröffentlicht); siehe aber zusammenfassend *McGonagle*, IRIS 2006-4:15/26, abrufbar unter <http://merlin.obs.coe.int/iris/2006/4/article26.de.html>.

seitens der klagenden Unternehmen zugesagt, die mitgeteilten Informationen nur im Rahmen der richterlich vorgegebenen Zweckbindung zu benutzen.⁷⁰¹

c) Sonstige Verfahren

2007 ordnete der *High Court* gegen Eircom Ltd. und sechs andere Zugangsanbieter an, Rechteinhabern die Namen und Adressen von 23 Personen preiszugeben.⁷⁰² Die Auskunftspflicht wurde 2010 durch den *High Court* bekräftigt. Bei dieser Gelegenheit vertrat das Gericht zudem den Standpunkt, dass das Verfahren zur Auskunftserteilung beschwerlich und letztlich zwecklos ist, um der „Internet-Piraterie“ beizukommen.⁷⁰³ In Folge der Entscheidungen des *High Court* in den Jahren 2005 – 2007 wurden in drei Fällen Verfahren gegen Personen eingeleitet, deren Namen und Adressen offengelegt worden waren. In einem Fall stellte sich der Verdacht der Urheberrechtsverletzung als unbegründet heraus, in den beiden anderen Verfahren wurde ein Vergleich geschlossen. Daneben ist es zu weiteren außergerichtlichen Vergleichen zwischen der Irish Recorded Music Association (IRMA) und Nutzern gegen Zahlung von durchschnittlich 2.500 Euro gekommen.⁷⁰⁴ Der *High Court* weist darauf hin, dass Anwaltskosten in Höhe von 680.000 Euro für die Identifikation von Personen im Wege gerichtlicher Anordnungen von 2005 bis 2007 Vergleichszahlungen in Höhe von 80.000 Euro gegenüberstehen.⁷⁰⁵

2. Stand der Gesetzgebung/ Vergleichsregelung

In der Republik Irland besteht keine gesetzliche Regelung, die es Zugangsanbietern auferlegt, im Falle von Urheberrechtsverletzungen Warnhinweise an ihre Kunden zu versenden und gegebenenfalls Internetanschlüsse zu unterbrechen oder zu sperren. Maßnahmen zur Sperrung oder Deaktivierung des Zugangs zu Webseiten sind nach der Rechtsprechung ebenso wenig zulässig, wie die Unterbrechung oder Kappung des Internetzugangs.⁷⁰⁶

⁷⁰¹ Nachdem die klagenden Produktionsgesellschaften anerkannt hatten, dass die Zugangsanbieter keine Verantwortung trifft und sie die bei der Ermittlung der Informationen verbundenen Kosten tragen, konnte das Verfahren beendet werden.

⁷⁰² Vgl. EMI Records (Ireland) Ltd, Sony Music Entertainment Ireland Ltd, Universal Music Ireland Ltd, Warner Music Ireland Ltd and Wea International Inc v UPC Communications Ireland Ltd, *Charleton J., High Court Commercial*, 11.10.2010, [2010] IEHC 377 Rn. 9. Vgl. auch etwa Blog: IRMA to pursue and prosecute 23 people for illegally sharing music online (*UnaRocks*), veröffentlicht am 7.6.2007, abrufbar unter: <http://unarocks.blogspot.com/2007/06/irma-to-pursue-and-prosecute-23-people.html>.

⁷⁰³ EMI Records (Ireland) Ltd, Sony Music Entertainment Ireland Ltd, Universal Music Ireland Ltd, Warner Music Ireland Ltd and Wea International Inc v UPC Communications Ireland Ltd, *Charleton J., High Court Commercial*, 11.10.2010, [2010] IEHC 377 Rn. 62.

⁷⁰⁴ *McGonagle*, IRIS 2006-4:15/26, abrufbar unter: <http://merlin.obs.coe.int/iris/2006/4/article26.de.html>.

⁷⁰⁵ EMI Records (Ireland) Ltd, Sony Music Entertainment Ireland Ltd, Universal Music Ireland Ltd, Warner Music Ireland Ltd and Wea International Inc v UPC Communications Ireland Ltd, *Charleton J., High Court Commercial*, 11.10.2010, [2010] IEHC 377 Rn. 62.

⁷⁰⁶ EMI Records (Ireland) Ltd, Sony Music Entertainment Ireland Ltd, Universal Music Ireland Ltd Warner Music Ireland Ltd and Wea International Inc v UPC Communications Ireland Ltd, *Charleton J., High Court Commercial*, 11.10.2010, [2010] IEHC 377.

Unabhängig davon existiert ein Vergleich zwischen Eircom Ltd., dem führenden Internet Service Provider Irlands, und vier großen irischen Musikproduktionsgesellschaften (EMI Records Ltd., Sony B. M. G. Music Entertainment Ltd., Universal Music Ireland Ltd., Warner Music Ireland Ltd.), der eine Warnhinweisregelung mit einem „*Graduated Response*“-Verfahren vorsieht, das in der Abschaltung des Internetanschlusses enden kann. Ferner gibt es ein auf der Grundlage des Vergleichs vereinbartes Protokoll sowie ein Regelwerk („*Principles for Managing Copyright Infringements by Users of P2P Internet Applications*“). Es ist nicht ersichtlich, dass andere irische Diensteanbieter zu einer entsprechenden Vereinbarung bereit sind.⁷⁰⁷ Dies mag daran liegen, dass das irische Urheberrecht derzeit einer eingehenden Überprüfung unterzogen wird,⁷⁰⁸ deren Ergebnis die Einführung einer gesetzlichen Warnhinweisregelung sein kann.⁷⁰⁹

Die Beweggründe für Eircom, den Vergleich zu schließen, liegen nicht offen. Vorteile bringt die Einigung jedoch insofern mit sich, als „Internetpiraterie“ in der Rechtsprechung als massives rechtliches Problem eingeordnet wurde und die Verweigerung, dem entgegenzuwirken, schwer erklärbar ist und am Ende zu Imageverlusten führt. Zudem konnte an der konkreten Ausgestaltung des Verfahrens konstruktiv mitgewirkt werden. Des Weiteren konnte die Warnung mit einem Hinweis auf legale Alternativen in Kooperation mit den klagenden Musikproduktionsgesellschaften zu eigenem wirtschaftlichen Nutzen verbunden werden.⁷¹⁰

3. Vergleich und Protokoll zur Warnhinweisregelung

Im Jahr 2008 hatten mehrere Musikproduktionsunternehmen gegen Eircom Plc., mit dem Ziel geklagt, Copyrightverletzungen im Internet per gerichtlicher Anordnung unterbinden zu lassen. Es ging darum, eine Überwachungs- bzw. Filtertechnologie im Netzwerk des Diensteanbieters zum Einsatz zu bringen, um Urheberrechtsverletzungen bei der Nutzung von P2P-Filesharing zu identifizieren und zu verhindern.

Im Januar 2009 schlossen die Streitparteien einen privatrechtlichen, also gerichtlich weder autorisierten noch angeordneten Vergleich, auf dessen Grundlage ein Protokoll ausge-

⁷⁰⁷ Vgl. Blog: Irish Government Wants File-Sharing Compromise, Or Legislation Will Follow (*enigmax*), veröffentlicht am 15.11.2010, abrufbar unter: <http://torrentfreak.com/irish-government-wants-file-sharing-compromise-or-legislation-will-follow-101115/>.

⁷⁰⁸ Siehe dazu *McCallig*, IRIS 2011-7:1/27 abrufbar unter:

<http://merlin.obs.coe.int/iris/2011/7/article27.de.html>; siehe auch *Kennedy*, Radical copyright law reform to boost Ireland's digital economy?, veröffentlicht am 9.5.2011, abrufbar unter:

<http://www.siliconrepublic.com/new-media/item/21695-radical-copyright-law-reform/>; Consultation on the Review of the Copyright and Related Rights Act 200, abrufbar unter:

http://www.djei.ie/science/ipr/copyright_review_2011.htm; Blog: Ireland Set To Force ISPs To Disconnect Pirates (*enigmax*), veröffentlicht am 21.6.2011, abrufbar unter: <http://torrentfreak.com/ireland-set-to-force-isps-to-disconnect-pirates-110621/>.

⁷⁰⁹ Vgl. *Kennedy*, Telcos, ISPs anxious as digital copyright law changes loom, veröffentlicht am 22.6.2011, abrufbar unter: <http://www.siliconrepublic.com/comms/item/22323-telcos-isps-anxious-as-dig/>.

⁷¹⁰ Siehe unten S. 152.

handelt sowie ein Warnhinweisverfahren („*Principles for Managing Copyright Infringements by Users of P2P Internet Applications*“) vereinbart wurden⁷¹¹, das Einzelheiten zur Umsetzung des Vergleichs, insbesondere die wesentlichen Verpflichtungen und Verantwortlichkeiten der Parteien im Detail anordnet.⁷¹²

- Vergleich und Protokoll sehen zunächst vor, dass Musikunternehmen gegenüber Eircom monatlich von ihnen ermittelte Urheberrechtsverletzungen anzeigen. Eircom prüft daraufhin in einem maximal fünfstufigen Verfahren die Versendung von Warnhinweisen und die Verhängung von Sanktionen.
- Die Musikproduktionsgesellschaften haben sich dazu verpflichtet, auch gegen andere Zugangsanbieter entsprechende Verfahren mit dem Ziel eines entsprechenden Vergleichs anzustrengen, um Wettbewerbsnachteilen für Eircom durch Abwanderungen von Kunden zu Konkurrenzunternehmen oder das Fernbleiben neuer Kunden entgegen zu wirken.
- Die Parteien haben sich zudem darauf verständigt, dass Eircom einem Antrag⁷¹³ der Musikproduktionsgesellschaften zur Erwirkung einer gerichtlichen Anordnung nicht entgegentritt, mit der diese den Zugang zur Website „Pirate Bay“ sperren lassen wollen, über die Musikinhalte in P2P-Netzwerken auffindbar gemacht werden. Eircom erklärte, einen solchen Antrag weder zu unterstützen noch ihm zuzustimmen.
- Angedacht war es, mit der Warnhinweis-Regelung ein eigenes kostenpflichtiges legales Angebot von Eircom mit Musik-Downloads einzurichten. Eircom-Kunden sollte kostenfreier legaler Zugang zu Musik-Streamings gewährt werden. Dieser Dienst („MusicHub“) wurde Ende 2010 in Kooperation mit der Musikindustrie

⁷¹¹ HINWEIS: Der Vergleich sowie das auf der Grundlage des Vergleichs vereinbarte Protokoll und Regelwerk („*Principles for Managing Copyright Infringements by Users of P2P Internet Applications*“) sind nicht öffentlich zugänglich. Öffentlich zugänglich sind nur „Sekundärquellen“. Dabei handelt es sich im Wesentlichen um zwei Entscheidungen des *High Court* – nämlich: *EMI Records (Ireland) Ltd., Sony B. M.G. Music Entertainment (Ireland) Ltd., Universal Music Ireland Ltd. and Warner Music Ireland Ltd. v. Eircom Ltd.*, *Charleton J.*, 16.4.2010, [2010] IEHC 108 und *EMI Records (Ireland) Ltd, Sony Music Entertainment Ireland Ltd, Universal Music Ireland Ltd, Warner Music Ireland Ltd and Wea International Inc. v. UPC Communications Ireland Ltd*, *Charleton J., High Court Commercial*, 11.10.2010, [2010] IEHC 377 –, um Nachrichten von Informationsdiensten (hier: <http://www.siliconrepublic.com/>) sowie insbesondere um ein nicht verifiziertes Dokument mit dem Titel: „*Briefing Note on arrangement between Eircom and the Irish Record Music Association (IRMA) with regard to Copyright Infringement, March 2009*“, das sich offenbar auf einen Protokoll-Entwurf bezieht und das verschiedentlich im Internet kursiert (z. B. <http://www.scribd.com/doc/13630351/Eircom-Irma-Briefing-Note-March-2009>). Die nachfolgenden Ausführungen beruhen auf diesen Sekundärquellen und auf dem Regelwerk zum Protokoll („*Principles for Managing Copyright Infringements by Users of P2P Internet Applications*“), das dem Verfasser der Studie vorliegt. Weitere Quelle ist ein vertrauliches Papier von IFPI (*International Federation of the Phonographic Industry*) mit dem Titel: *IFPI Market Research, Measuring the Impact of Graduated Response – Ireland. Update: October 2011*. Dieses Papier liegt dem Verfasser der Studie ebenfalls vor.

⁷¹² Vgl. zu dem Inhalt des Protokolls *High Court EMI Records (Ireland) Ltd., Sony B. G. Music Entertainment (Ireland) Ltd., Universal Music Ireland Ltd. and Warner Music Ireland Ltd. v. Eircom Ltd.*, *Charleton J.*, 16.4.2010, [2010] IEHC 108 Rn. 11.

⁷¹³ Siehe unten S. 164.

eingeführt.⁷¹⁴ Eircom weist den Nutzer auf jeder Stufe des „*Graduated Response*“-Verfahrens auf dieses Angebot hin.

- Es ist vereinbart, dass Eircom Ltd. die Aktivitäten und den Datenverkehr seiner Kunden nicht überwachen muss.
- Der Provider ist dazu verpflichtet, insbesondere alle Bestimmungen des Datenschutzrechts zu beachten und keine persönlichen oder vertraulichen Informationen hinsichtlich seiner Kunden (Anschlussinhaber) irgendwelcher Art gegenüber den Musikproduktionsgesellschaften oder Dritten offenzulegen. Eircom Ltd. wird nach den Abreden namentlich keine personenbezogenen Daten an die Musikproduzenten übermitteln, die eine Identifizierung eines Kunden von Eircom Ltd. ermöglichen.
- Um die Zahl derer zu minimalisieren, die potentiell von den Warnhinweisen betroffen sind, ist vorgesehen, dass Eircom Ltd. vor Implementierung der Warnhinweis-Regelung eine an ihre Kunden (Anschlussinhaber) gerichtete Erziehungs- und Aufklärungskampagne durchzuführen hat, die diesen die Illegalität von Filesharing bzw. den Missbrauch von P2P-Software sowie das Warnhinweis-system bewusst macht.⁷¹⁵

4. Das Warnhinweis-Modell in der Republik Irland

Nach einem Überblick über die rechtlichen Rahmenbedingungen nach irischem Recht, den Vergleich zwischen Eircom und den Musikunternehmen sei im Folgenden das in Irland praktizierte Modell beschrieben.

a. Ausgestaltung

aa. Regelungsziel (Schutzzweck)

Die Warnhinweis-Regelung bezweckt es, Urheberrechtsverletzungen durch Nutzer von P2P-Netzwerken zu verhindern oder zu reduzieren. Erfasst sind nur Urheberrechte, die von den Musikunternehmen wahrgenommen werden. Es geht nur um Musikstücke, an denen die beteiligten Musikunternehmen Rechte besitzen. Anwendbar ist die Regelung nur gegenüber Kunden von Eircom. Mit ihr soll verhaltenssteuernd auf die Nutzer eingewirkt werden. Diese Wirkung soll in mehreren Schritten erzielt werden, nämlich zunächst durch

⁷¹⁴Vgl. Müller, Eircom Musikservice soll Three- Strikes relativieren, veröffentlicht am 12.12.2010, abrufbar unter: <http://www.gulli.com/news/14875-eircom-musikservice-soll-three-strikes-relativieren-2010-12-12> ; Blog: ISP 3 Strikes Anti- Piracy Strategy Rewarded By Big Four Music Service (*enigmax*), veröffentlicht am 8.12.2010, abrufbar unter: <http://torrentfreak.com/isp-3-strikes-anti-piracy-strategy-rewarded-by-big-four-music-service-101208/>.

⁷¹⁵Vgl. *High Court* EMI Records (Ireland) Ltd., Sony B. G. Music Entertainment (Ireland) Ltd., Universal Music Ireland Ltd. and Warner Music Ireland Ltd. v. Eircom Ltd., *Charleton J.*, 16.4.2010, [2010] IEHC 108 Rn. 11; dort auch Angaben zu weiteren Regelungsgegenständen des Protokolls.

erzieherische Aufklärung über die Urheberrechtsverletzung, dann abschreckend durch die Androhung einer Sanktion und schließlich durch Sanktionsverhängung.⁷¹⁶

bb. Systematische Verortung der Warnhinweis-Regelung

Das in Irland praktizierte Warnhinweismodell ist ohne gesetzliche Grundlage das Ergebnis eines privaten Vergleichs und bindet allein die Vertragsparteien. Die Regelung wirkt nur gegenüber Eircom-Vertragskunden und ist gerichtlich weder autorisiert noch angeordnet, wohl aber durch den irischen *High Court* sowohl, was die Vereinbarung als auch ihre Umsetzung betrifft⁷¹⁷, rechtlich bestätigt.

cc. Anwendungsbereich

Die Warnhinweis-Regelung ist einerseits nur anwendbar auf Verletzungen solcher Urheberrechte, die von den Musikproduktionsgesellschaften wahrgenommen werden, andererseits muss bei einer Urheberrechtsverletzung eine Eircom zugewiesene IP-Adresse involviert sein, die bei dem betreffenden Verstoßvorgang einem Eircom-Kunden zugeteilt gewesen ist. Sachlich betrifft die Regelung nur Urheberrechtsverletzungen, die im Rahmen von Filesharing bzw. bei P2P-Netzwerken stattfinden. Adressaten von Warnhinweisen sind deshalb nur Eircom-Anschlussinhaber, die sich an Rechtsverletzungen innerhalb dieser Erscheinungsform beteiligen. Im Übrigen ist der persönliche und sachliche Anwendungsbereich der Warnhinweis-Regelung grundsätzlich nicht beschränkt. Es werden alle Kunden des Providers und alle Internet-Anschlüsse erfasst. Im Hinblick auf das Abschalten des Internetzugangs als Sanktion nach mehrfachen Rechtsverletzungen können allerdings Einschränkungen bestehen. Die verhängten Sanktionen betreffen dabei nur den Internet-Access-Service von Eircom. Andere Telekommunikationsdienste des Providers bleiben nutzbar.

dd. Regelungsinhalt

Das Verfahren in Irland erfolgt durch eine schematische Prüfung, die durch einen Entscheidungsspielraum ergänzt wird.

1) Schematische Prüfung

Grundlegende Voraussetzung für das „*Graduated Response*“-Verfahren gegen einen Eircom-Kunden ist, dass ein am Vergleich beteiligtes Musikproduktionsunternehmen gegenüber dem Internet-Service-Provider in einer bestimmten Form⁷¹⁸ die Verletzung von Urheberrechten unter Angabe der IP-Adresse, die im Rahmen eines illegalen Uploading- oder Downloading-Vorgangs in einem P2P-Netzwerk aufgedeckt wurde, nachweist.

⁷¹⁶ Siehe im Einzelnen unten S. 155.

⁷¹⁷ Siehe unten S. 161.

⁷¹⁸ Siehe noch unten S. 159.

a) Level 1 („First Warning“)

Dies zieht als erste Rechtsfolge des gestaffelten Verfahrens die Einstufung des betreffenden Anschlussinhabers auf „Verletzungslevel 1“ („On Notice“) und die Pflicht des Diensteanbieters nach sich, dem Anschlussinhaber den Hinweis zu erteilen („**First Warning**“). Dabei ist dieser Kunde darauf hinzuweisen, dass sein Anschluss ermittelt wurde, bei der behaupteten Verletzung (zu einer bestimmten Zeit) von Urheberrechten an einem bestimmten Werk beteiligt gewesen zu sein. Diese erste Warnung dient vornehmlich einem erzieherischen bzw. Aufklärungs-Zweck, damit keine weiteren Rechtsverletzungen über den betroffenen Anschluss mehr vorkommen. Sie erfolgt auch mit Blick auf die Möglichkeit, dass der Internetanschluss missbräuchlich etwa von einem Arbeitnehmer, einem Familienmitglied oder sonst wem innerhalb des Empfangsbereichs des WLAN-Routers des Anschlussinhabers genutzt worden ist.

Auf der ersten Stufe kam es aufgrund Grund einer technischen Funktionsstörung⁷¹⁹ im Oktober 2010 zu einer Fehlversendung von Warnhinweisen an ca. 300 Eircom-Kunden, die keine Verletzungshandlungen begangen hatten. Mit diesem Vorgang wurde, auf Beschwerde eines Anschlussinhabers der Datenschutzbeauftragte Irlands (*Data Protection Commissioner*) befasst.⁷²⁰ In der förmlichen Untersuchung hat der Datenschutzbeauftragte das „*Graduated Response*“-System **im Hinblick auf den Datenschutz untersucht**.⁷²¹ Inzwi-

⁷¹⁹Die fälschliche Mitteilung an die Anschlussinhaber hing mit einem Fehler bei der Umstellung des Servers von der Sommer- auf die Winterzeit zusammen. Dadurch sind dynamische IP-Adressen nicht den richtigen Personen zugeordnet worden. Den betreffenden Anschlussinhabern wurde so mit der ersten Warnung eine Urheberrechtsverletzung vorgeworfen, die irgendein anderer Kunde unter derselben IP-Adresse eine Stunde früher oder später begangen hatte. Eircom Ltd. hat diesen Fehler eingeräumt und erklärt, dass die fälschlicherweise beschuldigten Kunden auf die Problematik hingewiesen worden sind und ihnen eine Gutschrift in Höhe von 50 € für die nächste Rechnung erteilt wurde. Letztlich sei nur in einem Fall Beschwerde eingelegt worden. Eircom Ltd. habe geeignete Schritte unternommen, um sicherzustellen, dass das Problem nicht nochmals auftrete. Siehe *Kennedy*, Data commissioner investigating Eircom 'three strikes' system, veröffentlicht am 21.6.2011, abrufbar unter: <http://www.siliconrepublic.com/comms/item/22309-data-commissioner-investiga/>; *McIntyre*, Irish „Three Strikes“ System Investigated By Data Protection Commissioner, veröffentlicht am 15.6.2011, abrufbar unter: <http://unurl.org/15>; Blog: ISP Wrongfully Sent 300 'First Strike' Letters To Innocents (*enigmax*), veröffentlicht am 17.6.2011, abrufbar unter: <http://torrentfreak.com/isp-wrongfully-sent-300-first-strike-letters-to-innocents-110617/>; *Müller*, Eircom: 300 falsche Three- Strikes- Warnungen versandt, veröffentlicht am 18.6.2011, abrufbar unter: <http://www.gulli.com/news/16373-eircom-300-falsche-three-strikes-warnungen-versandt-2011-06-18>.

⁷²⁰*Kennedy*, Data commissioner investigating Eircom 'three strikes' system, veröffentlicht am 21.6.2011, abrufbar unter: <http://www.siliconrepublic.com/comms/item/22309-data-commissioner-investiga/>; *McIntyre*, Irish „Three Strikes“ System Investigated By Data Protection Commissioner, veröffentlicht am 15.6.2011, abrufbar unter: <http://unurl.org/15>.

⁷²¹Nach der Einschätzung von *McIntyre*, Irish „Three Strikes“ System Investigated By Data Protection Commissioner, veröffentlicht am 15.6.2011, abrufbar unter: <http://unurl.org/15>, soll mit der Untersuchung die Rechtmäßigkeit des „Three Strikes“-Regimes an sich überprüft werden. Nach Ansicht von *McIntyre* „scheint [es] wahrscheinlich, dass der Datenschutzbeauftragte eine Entscheidung im Sinne seiner früher geäußerten Ansichten treffen wird, wonach die Verwendung von IP-Adressen zur Sperre von Internetverbindungen unverhältnismäßig ist und keine "faire Nutzung" personenbezogener Daten darstellt.“ Der Datenschutzbeauftragte habe dann „die Befugnis und letztlich auch die Pflicht, eine Verfügung zu erlassen, mit der Eircom die Nutzung personenbezogener Daten für diese Zwecke untersagt wird – ein Ergebnis, welches das Three-Strikes-System ins Wanken bringen würde, sofern Eircom nicht erfolgreich Einspruch erhebt oder die Musikindustrie mit ihrer Kampagne zur Einführung eines Three-Strikes-Systems ins irische Rechtssystem doch noch reüssiert.“

schen ist die sechsmonatige Untersuchung abgeschlossen und das Untersuchungsergebnis dem Provider mitgeteilt worden, der innerhalb von 21 Tagen auf die Entscheidung des Datenschutzbeauftragten reagieren muss.⁷²² Medienberichten zu Folge hat die Behörde wegen Verstoßes gegen das Datenschutzrecht bzw. Verletzung der Privatsphäre gegenüber Eircom angeordnet, das „**Graduated Response**“-Verfahren zu stoppen.⁷²³ Der Provider soll diese Entscheidung nicht akzeptiert und Berufung beim *Circuit Court* eingelegt haben mit der Folge, dass er bis zum Ende des Verfahrens die Warnhinweis-Regelung weiter anwenden kann.⁷²⁴

b) *Level 2 („Second Warning“)*

Im nächsten Schritt erfolgt die Heraufstufung des Kunden auf „Verletzungslevel 2“ („*Severe Warning*“) und die Verpflichtung des Diensteanbieters zum „**Second Warning**“. Dies setzt zum einen voraus, dass der Provider nach dem Versand des „*First Warning*“ einen entsprechenden „Nachweis“ eines weiteren Urheberrechtsverstoßes erhält, der sich auf denselben Anschlussinhaber bezieht. Zum anderen müssen seit der ersten Rechtsverletzung mindestens vierzehn Tage verstrichen sein. Schließlich muss der Nachweis der Rechtsverletzung den Provider innerhalb eines Jahres nach Einstufung des Anschlussinhabers auf „Level 1“ erreichen. Der Kunde verbleibt dort ein Jahr, sofern nicht eine Heraufstufung auf „Level 2“ erfolgt.

Im Rahmen dieser zweiten Warnung hat der Diensteanbieter dem Kunden in einem förmlichen Schreiben mitzuteilen, dass dessen IP-Adresse erneut im Zusammenhang mit einem Urheberrechtsverstoß ermittelt wurde. Der Anschlussinhaber wird zudem gewarnt, dass der Internet-Access-Service⁷²⁵ beendet wird, falls eine weitere Urheberrechtsverletzung stattfindet. Diese „*Second Warning*“ enthält Einzelheiten zu den festgestellten Rechtsverletzungen, wiederholt die „erzieherische Botschaft“ des „*First Warning*“ und liefert Kontaktdaten, die der Anschlussinhaber bei Fragen nutzen kann.

⁷²² Kennedy, Eircom has 21 days to respond to halt 'three strikes' order by DPC, veröffentlicht am 19.12.2011, abrufbar unter: <http://www.siliconrepublic.com/comms/item/25072-eircom-has-21-days-to/> (unter Berufung auf eine Aussage der Datenschutzbehörde); Out-Law.com, Irish ISP ordered to stop using 'three strikes' system against illegal file-sharers, veröffentlicht am 20.12.2011; abrufbar unter: <http://www.out-law.com/en/articles/2011/december/irish-isp-ordered-to-stop-using-three-strikes-system-against-illegal-file-sharers/>.

⁷²³ McIntyre, Christmas and New Year privacy roundup, veröffentlicht am 2.1.2012, abrufbar unter: <http://www.tjmcintyre.com/2012/01/christmas-and-new-year-privacy-roundup.html> (mit Vermutungen zu den Gründen dieser Entscheidung); siehe auch 'Massive blow' to music industry as Eircom anti-piracy measures rejected, veröffentlicht am 18.12.2011, abrufbar unter: <http://businessetc.thejournal.ie/massive-blow-to-music-industry-as-eircom-anti-piracy-measures-rejected-307584-Dec2011/>; Out-Law.com, Irish ISP ordered to stop using 'three strikes' system against illegal file-sharers, veröffentlicht am 20.12.2011; abrufbar unter: <http://www.out-law.com/en/articles/2011/december/irish-isp-ordered-to-stop-using-three-strikes-system-against-illegal-file-sharers/>.

⁷²⁴ McIntyre, Christmas and New Year privacy roundup, veröffentlicht am 2.1.2012, abrufbar unter: <http://www.tjmcintyre.com/2012/01/christmas-and-new-year-privacy-roundup.html> (unter Berufung auf Mark Tighe von der *Sunday Times*).

⁷²⁵ Nicht betroffen sind andere Internet-Dienstleistungen wie VOIP oder IPTV.

c) *Level 3 („Termination Notice“ und Anschlussunterbrechung)*

Auf der nächsten Stufe erfolgen die Überprüfung der „Beweislage“ und gegebenenfalls die Heraufstufung des Anschlussinhabers auf „Verletzungslevel 3“. Dieses setzt voraus, dass dem Provider nach Versand des „*Second Warning*“ eine dritte Urheberrechtsverletzung nachgewiesen wird, die sich auf denselben Anschlussinhaber bezieht. Während auf den vorangehenden Ebenen eine automatische Prüfung erfolgt, nimmt der Provider nunmehr eine eigenständige Prüfung vor. Verläuft diese „positiv“, hat der Provider die Pflicht zur Versendung einer „**Termination Notice**“ an den Anschlussinhaber, die diesem anzeigt, dass sein Internetanschluss innerhalb von vierzehn Tagen abgeschaltet wird. Nach Ablauf dieser Frist ist der Anschluss für eine Woche zu unterbrechen.⁷²⁶ Vor Durchführung dieser Maßnahmen müssen abermals mindestens vierzehn Tage nach der vorangehenden Rechtsverletzung verstrichen sein. Weiterhin muss der Diensteanbieter den Nachweis der Rechtsverletzung innerhalb eines Jahres nach Heraufstufung des Kunden auf „Level 2“ erhalten, da der Kunde auf dieser Stufe ebenfalls ein Jahr verbleibt, falls nicht eine Eingruppierung auf „Level 3“ stattfindet.

d) *Level 4 (Wiederanschluss)*

Nach Ablauf der Wochenfrist erfolgt der Wiederanschluss an das Internet. („Level 4“).

e) *Level 5 (Einjährige Anschluss Sperre)*

Die letzte Stufe des „*Graduated Response*“-Verfahrens bringt die Heraufstufung des Kunden auf „Level 5“ mit sich. Sie löst die Pflicht des Providers zur weiteren Benachrichtigung seines Kunden sowie die Sperrung von dessen Internetanschluss für ein Jahr aus.⁷²⁷ Dazu muss dem Provider von dem Rechteinhaber in Bezug auf denselben Anschlussinhaber nach dessen Wiederanschluss an das Internet eine vierte Urheberrechtsverletzung nachgewiesen werden.

Nach Ablauf der 12 Monate wird die Zugangssperre aufgehoben und die Person hat die Möglichkeit, wieder den Breitbanddienst des Internet-Providers zu erwerben.

⁷²⁶ Vgl. *Sobiraj*, Eircom kickt seit heute Filesharer aus dem Internet, veröffentlicht am 24.5.2010, abrufbar unter <http://www.gulli.com/news/13360-eircom-kickt-seit-heute-filesharer-aus-dem-internet-2010-05-24> ; *Kennedy*, Data commissioner investigating Eircom ‘three strikes’ system, veröffentlicht am 21.6.2011, abrufbar unter: <http://www.siliconrepublic.com/comms/item/22309-data-commissioner-investiga/>.

⁷²⁷ *Sobiraj*, Eircom kickt seit heute Filesharer aus dem Internet, veröffentlicht am 24.5.2010, abrufbar unter <http://www.gulli.com/news/13360-eircom-kickt-seit-heute-filesharer-aus-dem-internet-2010-05-24> ; *Kennedy*, Data commissioner investigating Eircom ‘three strikes’ system, veröffentlicht am 21.6.2011, abrufbar unter: <http://www.siliconrepublic.com/comms/item/22309-data-commissioner-investiga/>.

Vgl. *Sobiraj*, Eircom kickt seit heute Filesharer aus dem Internet, veröffentlicht am 24.5.2010, abrufbar unter <http://www.gulli.com/news/13360-eircom-kickt-seit-heute-filesharer-aus-dem-internet-2010-05-24> ; *Kennedy*, Data commissioner investigating Eircom ‘three strikes’ system, veröffentlicht am 21.6.2011, abrufbar unter: <http://www.siliconrepublic.com/comms/item/22309-data-commissioner-investiga/>.

2) Beschwerderecht des Anschlussinhabers

Das irische Modell wird nicht automatisch per Benachrichtigung durch eine Musikproduktionsgesellschaft betrieben. Dem Anschlussinhaber steht vielmehr auf allen Verfahrensstufen die Möglichkeit zur rechtlichen Beschwerde oder zur Gegendarstellung in tatsächlicher Hinsicht gegenüber dem Provider zu. Er kann darlegen, dass er entweder zu Unrecht als Täter identifiziert wurde oder dass die Sperrung seines Zugangs zum Internet nicht angemessen wäre. Wenn der Provider unter Berücksichtigung des Vorbringens des Anschlussinhabers der Ansicht ist, der Urheberrechtsverstoß habe nicht in der behaupteten Art und Weise stattgefunden, ist er ohne Rücksprache mit dem Musikproduktionsunternehmen berechtigt, den betreffenden Kunden von einem Level zurückzustufen oder die Abschaltung seines Anschlusses zu unterlassen.⁷²⁸

Das Abschalten als ultima ratio soll nur erfolgen, wenn der Provider vollständig davon überzeugt ist, dass

- ein eindeutiger Nachweis⁷²⁹ einer anhaltenden Urheberrechtsverletzung erbracht ist,
- dass die Person, der die Rechtsverletzung vorgeworfen wird, die hinreichende Gelegenheit hatte, seine Umstände zu erläutern, und
- dass alle Möglichkeiten ausgeräumt sind, zu der Überzeugung zu gelangen, dass die betreffende Person Opfer eines zufälligen Rechtsverstoßes war.

Eircom hat auch das Recht, den Anschlussinhaber zurückzustufen oder von Sanktionen abzusehen, wenn bestimmte „mildernde Umstände“ vorliegen, unter denen die Abschaltung des Anschlusses nicht gerechtfertigt wäre. So erfolgt keine Unterbrechung oder Sperrung bei Personen, die aus ernsthaften medizinischen Gründen oder zur Bestreitung ihres Lebensunterhaltes von dem Zugang zum Breitband-Internet abhängig sind. Weiterhin kann die Sanktion etwa durch eine Verwarnung ersetzt werden, wenn die Rechtsverletzung in einem Unternehmen stattfindet, also die IP-Adresse eines Geschäftskunden („*Business Customers*“) involviert ist, und dies im Widerspruch zu den Richtlinien zur Internet-Nutzung innerhalb des Betriebes steht.

Der Provider hat auf Einwände einzugehen und Fragen des Anschlussinhabers zu beantworten und dieses Vorbringen beim weiteren Vorgehen zu berücksichtigen. Rechtsschutz gegenüber Eircom – etwa unter Beteiligung eines neutralen Schlichters oder einer neutralen Schiedsstelle – ist nicht ersichtlich.

Abgesehen davon dürfte es rechtlich möglich sein, dass der Anschlussinhaber sich zivilrechtlich gegenüber Eircom zur Wehr setzt und namentlich Vertragserfüllung im Klagewe-

⁷²⁸ Eircom. muss in diesem Fall den Rechteinhaber darüber informieren, dass die IP-Adresse nicht unter die Bestimmungen der Vereinbarungen fällt.

⁷²⁹ Siehe aber noch unten S. 159 zu den Anforderungen an den zu erbringenden Nachweis.

ge geltend macht, wenn er das Abschalten seines Anschlusses für unzulässig hält. Der Provider-Vertrag schließt diese Möglichkeit nicht aus.

b. Organisatorische Umsetzung des Warnhinweismodells

aa. Aufgabe der Rechteinhaber

Das Verfahren basiert darauf, dass die Musikproduktionsgesellschaften Unternehmen damit beauftragen, Rechtsverstöße in P2P-Netzwerken zu ermitteln, und dann gegenüber dem Provider die Rechtsverstöße nachweisen. Dazu ist eine geeignete Software einzusetzen, die Urheberrechtsverletzungen in P2P-Netzwerken aufdecken und die für den Nachweis notwendigen Daten liefern kann.⁷³⁰ Die Software lädt Daten geschützter Werke herunter und spürt so IP-Adressen auf, über die die betroffenen Daten übertragen werden.⁷³¹ In diesem Ermittlungsprozess erfahren die Produktionsgesellschaften nur, dass eine bestimmte IP-Adresse in die Urheberrechtsverletzung involviert ist, nicht aber, dass etwa eine an einem bestimmten Ort in Irland lebende bestimmte Person sich rechtswidrig verhalten hat.⁷³²

Soweit es sich bei den ermittelten IP-Adressen um Eircom zur Verfügung gestellte Adressen handelt, zeigt das Musikproduktionsunternehmen dem Provider in monatlichen Abständen an („*Notification*“), dass IP-Adressen beim illegalen Laden urheberrechtlich geschützter Werke in P2P-Netzwerken identifiziert wurden. Der „Nachweis“ muss den folgenden Anforderungen genügen bzw. die Anzeige („*Notification*“) muss mindestens die folgenden Punkte enthalten:

- detaillierte Angaben zum Inhaber des Urheberrechts (Name und Adresse),
- die Angabe des Grundes der Mitteilung (Urheberrechtsverletzung),
- Informationen zum verletzten Werk sowie seines Urhebers (Metadaten in einer Datei, wie z. B. Künstler, Lied, Musik-, Albumtitel),
- die IP-Adresse, die bei der Urheberrechtsverletzung ermittelt worden ist,
- den „Zeit-Stempel“, wann die Ermittlung initiiert und wann sie abgeschlossen wurde,

⁷³⁰ Siehe sogleich.

⁷³¹ Vgl. die Beschreibung der DtecNet-Software in EMI Records (Ireland) Ltd, Sony Music Entertainment Ireland Ltd, Universal Music Ireland Ltd, Warner Music Ireland Ltd and Wea International Inc v UPC Communications Ireland Ltd, *Charleton J., High Court Commercial*, 11.10.2010, [2010] IEHC 377, Rn. 34. Eingesetzt werden kann auch eine vergleichbare Software zur Aufdeckung von Urheberrechtsverstößen.

⁷³² Denn eine IP-Adresse ist nicht mehr als eine Nummer, die ein Internet-Service-Provider einem Computer zuteilt, wenn hierüber Zugang zum Internet gewährt wird. Die IP-Nummer identifiziert elektronisch den Nutzer des Internet. Nummernbestände für IP-Adressen werden von einer internationalen Institution generiert und diese wiederum werden ISPs zur Verfügung gestellt. Anhand der IP-Nummer bzw. -adresse lässt sich feststellen, wer der betreffende Internet-Service-Provider ist, denn es ist kein Geheimnis, welcher ISP welchen Bestand mit Tausenden oder Millionen von IP-Adressen erhalten hat. Weil nun ISPs Tausende von Kunden haben und zudem IP-Adressen vielfach dynamisch, d. h. bei jedem Zugang zum Internet erneut vergeben werden, hilft einem die Kenntnis einer „urheberrechtsverletzenden IP-Adresse“ und deren Zuteilung an einen ISP nicht weiter, um die Identität der Rechteinhabers herauszufinden.

- das P2P-Protokoll und die P2P-Anwendungssoftware, die der Anschlussinhaber benutzt hat, und
- den digitalen Fingerprint/Hash des urheberrechtlich geschützten Materials.⁷³³

Zudem muss der Nachweis dem Standard eines Beweises entsprechen, der in der Vergangenheit erbracht worden ist und in Zukunft verlangt werden dürfte, um im Rahmen eines Prozesses vor einem irischen Gericht „*Norwich Pharmacal Orders*“ („*Disclosure Orders*“) zur Auskunftserteilung zu erhalten.⁷³⁴ Fehlen in der „*Notification*“ Informationen bzw. ist eine Urheberrechtsverletzung nicht in der entsprechenden Form nachgewiesen, wird Eircom gegenüber einem Anschlussinhaber nicht tätig.

Insgesamt ist sicherzustellen, dass die betreffenden Daten gesetzeskonform erlangt werden. Die Rechteinhaber haben fortlaufend die Genauigkeit, Integrität und Stimmigkeit der an den Diensteanbieter im Rahmen der „*Notification*“ übermittelten Informationen zu gewährleisten. Es muss gegenüber dem Provider eine seriöse, jährlich erstellte Zertifizierung erbracht werden, dass die notwendigen regulatorischen Kontrollen im Hinblick auf den Bezug, das Generieren sowie die Weiterverarbeitung der Daten durch einen beauftragten Dienstleister weiter betrieben werden und funktionieren.

bb. Aufgabe der Provider

Auf der anderen Seite ist der Diensteanbieter gegenüber den Rechteinhabern und Musikproduktionsgesellschaften fortlaufend dafür verantwortlich sicherzustellen, dass die erhaltenen „*Notifications*“ ordnungsgemäß („*in a fair and consistent way*“) bearbeitet und behandelt werden. Er muss jährlich eine seriöse, von unabhängiger Seite erstellte, Zertifizierung erbringen, dass die regulatorischen Kontrollen hinsichtlich der Umsetzung des „*Graduated Response*“-Verfahrens korrekt weiter betrieben werden und funktionieren. Der Diensteanbieter hat zudem den Rechteinhabern und Musikproduktionsgesellschaften zusammenfassende Berichte zu übermitteln, die auf einer in geeigneter Weise zusammengefassten Grundlage das Fortschreiten von Urheberrechtsverletzern im Zuge des „*Graduated Response*“-Verfahrens anzeigen.

Die Kundenverträge von Eircom bestimmen ausdrücklich, dass Anschlussinhaber den Internetzugang nicht dazu nutzen dürfen, Material zu kreieren, zu „beherbergen“ oder zu übermitteln, das Urheberrechte verletzt. Vorgesehen ist dort auch, dass der Vertrag im Falle einer Vertragsverletzung suspendiert und beendet werden kann. Im Übrigen liegt es in der Verantwortung des Diensteanbieters, Verfahren einzurichten, um mit Tatsachengendarstellungen und/oder Beschwerden in Bezug auf die „*Notifications*“ und/oder die „*Graduated Responses*“ umzugehen und sie zu beantworten.

⁷³³ Letzteres erlaubt Eircom Ltd. zu verifizieren, dass die Urheberrechte der geschützten Werke, die von den Musikproduktionsgesellschaften identifiziert worden sind, tatsächlich von diesen wahrgenommen werden.

⁷³⁴ Siehe dazu oben S. 148.

5. Entscheidungen des *High Court* mit Bezug zur Vergleichsregelung

Die Vergleichs- und Protokollregelung war bereits Gegenstand verschiedener Entscheidungen des irischen *High Court*, die nachfolgend ausgewertet werden.

a. Vereinbarkeit der Warnhinweis-Regelung mit irischem Datenschutz- und Verfassungsrecht

In einer Entscheidung aus dem April 2010 befasste sich das Gericht mit dem Vergleich und Protokoll.⁷³⁵ Es ging um Fragen des Verfassungs- und Datenschutzrechts. Weil im Rahmen des Warnhinweisverfahrens auf eine große Menge von Daten zugegriffen wird, hatte eine der Streitparteien den Datenschutzbeauftragten Irlands (*Data Protection Commissioner*) eingeschaltet. Dieser warf drei Fragen zur datenschutzrechtlichen Bewertung des Vergleichs auf. Im Ergebnis erklärte das Gericht das Modell für verfassungs- und datenschutzrechtlich beanstandungsfrei.

aa. IP-Adresse als personenbezogenes Datum

Zunächst ging es darum, ob eine IP-Adresse als personenbezogenes Datum im Sinne der Bestimmungen des irischen *Data Protection Act 1988 and 2003* einzuordnen ist.⁷³⁶

bb. Verfassungsrechtliche Bewertung des „*Graduated Response*“-Verfahrens

Die zweite Frage betraf die Vereinbarkeit der letzten Stufe des „*Graduated Response*“-Verfahrens, also die Abschaltung des Internet-Anschlusses durch Eircom, mit dem irischen Verfassungsrecht. Fraglich war, ob die (Weiter-)Verarbeitung („*processing*“⁷³⁷) personenbezogener Daten durch Eircom im Zusammenhang mit der Sperrung des Internetzugangs – in der Annahme, dass die Weiterverarbeitung für die Wahrung legitimer Interessen des Providers notwendig ist – ungerechtfertigt fundamentale Rechte und Freiheiten oder legitime Interessen des Betroffenen („*data subject*“⁷³⁸) beeinträchtigt.⁷³⁹ Der *High Court* verneint

⁷³⁵ *High Court* EMI Records (Ireland) Ltd., Sony B. G. Music Entertainment (Ireland) Ltd., Universal Music Ireland Ltd. and Warner Music Ireland Ltd. v. Eircom Ltd., *Charleton J.*, 16.4.2010, [2010] IEHC 108.

⁷³⁶ Siehe dazu unten S. 297.

⁷³⁷ Vgl. Section 1(1) *Data Protection Act, 1988 as amended*: “*processing*’ of or in relation to information or data, means performing any operation or set of operations on the information or data, whether or not by automatic means, including— [...]”. Vgl. auch § 3 Abs. 4 BDSG.

⁷³⁸ Vgl. Section 1(1) *Data Protection Act, 1988 as amended*: “*data subject* means an individual who is the subject of personal data”. Vgl. auch § 3 Abs. 1 BDSG.

⁷³⁹ Vgl. Section 2A (1) *Data Protection Act, 1988 as amended*: “*Personal data shall not be processed by a data controller unless section 2 of this Act (as amended by the Act of 2003) is complied with by the data controller and at least one of the following conditions is met:*” “(d) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.” – Siehe auch zusammenfassend McGonagle, IRIS 2010-6:1/34 (<http://merlin.obs.coe.int/iris/2010/6/article34.de.html>).

dies.⁷⁴⁰ Nach Ansicht des Gerichts handelt es sich beim „*copyright*“ um ein fundamentales Recht nach der irischen Verfassung. Die Vertragsbedingungen von Eircom, die eine Nutzung des Internet zur Verletzung von *copyright* untersagen, seien deshalb rechtmäßig und angemessen und der Nutzer habe sich mit der im Vertrag vorgesehenen Abschaltung seines Internetanschlusses für den Fall vertragswidrigen Verhaltens einverstanden erklärt. Die Verarbeitung („*processing*“) der Daten, einschließlich deren Übertragung von einem Musikproduktionsunternehmen an Eircom, der Warnung von Eircom-Kunden und der Sperrung des Netz-Zugangs, diene damit sowohl der Vertragserfüllung als auch der Einhaltung gesetzlicher Bestimmungen. Weil es grundsätzlich auch kein Recht gebe, verfassungsmäßige Rechte anderer zu verletzen, sei die Abschaltung des Internetzugangs bei dreimaliger Urheberrechtsverletzung nicht unangemessen und damit auch nicht ungerechtfertigt im Hinblick auf fundamentale Rechte und Freiheiten oder legitime Interessen des Betroffenen, zumal das Protokoll insoweit relevante Ausnahmen vorsehe. Das Gericht hält die Regelungen auch nicht für inhuman oder willkürlich. Im Recht des Betroffenen zur Gegendarstellung gegenüber Eircom sieht der *High Court* eine angemessene Verfahrensgarantie in Übereinstimmung mit Art. 1 Abs. b der Richtlinie 2009/140/EG.

cc. Weitere datenschutzrechtliche Aspekte

Bei der dritten Frage ging es erneut um Datenschutz. Zum einen war gefragt, ob im Hinblick auf Section 2A (1) und 2B (1) des *Data Protection Act 1988 (as amended)* die Umsetzung des vorgesehenen Verfahrens und insbesondere die Abschaltung des Internetzugangs als Sanktion im Rahmen des Prozesses überhaupt zulässig ist.⁷⁴¹ Gefragt war erstens danach, ob Eircom und die Produktionsgesellschaften damit an einer Verarbeitung von sensiblen personenbezogenen Daten („*sensitive personal data*“⁷⁴²) beteiligt sein würden. Die Frage wurde aufgeworfen, weil die Daten mit der Begehung einer Straftat in Verbindung gebracht werden können. Zweifel bestanden zum anderen deshalb, weil die Kapung des Internetanschlusses durch Eircom damit begründet würde, dass der betreffende Kunde mit dem Laden urheberrechtlich geschützten Materials mit einer strafbaren Handlung in Verbindung gebracht werde, ohne dass diese Gegenstand strafbehördlicher Untersuchung gewesen und der Betroffene verurteilt worden sei. Das Gericht hält das gestaffelte Verfahren auch insoweit für rechtmäßig.⁷⁴³ Von einer Beschuldigung mit einer Straftat

⁷⁴⁰ EMI Records (Ireland) Ltd., Sony B. G. Music Entertainment (Ireland) Ltd., Universal Music Ireland Ltd. and Warner Music Ireland Ltd. v Eircom Ltd., *Charleton J.*, 16.4.2010, [2010] IEHC 108, Rn. 26 ff.

⁷⁴¹ Siehe auch zusammenfassend McGonagle, IRIS 2010-6:1/34, abrufbar unter: <http://merlin.obs.coe.int/iris/2010/6/article34.de.html>.

⁷⁴² Vgl. Section 1(1) *Data Protection Act, 1988 as amended*: „*‘sensitive personal data’ means personal data as to— (a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject, (b) whether the data subject is a member of a trade union, (c) the physical or mental health or condition or sexual life of the data subject, (d) the commission or alleged commission of any offence by the data subject, or (e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.*“ Vgl. auch § 3 Abs. 9 BDSG.

⁷⁴³ EMI Records (Ireland) Ltd., Sony B. G. Music Entertainment (Ireland) Ltd., Universal Music Ireland Ltd. and Warner Music Ireland Ltd. v Eircom Ltd., *Charleton J.*, 16.4.2010, [2010] IEHC 108, Rn. 36 ff.

sei in Vergleich und Protokoll nicht die Rede, noch liege sie im Interesse der Parteien des Vergleichs, sondern es gehe allein um zivilrechtliche Fragen.

b. Sperrung von Pirate Bay

Im Juli 2009 entschied der *High Court* in Sachen Sperrung von „Pirate Bay“. Er verpflichtete Eircom per gerichtlicher Anordnung, den Zugang der Kunden zur Website von „Pirate Bay“ zu blockieren oder in anderer Weise abzuschalten.⁷⁴⁴ Das Gericht stützt diese Anordnung auf Section 40 (4) des *Copyright and Related Rights Act 2000*. Die Entscheidung erging nach Anhörung der klagenden Musikproduktionsgesellschaften. Eircom war vor Gericht zwar erschienen, hatte aber gemäß der im Vergleich getroffenen Abrede keine Erklärung abgegeben, also weder der Anordnung zugestimmt, noch dagegen Einwände erhoben. Im Zusammenhang mit der nachfolgend vorgestellten Entscheidung aus dem Oktober 2010 kehrte der *High Court* jedoch wegen Fehlens einer gesetzlichen Grundlage für diese Sperrung von der Entscheidung von 2009 ab.

c. Anordnungen zur Sperrung auf gesetzlicher Grundlage

Der Entscheidung aus dem Oktober 2010⁷⁴⁵ lag eine Klage der Musikkonzerne EMI, Sony, Universal, Warner und WEA zugrunde, mit der diese eine Anordnung gegen den Internet-service- Provider UPC Ltd. erwirken wollten, um Urheberrechtsverletzungen durch Filesharer zu unterbinden. Die Kläger verfolgten mit ihrem Vorgehen unter dem *Copyright and Related Rights Act 2000* zwei verschiedene Ziele.

- Zum einen beantragten sie eine Anordnung gemäß Section 37 und 40 (4) des *Copyright and Related Rights Act 2000*, die den Provider davon abhält, die von ihnen wahrgenommenen Urheberrechte dadurch zu verletzen, dass er der Allgemeinheit ohne ihre Zustimmung Kopien der betreffenden Werke über seinen Internetdienst zugänglich macht.
- Unbeschadet dessen beantragten die Kläger eine Anordnung nach Section 40 (4) des *Copyright and Related Rights Act 2000*, wonach UPC Ltd. den Zugang ihrer Abonnenten zur Website von „Pirate Bay“ blockieren oder in anderer Weise abschalten muss. Die Musikproduktionsgesellschaften beehrten dabei eine „Three-Strikes-Lösung“ entsprechend der Regelung im Vergleich mit Eircom.

⁷⁴⁴ EMI Records (Ireland) Ltd., Sony BMG Music Entertainment (Ireland) Ltd., Universal Music (Ireland) Ltd. and Warner Music (Ireland) Ltd. v. Eircom Plc., *Charleton J.*, 24.7.2009 [2009] IEHC 411.

⁷⁴⁵ EMI Records (Ireland) Ltd, Sony Music Entertainment Ireland Ltd, Universal Music Ireland Ltd, Warner Music Ireland Ltd and Wea International Inc v UPC Communications Ireland Ltd, *Charleton J.*, *High Court Commercial*, 11.10.2010, [2010] IEHC 377.

aa. Keine gesetzliche Grundlage im irischen Recht

Der *High Court* fand im irischen Recht keine gesetzliche Grundlage für eine gerichtliche Anordnung, den Zugang zu Websites zu blockieren oder abzuschalten, eine Datenübertragung zu unterbrechen oder umzuleiten oder den Zugang zum Internet abzutrennen. Das Gesetz lässt die genannten Maßnahmen nicht zu, sondern gestattet nach Section 40 (4) des *Copyright and Related Rights Act 2000* lediglich, einem Internet-Host-Service die Entfernung urheberrechtlich geschützten Materials von seinen Seiten aufzugeben.

Die EU-Richtlinie über den elektronischen Geschäftsverkehr 2000/31/EG sehe zwar Anordnungen gegen Urheberrechtsverletzungen vor. Zudem gestatte die Urheberrechtsrichtlinie 2001/29/EG den Inhabern der Urheberrechte, derartige Anordnungen gegen Diensteanbieter zu beantragen. Es sei aber Aufgabe der Mitgliedstaaten, Bedingungen und Modalitäten der Anordnungen festzulegen, was durch den irischen Gesetzgeber nicht erfolgt sei. Da es zum einen an einer gesetzlichen Grundlage fehle und das Gericht zum anderen nach dem Gewaltenteilungsgrundsatz das gesetzgeberische Unterlassen zu achten habe, wies der *High Court* die Anträge der klagenden Musikproduktionsgesellschaften zurück. Sein Urteil aus dem Jahr 2009, in dem es gegen Eircom Plc. die Sperrung des Zugangs zur Website von „Pirate Bay“ anordnete, hält das Gericht dagegen nunmehr für ausdrücklich falsch, weil eben keine gesetzliche Grundlage hierfür im irischen Recht existiere.

In Folge und in Reaktion auf diese Entscheidung hat die irische Regierung für Januar 2012 den Erlass einer Verordnung oder den Vorschlag einer gesetzlichen Regelung angekündigt, die den „Beanstandungen“ des High Court im Hinblick auf die Umsetzung europarechtlicher Vorgaben Rechnung tragen und es den Rechteinhabern ermöglichen soll, Internet Service Provider per gerichtlicher Anordnung zur Sperrung des Zugangs zu urheberrechtsverletzenden Internetseiten (wie *Pirate Bay*) zu zwingen.⁷⁴⁶ Weil bislang kein Regelungsentwurf vorgelegt worden ist und seitens der Musikindustrie Irlands befürchtet wird, dass ihre eigenen Ansprüche an Rechtsbehelfe zum Schutz der Urheberrechte im Internet nicht vollumfänglich befriedigt werden, haben nunmehr Vertreter der Musikindustrie den irischen Staat vor dem *High Court* wegen unzureichender Umsetzung europäischer Richtlinien verklagt.⁷⁴⁷

⁷⁴⁶ O`Halloran, Illegal downloading to be curbed by Government order, *The Irish Times* v. 19.12.2011, abrufbar unter: <http://www.irishtimes.com/newspaper/frontpage/2011/1219/1224309259318.html>; Government set to legislate against illegal downloading next month, veröffentlicht am 20.12.2011, abrufbar unter: <http://businessetc.thejournal.ie/government-set-to-legislate-against-illegal-downloading-next-month-309741-Dec2011/>; EMI Sues Irish State For Not Implementing Piracy Blocking Provisions, veröffentlicht am 12.1.2012, abrufbar unter: <http://torrentfreak.com/emi-sues-irish-state-for-not-implementing-piracy-blocking-provisions-120112/>.

⁷⁴⁷ Madden, IRMA lunches action against State over anti-piracy order, *Irish Times* v. 12.1.2012, abrufbar unter: <http://www.irishtimes.com/newspaper/finance/2012/0112/1224310141468.html>; McIntyre, More on the music industry case against Ireland, veröffentlicht am 12.1.2012, abrufbar unter: <http://www.tjmccintyre.com/2012/01/more-on-music-industry-action-against.html> (McIntyre spricht von einer konzertierten Aktion der großen Musikunternehmen, einschließlich Sony, Universal, Warner und WEA); ders., Music Industry v. Ireland, veröffentlicht am 11.1. 2012, abrufbar unter:

bb. Bestätigung der Entscheidung zum Eircom-Vergleich

Im Hinblick auf datenschutzrechtliche Fragen legte das Gericht aber Wert auf die Feststellung, dass das Ergebnis die Bewertung des Vergleichs/Protokolls zwischen den Musikproduktionsgesellschaften und Eircom im Hinblick auf die datenschutzrechtlichen Bestimmungen nicht betreffe und dass auch unter Berücksichtigung der neuen Erkenntnisse kein Grund für eine Abkehr von der Entscheidung aus dem April 2010⁷⁴⁸ bestehe. Der *High Court* bestätigte, dass die Ermittlung von unautorisierten Downloads urheberrechtlich geschützten Materials unter Nutzung von P2P-Technologie keine rechtlich beanstandbaren Auswirkungen auf die Privatsphäre und den Datenschutz habe.⁷⁴⁹

Zum einen erlangten die Musikproduktionsgesellschaften mit dem im Wesentlichen anonym ablaufenden Prozess der Aufdeckung keine Namen oder Adressen, die sie zur Datenverarbeitung, künftiger Kommunikation oder als Beweis in einem potentiellen Strafverfahren nutzen könnten, sondern nicht mehr als einen Satz von (IP-)Nummern.

Zum anderen würden mit der Kommunikation zwischen einem Produktionsunternehmen und einem Internetzugangsdiensteanbieter, dass zu einem bestimmten Datum und zu einer bestimmten Zeit unter der angegebenen IP-Adresse Urheberrecht verletzt worden sei, keine vertraulichen Informationen öffentlich gemacht.

Im Hinblick auf das Verhältnis zwischen dem Provider und seinen Kunden sei ausschließlich deren Vertragsbeziehung betroffen. Die Vollziehung eines Vertrages in Bezug auf Anti-Piraterie-Regelungen in den Vertragsbedingungen wirke sich nicht unzulässig auf die Privatsphäre des Kunden aus.

6. Zusammenfassung

In Irland ist, wie in Frankreich, bereits ein Warnhinweismodell etabliert. Allerdings wurde es dort im Rahmen eines gerichtlichen Vergleichs zwischen dem größten Zugangsanbieter

<http://www.tjmcintyre.com/2012/01/music-industry-sues-irish-state.html>; Out-Law.com, EMI takes Irish Government to court over website blocking delays, veröffentlicht am 16.1.2012, abrufbar unter: Weckler, Music industry launches new High Court action against state, The Daily Business Post, abrufbar unter:

<http://www.businesspost.ie/#!story/Agenda/Music/Music+industry+launches+new+High+Court+action+against+state/19410615-5218-4f0d-74f6-ef0c79393950>; heise online, Musikindustrie verklagt Irland wegen unzureichendem Copyright-Schutz, veröffentlicht am 12.1.2012, abrufbar unter: <http://www.heise.de/newsticker/meldung/Musikindustrie-verklagt-Irland-wegen-unzureichendem-Copyright-Schutz-1410422.html>.

⁷⁴⁸ *High Court* EMI Records (Ireland) Ltd., Sony B. G. Music Entertainment (Ireland) Ltd., Universal Music Ireland Ltd. and Warner Music Ireland Ltd. v. Eircom Ltd., *Charleton J.*, 16.4.2010, [2010] IEHC 108.

⁷⁴⁹ EMI Records (Ireland) Ltd, Sony Music Entertainment Ireland Ltd, Universal Music Ireland Ltd, Warner Music Ireland Ltd and Wea International Inc v UPC Communications Ireland Ltd, *Charleton J.*, *High Court Commercial*, 11.10.2010, [2010] IEHC 377, Rn. 68 ff.

Eircom und vier großen irischen Musikproduktionsgesellschaften vereinbart. Auch hier wird der Zugangsanbieter auf Meldungen der Rechteinhaber hin tätig. Nach mehrfacher fruchtloser Versendung von Warnhinweisen kann eine einjährige Anschlussperre verhängt werden. Auch in Irland existiert ein Auskunftsanspruch, der jedoch unverbunden neben dem Warnhinweismodell steht. Eircom betreibt mittlerweile in Kooperation mit den Rechteinhabern ein legales Musikangebot.

ENTWURF/ VERTRAULICH

IV. Finnland

Auch in Finnland lag ein Gesetzesentwurf zu einem Warnhinweismodell vor, der aber nicht beschlossen wurde.

1. Ausgangslage (Überblick)

Für das finnische Recht⁷⁵⁰ soll auf die urheberrechtliche Ausgangslage und auf aktuelle Rechtsprechung eingegangen werden.

a. Urheberrecht in Finnland

Nach **finnischem Urheberrecht**⁷⁵¹ steht dem Urheber eines Werkes im Hinblick auf dessen Verwertung grundsätzlich das ausschließliche Recht zu, über sein Werk durch Reproduktion, also Kopieren des Werks in jeder Form,⁷⁵² und durch öffentliche Zugänglichmachung zu verfügen.⁷⁵³ Ein Werk wird u. a. dann öffentlich zugänglich gemacht, wenn es der Öffentlichkeit drahtgebunden oder nicht drahtgebunden kommuniziert wird. Das schließt die Kommunikation in einer Weise mit ein, die es Mitgliedern der Öffentlichkeit ermöglicht, auf das Werk von einem Ort und zu einer Zeit ihrer Wahl Zugriff zu nehmen.⁷⁵⁴ Ein öffentliches Zugänglichmachen liegt auch vor, wenn eine Werkkopie öffentlich zum Verkauf angeboten oder auf andere Weise vertrieben wird.⁷⁵⁵ Das Urheberrecht Finnlands erlaubt u. a. die eigene Anfertigung einzelner Kopien zu privaten Zwecken gegen Kompensationsabgabe.⁷⁵⁶ Eine Ausnahme gilt, wenn das Werk rechtswidrig hergestellt oder rechtswidrig öffentlich zugänglich gemacht worden ist.⁷⁵⁷

b. Rechtsdurchsetzung

Zur Rechtsdurchsetzung kann der Rechteinhaber im Einzelfall im Wege gerichtlicher Anordnung Kontaktinformationen von einem Service Provider über einen Anschlussinhaber,

⁷⁵⁰ Der Verfasser dankt Herrn Professor Dr. Marcus Norrgård, LLD, Helsinki und Rechtsanwalt Tatu Kulmala, Turku.

⁷⁵¹ COPYRIGHT ACT 8.7.1961/404 (Amendments up to 31.10.2008/663 included) – Nicht offizielle Übersetzung ins Englische (20.4.2010). Im Folgenden: *Copyright Act*.

⁷⁵² Chapter 1 Section 2 (2) *Copyright Act*.

⁷⁵³ Chapter 1 Section 2 (1) *Copyright Act*.

⁷⁵⁴ Chapter 1 Section 2 (3) Nr. 1 *Copyright Act*.

⁷⁵⁵ Chapter 1 Section 2 (3) Nr. 3 *Copyright Act*.

⁷⁵⁶ Chapter 2 Section 12 (1), Chapter 2a Section 26a ff. *Copyright Act*.

⁷⁵⁷ Chapter 2 Section 11 (5) Satz 1 *Copyright Act*. Ausnahmen zu dieser Einschränkung bestehen etwa für bestimmte vorübergehende Vervielfältigungen nach Chapter 2 Section 11 (5) Satz 2 i. V. m. Chapter 2 Section 11a *Copyright Act*.

der möglicherweise Urheberrechte verletzt hat, erhalten.⁷⁵⁸ Dem schließen sich Durchsetzungsrechte an.⁷⁵⁹ Das Gericht kann nach Chapter 7 Section 60c *Copyright Act* auf Antrag des Rechteinhabers oder seines Repräsentanten gegenüber einem (Access) Service Provider anordnen (*injunction to discontinue*), die öffentliche Zugänglichmachung des angeblich urheberrechtsverletzenden Materials zu unterbrechen, falls dies im Hinblick auf den Rechteverletzer, den Diensteanbieter (Intermediär) oder den Urheber nicht unzumutbar erscheint.⁷⁶⁰

c. Rechtsprechung

aa. Zugangssperren

Die Rechtsprechung ordnet seit 2008 Zugangssperren nach Urheberrechtsverletzungen im Internet auf Grundlage von Section 60c des finnischen Urheberrechtsgesetzes an.⁷⁶¹

bb. Schadensersatz

Im Hinblick auf das Betreiben eines P2P-Netzwerkes hat der Oberste Gerichtshof Finnlands im Juni 2010 Schadensersatzansprüche wegen des Betriebs eines Dienstes („Finreactor“) zur nicht genehmigten Verbreitung und Vervielfältigung urheberrechtlich geschützten Materials bestätigt.⁷⁶²

2. Gescheiterter Entwurf eines Warnhinweismodells

In Finnland besteht derzeit kein Gesetz oder aktuelles Gesetzesvorhaben zu einer Warnhinweisregelung bei Urheberrechtsverletzungen im Internet.

⁷⁵⁸ Siehe Chapter 7 Section 60a *Copyright Act*. Section 60a (14.10.2005/821)

(1) *In individual cases, notwithstanding confidentiality provisions, an author or his representative shall be entitled, by the order of the court of justice, to obtain contact information from the maintainer of a transmitter, server or a similar device or other service provider acting as an intermediary about a tele-subscriber who, unauthorised by the author, makes material protected by copyright available to the public to a significant extent in terms of the protection of the author's rights.*

⁷⁵⁹ Siehe Chapter 7 Section 60b *Copyright Act*.

⁷⁶⁰ Section 60c (21.7.2006/679)

(1) *In trying a case referred to in section 60b, the court of justice may, upon the request of the author or his representative, order the maintainer of the transmitter, server or other device or any other service provider acting as an intermediary to discontinue, on pain of fine, the making of the allegedly copyright-infringing material available to the public (injunction to discontinue), unless this can be regarded as unreasonable in view of the rights of the person making the material available to the public, the intermediary and the author.*

⁷⁶¹ Siehe dazu unten S.172.

⁷⁶² Urteil vom 30.6.2010 Nr. 1396, KKO:2010:47 („Finreactor I“) und Urteil vom 30.6.2010 Nr. 1398, KKO:2010:48 („Finreactor II“). Siehe dazu eingehend *Mansala*, IRIS 2010-7:1/104.

a. Entwicklung bis Frühjahr 2011

Allerdings gab es einen Gesetzesentwurf der finnischen Regierung zur Änderung von § 60a (i) des Urheberrechtsgesetzes und des Gesetzes zum Schutz der Privatsphäre bei elektronischer Kommunikation⁷⁶³. Er wurde im Oktober 2010 in das Parlament eingebracht und mit dem Inkrafttreten der Gesetzesänderungen wurde für das Frühjahr 2011 gerechnet. Die geplante Regelung zielte zum einen darauf ab, die rechtswidrige Verbreitung von urheberrechtlich geschützten Inhalten zu reduzieren. Zum anderen sollten Rechteinhaber eine kostengünstigere Alternative zur gerichtlichen Rechtsdurchsetzung erhalten, die auch der Entlastung der nationalen Gerichte dienen sollte.⁷⁶⁴ Nach dem Modell sollten die Daten zur Feststellung der Identität des Anschlussinhabers bei dem Internet Service Provider verbleiben und dem Rechteinhaber nicht offengelegt werden.⁷⁶⁵

b. Inhalt des gescheiterten Entwurfs

Nach dem Entwurf war ein Diensteanbieter gesetzlich dazu verpflichtet, eine schriftliche Nachricht einer in Finnland aktiven Organisation zur Überwachung von Urheberrechten⁷⁶⁶ (*notice sender*) ohne Verzögerung an einen Kunden weiterzuleiten.⁷⁶⁷ Diese Pflicht zur „automatischen“ Weiterleitung setzte voraus, dass die Nachricht des *notice sender* in finnischer und schwedischer Sprache verfasst ist und den folgenden Inhalt hat:

- den Namen und Kontaktinformationen des *notice sender*,
- einen Hinweis, dass der Provider die Nachricht auf Verlangen des *notice sender* weiterleitet,
- eine Erklärung des *notice sender*, dass nach seinen Ermittlungen urheberrechtlich geschütztes Material unter Verletzung des *Copyright Act* öffentlich zugänglich gemacht worden ist,
- eine Erklärung des *notice sender*, über dessen Recht, namens solcher Urheber zu handeln, deren Werke zugänglich gemacht wurden, und

⁷⁶³ *Government`s Proposal 235 / 2010.*

⁷⁶⁴ Siehe Blog: File-Sharers To Receive Warning Letters, But No 3 Strikes (*enigmax*), veröffentlicht am 2.11.2010, abrufbar unter: <http://torrentfreak.com/file-sharers-to-receive-warning-letters-but-no-3-strikes-101102/>; Siehe Blog: Three Strikes, finnische Version (*cen*), veröffentlicht am 26.11.2010 abrufbar unter: <http://www.ip-notiz.de/three-strikes-finnische-version/2010/11/26/>.

⁷⁶⁵ Siehe Blog: File-Sharers To Receive Warning Letters, But No 3 Strikes (*enigmax*), veröffentlicht am 2.11.2011, abrufbar unter: <http://torrentfreak.com/file-sharers-to-receive-warning-letters-but-no-3-strikes-101102/> unter Zitierung des Regierungsministers *Jorma Walden*.

⁷⁶⁶ Z. B. das „*Copyright Information and Anti-Piracy Centre in Finland*“ (CIAPC). Dabei handelt es sich um eine seit langem existierende Non-Profit-Organisation, die sich den Schutz des *Copyright* zur Aufgabe macht. Siehe: <http://antipiracy.fi/inenglish/>.

⁷⁶⁶ Siehe *Müller*, Finnland: Warnmails für Urheberrechtsverletzer, veröffentlicht am 3.11.2010, abrufbar unter: <http://www.gulli.com/news/14632-finnland-warnmails-fuer-urheberrechtsverletzer-2010-11-03>.

⁷⁶⁷ Der Provider war dementsprechend dazu berechtigt, mit den Informationen zur Identifizierung des Anschlussinhabers so umzugehen, wie dies zur Weiterleitung der Nachricht notwendig ist.

- einen Hinweis zur Aufklärung auf der Website des Ministeriums für Erziehung und Kultur. Dort stehen Informationen über Urheberrechtsverletzungen und deren Vermeidung bereit.

Weitere Informationen hinsichtlich der vermeintlichen Rechtsverletzung durfte die Nachricht des *notice sender* nicht enthalten.

Um den Schutz personenbezogener Kundendaten zu gewährleisten, sollten die Provider gegenüber dem Rechteinhaber keine Angaben über die Identität der der IP-Adresse zugeordneten Person offenlegen dürfen. Begründet wurde dies damit, dass es sich bei dem Anschlussinhaber nicht notwendig um dieselbe Person handeln muss, der die Urheberrechtsverletzung zur Last gelegt wird. Zulässig sollte es aber sein, dass der Anschlussinhaber nach Erhalt des Hinweises mit dem *notice sender* in Kontakt tritt und seine Identität selbst offengelegt.⁷⁶⁸ Die mit der Weiterleitung dem Diensteanbieter entstehenden Kosten sollten nach dem Entwurf durch den *notice sender*, also von Rechteinhaberseite, erstattet werden. Der Gesetzesentwurf sah keine Sanktion, vor wie etwa eine Drosselung der Übertragungsrate oder eine Zugangssperre bei fortgesetzter Urheberrechtsverletzung.⁷⁶⁹

c. Diskussion des Vorschlags in Finnland

An dem Gesetzgebungsvorschlag wurde kritisiert, dass er mangels Sanktion für nicht effektiv gehalten wurde. Moniert wurde zudem, dass die Kosten des Systems den Rechteinhabern auferlegt werden sollten. Die Diensteanbieter lehnten die geplante Neuregelung hauptsächlich wegen der für sie damit verbundenen Einbindung in das System zum Vorgehen gegen Urheberrechtsverletzungen ab. Sie verwahrten sich grundsätzlich dagegen, Aufgaben in diesem Zusammenhang zu übernehmen, die auch für sie Aufwand bedeute und mit denen praktische Schwierigkeiten verbunden seien. Probleme sahen sie insbesondere im Zusammenhang mit der Identifizierung und Benachrichtigung der potentiellen Rechteverletzer. Das bestehende System zur Rechtsverfolgung wurde als effektiv und angemessen angesehen.

⁷⁶⁸ Insoweit kann die Regelung auch so empfunden werden, dass sie einen Anreiz gibt, Internet-Nutzer „in den Hinterhalt zu locken“.

⁷⁶⁹ Vgl. Müller, Finnland: Warnmails für Urheberrechtsverletzer, veröffentlicht am 3.11.2010, abrufbar unter: <http://www.gulli.com/news/14632-finnland-warnmails-fuer-urheberrechtsverletzer-2010-11-03> ; Siehe Blog: File- Sharers To Recieve Warning Letters, But No 3 Strikes (*enigmax*), veröffentlicht am 2.11.2010 abrufbar unter: <http://torrentfreak.com/file-sharers-to-receive-warning-letters-but-no-3-strikes-101102/>.

3. Weitere Entwicklung

a. Politische Entwicklung

Seit einem Regierungswechsel im April 2011 ist der Gesetzesentwurf hinfällig. Zurzeit ist unklar, wie es um die Zukunft von Warnhinweisen steht. Die konservative Partei ist im November 2011 zum zweiten Mal seit den Wahlen im April mit der Regierungsbildung gescheitert. Sozialdemokraten und die Linkspartei wollen nicht mehr an den Koalitionsverhandlungen mit der Partei des bisherigen Finanzministers sowie drei weiteren Fraktionen teilnehmen, so dass nunmehr Verhandlungen mit der liberalen Partei aufgenommen werden sollen.⁷⁷⁰ Das zuständige Ministerium für Erziehung und Kultur ist gegenwärtig mit einem Mitglied der Linkspartei besetzt, der vorherige Minister gehörte der moderat liberalen Volkspartei an.

b. Rechtsprechung

Die finnische Rechtsprechung hält Zugangssperren auch ohne vorherige Warnhinweise auf der Grundlage von Section 60c des finnischen Urheberrechtsgesetzes auch nach dem Scheitern des Warnhinweismodells für zulässig. In drei Verfahren aus dem Mai 2011 wurde ein Internet Service Provider per Anordnung dazu verpflichtet, den individuellen Zugang von Kunden zum Internet zu sperren, die illegal urheberrechtlich geschütztes Material in Filesharing-Netzwerken verbreitet hatten.⁷⁷¹ Nach dieser Rechtsprechung ist eine Zugangssperre zumutbar und verhältnismäßig, wenn ein signifikantes Ausmaß von Urheberrechtsverstößen vorliegt und dem Anschlussinhaber im Vertragsverhältnis zu seinem Provider rechtsmissbräuchliche Nutzungen untersagt sind.

4. Zusammenfassung

In Finnland stand bis zum Frühjahr 2011 ein Warnhinweismodell kurz vor der Einführung. Nach einem Regierungswechsel wurde es jedoch nicht verabschiedet. Der Ansatz sah eine

⁷⁷⁰ *Wiener Zeitung.at*, Finnland- Koalitionsverhandlungen erneut gescheitert, veröffentlicht am 2.6.2011, abrufbar unter: http://www.wienerzeitung.at/nachrichten/politik/europa/45098_Finnland-Koalitionsverhandlungen-erneut-gescheitert.html.

⁷⁷¹ *Teosto & IFPI v TeliaSonera*, *Helsinki District Court* 9.5.2011 nr 17230 (H 11/11165), nr 172228 (H 11/11018) und nr 172229 (H 11/11163). Zuvor grundlegend *Teosto & ÅKT v TeliaSonera*, *Helsinki District Court* 23.6.2008 nr 18661 (08/3008) (vor Klageerhebung hatten die Kläger gegenüber dem beklagten Provider eine Anordnung auf Mitteilung der Kontaktinformationen hinsichtlich der fraglichen IP-Adressen erwirkt). In den Verfahren aus dem Jahr 2011 ging es um 19.957, 21.174 bzw. 15.762 Musikwerke, die urheberrechtswidrig öffentlich zugänglich gemacht worden waren; das erste Verfahren aus dem Jahre 2008 betraf 10.058 Musikwerke, Siehe auch Blog: *Court Orders ISPs To Disconnect File-Sharers (enigmax)*, veröffentlicht am 29.6.2011, abrufbar unter: <http://torrentfreak.com/court-orders-isps-to-disconnect-file-sharers-110629/>. Ferner *ifpi „ISP Cooperation – Update“* (May 2011) mit dem Hinweis auf Verfahren aus 2008. Danach haben zwei Gerichte gegenüber ISPs eine Anordnung erlassen, die diese verpflichtet, den Internet-Zugang von „P2P-Uploadern“ mit hohem Datenvolumen auszusetzen.

reine Warnhinweisversendung ohne Sanktionen vor. Das finnische Recht kennt einen Auskunftsanspruch. Bemerkenswert ist, dass die Rechtsprechung in Finnland Zugangssperren in konkreten Fällen auf Basis des geltenden Rechts anordnet.

ENTWURF/ VERTRAULICH

V. Belgien

Die Einführung eines dem französischen System vergleichbaren abgestuften Sanktionsmodells wird auch vom belgischen Gesetzgeber diskutiert. Im Januar 2011 waren entsprechende Gesetzesvorschläge zum Schutz kultureller Werke im Internet (*Proposition de Loi favorisant la protection de la création culturelle sur Internet*) in die belgische Abgeordnetenkammer (*Chambre des Représentants de Belgique*) und den belgischen Senat (*Sénat de Belgique*) eingebracht worden.⁷⁷² Die beiden nahezu wortgleichen Entwürfe werden derzeit nach dem optionalen Zweikammersystem (*procédure bicamérale optionelle*, Art. 78 der belgischen Verfassung⁷⁷³) verhandelt.⁷⁷⁴ Die Entwürfe entsprechen ebenfalls nahezu wortgleich einem Vorschlag, der bereits einmal im Jahr 2010 vorgelegt worden war.⁷⁷⁵

1. Die Gesetzesentwürfe

Die Entwürfe sehen eine Reihe von Maßnahmen zur Verbesserung des Urheberrechtsschutzes im Internet vor. Sie setzen dabei verstärkt auf die Zusammenarbeit von Rechteinhabern, Zugangsdiensteanbietern und Betreibern von Internetportalen. Kern der Maßnahmen bildet der Vorschlag eines abgestuften Sanktionsmechanismus bei Urheberrechtsverstößen im Internet. Darüber hinaus stellt die Förderung legaler Angebote einen weiteren wesentlichen Aspekt der Entwürfe dar.

a. Das abgestufte Warnhinweisverfahren

Mit dem Ziel der Bekämpfung von Urheberrechtsverstößen im Internet wird im Rahmen der Gesetzesentwürfe ein mehrstufiges Verfahren vorgeschlagen. Dieses entspricht dem Ansatz nach dem französischen Modell, es ist jedoch im Hinblick auf die Abstufungen des Verfahrens weiterhin unterteilt. Die Einrichtung einer eigenständigen staatlichen Behörde zur Durchführung des Verfahrens ist nicht vorgesehen. Jedoch sollen spezielle, vom Ministerium beauftragte Bevollmächtigte (*agents commissionnés*) mit Ermittlungs- und Handlungsbefugnissen ausgestattet werden. In ihre Kompetenz sollen u.a. die Verhängung von

⁷⁷² Proposition de loi favorisant la protection de la création culturelle sur Internet, déposée par M. David Carnival et consorts à la Chambre des Représentants de Belgique, DOC 53 1120/001, abrufbar unter: <http://www.lachambre.be/FLWB/PDF/53/1120/53K1120001.pdf>; Proposition de loi favorisant la protection de la création culturelle sur Internet, déposée par M. Richard Miller au Sénat de Belgique, Document législatif n° 5-741/1, abrufbar unter: <http://www.senate.be/www/?MIval=/publications/viewPub.html&COLL=S&LEG=5&NR=741&VOLGNR=1&LANG=fr>.

⁷⁷³ In der koordinierten Fassung vom 17. Februar 1994, zuletzt geändert am 22.12.2008. Abrufbar unter: http://www.senate.be/deutsch/const_de.html.

⁷⁷⁴ Vgl. *Cannie*, Gesetzesentwurf für besseren Schutz kultureller Werke im Internet, IRIS 2011/5, S. 1.

⁷⁷⁵ Document législatif n° 4-1748/1, abrufbar unter: <http://www.senate.be/www/?MIval=/publications/viewPub.html&COLL=S&LEG=4&NR=1748&VOLGNR=1&LANG=fr>.

Geldbußen von bis zu 100 Euro und auch die Weitergabe des Sachverhalts an die Staatsanwaltschaft fallen.⁷⁷⁶

aa. Ausgangspunkt des Verfahrens

Ausgangspunkt des Verfahrens stellt Art. 14 des Gesetzentwurfs dar. Er enthält die Klarstellung, dass es jedem Internetnutzer untersagt ist, ohne Berechtigung Werke und Leistungen, die dem Schutz des Geistigen Eigentums unterliegen, im Internet zu verbreiten oder aus dem Internet herunterzuladen. Erfasst werden also primär der Download von Internetseiten mit illegalen Angeboten und der Datenaustausch, etwa mittels Filesharing.

bb. Ablauf des Verfahrens

Werden Verstöße hiergegen entdeckt, soll das Verfahren wie folgt ablaufen:

Wird ein erster Verstoß festgestellt, soll zunächst eine Verwarnung des Anschlussinhabers erfolgen (Art. 17 Nr. 1). Diese soll durch den Internetzugangsanbieter versendet werden und Informationen darüber enthalten, wann der festgestellte Verstoß erfolgte. Der Anschlussinhaber soll außerdem auf die gesetzlichen Bestimmungen und möglichen Sanktionen hingewiesen werden. Dem Anschlussinhaber sind zudem Kontaktdaten mitzuteilen, wo Einwendungen gegen die Verwarnung vorgebracht oder Informationen im Hinblick auf die streitgegenständlichen Inhalte erhalten werden können.

Kommt es innerhalb von sechs Monaten zu einem erneuten Verstoß, soll der Anschlussinhaber, in diesem Fall per Einschreiben, eine erneute Verwarnung erhalten (Art. 17 Nr. 2). Zudem soll ein Bußgeld von bis zu 100 Euro verhängt werden können. Der Anschlussinhaber soll hiergegen Einspruch einlegen können.

Erfolgen innerhalb von zwei Jahren weitere Verstöße, ist die Einschaltung der Staatsanwaltschaft vorgesehen (Art. 18). Als Sanktion soll eine Geldstrafe in Höhe von 100 bis zu 1.000 Euro verhängt werden können. Zudem kann vom Gericht eine Beschränkung der Internetkommunikation angeordnet werden. Der Internetanschluss soll danach zunächst nicht gänzlich gekappt, sondern nur der Zugang zum Breitbandinternet gesperrt werden. Erst wenn es innerhalb von drei Jahren zu einem weiteren Verstoß kommt, kann eine vollständige Sperrung des Internetzugangs erfolgen. Die Strafsumme kann sich dann verdoppeln. Der Vertrag mit dem Internetzugangsdiensteanbieter soll von der teilweisen oder gänzlichen Sperre nicht berührt werden; der Anschlussinhaber bleibt nach dem Entwurf weiter zur Zahlung des vertraglich vereinbarten Entgeltes verpflichtet (Artt. 18, 19).

⁷⁷⁶ Eine vergleichbare Konstruktion wurde im Rahmen des Gesetz vom 15. Mai 2007 betreffend Fälschungen und Piraterie des Geistigen Eigentums (*Loi du 15 mai 2007 relative à la contrefaçon et à la piraterie des droits de propriété intellectuelle*) eingeführt. Gesetz abrufbar unter:
http://www.ejustice.just.fgov.be/cgi_loi/loi_a.pl?sql=dt=%27loi%27&rech=1&cn=2007051559&caller=image_a1&language=fr&tri=dd+as+rank&fromtab=loi&numero=1&la=f&pdf_page=14&pdf_file=http://www.ejustice.just.fgov.be/mopdf/2007/07/18_1.pd.

Gerichtlich verhängte Sperren sind auch von anderen Internetdiensteanbietern zu beachten. Werden die Sperrauflagen, auch im Rahmen eines neu begründeten Vertrages über einen Internetzugang, nicht berücksichtigt, sollen gegen den betreffenden Diensteanbieter Geldstrafen in Höhe von 200 bis 2.000 Euro verhängt werden können (Artt. 20, 21).

b. Weitere Maßnahmen

Das vorgeschlagene Modell abgestufter Sanktionsmaßnahmen ist nur eine von fünf sogenannten „Säulen“ (*Pilier*), die in den Gesetzesentwürfen zum Schutz der Urheberrechte im Internet vorgeschlagen werden. Die weiteren vier Säulen sind:

aa. Maßnahmen gegen sog. Piraten-Seiten (Artt. 3, 4)

Die Zugangsdiensteanbieter sollen dabei stärker in die Pflicht genommen werden, bei der Bekämpfung illegaler Angebote im Internet mitzuwirken. Teilt der Zugangsdiensteanbieter ein illegales Angebot, über das er Kenntnis erlangt hat, der Staatsanwaltschaft nicht umgehend mit, sollen ihm zukünftig Strafen drohen.

bb. Förderung legaler Angebote im Internet und Aufklärung der Internetnutzer (Artt. 5, 6, 25)

Den Internetdiensteanbietern soll danach insbesondere die Pflicht auferlegt werden, bereits im Rahmen der Verträge mit ihren Kunden die Anschlussinhaber über die gesetzlichen Maßgaben aufzuklären, Hinweise zu geben zu Angeboten legaler Art sowie zur Sicherung des Internetanschlusses gegen den unberechtigten Zugriff Dritter und über mögliche Sanktionen und Auflagen bei Verstößen zu informieren (Art. 5).

Hierüber hinaus sehen die Gesetzesentwürfe vor, Werbepraktiken von Internetzugangsanbietern einzuschränken, bei denen mit der Möglichkeit des unbegrenzten Datentransfers über die angebotene Datenverbindung geworben wird (Art. 6).

Vorgeschlagen wird zudem die Einrichtung einer Internetseite, auf der ein Verzeichnis mit allen legalen Angeboten enthalten ist (Art. 26). Die Pflege dieser Datenbank soll dem sog. Rat zum Schutz von Urheberrechten (*Conseil de la protection des droits d'auteur*) überantwortet werden. Dem neu einzurichtenden Rat kommt nach den Gesetzesentwürfen im Übrigen vor allem beratende Funktion zu (Artt. 25 ff).

cc. Zurverfügungstellung urheberrechtlich geschützter Werke und Leistungen in Datenbanken (Artt. 7 ff.)

Zur Förderung des legalen Angebots von Werken im Internet sieht der Gesetzesvorschlag Maßnahmen zur Einrichtung von Datenbanken vor. Grundlage bildet die gesetzlich veran-

kerte Verpflichtung der Rechteinhaber und der Datenbankenbetreiber, sich über die Verwertung von Werken in Online-Angeboten zu einigen (Artt, 7, 11).

dd. Austausch urheberrechtlich geschützter Werke und Leistungen durch Zugangsdiensteanbieter (Artt. 12, 13)

Neben der Vereinbarung betreffend die öffentliche Zugänglichmachung von Werken zwischen Datenbankbetreibern und Rechteinhabern sehen die Entwürfe den Abschluss von Vereinbarungen zwischen den Rechteinhabern und den Diensteanbietern vor. Im Rahmen dieser Vereinbarungen sollen die Grenzen und Bedingungen abgesteckt werden, innerhalb derer die Anschlussinhaber zum Datentransfer berechtigt sein sollen.

2. Stand des Gesetzgebungsverfahrens

Zu dem eingebrachten Gesetzesvorschlag wurde im Mai 2011 im Finanz- und Wirtschaftsausschuss des Senats (*Commission des Finances et des Affaires économiques*), an den die Vorlage weiterverwiesen worden war, eine Expertenanhörung durchgeführt. Befragt wurden Wissenschaftler des Centre de Recherche Information, Droit et Société (CRIDS), Facultés Universitaires Notre-Dame de la Paix à Namur, ein Vertreter der Net Users' Rights Protection Association (NURPA), Vertreter der Verwertungsgesellschaften SACD-SCAM und SAJ, ein Vertreter der Künstlervereinigung SMartbe, ein Vertreter des Verbandes der Internetdiensteanbieter ISPA Belgium, Vertreter der Verbraucherorganisation Test-Achats sowie ein Vertreter der Künstlervereinigung SABAM.

Knapp zwei Wochen nach der Anhörung folgte ein Änderungsantrag, mit dem die Artt. 14 bis 24 des Gesetzesentwurfs, namentlich die Vorschriften zur Errichtung und Durchführung des Warnhinweisverfahrens, gestrichen werden sollten.⁷⁷⁷ Begründet wurde der Änderungsantrag unter Bezugnahme auf die zuvor durchgeführte Anhörung damit, dass das vorgeschlagene Warnhinweismodell nicht durchführbar erscheine. Vonseiten der Verwertungsgesellschaften sei ein solches Verfahren zudem nicht angefragt worden und seine Umsetzung nur möglich unter Verletzung der Persönlichkeitsrechte der Verbraucher.

3. Die Entscheidung in der Rechtssache Scarlet Extended/SABAM

Am 24. November 2011 wurde vom Europäischen Gerichtshof die Entscheidung⁷⁷⁸ in der Sache Scarlet Extended ./ SABAM erlassen. Sie betrifft nicht das weiterhin im Entwurf vorliegende Warnhinweismodell, wohl aber einen anderen Ansatz zur Bekämpfung von Internetpiraterie. Die belgische Verwertungsgesellschaft SABAM hatte gegen den Zugangsan-

⁷⁷⁷ Amendements déposée par Richard Miller/François Bellot, Document législatif n° 5-741/2, abrufbar unter: <http://www.senate.be/www/?Mlval=/publications/viewPub.html&COLL=S&LEG=5&NR=741&VOLGNR=2&LANG=fr>.

⁷⁷⁸ Scarlet Extended, Az. C-70/10.

bieter Scarlet ein Urteil erwirkt, wonach dieser unter Androhung eines Zwangsgelds und mit einer Frist von sechs Monaten dazu verpflichtet war, Urheberrechtsverletzungen zu verhindern. Dazu sollte der Anbieter das Senden und Empfangen von Musikfiles über Peer-to-Peer-Netzwerke präventiv überwachen und auf seine Kosten ein Filter- und Sperrsystem für elektronische Übermittlungen einrichten. Der *Cour d'appel de Bruxelles* reichte in dieser Sache im Januar 2010 ein Vorabentscheidungsersuchen nach Art. 267 AEUV ein, das sich mit der Zulässigkeit des Filter- und Sperrsystems befasste. Der Generalanwalt *Cruz Villalón* verwies in seinem Schlussantrag aus April 2010 hinsichtlich der Zulässigkeit des Modells, das mit den EU-Grundrechten aus Art. 8 (Schutz personenbezogener Daten) und 11 (Meinungsäußerungs- und Informationsfreiheit) der EU-Grundrechtecharta in Konflikt geraten könne, auf die Ausgestaltungsbefugnisse in den gesetzlichen Grundlagen der Mitgliedstaaten. Den ISP allein und auf seine eigenen Kosten für das Unterbinden von Rechtsverstößen per Filter- und Sperrsystem verantwortlich zu machen, sei aber neu, sehr ungewöhnlich und auf Grundlage der gesetzlichen Regelung in Belgien nicht mit dem EU-Recht vereinbar, so Pedro in seinem Antrag im April 2011.

Der EuGH bestätigt diese Auffassung und erklärt das einseitige Modell für europarechtswidrig. Eine umfassende und präventive Verpflichtung des Providers, Inhalte im "Peer-to-Peer"-Verkehr des Kunden zu identifizieren, illegale Dateien herauszufiltern, die Handelnden zu ermitteln und danach gegebenenfalls Datenverkehr zu sperren, sei aus verschiedenen Gründen europarechtswidrig. Die Probleme einer aktiven Überwachung sah das Gericht maßgeblich in Verstößen gegen die Informationsfreiheit und das Datenschutzrecht der Nutzer. Zugleich betont der Gerichtshof in dieser Entscheidung aber die Bedeutung des „Schutzes des Rechtes am Geistigen Eigentum“, das nach dem Recht der Europäischen Union zum Eigentum gehört, und bestätigt seine Rechtsprechung aus der Entscheidung *Promusicae*⁷⁷⁹ aus dem Januar 2008. Zugleich bekräftigt er die in der Entscheidung *L'Oréal*⁷⁸⁰ betonte Befugnis der nationalen Gerichte, den Zugangsanbietern Maßnahmen aufzugeben, die einen effektiven Urheberrechtsschutz in den Mitgliedstaaten gewährleisten. Ausdrücklich weist der EuGH auch darauf hin, dass den Providern präventive und repressive Maßnahmen zur Eindämmung von Rechtsverletzungen aufgegeben werden können. Sie seien unter Abwägung der Eigentümerinteressen der Rechteinhaber und der unternehmerischen Freiheit der Provider zu treffen. Insoweit lehnt der EuGH einseitige Lösungen zugunsten der Rechteinhaber oder der Provider ab.

⁷⁷⁹ Az. C-275/06.

⁷⁸⁰ *L'Oréal* u. a., V. 12. Juli 2011, C-324/09, Slg. 2011, Randnr. 131.

4. Zusammenfassung

Auch in Belgien wird ein Warnhinweismodell diskutiert, das ein abgestuftes Modell vorsieht, bei dem Provider Warnhinweise versenden sollen, deren Nichtbeachtung zunächst die Drosselung von Anschlüssen und schließlich auch deren Sperrung zur Folge haben soll.

VI. Schweden

1. Ausgangssituation

Schweden⁷⁸¹ gehört weltweit zu den zehn Ländern mit der höchsten Verbreitung von Breitbandanschlüssen und dem Anteil an Glasfasernetzen.⁷⁸² Die allgemeine Internetnutzung begann in Schweden vergleichsweise früh und in Folge eines nicht hinreichend geschützten nationalen Urheberrechts entwickelte sich Online-Piraterie rasant und führte nach Angaben der Rechteinhaber zu einem Rückgang der Verkaufszahlen.⁷⁸³

2. Urheberrecht

Das schwedische Urheberrecht ist im Gesetz 1960:729 über Urheberrechte an Werken der Literatur und Kunst⁷⁸⁴ (im Folgenden: Urheberrechtsgesetz) verankert. Es basiert auf dem Grundsatz, dass dem Urheber das ausschließliche moralische und wirtschaftliche Recht an der Verwertung seines Werks zusteht. Ausnahmen sind nur zum Zwecke der Befriedigung religiöser, kultureller oder sozialer Bedürfnisse zulässig.⁷⁸⁵

§ 2 Urheberrechtsgesetz bestimmt:

„Unbeschadet der in diesem Gesetz nachfolgend vorgesehenen Beschränkungen umfasst das Urheberrecht das ausschließliche Recht, das Werk zu verwerten; es erfasst dabei das Recht der Vervielfältigung sowie das Recht, das Werk öffentlich wiederzugeben, sei es in seiner ursprünglichen oder in einer veränderten Form, umgestaltet oder angepasst, in einer anderen literarischen oder künstlerischen Art und Weise oder auf anderem technischen Wege. {...}“⁷⁸⁶

⁷⁸¹ Der Verfasser dankt Herrn Rechtsanwalt Henrik Bengtsson, Stockholm.

⁷⁸² Adermon/Liang, S. 5.

⁷⁸³ IFPI, DMR 2011, S. 11.

⁷⁸⁴ Lag [1960:729] om upphovsrätt till litterära och konstnärliga verk.

⁷⁸⁵ Ullberg in „Die Zulässigkeit einer Kulturfltrate nach nationalem und europäischem Recht“ vom 13.3.2009, Kurzgutachten des Instituts für Europäisches Medienrecht (EMR) in Zusammenarbeit mit der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel, im Auftrag der Bundestagsfraktion BÜNDNIS 90/DIE GRÜNEN und Fraktion der Grünen/Freie Europäische Allianz im Europäischen Parlament, S. 40.

⁷⁸⁶ Übersetzung: Ullberg in „Die Zulässigkeit einer Kulturfltrate nach nationalem und europäischem Recht“ vom 13.3.2009, Kurzgutachten des Instituts für Europäisches Medienrecht (EMR) in Zusammenarbeit mit der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel, im Auftrag der Bundestagsfraktion BÜNDNIS 90/DIE GRÜNEN und Fraktion der Grünen/Freie Europäische Allianz im Europäischen Parlament, S. 41.

Wie der dortige Gesetzgeber bei Implementierung der InfoSoc-Richtlinie⁷⁸⁷ ausdrücklich klargestellt hat, ist der Austausch urheberrechtlich geschützter Inhalte via P2P-Filesharing von Art. 2 des Urheberrechtsgesetzes erfasst und damit illegal⁷⁸⁸. In Umsetzung der Enforcement-Richtlinie⁷⁸⁹ wurden weitere Bestimmungen in das Urheberrechtsgesetz aufgenommen, die am 1. April 2009 in Kraft traten. Die Gesetzesänderung wurde als bedeutender Schritt in Richtung einer besseren Verfolgung von Urheberrechtsverletzungen im Internet angesehen. In etwa demselben Zeitraum wurden die Betreiber von „Pirate Bay“ gerichtlich wegen Urheberrechtsverstößen verurteilt⁷⁹⁰ und es kam zu einer Einstellung von mehreren BitTorrent-Diensten.⁷⁹¹ Zugleich etablierte sich Spotify⁷⁹² in Schweden zu einem legalen Online-Musikanbieter.⁷⁹³

Die in Umsetzung der Enforcement-Richtlinie⁷⁹⁴ erlassene Neuregelung, war nicht die erste Reform im Hinblick auf Filesharing, wurde aber öffentlich mehr wahrgenommen und als weitreichender empfunden als vorangegangene Reformen.⁷⁹⁵ Es wurde erwartet, dass aufgrund dieser Reform und dem mit großem öffentlichen Interesse verfolgten Verfahren gegen die Betreiber der Webseite „The Pirate Bay“, ein starker Abschreckungseffekt im Hinblick auf Internet-Piraterie erzeugt werde.⁷⁹⁶

Die schwedische Bevölkerung war überwiegend gegen das Gesetz, was sich bei den schwedischen Wahlen zum Europäischen Parlament am 7. Juni 2009 niederschlug, wo die schwedische Piratenpartei 7 Prozent der Wählerstimmen erlangte und sich einen Sitz im Europäischen Parlament sicherte.⁷⁹⁷

a. Auskunftsanspruch

Im Rahmen der Gesetzesänderung⁷⁹⁸ wurde in § 53c Urheberrechtsgesetz ein Auskunftsanspruch der Rechteinhaber eingeführt, nach dem eine gerichtliche Anordnung zur Auskunftserteilung gegen u.a. die Zugangsanbieter ergehen kann. Dort heißt es:

⁷⁸⁷ Richtlinie 2001/29/EG vom 22.5.2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft.

⁷⁸⁸ Vgl. § 2 *Lag [1960:729] om upphovsrätt till litterära och konstnärliga verk*.

⁷⁸⁹ Richtlinie 2004/48/EG vom 29.4.2004 zur Durchsetzung der Rechte des geistigen Eigentums.

⁷⁹⁰ *JFPI*, DMR 2011, S. 11.

⁷⁹¹ *JFPI*, DMR 2011, S. 11.

⁷⁹² Spotify ist eine voll lizenzierte Musik-Streaming-Software mit der Nutzer auf über 13 Mio. Songs zugreifen können. Die Lizenzgebühren werden über zwei Wege finanziert: Entweder der Nutzer bezahlt sein Konto mit einem Abonnement oder er akzeptiert Werbeeinblendungen. Derzeit lässt sich ein Konto für Spotify in Schweden, Norwegen, Dänemark, Finnland, Großbritannien, Frankreich, Spanien, den Niederlanden und den Vereinigten Staaten anlegen.

⁷⁹³ *JFPI*, DMR 2011, S. 11.

⁷⁹⁴ Richtlinie 2004/48/EG vom 29.4.2004 zur Durchsetzung der Rechte des geistigen Eigentums.

⁷⁹⁵ *Adermon/Liang*, S. 6.

⁷⁹⁶ *Adermon/Liang*, S. 6.

⁷⁹⁷ *Adermon/Liang*, S. 6.

⁷⁹⁸ *Lag [1960:729] om upphovsrätt till litterära och konstnärliga verk*.

„Macht der Antragsteller glaubhaft, dass ein Dritter das Urheberrecht an einem der in § 53 genannten Werke verletzt hat, kann das Gericht unter Androhung eines Zwangsgelds die in Abs. 2 genannte(n) Person(en) dazu verpflichten, Auskunft über den Ursprung und die Vertriebswege der Waren oder Dienstleistungen zu geben, die von der Rechtsverletzung betroffen sind (Verfügung auf Auskunft). Eine solche Maßnahme kann auf Antrag des Rechtsinhabers, seines Vertreters oder desjenigen angeordnet werden, dem ein gesetzliches Verwertungsrecht an dem Werk zusteht. Sie darf nur angeordnet werden, wenn die Auskunft die Untersuchung der Rechtsverletzung hinsichtlich der Waren oder Dienstleistungen erleichtern kann.

Zur Auskunft ist verpflichtet, wer

[...]

in gewerblichem Ausmaß eine für die Rechtsverletzung genutzte elektronische Kommunikations- oder andere Dienstleistung erbracht hat

[...].⁷⁹⁹

§ 53d des schwedischen Urheberrechtsgesetzes schränkt diesen Anspruch ein und bestimmt:

„Eine Verfügung auf Auskunft darf nur erlassen werden, wenn die Gründe für die Maßnahme die Ungelegenheiten oder anderen Nachteile aufwiegen, die die Maßnahme für denjenigen, gegen den sie sich richtet, oder für andere entgegenstehende Interessen mit sich bringt.

[...]

Das Gesetz 1998:204⁸⁰⁰ über personenbezogene Daten beschränkt die Verarbeitung dieser Angaben.⁸⁰¹

Das Gesetz über personenbezogene Daten (im Folgenden Datenschutzgesetz) bestimmt, dass personenbezogene Daten grundsätzlich nur dann verarbeitet werden dürfen, wenn die betroffene Person zuvor eingewilligt hat oder die Verarbeitung aufgrund spezieller Regelungen des Datenschutzgesetzes erlaubt ist. Insoweit heißt es in § 10 Datenschutzgesetz:

„Persönliche Daten dürfen nur verarbeitet werden, wenn die hiervon betroffene Person in die Verarbeitung eingewilligt hat oder wenn diese erforderlich ist

⁷⁹⁹ Übersetzung aus den Schlussanträgen des Generalanwalts *Niilo Jääskinen* vom 17.11.2011 in der Rechtssache C-461/10 – *Bonnier u.a./ePhone*.

⁸⁰⁰ *Personuppgiftslag (1998:204)*.

⁸⁰¹ Übersetzung aus den Schlussanträgen des Generalanwalts *Niilo Jääskinen* vom 17.11.2011 in der Rechtssache C-461/10 – *Bonnier u.a./ePhone*.

für die Erfüllung eines Vertrages zwischen dem Betroffenen und der verantwortlichen Stelle oder zur Durchführung von vorvertraglichen Maßnahmen, die durch den Betroffenen veranlasst worden sind;

für die Wahrnehmung rechtlicher Verpflichtungen durch die verantwortliche Stelle;

für die Wahrung lebenswichtiger Interessen des Betroffenen;

für die Wahrung eines wichtigen öffentlichen Interesses;

für die Erfüllung solcher Pflichten, die sich für die verantwortliche Stelle oder einen Dritten, dem die persönlichen Daten weitergeleitet werden, in Wahrnehmung öffentlicher Aufgaben ergeben;

zu Zwecken, die berechnigte Interessen der verantwortlichen Stelle oder eines Dritten betreffen, dem die Daten zur Befriedigung von Ansprüchen weitergeleitet werden, sofern die Interessen des Dritten schwerer wiegen als das Schutzbedürfnis der betroffenen Person gegen Verletzungen ihrer persönlichen Integrität.⁸⁰²

§ 21 des Datenschutzgesetzes verbietet anderen, als behördlichen Parteien, die Verarbeitung solcher persönlicher Daten, die strafrechtlich relevante Gesetzesverstöße, strafgerichtliche Verurteilungen, strafverfahrensrechtliche Zwangsmaßnahmen oder behördlich angeordnete Freiheitsbeschränkungen betreffen. Die Datenkontrollbehörde, der die Überwachung der Nutzung personenbezogener Daten obliegt, kann von diesem Verbot u.a. dann Ausnahmen zulassen, wenn die damit verfolgten Zwecke die berechtigten Interessen der verantwortlichen Stelle oder eines Dritten betreffen, dem die Daten zur Befriedigung von Ansprüchen weitergeleitet werden, sofern die Interessen des Dritten schwerer wiegen, als das Schutzbedürfnis der registrierten Person gegen Verletzungen ihrer persönlichen Integrität.

Solche Ausnahmen wurden zugunsten der Musikverbände (IFPI Svenska Gruppen⁸⁰³) und der Antipiraterieorganisation *Antipiratbyrå*⁸⁰⁴ gewährt und entsprechende Genehmigungen zur Erhebung personenbezogener Daten zum Zwecke der Bekämpfung illegalen Filesharings im Interesse ihrer Auftraggeber erteilt.⁸⁰⁵ Diese Genehmigungen waren allerdings auf Einzelfälle beschränkt und zeitlich begrenzt. Sie wurden der IFPI und der *Antipiratbyrå* zu dem Zweck erteilt, IP-Adressen von Anschlussinhabern, die dem Filesharing verdächtig wurden, zu verarbeiten.⁸⁰⁶

⁸⁰² Übersetzung: Ullberg in „Die Zulässigkeit einer Kulturflatrate nach nationalem und europäischem Recht“ vom 13.3.2009, Kurzgutachten des Instituts für Europäisches Medienrecht (EMR) in Zusammenarbeit mit der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel, im Auftrag der Bundestagsfraktion BÜNDNIS 90/DIE GRÜNEN und Fraktion der Grünen/Freie Europäische Allianz im Europäischen Parlament, S. 48.

⁸⁰³ *International Federation of the Phonographic Industry*, abrufbar unter: <http://www.ifpi.se/>.

⁸⁰⁴ Eine schwedische Antipiraterie-Organisation, vgl. <http://www.antipiratbyran.com/>.

⁸⁰⁵ Regierungsbericht Dnr 1631-2006 und Dnr 1632-2006.

⁸⁰⁶ Ullberg in „Die Zulässigkeit einer Kulturflatrate nach nationalem und europäischem Recht“ vom 13.3.2009, Kurzgutachten des Instituts für Europäisches Medienrecht (EMR) in Zusammenarbeit mit der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel, im Auftrag der Bundestagsfraktion

Darüber hinaus sieht Kapitel 6, § 20 Abs. 1 des Gesetzes 2003:389⁸⁰⁷ über elektronische Kommunikation, das die E-Datenschutzrichtlinie⁸⁰⁸ in das nationale Recht umsetzt, vor, dass derjenige, der im Zusammenhang mit der Bereitstellung eines elektronischen Kommunikationsnetzes oder eines elektronischen Kommunikationsdienstes Angaben über Teilnehmer erhalten oder Zugang zu ihnen erlangt hat, diese nicht unbefugt weitergeben oder benutzen darf. Diese u.a. für die Zugangsanbieter geltende Verschwiegenheitspflicht ist so ausgestaltet, dass sie nur ein Verbot enthält, bestimmte Informationen unbefugt weiterzugeben oder zu nutzen. Sie ist damit anderen Bestimmungen untergeordnet, nach denen die Informationen weitergegeben werden dürfen, so dass die Weitergabe dann nicht unbefugt ist.⁸⁰⁹ Im Gesetzgebungsverfahren war davon ausgegangen worden, dass der Auskunftsanspruch keine speziellen Gesetzesänderungen erforderlich mache, da die neuen Bestimmungen dem Grundsatz der Verschwiegenheitspflicht vorgehen.⁸¹⁰ Aufgehoben werden kann die Verschwiegenheitspflicht im Hinblick auf die Auskunftserteilung also im Ergebnis durch richterliche Anordnung.⁸¹¹

b. Durchsetzung des Auskunftsanspruchs

aa. Speicherpflicht der Zugangsanbieter

Im April 2009 erklärten sich mehrere schwedische Provider⁸¹² bereit, die gespeicherten IP-Daten zu löschen, um der Gefahr zu begegnen, dass Anschlussinhaber aufgrund der neuen Rechtslage verfolgt würden.⁸¹³ Das Vorhaben scheiterte jedoch, weil die marktführenden dortigen Zugangsanbieter⁸¹⁴ ihre Mitwirkung verweigerten.⁸¹⁵

Nach schwedischem Recht sind Zugangsanbieter nicht verpflichtet Daten zu speichern, die benötigt werden, um eine IP-Adresse einem Anschlussinhaber zuzuordnen. Die Richtlinie 2006/24/EG über die **Vorratsspeicherung** von Daten⁸¹⁶, die in Schweden eine heftige poli-

tion BÜNDNIS 90/DIE GRÜNEN und Fraktion der Grünen/Freie Europäische Allianz im Europäischen Parlament, S. 48.

⁸⁰⁷ Lag [2003:389] om elektronisk kommunikation.

⁸⁰⁸ Richtlinie 2002/58/EG vom 12.07.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (zuletzt geändert durch die Richtlinie 2009/136/EG), abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:DE:PDF>; dazu oben Kapitel „Die datenschutzrechtlichen Probleme von Warnhinweismodellen“.

⁸⁰⁹ Schlussanträge des Generalanwalts *Niilo Jääskinen* vom 17.11.2011 in der Rechtssache C-461/10 – Bonnier u.a./ePhone.

⁸¹⁰ Nach den Angaben des Obersten Gericht Schwedens (*Högsta domstol*) in der Rechtssache C-461/10, das sich dabei auf den Vorschlag 2008/09:67, S. 143 bezieht, vgl. Schlussanträge des Generalanwalts *Niilo Jääskinen* vom 17.11.2011 in der Rechtssache C-461/10 – Bonnier u.a./ePhone.

⁸¹¹ So das in der Rechtssache C-461-10 vorliegende Oberste schwedische Gericht, vgl. Generalanwalts *Niilo Jääskinen* vom 17.11.2011 in den Schlussanträgen zur Rechtssache C-461/10 – Bonnier u.a./ePhone.

⁸¹² Bahnhof, Alltele und Tele2.

⁸¹³ *Adermon/Liang*, S. 6.

⁸¹⁴ Telia Sonera, Bredbandsbolaget und Com Hem.

⁸¹⁵ *Adermon/Liang*, S. 6.

⁸¹⁶ Richtlinie 2006/24/EG vom 15.3.2006 zur Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung

tische Debatte auslöste, wurde nicht in nationales Recht umgesetzt. Der Umsetzungsentwurf des Gesetzgebers wurde von einer parlamentarischen Minderheit blockiert. Auch im Bereich der **Telekommunikation**, die im Gesetz 2003:389⁸¹⁷ über elektronische Kommunikation geregelt ist, ist keine gesetzliche Pflicht zur Speicherung bestimmter Daten normiert. Kapitel 6 des Gesetzes, welches die Privatsphäre im Bereich der Telekommunikation regelt, bestimmt jedoch, dass die Zugangsanbieter Daten nur dann weitergeben dürfen, soweit sie Straftaten betreffen, die mit Freiheitsstrafe belegt sind (§ 22).

bb. Überprüfung des Auskunftsanspruchs durch den EuGH (Bonnier Audio AB/ePhone)

Es gibt derzeit vor dem schwedischen Obersten Gerichtshof Auskunftsverfahren⁸¹⁸, die bislang nicht entschieden sind, weil der Oberste Gerichtshof diesbezüglich ein Vorabentscheidungsersuchen in der Rechtssache **Bonnier Audio AB/ePhone**⁸¹⁹ an den EuGH gerichtet hat. Gegenstand dieser Vorabentscheidung ist die Frage, ob die Richtlinie 2006/24/EG⁸²⁰ der Anwendung einer nationalen Vorschrift entgegenstehe, nach der in einem zivilrechtlichen Verfahren einem Internetdienstleister zu dem Zweck, einen bestimmten Teilnehmer identifizieren zu können, aufgegeben werden kann, einem Urheberrechtinhaber oder dessen Vertreter Auskunft über den Teilnehmer zu geben, dem der Internetdienstleister eine bestimmte IP-Adresse zugeteilt hat, über die die Verletzung begangen worden sein soll. Dabei sei davon auszugehen, dass der Antragsteller glaubhaft gemacht hat, dass eine Urheberrechtsverletzung vorliegt und die Maßnahme verhältnismäßig ist.

Das vorlegende Gericht war trotz des Urteils *Promusicae*⁸²¹ rechtlich unsicher, ob das Unionsrecht der Anwendung des § 53c Urheberrechtsgesetz entgegensteht, da dort auf die Richtlinie 2006/24/EG, mangels zeitlicher Anwendbarkeit, nicht Bezug genommen worden war.⁸²²

Eine Entscheidung des EuGH ist in dieser Sache im Dezember 2011 nicht ergangen. Der Generalanwalt hat in seinen Schlussanträgen⁸²³ aus dem November 2011 die Ansicht vertreten, dass das Ausgangsverfahren nicht in den sachlichen Anwendungsbereich der Richt-

der Richtlinie 2002/58/EG, abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:DE:PDF>.

⁸¹⁷ *Lag [2003:389] om elektronisk kommunikation*.

⁸¹⁸ Az.: Ö 4817-09.

⁸¹⁹ Rechtssache C-461/10.

⁸²⁰ Richtlinie 2006/24/EG vom 15.3.2006 zur Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:DE:PDF>.

⁸²¹ *EuGH*, Urteil vom 29.1.2008 – C 275/06 in GRUR 2008, 241 – *Promusicae/Telefónica*.

⁸²² Schlussanträge des Generalanwalts in der Rechtssache C-461-10, abrufbar unter: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=114613&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=13661>.

⁸²³ Schlussanträge des Generalanwalts in der Rechtssache C-461-10, abrufbar unter: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=114613&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=13661>.

linie 2006/24/EG falle. Diesem liege ein zivilrechtliches Verfahren zugrunde und die Daten seien nicht von einer nationalen Behörde sondern von Privatpersonen begehrt worden. Die Richtlinie solle sicherstellen, dass

“die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten {...} zur Verfügung stehen” (Art. 1 2006/24/EG).

Im Ergebnis stünde die Richtlinie der Anwendung einer entsprechenden nationalen Vorschrift somit nicht entgegen. Die Speicherung der für die Auskunftserteilung benötigten Daten auf Vorrat, müsse im Hinblick auf ihre Weitergabe und Verwendung zu diesem Zweck jedoch aufgrund detaillierter nationaler Rechtsvorschriften erfolgen, die unter Beachtung der für den Schutz personenbezogener Daten geltenden unionsrechtlichen Bestimmungen erlassen worden sind.⁸²⁴

cc. Effizienz des Auskunftsanspruchs

Zur Wirkung der Gesetzesänderung in Schweden liegt eine Studie vor.

1) *Rückgang von Datenverkehr*

Bezüglich der Auswirkungen des Auskunftsanspruchs auf Musik- und Filmverkäufe in Schweden liegt eine Studie von *Adermon* und *Liang* (2010) vor. Sie untersucht die Änderungen des Datenverkehrs seit Inkrafttreten der Neuregelungen im Urheberrechtsgesetz und gelangt zu dem Ergebnis, dass der Datenverkehr in Schweden mit dem Inkrafttreten dieser Vorschriften zum 1. April 2009 um 40 Prozent sank und bis Ende 2009 nicht mehr das Volumen zum Zeitpunkt vor der Reform erreichte.⁸²⁵ Zum Vergleich wurde der Datenverkehr in Norwegen und Finnland untersucht, wo die Bedingungen denen in Schweden bis auf die neue Gesetzeslage sehr ähnlich sind. In den Vergleichsstaaten war kein vergleichbarer Rückgang des Datenverkehrs zu messen.⁸²⁶

Da die Reform nur Internetpiraterie im Fokus hatte, halten *Adermon* und *Liang* die Abschreckungswirkung der neuen Gesetzeslage für die alleinige Ursache des Rückgangs des Datenverkehrs in Schweden.⁸²⁷

2) *Positive Auswirkungen auf das Piraterieverhalten*

Der Rückgang des Datenverkehrs wirkte sich positiv auf den Verkauf von Musikprodukten aus. Im Zeitraum nach der Gesetzesänderung stieg der Verkauf von Musik auf physischen Tonträgern um 0,72 Prozent an. Bei digitaler Musik war es sogar ein Anstieg von 1,31 Pro-

⁸²⁴ Schlussanträge des Generalanwalts in der Rechtssache C-461-10, abrufbar unter: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=114613&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=13661>.

⁸²⁵ *Adermon/Liang*, S. 3.

⁸²⁶ *Adermon/Liang*, S. 8.

⁸²⁷ *Adermon/Liang*, S. 3.

zent.⁸²⁸ Für Kinobesuche und DVD-Verkäufe beobachteten *Adermon* und *Liang* keinen vergleichsweise nennenswerten Anstieg der Verkaufszahlen.⁸²⁹ Anhand dieser Zahlen gelangte die Studie zu dem Ergebnis, dass die Verkäufe von physischen Musikträgern 72 Prozent höher wären, wenn es keine Piraterie-Angebote gäbe. Dies mache 43 Prozent des Rückgangs der Verkaufszahlen in den Jahren zwischen 2000 und 2008 in Schweden aus.⁸³⁰ Der Datenverkehr sei über einen Zeitraum von sechs Monaten nach der Gesetzesänderung um 18 Prozent zurückgeblieben. Physische Verkäufe von Musik seien um 27 Prozent und digitale Musikverkäufe um 48 Prozent angestiegen. Auswirkungen auf den Verkauf von Kinokarten oder DVDs seien hingegen nicht erkennbar gewesen.⁸³¹

Adermon und *Liang* schlussfolgern aus diesen Ergebnissen, dass illegale Musik ein starkes Substitut für legale Musik sei, während sich dies bei Filmen nicht feststellen ließe. Die Abnahme des rechtsverletzenden Verhaltens habe zu einer verstärkten Nachfrage nach legaler Musik geführt. Nach sechs Monaten war das Aufkommen an rechtsverletzendem Verhalten aber wieder auf dem Level vor der Reform und legale Musik wurde weniger nachgefragt, vor allem auf physischen Tonträgern. Im Bereich digitaler Musik wuchs die Nachfrage weiter, was darauf hindeute, dass die Migration zu diesem Markt permanent sei.⁸³² Die Rechteinhaber nehmen an, dass sich die Nutzer nach neuen legalen Angeboten umgeschaut haben und dabei Spotify als echte langfristige Alternative zur Piraterie entdeckten.⁸³³

Weitere Untersuchungen im Mai 2010 ergaben, dass **52 Prozent** der illegalen Filesharer angaben, sie hätten ihre Aktivität aufgrund der neuen Rechtslage **reduziert**; nur acht Prozent gaben an, sie würden mehr Filesharing betreiben als zuvor.⁸³⁴ Etwa ein Drittel der Nutzer (34 Prozent) gaben als Grund für ihr verändertes Nutzungsverhalten das neue Recht an; über die Hälfte (56 Prozent) benannten Spotify als Ursache.⁸³⁵ Die Einnahmen der Musikindustrie im Bereich digitaler Musik sollen sich in 2009 verdoppelt haben und im Jahr 2010 um ca. 80 Prozent gestiegen sein.⁸³⁶

3) Nachlassen der Wirkung

Die festgestellten Auswirkungen waren sechs Monate nach Inkrafttreten des Gesetzes zum April 2009 nicht mehr in der gleichen Weise feststellbar. Lediglich bei den Verkaufszahlen von digitaler Musik blieb ein nachhaltiger Rückgang zu verzeichnen.⁸³⁷ Dies begründe

⁸²⁸ *Adermon/Liang*, S. 3.

⁸²⁹ *Adermon/Liang*, S. 3.

⁸³⁰ *Adermon/Liang*, S. 3.

⁸³¹ *Adermon/Liang*, S. 18.

⁸³² *Adermon/Liang*, S. 18.

⁸³³ *IFPI*, DMR 2011, S. 11, unter Berufung auf *Per Sundin*, Managing Director, Universal Music Schweden.

⁸³⁴ *IFPI*, DMR 2011, S. 11, unter Berufung auf GfK.

⁸³⁵ *IFPI*, DMR 2011, S. 11, unter Berufung auf GfK.

⁸³⁶ *IFPI*, DMR 2011, S. 11, unter Berufung auf GfK.

⁸³⁷ *Adermon/Liang*, S. 3.

Zweifel an der Effektivität des Auskunftsanspruchs⁸³⁸, sofern es um nachhaltige Wirkung gehe. Zudem wird die anfängliche Wirksamkeit auch mit dem öffentlichen Interesse in Verbindung gebracht, das den Fokus auf die Illegalität von Internetpiraterie legt.⁸³⁹

4) Ursachen für Nachlassen der Wirkung

Als Ursache für das Nachlassen der Wirkung wird die bis dato nicht mögliche gerichtliche Durchsetzung des Auskunftsanspruchs genannt, weil Bekämpfung von Illegalität ohne Durchsetzungsmöglichkeit für eine Sanktion keine nachhaltige Verhaltensänderung erzeugen kann.⁸⁴⁰ Von Seiten der Rechteinhaber wird eine Lösung zur Piraterie-Bekämpfung unter Einbindung der Provider gefordert.⁸⁴¹

c. Strafrechtliche Verfolgung von Urheberrechtsverletzungen

Ein Rechtsverletzer kann nach § 53 Urheberrechtsgesetz strafrechtlich belangt werden. Eine Straftat stellt P2P-Filesharing nach schwedischem Recht aber nur bei einem extensivem Ausmaß dar, also wenn entweder eine große Anzahl von Werken angeboten wird oder der Täter der erste ist, der ein Werk zur Verfügung stellt. Problematisch ist dabei insbesondere die Strafverfolgung. Seit 2009 werden in Schweden zwei besonders ausgebildete Staatsanwälte eingesetzt, die speziell für den Bereich der Internetrechtsverletzungen zuständig sind. Strafurteile in Bezug auf Filesharing-Straftaten sind in Schweden noch rar.

3. Lösungsansatz des Justizministeriums unter Einbindung der Zugangsanbieter

Auch in Schweden wird eine Lösung zur Bekämpfung von Internetpiraterie unter Beteiligung der Zugangsanbieter diskutiert. Im September 2007 veröffentlichte das Justizministerium einen Bericht⁸⁴², der sich mit dem Thema urheberrechtlicher Belange und Internet beschäftigte. Dieser schlug die Aufnahme einer Vorschrift in das Urheberrechtsgesetz unter Beteiligung der Zugangsanbieter vor.

Der Vorschlag sieht die Pflicht der Zugangsanbieter vor, einen Vertrag über einen Anschluss, der für die systematische Verletzung von Urheberrechten und verwandten Schutzrechten genutzt wird, mit sofortiger Wirkung kündigen zu können. Auf Antrag der Rechteinhaber sollte ein Gericht – unter Androhung eines Zwangsgeldes – zudem anordnen können, dass die Zugangsanbieter Maßnahmen zu ergreifen haben, die geeignet sind, um ihrer vorgenannten Verpflichtung nachzukommen. Der Zugangsanbieter sollte verpflichtet

⁸³⁸ Adermon/Liang, S. 3.

⁸³⁹ Adermon/Liang, S. 18.

⁸⁴⁰ IFPI, DMR 2011, S. 11, unter Berufung auf IFPI Sweden chief executive Ludvig Werner.

⁸⁴¹ IFPI, DMR 2011, S. 11, unter Berufung auf IFPI Sweden chief executive Ludvig Werner.

⁸⁴² Regierungsbericht Ds 2007:29.

sein, den Anschlussinhaber über die ergriffenen Maßnahmen in Kenntnis zu setzen. Das Interesse der Anschlussinhaber an der Aufrechterhaltung der Verbindung sei bei der Beurteilung zu berücksichtigen, ob der Anschluss gekündigt und ob eine einstweilige Verfügung erlassen werden soll.⁸⁴³ Dieser Regierungsvorschlag ist bislang nicht in einen Gesetzesvorschlag gemündet, was auch darauf zurückzuführen sein mag, dass die Entscheidung des EuGH zum schwedischen Auskunftsanspruch abgewartet wird, bevor eine erneute Debatte geführt wird.

4. Zusammenfassung

Auch in Schweden wurde bereits 2007 ein Warnhinweismodell unter Einbindung der Zugangsanbieter auf Initiative des Justizministeriums überprüft. Dieser Ansatz wurde aber nicht weiter verfolgt und stattdessen ein Auskunftsanspruch etabliert, der derzeit vom Europäischen Gerichtshof überprüft wird. Bevor es zur Vorlage kam, konnte die Effizienz der in Schweden neu eingeführten Sanktion überprüft werden. Die Wirkung des Sanktionsmodells war zunächst deutlich spürbar, nahm aber abrupt ab, als die Durchsetzung ausgesetzt wurde.

⁸⁴³ Regierungsbericht Ds 2007:29.

VII. Warnhinweismodelle außerhalb der Europäischen Union

Wie nicht zuletzt die Vereinbarung des multilateralen⁸⁴⁴ Anti-Counterfeiting Trade Agreement (ACTA)⁸⁴⁵ dessen finale Fassung seit Mai 2011 vorliegt, zeigt, ist die Diskussion um den verbesserten Schutz von Urheberrechten im Internet nicht auf den europäischen Rechtskreis begrenzt. Spezifische Schutzsysteme sind in einer Vielzahl von Staaten auf gesetzlicher Grundlage oder auf der Basis einer Vereinbarung der beteiligten Wirtschaftszweige bereits eingeführt oder werden zumindest als Entwurf diskutiert. Ausgehend davon, dass der Inhaber des Internetanschlusses, über den Urheberrechtsverletzungen begangen werden, einerseits, und der Diensteanbieter, der dem Anschlussinhaber den Internetzugang auf vertraglicher Basis zur Verfügung stellt, andererseits, eine Schlüsselstellung einnehmen, stehen Systeme, die zunächst eine Versendung von Hinweisen an den Anschlussinhaber zum Gegenstand haben, im Mittelpunkt. Die Zugangsdiensteanbieter sind dabei zur Mitwirkung in die Pflicht genommen. Die Hinweisverfahren stellen sich regelmäßig als Vorstufe eines gerichtlichen Verfahrens dar. Sie knüpfen zum Teil selbst bereits Sanktionen an die Wiederholung einer Rechtsverletzung; mitunter ist dies der Verlust oder die Verlangsamung des Internetzugangs bzw. durch Kündigung des Vertrages oder Sperre.

Beispielhaft sollen im Folgenden einige Regelungen dargestellt werden. Im asiatischen Raum traten etwa bereits 2009 entsprechende Regelungen in Kraft (Taiwan und Südkorea). Chile hat 2010 ein Verfahren eingeführt. In Neuseeland und den Vereinigten Staaten von Amerika wurden Verfahren in diesem Jahr verabschiedet bzw. vereinbart. In Kanada wird derzeit ein Entwurf diskutiert.

1. Vereinigte Staaten von Amerika

In den Vereinigten Staaten von Amerika trafen die Verbände der Film- und Musikindustrie und die großen Internetdiensteanbieter⁸⁴⁶ im Juli 2011 eine Vereinbarung, nach der die Provider ihren Kunden im Falle eines Urheberrechtsverstößes Warnhinweise zusenden.⁸⁴⁷

⁸⁴⁴ Beteiligt waren die USA, Japan, Kanada, Europäische Union und deren Mitgliedsstaaten, Schweiz, Südkorea, Singapur, Australien, Neuseeland, Mexiko, Jordanien, Marokko und die Vereinigten Arabischen Emirate.

⁸⁴⁵ Siehe dazu unten S. 273. Am 30. September 2011 wurde ACTA von Kanada, Australien, Japan, Marokko, Neuseeland, Südkorea, Singapur und den USA unterschrieben.

⁸⁴⁶ AT&T, Comcast, Cablevision, Time Warner Cable und Verizon.

⁸⁴⁷ Pressemitteilung der *Recording Industry Association of America (RIAA)*. vom 6.7.2011, abrufbar unter: http://www.riaa.com/newsitem.php?content_selector=newsandviews&news_month_filter=7&news_year_filter=2011&id=2DDC3887-A4D5-8D41-649D-6E4F7C5225A5 ; Memorandum of Understanding vom 6.7.2011, abrufbar unter:

<http://www.copyrightinformation.org/sites/default/files/Momorandum%20of%20Understanding.pdf>.

Diesem sog. „*Copyright Alert System*“ liegt der Gedanke zugrunde, dass dem Anschlussinhaber ein Recht zusteht, von Rechtsverstößen, die über seinen Anschluss begangen werden, in Kenntnis gesetzt zu werden.⁸⁴⁸

Das Verfahren sieht die Versendung von bis zu sechs Warnhinweisen vor. Auf die Meldung eines Rechtsverstoßes seitens des Rechteinhabers versendet der Internetdiensteanbieter einen Warnhinweis, der über Art und Folgen der Urheberrechtsverletzung sowie über Möglichkeiten zur Sicherung des Anschlusses und der Nutzung legaler Angebote aufklärt. Erfolgt ein zweiter Verstoß, kann ein weiterer Warnhinweis erteilt werden oder - wie auch bei einem dritten und vierten Verstoß - der Warnhinweis mit einer technischen Maßnahme verbunden werden, die den Anschlussinhaber dazu anhält, den Erhalt des Warnhinweises zu bestätigen. Zugleich wird der Anschlussinhaber nochmals über die gesetzlichen und vertraglichen Folgen des Verstoßes aufgeklärt. Bei einem fünften oder sechsten Verstoß erhält der Anschlussinhaber einen Warnhinweis verbunden mit einer Sanktion, die z.B. in einer vorübergehenden Bandbreitenreduzierung bestehen kann.⁸⁴⁹ Vor Verhängung einer der genannten Sanktionen kann sich der Anschlussinhaber an einen unabhängigen Gutachter wenden, der den vorgeworfenen Rechtsverstoß prüft.⁸⁵⁰

Eine Pflicht der Internetzugangsdiensteanbieter, den Anschluss zu kündigen, besteht nicht. Jedoch obliegt ihnen bereits nach Sec. 512 des *Digital Millennium Copyright Act* von 1998, in ihren Verträgen eine Kündigungsmöglichkeit für Wiederholungstäter vorzusehen, sofern sie nicht ihre Haftungsprivilegierung verlieren wollen.⁸⁵¹

Neben der Versendung der Warnhinweise sieht die Vereinbarung der beteiligten Wirtschaftsbranchen die Einrichtung eines *Center for Copyright Information* vor, das das System begleiten und Aufklärung bei den Verbrauchern betreiben soll.⁸⁵²

Eine zweite Initiative zur Bekämpfung von Urheberrechtsverletzungen in den Vereinigten Staaten von Amerika besteht in dem sog. *Protect IP Act*, einem im Mai 2011 in den Senat eingebrachten Gesetzesentwurf. Diesem zufolge sollen Suchmaschinenbetreiber, Domain-Name-Service(DNS)-Provider und Werbeunternehmen aufgrund eines gerichtlichen Beschlusses verpflichtet werden können, Webseiten zu sperren, die einen Rechtsverstoß darstellen oder zu einem solchen animieren.⁸⁵³ Eine verschärfte Version dieses Entwurfs wurde

⁸⁴⁸ Lindner, Alternative Modelle zur Begegnung von Urheberrechtsverstößen im Internet, vom 25.11.2011, S. 11.

⁸⁴⁹ Anderson, Major ISPs agree to „six strikes“ copyright enforcement plan, veröffentlicht am 7.7.2011, abrufbar unter: <http://arstechnica.com/tech-policy/news/2011/07/major-isps-agree-to-six-strikes-copyright-enforcement-plan.ars>.

⁸⁵⁰ Lindner, Alternative Modelle zur Begegnung von Urheberrechtsverstößen im Internet, vom 25.11.2011, S. 13.

⁸⁵¹ Lindner, Alternative Modelle zur Begegnung von Urheberrechtsverstößen im Internet, vom 25.11.2011, S. 12.

⁸⁵² Lindner, Alternative Modelle zur Begegnung von Urheberrechtsverstößen im Internet, vom 25.11.2011, S. 11.

⁸⁵³ Blog: : Hollywood lanciert verschärftes Anti-Piraterie-Gesetz (jh), veröffentlicht am 27.10.2011, abrufbar unter: heise online: <http://heise.de/-1367627>.

im Oktober 2011 mit dem sog. *Stop Online Piracy Act* in den Senat eingebracht, nach dem rechtsverletzende Webseiten praktisch unsichtbar gemacht werden können.⁸⁵⁴

2. Chile

In Chile trat im Mai 2010 ein Gesetz in Kraft, das ein Warnhinweissystem vorsieht. Es verpflichtet die Provider, auf Anzeige der Rechteinhaber ihre Anschlusskunden auf die festgestellten Urheberrechtsverletzungen hinzuweisen. Die Diensteanbieter sind außerdem verpflichtet, in ihren vertraglichen Vereinbarungen mit den Anschlussinhabern ein Kündigungsrecht für den Fall vorzusehen, dass wiederholt Rechtsverletzungen erfolgen. Eine Kündigung des Internetanschlusses kann zudem im Rahmen einer einstweiligen Verfügung durch den Zivilrichter angeordnet werden.⁸⁵⁵

3. Republik Korea (Südkorea)

In Südkorea trat im Juli 2009, begleitet durch eine öffentliche Informationskampagne, per Gesetz eine „*Three-Strikes*“-Regelung in Kraft.⁸⁵⁶ Die Regelung zielt vorrangig auf Urheberrechtsverletzungen in Blogs und unter Nutzung von File-Hosting-Diensten ab.⁸⁵⁷

Das südkoreanische Verfahren verläuft auf zwei Ebenen. Es beginnt grundsätzlich damit, dass die Urheberrechtskommission (Korea Copyright Commission (KCC)), aufgrund der Beschwerde eines Rechteinhabers oder aufgrund eigener Ermittlungen eine Mitteilung an den entsprechenden Internetdiensteanbieter macht und von diesem verlangt, dass er den betreffenden Nutzer ermahnt, kein urheberrechtlich geschütztes Material mehr einzustellen. Die Provider sind verpflichtet, über jede dem Internetnutzer gegenüber ergriffene Maßnahme Bericht zu erstatten.⁸⁵⁸

Stellt der Nutzer nach Erhalt von drei Warnhinweisen sein Verhalten nicht ein, so übergibt die Urheberrechtskommission den Fall an das Ministerium für Kultur und Tourismus, das dann das eigentliche „*Three-Strikes*“-Verfahren einleitet. Die im Rahmen dieses Verfahrens versendeten Warnhinweise können Sanktionen zur Folge haben.⁸⁵⁹ Das Ministerium kann sein Verfahren auch unabhängig von dem der Urheberrechtskommission in Gang bringen. Das Ministerium kann, ermächtigt durch Gesetz, die Internetdiensteanbieter anweisen, bei Rechtsverstößen Warnhinweise an die Anschlussinhaber zu versenden. Wird derselbe

⁸⁵⁴ Blog: Hollywood lanciert verschärftes Anti-Piraterie-Gesetz (*jh*), veröffentlicht am 27.10.2011, abrufbar unter: heise online: <http://heise.de/-1367627>.

⁸⁵⁵ *ifpi*, ISP Cooperation – Update vom Mai 2011, S. 2.

⁸⁵⁶ South Korea – A Market Revived.

⁸⁵⁷ South Korea – A Market Revived.

⁸⁵⁸ South Korea- A Market Revived.

⁸⁵⁹ South Korea – A Market Revived.

Anschlussinhaber innerhalb eines Zeitraums von 6 Monaten dreimal verwarnt, kann das Ministerium eine Sperrung des Internetanschlusses anordnen. Die Dauer der Anschluss-sperren ist gestaffelt. Vorgesehen ist ein Monat für die erste Sperre, ein bis drei Monate für die zweite Sperre und bis zu sechs Monate für weitere Sperren.⁸⁶⁰ Bei Nichteinhaltung ihrer Verpflichtungen können die Provider jeweils mit einem Bußgeld von bis zu drei Millionen südkoreanischen Won⁸⁶¹ belegt werden.⁸⁶²

Zur Bekämpfung der Internetpiraterie hat Südkorea neben dem Warnhinweismodell weitere Regelungen getroffen. So müssen sich bestimmte Onlineangebote, wie Peer-to-Peer-Services, registrieren und darüber hinaus bestimmte Maßnahmen ergreifen, um illegalen Datenaustausch zu blockieren. Gegen unlicenzierte Peer-to-Peer-Angebote sowie File-Hosting-Dienste und Blogs aus dem Ausland wird mit Webseitensperren vorgegangen.

4. Taiwan

Bereits im Juli 2009 ist in Taiwan eine gesetzliche Regelung in Kraft getreten, die das Versenden von Warnhinweisen durch die Internetzugangsanbieter vorsieht. Als Sanktionierung von wiederholten Verstößen gegen Urheberrechte sind Zugangssperren vorgesehen.

Der Diensteanbieter hat den Anschlussinhaber darauf hinzuweisen, dass sein Anschluss ganz oder teilweise gesperrt werden kann, wenn dieser Gegenstand dreier Warnhinweise war. Bei Nichteinhaltung der Netzsperrungen durch die Diensteanbieter verlieren diese die für sie bis dahin geltende Haftungsprivilegierung und werden für Rechtsverstöße ihrer Kunden sekundär herangezogen.⁸⁶³

5. Neuseeland

In Neuseeland ist eine „Three-Strikes“-Regelung Anfang September 2011 in Kraft getreten. Sie wurde durch eine Änderung des Urhebergesetzes, *Copyright Amendment Act 1994*, implementiert. Nach dem neu eingeführten Verfahren erfolgt bei einem durch den Rechteinhaber festgestellten Verstoß gegen Urheberrechte im Internet zunächst die Versendung von Warnhinweisen durch den Internetdiensteanbieter.⁸⁶⁴ Nach dem dritten Warnhinweis steht dem Rechteinhaber die Möglichkeit zu, das Verfahren vor dem sog. *Copyright-*

⁸⁶⁰ *ifpi*, ISP Cooperation – Update vom Mai 2011, S. 4 f.

⁸⁶¹ Dies entspricht derzeit rund 1.900,- €.

⁸⁶² South Korea – A Market Revived.

⁸⁶³ *ifpi*, ISP Cooperation – Update vom Mai 2011, S. 5.

⁸⁶⁴ *Ministry of Economic Development New Zealand, Copyright (Infringing File Sharing) Amendment Act*, abrufbar unter: http://www.med.govt.nz/templates/ContentTopicSummary___46155.aspx.

Tribunal anhängig zu machen. Das Tribunal besteht aus einem Vorsitzenden und fünf Mitgliedern, die vom Generalgouverneur auf Vorschlag des Wirtschaftsministers ernannt werden.⁸⁶⁵

Das *Copyright-Tribunal* kann dem Anschlussinhaber eine Geldstrafe von bis zu 15.000 Neuseeländischen Dollar⁸⁶⁶ auferlegen.⁸⁶⁷ Die konkrete Höhe der Strafe richtet sich nach dem Schaden, den der Rechteinhaber erlitten hat.⁸⁶⁸ Darüber hinaus räumt das Gesetz den Gerichten die Befugnis ein, unter bestimmten Umständen und bei wiederholter Rechtsverletzung dem Anschlussinhaber den Internetzugang für bis zu sechs Monaten zu sperren.⁸⁶⁹ Diese Ermächtigung tritt jedoch nur in Kraft, sofern sich die Verwarnungen und die Maßnahmen des *Copyright-Tribunal* als ineffektiv erweisen sollten. Es wird erwartet, dass hierzu im Jahr 2013 eine Überprüfung erfolgen wird.⁸⁷⁰

6. Kanada

Ein Warnhinweismodell wird auch in Kanada diskutiert. Ein Vorschlag findet sich hierzu im Entwurf des *Copyright Modernization Act* (C-11 [1]), der im Herbst 2011 in das kanadische Parlament eingebracht wurde. Auf Anstoß der Rechteinhaber sind die Internetzugangsdiensteanbieter hiernach verpflichtet, den Inhabern der betroffenen Anschlüsse beim Verdacht von Urheberrechtsverletzungen Warnhinweise zuzusenden.⁸⁷¹ Darüber hinaus soll den Zugangsdiensteanbietern die Pflicht auferlegt werden, auf richterliche Anordnung die Bestandsdaten ihrer Kunden an die Rechteinhaber herauszugeben. Den Rechteinhabern soll auf diese Weise eine gerichtliche Verfolgung der Urheberrechtsverletzung ermöglicht werden.⁸⁷² Spezielle weitergehende Sanktionen, wie etwa Internetsperren, sieht der Entwurf nicht vor.⁸⁷³

⁸⁶⁵ *Ministry of Justice New Zealand, About the Tribunal*, abrufbar unter:

<http://www.justice.govt.nz/tribunals/copyright-tribunal/about-the-tribunal>.

⁸⁶⁶ Dies entspricht derzeit rund 8.400 €.

⁸⁶⁷ Blog: ISP CEO Slams Copyright Law and Outdated Business Models (*enigmax*), veröffentlicht am 15.8.2011, abrufbar unter: <http://torrentfreak.com/isp-ceo-slams-copyright-law-and-outdated-business-models-110815/>.

⁸⁶⁸ *Ministry of Economic Development New Zealand, Copyright (Infringing File Sharing) Amendment Act*, abrufbar unter: http://www.med.govt.nz/templates/ContentTopicSummary___46155.aspx.

⁸⁶⁹ Lee, New Zealand traffic down as „three strikes“ copyright law takes effect, vom 7.9.2011, abrufbar unter: <http://arstechnica.com/tech-policy/news/2011/09/nz-traffic-down-as-three-strikes-copyright-law-takes-effect.ars>.

⁸⁷⁰ *Ministry of Economic Development New Zealand, Copyright (Infringing File Sharing) Amendment Act*, abrufbar unter: http://www.med.govt.nz/templates/ContentTopicSummary___46155.aspx.

⁸⁷¹ Blog: Kanada plant Warnhinweise an Copyright-Sünder (*Stefan Krempl/ anw*), veröffentlicht am 5.10.2011, abrufbar unter: heise online: <http://www.heise.de/newsticker/meldung/Kanada-plant-Warnhinweise-an-Copyright-Suender-1355412.html>.

⁸⁷² Blog: Urheberrecht: Kanadische Regierung plant enge Kooperation von Providern und Rechteinhabern (*sac*), veröffentlicht am 6.10.2011, abrufbar unter: <http://unurl.org/eEV>.

⁸⁷³ Blog: Kanada plant Warnhinweise an Copyright-Sünder (*Stefan Krempl/ anw*), veröffentlicht am 5.10.2011, abrufbar unter: heise online: <http://www.heise.de/newsticker/meldung/Kanada-plant-Warnhinweise-an-Copyright-Suender-1355412.html>.

D. Effizienz/ Wirksamkeit

I. Rechtsvergleichende Bewertung von Warnhinweismodellen

Essentiell für die Bewertung von Warnhinweismodellen und die konkrete Art ihrer Ausgestaltung ist die Beantwortung der Frage nach ihrer Effektivität und Effizienz.

Effektivität (Wirksamkeit) bezeichnet dabei das Verhältnis von dem erreichten Ziel und dem definierten, d.h. beabsichtigten Ziel der Regelung. **Effizienz (Wirtschaftlichkeit)** steht demgegenüber für die Kosten-Nutzen-Relation einer Maßnahme oder Regelung. Kosten wie Nutzen sind dabei im weitesten Sinne zu verstehen. Sie ergeben sich aus den konkreten tatsächlichen Auswirkungen der Regelung und aus den Wirkungen, die darüber hinaus aus dem Inhalt und Zusammenhang des Regelungsmodells zu schließen sind. Kosten und Nutzen lassen sich unter verschiedenen Gesichtspunkten beurteilen. Eine Regelung ist effizient, wenn die Kosten und Nutzen in einem angemessenen Verhältnis zueinander stehen.

1. Technische Perspektive

Ein Warnhinweisssystem, das anlassbezogen auf Urheberrechtsverletzungen im Internet reagieren soll, wird entscheidend daran zu messen sein, inwieweit begangene Urheberrechtsverletzungen in technischer Hinsicht überhaupt aufgespürt werden können. Neben der Rechtsverletzung als solcher, ist es erforderlich, einen Verantwortlichen identifizieren zu können, der schließlich Adressat des Warnhinweises sein würde. Dies wäre im günstigsten Fall der Rechteinhaber selbst, jedenfalls aber ein bestimmtes technisches Gerät (Router oder Computer), das verwendet wurde, und damit der Inhaber eines Internetanschlusses, von dem aus gehandelt wurde.

a. Identifikation des Verantwortlichen

Ausgangspunkt ist, dass Bewegungen von Internetnutzern in dem hier interessierenden Bereich von Urheberrechtsverletzungen regelmäßig nicht unter eigenem Namen erfolgen (*Realname/Klarname*). Sofern eine Namensangabe für die Nutzung eines Dienstes überhaupt notwendig ist, wird regelmäßig allenfalls unter einem Namen (*Nickname/Benutzername*) gehandelt, der – jedenfalls der Allgemeinheit – keinen Rückschluss auf eine bestimmte natürliche Person zulässt. Das einzig individualisierbare technische Datum, das bei computerprogramm-basierten Nachforschungen nach Urheberrechtsverletzungen mit Blick auf einen Beteiligten im Internet zuverlässig auffindbar ist, ist nach

dem aktuellen Stand der Technik, die jeweils von einem Gerät verwendete IP-Adresse. Die IP-Adresse gibt wiederum jedoch nicht Aufschluss über eine bestimmte natürliche Person als Nutzer des Gerätes, sondern ist lediglich dem Router, über den die Verletzungshandlungen begangen wurden, und damit dem jeweiligen Inhaber des Internetanschlusses zuordenbar.

Da die IP-Adressen vom jeweiligen Internetzugangsdienstanbieter verwaltet bzw. auch an seine Kunden vergeben wird, ist ihm im Grundsatz bekannt, welche seiner (dynamisch vergebenen) IP-Adressen zu welchem Zeitpunkt von welchem seiner Kunden genutzt wurde. Insofern ist eine Zuordnung der IP-Adresse zu einem Anschluss und damit einer natürlichen Person bzw. einer Institution, gleich welcher Rechtsform, möglich.⁸⁷⁴ Über seine Kundendatenbank ist die zustellfähige Anschrift des jeweiligen Anschlussinhabers ermittelbar.

Der konkrete Rechteevertzler ist auf diesem Wege jedoch nicht identifizierbar. Denn die Nutzung des Anschlusses und damit die Nutzung einer diesem zugeordneten IP-Adresse ist nicht auf die Person des Anschlussinhabers begrenzt. Ungeachtet des Falls der ungewollten Nutzung eines Internetzugangs, insbesondere WLAN-Anschlusses, durch unbefugte Dritte, wird der Anschlussinhaber vielfach ein Interesse daran haben, seinen Anschluss auch weiteren Personen zu Mitbenutzung zur Verfügung zu stellen. Dies wird insbesondere innerhalb der Familie der Fall sein, ist aber über diesen privat-häuslichen Bereich hinaus relevant etwa bei Hotspots im öffentlichen oder quasi-öffentlichen Raum oder Internetzugängen innerhalb von Unternehmen, die zumeist den Nutzerkreis durch Zugangspasswort beschränken.⁸⁷⁵ Die Identität des Rechteevertzlers ist auch insofern nicht gerichtsfest beweisbar.

Vor dem Hintergrund der technischen Möglichkeiten, eine Urheberrechtsverletzung individuell zuzuordnen, bleibt als Zielperson eines Warnhinweismodells derzeit lediglich der Anschlussinhaber. Gegen diesen können, wenn auch nicht ohne weiteres als Täter einer Urheberrechtsverletzung, im Zweifel in seiner Eigenschaft als Störer Ansprüche geltend gemacht werden. Soweit nach Ansicht des Bundesgerichtshofes⁸⁷⁶ den Inhaber eines Internetanschlusses, von dem aus ein urheberrechtlich geschütztes Werk ohne Zustimmung des Berechtigten öffentlich zugänglich gemacht worden ist, die sekundäre Darlegungslast trifft, hat der Anschlussinhaber den Nachweis zu erbringen, dass nicht er, sondern ein Dritter die Rechtsverletzung begangen hat. Diese Rechtsprechung erlaubt es, ein sich an den

⁸⁷⁴ Zur geltenden Rechtslage vgl. § 101 Abs. 9 UrhG.

⁸⁷⁵ Siehe auch die Sonderregelung des § 99 UrhG für den Fall, dass ein Arbeitnehmer als Täter der Urheberrechtsverletzung in Betracht kommt.

⁸⁷⁶ Urt. v. 12.5.2010 – I ZR 121/08, NJW 2010, 2061 – Sommer unseres Lebens. Dazu *Schwartmann/Kocks*, K&R 2010, 433 ff.

Anschlussinhaber wendendes anlassbezogenes Warnhinweismodell, als tunlich anzusehen.⁸⁷⁷

b. Identifikation der Rechtsverletzung

Wie dargestellt⁸⁷⁸, werden zur Begehung von Urheberrechtsverletzungen verschiedene Techniken eingesetzt, insbesondere Peer-to-Peer-Filesharing („Tauschbörsen“), Abruf über Streaming-Portale und Sharehoster.

Nicht bei jeder dieser Vorgehensweisen ist die IP-Adresse des Gerätes bzw. Anschlusses, mit bzw. unter dem die Rechtsverletzung begangen wurde, ermittelbar. Nach derzeitigem Stand der Technik ist vielmehr nur bei demjenigen Teil der Urheberrechtsverletzungen, der über Peer-to-Peer-Filesharing erfolgt, eine Nachverfolgung der IP-Adresse durch den Rechteinhaber möglich.

Beim sog. One-click-Hosting (z.B. RapidShare) können beispielsweise Benutzer Dateien auf einen Rechner im Internet hochladen. Auf diese Dateien kann Zugriff über einen Link genommen werden. Nur wer diesen konkreten Link kennt, kann die jeweilige Datei abrufen. Um die Dateien jedoch allgemein auffindbar zu machen, gibt es entsprechende Suchmaschinen. Die Webhoster, die ihre Infrastruktur für den Up- und Download zur Verfügung stellen, führen keine Identitätsprüfung ihrer Nutzer durch. Da sie nicht Normadressat von § 101 Abs. 9 UrhG sind, bestünde zudem kein Auskunftsanspruch.

aa. Identifikation in Peer-to-Peer-Netzen (Vorgehen und Unsicherheiten)

Peer-to-Peer-Netzwerke erlauben den unmittelbaren Austausch von Dateien, z.B. Musikdateien, zwischen zwei oder mehr Rechnern über das Internet ohne deren zwischengeschaltete Ablage auf einem Server. Mittels einer eingesetzten Software kann nach im Netzwerk vorhandenen Dateien gesucht werden. Bei der gezielten Suche nach bestimmten Dateiinhalten spielt für den Nutzer des Netzwerkes zunächst vor allem der Dateiname zur Identifikation eine wesentliche Rolle.

Entscheidet er sich für das Herunterladen einer bestimmten Datei, wird von der eingesetzten Software innerhalb des Netzwerks nach gleichen Dateien gesucht. Grund hierfür ist, dass beim Peer-to-Peer-Filesharing von verschiedenen im Peer-to-Peer-Netz vorhandenen Rechnern jeweils lediglich ein Teil der ausgewählten Datei heruntergeladen wird, um den Ladevorgang zu erleichtern bzw. zu verkürzen. Die Datei wird auf dem Rechner des Herun-

⁸⁷⁷ Zur Ermittlung des Anschlussinhabers s. Tz. 12 und Tz. 26 ff des o. a. Urteils. Zu beachten ist, dass ausweislich der Entscheidungsgründe die Rechteinhaberseite in den unteren Instanzen dargelegt hatte, die IP-Adresse sei von ihr mithilfe einer „zuverlässigen und eingehend überwachten Software“ ermittelt worden. Diesen Vortrag hatte die Beklagte jedoch erstinstanzlich offenbar nur pauschal bestritten und ihr Bestreiten zweitinstanzlich nicht substantiiert, so dass der Vortrag der Klägerin insoweit als unstrittig anzusehen war. Auch in der Entscheidung des *OLG Hamburg*, Beschluss v. 3.11.2010 – 5 W 126/10, abrufbar unter www.landesrecht.hamburg.de, war die Einlassung des Beklagten offenbar nicht wesentlich detaillierter.

⁸⁷⁸ Siehe oben S.34.

terladenden aus diesen Einzelteilen wieder zu einer vollständigen Datei zusammengesetzt. Damit gleiche Dateikopien auf verschiedenen Rechnern in dem Peer-to-Peer-Netzwerk schnell aufgefunden werden können, wird, weil dieser unabhängig vom jeweiligen Namen der Datei ist, nach Dateien mit einem gleichen sog. Hashwert gesucht.

Der Hashwert ist ein mithilfe eines Hash-Algorithmus (Streuwertfunktion) erzeugter, alphanumerischer Wert mit Einwegcharakter,⁸⁷⁹ der – so die Idealvorstellung – alle Kopien ein- und derselben Datei eindeutig kennzeichnet, gleich, auf welchem Datenträger sie abgelegt sind. Der Hashwert bildet auf diese Weise eine Art Fingerabdruck einer Datei, der, bis auf äußerst unwahrscheinliche Fälle begrenzt, nur ihr zugeordnet werden kann.

Der Such-, Download- und Zusammenführungsprozess der Dateiteile wird allein durch die eingesetzte Software gesteuert. Diese entscheidet auch darüber, welcher Teil der Datei von welchem der Rechner aus dem Peer-to-Peer-Netzwerk heruntergeladen wird. Damit keine Störungen auftreten, muss im Zweifel jeder Teil von jedem Rechner heruntergeladen werden können, weshalb auf jedem beteiligten Rechner eine vollständige Kopie der Datei vorhanden sein muss.

Während des Ladevorgangs ist die IP-Adresse der beteiligten Rechner ab- bzw. auslesbar, über die sich die Rechner miteinander verbunden haben. Die IP-Adresse bildet insofern den Anknüpfungspunkt für die Identifikation des Täters bzw. zumindest den von ihm benutzten Router/Internetanschluss.

Über die eigene Teilnahme an einem Netzwerk durch den Rechteinhaber bzw. von ihm Beauftragte können somit auch gezielt IP-Adressen ermittelt und mit der Bereitstellung von Dateien im Peer-to-Peer-Netzwerk in Verbindung gebracht werden.⁸⁸⁰ Der Nachweis, dass zwischen zwei IP-Adressen zu einem bestimmten Zeitpunkt eine bestimmte Datei mit urheberrechtlich geschütztem Inhalt ausgetauscht wurde, ist für die weitere Rechtsdurchsetzung essentiell. Die Möglichkeiten hier entscheiden daher mit über die Effektivität eines vorgesehenen Warnhinweisverfahrens.

Für den Nachweis des Tauschs urheberrechtlich geschützten Materials bedarf es der Originaldatei mit dem Hashwert zu Vergleichszwecken bzw. zum Nachweis der Identität der Dateikopien und einer für den Zweck der Durchführung des Verfahrens geeigneten speziellen Software, z.B. „File Sharing Monitor“.⁸⁸¹ Diese Software stellt einen abgewandelten Filesharing-Client dar, verbindet sich mit den Netzwerken, deren Protokoll sie versteht,

⁸⁷⁹ D.h. dass aus einer bestimmten Zeichenfolge bzw. Datei bei Anwendung des Algorithmus immer wieder derselben Hashwert entsteht, sich aber umgekehrt aus dem Hashwert nicht der Ursprungswert errechnen lässt.

⁸⁸⁰ Den Upload sollen sog. *Leecher-Mods* verhindern, d.h. veränderte Filesharing-Clients, die keinen Upload zulassen, sondern nur einen Download. Damit stellt der Verwender des *Leecher-Mods* selbst keine Dateien zum Download bereit, macht also im Zweifel nicht öffentlich zugänglich nach § 19a UrhG. Die Hersteller der Clients unterbinden aber mit jeder neuen Version des Clients weitere Versionen von *Leecher-Mods*.

⁸⁸¹ Basierend auf dem Open-Source-Client Shareaza und beherrschend (jedenfalls) die Protokolle Gnutella, Gnutella2, eDonkey2000 und BitTorrent.

und sammelt IP-Adressen sowie die GUID⁸⁸² der Benutzer. Zum Nachweis der Urheberrechtsverletzung lädt die Software einen Teil der anhand des Hashwerts identifizierten, urheberrechtlich geschützten Datei herunter, versehen mit einem Zeitstempel. Der Zeitstempel, der im Idealfall bis auf Millisekunden genau den Zeitpunkt des Auffindens bzw. des Herunterladens durch den Ermittlungssoftware-Client und damit des Bereitstellens durch den anderen Teilnehmer bestimmen soll, ist notwendig, um bei Auskunft durch den Zugangsdienstleister nachweisen zu können, welche (beim Herunterladen identifizierte) IP-Adresse zu welchem exakten Zeitpunkt welchem Anschlussinhaber zugewiesen war. Hierfür ist eine exakte Übereinstimmung des Zeitstempels aufseiten der Ermittlungssoftware und der Ermittlung der IP-Adressen durch den Zugangsdienstleister notwendig, anderenfalls kann eine zeitliche Übereinstimmung nicht nachgewiesen werden. Für die Beweisführung bei Gericht müsste eigentlich die Originaldatei beigebracht und abgespielt werden und es müsste der Hashwert der Originaldatei erzeugt werden. Vielfach sind Gerichte aber bereits hinreichend überzeugt, wenn Screenshots des Vorgangs beigebracht werden und eidesstattlich versichert wird, dass diese Screenshots echt sind, dass die Dateien abgespielt wurden, der Hashwert erzeugt wurde und dass die Dateien tatsächlich das in Rede stehende Werk enthalten.

Die Zuverlässigkeit der speziellen Software und die Zuverlässigkeit des Verfahrens unter Nutzung von Hashwerten werden unterschiedlich beurteilt. Während beispielsweise das OLG Hamburg⁸⁸³ davon ausgeht, dass eine Datei stets anhand des Hashwertes eindeutig identifiziert werden kann,⁸⁸⁴ steht das OLG München⁸⁸⁵ auf dem Standpunkt, dass mehrere unterschiedliche Hashwerte in einem Verletzungsvorgang sowohl bedeuten können, dass die Verletzungshandlungen von mehreren unterschiedlichen Personen begangen wurden, wie auch, dass sie bei mehrfachem Download durch ein- und dieselbe Person entstanden sind. Dies soll die in dem Verfahren beauftragte Ermittlungsfirma selbst vorgetragen haben. Nach Ansicht des OLG München ist die Bestimmung des Hashwertes mit einer „hohen Fehlerquote“ verbunden.

Betrachtet man das Vorgehen aus technischer Sicht, sind – abstrakt – insbesondere an folgenden Stellen Umsetzungsschwierigkeiten denkbar, die ein Verfahren belasten bzw. eine solche Software in der Zuverlässigkeit herabsetzen können:

⁸⁸² GUID bedeutet Globally Unique Identifier, eine hexadezimale Nummer mit 32 Stellen, die erzeugt wird, sobald ein eDonkey-kompatibler Client installiert wird. Mithilfe des GUIDs wird der Benutzer beim Login bei einem Server immer wieder eindeutig identifiziert.

⁸⁸³ Beschluss v. 3.11.2010 – 5 W 126/10, abrufbar über www.landesrecht.hamburg.de. Nach Ansicht des OLG Hamburg verstößt das Vorgehen auch nicht gegen Datenschutzrecht, anders als in der Schweiz (dort Logistep AG, *Schweizerisches Bundesgericht* v. 8.9.2010 – 1 C 285/2009). In der Entscheidung beruft sich das OLG Hamburg auch auf die BGH-Entscheidung „Sommer unseres Lebens“, wobei dort die Zuverlässigkeit des Verfahrens in den Urteilsgründen kaum inhaltlich thematisiert wird, sondern letztlich die Beklagte ihrer Verpflichtung zum erheblichen Bestreiten nicht nachgekommen sein soll. Die BGH-Entscheidung ist also diesbezüglich in der Begründung nicht wirklich ergiebig.

⁸⁸⁴ Die Wahrscheinlichkeit, dass zwei unterschiedliche Dateien denselben Hashwert haben, soll bei etwa 1: 340 Sextillionen liegen.

⁸⁸⁵ Beschluss v. 27.9.2010 – 11 W 1894/10, MIR-DokNr. 148-2010.

- Bei der Authentifizierung einer Zielfile können Fehler auftauchen bei der Korrektheit der Auswahl der Zielfile, bei der Bildung der Prüfsumme bzw. des Hashwertes zur Wiedererkennung der Zielfile (z.B. Fehler im Algorithmus), im Hashprogramm selbst sowie bei der Übertragung der Werte bzw. bei der Speicherung im Suchprogramm.
- Bei der Identifizierung einer Zielfile und der Protokollierung können Fehler auftauchen, z.B. durch Erzeugen von false positives.⁸⁸⁶
- Bei der Ergebnisverarbeitung in dem Programm können Fehler auftauchen bei jedem Speicher- oder Übertragungsvorgang, streng genommen auch bei sonstigen Auswertungen einschließlich des Ausdrucksens.

Eine Steigerung der Qualität der Software bzw. der Trefferquote ist, nimmt man nicht ohnehin bereits jetzt eine ausreichende Zuverlässigkeit des Verfahrens an, erzielbar, wenn möglichst viele Parameter zur Bestimmung der Identität der in Rede stehenden Datei in die Betrachtung einbezogen werden. So ist denkbar, zur Identifizierung neben dem Zeitstempel und dem Hashwert noch die Dateigröße einzubeziehen. Damit wird jedenfalls verhindert, dass Hashwerte, wie verschiedentlich in Foren diskutiert, gefälscht und für Dateien vollkommen anderer Größenordnungen verwendet werden.

Als Identifizierungsparameter kämen darüber hinaus etwa die Metadaten der betreffenden Dateien in Betracht. Diese enthalten Informationen über Eigenschaften der Datei, bei Musikdaten etwa Name des Sängers, Titel und Größe der Datei. Sie bleiben, sofern sie in der Datei vorhanden sind, anders als der Hashwert, auch bei Komprimierungsvorgängen, Dateikürzungen oder Formatänderungen gleich.

bb. Dauer der Speicherung von Daten

Ein weiterer nicht unerheblicher Parameter zur Identifizierung des IP-Inhabers ist die Dauer der Speicherung von Verkehrsdaten.

Eine Pflicht zur Speicherung besteht nach aktueller Rechtslage nicht. In der derzeitigen Praxis gibt es daher Zugangsdiensteanbieter, die die von § 101 Abs. 9 UrhG erfassten Verkehrsdaten bereits unmittelbar nach Verbindungsende löschen, andere nach wenigen Stunden. Eine Ermittlung des Anschlussinhabers anhand der IP-Adresse ist danach nicht mehr möglich.

Die Problematik, die sich derzeit bereits betreffend den Auskunftsanspruch stellt, ist daher ebenfalls zu thematisieren bei der Frage der Wahl bzw. der Festsetzung der Modalitäten eines Warnhinweismodells, dessen Effektivität auch davon abhängt, ob der die IP-Adresse überhaupt zugeordnet werden kann.

⁸⁸⁶ In Irland ist es in Folge eines Fehlers bei der Umstellung des Servers von der Sommer- auf die Winterzeit zu einer Fehl-Versendung von etwa 300 Warnhinweisen der ersten Stufe gekommen. Siehe dazu oben S. 155.

c. Bewertung

Nach derzeitiger Rechtslage und dem Stand der Technik ist, soweit nicht unter dem Klarnamen gehandelt wird, einziges Identifizierungsmerkmal im Internet die vom jeweiligen Nutzer verwendete IP-Adresse. Die IP-Adresse selbst gibt jedoch noch keinen Aufschluss über die konkret handelnde Person, sondern im Zweifel nur über den Inhaber des zur Begehung der Rechtsverletzung in Anspruch genommenen Internetanschlusses. Nur dieser Anschlussinhaber wird daher primär Adressat eines Warnhinweises sein können. Die Zuordnung ist über die Internetdiensteanbieter technisch unter Rückgriff auf Verkehrs- und Bestandsdaten möglich. Die Effektivität eines Modells, dass sich anlassbezogen an den unmittelbar Handelnden bzw. den Anschlussinhaber, als ggf. verantwortlich angesehene Person, richtet, hängt daher entscheidend davon ab, wie gut und sicher die Urheberrechtsverletzung festgestellt, einer konkreten IP-Adresse zugeordnet und eine Identifizierung vorgenommen werden kann. Denkbar sind hier insbesondere Verbesserungen der Qualität der eingesetzten Software, insbesondere durch Ergänzung der Such- und Identifizierungsparameter für die urheberrechtlich relevanten Dateien.

Jedenfalls soweit vom Rechteinhaber der Nachweis einer konkreten Rechtsverletzung abverlangt wird, beschränken sich nachzeitigem Stand der Technik die Möglichkeiten der Verfolgung auf Peer-to-Peer-Netzwerke. Ein Warnhinweismodell muss sich also – nach dem aktuellen Stand der Technik – von vornherein darauf begrenzen, bei Urheberrechtsverletzungen unter Einsatz von Peer-to-Peer-Filesharing den Anschlussinhaber anzusprechen. Andere Technologien bleiben derzeit außen vor.

Dieser Befund setzt Warnhinweise, wie die untersuchten, dem Vorwurf nur begrenzter Wirksamkeit aus, da unrechtmäßiges Verhalten im Internet von vorne herein nur in begrenztem Rahmen überhaupt erfasst werde.

Nach den Ergebnissen einer von der Universität Rennes durchgeführten Studie⁸⁸⁷ erfolgt die Nutzung von Musik und Videos im Internet vorwiegend über Streamingportale wie etwa Youtube, Dailymotion oder Deezer und vergleichbare Angebote.⁸⁸⁸ Dies entspricht den Ergebnissen der letzten Hadopi-Studie, wonach die kostenlose legale wie illegale Nutzung urheberrechtlich geschützten Materials vor allem über Streamingplattformen erfolgt.⁸⁸⁹ Die Ergebnisse der Hadopi sind insofern noch differenzierter, als sie das Verhalten weiterhin nach Nutzergruppen auftrennt. Besonderheiten weisen hierbei die Nutzungsgewohnheiten von denjenigen auf, die im Rahmen der Befragung auch angaben, illegal Inhalte zu nutzen. Bei diesen Befragten überwiegt die Nutzung der Streamingportale für

⁸⁸⁷ Dejean/Pénard/Suire, M@souin/CREM/Université de Rennes 1, Une première évaluation des effets de la loi Hadopi sur les pratiques des internautes français, März 2010, abrufbar unter: <http://www.marsouin.org/IMG/pdf/NoteHadopix.pdf>.

⁸⁸⁸ Vgl. S. 4 f. der Studie, insbesondere Grafik 2.

⁸⁸⁹ Hadopi, *biens culturels et usages d'internet: pratiques et perceptions des internautes français, 2ème vague barométrique* (Zweite Untersuchung der Hadopi, vorgelegt am 18.5.2011), abrufbar unter: http://www.hadopi.fr/sites/default/files/page/pdf/t1_etude_longue.pdf, Folien 42 f.

den Bereich Musik (80 Prozent) und für Fotos (70 Prozent). Der Peer-to-Peer-Austausch von Inhalten ist deutlich geringer und rangiert (je nach Inhalt, der betroffen ist, zwischen sieben Prozent für Fotos und 28 Prozent für Video/Filme⁸⁹⁰) erst hinter der Nutzung von Seiten, auf denen Inhalte zum Download angeboten werden, bspw. Dienste wie MegaUpload oder Rapidshare.⁸⁹¹ Im Bereich Videos/Filme und Fernsehserien sowie bei Büchern steht die Nutzung über Downloadplattformen derjenigen Nutzung über Streamingplattformen gleich. Im Bereich Software wird sogar wesentlich (57 Prozent) auf das Downloadangebot zurückgegriffen.⁸⁹²

Bei denjenigen, die grundsätzlich Inhalte nur legal nutzen, überwiegt in allen Bereichen deutlich die Nutzung von Streamingdiensten. Ausnahme bildet insofern der Bereich Software, bei dem Streamingdienste und Downloadplattformen mit jeweils 43 Prozent gleichauf liegen. Insgesamt geringer ist hier auch die Nutzung von Peer-to-Peer-Diensten, die je nach Bereich zwischen 4 Prozent (Fernsehserien) und 12 Prozent (Software) liegen.⁸⁹³

Die Zahlen sind vergleichbar mit den Daten, die für das Vereinigte Königreich genannt werden. Hiernach werden 37 Prozent der Urheberrechtsverletzungen im Internet durch illegales Peer-to-Peer-Filesharing vorgenommen.⁸⁹⁴ Damit ist es im Vereinigten Königreich die meistgenutzte Technologie für Urheberrechtsverletzungen im Internet.

Eine ähnliche Bewertung hat der britische *High Administrative Court* vorgenommen. Auch wenn sich das Warnhinweissystem nur auf 37 Prozent der Fälle von Urheberrechtsverletzungen erstreckt, würde eine deutliche Reduzierung von illegalem Peer-to-Peer-Filesharing zu einer deutlichen Verringerung des Ausmaßes von Urheberrechtsverletzungen im Internet insgesamt führen. Vor diesem Hintergrund ging er von der Verhältnismäßigkeit der gesetzlichen Regelung aus.⁸⁹⁵

2. Pädagogische Perspektive

Eine der wesentlichen Überlegungen, die der Einführung eines Warnhinweissystems zugrunde liegen, ist es, auf das Verhalten der Internetnutzer in positiver Weise Einfluss zu nehmen. Der Internetnutzer, der sich in urheberrechtswidriger Weise verhält bzw. als Anschlussinhaber seinen Pflichten zur Sicherung seines Internetzugangs nicht nachkommt, soll über die rechtliche Bewertung und Folgen seines Handelns aufgeklärt und hierüber dazu angehalten werden,

- Rechtverstöße zukünftig zu unterlassen,

⁸⁹⁰ Die gebildeten Kategorien sind: Musik/Musikvideos, Video/Filme, Fernsehserien, Fotos, Videospiele, Bücher, Software.

⁸⁹¹ *Hadopi*, 2ème vague barométrique, a.a.O., Folie 43.

⁸⁹² *Hadopi*, 2ème vague barométrique, a.a.O., Folie 43.

⁸⁹³ *Hadopi*, 2ème vague barométrique, a.a.O., Folien 42.

⁸⁹⁴ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 230.

⁸⁹⁵ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 230.

- seinen Konsum kultureller Güter auf legale Angebote umzustellen bzw.
- Vertrauen in den Konsum kultureller Güter über das Internet zu gewinnen - insbesondere solche Nutzer, die ggf. aus Furcht vor Rechtsübertretungen das Internet derzeit noch nicht als Bezugsmedium nutzen.

Mutmaßungen dazu, wie Nutzer auf die Versendung von Warnhinweisen reagieren, sind vielfältig. Einerseits wird behauptet, Rechtsdurchsetzungsbemühungen in der Vergangenheit hätten bereits keinerlei Auswirkungen gezeigt, weshalb auch von Warnhinweisen keine signifikante Wirkung zu erwarten sei.⁸⁹⁶ Die Kläger in dem Verfahren vor dem britischen *High Administrative Court* hielten andererseits eine derart starke Abschreckungswirkung für möglich, dass sie die Befürchtung formulierten, Internetnutzer könnten durch die Einführung eines Warnhinweissystems in ihrem freien Gebrauch des Internets insgesamt eingeschränkt werden.⁸⁹⁷

Warnhinweismodelle sind zudem der Kritik ausgesetzt, sie würden die Internetnutzer nur dazu veranlassen, andere Techniken zu benutzen, um zukünftig weiterhin unbemerkt Urheberrechtsverletzungen zu begehen. Soweit daher mit der Einführung von Warnhinweissystemen die Rechtsverfolgung von Urheberrechtsverletzungen angestrebt werde, führe dies nur zu einem Wettlauf zwischen Verschlüsselungs- und Anonymisierungsdiensten einerseits und Ermittlungstechniken andererseits.⁸⁹⁸

a. Generelle Bedeutung der Rechtsdurchsetzung

Dem Vorwurf, dass **Rechtsdurchsetzungsbemühungen** grundsätzlich ineffektiv seien, stehen in Deutschland Zahlen entgegen, die die Entwicklung von Urheberrechtsverletzungen in den vergangenen Jahren aufzeigen. So ist die Anzahl der Personen, die sich unlicenzierte Inhalte aus dem Internet herunterladen, nach den Ergebnissen der DCN-Studie in den letzten Jahren, in denen von Seiten der Rechteinhaber Urheberrechtsverletzungen im Internet konsequent verfolgt werden, stetig gesunken. Wurden im Jahr 2005 noch 412 Mio. Musiktitel unter Verstoß gegen Urheber- und Leistungsschutzrechte heruntergeladen, so waren es 2009 nur mehr 258 Mio. und 2010 schließlich 185 Mio.⁸⁹⁹ Die Zahl der Nutzer illegaler Internetangebote⁹⁰⁰ im Bereich Musik sank zugleich von 4,4 Mio. im Jahr 2005 auf 3,1 Mio. im Jahr 2010.⁹⁰¹

Soweit die Zahlen die tatsächliche Entwicklung in Deutschland widerspiegeln, kann nicht zwangsläufig darauf geschlossen werden, dass allein die verstärkte Rechtsverfolgung für den Rückgang der Rechtsverstöße gesorgt hat. Wenngleich sie eine – möglicherweise bedeutende – Rolle hierbei spielt, können für die Ergebnisse auch andere Faktoren, nament-

⁸⁹⁶ Karaganis, S.iii.

⁸⁹⁷ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 235 ff.

⁸⁹⁸ Karaganis, S.32.

⁸⁹⁹ Brennerstudien 2006 und 2010, DCN-Studie 2011.

⁹⁰⁰ Gruppe der Befragten: Deutsche über 10 Jahre.

⁹⁰¹ Brennerstudie 2006, DCN-Studie 2011.

lich Aufklärungskampagnen und die zunehmende Verbreitung legaler digitaler Geschäftsmodelle, (mit-)verantwortlich sein. Einen Hinweis auf die nicht unerhebliche Bedeutung der konsequenten Verfolgung von Rechtsverstößen geben jedoch Zahlen aus **Schweden**. Messungen dort belegen, dass zu dem Zeitpunkt, zu dem der gesetzliche Auskunftsanspruch in Kraft trat, schlagartig der gesamte Internetdatenverkehr um 40 Prozent zurückging.⁹⁰² Nähme man an, was nahe liegt, dass vor allem die illegale Betätigung im Internet eingestellt wurde, so wäre dies ein Hinweis auf deren immensen Umfang. Zum anderen zeigt es, dass die erhöhte Wahrscheinlichkeit, als Täter mit der eigenen Rechtsverletzung in Zusammenhang gebracht zu werden, von nicht unerheblichem Einfluss auf das Nutzerverhalten ist.

Auf die Bedeutung der Rechtsdurchsetzung weisen auch Ergebnisse einer im Januar 2008 durchgeführten Studie aus dem **Vereinigten Königreich** hin.⁹⁰³ Hiernach gaben zwei Drittel derjenigen, die im Internet unautorisiert auf Inhalte zugreifen, an, dieses Vorgehen einzustellen, wenn ihrem Eindruck nach die Wahrscheinlichkeit größer wäre, das ihr Handeln entdeckt würde. Jedoch hielten 68 Prozent die Wahrscheinlichkeit belangt zu werden für sehr gering.⁹⁰⁴ 51 Prozent der Befragten gaben an, sie würden Filesharing auch dann fortsetzen, wenn es mehr Berichte über Strafverfahren gegen illegale Filesharer gäbe, da sie die Wahrscheinlichkeit belangt zu werden, dennoch für sehr gering hielten.⁹⁰⁵ Bei den männlichen Teenagern waren es sogar zwei Drittel.⁹⁰⁶

Den Zusammenhang zwischen der gesetzlichen Einführung des Warnhinweismodells in **Frankreich** und einem festgestellten Anstieg der Musikverkaufszahlen über iTunes untersuchen *Danaher, Smith, Telang* und *Chen* in einer jüngeren Studie.⁹⁰⁷ Sie gelangen zu dem Ergebnis, dass der Anstieg fast ausschließlich auf einen Rückgang des Piraterieverhaltens der Nutzer aufgrund der Gesetzesänderung und der damit verbundenen Aufmerksamkeit zu der Thematik zurückzuführen ist.⁹⁰⁸

b. Ausweichen auf andere Techniken wegen technischen Anwendungsrahmens

Allen untersuchten Warnhinweismodellen ist gemeinsam, dass sie allein mittels Peer-to-Peer-Filesharing begangene Rechtsverletzungen einbeziehen und sich nicht auch auf andere Begehungsform von Urheberrechtsverletzungen im Internet erstrecken. Soweit die Systeme daher dem Vorwurf begrenzter Wirksamkeit ausgesetzt sind, weil unrechtmäßiges

⁹⁰² *Adermon/Liang*, S.3.

⁹⁰³ 2008 Digital Entertainment Survey. Es wurden 1.608 Personen im Alter zwischen 15 und 54 Jahre, zu jeweils 50 Prozent männlich bzw. weiblich und aus verschiedenen Regionen des Landes, befragt. *Wiggin& Entertainment Media Research 2008*, S. 5.

⁹⁰⁴ *Wiggin& Entertainment Media Research 2008*, S. 13.

⁹⁰⁵ *Wiggin& Entertainment Media Research 2008*, S. 13.

⁹⁰⁶ *Wiggin& Entertainment Media Research 2008*, S. 13.

⁹⁰⁷ Hierzu ausführlich unten, S. 209.

⁹⁰⁸ *Danaher, Smith, Telang, Chen*, S.2f.

Verhalten im Internet von vorneherein nur in begrenztem Rahmen überhaupt erfasst werde, kann auf die bereits gemachten Ausführungen verwiesen werden. Darüber hinaus steht im Raum, dass Nutzer dazu angehalten würden, **auf andere Techniken auszuweichen, die vom Warnhinweissystem nicht erfasst sind.**⁹⁰⁹ Ob das tatsächlich der Fall ist, bedarf weiterer Untersuchung des Nutzerverhaltens. Hierauf soll im Folgenden näher eingegangen werden. Ausgehend davon, dass sich Ursachen, Verhaltensweisen, alternativen Verhaltensweisen, Abschreckungswirkung und Unrechtsbewusstsein der Nutzer im Internet empirisch-wissenschaftlich nicht eindeutig bestimmen lassen⁹¹⁰, ging der britische *High Administrative Court* davon aus, dass derartige nicht belegbare Bedenken nicht geeignet seien, die Verhältnismäßigkeit der Warnhinweisregelungen zu erschüttern.⁹¹¹

Ungeachtet der wissenschaftlichen Erkenntnislage und ihrer Bewertung ist darüber hinaus zu berücksichtigen, dass Warnhinweissysteme in ihrer Zielrichtung multipel sind. Im Mittelpunkt steht dabei primär das Ziel der Verminderung von Urheberrechtsverstößen. Dieses kann durch Sanktionierung, Aufklärung, Erziehung, aber auch Medienkompetenz erzielt werden. Eine weitere Komponente ist ein rechtsstaatlicher Ansatz, der Aufklärung vor Sanktionierung stellt und einen Beitrag dazu leisten vermag, dass strafrechtliche Sanktionen und kostenintensive zivilrechtliche Rechtsverfolgung nicht den Unwissenden treffen. Vor diesem Hintergrund wäre, sofern die Faktenlage tatsächlich hierfür spräche, ein gezieltes Ausweichen von Nutzern auf andere Techniken in der Folge der Einführung eines Warnhinweismodells als Leistung der Aufklärungsarbeit zu bewerten.

c. Verhaltenssteuerung

Zur Frage, inwieweit **durch die Versendung von Warnhinweisen** auf das Verhalten der Internetnutzer **tatsächlich Einfluss** genommen wird bzw. gezielt Einfluss ausgeübt werden kann, wurden bereits zahlreiche Untersuchungen durchgeführt. Zum Teil knüpfen sie unmittelbar an die Wirkung existierender Modelle an, andere Untersuchungen sind abstrakter Art und losgelöst von einem konkreten Modell oder Regelungsrahmen. Insbesondere die Hadopi hat im Rahmen der ihr von Gesetzes wegen auferlegten Berichtspflicht Auswertungen durchgeführt, deren Fokus u.a. darauf lagen, Erkenntnisse über das Verhalten und Selbstverständnis der Nutzer im Internet zu gewinnen. Aufgrunddessen, dass das Verfahren in Frankreich dasjenige ist, welches bereits seit fast eineinhalb Jahren durchgeführt wird, können insbesondere die dort gewonnenen Daten Anhaltspunkte liefern. Da-

⁹⁰⁹ In Irland, wo bislang lediglich ein Provider aufgrund einer privatrechtlichen Vereinbarung eine Warnhinweis-Regelung eingeführt hat, stellt sich zudem die – ähnlich gelagerte – Frage, ob die Regelung nicht zu einem Ausweichen auf andere Diensteanbieter führt. Nach Angaben des Providers (Eircom Ltd.) hat allerdings die Implementierung des „*Graduated Response*“-Verfahrens keine(n) signifikante(n) Kundenabwanderung bzw. Anbieterwechsel bewirkt. Im Hinblick auf das Neukundengeschäft in der Republik Irland lassen Daten aber wohl den Schluss zu, dass die Einführung der Warnhinweis-Regelung einen vergleichsweise geringeren Zugewinn an neuen Kunden bei dem Provider (mit)verursacht hat.

⁹¹⁰ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 232.

⁹¹¹ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 234.

tenmaterial, das auf konkreten Erfahrungen beruht, liegt in gewissem Umfang auch für die Republik Irland und die dort praktizierte Warnhinweis-Regelung vor, wurde aber nicht zur Veröffentlichung im Rahmen dieser Studie freigegeben.⁹¹²

aa. Abkehr von Peer-to-Peer-Nutzung - Änderung des Nutzerverhaltens hin zur Legalisierung

1) Zielgruppe

Geht es zunächst um die Frage, wie sich das Verhalten von Internetnutzern durch die Einführung eines Warnhinweismodells verändert (und noch nicht um die hierzu beitragenden Parameter), sind zunächst die jeweiligen Zielgruppen voneinander abzugrenzen. Soll im Wesentlichen die Abkehr von rechtsverletzendem Verhalten erzielt werden, betrifft dies diejenigen, die unrechtmäßige Angebote in Anspruch nehmen. Soweit abgestufte Sanktionsmodelle insgesamt Einfluss auf das Verhalten von Internetnutzern haben können, sind die Internetnutzer als Gesamtgruppe zu betrachten.

Anlässlich einer vom Markt- und Meinungsforschungsinstitut IPSOS im Mai 2008 vorgelegten, für die französische Bevölkerung repräsentativen Studie, waren 1010 Personen ab dem Alter von 15 Jahren befragt worden.⁹¹³ Im Rahmen der Umfrage bejahten 21 Prozent der Befragten, **bereits einmal illegal Musik** aus dem Internet von **kostenlosen Webseitenangeboten** heruntergeladen zu haben. Dies entspricht **31 Prozent** derjenigen, die über einen Internetanschluss verfügen. Nach einer französischen Studie aus dem Jahr 2009 waren es **38 Prozent**, d.h. über ein Drittel aller Internetnutzer, die bereits einmal über **Peer-to-Peer-Netzwerke** illegal Musik heruntergeladen haben.⁹¹⁴ Fünf Prozent gaben an, dies „oft“ getan zu haben, zwölf Prozent „manchmal“ und 21 Prozent „selten“.⁹¹⁵ Den aktuellen Daten einer Studie der Hadopi⁹¹⁶ zufolge beziehen **fünf Prozent** derjenigen, die Kulturgüter⁹¹⁷ über das Internet konsumieren, diese ausschließlich auf illegalem Wege.⁹¹⁸ Dieser Anteil der Nutzer ist ebenso groß, wie derjenige, der eigenen Angaben zufolge solche

⁹¹² Siehe aber noch unten S. 209.

⁹¹³ IPSOS, Les Français face au téléchargement illégal de musique sur Internet - Les chiffres et résultats complets du sondage, 26.5.2008, abrufbar unter: <http://www.ipsos.fr/ipsos-public-affairs/sondages/francais-face-au-telechargement-illegal-musique-sur-internet>.

⁹¹⁴ 33 Prozent gaben an, bereits einmal legale Bezahlendienste in Anspruch genommen zu haben. *Pratiques et attentes des internautes: la consommation de contenus culturels sur Internet*, September 2009, abrufbar unter: http://lesrapports.ladocumentationfrancaise.fr/cgi-bin/brp/telestats.cgi?brp_ref=104000006&brp_file=0000.pdf (dort angefügt, S. 69 ff., an den Bericht von Zelnik/Toubon/Cerutti an den Kultus- und Kommunikationsminister, *Création et Internet, Rapport au Ministre de la Culture et de la Communication*, Januar 2010), Folie 11. Bei Filmen waren es 31 Prozent gegenüber 14 Prozent, die bereits einmal legale Bezahlendienste genutzt haben, vgl. Folie 26.

⁹¹⁵ *Pratiques et attentes des internautes*, a.a.O., Folie 11.

⁹¹⁶ Hadopi, biens culturels et usages d'internet: pratiques et perceptions des internautes français, 2ème vague barométrique (Zweite Untersuchung der Hadopi, vorgelegt am 18.5.2011), abrufbar unter: http://www.hadopi.fr/sites/default/files/page/pdf/t1_etude_longue.pdf.

⁹¹⁷ Musik, Video, Videospiele, Bücher, Fernsehserien, Fotos, Software.

⁹¹⁸ Basis für diesen prozentualen Anteil sind diejenigen Internetnutzer, die innerhalb eines Zeitraums von 12 Monaten vor der Befragung entsprechende Güter über das Internet konsumiert haben.

Güter gar nicht über das Internet bezieht. Fast **zwei Drittel** (64 Prozent) der im Rahmen der Studie Befragten waren der Ansicht, die genannten Inhalte **ausschließlich legal** zu nutzen.⁹¹⁹ Soweit eine illegale Nutzung urheberrechtlich geschützter Inhalte erfolgt, geschieht dies in der Mehrzahl der Fälle gelegentlich. 35 Prozent der Befragten, die angaben, Inhalte illegal zu nutzen, tun dies regelmäßig, neun Prozent sogar täglich.⁹²⁰

Zu berücksichtigen ist bei der Bewertung dieser Daten, dass allen Befragungen eine Selbsteinschätzung der Nutzer bezüglich der Rechtmäßigkeit bzw. Unrechtmäßigkeit ihres eigenen Handelns zugrunde liegt. Das eigene Rechtsbewusstsein kann jedoch deutlich von der tatsächlichen Rechtslage abweichen. Auf die Frage etwa, warum Internetnutzer noch niemals Musik aus dem Internet heruntergeladen hätten, entschieden sich im Rahmen der Studie aus dem Jahr 2009 zwölf Prozent für die Antwort „**weil es illegal ist**“. Ein solches Ergebnis darf als Indikator dafür gesehen werden, dass über die rechtlichen Vorgaben bzw. die Existenz legaler Angebote nur begrenzte Kenntnis vorhanden ist. 17 Prozent gaben an, hierzu nicht ausreichende Kenntnis bzw. Routine zu haben.⁹²¹

2) *Besonders betroffene Bereiche*

Besonders von Urheberrechtsverstößen betroffen sind nach den Ergebnisse der Hadopi der Musik- sowie der Film- und Fernsehbereich. Unter denjenigen Internetnutzern, die sich auch illegal im Internet betätigen, lag im Rahmen der Befragungen durch die Hadopi die Nutzung von Musik/Musikvideos bei 77 Prozent, der Bereich Video/Film bei 71 Prozent und Fernsehserien bei 59 Prozent.⁹²²

Unter der spezifischen Perspektive der Musik wurde im Rahmen einer im Auftrag der Verwertungsgesellschaft SACEM ebenfalls Ende 2010 durchgeführten Studie⁹²³ ermittelt, dass **zwölf Prozent derjenigen, die Musik über das Internet nutzen**,⁹²⁴ hierfür auch auf illegale Downloadangebote zurückgreifen.⁹²⁵ Nach den Ergebnissen der Studie hochgerechnet sind dies rund 4,9 Prozent der Gesamtbevölkerung Frankreichs. Gemäß den Ergebnissen einer vom Institut Opinionway im Auftrag des französischen Premierministers erstellten Studie⁹²⁶ haben insgesamt 82 Prozent der Internetnutzer bereits einmal Musik über das Internet gehört.⁹²⁷

⁹¹⁹ Hadopi, 2ème vague barométrique, a.a.O., Folie 45. Aufschlüsselung nach Altersstufen, dort Folien 46, 47.

⁹²⁰ Hadopi, 2ème vague barométrique, a.a.O., Folie 51. Aufschlüsselung nach Altersstufen, dort Folien 52.

⁹²¹ *Pratiques et attentes des internautes*, a.a.O., Folie 18.

⁹²² *Pratiques et attentes des internautes*, a.a.O., Folie 36. Unterscheidung nach Altersklassen vgl. Folie 37 f.

⁹²³ SACEM, *Les Français et la musique*, Studie durchgeführt durch das Institut Opinionway, Januar 2011, abrufbar unter:

http://www.sacem.fr/files/content/sites/fr/files/mediatheque/sacem/presse/etudes/etude%20sacem/sondage_francais_musique/sondage_les_francais_et_la_musique_2011.pdf.

⁹²⁴ Dies sind nach den Daten der Studie 41 Prozent der Gesamtbevölkerung.

⁹²⁵ *Pratiques et attentes des internautes*, a.a.O., Folie 12. Die Nutzung illegaler direkter Downloadangebote gestanden 8 Prozent ein.

⁹²⁶ *Pratiques et attentes des internautes*: la consommation de contenus culturels sur Internet, September 2009, abrufbar unter: <http://www.culture.gouv.fr/mcc/Espace-Presse/Dossiers-de-presse/Rapport-Creation-et->

Festzuhalten bleibt, dass zwar eine große Zahl an Internetnutzern der eigenen Einschätzung zufolge bereits einmal auf unrechtmäßige Weise auf urheberrechtlich geschützte Inhalte zugegriffen hat. Für die überwiegende Mehrzahl der Nutzer stellt dies jedoch kein übliches Handeln dar.

3) *Gerechtigkeitsempfinden und Verständnis für Interessen der Urheber*

Die Motivation zur Achtung von Rechten kann ursächlich in der Gefahr einer Sanktionierung des Verstoßes begründet liegen. Sie kann aber auch in ethisch-moralischem Verständnis ihre Grundlage haben, für die Akzeptanz eine wesentliche Grundlage bildet.

Warnhinweismodelle wurden in den dargestellten Staaten u.a. als Beitrag zur Aufklärung eingerichtet. Dieser Ansatz folgt der Annahme, einem beträchtlichen Teil der Rechteverletzer sei nicht bewusst, dass ihr Verhalten die Rechte und moralischen Interessen anderer in nicht unerheblichen Maß beeinträchtigt. Im Vereinigten Königreich etwa war es ein ganz zentrales Anliegen des Gesetzgebers, den Empfänger des Warnhinweises über die Rechtswidrigkeit seines Verhaltens und die möglichen hieraus resultierenden Konsequenzen für andere zu informieren. Bezweckt werden sollte damit letztlich, den Internetnutzer zu veranlassen, sein Verhalten zu ändern. Ob oder inwieweit dies gelingen mag, ist nicht unumstritten. So wird vertreten, dass pragmatische Belange bei den Internetnutzern in jedem Fall gegenüber moralischen Bedenken obsiegen.⁹²⁸ Nachweise für diese These gibt es nicht. Der britische *High Administrative Court* ging seinerseits indes davon aus, dass die Annahme, dass Verbraucher nur zur Verfolgung ihrer eigenen wirtschaftlichen Interessen handeln und nicht rational auf moralische, altruistische oder nachhaltige Aspekte reagieren, heutzutage überholt sei.⁹²⁹

4) *Erkennbare Verhaltensänderungen*

Vor diesem Hintergrund stellt sich die Frage, ob und wenn ja welche Änderungen durch die Einführung eines Warnhinweissystems auf das Verhalten dieser Gruppe von Internetnutzern erkennbar sind.

a) *Auswirkung von Warnhinweisen auf Nutzerverhalten*

Nach den Ergebnissen des 2008 Digital Entertainment Survey aus dem Vereinigten Königreich⁹³⁰ gaben 70 Prozent der Personen, die unautorisierte Inhalte im Internet nutzen, an, dass sie illegales Filesharen im Internet einstellen würden, wenn sie einen Warnhinweis

Internet (dort angefügt, S. 69 ff., an den Bericht von *Zelnik/Toubon/Cerutti* an den Kultus- und Kommunikationsminister, *Rapport au Ministre de la Culture et de la Communication*, Januar 2010).

⁹²⁷ *Pratiques et attentes des internautes*, a.a.O., Folie 6.

⁹²⁸ *Karaganis*, S.34.

⁹²⁹ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 233.

⁹³⁰ 2008 Digital Entertainment Survey. Es wurden 1.608 Personen im Alter zwischen 15 und 54 Jahre, zu jeweils 50 Prozent männlich bzw. weiblich und aus verschiedenen Regionen des Landes, befragt. *Wiggin& Entertainment Media Research 2008*, S. 5.

von ihrem Diensteanbieter erhielten.⁹³¹ Am höchsten war der Anteil bei den Teenagern (78 Prozent der männlichen Teenager und 75 Prozent der weiblichen Teenager).⁹³² Im Rahmen einer erneuten Befragung im Folgejahr waren es nur noch 33 Prozent der Internetnutzer. Ihr lag jedoch eine veränderte Fragestellung zugrunde. Die Befragten sollten nämlich ausdrücklich davon ausgehen, eine Mitteilung von ihrem Diensteanbieter zu erhalten, die keine Sanktion androhte.⁹³³ Die Werte aus den Jahren 2008 und 2009 sind daher nicht ohne weiteres vergleichbar. Die Ergebnisse aus dem Jahr 2009 können jedoch als weiteres Indiz für die Bedeutung der Rechtsdurchsetzung gewertet werden.⁹³⁴

Prognostische Befragungen wurden auch in Deutschland durchgeführt. Nach einer Befragung im Februar 2011 sind 57 Prozent der deutschen Bevölkerung der Ansicht, dass Warnhinweise Nutzer illegalen Filesharings dazu bewegen würden, diese Praxis einzustellen.⁹³⁵ Die Befragten sollten von dem Szenario ausgehen, dass die Versendung des Warnhinweises in einer Sanktion, wie etwa die Verhängung von Bußgeld, die Einschränkung der Nutzungsintensität des Internetzugangs, die Reduktion der Datenübertragungsgeschwindigkeit oder die zeitweise Aussetzung des Internetanschlusses, münde.⁹³⁶ 31 Prozent gehen vor diesem Hintergrund davon aus, Nutzer würden bereits nach einem ersten Warnhinweis die illegale Nutzung einstellen, 26 Prozent, dies würde nach dem zweiten Warnhinweis geschehen. 43 Prozent sind der Ansicht, die Versendung eines Warnhinweises bliebe ohne Auswirkungen.⁹³⁷ Höher ist der Anteil unter denjenigen, die Medieninhalte illegal herunterladen. Von ihnen gehen 81 Prozent davon aus, dass Warnhinweise Nutzer dazu bewegen würden, illegales Filesharing einzustellen.⁹³⁸

In Frankreich war, noch bevor das Warnhinweissystem etabliert wurde, im Rahmen der IPSOS-Studie ermittelt worden, welche potentielle Wirkung Warnhinweise auf das Verhalten der Internetnutzer hätten. Dort gaben zu diesem Zeitpunkt insgesamt **90 Prozent** der Befragten (bzw. 88 Prozent derjenigen, die zugaben, unautorisiert Inhalte herunterzuladen) an, dass sie illegales Downloaden spätestens nach der zweiten Verwarnung **einstellen würden**.⁹³⁹ Derart hohe Erwartungen konnten die auf die Einführung des Warnhinweissystems in Frankreich folgenden Untersuchungen jedoch nicht bestätigen.

Ende 2009, also kurz nachdem das erste Hadopi-Gesetz von der französischen Nationalversammlung verabschiedet worden war, wurde unter Beteiligung der Universität Rennes

⁹³¹ *Wiggin& Entertainment Media Research 2008*, S. 13.

⁹³² *Wiggin& Entertainment Media Research 2008*, S. 13.

⁹³³ 2009 Digital Entertainment Survey. Befragt wurden 1.512 Nutzer im Vereinigten Königreich im Mai 2009. *Wiggin& Entertainment Media Research 2009*.

⁹³⁴ *Wiggin& Entertainment Media Research 2009*.

⁹³⁵ *DCN-Studie*, S. 48.

⁹³⁶ *DCN-Studie*, S. 48.

⁹³⁷ *DCN-Studie*, S. 48.

⁹³⁸ *DCN-Studie*, S. 49.

⁹³⁹ *IPSOS, Les Français face au téléchargement illégal de musique sur Internet - Les chiffres et résultats complets du sondage*, 26.5.2008, abrufbar unter: <http://www.ipsos.fr/ipsos-public-affairs/sondages/francais-face-au-telechargement-illegal-musique-sur-internet>.

eine Studie erstellt, die ebenfalls das Nutzerverhalten zum Untersuchungsgegenstand hatte. Interviewt wurden 2.000 Personen, die einen repräsentativen Querschnitt für die Region Bretagne darstellten. Nach den auf dieser Befragung basierenden Auswertungen stellten **15 Prozent** derjenigen, die bis dato Musik und Videos über Peer-to-Peer-Netze im Internet konsumierten, die **Nutzung dieses Verbreitungsweges** nach Verabschiedung des Hadopi-Gesetzes **ein**.⁹⁴⁰ Lediglich **ein Drittel** von ihnen gab jedoch an, die illegale Nutzung von Musik und Videos **gänzlich aufgegeben** zu haben. Zwei Drittel reduzierten demnach ihr Konsumverhalten allenfalls und stellten es lediglich auf andere Nutzungsarten um. Insgesamt wurde sogar eine **dreiprozentige Steigerung der illegalen Nutzung** urheberrechtlich geschützter Inhalte in den drei Monaten nach Verabschiedung des Hadopi-Gesetzes festgestellt.⁹⁴¹

Eine vergleichbare Frage wurde in einer im Auftrag der Hadopi im Frühjahr 2011, also mehr als ein Jahr später, durchgeführten Untersuchung gestellt, in deren Rahmen 1.500 Internetnutzer einbezogen waren.⁹⁴² Von den Befragten erklärten **sieben Prozent**, dass sie selbst, eine Person aus ihrem Haushalt oder jemand aus ihrem näheren Umfeld bereits einen **Warnhinweis von der Hadopi erhalten** hätten.⁹⁴³ Von diesen Internetnutzern gab die **Hälfte** an, seitdem **keine illegale Nutzung** von Inhalten im Internet mehr zu tätigen, und weitere 22 Prozent, die illegale Nutzung zumindest eingeschränkt zu haben. Ein Viertel gab sich unbeeindruckt.⁹⁴⁴

Im Rahmen der zweiten im Auftrag der Hadopi durchgeführten Studie gaben fast **zwei Drittel** (64 Prozent) der Befragten an, innerhalb der letzten zwölf Monate Inhalte im Internet **ausschließlich legal** genutzt zu haben.⁹⁴⁵ Rückschlüsse auf eine Tendenz lassen sich hieraus, auch im Vergleich zur ersten Studie (zwischen den Befragungen lagen sechs bzw. neun Monate),⁹⁴⁶ indes nicht ziehen. Hier hatten 51 Prozent der Befragten angegeben, noch niemals Inhalte illegal im Internet genutzt zu haben.⁹⁴⁷ Eine zeitliche Begrenzung lag der Fragestellung hier nicht zugrunde.

Nach Daten der IFPI ist die Peer-to-Peer-Nutzung in Frankreich im Zeitraum zwischen April 2010 und April 2011 um insgesamt **31 Prozent** gesunken mit einem deutlichen Einbruch

⁹⁴⁰ Dejean/Pénard/Suire, M@rsouin/CREM/Université de Rennes 1, Une première évaluation des effets de la loi Hadopi sur les pratiques des internautes français, März 2010, abrufbar unter: <http://www.marsouin.org/IMG/pdf/NoteHadopix.pdf>, S. 198, Fn. 878.

⁹⁴¹ Dejean/Pénard/Suire, M@rsouin/CREM/Université de Rennes 1, Une première évaluation des effets de la loi Hadopi sur les pratiques des internautes français, März 2010, abrufbar unter: <http://www.marsouin.org/IMG/pdf/NoteHadopix.pdf>, S. 198, Fn. 878.

⁹⁴² Hadopi, 2ème vague barométrique, a.a.O.

⁹⁴³ Hadopi, 2ème vague barométrique, a.a.O., Folie 27.

⁹⁴⁴ Zwei Prozent gaben an, dass Internet noch verstärkt für die illegale Nutzung von Werken zu nutzen. Hadopi, 2ème vague barométrique, a.a.O., Folien 26, 28.

⁹⁴⁵ Hadopi, 2ème vague barométrique, a.a.O., Folie 45. Aufschlüsselung nach Altersstufen, dort Folien 46, 47.

⁹⁴⁶ Hadopi, biens culturels et usages d'internet: pratiques et perceptions des internautes français (Erste Untersuchung der Hadopi, vorgelegt am 23.1.2011), abrufbar unter: <http://www.hadopi.fr/download/hadopiT0.pdf>.

⁹⁴⁷ Hadopi, pratiques et perception, a.a.O., Folie 59.

zum Zeitpunkt der Versendung der ersten Warnhinweise.⁹⁴⁸ Über die Methodik der Erhebung dieser Daten ist indes nichts Näheres bekannt.

Zur Frage, ob die **Existenz der Hadopi** generell zu einer Veränderung des Nutzungsverhaltens (im Hinblick auf den Bezug von Musik, Videos, Büchern, Fernsehserien, Fotos und Software über das Internet) geführt hat, stimmten dem in der zweiten Befragung der Hadopi 41 Prozent der Befragten zu, insgesamt 48 Prozent sahen ihr Verhalten nicht bzw. eher nicht als durch die Hadopi beeinflusst an. Die Zahlen zeigten insofern eine deutliche Veränderung im Vergleich zur ersten Befragung durch die Hadopi im Jahr 2010. Hier hatten insgesamt nur 25 Prozent eine Verhaltensänderung bejaht.⁹⁴⁹ Diese Veränderungen beziehen sich sowohl auf das legale als auch auf das illegale Nutzungsverhalten.⁹⁵⁰ Von denen, die angaben, über das Internet illegale Nutzung von Werken zu tätigen, und zugleich angaben, dass die Existenz der Hadopi ihr Verhalten verändert hätte, gaben **38 Prozent** an, die **illegale Nutzung vollständig eingestellt** zu haben, 55 Prozent gaben an, ihren Konsum reduziert zu haben. Sieben Prozent gaben an, dass sich der illegale Konsum selbst nicht wesentlich verändert habe;⁹⁵¹ dies lässt darauf schließen, dass dieser Teil der Nutzer im Wesentlichen auf andere Quellen bzw. Nutzungsarten umgeschwenkt hat.

Die Frage, inwieweit Internetnutzer ihre Aktivitäten auf andere Wege und technische Möglichkeiten verlagert haben, ist im Detail nicht geklärt. Die Hadopi, die selbst diese Frage in ihrem Tätigkeitsbericht aufwirft,⁹⁵² hat eine Studie in Auftrag gegeben, die sich mit den Auswirkungen beschäftigt. Eine weitere Studie soll die rechtlichen Grenzen der Überprüfung der Nutzung von Streamingdiensten aufzeigen.

Nach Daten der IFPI hat der generelle Anstieg der Internetaktivität keine Entsprechung gefunden in der Nutzung unlizenzierter Dienste im Internet. Trotz einer Steigerung der Internetaktivität im Zeitraum von April 2010 bis April 2011 um zehn Prozent sei eine Verringerung des Zugriffs auf unlizenzierte Angebote um sieben Prozent zu verzeichnen gewesen: Während im April 2010 etwa 24 Prozent der Internetnutzer unlizenzierte Angebote konsumiert hätten, seien es im April 2011 rund 20 Prozent gewesen. Seit Beginn der Versendung der ersten Warnhinweise sei die Nutzung um zwölf Prozent zurückgegangen.⁹⁵³

Soweit es die Umsatzzahlen der verschiedenen Branchen betrifft, ist eine Auswirkung des in Frankreich eingeführten Warnhinweismodells nicht mit Sicherheit herzuleiten.

Für die Umsatzzahlen der französischen Musikindustrie lässt sich dabei auf verschiedene Quellen zurückgreifen. Gemeinsam bescheinigen diese der Musikbranche zwar stetig sin-

⁹⁴⁸ IFPI, *Measuring the Impact of Graduate Response*, July 2011, S. 2.

⁹⁴⁹ 52 Prozent votierten dafür, dass die Hadopi ihr Verhalten „nicht“ bzw. „eher nicht“ beeinflusst habe, vgl. *Hadopi, 2ème vague barométrique*, a.a.O., Folie 16. Aufschlüsselung im Einzelnen nach Altersgruppen, *Hadopi, 2ème vague barométrique*, a.a.O., Folie 18.

⁹⁵⁰ Hierzu die Aufschlüsselung im Einzelnen, *Hadopi, 2ème vague barométrique*, a.a.O., Folie 17.

⁹⁵¹ *Hadopi, 2ème vague barométrique*, a.a.O., Folie 19, 20.

⁹⁵² Bericht abrufbar unter: <http://www.hadopi.fr/sites/default/files/page/pdf/rapport-d-activite-hadopi.pdf> (Seite 8-9).

⁹⁵³ IFPI, *Measuring the Impact of Graduate Response*, July 2011, S. 2.

kende Umsätze, unterscheiden sich dabei jedoch in den zugrunde gelegten Untersuchungsgegenständen und angegebenen Werten.

Der Bundesverband der Musikindustrie untersuchte zunächst die Umsatzzahlen allein des französischen Tonträgermarktes in den Jahren 2007 und 2008, der sich demnach wie folgt darstellt:

	2007	2008	Zuwachs/Verlust
Umsatz in Mio. €	1.175,0	1.060,5	- 9,7 %

Werte entnommen aus: Bundesverband Musikindustrie, Musikindustrie in Zahlen 2009, S. 50

Den Umsatz der französischen Musikindustrie für die Jahre 2009 und 2010 gab der Bundesverband der Musikindustrie indes insgesamt für den physischen und den digitalen Musikverkauf wie folgt an:

	2009	2010	Zuwachs/Verlust
Umsatz in Mio. €	993,3	965,5	- 2,8 %

Werte entnommen aus: Bundesverband Musikindustrie, Musikindustrie in Zahlen 2010, S. 61.

Die IFPI veröffentlichte in einer Studie von 2011 detaillierte Umsatzzahlen für die Jahre 2006 bis 2010, die zwischen physischem und digitalem Musikverkauf sowie Aufführungsrechten differenzieren:

Jahr	Physischer Musikverkauf in Mio. \$	Digitaler Musikverkauf in Mio \$	Aufführungsrechte	Umsatz in Mio. \$	Umsatz in Mio. €	Verlust/ Zuwachs
2010	641,1	146,1	78,1	865,3	649,5	- 5,1 %
2009	704,1	128,7	79,4	912,2	684,1	- 2,4 %
2008	728,8	128,7	77,5	935,0	701,3	- 12,9 %
2007	910,3	92,9	70,4	1.073,5	805,2	- 15,5 %
2006	1.126,0	75,6	69,0	1.270,6	952,9	- 8,4 %

Werte entnommen aus: IFPI, Recording Industry in Numbers 2011, S. 45.

Darüber hinaus belegt die SNEP (Syndicat national de l'édition phonographique)⁹⁵⁴ der französischen Musikindustrie von 2008 bis hin zu den ersten neun Monaten des Jahres 2011 die folgenden Umsätze:

Jahr	Physischer Musikverkauf	Digitaler Musikverkauf	Umsatz in Mio. €	Verlust/ Zuwachs
2011 (ersten 9 Monate)	242,2	79,1	321,3	- 5,7 %
2010	466,3	88,1	554,4	- 5,9 %
2009	512	75,8	587,8	- 3,2 %
2008	530	76,3	606,3	- 15 %

Werte entnommen aus: SNEP, Les chiffres du marché, abrufbar unter:
<http://www.disqueenfrance.com/fr/catalogpage1list.xml?cat=251362> (Stand: 19.01.2012).

Aufgrund der verschiedenen Untersuchungsgegenstände sind die angegebenen Gesamtumsätze nur bedingt vergleichbar. Gleichwohl bescheinigen alle Quellen zunächst einen erkennbaren Umsatzrückgang im Jahr 2008 (Bundesverband der Musikindustrie: - 9,7 %; IFPI: - 12,9 %; SNEP: - 15 %). Hingegen soll im Jahr 2009 ein geringerer Umsatzrückgang zu verzeichnen gewesen sein (IFPI: - 2,4%; SNEP: -3,2 %), während dieser 2010 wiederum anstieg (IFPI: - 5,1%; SNEP: - 5,9%).

Ordnet man diese Werte zeitlich den Ereignissen um das französische Warnhinweismodell zu, so ist der Umsatz der Musikindustrie im Jahr 2009, in dem das HADOPI-Gesetz auf seine Verfassungsmäßigkeit hin überprüft und schließlich verabschiedet worden ist, nur noch leicht gesunken. In dem ersten Jahr seines Inkrafttretens 2010 jedoch, hatte die französische Musikindustrie sogleich wieder höhere Verluste zu verzeichnen.

Ob die dargelegten Umsatzschwankungen, vor allem in 2009, aber tatsächlich auf die Entwicklungen in Frankreich zurückzuführen sind, lässt sich nicht sagen. Andere Ursachen sind hier möglich.

Auch die Umsatzwerte der anderen Branchen besitzen insoweit keine weitergehende Aussagekraft.

Die Umsatzzahlen der Filmbranche (Kino) halten sich nach den Angaben der SEVN (Syndicat de l'Édition Vidéo Numérique⁹⁵⁵) seit 2008 im Wesentlichen konstant und können sogar ein leichten Umsatzzuwachs verzeichnen:

⁹⁵⁴ Dt.: Nationale Gewerkschaft für das phonographische Verlagswesen.

⁹⁵⁵ Dt.: Gewerkschaft für das digitale Videoverlagswesen.

Jahr	Umsatz in Mio. €
2011 (ersten 9 Monate)	495,12
2010	837,10
2009	799,71
2008	779,17

Werte entnommen aus: SEVN, Les chiffres de la vidéo, abrufbar unter: http://www.sevn.fr/?page_id=6.

Demnach konnte die Kinofilmbranche im Jahr 2009 ein Plus von mehr als 20 Mio. € (2,56 %) verbuchen, im Jahr 2010 von mehr als 37 Mio. € (4,4 %).

Für die Buchbranche bescheinigen nationale Quellen die folgenden Umsatzzahlen:

Jahr	Bücher Umsatz in Mio. € ⁹⁵⁶	eBooks Umsatz in Mio. €
2011 (ersten 9 Monate)	2.703	noch nicht erfasst
2010	2.800 ⁹⁵⁷	52,9 ⁹⁵⁸
2009	2.829	49 (exl. Steuern), entspricht 1,8 % des ges. Umsatzes ⁹⁵⁹
2008	2830	keine Angaben

Die wenigen Angaben für eBooks besitzen keine Aussagekraft. Im Bereich der herkömmlichen Bücher blieben die Umsätze der Branche seit 2008 stabil. Auswirkungen des französischen Warnhinweismodells auf den Umsatz lassen sich hier nicht erkennen.

Gleiches gilt für den Bereich Video (DVD u. Bluray) für den die SEVN folgende Umsatzzahlen angibt:

⁹⁵⁶ Chiffres clés de la culture, abrufbar unter: <http://www2.culture.gouv.fr/culture/deps/chiffres-cles2011/11-livres-2011.pdf>.

⁹⁵⁷ Quelle: <http://www.ipsos.fr/ipsos-mediact/actualites/bilan-marche-livre-2010-annee-pleine-surprises> (Stand: 16.01.2012).

⁹⁵⁸ Quelle: <http://www.actualitte.com/actualite/monde-edition/economie/exclusif-en-france-l-ebook-represente-1-8-du-chiffre-d-affaires-26864.htm> (Stand: 16.01.2012).

⁹⁵⁹ Quelle : Chiffres clés 2009, abrufbar unter: http://www.centrenationaldulivre.fr/IMG/pdf/Chiffres-cles_2009-2010.pdf (Stand: 16.01.2012).

Jahr	Umsatz in Mio. €	Verlust/ Zuwachs
2011 (ersten 9 Monate)	801,99	- 8,8 %
2010	1.385,30	- 0,32 %
2009	1.389,81	+ 0,5 %
2008	1.382,25	

Werte entnommen aus: SEVN, Les chiffres de la vidéo, abrufbar unter: http://www.sevn.fr/?page_id=6.

Die Umsatzzahlen dieser Branche sind seit einem leichten Zuwachs 2009 ab 2010 gesunken. Rückschlüsse auf die Wirksamkeit des Warnhinweisverfahrens können hier nicht gezogen werden.

Insoweit sind die Ergebnisse weiterer Recherchen abzuwarten. Einen Versuch einen direkten Zusammenhang zwischen der Einführung des Warnhinweismodells in Frankreich und dessen Effekt auf die Musikverkäufe über die digitale Vertriebsplattform iTunes nachzuweisen, ist Gegenstand einer Studie von *Danaher, Smith, Telang* und *Chen* aus den USA.⁹⁶⁰ Sie betrachtet die Verkaufszahlen der vier Major-Labels⁹⁶¹ für die Verkäufe über iTunes für den Zeitraum vom 28. Juli 2008 bis Mai 2011. Ab dem Zeitpunkt, ab welchem bei der französischen Bevölkerung ein Bewusstsein dafür entstand, dass mit der Einführung des Warnhinweismodells Urheberrechtsverletzungen im Internet zukünftig sanktioniert werden können, stellte die Studie einen Anstieg der Einzeltrack-Verkäufe um **22,5 Prozent** und der Album-Verkäufe über iTunes um **25 Prozent** fest.⁹⁶² Den Zeitpunkt der Bewusstseinsbildung bei der Bevölkerung bestimmten sie anhand von Google-Trends⁹⁶³ für März 2009. In den Vergleichsländern Vereinigtes Königreich, Italien, Spanien, Deutschland und Belgien⁹⁶⁴ war kein ähnlich starker Anstieg im selben Zeitraum zu verzeichnen. Daher sieht die Studie als Ursache für den Anstieg der Verkaufszahlen die seinerzeit anstehende Gesetzesänderung an.⁹⁶⁵ Ausgehend von dieser These, wurde der Anstieg der Verkaufszahlen für die unterschiedlichen Musik-Genres untersucht und mit folgender Erwägung belegt: Wenn die Umsatzzuwächse auf zurückgehendes Piraterieverhalten der Nutzer mit Blick auf die bevorstehende Gesetzesänderung zurückzuführen sind, dann müsste der Anstieg bei den stärker von Piraterie betroffenen Genres höher sein, als bei den weni-

⁹⁶⁰ Verfügbar seit dem 21.01.2012 unter: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989240

⁹⁶¹ Universal Music, Warner Music, EMI und Sony Music.

⁹⁶² *Danaher, Smith, Telang, Chen*, S.2.

⁹⁶³ Anzahl der Eingabe der Suchbegriffe „Hadopi“ oder den französischen Begriff für „Three Strikes Law“; *Danaher, Smith, Telang, Chen*, S.10.

⁹⁶⁴ *Danaher, Smith, Telang, Chen*, S.8.

⁹⁶⁵ *Danaher, Smith, Telang, Chen*, S.15.

ger betroffen.⁹⁶⁶ Die Überprüfung ergab, dass der Anstieg in dem am stärksten von Piraterie betroffenen Genre (Rap/HipHop) mit 30 Prozent, wesentlich höher war, als in anderen Genres.⁹⁶⁷ Bei den am geringsten betroffenen Genres (wie Christliche Musik, Klassik, Jazz) wurde lediglich ein Anstieg von 7 Prozent ermittelt.⁹⁶⁸

Auf dieser Grundlage bezifferten *Danaher u.a.* die Effekte der Einführung der Warnhinweisregelung. Dazu wurden bei iTunes-Verkäufen die tatsächlichen Verkaufszahlen unter Berücksichtigung des Warnhinweissystems den hypothetischen Zahlen unter Ausblenden des Warnhinweissystems gegenüber gestellt und die Differenz berechnet. Bei den über iTunes verkauften Einzeltracks wurde im Untersuchungszeitraum ein **Mehrumsatz** von 4,7 Mio. Euro und bei Alben-Verkäufen ein solcher von 4,9 Mio. Euro errechnet.⁹⁶⁹ Insgesamt ergibt sich damit eine Umsatzsteigerung bei den iTunes-Verkäufen von 9,6 Mio. Euro.⁹⁷⁰ Die vier untersuchten Major-Labels halten 70 Prozent der Marktanteile in Frankreich, während die in der Untersuchung nicht berücksichtigten Independent Labels 30 Prozent ausmachen.⁹⁷¹ Geht man davon aus, dass die nicht berücksichtigten Independent Labels denselben Anstieg verzeichneten und rechnet man diesen Effekt auf sie um, so ergibt sich eine Umsatzsteigerung bei den iTunes-Verkäufen von insgesamt **13,8 Mio. Euro**.⁹⁷²

Der Effekt der ansteigenden Verkaufszahlen bei iTunes stellte sich ein, bevor die Warnhinweisregelung in Kraft trat, also insbesondere bevor Verstöße strafrechtlich verfolgt wurden.⁹⁷³ Da das Gesetzesvorhaben im Zusammenhang mit der Illegalität von Filesharing vor und nach Inkrafttreten in den Medien diskutiert wurde und die Hadopi-Behörde Aufklärungskampagnen zur Illegalität von Filesharing und zu legalen Alternativen betrieben hat⁹⁷⁴, kann die Studie keine verbindliche Aussage darüber treffen, ob die gemessenen Effekte gänzlich den drohenden Sanktionen oder einer Kombination aus Sanktionen, Medieninteresse und Bildung bzw. Aufklärung der Nutzer zuzuschreiben sind.⁹⁷⁵ Hier sehen die Verfasser Bedarf für weitere Recherche.⁹⁷⁶

Zu berücksichtigen ist, dass die Studie nur die Musikbranche und den Vertriebskanal iTunes ins Auge fasst.⁹⁷⁷ Über die Auswirkungen der Hapodi-Gesetzgebung insgesamt gibt sie also nur teilweisen Aufschluss.⁹⁷⁸ Unberücksichtigt bleibt der Effekt der Gesetzesänderung auf den Verkauf physischer Tonträger sowie auf weitere legale, digitale Musiknut-

⁹⁶⁶ *Danaher, Smith, Telang, Chen, S.3.*

⁹⁶⁷ *Danaher, Smith, Telang, Chen, S.3.*

⁹⁶⁸ *Danaher, Smith, Telang, Chen, S.3.*

⁹⁶⁹ *Danaher, Smith, Telang, Chen, S.17.*

⁹⁷⁰ *Danaher, Smith, Telang, Chen, S.17.*

⁹⁷¹ *Danaher, Smith, Telang, Chen, S.8*

⁹⁷² *Danaher, Smith, Telang, Chen, S.17.*

⁹⁷³ *Danaher, Smith, Telang, Chen, S.18.*

⁹⁷⁴ *Danaher, Smith, Telang, Chen, S. 18.*

⁹⁷⁵ *Danaher, Smith, Telang, Chen, S.18.*

⁹⁷⁶ *Danaher, Smith, Telang, Chen, S.18.*

⁹⁷⁷ *Danaher, Smith, Telang, Chen, S.18.*

⁹⁷⁸ *Danaher, Smith, Telang, Chen, S.19.*

zung.⁹⁷⁹ Der Effekt auf die Verkaufszahlen anderer Branchen wie Film, Fernsehen, Buch etc. bleibt ebenfalls ungeprüft.⁹⁸⁰ Legt man zugrunde, dass in den nicht untersuchten Bereichen ähnlich positive Verkaufsanstiege zu verzeichnen sind, schließen *Danahe u.a.*, dass die durch die Gesetzesänderung hervorgerufenen Effekte auf die **Umsatzsteigerung** der betroffenen Branchen weitaus **höher** sein müssen, **als** die von ihnen **berechneten Zahlen**.⁹⁸¹ Dass die für iTunes ermittelten Zuwächse pauschal übertragen werden können, erscheint indes angesichts der hier zugrunde gelegten, tatsächlich gemessenen Umsatzzahlen nicht sicher.

Für die **Republik Irland** liegen im Wesentlichen keine „offiziellen“ Daten zur verhaltenssteuernden bzw. –ändernden Wirkung des dort praktizierten **„Graduated Response“-Verfahrens** vor. Medienberichten zu Folge wurde bislang kein Anschluss eines Eircom-Kunden wegen viermaliger Rechtsverletzung abgeschaltet, zahlreiche Internet-Zugänge sollen aber für sieben Tage unterbrochen worden sein.⁹⁸² Im Übrigen liegt dem Verfasser der Studie Datenmaterial vor, das ihm von den an dem Verfahren beteiligten Provider (Eircom Ltd.) und den betreffenden Rechteinhabern zur Verfügung gestellt wurde. Diese Daten hat der Verfasser der Studie auch ausgewertet. Die konkreten Ergebnisse dürfen allerdings nicht veröffentlicht werden, weil die Daten selbst von den Betroffenen bis zur Fertigstellung dieser Studie **nicht zur Veröffentlichung freigegeben** wurden. Der Hinweis auf eine Tendenz ist aber gestattet. Danach lässt sich festhalten, dass die Warnhinweisregelung nur bei solchen Kunden deutlich gewirkt hat, die selbst konkret von einem Warnhinweis bzw. einer Sanktion betroffen waren. Des Weiteren existieren von IFPI erhobene Daten zu den in der Republik Irland in der Zeit von 2006 bis 2010 mit dem Verkauf aufgenommener Musik erzielten **Umsätzen**.⁹⁸³ Danach ist in diesem Zeitraum der Gesamtumsatz stetig zurückgegangen⁹⁸⁴:

Recorded Music Sales (US\$ million, trade value)

	Physical	Digital	Total (US\$)	Total (EUR)	Total % Change
2010	45.4	13.5	58.9	44.2	-16.9%
2009	58.5	12.4	70.9	53.2	-25.9%
2008	85.3	10.4	95.7	71.8	-17.5%
2007	108.0	8.0	116.0	87.0	-7.7%
2006	121.5	4.3	125.8	94.3	-2.3%

Note: Performance rights revenues not included.

⁹⁷⁹ *Danaher, Smith, Telang, Chen*, S.19.

⁹⁸⁰ *Danaher, Smith, Telang, Chen*, S.19.

⁹⁸¹ *Danaher, Smith, Telang, Chen*, S.19 f.

⁹⁸² *McIntyre*, Christmas and New Year privacy roundup, veröffentlicht am 12.1.2012, abrufbar unter: <http://www.tjmcintyre.com/2012/01/christmas-and-new-year-privacy-roundup.html> (unter Berufung auf Tighe von der Sunday Times).

⁹⁸³ IFPI, Recording Industries in Numbers 2011.

⁹⁸⁴ IFPI, Recording Industries in Numbers 2011, S. 49.

Insgesamt ist dieser Umsatz von 125,8 US\$ million (2006) auf 58,9 US\$ million (2010), d. h. um 66,9 US\$ million bzw. ca. 53,2 % gefallen.⁹⁸⁵ Während der Umsatz bei den physischen Tonträgern deutlich um 76,1 US\$ million bzw. 62,6 % abgenommen hat,⁹⁸⁶ ist er allerdings bei digitaler Musik diametral um 9,2 US\$ million bzw. 214 % angestiegen. Hat dabei in dem Zeitraum von 2006 bis 2009 der Rückgang des Gesamtumsatzes kontinuierlich zugenommen, so lässt sich im Jahre 2010 insoweit eine „Trendwende“ feststellen, als der Rückgang in den Umsatzzahlen insgesamt erstmals rückläufig, d. h. nicht weiter angestiegen ist und leicht unter dem Niveau des Jahres 2008 liegt. Die Aussagekraft dieses Zahlenmaterials ist freilich gering. Denn zum einen ist den Zahlen schon nicht zu entnehmen, ob und inwieweit der Umsatzrückgang in Irland auf illegalem P2P-Filesharing oder sonstiger Internet-Piraterie beruht, die wirtschaftlichen Einbußen der irischen Musikindustrie also kausal auf dieses Verhalten zurückzuführen sind. Zum anderen und insbesondere lassen sich aus den Umsatzzahlen auch umgekehrt **keine eindeutigen Schlüsse zu den Auswirkungen der irischen Warnhinweis-Regelung** ziehen. Zwar hat sich der Umsatzrückgang insgesamt bei legalen Verkäufen im Jahre 2010 zum ersten Mal seit der Datenerhebung im Jahre 2006 abgeschwächt.⁹⁸⁷ Unklar ist aber auch hier, ob und inwieweit für diesen Umstand (gerade) das „*Graduated Response*“-Verfahren ursächlich ist. Die Auswirkungen des Verfahrens auf das Nutzerverhalten im Internet sind dabei umso fraglicher, als dieses nach einer dreimonatigen Testphase erst im August 2010 fest installiert wurde. Umsatzzahlen der irischen Musikindustrie für das Jahr 2011 liegen bislang nicht vor.⁹⁸⁸ Nach Analyse von IFPI gibt es jedenfalls keinen Hinweis, dass seit der Einführung der Warnhinweisregelung „Internet-Piraterie“ in Irland insgesamt abgenommen hat. Dies stimmt in etwa mit einer Einschätzung des Providers überein, wonach sich die Wirkung der Warnhinweisregelung nicht auf den übrigen Markt übertragen hat.

b) Bedeutung von Sanktionen

Die dargelegten Warnhinweismodelle haben gemeinsam, dass die Versendung eines Hinweises als Mittel der Aufklärung und Verwarnung der Anwendung repressiver Maßnahmen vorangestellt ist. Es stellt sich insofern die Frage, inwieweit die Anzeichen eines positiven

⁹⁸⁵ Nach anderer Quelle hat die irische Musikindustrie zwischen 2005 und 2009 einen Verlust bei den Verkaufswerten in Höhe von 40 % hinnehmen müssen; vgl. http://irma.ie/breaking_news.htm (Nachricht vom 16th April 2010 – Overwhelming Victory for Irish Artists in High Court).

⁹⁸⁶ Nach anderer Quelle ist der Umsatz bei CD-Verkäufen in Irland von € 146 million im Jahre 2006 auf € 56 million im Jahre 2010; vgl. O'Halloran, *Illegaldownloading to be curbed by Government order*, *The Irish Times* vom 19.12.2011 (abrufbar unter:

<http://www.irishtimes.com/newspaper/frontpage/2011/12/19/1224309259318.html>) unter Berufung auf „offizielle Zahlen“, die freilich von dem Autor des Artikels nicht weiter belegt werden.

⁹⁸⁷ Diese Abschwächung lässt sich nicht (allein) auf eine entsprechende Umsatzsteigerung bei den Verkäufen digitaler Musik zurückführen.

⁹⁸⁸ Laut EMI (Ireland) hat sich der *Gewinn* des Unternehmens im Finanzjahr 2011 allerdings nahezu halbiert, was hauptsächlich der „Internet-Piraterie“ zugeschrieben wird; vgl. *Madden, IRMA launches action against State over anti-piracy order*, *The Irish Times* vom 12.1.2012, (abrufbar unter: <http://www.irishtimes.com/newspaper/finance/2012/01/12/1224310141468.html>).

Effekts auf den Umfang von Urheberrechtsverletzungen im Internet allein Gründen der Aufklärung folgen oder aus der Androhung einer Konsequenz, namentlich einer Sanktionierung erneuter Verstöße, resultieren.

Eindeutige Erkenntnisse hierzu liegen, wie mitunter bereits erwähnt, nicht vor. Indes weisen Ergebnisse der Befragungen und Erfahrungswerte darauf hin, dass rechtliche Konsequenzen eine nicht unerhebliche Rolle dabei spielen, wie effektiv sich der Hinweis bzw. die Verwarnung im Verhalten der Nutzer widerspiegelt. Zu erwarten ist, dass die ernstzunehmende Androhung von Konsequenzen den edukativen Effekt eines Warnhinweises, wenn auch nicht bedingen, so doch jedenfalls verstärken.

Sanktionen⁹⁸⁹ könnten darüber hinaus strafrechtlicher Art sein. Dass reine Aufklärung ohne Androhung einer Sanktion jedenfalls weniger wirkungsvoll ist, zeigt die Betrachtung Schwedens. Die zunächst wahrnehmbare Steigerung der Verkaufszahlen im Bereich Musik stagnierte dort sechs Monate, nachdem das Gesetz zur verbesserten Rechtsverfolgung von Urheberrechtsverletzungen im Internet verabschiedet worden war. Dies wird darauf zurückgeführt, dass die befürchtete Rechtsverfolgung der Nutzer ausblieb.⁹⁹⁰

bb. Veränderung des Konsumverhaltens: Gibt es Indikatoren dafür, dass die Nutzer zur Legalisierung ihres Verhaltens angehalten werden?

Im Hinblick auf die Entwicklung legaler Angebote wurde im Vergleich der ersten zur zweiten Studie der Hadopi ein Anstieg der Nutzung legaler Nutzungsmöglichkeiten von kulturellen Werken verzeichnet. Während es in der ersten Studie noch 35 Prozent der Befragten waren, die angaben, regelmäßig legale Angebote zu nutzen, waren es in der zweiten Studie 50 Prozent. Demgegenüber fiel der Anteil derjenigen, die angaben, **eher nicht bzw. keine legalen Angebote regelmäßig zu nutzen**, von 45 auf **37 Prozent**.⁹⁹¹ Es zeigt sich insofern eine deutlichere Zweiteilung zwischen denjenigen Nutzern, die legal konsumieren, und solchen, die gar keine Angebote bzw. keine legalen Angebote im Internet für sich in Anspruch nehmen.

Betreffend die Akzeptanz und Förderung legaler Angebote im Netz wurde im Rahmen der zweiten Studie der Hadopi die Frage gestellt, ob die Hadopi für den einzelnen Nutzer Anregungen dazu geschaffen hat, legale Angebote zu nutzen. Die Frage wurde von insgesamt der Hälfte der Befragten bejaht, von 37 Prozent verneint.⁹⁹²

In Schweden, wo infolge der gesetzlichen Implementierung eines Auskunftsanspruchs in einer ersten Welle eine Steigerung der Verkaufszahlen im Bereich Musik verzeichnet wurde,⁹⁹³ konnte festgestellt werden, dass die Migration zum legalen Angebot im Bereich digitaler Musik nachhaltig blieb. Dies wurde dahin interpretiert, dass Internetnutzer, die zu-

⁹⁸⁹ Zur Bedeutung der Rechtsdurchsetzung siehe unten S. 226.

⁹⁹⁰ IFPI, DMR 2011, S. 11.

⁹⁹¹ Hadopi, 2ème vague barométrique, a.a.O., Folie 21.

⁹⁹² Hadopi, 2ème vague barométrique, a.a.O., Folie 22.

⁹⁹³ IFPI, DMR 2011, S. 11.

nächst aus Furcht vor einer Sanktion zu einem legalen Angebot wechselten, dies offenbar dauerhaft weiter nutzten.⁹⁹⁴

d. Zwischenfazit

Exakte Voraussagen dazu, wie die Reaktionen auf die Anwendung eines Warnhinweisverfahrens sein werden, lassen sich nicht machen. Auch die Erfahrungen, die man aus dem französischen und irischen Modell gewinnen konnte, sind noch nicht abschließend bzw. nicht hinreichend aussagekräftig. Es gibt Anzeichen dafür, dass die Gründe für eine Verhaltensänderung der Nutzer von vielen Faktoren abhängen. Dies können, neben kulturellen Besonderheiten, Faktoren, wie etwa die Zugänglichkeit und Erschwinglichkeit legaler Angebote, die Kennzeichnung, die Aufklärung der Verbraucher, die Sanktionierung und die Rechtsverfolgung von Verstößen sein. Der tatsächlich zu erzielende Effekt wird daher immer auch von den konkreten Umständen des nationalen Regelungssystems und der Akzeptanz der Nutzer abhängen. Jedenfalls aber führen die Betrachtungen der verschiedenen Länder nicht zu dem Ergebnis, dass eine solche Annahme unrichtig sei.⁹⁹⁵

3. Informationelle Perspektive

Ein grundlegender Faktor für die Verhinderung illegaler Nutzung urheberrechtlich geschützter Werke im Internet ist das Wissen des Nutzers um die rechtlichen Rahmenbedingungen einerseits und die darauf aufsetzende richtige Einschätzung der Rechtmäßigkeit des eigenen Handelns andererseits. Aufklärung und Hilfestellung bei der Beurteilung konkreter Angebote kommt daher eigenständige Bedeutung zu.

a. Unterscheidung rechtmäßig - unrechtmäßig

Dies erscheint umso bedeutender, als Zahlen darauf hinweisen, dass Internetnutzern legale Angebote im Internet nicht hinreichend bekannt sind. Nach einer Studie, die im September 2009 in Frankreich durchgeführt wurde, haben 82 Prozent der Internetnutzer zwar bereits einmal Musik über das Internet gehört,⁹⁹⁶ lediglich 66 Prozent der Internetnutzer kennen jedoch überhaupt nur legale Musikangebote.⁹⁹⁷

Eine große Unsicherheit spiegelt sich zudem darin wieder, dass eine nicht unerhebliche Zahl der Internetnutzer keine Vorstellungen davon hat, wie illegale von legalen Angeboten zu unterscheiden sind. Nach der zweiten Studie der Hadopi konnten 22 Prozent der Internetnutzer keine Indikatoren dafür benennen, die ein legales Angebot einer Webseite

⁹⁹⁴ Adermion/Liang, S. 18.

⁹⁹⁵ Vgl. *High Administrative Court*, [2011] EWHC 1021 (Admin), par.256.

⁹⁹⁶ *Pratiques et attentes des internautes*, la consommation de contenus culturels sur Internet, Folie 6.

⁹⁹⁷ *Pratiques et attentes des internautes*, la consommation de contenus culturels sur Internet, Folie 9.

kennzeichnen.⁹⁹⁸ Dabei ist eine deutliche Tendenz für eine steigende Unsicherheit der Nutzer zu verzeichnen, denn im Vergleich zur ersten Studie der Hadopi ist diese Zahl um rund sechs Prozentpunkte angestiegen.⁹⁹⁹ Zugleich ist interessant, dass hier erhebliche Unterschiede bestehen zwischen den Internetnutzern, die grundsätzlich legal auf Inhalte zugreifen, und denjenigen, die Inhalte (auch) illegal nutzen. Von denjenigen, die eine illegale Nutzung von Inhalten zugaben, fühlten sich lediglich neun Prozent nicht in der Lage, Kriterien zu benennen, während es bei denjenigen, die angaben, nur legal auf Angebote zuzugreifen, fast ein Drittel (28 Prozent) waren.¹⁰⁰⁰ Vor diesem Hintergrund könnte möglicherweise auch die eigene Einschätzung dazu, ob legale oder illegale Angebote genutzt werden, zu relativieren sein.

Zu berücksichtigen ist, dass im Kontext anderer Studien der Preis als besonderer Faktor für die Akzeptanz von Internetangeboten ermittelt wurde. Eine Vereinfachung der Erkennbarkeit legaler Angebote sahen nur drei Prozent der Internetnutzer als ausschlaggebend an für eine stärkere Wahrnehmung von Internetangeboten.¹⁰⁰¹

Eine wesentliche Rolle bei der Bewertung der Rechtmäßigkeit eines Angebots spielt offenbar die Marke des Anbieters. Insgesamt 44 Prozent der von der Hadopi befragten Internetnutzer sahen hierin einen wesentlichen Anhaltspunkt für die Rechtmäßigkeit eines Webseitenangebots. An zweiter Stelle (42 Prozent) rangierte die Tatsache, dass der Anbieter einer Webseite konkrete Nutzungskonditionen vorgibt. Erst danach (37 Prozent) folgte die Labelisierung durch die Hadopi als Indikator.¹⁰⁰²

Die Tatsache, dass ein Angebot kostenpflichtig ist, rangiert in der Bedeutung aller Indikatoren zwar nur auf Platz fünf (31 Prozent).¹⁰⁰³ Nach den von der Hadopi durchgeführten Befragungen wird jedoch von der Mehrheit der französischen Internetnutzer (54 Prozent) die Entgeltlichkeit eines Angebots mit der Rechtmäßigkeit dieses Angebots verknüpft. Während 31 Prozent der Befragten keine Bewertung über Rechtmäßig- bzw. Unrechtmäßigkeit eines Angebots mit diesem Kriterium verbanden, sahen 15 Prozent der Befragten in der Entgeltlichkeit nicht unbedingt einen Indikator für die Zulässigkeit eines Angebots.¹⁰⁰⁴ Diese Werte haben sich im Vergleich zu der vorangegangenen Befragung nicht wesentlich verändert.¹⁰⁰⁵

Zur Frage, welche Inhalte legal oder illegal angeboten werden, kommt die Bewertung des eigenen Handelns hinzu. Studien und Umfrageergebnissen im Vereinigtem Königreich

⁹⁹⁸ Hadopi, 2ème vague barométrique, Folie 33 ff.

⁹⁹⁹ Hadopi, 2ème vague barométrique, Folie 33, 34.

¹⁰⁰⁰ Hadopi, 2ème vague barométrique, Folie 34.

¹⁰⁰¹ *Pratiques et attentes des internautes*, la consommation de contenus culturels sur Internet, Folie 17.

¹⁰⁰² Hadopi, 2ème vague barométrique, Folie 34 ff.

¹⁰⁰³ Hadopi, 2ème vague barométrique, Folie 33 ff.

¹⁰⁰⁴ Hadopi, 2ème vague barométrique, Folie 30 bis 32.

¹⁰⁰⁵ Dort sahen 30 Prozent der Befragten in der Entgeltlichkeit nicht zwangsläufig, 53 Prozent der Befragten definitiv einen Indikator für die Rechtmäßigkeit eines Angebots, 17 Prozent hatten hierzu keine Meinung. Hadopi, 2ème vague barométrique, Folie 30.

zufolge wissen etwa 73 Prozent der dortigen Verbraucher nicht, was sie kopieren oder aufnehmen dürfen,¹⁰⁰⁶ 44 Prozent aller Verbraucher halten dort Filesharing im Peer-to-Peer-Netzwerk für legal.¹⁰⁰⁷

Auch in Deutschland wissen viele Nutzer nicht, welche Nutzungen legal bzw. illegal sind. Studienergebnissen zufolge zeichnet sich hier die Situation aber nicht in gleichem Maße ab, wie im Vereinigten Königreich. Das Bewusstsein, dass Urheberrechtsverstöße im Internet ernsthafte rechtliche Konsequenzen haben können, ist bei den Internetnutzern danach durchaus vorhanden. 80 Prozent der Deutschen wissen, dass das Herunterladen oder Anbieten von urheberrechtlichen geschützten Medieninhalten im Internet rechtliche Schritte nach sich ziehen kann.¹⁰⁰⁸ 87 Prozent davon, haben dies aus Beiträgen in den Medien erfahren.¹⁰⁰⁹ Zwölf Prozent der Bevölkerung kennen jemanden, der bereits wegen einer Urheberrechtsverletzung rechtlich belangt wurde.¹⁰¹⁰ Erhöht ist dieser Anteil bei den aktiven Downloadern. Hier wissen 96 Prozent, dass das Herunterladen oder Anbieten von urheberrechtlich geschützten Medieninhalten im Internet rechtliche Folgen haben kann.¹⁰¹¹

Eine überwiegende Anzahl von Nutzern weiß auch, welche Handlungen legal bzw. illegal sind. 15 Prozent der Deutschen sind hingegen etwa der Ansicht, dass der Download aus Peer-to-Peer-Netzwerken legal sei.¹⁰¹² Unter denjenigen, die das Internet zum Download benutzen, sind es 17 Prozent.¹⁰¹³ Acht Prozent dieser Nutzer halten das Hochladen von urheberrechtlich geschützten Materialien, an denen sie keine Rechte haben, auf Server von Sharehostern wie bspw. Rapidshare für rechtmäßig.¹⁰¹⁴

b. Aufklärungsarbeit allgemein

Die mit den Hadopi-Gesetzen durchgeführten Urheberrechtsnovellen waren in Frankreich nicht zuletzt auch angesichts der damit verbundenen Diskussion um das Sanktionsmittel der Internetsperre in der französischen Öffentlichkeit breit diskutiert worden. Dennoch ist die Arbeit der Hadopi als zentrale Stelle des neuen Schutzsystems innerhalb der französischen Bevölkerung noch nicht umfänglich bekannt. In der von SACEM beauftragten Studie hatten nur 54 Prozent der Befragten von der Hadopi überhaupt einmal gehört. Lediglich 40 Prozent kannten ihren Aufgabenbereich.¹⁰¹⁵

¹⁰⁰⁶ *Consumer Focus*, Outdated copyright law confuses consumers, 24.02.2010, Link: <http://www.consumerfocus.org.uk/news/outdated-copyright-law-confuses-consumers>, zuletzt aufgerufen am 19.08.2011.

¹⁰⁰⁷ *Harris Interactive/BPI*, Digital Music Survey, 2010.

¹⁰⁰⁸ Vgl. *DCN-Studie*, S. 38.

¹⁰⁰⁹ Vgl. *DCN-Studie*, S. 38.

¹⁰¹⁰ Bei den illegalen Nutzern sind es 30 Prozent. Vgl. *DCN-Studie*, S. 50, 51.

¹⁰¹¹ Vgl. *DCN-Studie*, S. 39.

¹⁰¹² Vgl. *DCN-Studie*, S. 40.

¹⁰¹³ Vgl. *DCN-Studie*, S. 43.

¹⁰¹⁴ Vgl. *DCN-Studie*, S. 44.

¹⁰¹⁵ *SACEM*, Les Français et la musique, Studie durchgeführt durch das Institut Opinionway, Januar 2011, Folie 16.

In die gleiche Richtung weisen die Ergebnisse der Hadopi. Zum Warnhinweisverfahren befragt gaben lediglich 22 Prozent der Internetnutzer an, das von der Hadopi durchgeführte Verfahren inhaltlich zu kennen.¹⁰¹⁶ Unter denen, die zugleich angaben, das Internet für illegale Nutzung von Werken zu verwenden, waren es hingegen 30 Prozent.¹⁰¹⁷ Hier scheint daher die Aufmerksamkeit für die (letztlich auch rechtlichen) Rahmenbedingungen und vor allem Konsequenzen stärker gegeben zu sein als bei denen, die von vorneherein das Internet nur zur legalen Werknutzung verwenden.

Auch für Irland liegen ausgewertete Ergebnisse vor, die aber nicht veröffentlicht werden dürfen.¹⁰¹⁸

Insofern zeigt sich, dass durchaus erhebliche Anstrengungen erforderlich sind, echte Aufmerksamkeit für derartige Problematiken und Lösungsansätze in der breiten Öffentlichkeit zu erzielen.

Interessanterweise spielt die Labelisierung von Webseiten in der Wahrnehmung der Internetnutzer als Indikator für die Rechtmäßigkeit eines Webseitenangebots, wie aufgezeigt, eine durchaus bedeutende, jedoch keine überragende Rolle. Sie rangiert an dritter Stelle hinter der Marke bzw. dem Namen des Anbieters als Referenz und der Tatsache, dass vom Anbieter Nutzungskonditionen vorgegeben werden. Im Vergleich zur ersten Studie der Hadopi ist das Vertrauen in eine Kennzeichnung noch gesunken; ihre Wahrnehmung als Bewertungsfaktor fiel um fünf Prozentpunkte ab, während sich der Anteil derjenigen, die keine Zuordnung vornehmen konnten, noch um sieben Prozentpunkte stieg. Dies verdeutlicht weiterhin eine nicht unwesentliche Verunsicherung der Nutzer und den Bedarf an Aufklärung.

c. Zwischenfazit

Inwieweit Aufklärung zu einer Veränderung des Nutzerverhaltens beiträgt, ist nicht abschließend geklärt. Positive Effekte sind aber wahrscheinlich. Unabhängig von jeder gezielten Einwirkung auf die Nutzer und deren Verhaltensschemen kann Aufklärung dazu beitragen, die offenbar nicht immer gänzlich umrissenen rechtlichen Rahmenbedingungen, wie auch die aus dem Handeln resultierenden Folgen, klarzustellen.

Die Daten zeigen, dass ein Bedürfnis einerseits besteht, dem Nutzer die Unterscheidung von legalen und illegalen Angeboten zu vereinfachen. Hierzu beitragen können Kennzeichnungen legaler Angebote, die jedoch wie die tragkräftige Marke eines Unternehmens bekannt gemacht und umworben werden müssten, um entsprechende Reichweite in der Wahrnehmung zu erzielen. Andererseits werden auch die Handlungsmöglichkeiten, die

¹⁰¹⁶Hadopi, 2ème vague barométrique, Folie 24, Ausschlüsselung nach Alter und Geschlecht Folie 25.

¹⁰¹⁷Hadopi, 2ème vague barométrique, Folie 24.

¹⁰¹⁸ Siehe oben S. 209.

sich dem aktiven Internetnutzer stellen, nicht immer der rechtlich richtigen Bewertung zugeordnet, so dass auch hier Bedarf für Aufklärung besteht.

Kenntnis über die Rechtslage, mögliche zu erwartende Folgen bzw. Sanktionen sowie Auswirkungen des eigenen Handelns auf Dritte und die Allgemeinheit, setzen dabei im Rahmen der Aufklärung unterschiedliche Impulse: sie fördern Rechtskenntnis, Unrechtsbewusstsein und Gerechtigkeitsempfinden.

Insofern sind positive Auswirkungen im Sinne einer Verhaltensänderung nicht auszuschließen. Jedenfalls aber können durch Aufklärung Fälle vermieden werden, die nach derzeitiger Rechtslage ungewollt Unrecht erzeugen und daher als ungerecht empfunden werden. So kann verhindert werden, dass ein Rechteverletzer der Rechtsverfolgung ausgesetzt wird, der in Unkenntnis unrechtmäßig handelt, ggf. Peer-to-Peer-Filesharing zum ersten Mal verwendet. Dies gilt in gleichem Maße für den in Anspruch genommenen Anschlussinhaber, dem die über seinen Anschluss begangenen Handlungen nicht bekannt sind.

4. Effizienz und wirtschaftliche Perspektive

Um eine Aussage zur Effizienz einer Warnhinweisregelung im Sinne einer Kosten-Nutzen-Analyse treffen zu können, ist abschließend ist zu untersuchen, welcher Aufwand in volkswirtschaftlicher Hinsicht mit der Einführung und Durchführung eines Warnhinweisverfahrens verbunden ist und in welchem Verhältnis dieser zu den dargelegten eingetretenen bzw. zu erwartenden Effekten steht¹⁰¹⁹.

Schwierigkeiten ergeben sich hierbei aus der Tatsache, dass nur begrenzt Modelle bereits umgesetzt sind, dass sich die Modelle in ihrer Umsetzung nicht unerheblich unterscheiden und schließlich effektive Zahlen nur unzureichend bekannt sind.

Aussagekräftiges Zahlenmaterial existiert allerdings zu den Kosten und Nutzen des vorgesehenen Warnhinweismodells im Vereinigten Königreich.¹⁰²⁰ Danach entstehen für die Diensteanbieter über einen Zeitraum von 10 Jahren Gesamtkosten in Höhe von £290 - 500 Mio. Für die Rechteinhaber wird der Gesamtnutzen über einen Zeitraum von 10 Jahren auf einen Betrag in Höhe von £1.7 Mrd. beziffert. Angaben sind etwa auch für die Hadopi in Frankreich vorhanden. Der Behörde stand für das Jahr 2011 ein Budget in Höhe von 13,79 Millionen Euro zur Verfügung (im Jahr 2010 waren es 10,85 Millionen Euro),¹⁰²¹ um ihre Aufgaben zu erfüllen. Hierzu gehört als wesentlicher Bereich das Warnhinweisverfahren. Zuverlässige Daten dazu, welcher zahlenmäßige Aufwand aufseiten der

¹⁰¹⁹ Zur juristischen Relevanz der ökonomischen Auswirkungen für das Erfordernis zur Einführung eines Warnhinweismodells, siehe unten S. 311.

¹⁰²⁰ Siehe im Einzelnen oben S. 137.

¹⁰²¹ Vgl. *Rapport d'activité 2010*, a.a.O., S. 78. Hiervon entfallen 4,43 Millionen auf Personalkosten, 6,6 Millionen auf Betriebskosten und 2,757 Millionen auf Investitionskosten.

Internetdiensteanbieter und der Rechteinhaber im Rahmen des Verfahrens in Frankreich entsteht, liegen nicht vor.

Für Irland ist nach der Datenlage¹⁰²² unklar, ob und inwieweit das „*Graduated Response*“-Verfahren tatsächlich dem Provider und den Musikproduktionsgesellschaften einerseits wirtschaftliche bzw. finanzielle Kosten verursacht und andererseits wirtschaftlich bzw. finanziell nützt. Mit der Einführung und Durchführung der Warnhinweisregelung sowie einem dadurch bedingten Rückgang von Urheberrechtsverletzungen sind zwar ohne Zweifel ökonomische Folgen verbunden wie Aufwendungen für die technische Einführung und Vorhaltung der Systeme und vom Provider gegebenenfalls hinzunehmende Kundenabwanderungen oder vergleichsweise geringeren Neuzugewinn von Neukunden. Auf der anderen Seite stehen unter Umständen ein mit dem durch das „*Graduated Response*“-Verfahren aufgenommenen Kampf gegen Urheberrechtsverletzungen im Internet einhergehender Imagegewinn für den Provider in der Öffentlichkeit und eine Zunahme beim Verkauf lizenzierter Produkte. Wirtschaftlicher Aufwand und Nutzen sind aber ohne entsprechende konkrete Zahlenangaben nicht seriös bezifferbar und damit bewertbar.

Die volkswirtschaftlichen Auswirkungen von Urheberrechtsverletzungen im Internet sind stark umstritten. Im Vereinigten Königreich etwa nimmt der *High Court an*, dass es für die Frage der Verhältnismäßigkeit der Warnhinweisregelung nicht ausschlaggebend auf konkrete Zahlen zur Problematik ankommt, sondern darauf, dass die Zahlen Indizien darstellen, dass P2P-Filesharing in erheblicher Weise Einfluss nimmt auf die Anzahl rechtmäßiger Verkäufe, die anderenfalls erfolgt wären.¹⁰²³ Verlorene Einnahmen wiederum führten dazu, dass weniger in Künstler und Produktionen von Inhalten investiert werde.¹⁰²⁴ Freilich besteht keine Einigkeit darüber, in welcher Art und in welchem Umfang Filesharing auf die Kreativwirtschaft einwirkt und ob gesunkene Verkaufszahlen in den letzten Jahren nicht (auch) andere Ursachen gehabt haben könnten. Die meisten Studien gelangen aber zu dem Ergebnis, dass illegales Filesharing eine Rolle bei der Abnahme von Verkaufszahlen spielt. Schätzungen für eine Substitutionsrate – d. h. eine Rate zur Berechnung verlorener Einnahmen der Industrie, weil das Produkt im P2P-Netzwerk umsonst zugänglich war – bewegen sich bei Angaben zwischen Null bis 20 Prozent.¹⁰²⁵

¹⁰²² Siehe oben S. 218.

¹⁰²³ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 252ff.

¹⁰²⁴ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 252.

¹⁰²⁵ Siehe *High Administrative Court*, [2011] EWHC 1021 (Admin), par.252 mit einer Übersicht zu den relevanten Studien.

E. Rechtsdurchsetzung

I. Grundzüge nationaler urheberrechtlicher Vorgaben im einfachen Recht

Die einfachgesetzlichen Vorgaben des deutschen Urheberrechts sind im Urheberrechtsgesetz v. 9.9.1965¹⁰²⁶ enthalten. Im Zentrum stehen der Urheber und dessen Urheberpersönlichkeitsrecht. Geschützt werden, soweit im Rahmen der Untersuchung vordringlich relevant, Sprachwerke einschließlich Computerprogramme (zum Begriff s. § 69a UrhG), Werke der Musik, Lichtbildwerke, Filmwerke und Darstellungen wissenschaftlicher oder technischer Art (§ 2 Abs. 1 Nrn. 1 ff. UrhG). Der **Werkbegriff** setzt eine persönliche geistige Schöpfung voraus. Neben Schöpfungen mit Werkqualität schützt das deutsche Urheberrecht auch verwandte Schutzrechte für Gestaltungen wie z.B. Lichtbilder (§ 72 UrhG) und Laufbilder (§ 95 UrhG) sowie die Rechte der Hersteller von Datenbanken (§§ 87a ff UrhG) und der Hersteller von Tonträgern und schließlich die Rechte der Sendeunternehmen (§§ 85 ff UrhG). Im Internet liegen diese Werke und anderen Gestaltungen naturgemäß in Dateiform vor bzw. werden in Dateiform gespeichert oder übertragen.

Um der Rechtsposition des Urhebers Rechnung zu tragen, werden ihm im Rahmen seines Urheberrechts ein **Urheberpersönlichkeitsrecht** (Veröffentlichungsrecht, § 12 UrhG, Recht auf Anerkennung der Urheberschaft, § 13 UrhG und Recht auf Verhinderung der Entstellung des Werkes, § 14 UrhG) und die Verwertungsrechte der §§ 15 ff. UrhG (Vervielfältigungs-, Verbreitungs- und Ausstellungsrecht sowie das Recht der öffentlichen Wiedergabe, darunter v.a. das Recht der öffentlichen Zugänglichmachung, § 19a UrhG, z.B. durch Einstellen in das Internet) zugestanden. Das Urheberrecht ist grundsätzlich **nicht übertragbar**, es sei denn in Erfüllung einer Verfügung von Todes wegen oder im Wege der Erbauseinandersetzung (§§ 28, 29 UrhG). Wirksam sind jedoch Vereinbarungen, mit denen der Urheber einem anderen Nutzungsrechte einräumt (§§ 29 Abs. 2, 31 UrhG). Die Wirkungskdauer des Urheberrechts beträgt **70 Jahre** post mortem auctoris (§ 64 UrhG). Es ist ein Ausschließungsrecht, d.h. der Urheber bzw. der Berechtigte kann im Grundsatz auf der Grundlage seines Urheberrechts bzw. der ihm vertraglich eingeräumten Rechte, Handlungen in Bezug auf das Werk bzw. das geschützte Gut verbieten, die nicht mit seinem Einverständnis geschehen.

Jedoch unterliegt das Ausschließungsrecht nicht unerheblichen gesetzlichen **Schranken** mit der Folge, dass bei Eingreifen einer solchen Schranke das Ausschließungsrecht nicht geltend gemacht werden kann. Solche Schranken sind in §§ 44a ff. UrhG geregelt, wie etwa notwendige vorübergehende Vervielfältigungen in technischen Verfahren (§ 44a UrhG), Zitate (§ 51 UrhG), die öffentliche Wiedergabe von Werken ohne Erwerbzweck der Beteiligten (§ 52 UrhG), die öffentliche Zugänglichmachung für Zwecke von Unterricht und

¹⁰²⁶ BGBl. I, S. 1273, zul. geändert durch Gesetz vom 17.12.2008 (BGBl. I S. 2586) m.W.v. 01.09.2009.

Forschung (§ 52a UrhG) oder Lichtbildaufnahmen von Werken an öffentlichen Plätzen (§ 59 UrhG). Die bedeutendste Schranke im Zusammenhang mit Urheberrechtsverletzungen im Internet ist jedoch die Privatkopieschranke nach § 53 UrhG.¹⁰²⁷

Greift ein Nichtberechtigter in das Urheberrecht bzw. andere urheberrechtlich geschützte Rechte ein, stehen dem Rechteinhaber die in §§ 97 ff. UrhG vorgesehenen Ansprüche nach dortiger näherer Maßgabe zu. Wichtigster Anspruch zur Unterbindung von Rechtsverletzungen ist der **Unterlassungsanspruch** nach § 97 Abs. 1 UrhG. Darüber hinaus besteht bei schuldhaftem Handeln ein Anspruch auf **Schadensersatz** (§ 97 Abs. 2 UrhG). Daneben bestehen Ansprüche auf Vernichtung, Rückruf bzw. Überlassung urheberrechtsverletzender Vervielfältigungstücke (§ 98 UrhG). Sofern die Verletzung in gewerblichem Ausmaß erfolgt, gibt § 101 UrhG dem Berechtigten Ansprüche gegen den Verletzer bzw. gegen bestimmte Dritte (§ 101 Abs. 2, 9 UrhG) über Herkunft und Vertriebsweg der rechtsverletzenden Vervielfältigungsstücke bzw. sonstigen Erzeugnisse. Die Vorschriften der §§ 106 ff. UrhG stellen Urheberrechtsverletzungen unter ein gesetzliches Strafmaß von bis zu drei, bei gewerbsmäßigem Handeln (108a UrhG) bis zu fünf Jahren Freiheitsstrafe oder Geldstrafe. Es handelt sich, mit Ausnahme des gewerbsmäßigen Handelns, zwar grundsätzlich um Antragsdelikte, die Staatsanwaltschaft kann jedoch auch ein besonderes öffentliches Interesse bejahen (§ 109 UrhG). Als Besonderheit im Urheberrecht kann das Gericht auf Antrag des Rechteinhabers anordnen, dass die Verurteilung öffentlich bekannt gemacht wird (§ 111 UrhG).

II. Einzelheiten zu den Voraussetzungen zivilrechtlicher Durchsetzung von Urheberrechten

Zivilrechtliche Ansprüche setzen eine Verletzung der geschützten dinglichen Rechte voraus, d.h. der Urheberrechte, Verwertungsrechte, ausschließlichen Nutzungsrechte sowie Urheberpersönlichkeitsrechte.¹⁰²⁸

1. Rechtswidrigkeit der Verletzung

Die Verletzung muss **rechtswidrig** sein, was der Fall ist, wenn kein Rechtfertigungsgrund vorliegt. Als Rechtfertigungsgründe kommen – in den hier interessierenden Fällen – allenfalls die Zustimmung des Rechteinhabers bzw. die Erschöpfung oder eine gesetzliche Erlaubnis für die betreffende Verwendung in Betracht.¹⁰²⁹

Die Zustimmung des Rechteinhabers wird von den Verletzern oft nicht als ausdrücklich gegeben behauptet, sondern als sich aus dem tatsächlichen Verhalten – in Form einer konkludenten Einwilligung – ergebend.¹⁰³⁰ Wer Inhalte ohne Zugangsbeschränkung im

¹⁰²⁷ Dazu S. 227.

¹⁰²⁸ Dazu ausführlich Dreier in Dreier/Schulze § 97 Rn. 3 ff.; Nordemann in Fromm/Nordemann § 97 Rn. 8 ff.

¹⁰²⁹ Dreier in Dreier/Schulze § 97 Rn. 15; Nordemann in Fromm/Nordemann § 97 Rn. 22 ff.

¹⁰³⁰ Vgl. Möllmann/Bießmann in Schwartmann, S. 1273; Weidert/Molle in Ensthaler/Weidert, S. 449 ff.

Internet zugänglich macht, erteilt damit seine Einwilligung jedenfalls zum Abruf dieses Angebots durch den Internetnutzer und zu den damit notwendigerweise verbundenen Verwertungshandlungen¹⁰³¹, jedoch nicht zwingend auch für weitere Nutzungs- oder Verwertungshandlungen. Hat der Rechteinhaber auf seiner Webseite beispielsweise mitgeteilt, „auf einen wirksamen Kopierschutz bewusst verzichtet zu haben“, lässt er erkennen, dass er das Vervielfältigungsproblem erkannt hat. Nach Ansicht der Literatur ist in einem solchen Fall nicht von einer Einwilligung des Berechtigten in eine Vervielfältigung jenseits des Abrufs auszugehen.¹⁰³²

An einer rechtswidrigen Verletzung fehlt es auch, wenn gesetzlich die Nutzung bzw. bestimmte Verwendungen erlaubt sind, d.h. die Schrankenregelungen nach §§ 44a – 63a UrhG greifen. Eine vorliegend wichtige Bestimmung ist die Privilegierung sog. Privatkopien (§ 53 Abs. 1 UrhG); danach ist es unter bestimmten Voraussetzungen zulässig, einzelne Vervielfältigungen eines Werkes zum privaten Gebrauch herzustellen oder herstellen zu lassen. Privater Gebrauch erfolgt in der Privatsphäre zur Befriedigung rein persönlicher Bedürfnisse.¹⁰³³ Die Privilegierung gilt auch für digitale Vervielfältigungen.¹⁰³⁴ Das UrhG enthält in der am 1.1.2008 in Kraft getretenen Fassung, gegenüber dem älteren Recht, Beschränkungen der Privilegierung von Privatkopien. Nun ist eine Vervielfältigung auch dann verboten, wenn eine „offensichtlich rechtswidrig ... öffentlich zugänglich gemachte Vorlage“ verwendet wird. Diese Verschärfung zielt auf die Nutzung von Internettauschbörsen ab, weil nunmehr offensichtlich rechtswidrig in das Internet eingestellte Werke selbst zu privaten Zwecken nicht heruntergeladen werden dürfen. Dadurch hat sich auch die Situation für Personen, die nur Downloads vornehmen, verschärft. Unzulässig ist mithin nicht nur der Upload, sondern auch der Download von urheberrechtlich geschützten Werken in Internettauschbörsen.¹⁰³⁵

Darüber, wann eine Vorlage offensichtlich rechtswidrig hergestellt bzw. öffentlich zugänglich gemacht wurde, bestehen in Einzelheiten unterschiedliche Ansichten.¹⁰³⁶ Ist für den unbefangenen Nutzer einer Internettauschbörse klar erkennbar,¹⁰³⁷ dass die Herstellung oder das öffentliche Zugänglichmachen der zum Download angebotenen (Kino-) Filme oder Musiktitel offensichtlich rechtswidrig ist, ist eine Privatkopie durch Download nicht gestattet. Beim Anbieten aktueller, d.h. gerade erst auf den Markt gelangter Kinofilme oder Musiktitel im Rahmen von unentgeltlichen Filesharing-Netzwerken dürfte es sich i.d.R. um

¹⁰³¹ So kann die Stellung von urheberrechtlich geschützten Abbildungen durch den Berechtigten auf der eigenen Website, in einer Form, durch die eine Indexierung durch Suchmaschinenbetreiber nicht verhindert wird, als eine konkludente Einwilligung in die Herstellung und Zugänglichmachung von so genannten Thumbnails in der Trefferliste einer Suchmaschine gesehen werden; *BGH MMR* 2010, 475 – *Vorschaubilder*.

¹⁰³² So *Musiol GRUR-RR* 2009, S. 3; *Otten GRUR-RR* 2009, S. 372; *Wilhelmi ZUM* 2008, S. 948. Anders aber *OLG Zweibrücken MMR* 2009, 45.

¹⁰³³ *BGH GRUR* 1978, 475 – *Vervielfältigungsstücke*; *Nordemann in Fromm/Nordemann* § 53 Rn. 6 ff.

¹⁰³⁴ *Dreier in Dreier/Schulze* § 53 Rn. 8.

¹⁰³⁵ *Dreier in Dreier/Schulze* § 53 Rn. 11; *Röhl/Bosch NJW* 2008, S. 1417.

¹⁰³⁶ Dazu *Dreier in Dreier/Schulze* § 53 Rn. 12; *Weidert/Molle in Ensthaler/Weidert*, S. 446; *Schwartzmann K&R* 2011 Beiheft 2/2011, S. 9 ff.

¹⁰³⁷ So *Nordemann in Fromm/Nordemann* § 53 Rn. 14.

eine offensichtlich rechtswidrig zugänglich gemachte Vorlage handeln, denn in diesen Fällen muss jedenfalls derjenige Nutzer, der weiß, dass es sich um einen gerade erst veröffentlichten Film oder Musiktitel handelt, davon ausgehen, dass solche Inhalte, von dem einem im Grundsatz stets kommerzielle Interessen verfolgenden Rechteinhaber, nicht unentgeltlich zur Verfügung gestellt werden. Da jedoch einzelne Rechteinhaber, dazu übergehen, ihre Inhalte bewusst kostenlos zum Download bereit zu stellen, kann es im Einzelfall schwierig erkennbar sein, ob die Vorlage offensichtlich rechtswidrig öffentlich zugänglich gemacht wurde oder nicht.¹⁰³⁸

2. Verschulden

Im Gegensatz zu Unterlassungsansprüchen, deren Durchsetzung kein Verschulden auf Seite des Verletzers voraussetzt (§ 97 Abs. 1 Satz 1 UrhG), besteht ein Schadensersatzanspruch nur bei schuldhaftem, d.h. vorsätzlichem oder fahrlässigem Handeln (§ 97 Abs. 2 Satz 1 UrhG).

3. Anspruchsberechtigte

Aktivlegitimiert ist grundsätzlich der Urheber bzw. der Inhaber verwandter Schutzrechte. Sind einem Dritten ausschließliche Nutzungsrechte eingeräumt, ist dieser aktivlegitimiert, soweit die ihm zustehenden Rechte reichen.¹⁰³⁹ Der Urheber bleibt jedoch aktivlegitimiert für den Bereich außerhalb der räumlichen oder sachlichen Grenzen der Ausschließlichkeit. Der Urheber bzw. Inhaber eines verwandten Schutzrechts kann neben dem Nutzungsberechtigten ebenfalls aktivlegitimiert sein, soweit ihm noch ein schutzwürdiges Interesse zusteht.¹⁰⁴⁰ Sind einem Dritten nur einfache Nutzungsrechte eingeräumt, ist dieser nicht aktivlegitimiert, sondern weiterhin der Urheber bzw. Inhaber des verwandten Schutzrechts (oder eines ausschließlichen Nutzungsrechts)¹⁰⁴¹.

Bei der Verfolgung massenhafter Rechtsverletzungen im Internet, z.B. im Fall des Filesharings, machen die Rechteinhaber ihre Rechte häufig nicht selbst geltend. Vielmehr werden vielfach so genannte „Anti-Piracy-Unternehmen“ beauftragt, die Rechtsverletzungen zu ermitteln und zu dokumentieren oder sogar zivilrechtlich zu verfolgen. Aktivlegitimiert ist ein solches Unternehmen nur, wenn es auch Inhaber ausschließlicher Nutzungsrechte ist¹⁰⁴² und die ununterbrochene Rechtskette von Übertragungen für jedes zum Download angebotene Werk (Musiktitel oder Filme) darlegen kann.¹⁰⁴³

¹⁰³⁸ Röhl/Bosch NJOZ 2008, S. 1205.

¹⁰³⁹ So Dreier in Dreier/Schulze § 97 Rn. 19; Weidert/Molle in Ensthaler/Weidert, S. 360.

¹⁰⁴⁰ Vgl. Dreier in Dreier/Schulze § 97 Rn. 19; Möllmann/Bießmann in Schwartmann, S. 1274; von Wolff in Wandtke/Bullinger §97 Rn. 9.

¹⁰⁴¹ Dreier in Dreier/Schulze § 97 Rn. 20; von Wolff in Wandtke/Bullinger §97 Rn. 11., wobei des Öfteren vertragliche Verpflichtungen zur Rechtsverfolgung durch den Rechteinhaber vereinbart werden.

¹⁰⁴² Vgl. Möllmann/Bießmann in Schwartmann, S. 1300.

¹⁰⁴³ Dreier in Dreier/Schulze § 97 Rn. 19. Ein pauschales Bestreiten der Rechteinhaberschaft ist unbeachtlich, es sei denn, einzelfallbezogen konkrete Anhaltspunkte vorgetragen werden, die Zweifel an der Rechteinhaberschaft des Klägers wecken können, LG Köln ZUM-RD 2010, 279.

4. Anspruchsverpflichtete

a. Haftung als Täter/Teilnehmer, telemedienrechtliche Haftungsprivilegierung

Anspruchsgegner ist zunächst jeder Täter oder Teilnehmer, sofern zwischen seinem Verhalten und der Rechtsverletzung ein Kausalzusammenhang besteht. Täter einer Urheberrechtsverletzung ist die Person, die eine rechtswidrige Handlung selbst vorgenommen hat oder der diese zugerechnet werden kann, weil sie sie veranlasst oder sich zu eigen gemacht hat.¹⁰⁴⁴ Dies sind im Falle von Urheberrechtsverletzungen im Internet – je nach Fallgestaltung – die Personen, die urheberrechtsverletzendes Material hochgeladen (Upload) oder mangels Eingreifen von § 53 UrhG in nicht rechtskonformer Weise heruntergeladen (Download) haben.

Als Täter einer Urheberrechtsverletzung kommen auch Internetdiensteanbieter in Betracht, wenn sich die in Rede stehenden Werke, die sie z.B. zum Download bereit gestellt haben, im telemedienrechtlichen Sinne als deren eigene Inhalte i.S.d. § 7 Abs. 1 TMG erweisen, was jedoch nicht der Regelfall ist. Internetdiensteanbieter stehen vielmehr auf dem Standpunkt, dass sie für Urheberrechtsverletzungen bzgl. fremder Inhalte nicht verantwortlich sind, die unter Nutzung der von ihnen bereit gestellten technischen Infrastruktur begangen werden. Damit rücken §§ 8 bis 10 TMG in den Blickpunkt. Telemedienrechtlich werden Internetdiensteanbieter privilegiert, indem über den Haftungsfiter¹⁰⁴⁵ der §§ 8 bis 10 TMG deren Verantwortlichkeit für fremde Inhalte, zu denen sie den Zugang vermitteln oder die sie speichern, begrenzt wird. Greift eine **Haftungsprivilegierung** des TMG ein, kommt eine weitere Prüfung der allgemeinen zivilrechtlichen und strafrechtlichen Vorschriften nicht mehr in Betracht. Diensteanbieter (vgl. auch § 2 Satz 1 Nr. 1 TMG) in diesem Sinne sind, soweit hier mit Blick auf fremde Inhalte bzw. Informationen interessierend, Informationsanbieter (Content-Provider), Anbieter von Speicherdiensten (Host-Provider) und Zugangsanbieter (Access-Provider, bisweilen auch als Internetzugangsdiensteanbieter bezeichnet).¹⁰⁴⁶

Zugangsanbieter sind nach **§ 8 TMG** von der Haftung freigestellt, wenn sie die Übermittlung der fremden Informationen nicht veranlasst, die Adressaten der Informationen nicht ausgewählt und die übermittelten Informationen nicht ausgewählt oder verändert haben. § 9 TMG sieht im Grundsatz die gleiche Begrenzung für Anbieter vor, die eine automatische, zeitlich begrenzte Zwischenspeicherung fremder Informationen vornehmen (Caching), soweit diese nicht allein zur Durchführung der Übermittlung dienen. § 10 TMG sieht unter etwas anderen Voraussetzungen eine Haftungsfreistellung für Host-Provider vor, die z.B. Speicherplatz für eine Webseite, Diskussionsforen, Internet-Auktionshäuser oder Blog-Systeme bereithalten, selbst aber keine Inhalte hierzu liefern; der Anbieter ist

¹⁰⁴⁴ Vgl. Dreier in Dreier/Schulze § 97 Rn. 23; Spindler in Spindler/Schuster § 97 Rn. 16.

¹⁰⁴⁵ Vgl. Weidert/Molle in Ensthaler/Weidert, S. 369; Wilmer NJW 2008, S. 1846.

¹⁰⁴⁶ Dazu Leupold/Glossner in Leupold/Glossner Teil 2 Rn. 448 ff.

hier nur verantwortlich, wenn er Kenntnis von der rechtswidrigen fremden Information erlangt hat und nach Kenntniserlangung nicht unverzüglich tätig wurde, um die Information zu entfernen oder den Zugang zu ihr zu sperren.¹⁰⁴⁷

Die Haftungsprivilegierung der §§ 8 bis 10 TMG gilt nach Ansicht des Bundesgerichtshofes¹⁰⁴⁸ jedoch nur für die strafrechtliche Verantwortlichkeit und Schadensersatzansprüche, ist hingegen auf **Unterlassungsansprüche** gegen Diensteanbieter **nicht anzuwenden**. Wird demnach ein Anbieter auf Unterlassung in Anspruch genommen, weil eine (gespeicherte) fremde Information die Rechte eines Dritten verletzt, haftet er nach den allgemeinen Grundsätzen ohne die Möglichkeit der Privilegierung. Dies gilt auch für den vorbeugenden Unterlassungsanspruch.¹⁰⁴⁹

b. Mögliche Haftung als Störer

aa. Allgemeine Voraussetzungen der Störerhaftung

Anspruchsverpflichtet – jedenfalls im Rahmen eines Unterlassungsanspruchs¹⁰⁵⁰ – kann neben dem Täter oder Teilnehmer auch ein nur mittelbar Verantwortlicher sein, der sogenannte Störer. Bei Versuchen der Unterbindung von Urheberrechtsverletzungen spielt insbesondere die Störerhaftung eine besondere Rolle, da der Verletzer häufig schwer zu ermitteln ist.¹⁰⁵¹ Störer ist, wer, ohne Täter oder Teilnehmer zu sein, willentlich und adäquat kausal an der rechtswidrigen Urheberrechtsverletzung mitgewirkt hat.¹⁰⁵² Auf ein Verschulden kommt es nicht an, sondern nur auf die Eröffnung einer Gefahrenquelle¹⁰⁵³. Die Störerhaftung setzt zwar eine Rechtsverletzung durch einen Dritten voraus, nicht erforderlich ist jedoch, dass der Täter oder Teilnehmer nicht in Anspruch genommen werden kann. Die Störerhaftung tritt also neben die des Täters oder Teilnehmers.¹⁰⁵⁴ Sie greift im Bereich

¹⁰⁴⁷ Dazu ausführlich Schmittmann in Schwartmann, S. 303 ff.; Weidert/Molle in Ensthaler/Weidert, S. 381 ff.

¹⁰⁴⁸ Vgl. BGH GRUR 2004, 860 – *Internet-Versteigerung I*; BGH GRUR 2007, 708 ff. – *Internet-Versteigerung II*; BGH GRUR 2008, 702 ff. – *Internet-Versteigerung III*; BGH MMR 2010, 567 – *Sommer unseres Lebens*; s.a. BGH v. 17.8.2011 – I ZR 57/09 – *Stiftparfüm*.

¹⁰⁴⁹ BGH GRUR 2007, 708 ff. – *Internet-Versteigerung II*; zuletzt BGH v. 17.8.2011 – I ZR 57/09 – *Stiftparfüm*.

¹⁰⁵⁰ Vgl. BGH GRUR 2004, 860 – *Internet-Versteigerung I*; BGH GRUR 2007, 708 ff. – *Internet-Versteigerung II*; BGH GRUR 2008, 702 ff. – *Internet-Versteigerung III*; BGH MMR 2010, 567 – *Sommer unseres Lebens*; s.a. BGH v. 17.8.2011 – I ZR 57/09 – *Stiftparfüm*. Vgl. Schmittmann in Schwartmann, S. 305 ff.; Weidert/Molle in Ensthaler/Weidert, S. 414; Gabriel/Albrecht ZUM 2010, 396. A.A. Breyer MMR 2009, S. 15. In der Literatur wird auf die Möglichkeit hingewiesen, dass diese Rechtsprechung des BGH künftig aufgegeben wird. Vgl. Lutz VuR 2010, S. 342; Mantz, MMR 2010, 569.

¹⁰⁵¹ Siehe oben S. 34 und S.196.

¹⁰⁵² BGH GRUR 1999, 419 – *Möbelklassiker*; BGH GRUR 2004, 860 – *Internet-Versteigerung I*; die bisherige eigene Rechtsprechung bestätigt durch BGH GRUR 2007, 708 ff. – *Internet-Versteigerung II*; BGH GRUR 2008, 702 ff. – *Internet-Versteigerung III*. Vgl. auch Dreier in Dreier/Schulze § 97 Rn. 33; Spindler in Spindler/Schuster § 97 Rn. 18.

¹⁰⁵³ Die Mitwirkung kann in der Unterstützung oder Ausnutzung der Handlung eines eigenverantwortlichen Dritten liegen, sofern der in Anspruch Genommene die rechtliche Möglichkeit zur Verhinderung dieser Handlung hatte (BGH GRUR 1999, 419 – *Möbelklassiker*).

¹⁰⁵⁴ So Nordemann in Fromm/Nordemann § 97 Rn. 158; Weidert/Molle in Ensthaler/Weidert, S. 395. A.A. Volkmann CR 2008, S. 237, der die Meinung vertritt, dass Prüfpflichten für die Hostprovider erst vorliegen sollen, wenn der Täter selbst nicht in Anspruch genommen werden kann. Dem Host-Provider sollte die Möglichkeit gegeben werden, der eigenen Inanspruchnahme durch Auskunft über die Inhaltsherkunft zu entgehen. Anders BGH MMR 2007, 518 ff. – kein Ausfall der Verantwortlichkeit des Betreibers eines Internetforums für dort eingestellte Beiträge, weil dem Verletzten die Identität des Täters bekannt ist.

der verschuldensunabhängigen Unterlassungsansprüche und Beseitigungsansprüche, nicht jedoch der Schadensersatzansprüche.¹⁰⁵⁵

Als Störer für Urheberrechtsverletzungen im Internet kommen insbesondere alle diejenigen in Betracht, die technische Infrastruktur für die Begehung der Urheberrechtsverletzungen bereitstellen, z.B. Internetdiensteanbieter, aber auch Inhaber eines (nicht hinreichend gesicherten) WLAN-Anschlusses. Da die beschriebene Haftungsprivilegierung nach §§ 8 ff. TMG bei der Behandlung fremder Inhalte für den Unterlassungsanspruch nicht gilt, sind auch Internetdiensteanbieter solchen Unterlassungsansprüchen ausgesetzt.

bb. Bestehen einer Prüfungspflicht als Voraussetzung für die Störerhaftung

Zur Eingrenzung des Kreises der denkbaren Störer kommt für den Bundesgerichtshof eine Störerhaftung im Grundsatz nur bei der Verletzung im Einzelfall zumutbarer Prüfpflichten in Betracht.¹⁰⁵⁶ Die Prüfpflicht entsteht i.d.R. erst, wenn der Störer Kenntnis von der Rechtsverletzung erlangt hat. Keine Prüfpflichten bestehen jedoch, wenn und soweit diese dem als Störer in Anspruch Genommenen nach den konkreten Umständen nicht zumutbar sind. Die Zumutbarkeit ist bereits auf der Tatbestandsebene zu prüfen. Dies betrifft im Grundsatz in erster Linie Störer, die nur organisatorische und technische Mittel für die von einem anderen begangene urheberrechtliche Rechtsverletzung bereitstellen.

Art und Ausmaß der Prüfpflichten sowie die konkret aus der Prüfung abzuleitenden Folgen werden nachfolgend im Zusammenhang mit einzelnen potenziellen Arten von Störern diskutiert.

1) Prüfungspflichten von Host-Providern

Im Fall eines Host-Providers wird die vorgenannte Prüfpflicht bei Kenntnis von rechts- bzw. urheberrechtsverletzenden fremden Inhalten auf der von ihm bereit gestellten Plattform ausgelöst. Host-Provider erlangen i.d.R. Kenntnis durch ein von dem Rechteinhaber versandtes Schreiben, in dem dieser auf den rechtsverletzenden Umstand hinweist (und i.d.R. eine Entfernung der urheberrechtsverletzenden Information von der Plattform verlangt; sog. Notice-and-Takedown-Letter).

Ob und inwieweit eine Prüfpflicht dem Host-Provider zumutbar ist, kann nur im Einzelfall nach einer umfassenden Abwägung entschieden werden. Bei der Frage der Zumutbarkeit sind die verschiedenen Rechte und die Eigenverantwortung von Verletzer, Host-Provider und Rechteinhaber zu berücksichtigen.¹⁰⁵⁷ Kriterien bei der Beurteilung der Zumutbarkeit sind z.B. Intensität der Gefahr, wirtschaftliche Vorteile des Diensteanbieters aufgrund der rechtsverletzenden Angebote, Funktion und Aufgabenstellung des Diensteanbieters und

¹⁰⁵⁵ BGH GRUR 2004, 860 ff. – *Internetversteigerung I*; BGH GRUR 2002, 619 – *Meißner Dekor*. Vgl. Dreier in Dreier/Schulze § 97 Rn. 33; Nordemann in Fromm/Nordemann § 97 Rn. 154.

¹⁰⁵⁶ BGH GRUR 2004, 864 – *Internet-Versteigerung I*.

¹⁰⁵⁷ OLG Hamburg ZUM-RD 2008, 537 ff. – *Rapidshare I*; OLG Hamburg MMR 2010, 53 – *Rapidshare II*. Vgl. auch Nordemann in Fromm/Nordemann § 97 Rn. 162.

Gewicht der Interessen des Rechteinhabers.¹⁰⁵⁸ Im Grundsatz ist es dem Betreiber eines Internetauktionshauses nicht zuzumuten, sämtliche einzustellenden Angebote unterschiedslos auf Rechtsverletzungen zu überprüfen, da solche Prüfpflichten das Geschäftsmodell in Frage stellen würden.¹⁰⁵⁹ Das Gleiche gilt für die Betreiber von Meinungsforen für die bei ihnen eingestellten Beiträge.¹⁰⁶⁰ Eine allgemeine proaktive Überwachungspflicht besteht nach den Grundsätzen der Störerhaftung also nicht. Bei einem konkreten Hinweis auf eine Rechtsverletzung muss der Host-Provider jedoch unverzüglich handeln, um die konkrete Rechtsverletzung zu unterbinden.

Hat der Host-Provider durch sein Verhalten Rechtsverletzungen des Dritten provoziert, z.B. durch Werbung für die mögliche rechtswidrige Nutzung auf seiner Plattform, darf er sich auf eine Unzumutbarkeit der Prüfpflicht nicht berufen.¹⁰⁶¹ Dem Host-Provider, der durch die Verletzungshandlung wirtschaftliche Vorteile z.B. in Form von Provision erlangt, sind umfangreichere Prüfpflichten zuzumuten.¹⁰⁶²

Die Rechtsprechung hat diese Prüfpflichten von Host-Providern für einen Bloghoster weiter konkretisiert. Nach der Entscheidung des Bundesgerichtshofes vom 25.10.2011, die auch im Zusammenhang mit der Entscheidung vom 17.8.2011¹⁰⁶³ zu sehen ist, in der ähnliche Anforderungen an den Provider gestellt werden, besteht für Bloghoster eine Prüfungspflicht, wenn der Hinweis (hier: auf eine behauptete Persönlichkeitsrechtsverletzung) so konkret gefasst ist, dass der Rechtsverstoß auf der Grundlage der Behauptungen des Betroffenen unschwer, d.h. ohne eingehende rechtliche und tatsächliche Überprüfung, bejaht werden kann.¹⁰⁶⁴ Damit will der Bundesgerichtshof den Provider nur dann nicht belasten, wenn wenig nachvollziehbare oder unsubstantiierte Behauptungen eines angeblich Verletzten in Rede stehen. Geht man jedoch von einer hinreichend konkreten Beanstandung aus¹⁰⁶⁵, muss durch den Provider zunächst die Beanstandung des Betroffenen an den für den Blog Verantwortlichen zur Stellungnahme weitergeleitet werden. Bleibt eine Stellungnahme aus, ist von der Berechtigung der Beanstandung auszugehen und der beanstandete Eintrag ist durch den Provider zu löschen. Stellt der für den Blog Verantwortli-

¹⁰⁵⁸ Vgl. zu den Kriterien Weidert/Molle in *Ensthaler/Weidert*, S. 398 ff.; *Wilmer* NJW 2008, S. 1849 ff.

¹⁰⁵⁹ *BGH GRUR* 2004, 860 – *Internet-Versteigerung I*; *BGH GRUR* 2008, 702 – *Internet-Versteigerung III*.

¹⁰⁶⁰ *OLG Düsseldorf MMR* 2006, 621.

¹⁰⁶¹ *OLG Hamburg GRUR-RR* 2006, 148 – *Cybersky*, bestätigt durch *BGH MMR* 2009, 625 – *Cybersky*. Vgl. *Gabriel/Albrecht ZUM* 2010, S. 394; *Weidert/Molle in Ensthaler/Weidert*, S. 403; *Dreier in Dreier/Schulze* § 97 Rn. 33.

¹⁰⁶² *BGH GRUR* 2004, 860 ff. – *Internetversteigerung I*; *Gabriel/Albrecht ZUM* 2010, S. 394.

¹⁰⁶³ *BGH v. 17.8.2011 – I ZR 57/09 – Stiftparfüm* (Markenrechtsverletzungen auf ebay betreffend).

¹⁰⁶⁴ *BGH v. 25.10.2011 – VI ZR 93/10*. Nach der Entscheidung v. 17.8.2011 („*Stiftparfüm*“, s. dort LS b) und Tz. 20 ff) hängt das Ausmaß des insoweit vom Betreiber zu verlangenden Prüfungsaufwandes von den Umständen des Einzelfalles ab, insbesondere vom Gewicht der angezeigten Rechtsverletzungen auf der einen und den Erkenntnismöglichkeiten des Betreibers auf der anderen Seite ab.

¹⁰⁶⁵ Nach der o. a. Entscheidung „*Stiftparfüm*“ (s. dort LS c) S.1) soll ein Beleg der Rechtsverletzung durch den Beanstandenden nur dann erforderlich sein, wenn schutzwürdige Interessen des Betreibers eines Marktplatzes dies rechtfertigen. Das könne der Fall sein, wenn der Betreiber nach den Umständen des Einzelfalles berechnete Zweifel am Bestehen eines Schutzrechtes, an der Befugnis der Geltendmachung desselben durch den Hinweisenden oder am Wahrheitsgehalt der mitgeteilten tatsächlichen Umstände einer Rechtsverletzung haben dürfe und deshalb eigene aufwändige Recherchen anstellen müsse, um eine Rechtsverletzung hinreichend sicher feststellen zu können.

che die Berechtigung der Beanstandung substantiiert in Frage, ist der Host-Provider grundsätzlich gehalten, dem Betroffenen dies mitzuteilen und ggf. Nachweise zu verlangen, aus denen sich die behauptete Rechtsverletzung ergibt¹⁰⁶⁶. Ergibt sich aus der Stellungnahme des Betroffenen oder den vorgelegten Nachweisen auch unter Berücksichtigung einer etwaigen Äußerung des für den Blog Verantwortlichen eine rechtswidrige Verletzung des Persönlichkeitsrechts, ist der beanstandete Eintrag von dem Provider zu löschen.

Der Bundesgerichtshof mutet dem Bloghoster also für den Fall der hinreichend konkreten Beanstandung einen regelrechten Dialog mit den im Übrigen Beteiligten zu, d.h. dem für den Blog redaktionell Verantwortlichen und dem (durch die ehrverletzende Äußerung) Betroffenen, einschließlich einer Wertungsentscheidung. Bemerkenswert ist, dass in dieses von dem Bundesgerichtshof vorgeschlagene Verfahren eine staatliche Stelle bzw. ein Gericht in keiner Weise eingeschaltet ist. Vielmehr ergibt sich das Verfahren, sofern man von einer hinreichend konkret beschriebenen Rechtsverletzung ausgehen kann, ausschließlich zwischen den Beteiligten. Dies allein erscheint auch sachgerecht. Zunächst ist es sachgerecht, den Host-Provider nicht zum Tätigwerden zu verpflichten, wenn die Äußerung zu der Rechtsverletzung lediglich unkonkret erfolgt. Nicht zumutbar ist es auch, einen Provider dazu zu verpflichten, in Zweifelsfällen ohne Rücksprache mit einem Betroffenen selbstständig die Wertungsentscheidung zu treffen, ob ein Rechtsverstoß vorliegt oder nicht. Richtig ist es demgegenüber, ihn nur bei einem unschwer feststellbaren Rechtsverstoß zu Tätigkeiten zu verpflichten. Dann aber geht der Bundesgerichtshof davon aus, dass der Host-Provider eine jede hinreichend konkrete Beanstandung an den für den Blog redaktionell Verantwortlichen weiter zu leiten und sich im Zweifel mit dessen Äußerungen zu der Rechtsverletzung auseinanderzusetzen hat. Dabei kommt dem Host-Provider die Verpflichtung zu, die Beanstandung durch den Betroffenen und etwa entgegenstehende Äußerungen des Redakteurs eigenständig zu bewerten, gegeneinander abzuwägen und daraufhin die Entscheidung über das Löschen der entsprechenden Äußerung zu treffen, erforderlichenfalls wohl auch gegen den Willen des Redakteurs.

Ist eine konkrete Rechtsverletzung gegeben, ist der als Störer in Anspruch genommene Host-Provider nicht nur verpflichtet diese zu unterbinden, sondern auch Vorsorgemaßnahmen zu ergreifen, um künftige Rechtsverstöße vergleichbarer Art zu verhindern¹⁰⁶⁷. Auch insoweit stellt sich die Frage der Zumutbarkeit technischer Maßnahmen, wie etwa Filtersoftware, Lösch-Interface, Keywordfilter oder auch manuelle Kontrolle.¹⁰⁶⁸ Hashwert-Filter beispielsweise sind nach Ansicht des *LG Düsseldorf* zwar genügend, um die in einem Notice-and-Takedown-Letter benannte konkrete Verletzungshandlung, nicht jedoch die

¹⁰⁶⁶ So auch der BGH in der o. a. Entscheidung „Stiftparfüm“, LS c) S. 2.

¹⁰⁶⁷ BGH GRUR 2004, 860 – *Internetversteigerung I*; BGH GRUR 2008, 702 ff. – *Internet-Versteigerung III*. Zu den konkreten Prüfpflichten Nordemann CR 2010, S. 656 ff.

¹⁰⁶⁸ Vgl. zur Zumutbarkeit der einzelnen Maßnahmen Gabriel/Albrecht ZUM 2010, S. 394 ff.; Nordemann CR 2010, S. 659 ff.; Rössel/Rössel CR 2005, S. 811 ff.

gleichartigen, klar erkennbaren Verletzungen zu beseitigen, da sich mit jeder Veränderung der Inhalte der Hashwert ändern soll und nicht exakt identische verletzende Inhalte nicht (mehr) zu finden sind.¹⁰⁶⁹ Nicht ausreichend zur Vermeidung künftiger Rechtsverletzungen ist i.d.R., dass der Host-Provider die Nutzer auf die Gefahr von Urheberrechtsverletzungen hinweist und diese in allgemein gehaltenen Erklärungen bzw. in seinen AGB untersagt oder der Hinweis in den AGB eines Host-Providers, dass die Nutzer die Urheberrechte zu berücksichtigen haben.¹⁰⁷⁰ Auch die Drohung eines Host-Providers, das Konto der Nutzer zu löschen ist für sich genommen nicht ausreichend.¹⁰⁷¹ Nicht genügend ist ebenfalls die Einräumung der Nutzung eines Lösch-Interface zugunsten des Rechteinhabers, da es die Rechtsverletzung nicht verhindern kann, sondern nur dem Rechteinhaber die Möglichkeit gibt, selbst die urheberrechtswidrigen Inhalte zu löschen.¹⁰⁷² Diese Negativaufzählung der verschiedenen von den Host-Providern angewendeten Mittel zeigt deutlich, dass im Bereich des Hostings fremder Informationen die Anforderungen der deutschen Rechtsprechung bzw. Literatur an die Host-Provider im Hinblick auf zumutbare Maßnahmen höher sind, als die von diesen typischerweise ohne besondere Anforderung ergriffenen Maßnahmen.

2) *Zugangsanbieter (Access-Provider) als Störer*

Zugangsanbieter (Access-Provider) ermöglichen ihren Kunden lediglich den Zugang zum Internet. Im Rahmen von § 8 TMG sind sie, soweit auf den Anspruch anwendbar, privilegiert.¹⁰⁷³ Die Zugangsanbieter sind deshalb für die durch von ihnen gestellte Infrastruktur erreichbaren Inhalte grundsätzlich nicht verantwortlich, weil sie i.d.R. vom Inhalt der weitergeleiteten Informationen keine Kenntnis erlangen.

Nicht abschließend geklärt ist, ob die Zugangsanbieter nach den Grundsätzen der Störerhaftung für Rechtsverletzungen Dritter auf Unterlassung in Anspruch genommen werden können. Ob eine Ausdehnung der Rechtsprechung zur Störerhaftung von Host-Providern auf die Zugangsanbieter in Betracht kommt, ist in der untergerichtlichen Rechtsprechung umstritten.

Für eine Anwendung der in der Rechtsprechung entwickelten Grundsätze auch auf Zugangsanbieter kann sprechen, dass die gesetzliche Regelung des § 7 Abs. 2 Satz 2 TMG nicht danach differenziert, ob es sich um einen Access- oder Host-Provider handelt. Diese sieht vor, dass Verpflichtungen zur Entfernung oder Sperrung zur Nutzung von Informationen nach allgemeinen Gesetzen auch im Fall der Nichtverantwortlichkeit der Diensteanbieter nach §§ 8 bis 10 TMG unberührt bleiben. Der Bundesgerichtshof, der sich bei seiner Begründung zur Einschränkung der Haftungsprivilegierung auf § 7 Abs. 2 Satz 2

¹⁰⁶⁹ LG Düsseldorf ZUM 2008, 341; Nordemann CR 2010, S. 656.

¹⁰⁷⁰ Vgl. Weidert/Molle in Ensthaler/Weidert, S. 402.

¹⁰⁷¹ So Nordemann CR 2010, S. 659.

¹⁰⁷² OLG Hamburg MMR 2010, 51 – Rapidshare II. Vgl. Gabriel/Albrecht ZUM 2010, S. 395.

¹⁰⁷³ Vgl. Leupold/Glossner in Leupold/Glossner Teil 2 Rn. 561 ff.

TMG stützt, hat nach Ansicht des *LG Hamburg* insoweit ebenfalls keine Abgrenzung vorgenommen.¹⁰⁷⁴

Nach der ständigen Rechtsprechung des *LG Hamburg* wird eine Störerhaftung der Zugangsanbieter grundsätzlich bejaht. Im Urteil vom 12.11.2008, das den Anspruch auf Sperrung des Zugangs zu einer Webseite behandelte, auf der urheberrechtsverletzende Inhalte abgerufen werden konnten, hat das Gericht festgestellt, eine solche DNS-Sperre komme nur auf der Grundlage der Störerhaftung in Betracht.¹⁰⁷⁵ Diese wiederum komme jedoch erst in Betracht, wenn der Zugangsanbieter Kenntnis von der Rechtsverletzung erlangt hat und die Entfernung oder Sperrung technisch möglich sowie zumutbar ist.¹⁰⁷⁶ Im konkreten Fall sah das Gericht zwar die Anordnung einer DNS-Sperre als technisch möglich, jedoch nicht als zumutbar an, weil eine Sperrung des Zugangs zu einzelnen Webseiten eine begrenzte Eignung aufwies und dadurch nur minimale Wirkung erzielte.¹⁰⁷⁷ Eine DNS-Sperrung kann z.B. nicht nur vom Nutzer, sondern auch vom Anbieter der Webseite umgangen werden, indem er die Inhalte unter einer anderen Domain bereithält, die dann wieder über den Server des Zugangsanbieters erreichbar wäre. Abgestellt wurde darauf, dass der Zugangsanbieter nur ein automatisch ablaufendes Verfahren zur Verfügung stellt, welches den Kunden den Zugriff auf die Internetinhalte ermöglicht.¹⁰⁷⁸ In einem weiteren Urteil bestätigte das *LG Hamburg*, dass die Sperrmaßnahmen, wie die Filterung des Datenverkehrs, eine URL-Sperre oder eine DNS-Sperre, technisch möglich sind, verneint jedoch deren rechtliche Zulässigkeit. Das Gericht hat bestätigt, dass Filter- und Sperrmaßnahmen einen Eingriff des Zugangsanbieters in das Fernmeldegeheimnis seiner Kunden darstellen (Art. 10 GG), denn die Sperrmaßnahmen setzen die Kenntnisnahme von Kommunikationsdaten voraus, welche über das für die typische Erbringung von TK-Dienste erforderliche Maß hinausgeht.¹⁰⁷⁹ Ein Eingriff ist nach Auffassung des Gerichts nach Art. 10 Abs. 2 Satz 1 GG nur bei einer gesetzlichen Beschränkung erlaubt. Eine solche Beschränkung ist für zivilrechtliche Filter- und Sperrmaßnahmen nicht gegeben und daher sind diese Maßnahmen rechtlich nicht zulässig.¹⁰⁸⁰

Das *LG Hamburg* hat in einer anderen Entscheidung jedoch die Störerhaftung des Zugangsanbieters bei Urheberrechtsverletzungen und seine Inanspruchnahme auf Sperrung einer Internetseite bejaht. Im Rahmen eines einstweiligen Verfügungsverfahrens hat das Gericht dem Zugangsanbieter untersagt, eine Webseite für illegales Filesharing („The Pirate Bay“) abzurufen und deren Seite an das Internet anzubinden.¹⁰⁸¹ Der Zugangsanbieter haftet nach Auffassung des Gerichts als Störer, da ihm möglich und nach der Abmah-

¹⁰⁷⁴ So *LG Hamburg* NJOZ 2010, 443.

¹⁰⁷⁵ *LG Hamburg* NJOZ 2010, 443.

¹⁰⁷⁶ *LG Hamburg* NJOZ 2010, 444.

¹⁰⁷⁷ Vgl. auch *Cichon* GRUR-Prax 2010, 345; *Bäcker* ZUM 2008, S. 394 ff.

¹⁰⁷⁸ *LG Hamburg* NJOZ 2010, 444 ff.

¹⁰⁷⁹ Vgl. *Feldmann* K&R 2011, S. 227.

¹⁰⁸⁰ *LG Hamburg* MMR 2010, 489 ff.

¹⁰⁸¹ *LG Hamburg* Urteil vom 6.5.2010, Az. 310 O 154/10, BeckRS 2010, 12237.

nung auch zumutbar gewesen sei, zu verhindern, dass die Webseite mit urheberrechtsverletzenden Inhalten abgerufen würde.¹⁰⁸²

Verschiedene andere Gerichte stehen demgegenüber auf dem Standpunkt, dass den Zugangsanbieter mangels zumutbarer Prüfpflichten keine Störerhaftung trifft.¹⁰⁸³ Eine Entscheidung des *OLG Frankfurt a.M.* betraf die Sperrung des Zugangs zur Suchmaschine *google.de*, über die jugendgefährdende Inhalte auffindbar waren. Das Gericht stellte klar, dass die vom Bundesgerichtshof entwickelten Grundsätze in Bezug auf den Betreiber einer Internetauktionsplattform (Host-Provider) auf Access-Provider nicht übertragen werden können. Anders als ein Host-Provider eröffne der Zugangsanbieter nicht eine Gefahrenquelle für Rechtsverstöße, sondern stelle nur den technischen Internetzugang bereit und habe keinen Einfluss auf die im Internet bereitgestellten Inhalte. Anders sei die Situation beim Host-Provider, der auf den auf seinen Internetseiten eingestellten Inhalt Einfluss nehmen und rechtswidrige Inhalte löschen kann.¹⁰⁸⁴ Eine vollständige Sperrung des Zugangs, die auch neutrale Inhalte beträfe, sei aber für einen Zugangsanbieter nicht zumutbar und würde zu einer Tätigkeit des Access-Providers führen, die gesellschaftlich und rechtspolitisch nicht erwünscht ist.¹⁰⁸⁵

Eine Störerhaftung der Access-Provider wurde auch in der jüngsten Rechtsprechung des *LG Köln* verneint.¹⁰⁸⁶ Zu entscheiden war über die Sperrung des Zugangs zu der Filesharingplattform *eDonkey*. Das Gericht stellte fest, dass der Zugangsanbieter nicht zu solchen Vorsorgemaßnahmen in Form von Zugangssperren (DNS- und/oder IP-Adressen-Sperre) verpflichtet sei, da zur Umsetzung dieser Maßnahmen der Zugangsanbieter die Datenkommunikation zwischen seinen Kunden kontrollieren müsse. Darüber hinaus hat das Gericht die Filter- und Sperrmaßnahmen ohne gesetzliche Grundlage als mit dem Fernmeldegeheimnis nicht zu vereinbaren angesehen. Die zur Verhinderung von Rechtsverletzungen genannten Vorsorgemaßnahmen wurden vom Gericht als unzumutbar eingeschätzt, da der Zugangsanbieter eine Vielzahl technischer Sicherheitsvorkehrungen in Form von Datenfiltern einrichten müsste, die wiederum immer neuen Gegebenheiten und neuen Verletzungsformen angepasst werden müssten.¹⁰⁸⁷

¹⁰⁸² *LG Hamburg* Urteil vom 6.5.2010, Az. 310 O 154/10, BeckRS 2010, 12237. So auch *LG Hamburg*, K&R 2011, 215 ff., das eine Störerhaftung des Betreibers eines Internet-Cafes bejahte, von welchem aus ein Gast urheberrechtlich geschützte Werke öffentlich zugänglich gemacht hat.

¹⁰⁸³ *OLG Frankfurt a.M.* MMR 2008, 166; *LG Düsseldorf* MMR 2008, 349; *LG Kiel* MMR 2008, 123.

¹⁰⁸⁴ *OLG Frankfurt a.M.* MMR 2008, 166. Vgl. auch *Spindler* MMR 2008, S. 168; *Feldmann* K&R 2011, S. 227.

¹⁰⁸⁵ Vgl. *Schnabel* K&R 2008, S. 29. Vgl. auch *Frey* MMR 2009, S. 221 ff., der als Konsequenz für die Umsetzung der Sperrungsmaßnahmen durch die Access-Provider sieht, dass Access-Provider zu „Gatekeepern des Rechts“ werden.

¹⁰⁸⁶ *LG Köln* Urteil vom 31.8.2011, Az. 280 362/10, abrufbar unter http://www.justiz.nrw.de/nrwe/lgs/koeln/lg_koeln/j2011/28_O_362_10_Urteil_20110831.html (Stand November 2011).

¹⁰⁸⁷ *LG Köln* Urteil vom 31.8.2011, Az. 280 362/10, abrufbar unter http://www.justiz.nrw.de/nrwe/lgs/koeln/lg_koeln/j2011/28_O_362_10_Urteil_20110831.html, Rn. 116 ff. (Stand November 2011).

In Bezug auf ein Tätigwerden des Zugangsanbieters zur Verhinderung von Rechtsverletzungen Dritter wurden in der Rechtsprechung technische Maßnahmen wie die DNS-Sperre, die Sperrung der IP-Adresse illegaler Angebote oder der Einsatz von Filtermechanismen, diskutiert. Diese Maßnahmen und somit ein Unterlassungsanspruch des Rechteinhabers gegen die Zugangsanbieter wurden von den Gerichten zumeist abgelehnt, da den technischen Maßnahmen die Realisierbarkeit und die volle Wirkung fehlten.¹⁰⁸⁸

3) Haftung bzw. Störerhaftung des Anschlussinhabers

Lediglich aus Gründen der Vollständigkeit der Darstellung der Störerhaftung im Bereich der Internetnutzung sei auch auf die Störerhaftung des Anschlussinhabers eingegangen.

Da ein Internetanschluss von mehreren natürlichen Personen genutzt werden kann, etwa bei gemeinsamer Nutzung des Internetzugangs durch Familienmitglieder oder bei unfreiwilliger Öffnung eines WLAN-Anschlusses für Dritte, muss der Anschlussinhaber nicht zwingend die Rechtsverletzung begangen haben.¹⁰⁸⁹ Wer von mehreren Nutzern zum fraglichen Zeitpunkt den Internetanschluss genutzt und die Urheberrechtsverletzung begangen hat, lässt sich von dem Verletzten kaum nachweisen.

Wird ein Werk über eine bestimmte IP-Adresse öffentlich zugänglich gemacht, besteht nach der jüngeren Rechtsprechung des Bundesgerichtshofes eine tatsächliche Vermutung dafür, dass der Inhaber des Internetanschlusses für die Rechtsverletzung verantwortlich ist.¹⁰⁹⁰ Die Vermutung ist jedoch widerleglich, d.h. der Anschlussinhaber kann geltend machen, dass eine andere Person die Rechtsverletzung begangen habe. Für die entsprechenden Tatsachen trägt er die sekundäre Darlegungslast, d.h. er muss, als im Grunde nicht beweisbelastete Partei, soweit möglich und zumutbar, der Aufklärungspflicht nachkommen, weil dem primär Beweisbelasteten entsprechende Informationen nicht zugänglich sind.¹⁰⁹¹ Im konkreten Fall muss der Anschlussinhaber glaubhaft darlegen, dass ein Dritter die Tat begangen hat.¹⁰⁹²

Nach Ansicht des Bundesgerichtshofes obliegt dem Inhaber eines WLAN-Anschlusses auch ohne einen Hinweis auf etwaige Rechtsverletzungen die Pflicht, sein Anschluss ab Inbetriebnahme durch hinreichende Maßnahmen gegen den Zugriff Dritter zu sichern. Tut er dies nicht, so soll der Anschlussinhaber jedenfalls als Störer haften. Die Störerhaftung setzt voraus, dass der Anschlussinhaber in irgendeiner Weise willentlich und adäquat kausal an der Verletzung des geschützten Rechts mitwirkt und dabei gegen Prüfpflichten verstoßen hat; dafür soll ausreichen, dass der Anschlussinhaber einen Internetanschluss geschaffen

¹⁰⁸⁸ OLG Frankfurt a.M. MMR 2008, 166; LG Düsseldorf MMR 2008, 349; LG Kiel MMR 2008, 123. Vgl. zu den Maßnahmen Bäcker ZUM 2008, S. 394 ff.

¹⁰⁸⁹ Waldhausen in Schwartmann, S. 1246.

¹⁰⁹⁰ BGH MMR 2010, 565 – Sommer unseres Lebens. Dies mag im konkreten Fall auch daran gelegen haben, dass der Anschlussinhaber, so kann man die Entscheidung verstehen, die Verlässlichkeit des Systems zur Ermittlung seiner IP-Adresse nicht ausreichend bestritten bzw. in Frage gestellt hatte. Vgl. auch Karger/Tremml GRUR-Prax 2010, S. 305.

¹⁰⁹¹ BGH NJW-RR 2004, 990. Vgl. auch Karger/Tremml GRUR-Prax 2010, S. 305.

¹⁰⁹² BGH MMR 2010, 565 – Sommer unseres Lebens; OLG Köln MMR 2010, 45; OLG Köln MMR 2010, 281.

und damit die objektive Gefahr von Rechtsverletzungen über seinen Anschluss ermöglicht hat.¹⁰⁹³ Der Umfang der Prüfpflichten bestimmt sich danach, inwieweit sie dem in Anspruch Genommenen im Einzelfall zumutbar sind.¹⁰⁹⁴

Nicht geklärt ist die Haftung des Anschlussinhabers für Urheberrechtsverletzungen von Familienangehörigen¹⁰⁹⁵ und das Bestehen von Aufklärungs- und Überwachungspflichten. Teilweise wird vertreten, dass die Eltern für über ihren Internetanschluss begangene Urheberrechtsverletzungen minderjähriger Kinder als Störer haften, wenn sie nicht geeignete Aufklärungs- und Überwachungsmaßnahmen getroffen haben.¹⁰⁹⁶ Die Eltern seien verpflichtet, alle nach dem Stand der Technik vernünftigen Maßnahmen zu ergreifen, damit der Internetanschluss nicht für Rechtsverletzungen genutzt werde.¹⁰⁹⁷ Nach einer anderen Auffassung seien dagegen bei volljährigen Kindern die Prüf- und Überwachungspflichten der Eltern stark reduziert.¹⁰⁹⁸ Bestehen beim Nutzungsverhalten von Familienmitgliedern keine konkreten Anhaltspunkte für eine Rechtsverletzung, sei eine ständige Überwachung der Eltern nicht zumutbar;¹⁰⁹⁹ nur wenn im Einzelfall konkrete Anhaltspunkte für eine Urheberrechtsverletzung bestehen, bestünden Prüfungs- und Überwachungspflichten.¹¹⁰⁰ Ob es bei Eröffnung des Internetverkehrs einer einweisenden Belehrung für die diesen benutzenden Kinder bedürfe, beurteile sich im Einzelfall nach dem Alter und dem Grad der Vernunft: Bei volljährigen Kindern dürfte eine solche Belehrung aufgrund des Wissensvorsprungs der Kinder entfallen¹¹⁰¹, minderjährige Kinder sollten bei Eröffnung des Internetzugangs über das Verbot von Urheberrechtsverletzungen umfassend aufgeklärt werden.¹¹⁰²

Abschließend ist die Fallgestaltung des Zugriffs unbekannter Dritte von außen auf den Internetanschluss anzusprechen¹¹⁰³. Nach der Rechtsprechung des Bundesgerichtshofes

¹⁰⁹³ Vgl. Möllmann/Bießmann in Schwartmann, S. 1299; Nümann/Mayer ZUM 2010, S. 326.

¹⁰⁹⁴ BGH GRUR 2004, 860 – *Internetversteigerung I*; BGH GRUR 2007, 711 – *Internetversteigerung II*.

¹⁰⁹⁵ Zur Haftung von Ehepartnern untereinander vgl. OLG Köln K&R 2011, 354. Hiernach haftet der Anschlussinhaber für Filesharing-Aktivitäten des Ehepartners nicht als Störer, auch wenn er diesem die Teilnahme an sog. Tauschbörsen nicht ausdrücklich untersagt hat, weil ein Haushalt normalerweise nur einen Internetanschluss habe, der als gemeinsamen Anschluss betrachtet würde, und sei es zweifelhaft, ob gegenseitige Überwachungspflichten der Ehegatten bestehen.

¹⁰⁹⁶ LG Hamburg MMR 2007, 131 ff.; LG Frankfurt a.M. MMR 2007, 805; OLG Köln K&R 2010, 131 ff. – das bloße, durch die Eltern ausgesprochene Verbot, an Internet-Tauschbörsen teilzunehmen, genügt nicht, um Rechtsverletzungen durch die Kinder im Rahmen der elterlichen Kontrollpflichten zu vermeiden.

¹⁰⁹⁷ LG Hamburg MMR 2007, 132; LG Frankfurt a.M. MMR 2007, 805. So sei es den Eltern minderjähriger Kinder zumutbar, Benutzerkonten mit individuellen Passwörtern zu erstellen, die bezüglich der Nutzungsbefugnisse so ausgestaltet sind, dass bereits die Installation einer Filesharing-Software verhindert werde. Auch die Einrichtung einer Firewall könne gefordert werden.

¹⁰⁹⁸ LG Mannheim MMR 2007, 268.

¹⁰⁹⁹ OLG Frankfurt a.M. MMR 2008, 170; LG Mannheim MMR 2007, 268; vgl. auch Weidert/Molle in Ensthaler/Weidert, S. 411; Röhl/Bosch NJW 2008, S. 1418; Solmecke MMR 2007, S. 268 ff. Anders LG Düsseldorf MMR 2009, 780 – verdachtsunabhängige Überwachung volljähriger Kinder durch die Eltern.

¹¹⁰⁰ OLG Frankfurt a.M. MMR 2008, 170.

¹¹⁰¹ LG Mannheim MMR 2007, 268.

¹¹⁰² Vgl. Röhl/Bosch NJW 2008, S. 1418.

¹¹⁰³ Für eine Störerhaftung bei ungesichertem WLAN vgl. LG Hamburg MMR 2006, 763; OLG Düsseldorf MMR 2008, 256; LG Frankfurt a.M. ZUM 2007, 406; gegen eine allgemeine Störerhaftung vgl. OLG Frankfurt a.M.

unterliegt der private Betreiber eines WLAN-Anschlusses der Pflicht zu prüfen, ob sein Anschluss durch angemessene Sicherungsmaßnahmen hinreichend dagegen geschützt ist, von unberechtigten Dritten für die Begehung von Rechtsverletzungen missbraucht zu werden.¹¹⁰⁴ Dem Betreiber eines WLAN ist zuzumuten, diejenigen Sicherungen einzuhalten, die zum Kaufzeitpunkt des WLAN-Routers für den privaten Bereich marktüblich sind; zur Sicherung von Computernutzungen ist daher für den Zugang zum Router, ein persönliches, ausreichend langes und sicheres Passwort zu vergeben.¹¹⁰⁵ Der Anschlussinhaber haftet insbesondere als Störer, wenn er die vom Hersteller im Zeitpunkt des Erwerbs des Routers vorgesehenen werkseitigen Standardsicherheitseinstellungen unverändert gelassen hat und einen unverschlüsselten WLAN-Zugang eröffnet.¹¹⁰⁶ Nicht zumutbar für den Anschlussinhaber ist dagegen, die Sicherheitseinstellungen nach dem Zeitpunkt des Erwerbs laufend an die sich ständig ändernden technischen Gegebenheiten anzupassen und dafür entsprechende finanzielle Mittel aufzuwenden.¹¹⁰⁷ Die Prüfpflicht eines WLAN-Anschlussinhabers besteht bereits ab Inbetriebnahme des Anschlusses und nicht erst nach der Kenntniserlangung einer ersten Rechtsverletzung wie bei der Störerhaftung des Plattformbetreibers. Damit besteht auch ein grundlegender Unterschied zur Haftung von Host-Providern, denn anders als bei diesen, handelt es sich beim Betrieb eines WLAN-Anschlusses nicht um ein Geschäftsmodell, das durch die Auferlegung präventiver und anlassunabhängiger Prüfpflichten in Frage gestellt würde.¹¹⁰⁸

Unabhängig davon, ob man die Auffassung vertritt, dass auf den privaten Anschlussinhaber die Haftungsprivilegierung des TMG Anwendung finden kann, ist eine etwaige Haftungsprivilegierung nur auf Schadensersatzansprüche, nicht aber auf Unterlassungsansprüche anwendbar.¹¹⁰⁹ Für den Anschlussinhaber gilt also bei den i.d.R. geltend gemachten Unterlassungsansprüchen die Haftungsprivilegierung des TMG ohnehin nicht.¹¹¹⁰

MMR 2008, 603 (eine Störerhaftung besteht nur beim Vorliegen konkreter Anhaltspunkte einer Rechtsverletzung).

¹¹⁰⁴ BGH MMR 2010, 566 – *Sommer unseres Lebens*. Kritisch dazu Mantz MMR 2010, S. 568 ff. Zu Schutzpflichten des Anschlussinhabers siehe Borges, NJW 2010, 2625 ff.

¹¹⁰⁵ BGH MMR 2010, 567 – *Sommer unseres Lebens*. Zum Begriff siehe Borges, NJW 2010, 2626. Nach seiner Meinung minimiert zwar die marktübliche Sicherung den Aufwand des Nutzers, stellt aber zugleich die Schwachstelle des Konzepts dar. Denn wegen der ungeheuren Dynamik bei Angriffen im Internet gehöre zu den Schutzpflichten des Nutzers die Pflicht zur Aktualisierung, ohne die Möglichkeit diese auf den Kaufzeitpunkt zu beschränken.

¹¹⁰⁶ Karger/Tremml GRUR-Prax 2010, S. 305.

¹¹⁰⁷ BGH MMR 2010, 567 – *Sommer unseres Lebens*.

¹¹⁰⁸ BGH MMR 2010, 567 – *Sommer unseres Lebens*.

¹¹⁰⁹ Siehe oben S. 231.

¹¹¹⁰ Zuletzt BGH MMR 2010, 567 – *Sommer unseres Lebens*. In der Literatur wird teilweise dagegen die Meinung vertreten, dass der private Anschlussinhaber als Zugangsvermittler in den Genuss der Haftungsprivilegierung gemäß § 8 TMG kommt, der normalerweise für Access Provider gilt. Vgl. Stang/Hühner GRUR-RR 2008, S. 275; Gietl ZUM 2007, S. 408; Lutz VuR 2010, S. 342.

5. Voraussetzungen für einen Unterlassungsanspruch, Erstbegehungs- bzw. Wiederholungsgefahr

Der Unterlassungsanspruch nach § 97 Abs. 1 Satz 1 UrhG setzt Wiederholungsgefahr voraus, also die Gefahr, dass eine konkrete Rechtsverletzung erneut begangen wird. Daneben besteht seit 1.9.2008 nach ausdrücklicher Regelung in § 97 Abs. 1 Satz 2 UrhG der vorbeugende Unterlassungsanspruch, der gewährt wird, wenn eine konkret drohende Erstbegehungsgefahr besteht.¹¹¹¹ Der Verletzer hat in jedem Fall weitere bzw. erstmalige Verletzungshandlungen sofort zu unterlassen, unabhängig davon, ob er schuldhaft gehandelt hat oder nicht.

Eine **Wiederholungsgefahr** wird in der Regel vermutet, wenn bereits eine Rechtsverletzung begangen worden ist.¹¹¹² An die Widerlegung der Wiederholungsgefahr stellt die Rechtsprechung hohe Anforderungen. So genügt zur Beseitigung der Wiederholungsgefahr die einfache Erklärung, künftig keine Verletzung mehr zu begehen¹¹¹³, ebenso wenig, wie die bloße Einstellung der Rechtsverletzung auf Seiten des Verletzers, z.B. durch Entfernung einer rechtswidrig öffentlich zugänglich gemachten Werkkopie aus dem Internet.¹¹¹⁴ Die Wiederholungsgefahr entfällt nur dann, wenn eine unbefristete, vorbehaltlose und strafbewehrte Unterlassungsverpflichtungserklärung abgegeben wird, die von dem Verletzten angenommen werden muss.¹¹¹⁵ Die Strafbewehrung bzw. Vertragsstrafe muss angemessen hoch sein, um den Verletzer von weiteren Rechtsverletzungen abzuhalten.¹¹¹⁶ Nach dem in der Praxis weitgehend durchgesetzten *Hamburger Brauch* setzt der Abmahnende die Höhe der Vertragsstrafe einseitig fest. Akzeptiert der Anspruchsgegner die Vertragsstrafe nicht, lässt sich deren Höhe vom zuständigen Gericht überprüfen.¹¹¹⁷ Nicht abschließend geklärt ist, ob der Rechteinhaber einen Anspruch auf die Unterlassung jeder Verletzungsform hat. Teilweise wird vertreten, dass die Unterlassungserklärung nicht nur für die konkrete Verletzungsform sondern für alle im Kern gleichartige Verletzungen gilt.¹¹¹⁸ In der Rechtsprechung kann allerdings im Einzelfall eine Unterlassungserklärung, die sich auf die gesamten Werke eines Rechteinhabers bezieht, ohne zu spezifizieren, wel-

¹¹¹¹ Nach gefestigter Rechtsprechung bestand der vorbeugende Unterlassungsanspruch schon vorher. Vgl. BGHZ 16, 170 – *Constanze II*.

¹¹¹² BGHZ 16, 167 – *Constanze II*; BGH GRUR 1961, 140 – *Familie Schölermann*. Vgl. auch von Wolff in *Wandtke/Bullinger* §97 Rn. 36; *Spindler in Spindler/Schuster* § 97 Rn. 36; *Dreier in Dreier/Schulze* § 97 Rn. 42.

¹¹¹³ BGH GRUR 1961, 140 – *Familie Schölermann*.

¹¹¹⁴ *Nordemann in Fromm/Nordeman* § 97 Rn. 31.

¹¹¹⁵ Zu den Folgen nach strafbewehrter Unterlassungserklärung auch von Wolff in *Wandtke/Bullinger* §97 Rn. 38.

¹¹¹⁶ Zur Höhe der Vertragsstrafe *Weidert/Molle in Ensthaler/Weidert*, S. 458 ff. *Dreier in Dreier/Schulze* § 97 Rn. 42; *Nordemann in Fromm/Nordeman* § 97 Rn. 32 ff.

¹¹¹⁷ BGH GRUR 1994, 146 – *Vertragsstrafenbemessung*.

¹¹¹⁸ So *Möllmann/Bießmann in Schwartmann*, S. 1276; *Weidert/Molle in Ensthaler/Weidert*, S. 455 ff. mit weiteren Hinweisen aus der Rechtsprechung; *Nordemann in Fromm/Nordeman* § 97 Rn. 30. A.A. *Spindler in Spindler/Schuster* § 97 Rn. 36; *Lutz VuR* 2010, S. 341.

che Verletzungshandlungen im Sinne von im Kern gleichartigen Verletzungshandlungen von der Unterlassungserklärung noch umfasst sind, unzureichend sein.¹¹¹⁹

Erstbegehungsgefahr ist bei allen vorbereitenden Maßnahmen zu bejahen, die eine künftige Verletzung nahe legen.¹¹²⁰ Die Beseitigung der Erstbegehungsgefahr stellt - im Gegensatz zur Wiederholungsgefahr – grundsätzlich weniger strenge Anforderungen. Eine strafbewehrte Unterlassungserklärung ist in diesem Fall nicht immer notwendig.¹¹²¹ Nach der Rechtsprechung des Bundesgerichtshofes kann sich der vorbeugende Unterlassungsanspruch auch gegen den Störer richten;¹¹²² bei Urheberrechtsverletzungen im Internet besteht ein Unterlassungsanspruch, soweit der Störer seine Prüfpflichten verletzt hat¹¹²³.

6. Schadensersatzanspruch

a. Verschulden

Im Unterschied zum Unterlassungsanspruch setzt der Schadensersatzanspruch ein Verschulden des Verletzers voraus. Vorsätzlich handelt der Verletzer, wenn er die Rechtsverletzung bewusst und gewollt begeht oder diese billigend in Kauf nimmt¹¹²⁴. Dies sind auch Fälle der (Internet-) Piraterie durch bewussten Upload urheberrechtlich geschützten Materials sowie Fälle, in denen sich der Verletzer bewusst über ihm bekannte Rechte Dritter hinwegsetzt.¹¹²⁵ Bei einem Tatsachen- und Rechtsirrtum kommt in der Regel Fahrlässigkeit in Betracht.¹¹²⁶ Die Rechtsprechung stellt im Urheberrecht an das Maß der zur Vermeidung einer Fahrlässigkeit zu wahrenden Sorgfalt strenge Anforderungen.¹¹²⁷ Bei Urheberrechtsverletzungen im Internet, besonders beim ersten Abruf von Inhalten von einer ihm bis dato unbekannten Webseite, weiß jedoch der einfache Nutzer oft nicht, dass er durch das Browsen und Herunterladen urheberrechtsrelevante Handlungen begeht. Daher kann ein Verschulden für den bloßen Nutzer, jedenfalls bei einem ersten Zugriff auf solche Inhalte, ausgeschlossen sein.¹¹²⁸ Trifft der Nutzer, auch der unbefangene, jedoch auf Inhalte, die im Regelfall nur entgeltlich angeboten werden, ist eine strenge Sorgfalt gefordert, wenn diese auf der von ihm aufgefundenen Webseite kostenlos zum Download angeboten werden.

¹¹¹⁹ Vgl. LG Köln, Urteil von 25.5.2010, Az. 28 O 168/2010, abrufbar unter: http://www.justiz.nrw.de/nrwe/lgs/koeln/lg_koeln/j2010/28_O_168_10beschluss20100525.html (Stand: November 2011).

¹¹²⁰ BGH GRUR 1964, 95 – *Tonandgeräte-Händler*; BGH GRUR 2003, 961 – *Paperboy*.

¹¹²¹ So von Wolff in *Wandtke/Bullinger* §97 Rn. 41; Weidert/Molle in *Ensthaler/Weidert*, S. 455; Kitz NJW 2008, S. 2374.

¹¹²² BGH GRUR 2007, 711 – *Internet-Versteigerung II*.

¹¹²³ Bei der Haftung des Inhabers eines WLAN-Anschlusses als Störer hat der BGH dessen Unterlassungspflicht recht weit eingegrenzt; der Störer ist insoweit nur verpflichtet, es zu unterlassen, Dritten Urheberrechtsverletzungen durch die unzureichende Sicherung seines WLAN-Anschlusses zu ermöglichen; BGH MMR 2010, 566 – *Sommer unseres Lebens*.

¹¹²⁴ Vgl. Dreier in *Dreier/Schulze* § 97 Rn. 56; Möllmann/Bießmann in *Schwartzmann*, S. 1277; von Wolff in *Wandtke/Bullinger* §97 Rn. 51.

¹¹²⁵ Dreier in *Dreier/Schulze* § 97 Rn. 56.

¹¹²⁶ Vgl. Dreier in *Dreier/Schulze* § 97 Rn. 56.

¹¹²⁷ BGH GRUR 1999, 51 – *Bruce Springsteen and his Band*; OLG Frankfurt a.M. GRUR 1998, 49 – *La Boheme*; OLG Düsseldorf GRUR-RR 2005, 213 – *OEM-Version*.

¹¹²⁸ So Weidert/Molle in *Ensthaler/Weidert*, S. 476.

Für Verwerter von Inhalten besteht eine Prüf- und Erkundigungspflicht. Insoweit haben sich diese bei Rechtsübertragungen über den Bestand und Umfang der Nutzungsberechtigung Gewissheit zu verschaffen,¹¹²⁹ so dass eine Zusicherung seitens der Übertragenden grundsätzlich nicht genügt. Die Verwerter müssen vielmehr eine etwaige Rechtekette vollständig überprüfen.¹¹³⁰ Fachkreise, z.B. Produzenten, Verleger, Sendeunternehmen und Herausgeber, unterliegen gesteigerter Sorgfaltspflicht.¹¹³¹

b. Höhe des Schadensersatzes, Berechnungsmethoden

Steht eine schuldhafte und rechtswidrige Urheberrechtsverletzung fest, besteht ein Anspruch auf Ersatz materieller Schäden nach § 97 Abs. 2 Satz 1 bis 3 UrhG. Diese Regelungen sehen ausdrücklich die in der Rechtsprechung etablierte dreifache Berechnungsmethode vor: konkreter Schaden, Herausgabe des Verletzergewinns oder Lizenzanalogie.¹¹³² Das Recht des Verletzten zur Wahl der Berechnungsmethode erlischt erst, wenn der Schadensersatz rechtskräftig zuerkannt oder erfüllt worden ist¹¹³³.

Wird der **konkrete Schaden** geltend gemacht, erfolgt die Schadensberechnung nach der Differenztheorie auf Grundlage des Unterschieds zwischen dem durch die Verletzung herbeigeführten Vermögenszustand und dem Vermögenszustand, der ohne die Urheberrechtsverletzung erreicht worden wäre, einschließlich des entgangenen Gewinns.¹¹³⁴ Den durch eine Urheberrechtsverletzung verursachten Schaden zu definieren und zu beziffern, bereitet in der Praxis allerdings große Schwierigkeiten. Darüber hinaus lassen sich Umsatzeinbußen und Gewinnminderungen selten kausal allein und ausschließlich auf die Urheberrechtsverletzung zurückführen.¹¹³⁵

Bei der **Herausgabe des** vom Verletzer durch die Rechtsverletzung erzielten **Gewinns** (§ 97 Abs. 2 Satz 2 UrhG) handelt es sich nicht um einen selbstständigen Gewinnabschöpfungsanspruch, sondern um eine Berechnungsmethode des gleichen einheitlichen Schadens.¹¹³⁶ Unabhängig davon, ob der Verletzte in der Lage gewesen wäre, ebenfalls den Gewinn zu erzielen, hat der Verletzer den Gewinn, der nach Abzug aller Steuern, sonstigen Abgaben und Kosten bleibt, herauszugeben.¹¹³⁷ Umstritten ist z.B., welche Kosten der Verletzer bei der Ermittlung seines Gewinns abziehen darf. Wurde nach der früheren Rechtsprechung des Bundesgerichtshofes der Abzug von Allgemeinkosten großzügig zu-

¹¹²⁹ Vgl. Möllmann/Bießmann in Schwartmann, S. 1278; von Wolff in Wandtke/Bullinger §97 Rn. 52.

¹¹³⁰ BGH GRUR 1988, 375 – Schallplattenimport.

¹¹³¹ BGH GRUR 1991, 333 – Lizenzmangel; OLG Frankfurt GRUR-RR 2006, 45 – Panther mit Smaragdauge. Vgl. Dreier in Dreier/Schulze § 97 Rn. 57.

¹¹³² BGH GRUR 2008, 94 – Zerkleinerungsvorrichtung.

¹¹³³ BGH GRUR 2000, 227 – Planungsmappe.

¹¹³⁴ So Spindler in Spindler/Schuster § 97 Rn. 46; Möllmann/Bießmann in Schwartmann, S. 1279; Vinck in Loewenheim § 81 Rn. 41.

¹¹³⁵ Vgl. Spindler in Spindler/Schuster § 97 Rn. 46; Dreier in Dreier/Schulze § 97 Rn. 60.

¹¹³⁶ § 97 Abs. 1 Satz 2 UrhG a.F. sah vor, dass der Verletzergewinn an Stelle des Schadensersatzes geltend gemacht werden könne.

¹¹³⁷ BGH GRUR 2002, 535 – Unikatrahmen. Vgl. Vinck in Loewenheim § 81 Rn. 47; von Wolff in Wandtke/Bullinger §97 Rn. 68.

gelassen¹¹³⁸, dürfen nunmehr bei der Berechnung des Verletzergewinns Gemeinkosten nur abgesetzt werden, wenn und soweit sie den schutzrechtsverletzenden Gegenständen unmittelbar zugerechnet werden können.¹¹³⁹ Herauszugeben ist der Gewinn, der kausal auf der Rechtsverletzung beruht.¹¹⁴⁰ Beruht der Gewinn – außer auf der Urheberrechtsverletzung – auch auf anderen Umständen, so ist der herauszugebende Gewinn auf den Teil zu beschränken, der auf die Verletzung zurückzuführen ist.¹¹⁴¹

In der Praxis ist die Geltendmachung einer angemessenen Lizenzgebühr (**Lizenzanalogie**) die am häufigsten herangezogene Methode. Hiernach soll der Verletzer nicht besser gestellt sein als derjenige, der sich beim Rechteinhaber um eine Lizenz bemüht hat, d.h. ein Lizenznehmer.¹¹⁴² Die Lizenzanalogie stellt mithin eine objektive Berechnungsmethode dar; es genügt für ihre Anwendung, dass die Überlassung von Ausschließlichkeitsrechten zur Benutzung durch Dritte gegen Entgelt rechtlich möglich und verkehrsüblich ist.¹¹⁴³ Als angemessen gilt die übliche Vergütung.¹¹⁴⁴ Zugrunde zu legen ist derjenige Betrag, den vernünftige Lizenzvertragsparteien vereinbart hätten.¹¹⁴⁵ Dies muss jedoch mindestens der angemessenen Vergütung im Sinne von § 32 UrhG entsprechen. In den Bereichen, in denen Tarifvergütungen gelten, können die Tarife bei der Bestimmung der Lizenz herangezogen werden; diese stellen jedoch nicht zwingend die Obergrenze des zu ergänzenden Betrags dar.¹¹⁴⁶ Kritisch zu prüfen ist insbesondere die Verkehrsgeltung der Tarifvergütungen. Anders als bei den Tarifvergütungen der großen Verwertungsgesellschaften (z.B. GEMA), steht die Verkehrsgeltung der Tarifvergütungen kleinerer Verwertungsgesellschaften nicht ohne weiteres fest.¹¹⁴⁷ Die Angemessenheit der Lizenzgebühr ist in der gerichtlichen Auseinandersetzung nach § 287 ZPO unter Berücksichtigung der Umstände des Einzelfalls zu schätzen.¹¹⁴⁸

Bisweilen werden von Rechteinhabern bzw. deren Vertretern, jedenfalls bei erstmaliger Ansprache eines bestimmten Verletzers, außergerichtlich Beträge geltend gemacht, die deutlich über dieser angemessenen Gebühr liegen, zuweilen in der Vorstellung, dass die bloße anwaltliche Inanspruchnahme den Betroffenen dazu führen wird, zur Erledigung der Sache und zur Vermeidung von Weiterungen, insbesondere der etwa folgenden gerichtli-

¹¹³⁸ Vgl. Weidert/Molle in *Ensthaler/Weidert*, S. 479; Spindler in *Spindler/Schuster* § 97 Rn. 55.

¹¹³⁹ BGH GRUR 2001, 329 – *Gemeinkostenanteil*; BGH GRUR 2007, 433 – *Steckverbindergehäuse*; für das Urheberrecht s. BGH GRUR 2007, 433 – *Steckverbindergehäuse*; BGH NJW 2009, 3729 – *Tripp-Trapp*. Vgl. Vinck in *Loewenheim* § 81 Rn. 47; Spindler in *Spindler/Schuster* § 97 Rn. 55.

¹¹⁴⁰ BGH GRUR 2001, 331 – *Gemeinkostenanteil*; BGH GRUR 2002, 535 – *Unikatrahmen*.

¹¹⁴¹ BGH GRUR 1987, 39 – *Videolizenzvertrag*. Vgl. Vinck in *Loewenheim* § 81 Rn. 47; von Wolff in *Wandtke/Bullinger* § 97 Rn. 67.

¹¹⁴² BGHZ 59, 291 – *Doppelte Tarifgebühr*; BGH GRUR 1987, 39 – *Videolizenzvertrag*; BGH GRUR 1990, 1009 – *Lizenzanalogie*.

¹¹⁴³ BGH GRUR 1990, 1009 – *Lizenzanalogie*; BGHZ 60, 211 – *Miss Petite*.

¹¹⁴⁴ Vgl. Nordemann in *Fromm/Nordemann* § 97 Rn. 92.

¹¹⁴⁵ BGH GRUR 1993, 899 – *Dia-Duplikate*; BGH GRUR 1990, 353 ff. – *Raubkopien*; BGH GRUR 1990, 1009 – *Lizenzanalogie*.

¹¹⁴⁶ BGHZ 59, 292 – *Doppelte Tarifgebühr*; LG München GRUR 2005, 576 – *O Fortuna*. Vgl. zu Tarifwerken; von Wolff in *Wandtke/Bullinger* § 97 Rn. 75; Vinck in *Loewenheim* § 81 Rn. 45.

¹¹⁴⁷ von Wolff in *Wandtke/Bullinger* § 97 Rn. 75; Weidert/Molle in *Ensthaler/Weidert*, S. 483.

¹¹⁴⁸ Vgl. Vinck in *Loewenheim* § 81 Rn. 45; Weidert/Molle in *Ensthaler/Weidert*, S. 484.

chen Inanspruchnahme, auch einen überzogenen Betrag zu bezahlen. Einige Verletzer zahlen die überzogenen Gebühren, entweder, weil sie die Angemessenheit der Lizenzgebührenforderung nicht beurteilen können oder (auch) weil sie befürchten, dass eine Auseinandersetzung und die damit verbundene Herstellung der Öffentlichkeit, jedenfalls innerhalb der Familie oder des sozialen Bezugskreises, für die Wahrnehmung bzw. den Ruf der Person schädlich ist.

Der Gesetzgeber hat im Zuge der Umsetzung der Enforcement-Richtlinie von der Festlegung eines allgemeinen Verletzerzuschlags abgesehen. Auch nach der Rechtsprechung des Bundesgerichtshofes gibt es einen solchen Zuschlag nicht.¹¹⁴⁹ Ausnahmsweise wird im deutschen Recht der GEMA ein 100%iger Tarifaufschlag zugebilligt, da sie einen aufwendigen und kostspieligen Rechteüberwachungsapparat aufrechtzuerhalten hat.¹¹⁵⁰ Eine Ausdehnung der GEMA-Rechtsprechung auf die Geltendmachung von Urheberrechtsverletzungen durch Verwertungsgesellschaften wurde abgelehnt.¹¹⁵¹

Der Rechteinhaber kann gemäß § 97 Abs. 2 Satz 4 UrhG auch den **immateriellen Schaden** ersetzt verlangen, sofern er in seinen Urheberpersönlichkeitsrechten¹¹⁵² verletzt ist. Nach der Rechtsprechung des Bundesgerichtshofes muss bei der Verletzung von Urheberpersönlichkeitsrechten zwischen dem Schutz vermögenswerter Interessen und dem Schutz ideeller Interessen unterschieden werden.¹¹⁵³ Auch eine Schadensersatzpflicht besteht bei der Verletzung vermögenswerter Interessen des Persönlichkeitsrechts, wenn sie erst nach dem Tod des Rechteinhabers entstanden sind. Bei Vermögensschäden richten sich diese Ansprüche nach § 97 Abs. 1 Satz 1 UrhG. Bei der Verletzung rein ideeller Interessen kommt eine Geldentschädigung in Betracht, wenn und soweit dies der Billigkeit entspricht.¹¹⁵⁴ Maßgeblich für die Höhe der Entschädigung ist die Schwere der Rechtsverletzung und der Grad des Verschuldens. Ein Ausgleich immaterieller Schäden durch Geldentschädigung setzt eine schwerwiegende und nachhaltige Verletzung des Urheberpersönlichkeitsrechts voraus,¹¹⁵⁵ die nicht in anderer Weise befriedigend ausgeglichen werden kann.¹¹⁵⁶

7. Abmahnung

Bei Urheberrechtsverletzungen soll vor der gerichtlichen Geltendmachung von Ansprüchen eine Abmahnung erfolgen; diese wird seit 1.9.2008 in § 97a UrhG ausdrücklich geregelt. Zweck der Abmahnung ist es, den Verletzer auf sein rechtsverletzendes Verhalten

¹¹⁴⁹ BGHZ 59, 291 ff. – *Doppelte Tarifgebühr*; BGH GRUR 1990, 355 – *Raubkopien*; BGHZ 97, 49 ff. – *Filmmusik*.

¹¹⁵⁰ BGHZ 59, 286 – *Doppelte Tarifgebühr*; BGHZ 17, 383 – *Betriebsferien*. Vgl. Spindler in Spindler/Schuster § 97 Rn. 50; Dreier in Dreier/Schulze § 97, Rn. 71.

¹¹⁵¹ BGH GRUR 1990, 355 – *Raubkopien*; BGH GRUR 1966, 572 – *Eisrevue III*. Vgl. von Wolff in Wandtke/Bullinger § 97 Rn. 78 ff.; Spindler in Spindler/Schuster § 97 Rn. 52 ff.

¹¹⁵² Umstritten ist, ob auch die Verletzung von Verwertungsrechte zu einem immateriellen Schadensersatz führen kann. So Schack § 21 Rn. 785; a.A. Nordemann in Fromm/Nordemann § 97 Rn. 119.

¹¹⁵³ BGH GRUR 2000, 712 ff. – *Marlene Dietrich*.

¹¹⁵⁴ Vgl. Weidert/Molle in Ensthaler/Weidert, S. 487; Dreier in Dreier/Schulze § 97 Rn.75.

¹¹⁵⁵ BGH GRUR1971, 525 – *Petit Jaqueline*. Vgl. Dreier in Dreier/Schulze § 97 Rn.75.

¹¹⁵⁶ BGHZ 128, 12 ff. – *Caroline von Monaco*.

aufmerksam zu machen und ihn vor einem Gerichtsverfahren zu warnen. Darüber hinaus wird bezweckt, einen kostspieligen Prozess zu vermeiden. Eine Pflicht zur außergerichtlichen Abmahnung besteht nicht;¹¹⁵⁷ andernfalls riskiert jedoch der Rechteinhaber die Kostentragung bei sofortigem Anerkenntnis des Verletzers.

a. Anforderungen an die Abmahnung

In der Abmahnung wird zur Vermeidung gerichtlicher Schritte unter Fristsetzung die Abgabe einer strafbewehrten Unterlassungserklärung gefordert. Die Abmahnung muss die Darstellung der tatsächlichen Umstände, Angaben zur Aktivlegitimation sowie zum in Anspruch Genommenen enthalten. Eine besondere Form für die Abmahnung ist nicht erforderlich, kann aber in Bezug auf die Beweiserbringung eine Rolle spielen. Zugang ist zu bewirken; nach der Rechtsprechung des Bundesgerichtshofes muss der Abgemahnte beweisen, dass ihm die Abmahnung nicht zugegangen ist, wenn der Abmahnende substantiiert darlegt und beweist, dass er diese gesandt hat.¹¹⁵⁸

Für die Abgabe der Unterlassungserklärung ist dem Verletzer eine angemessene Frist zu setzen. Die Angemessenheit ist für jeden Einzelfall gesondert zu prüfen.¹¹⁵⁹ Setzt der Abmahnende eine zu kurze Frist, wird durch die Abmahnung eine angemessene Frist in Lauf gesetzt.¹¹⁶⁰

Entbehrlich ist eine Abmahnung, wenn sie dem Rechteinhaber unzumutbar ist, insbesondere wenn ohne einstweiligen Rechtsschutz zu befürchten ist, dass Beweisstücke vernichtet werden oder die Rechtsverletzung nicht verhindert werden kann.¹¹⁶¹ Auf eine Abmahnung kann verzichtet werden, wenn der Verletzer sich seiner Handlung berührt oder schon ein gleichartiger Verstoß ohne Erfolg abgemahnt wurde.¹¹⁶²

b. Rechtsmissbräuchlichkeit der Abmahnung

Angesichts der Geltendmachung von Urheberrechtsverletzungen im Internet durch Anti-Piracy-Unternehmen (Abmahndienstleistungsunternehmen) oder spezialisierte Anwaltskanzleien, die im Auftrag von Rechteinhabern, gleichsam in maschineller Form, parallel eine fünf- bis sechsstellige Zahl von Fällen bearbeiten, verbunden oft mit Gebührenforderungen, die erheblich waren bzw. sind, stellt sich die Frage, ob bei massenhaften Durchführungen von Abmahnungen ein rechtsmissbräuchliches Verhalten vorliegt.¹¹⁶³

Teilweise wird vertreten, dass Anti-Piracy-Unternehmen, die zur Verwertung urheberrechtlich geschützter Werke in Internetausgabebörsen ermächtigt wurden, kein eigenes Recht auf

¹¹⁵⁷ Vgl. Kefferpütz in Wandtke/Bullinger §97a Rn. 2; Dreier in Dreier/Schulze § 97a Rn. 4.

¹¹⁵⁸ BGH GRUR 2007, 630 – Zugang des Abmahnschreibens. Vgl. Kefferpütz in Wandtke/Bullinger §97a Rn. 13 ff.

¹¹⁵⁹ Kefferpütz in Wandtke/Bullinger §97a Rn. 9; Möllmann/Bießmann in Schwartmann, S. 1285.

¹¹⁶⁰ Vgl. Kefferpütz in Wandtke/Bullinger §97a Rn. 9; Dreier in Dreier/Schulze § 97a Rn. 7.

¹¹⁶¹ OLG Hamburg GRUR-RR 2007, 29 – Cerebro-Card. Vgl. Dreier in Dreier/Schulze § 97a Rn. 4; Kefferpütz in Wandtke/Bullinger § 97a Rn. 4.

¹¹⁶² Vgl. Dreier in Dreier/Schulze § 97a Rn. 4. Weitere Fälle bei Kefferpütz in Wandtke/Bullinger §97a Rn. 3ff.

¹¹⁶³ Vgl. Solmecke/Dierking MMR 2009, 727 ff.

Abmahnung zukommt. Ein ausschließliches Nutzungsrecht auf der Grundlage eines Verwertungsrechts allein in Internettauschbörsen kann auf dinglicher Ebene nicht eingeräumt werden, da das Recht auf Zugänglichmachung in Internettauschbörsen keine eigenständige Nutzungsart im Sinne von § 31 Abs. 1 UrhG darstellt. Aus dem Recht auf Zugänglichmachung lässt sich also kein eigener Anspruch der Abmahndienstleistungsunternehmen gegenüber Dritten herleiten.¹¹⁶⁴

In der Rechtsprechung wurden Indizien entwickelt, die für eine Rechtsmissbräuchlichkeit der Abmahnung sprechen.¹¹⁶⁵ Die Ausübung eines Rechts kann im Einzelfall unzulässig sein, wenn der Abmahnende kein schutzwürdiges eigenes Interesse verfolgt. Werden mit den Massenabmahnungen nur formal bestehende Rechte verfolgt und bestehen keine ausreichenden wirtschaftlichen und ideellen Interessen des Abmahnenden, ist von einer rechtsmissbräuchlichen Abmahnung auszugehen.¹¹⁶⁶ Die reine Anzahl der Geltendmachung gleichgearteter Ansprüche stellt jedoch noch kein zwingendes Indiz für einen Rechtsmissbrauch dar, besonders wenn die Abmahnung – wie es bei der Rechtsverletzung in Internettauschbörsen in der Regel der Fall ist – nicht identische, sondern nur gleichartige Rechtsverletzungen verfolgen.¹¹⁶⁷ Nach der Rechtsprechung des Bundesgerichtshofes dürfen massenhafte Rechtsverletzungen auch im Wege eines massenhaften Verfahrens verfolgt werden.¹¹⁶⁸ Massenhafte Abmahnungen sind als solche nicht missbräuchlich, so dass eine Erstellung einer Vielzahl ähnlicher Abmahnschreiben mit Textbausteinen nicht zum Rechtsmissbrauch führt.¹¹⁶⁹

Ein Missbrauch wird hingegen angenommen, wenn das Gebührenerzielungsinteresse im Vordergrund steht.¹¹⁷⁰ Dies ist insbesondere der Fall, etwa wenn die Abmahntätigkeit wesentlich umfangreicher ist, als die nur zum Schein geführte Geschäftstätigkeit¹¹⁷¹, wenn der Abmahnende an den Gebühreneinkünften seines Anwalts mitverdient¹¹⁷² oder wenn der Abmahnende in keinem einzigen Fall (oder nur in sehr wenigen Fällen) versucht seine Ansprüche gerichtlich durchzusetzen.¹¹⁷³

Ferner kann ein Missbrauch auch wegen **übermäßiger Kostenbelastung des Abgemahnten** entstehen, wobei die Kostenbelastung in einfach gelagerten Fällen außerhalb des geschäftlichen Verkehrs bereits durch die Begrenzung auf einen Kostenersatz i.H.v. 100 Euro begrenzt wurde, § 97 Abs. 2 UrhG. Es nimmt aber nicht Wunder, dass diese Kostenbegrenzung insbesondere aufgrund der Vielzahl der Abmahnungen wegen Urheberrechtsverletzungen im Internet notwendig war. Als ein Indiz für Rechtsmissbrauch werden z.B.

¹¹⁶⁴ Vgl. dazu ausführlich *Adolphsen/Mayer/Möller* NJOZ 2010, 2395 ff.

¹¹⁶⁵ Zu den Indizien *Solmecke/Dierking* MMR 2009, 728 ff.

¹¹⁶⁶ Vgl. *Nümann/Mayer* ZUM 2010, 328; *Kefferpütz* in *Wandtke/Bullinger* §97a Rn. 19.

¹¹⁶⁷ *LG München I* MMR 2008, 856; *OLG Köln* GRUR-RR 2006, 204.

¹¹⁶⁸ *BGH* ZUM 2008, 781.

¹¹⁶⁹ Vgl. *LG-Köln* ZUM-RD 2006, 197; *Nordemann* in *Fromm/Nordeman* § 97 Rn. 190.

¹¹⁷⁰ So *Nordemann* in *Fromm/Nordeman* § 97 Rn. 191.

¹¹⁷¹ *OLG München* NJW-RR 1986, 599.

¹¹⁷² *Nordemann* in *Fromm/Nordeman* § 97 Rn. 191.

¹¹⁷³ *BGH* GRUR 1999, 1118.

getrennte Abmahnungen gegen verschiedene Verletzer angesehen, wenn die Verletzten miteinander verbunden sind.¹¹⁷⁴ Dies ist etwa der Fall, wenn konzernverbundene Unternehmen, unter Einschaltung desselben Anwalts, getrennt vorgehen, obwohl eine gemeinsame Klage mit keinerlei Nachteilen verbunden wäre.¹¹⁷⁵

c. Reaktionsmöglichkeiten des Abgemahnten

Nur auf eine berechtigte Abmahnung braucht der Abgemahnte zu reagieren. Berechtigt ist eine Abmahnung, wenn sie erforderlich ist, um dem Abgemahnten die Möglichkeit für die außergerichtliche und damit kostengünstige Lösung des Konflikts aufzuzeigen.¹¹⁷⁶

Bei einer berechtigten Abmahnung muss der Abgemahnte, will er die Wiederholungsfahr beseitigen, eine unbedingte und unbefristete strafbewehrte Unterlassungserklärung abgeben. Dagegen reicht bei einer Erstbegehungsgefahr die ernsthafte Erklärung aus, die rechtsverletzende Handlung nicht zu begehen.

Für den Fall eines Verstoßes gegen die Unterlassungserklärung hat der Abgemahnte eine Vertragsstrafe zu zahlen. Sie muss so hoch bemessen sein, dass sie den Verletzer davon abhält, die Verletzung fortzusetzen oder zu wiederholen. In Bezug auf die Höhe sind die Umstände des Einzelfalls entscheidend.

Bisweilen werden Abmahnungen deutlich weiter gefasst, als der konkret nachgewiesene Vorwurf reicht. So kann es sein, dass bei einem Nachweis (oder scheinbaren Nachweis) des Herunterladens verschiedener Musiktitel eines Interpreten der Rechteinhaber gleichsam vorgreiflich weitere Titel des Interpreten oder gar von weiteren von ihm vertretenen Interpreten in die Unterlassungsverpflichtungserklärung einbezieht oder Handlungen, die der Betroffene nicht begangen hat, aber begehen könnte. In diesen Fällen ist der Abgemahnte nicht verpflichtet, die Unterlassungsverpflichtungserklärung in der abgeforderten Form abzugeben, sondern sollte sie entsprechend beschränken. Teilweise wird jedoch eine weite Unterlassungserklärung für wirksam gehalten, in der sich der Verletzer nicht nur dazu verpflichtet, künftig keine Werke des abmahnenen Rechteinhabers mehr öffentlich zugänglich zu machen, sondern auch das öffentliche Zugänglichmachen sämtlicher Werke weiterer Rechteinhaber zu unterlassen.¹¹⁷⁷ Gibt der Abgemahnte nur eine beschränkte Unterlassungsverpflichtungserklärung i.S.e. zu stark beschränkten Unterlassungsverpflichtungserklärung ab, riskiert er in der Regel, dass diese zu einer nur bedingten Verpflichtung führt, was die Wiederholungs- und Erstbegehungsgefahr nicht entfallen lässt. Es besteht

¹¹⁷⁴ BGH GRUR 2006, 243 – *Mega Sale*, zum UWG, auf dessen Grundsätze für den Bereich des Urheberrechts zurückgegriffen werden kann. Vgl. Nordemann in *Fromm/Nordeman* § 97 Rn. 192.

¹¹⁷⁵ BGH GRUR 2000, 1091 – *Missbräuchliche Mehrfachverfolgung* zum UWG. Vgl auch *Solmecke/Dierking* MMR 2009, 729.

¹¹⁷⁶ *Dreier* in *Dreier/Schulze* § 97a Rn. 8.

¹¹⁷⁷ *OLG Köln* MMR 2011, 37 ff. Dazu vgl. *Raue* MMR 2011, S. 292 ff. Anderes gilt jedoch, wenn Zweifel an der Ernsthaftigkeit der abgegebenen Unterlassungserklärung bestehen können (*Spindler* in *Spindler/Schuster* § 97a Rn. 8.).

damit das Risiko, dass gegen den Abgemahnten eine einstweilige Verfügung erlassen wird.¹¹⁷⁸

Hat der Verletzer bereits einem anderen gegenüber eine Unterlassungserklärung abgegeben, ist eine Abmahnung nicht mehr erforderlich, da diese eine Wiederholungsgefahr auch gegenüber dem Verletzten ausräumt.¹¹⁷⁹

Bei einer unberechtigten Abmahnung braucht der Abgemahnte nicht zu antworten. Jedoch wird in der Praxis empfohlen, Schutzschriften bei den zuständigen Gerichten zu hinterlegen, um sich gegen etwaige Anträge des Abmahnenden auf einstweiligen Rechtsschutz zu schützen.¹¹⁸⁰ Der zu Unrecht Abgemahnte hat einen Anspruch auf Ersatz der Kosten, die ihm durch die unberechtigte Abmahnung entstanden sind, dies jedoch nur dann, wenn der Antrag auf einstweilige Verfügung nicht schon vor Einreichung der Schutzschrift zurückgenommen wurde.¹¹⁸¹ In Betracht kommen auch Gegenabmahnung und negative Feststellungsklage. Der unberechtigt Abgemahnte muss seinerseits den Abmahnenden im Fall der Erhebung einer negativen Feststellungsklage nicht vorher abmahnen.¹¹⁸² Der Abgemahnte hat die Kosten einer zweiten Abmahnung nicht zu tragen, wenn schon in der ersten Abmahnung die Aufforderung zur strafbewehrten Unterlassungserklärung enthalten ist.¹¹⁸³

Dem Verletzer kann aus dem durch die Urheberrechtsverletzung entstandenen Schuldverhältnis eine Aufklärungspflicht gegenüber dem Verletzten nach Treu und Glauben zukommen. Der Abgemahnte muss dem Abmahnenden vor allem die Abgabe einer Unterlassungserklärung gegenüber Dritten aufzeigen, die auch dem Abmahnenden gegenüber die Wiederholungsgefahr ausräumt.¹¹⁸⁴

In der Praxis beanstanden Betroffene insbesondere (auch) die technische bzw. fachliche Zuverlässigkeit des Verfahrens, mit dem der Rechteinhaber die IP-Adresse des Anschlussinhabers, von dessen Anschluss aus Rechtsverletzungen begangen worden sein sollen, ermittelt und beim Zugangsanbieter auf der Basis der IP-Adresse den Namen des (vermeintlichen) Verletzers erfahren hat (§ 101 Abs. 2 und 9 UrhG). Dem steht wohl auch die Bundesgerichtshof-Entscheidung „Sommer unseres Lebens“ nicht ausnahmslos entgegen, denn in dem vom Bundesgerichtshof entschiedenen Fall war das Bestreiten des Anschlussinhabers im Hinblick auf die Zuverlässigkeit der Ermittlungssoftware lediglich als zu unbe-

¹¹⁷⁸ Vgl. Möllmann/Bießmann in Schwartmann, S. 1286, die für ratsam halten, dass der Abgemahnte seine Erklärung äußerst sorgfältig formuliert.

¹¹⁷⁹ Dreier in Dreier/Schulze § 97a Rn. 8; Spindler in Spindler/Schuster § 97a Rn. 8.

¹¹⁸⁰ Spindler in Spindler/Schuster § 97a Rn. 10; LG Stuttgart MMR 2008, 64 für Filesharing.

¹¹⁸¹ Spindler in Spindler/Schuster § 97a Rn. 10.

¹¹⁸² BGH GRUR 2004, 792 – Gegenabmahnung; BGH GRUR 2006, 168.

¹¹⁸³ BGH GRUR 2010, 355.

¹¹⁸⁴ Spindler in Spindler/Schuster § 97a Rn. 11; Kefferpütz in Wandtke/Bullinger §97a Rn. 16 ff.

stimmt angesehen worden¹¹⁸⁵, was offen lässt, dass es ein hinreichend substantiiertes Bestreiten geben kann¹¹⁸⁶.

d. Ersatz von Abmahnkosten

Bei Abmahnung im Fall der Urheberrechtsverletzungen sieht § 97a Abs. 1 Satz 2 UrhG einen Anspruch des Verletzten auf Aufwendungsersatz bei einer berechtigten Abmahnung vor. Darüber hinaus können nur die für die Abmahnung erforderlichen Aufwendungen geltend gemacht werden. Als erforderlich werden die für eine Abmahnung entstandenen Rechtsanwaltskosten angesehen, wenn der Verletzte nicht über entsprechende Rechtskenntnisse verfügt¹¹⁸⁷. Dies gilt auch für Unternehmen mit eigener Rechtsabteilung ohne urheberrechtliche Kenntnisse.¹¹⁸⁸

Die Pflicht zur Erstattung von Rechtsanwaltskosten kann nach § 97a Abs. 2 UrhG auf 100 Euro begrenzt sein. Damit will der Gesetzgeber Privatpersonen, die Urheberrechtsverletzungen begangen haben, davor bewahren, dass sie in Bagatellfällen als überzogen empfundene Anwaltshonorare bezahlen müssen.¹¹⁸⁹ Wären solche überzogenen Forderungen nicht in der Praxis massenweise gestellt worden, hätte der Gesetzgeber hier nicht bereits eingreifen müssen. Im Hintergrund steht, dass bei Urheberrechtsverletzungen im Internet, etwa in Internetaustauschbörsen, durch Rechtsanwälte Massenabmahnungen durchgeführt und dafür zum Teil nicht unerhebliche Anwaltsgebühren geltend gemacht wurden¹¹⁹⁰. Da bei Urheberrechtsverletzungen in Internetaustauschbörsen durch die Gerichte recht erhebliche Streitwerte festgestellt werden¹¹⁹¹, sahen sich die Abgemahnten erheblichen Kosten in Form von Schadensersatz oder Abmahnkosten ausgesetzt.

¹¹⁸⁵ BGH a.a.O. Tz. 27: „Der Beklagte hat zwar bestritten, dass die Klägerin korrekt an seine IP-Adresse gelangt sei, und geltend gemacht, bei der Feststellung der IP-Adresse des wirklichen Täters müsse ein Ermittlungsfehler unterlaufen sein. Nach den vom Berufungsgericht in Bezug genommenen Feststellungen des Landgerichts hat die L. AG aber die fragliche IP-Adresse mit Hilfe der von ihr entwickelten zuverlässigen und eingehend überwachten Software ermittelt. Nachdem das Landgericht das pauschale Bestreiten des Beklagten als zu unbestimmt angesehen hatte und der Beklagte seinen Vortrag in zweiter Instanz nicht weiter substantiiert hat, konnte das Berufungsgericht insoweit ohne Rechtsfehler auf die Feststellungen des Landgerichts verweisen.“

¹¹⁸⁶ S. z.B. OLG München Beschluss v. 27.9.2010 – 11 W 1894/10, MIR-DokNr. 148-2010, zur Zuverlässigkeit der Erzeugung eindeutiger Hashwerte.

¹¹⁸⁷ BGH GRUR 2004, 789 – *Selbstauftrag*.

¹¹⁸⁸ LG Köln ZUM-RD 2007, 597 ff. Anderes gilt, wenn das Unternehmen über eigenes Rechtsabteilung verfügt, die mit den Rechtsverletzungen im Bereich des Urheberrechts vertraut ist; BGH GRUR 1984, 691 – *Anwaltsabmahnung*; BGH MMR 2008, 737 – *Abmahnkostenersatz*. A.A. Nordemann in *Fromm/Nordemann* § 97a Rn. 26.

¹¹⁸⁹ Vgl. amtliche Begründung BT-Drucksache 16/5048, S. 48.

¹¹⁹⁰ So versteigert zum Zeitpunkt der Fertigstellung der Studie eine Kanzlei mit Sitz im süddeutschen Raum (Urmann + Kollegen, <http://auktion.urmann.com/> [abgerufen am 10.12.2011]) Gebühren einschl. Schadensersatzbeträgen i.H.v. EUR 90 Mio. die aus 70.000 Urheberrechtsverletzungsfällen im Bereich des „adult entertainment“ stammen sollen. Damit ergibt sich ein Durchschnittswert von knapp EUR 1.300 pro Abmahnung, wohl als Summe von Anwaltsgebühren und Lizenzgebühren. Folgt man der Auffassung, dass das Herunterladen eines ganzen Albums oder eines Films keine „unerhebliche Rechtsverletzung“ i.S.d. § 97a Abs. 2 UrhG ist (vgl. LG Köln ZUM-RD 2010, 481. Vgl. auch Dreier in *Dreier/Schulze* § 97a Rn. 17), sind die Gebühren ggf. nicht von vornherein überzogen.

¹¹⁹¹ In der Regel setzen die Gerichte pro Musiktitel einen Streitwert von 10.000 Euro fest. Vgl. LG Köln MMR 2008, 126 ff.; OLG Düsseldorf abrufbar unter:

http://www.justiz.nrw.de/nrwe/olgs/duesseldorf/j2007/1_20_W_113_06beschluss20070213.html (Stand

Die Begrenzung auf 100 Euro einschl. Steuern und Auslagen kommt nur in Betracht¹¹⁹², wenn es sich um eine **erstmalige** Abmahnung handelt, ein **einfach** gelagerter Fall vorliegt und eine **unerhebliche** Rechtsverletzung **außerhalb des geschäftlichen Verkehrs** vorliegt.¹¹⁹³

- Ersteres beurteilt sich aus Sicht des Verletzten. Problematisch sind die Fälle, in denen mehrere Rechtsverletzungen zu Lasten mehrerer Rechteinhaber begangen werden, wie der Upload mehrerer Musiktitel unterschiedlicher Rechteinhaber über eine Internetausbörse.
- Ein einfach gelagerter Fall liegt bei so genannten Routinefällen vor, die von Anwälten und Gerichten ohne größeren Arbeitsaufwand beurteilbar sind.¹¹⁹⁴ Nach einer Auffassung sind Urheberrechtsverletzungen über Internetausbörsen niemals ein einfach gelagerter Fall,¹¹⁹⁵ weil die Ermittlung des hinter einer IP-Adresse stehenden Verletzers durch die Einschaltung eines Anti-Piracy-Unternehmens und die Durchführung eines Auskunftserteilungsverfahrens nach § 101 Abs. 9 UrhG erfolgt (und die entsprechenden Kosten einschließen soll). Nach einer anderen Auffassung sollte der eingeführte Auskunftsanspruch nach § 101 UrhG den Aufwand für die Ermittlung des Nutzers gerade vereinfachen, weshalb auch in rechtlicher Hinsicht i.d.R. nicht mehr von einem größeren Bearbeitungsumfang ausgegangen werden soll. Schließlich könnten die Abmahnenden bei immer gleichen Rechtsverletzungen weitgehend auf standardisierte Schreiben zurückgreifen.¹¹⁹⁶
- Die Unerheblichkeit der Rechtsverletzung beurteilt sich sowohl nach qualitativen als auch nach quantitativen Merkmalen.¹¹⁹⁷ Es muss sich um Bagatelverstöße handeln¹¹⁹⁸, z.B., wenn ein Stadtplanausschnitt auf der eigenen Website öffentlich zugänglich gemacht oder ein Lichtbild innerhalb einer Internetauktion verwendet wurde.¹¹⁹⁹ Der erstmalige Download eines einzelnen Musikstücks im Wege der Internetausbörsen kann noch als unerhebliche Rechtsverletzung angesehen werden.¹²⁰⁰ Anders liegt das öffentliche Zugänglichmachen ganzer Musikalben oder Filme.¹²⁰¹ Eine unerhebliche Rechtsverletzung liegt nach Ansicht des *AG München* beim Upload eines Hörbuchs

November 2011). Für weitere Entscheidungen und abweichende Streitwerte vgl. *Waldhausen in Schwartmann* S. 1249 ff. Kritisch zu den überhöhten Streitwerten *Dreier in Dreier/Schulze* § 97a Rn. 2.

¹¹⁹² Vgl. *Ewert/Hartz* MMR 2009, S. 85 ff.; ausführlich dazu *Malkus* MMR 2010, 383 ff.; *Tyra* ZUM 2009, S. 935 ff.

¹¹⁹³ Dazu *Ewert/Hartz* MMR 2009, S. 86 ff.

¹¹⁹⁴ Vgl. amtliche Begründung BT-Drucksache 16/5048, S. 49. Widerspricht der Abgemahnte der Abmahnung, ist nicht mehr von einem einfach gelagerten Fall auszugehen, s. *Nordemann in Fromm/Nordemann* § 97a Rn. 32.

¹¹⁹⁵ Vgl. *Nümann/Mayer* ZUM 2010, 324.

¹¹⁹⁶ So *Faustmann/Ramsperger* MMR 2010, 664.

¹¹⁹⁷ Ausführlich zu den Kriterien *Malkus* MMR 2010, 386 ff.

¹¹⁹⁸ Vgl. amtliche Begründung BT-Drucksache 16/5048, S. 48; *Dreier in Dreier/Schulze* § 97a Rn. 17.

¹¹⁹⁹ Vgl. amtliche Begründung BT-Drucksache 16/5048, S. 50. Die Unerheblichkeit der Rechtsverletzung beim Verwenden eines Lichtbildes innerhalb einer Onlineauktion ist in der Rechtsprechung bestätigt. Vgl. *OLG Brandenburg* MMR 2009, 258.

¹²⁰⁰ *AG Frankfurt a.M.* Urteil von 1.2.2010, Az. 30 C 2353/09-75, BeckRS 2010, 12644.

¹²⁰¹ *LG Köln* ZUM-RD 2010, 481. Vgl. auch *Dreier in Dreier/Schulze* § 97a Rn. 17.

über Filesharing nicht vor, da durch das Anbieten auf einer solchen Plattform mehrere 100.000 Nutzer auf das Werk zugreifen können¹²⁰². Als Quintessenz gilt wiederum, dass die Frage der Unerheblichkeit der Rechtsverletzung im Einzelfall zu betrachten ist.¹²⁰³

- Die Verletzungshandlung muss weiterhin außerhalb des geschäftlichen Verkehrs erfolgen. Ein Handeln im geschäftlichen Verkehr liegt vor, wenn die Tätigkeit auf einen wirtschaftlichen Vorteil gerichtet ist und nicht im privaten Bereich erfolgt.¹²⁰⁴ Bei Urheberrechtsverletzungen in Internettauschbörsen wird i.d.R. von einem Handeln außerhalb des geschäftlichen Verkehrs auszugehen sein,¹²⁰⁵ jedoch kann es ungeachtet dessen am vorangehenden Merkmal der Unerheblichkeit der Rechtsverletzung fehlen. Die Beweislast für das Vorliegen der Voraussetzungen des §97a UrhG liegt bei der Person, die sich auf die Beschränkung beruft, d.h. beim Verletzer.¹²⁰⁶

Die Kosten für die Ermittlung der Rechtsverletzung, z.B. für die Ermittlung von IP-Adressen, sollen nach der Intention des Gesetzgebers nicht Bestandteil des Betrags von 100 Euro sein;¹²⁰⁷ diese können von dem Abmahnenden als Schadensersatz verlangt werden¹²⁰⁸, dessen Höhe in der Rechtsprechung unterschiedlich beurteilt wurde.¹²⁰⁹

III. Auskunftsanspruch nach deutschem Recht

1. Ausgangslage

Zur Bekämpfung von Urheberrechtsverletzungen hat der Gesetzgeber mit Wirkung ab dem 1.8.2009 in § 101 Abs. 2 und 9 UrhG einen unmittelbaren Auskunftsanspruch von Rechteinhabern gegenüber Zugangsanbietern geschaffen. Der Auskunftsanspruch soll dem Rechteinhaber ermöglichen, die Identität des Rechteinverletzers zu ermitteln und ihm gegenüber urheberrechtliche Ansprüche, insbesondere auf Unterlassung und Schadensersatz, durchzusetzen.¹²¹⁰ § 101 Abs. 2 Nr. 3 UrhG gewährt dem verletzten Rechteinhaber

¹²⁰² AG München Urteil von 11.11.2009, Az.142 C 14130/09, abrufbar unter:

<http://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=AG%20M%FCnchen&Datum=11.11.2009&Aktenzeichen=142%20C%2014130/09> (Stand November 2011). Kritisch dazu *Faustmann/Ramsperger* MMR 2010, 665.

¹²⁰³ Vgl. *Faustmann/Ramsperger* MMR 2010, 662 ff.; *Malkus* MMR 2010, 385 ff.

¹²⁰⁴ An den Begriff, der weit auszulegen ist, sind nach der Rechtsprechung des BGH keine hohen Anforderungen zu stellen. Vgl. *BGH GRUR* 2004, 860 – *Internet-Versteigerung I*.

¹²⁰⁵ Vgl. *Faustmann/Ramsperger* MMR 2010, 666.

¹²⁰⁶ *Weidert/Molle in Ensthaler/Weidert*, S. 518; *Ewert/Hartz* MMR 2009, S. 88 ff.

¹²⁰⁷ Vgl. amtliche Begründung BT-Drucksache 16/5048, S. 49. Vgl. *Dreier in Dreier/Schulze* § 97a Rn. 16.

¹²⁰⁸ Dazu *Dreier in Dreier/Schulze* § 97a Rn. 20; *Faustmann/Ramsperger* MMR 2010, 666.

¹²⁰⁹ *AG Frankfurt a.M.* MMR 2010, 262 – 150 Euro für ein einzelnes Lied; *AG München* Urteil von 11.11.2009, Az.142 C 14130/09, abrufbar unter:

<http://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=AG%20M%FCnchen&Datum=11.11.2009&Aktenzeichen=142%20C%2014130/09> (Stand November 2011) - 500 Euro für ein Hörbuch.

¹²¹⁰ Bis zum Inkrafttreten dieser Regelung gingen Rechteinhaber den Umweg über ein Strafverfahren, denn dem Rechteinhaber stand ein Anspruch auf Auskunft nur gegen den Verletzer selbst zu (§ 101a UrhG a.F.); eine analoge Anwendung auf Internet-Zugangsdiensteanbieter wurde von der Rechtsprechung überwiegend abgelehnt (Dazu ausführlich *Welp* S. 33 ff. Vgl. auch *Dreier in Dreier/Schulze* § 101 Rn. 4 mit Hinweis auf Entscheidungen der Gerichte, die überwiegend eine analoge Anwendung des § 101a UrhG a.F. abgelehnt haben. So auch *Spittgerber/Klytta* K&R 2007, S. 79 ff.) Daher leiteten Rechteinhaber gegen Verletzer Strafver-

einen Anspruch gegen den Zugangsanbieter auf Auskunft über den Namen und die Anschrift derjenigen Person, die eine Urheberrechtsverletzung unter Nutzung der Dienste begangen hat. Anknüpfungspunkt ist dabei die IP-Adresse, die i.d.R. als dynamische IP-Adresse regelmäßig bzw. bei jeder aufgebauten Internetverbindung vom Diensteanbieter neu zugewiesen wird. Nur die Zugangsanbieter können durch den Abgleich der bei ihnen gespeicherten Daten ermitteln, welchem ihrer Kunden zum Verletzungszeitpunkt die dynamische IP-Adresse zugeteilt war. Kann – wie i.d.R. – die Auskunft nur unter Verwendung von Verkehrsdaten im Sinne von § 3 Nr. 30 TKG erteilt werden, muss der Auskunftserteilung gemäß § 101 Abs. 9 UrhG eine richterliche Anordnung vorausgehen.

Die Identifizierung des Verletzers durch den Datenabgleich beim Zugangsanbieter und die Herausgabe der Daten an Dritte hat datenschutzrechtliche Implikationen, da es sich bei den relevanten Kundendaten um personenbezogene Daten im Sinne von § 3 BDSG handelt.¹²¹¹Die Zugangsanbieter bewegen sich insofern in einem Spannungsverhältnis zwischen den Datenschutzbelangen ihrer Kunden und privaten Auskunftsansprüchen der Rechteinhaber. Notwendig ist- weil es an einer Einwilligung der Kunden zur Herausgabe der Daten mangelt- ein Erlaubnistatbestand für die Übermittlung personenbezogener Daten. Nach der Intention des Gesetzgebers wird den entsprechenden datenschutz- und grundrechtlichen Bedenken dadurch Rechnung getragen, dass der Auskunftsanspruch gegen die Zugangsanbieter in § 101 Abs. 9 UrhG einem Richtervorbehalt unterstellt ist. In § 101 Abs. 10 UrhG wird zudem – entsprechend den Anforderungen des Art. 19 Abs. 2 GG - auf die Einschränkung des Rechts auf Fernmeldegeheimnis hingewiesen.

2. Voraussetzungen des Auskunftsanspruchs gegen Zugangsanbieter

§ 101 Abs. 2 UrhG gewährt einen Auskunftsanspruch gegenüber einem Dritten, der nicht selbst Verletzer einer Rechtsnorm ist. Zu den auskunftspflichtigen Personen gehören auch solche, die ausschließlich die für die rechtsverletzenden Tätigkeiten genutzten Dienstleistungen erbracht haben (Satz 1 Nr. 3). Dies sind namentlich die Zugangsanbieter, weil deren Leistung zumindest kausal für die Rechtsverletzung ist. Werden sie in Anspruch ge-

fahren wegen Verstoßes gegen §§ 106, 108 UrhG ein. Nachdem die Staatsanwaltschaft im Zuge der Ermittlungsverfahren beim Internet-Zugangsdiensteanbieter die Identität des potenziellen Verletzers ermittelt hatte, nahm der Rechteinhaber Akteneinsicht nach § 406e Abs. 1 StPO und erhielt so die gewünschten Informationen zur Durchsetzung seiner zivilrechtlichen Ansprüche (vgl. *Hoeren* NJW 2008, S. 3099). Die Strafverfolgungsbehörden sahen sich instrumentalisiert (vgl. *Hoeren* NJW 2008, S. 3100; *Konziela* MMR 2009, S. 295 ff.) und gingen dazu über, das Interesse an einer öffentlichen Klage zu verneinen und die Betroffenen auf den Privatklageweg nach § 374 Abs. 1 Nr. 8 StPO zu verweisen (vgl. *Schwippert* in *Schwartzmann*, S. 93.). Mit Einführung des direkten Auskunftsanspruchs gegenüber dem Zugangsanbieter sollte dieser Umweg über strafrechtliche Verfahren ausgeräumt werden (vgl. *Hoeren* NJW 2008, S. 3100; *Schwippert* in *Schwartzmann*, S. 93; anders *Gietl/Mantz* CR 2008, S. 813, die sich für ein Nebeneinander der beiden Auskunftsverfahren aussprechen, aber von einer Akteneinsicht nur bei erhöhtem Verdachtsmoment ausgehen; anders auch *Schmidt* GRUR 2010, S. 673 ff., nach dem eine Beschränkung der Akteneinsicht in den Filesharingverfahren bei Urheberrechtsverletzungen nicht gewerblichen Ausmaßes eine Unterminierung des Urheberrechtsschutzes zur Folge hat).

¹²¹¹ Siehe §§ 11 ff. TMG.

nommen, so haben sie Auskunft über Namen und Anschrift der Person zu erteilen, die eine Urheberrechtsverletzung durch die Nutzung ihrer Dienste begangen hat.

Wegen der Einschränkung des Fernmeldegeheimnisses (Art. 10 GG) und damit zur Wahrung des Datenschutzes ist ein Erlaubnistatbestand für die Nutzung und Übermittlung personenbezogener Daten erforderlich. In der Literatur¹²¹² und Rechtsprechung¹²¹³ wird hierfür teilweise § 101 Abs. 1, 2 und 9 UrhG herangezogen.¹²¹⁴ Da das Auskunftsverfahren unter einem Richtervorbehalt stehe, würde dies automatisch auch den datenschutzrechtlichen Aspekten Rechnung tragen. Nach einer anderen Auffassung liegt eine datenschutzrechtliche Erlaubnisnorm für die Auskunftserteilung im Rahmen des Auskunftsverfahrens gemäß § 101 Abs. 9 UrhG nicht vor, da diese Regelung den verfassungsrechtlichen Anforderungen an Bestimmtheit und Normenklarheit nicht genüge.¹²¹⁵

Einige Tatbestandsmerkmale im geltenden Recht haben sich als praxistauglich und verlässlich erwiesen, andere sind schwierig zu definieren bzw. werden von der Rechtsprechung nicht gleichförmig behandelt, womit eine nicht unerhebliche Rechtsunsicherheit einhergeht.

a. Offensichtliche Rechtsverletzung und gewerbliches Ausmaß der Zugangsvermittlung

Der Auskunftsanspruch der Rechteinhaber setzt eine **Rechtsverletzung** voraus. Diese kann alle Urheberrechte sowie entsprechende Leistungsschutzrechte oder Urheberpersönlichkeitsrechte¹²¹⁶ betreffen.

§ 101 Abs. 2 UrhG verlangt darüber hinaus, dass es sich um eine **offensichtliche Rechtsverletzung** handelt oder der Verletzte gegen den Verletzer Klage erhoben hat.¹²¹⁷ Der unbestimmte Rechtsbegriff der „offensichtlichen Rechtsverletzung“ ist auslegungsbedürftig. Zu seiner Ausfüllung können die Merkmale der Offensichtlichkeit, die für Verfahren im einstweiligen Rechtsschutz entwickelt worden sind, auf § 101 Abs. 2 UrhG übertragen werden.¹²¹⁸ Offensichtlich ist eine Rechtsverletzung danach, wenn sie so eindeutig ist, dass eine Fehlentscheidung und damit eine ungerechtfertigte Belastung des Auskunftspflichtigen kaum möglich ist. Zweifel in tatsächlicher oder rechtlicher Hinsicht schließen die

¹²¹² Vgl. Hoffmann MMR 2009, S. 656; Maaßen MMR 2009, S. 513; Welp S. 270.

¹²¹³ OLG Frankfurt a.M. MMR 2009, 542.

¹²¹⁴ Zu anderen Regelungen wie § 14 Abs. 2 und § 15 Abs. 5 Satz 4 TMG, § 113 TKG oder § 96 Abs. 1 Satz 2 TKG als datenschutzrechtliche Erlaubnisnorm für das Auskunftsverfahren vgl. Hennemann, S. 164 ff.

¹²¹⁵ So Welp S. 271 ff.; zustimmend Hennemann, S. 166 ff.

¹²¹⁶ OLG Hamburg GRUR-RR 2007, 381.

¹²¹⁷ Bei einer Klageeinreichung muss der Beklagte als der Verletzer feststehen, da nach deutschem Recht eine Klage gegen Unbekannt nicht möglich ist. Genau diese Identität des Beklagten bzw. zu Verklagenden soll aber im Auskunftsverfahren ermittelt werden. Die Alternative, wonach der Verletzte gegen den Verletzer Klage erhoben hat, kommt also bei Auskunftsansprüchen gegen Internet-Zugangsdiensteanbieter nicht zum Tragen.

¹²¹⁸ Vgl. Weidert/Molle in Ensthaler/Weidert S. 500; Welp S. 150 ff.

Offensichtlichkeit aus.¹²¹⁹ Die Offensichtlichkeit der Rechtsverletzung ist objektiv zu beurteilen, d.h. bei der Auslegung ist nicht auf die subjektiven Sichtweisen der Beteiligten (Zugangsanbieter/Rechteinhaber) abzustellen.¹²²⁰ Dass darüber hinaus auch die Person des Rechteinhabers offensichtlich ist, ist nicht erforderlich.¹²²¹

Weitere Voraussetzung ist, dass der in Anspruch Genommene die Dienstleistungen, die für die rechtsverletzende Handlung genutzt wurden, **in gewerblichem Ausmaß** erbringt, was bei Zugangsanbietern, deren Geschäftsmodell auf der Zurverfügungstellung von Anschlüssen für das Internet bzw. auf der Zugangsvermittlung beruht, außer Frage steht.

b. Gewerbliches Ausmaß der Rechtsverletzung

Nicht eindeutig ist, ob darüber hinaus auch die **Rechtsverletzung selbst ein gewerbliches Ausmaß** erreichen muss ("doppelte Gewerbsmäßigkeit"), und wenn ja, wann sich eine Rechtsverletzung gewerblichen Ausmaßes ergibt.

Der Wortlaut des § 101 Abs. 2 Nr. 3 UrhG fordert ausdrücklich nur ein gewerbliches Handeln des Dienstleisters bzw. des Zugangsanbieters. Die Begründung zum Gesetzentwurf geht hingegen ausdrücklich davon aus, dass eine Rechtsverletzung in gewerblichem Maße vorliegen muss. Jedenfalls Sinn und Zweck der Norm legen eine solche Auslegung auch nahe.¹²²² Der Bundesrat kritisierte dies im Gesetzgebungsverfahren, da das gewerbliche Ausmaß gerade bei Urheberrechtsverletzungen im Internet erst infolge der Auskunft überhaupt ermittelt werden könne.¹²²³ Die h.M. in der Rechtsprechung bezieht das Erfordernis des „gewerblichen Ausmaßes“ auch auf die Rechtsverletzung, womit nur dann eine Auskunftspflicht besteht, wenn der Verletzer selbst in gewerblichem Ausmaß gehandelt hat.¹²²⁴

Unklar ist zudem, wie der Begriff des gewerblichen Ausmaßes selbst zu verstehen ist. Einigkeit besteht darüber, dass der Begriff nicht wie im deutschen Handels- oder Gewerberecht zu verstehen ist. Da § 101 UrhG die Enforcement-Richtlinie¹²²⁵ umsetzt und richtlinienkonform auszulegen ist, ist zur Auslegung auf die dortigen Begriffsbestimmungen zurückzugreifen.¹²²⁶ Ein gewerbliches Ausmaß liegt demnach dann vor, wenn die Rechtsverletzung zwecks Erlangung eines unmittelbaren oder mittelbaren wirtschaftlichen oder kommerzi-

¹²¹⁹ So die amtliche Begründung des Regierungsentwurfs, BT-Drucks. 16/5048, 39; *OLG Hamburg*, GRUR-RR 2005, 213 – Rammstein; *LG Köln* ZUM 2005, 239. Vgl. auch *LG Hamburg* MMR 2009, 571 für § 101 Abs. 2 UrhG.

¹²²⁰ Vgl. *Spindler* ZUM 2008, S. 643.

¹²²¹ *OLG Köln* MMR 2008, 822. So auch *Musiol*, GRUR-RR 2009, S. 4.

¹²²² Vgl. amtliche Begründung des Regierungsentwurfs, BT-Drucks. 16/5048, 49 („im geschäftlichen Verkehr“). Vgl. dazu *Dreier in Dreier/Schulze* § 101 Rn. 12; *Bohne* CR 2010, S. 105.

¹²²³ BT-Drucks. 16/5048, S. 53, 59 ff.; BR-Drucks. 279/1/02, S. 3.

¹²²⁴ *OLG Oldenburg* GRUR-RR 2009, 299; *OLG Zweibrücken* MMR 2009, 43; *OLG Frankfurt a.M.* MMR 2009, 542. So auch *Musiol*, GRUR-RR 2009, S. 3. Anders *LG Bielefeld* MMR 2009, 70; *Schwarz/Brauneck* ZUM 2006, S. 704 ff.; *Bohne*, CR 2010, S. 106 ff., der sich gegen ein gewerbliches Ausmaß der Rechtsverletzung ausspricht. So auch *Hennemann*, S. 155.

¹²²⁵ Richtlinie 2004/48/EG vom 29.4.2004 zur Durchsetzung der Rechte des geistigen Eigentums (Enforcement-Richtlinie), ABl. EU Nr. L 195 v 2.6.2004, S. 16 ff.

¹²²⁶ *Musiol*, GRUR-RR 2009, S. 3.

ellen Vorteils vorgenommen wird.¹²²⁷ Der wirtschaftliche Vorteil beim öffentlichen Zugänglichmachen von Werken im Rahmen von Internettauschbörsen liegt in den ersparten Aufwendungen, da das legale Herunterladen eines urheberrechtlich geschützten Werks i.d.R. nur gegen Entgelt erfolgen kann.¹²²⁸ Während die Richtlinie das Merkmal des gewerblichen Ausmaßes subjektiv verstand, stellt § 101 UrhG auf objektive Kriterien ab. Ein gewerbliches Ausmaß soll sich nach § 101 Abs. 1 Satz 2 UrhG sowohl aus der Anzahl als auch aus der Schwere der Rechtsverletzung(en) ergeben.

Das Kriterium der Anzahl der Rechtsverletzungen scheint bei Urheberrechtverletzungen in Internet jedoch von vornherein verfehlt, da sich **vor** der Auskunftserteilung einem Nutzer mehrere Verletzungshandlungen in der Regel nicht zuordnen lassen, es sei denn, man würde bei Herunterladen eines Musikalbums mit mehreren Titeln je Titel eine eigenständige Rechtsverletzung annehmen. Jedenfalls ein einmaliges öffentliches Zugänglichmachen eines einzelnen Musiktitels kann ein Handeln in gewerblichem Ausmaß über die Anzahl nicht begründen.¹²²⁹

Damit kommt der Schwere der Rechtsverletzung entscheidende Bedeutung zu, wobei es hierzu in der untergerichtlichen Rechtsprechung keine einheitliche Ansicht gibt. Ein gewerbliches Ausmaß kann vorliegen, wenn ein vollständiges Musikalbum vor oder unmittelbar nach der Veröffentlichung in Deutschland, wenn auch nur einmalig, öffentlich zugänglich gemacht wird.¹²³⁰ Andere Gerichte sehen einen einmaligen Download eines Albums nicht als Verletzung im gewerblichen Ausmaß an.¹²³¹ Maßgeblich für das Vorliegen eines gewerblichen Ausmaßes soll vielmehr sein, wenn anhand der Platzierungen der Titel in den Verkaufsstatistiken eine hohe kommerzielle Nachfrage an dem urheberrechtlich geschützten Werk besteht.¹²³² Eine ausreichende Schwere der Rechtsverletzung soll einer Ansicht nach gegeben sein, wenn das geschützte Werk innerhalb einer Verkaufs- oder Verwertungsphase von bis zu sechs Monaten nach der Veröffentlichung in einer Internettauschbörse angeboten wird. Nach Ablauf dieser Frist sollen besondere Umstände vorliegen müssen, wenn ein Fortdauern der relevanten Verwertungsphase und damit eine Rechtsverletzung in gewerblichem Ausmaß weiterhin angenommen werden soll,¹²³³ z.B. bei einem fortdauernden kommerziellen Erfolg des Werkes. Bei einem Musikalbum soll dies der Fall sein bei und für die Dauer einer Platzierung in den „Top 50“ der Verkaufsstatis-

¹²²⁷ Erwägungsgrund 14 der Enforcement-Richtlinie.

¹²²⁸ Vgl. *Jünger/Geißler* MMR 2008, S. 788; *Musiol*, GRUR-RR 2009, S. 3.

¹²²⁹ So *Musiol*, GRUR-RR 2009, S. 3; *Otten* GRUR-RR 2009, S. 370; *Schwippert* in *Schwartzmann*, S. 95. Vgl. auch *OLG Oldenburg* MMR 2009, 189, dem für das gewerblich Ausmaß der einmalige Download eines Musikalbums nicht genügt. Ebenso *LG Frankenthal* MMR 2008, 830, das in Anlehnung an die Praxis der Staatsanwaltschaften ein gewerbliches Ausmaß erst bei etwa 3000 Musikstücken oder 200 Filmen erreicht sehen will.

¹²³⁰ *LG Oldenburg* GRUR-RR 2009, 16; *OLG Frankfurt a.M.* MMR 2009, 542; *OLG Karlsruhe* MMR 2010, 419. So auch die Beschlussempfehlung des Rechtsausschusses des Bundestages, BT-Drucks.16/8783, 44, 50. Gegen einen zeitlichen Zusammenhang zu der Veröffentlichung etwa eines Musikalbums beim Vorliegen einer schweren Rechtsverletzung *Spindler* ZUM 2008, S. 642; *Spindler* in *Spindler/Schuster* § 101 Rn. 4.

¹²³¹ *OLG Oldenburg* MMR 2009, 189.

¹²³² *LG Kiel* MMR 2009, 643.

¹²³³ *OLG Köln* MMR 2011, 108, 110; a.A. *OLG Oldenburg* MMR 2009, 188.

tik der Musikindustrie.¹²³⁴ In dieser Phase sei i.d.R. der ursprünglich geforderte Kaufpreis für das Album noch nicht herabgesetzt. Sieht man dies als ein taugliches Kriterium an, spricht ein „Verramschen“ des Werkes zu Ausverkaufspreisen bzw. eine sehr erhebliche Preisherabsetzung gegen ein Andauern dieser Verwertungsphase, wobei jedoch übliche Preisschwankungen durch die Gewährung von Sonderangeboten nicht berücksichtigt werden sollen.¹²³⁵ Nach wiederum anderer Auffassung soll bereits drei Monate nach Veröffentlichung nur unter besonderen Umständen eine zur Begründung eines gewerblichen Ausmaßes hinreichende Schwere der Rechtsverletzung angenommen werden können.¹²³⁶

Ein gewerbliches Ausmaß liegt nach Ansicht des *OLG Köln* bereits beim einmaligen öffentlichen Zugänglichmachen eines Werks über eine Internettauschbörse schon deswegen vor, weil die Vervielfältigung nicht mehr kontrollierbar ist.¹²³⁷ Das *OLG München*¹²³⁸ geht ähnlich weit und schließt aus dem bloßen Umstand, dass eine (Film-) Datei mit urheberrechtlich geschütztem Inhalt auf einer Internet-Tauschbörse abrufbar ist, auf das grundsätzliche Vorliegen eines gewerblichen Ausmaßes; weiterer erschwerender Umstände bedürfte es nicht.

Einer schweren Rechtsverletzung steht nicht entgegen, wenn der Urheberrechtsberechtigte auf einen wirksamen technischen Kopierschutz verzichtet hat, da dieser Verzicht als solcher nicht als eine Einwilligung des Berechtigten in die Vervielfältigung betrachtet werden kann.¹²³⁹

c. Auskunftsverfahren gegen Zugangsanbieter gemäß § 101 Abs. 9 UrhG

aa. Grundlagen

Die Auskunftserteilung nach § 101 Abs. 9 UrhG ermöglicht dem Rechteinhaber bei bestimmten Formen der Rechtsverletzung, die Identität von Rechteinverletzern im Internet zu ermitteln. Anknüpfungspunkt ist dabei die IP-Adresse, die i.d.R. als dynamische IP-Adresse regelmäßig bzw. bei jeder aufgebauten Internetverbindung vom Diensteanbieter neu zugewiesen wird. Nur die Zugangsanbieter können durch den Abgleich der bei ihnen gespeicherten Daten ermitteln, welchem ihrer Kunden zum Verletzungszeitpunkt die dynamische IP-Adresse zugeteilt war.

Urheberrechtsverletzungen beim Handeln über P2P-Netzwerke lassen sich anhand der IP-Adresse und eines Zeitstempels verfolgen. Aus einer dynamischen IP-Adresse, die zu einem bestimmten Zeitpunkt einem Kunden des Zugangsanbieters zugewiesen ist, ergibt sich aber nur die Identität des Anschlussinhabers, nicht jedoch zwangsläufig die des

¹²³⁴ *OLG Köln* MMR 2011, 110.

¹²³⁵ *OLG Köln* MMR 2011, 246 ff.

¹²³⁶ *OLG Zweibrücken* MMR 2009, 43 ff.

¹²³⁷ *OLG Köln* GRUR-RR 2009, 9.

¹²³⁸ *OLG München* v. 26.7.2011 Az. 29 W 1268/11, <http://www.telemedicus.info/urteile/1313-29-W-126811.html>.

¹²³⁹ So *Musiol*, GRUR-RR 2009, S. 3; *Otten* GRUR-RR 2009, S. 372; *Wilhelmi* ZUM 2008, 948. Anders aber *OLG Zweibrücken* MMR 2009, 45.

Verletzers. Bei Ermittlung der IP-Adresse und des Verletzungszeitpunkts kann der Rechteinhaber im Wege des Auskunftsverfahrens nach § 101 Abs. 9 UrhG eine richterliche Anordnung über die Zulässigkeit der Verwendung von Verkehrsdaten beantragen.

Das Verfahren nach § 101 Abs. 9 UrhG ist ein – durchaus zeit- und kostenintensives – Vorverfahren, das der eigentlichen Geltendmachung der materiell-rechtlichen Auskunftsansprüche gemäß § 101 Abs. 2 UrhG vorausgeht. Ist die richterliche Anordnung nach § 101 Abs. 9 UrhG erlangt, wird der Zugangsanbieter aufgefordert, dem Rechteinhaber den Namen und die Anschrift des Anschlussinhabers mitzuteilen. Der Anschlussinhaber wird dadurch identifiziert, dass der Zugangsanbieter seine Daten abgleicht und vor allem ermittelt, wem er zum Verletzungszeitpunkt eine bestimmte IP-Adresse zugewiesen hat.

bb. Verkehrsdaten

Verkehrsdaten sind nach § 3 Nr. 30 TKG Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden, z.B. die Daten über Beginn und Ende der jeweiligen Internetverbindung. Verkehrsdaten weisen einen Bezug zu dem konkreten Telekommunikationsvorgang auf und unterliegen daher dem geschützten Fernmeldegeheimnis (§ 88 TKG und Art. 10 Abs. 1 GG). War der Bundesgerichtshof zunächst davon ausgegangen, dass die im Rahmen der Ermittlung des Verletzers notwendige IP-Adresse als Bestandsdatum anzusehen ist,¹²⁴⁰ ist nunmehr gesichert, dass er sie – unter Berücksichtigung der Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung¹²⁴¹ – mit der h.M.¹²⁴² als Verkehrsdatum beurteilt.¹²⁴³ Das Bundesverfassungsgericht sieht in der Speicherung und Herausgabe von IP-Adressen einen Eingriff in Art. 10 GG, jedoch kommt dem Gesetzgeber bei der Ausgestaltung von Auskunftsmöglichkeiten ein weiter Spielraum zu¹²⁴⁴.

Dynamische IP-Adressen als solche lassen keinen Schluss auf einen bestimmten Anschlussinhaber zu. Die Verbindung von dynamischer IP-Adresse und Anschlussinhaber ist nur dadurch möglich, dass die Umstände eines Telekommunikationsvorgangs, die bei der Erbrin-

¹²⁴⁰ BGH MMR 2010, 565.

¹²⁴¹ BVerfG Urteil vom 2.3.2010, abrufbar unter:

http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html.

¹²⁴² Vgl. Hoeren NJW 2008, S. 3100; Spindler ZUM 2008, S. 645; Wehr/Ujica MMR 2010, S. 667; Kitz NJW 2008, S. 2376; Mantz MMR 2010, S. 569; OLG Karlsruhe MMR 2010, 420; BGH MMR 2011, 341. So auch die amtliche Begründung des Regierungsentwurfs, BT-Drucks. 16/5048, 39 ff. Denn die dynamischen IP-Adressen, die bei jeder neuen Internetverbindung neu zugeteilt sind, werden bei der Erbringung des Telekommunikationsdienstes genutzt und gehören somit zur konkreten Telekommunikationsverbindung. Im Gegensatz dazu sind die festen IP-Adressen einem bestimmten Nutzer fest zugeordnet, so dass sie neben Namen und Anschrift des Nutzers zu den Bestandsdaten gehören (Spindler ZUM 2008, S. 645; Wehr/Ujica MMR 2010, S. 667). Man braucht hier keinen Rückgriff auf Telekommunikation, um eine IP-Adresse einem Nutzer zuzuordnen.

¹²⁴³ BGH MMR 2011, 341. Dazu Karg MMR 2011, S. 345, der die Entscheidung des BGH begrüßt, kritisiert aber die fehlende entsprechende Argumentation.

¹²⁴⁴ BVerfG Urteil vom 2.3.2010, abrufbar unter:

http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html, Rn. 45, 176, 238.

gung des TK-Dienstes erhoben werden, ausgewertet werden.¹²⁴⁵ Es handelt sich dabei also um Verkehrsdaten und die Regeln hierfür finden Anwendung.¹²⁴⁶

cc. Richtervorbehalt bei Verkehrsdaten

Das Erfordernis einer richterlichen Anordnung zur Verwendung von Verkehrsdaten zur Auskunftserteilung war eine im Vorfeld der Gesetzesänderung sehr umstrittene Regelung.¹²⁴⁷ Nach Auffassung des Gesetzgebers sollte der Richtervorbehalt gerade die Zugangsanbieter von der Beurteilung darüber entlasten, ob eine offensichtliche Rechtsverletzung vorliegt. Zudem trägt die richterliche Anordnung dem verfassungsrechtlichen Schutz von Verkehrsdaten Rechnung, die dem geschützten Fernmeldegeheimnis unterliegen. Der Richtervorbehalt dient schließlich dazu, Grundrechtseingriffe einer vorherigen unabhängigen Kontrolle zuzuführen.¹²⁴⁸

Das Gericht prüft das Vorliegen der Anspruchsvoraussetzungen nach § 101 Abs. 2 UrhG. Dies mündet lediglich in eine gerichtliche Entscheidung über die Zulässigkeit der Verwendung von Verkehrsdaten zur Auskunftserteilung.¹²⁴⁹ Der Bundesrat hat dies im Gesetzgebungsverfahren kritisiert und befürchtet, der Richtervorbehalt werde die Gerichte in hohem Maße belasten und dem Verletzten erhebliche Kosten aufbürden.¹²⁵⁰

Die richterliche Anordnung über die Auskunftserteilung richtet sich nach dem Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG).¹²⁵¹ Zuständig sind die landgerichtlichen Zivilkammern. Die örtliche Zuständigkeit richtet sich nach Wohnsitz, Sitz oder Niederlassung des zur Auskunft Verpflichteten.¹²⁵² Gegen die Entscheidung des Landgerichts ist die Beschwerde zum Oberlandesgericht innerhalb einer Frist von zwei Wochen statthaft (§ 101 Abs. 9 Satz 6 und 7 UrhG). Das Beschwerderecht steht auch dem Zugangsanbieter zu, da die Entscheidung seine datenschutzrechtlichen Pflichten gegenüber den Anschlussinhabern als seine Kunden berührt.¹²⁵³ Kein Beschwerderecht soll dagegen dem Anschlussinhaber bzw. dem Verletzer zustehen, da weder ein schwerwiegender Eingriff vorliege noch die vom Zugangsanbieter vorgenommene Auskunft rückgängig gemacht werden könne, wenn der Beschwerde stattgegeben werde.¹²⁵⁴ Das Gesetz sieht keine Rechtsmittel gegen einstweilige Zwischen-

¹²⁴⁵ Vgl. *Bär* MMR 2007, S. 812 (Anmerkung zu *AG Offenburg* MMR 2007, 809).

¹²⁴⁶ So *Bär* MMR 2007, S. 812 (Anmerkung zu *AG Offenburg* MMR 2007, 809); *Czychowski/Nordemann* NJW 2008, S. 3096; *Kindt* MMR 2009, S. 149; *Hoeren* NJW 2008, S. 3100; *Kondziela* MMR 2009, S. 298.

¹²⁴⁷ Dazu ausführlich *Welp* S. 334 ff.

¹²⁴⁸ *BVerfG* NJW 2001, 1122.

¹²⁴⁹ Vgl. amtliche Begründung des Regierungsentwurfs, BT-Drucks. 16/5048, 40, 63.

¹²⁵⁰ Vgl. amtliche Begründung des Regierungsentwurfs, Stellungnahme Bundesrat, BT-Drucks. 16/5048, 55 ff.

¹²⁵¹ BGBl. I S. 2586 (in Kraft seit 1.9.2009).

¹²⁵² Hat dieser im Inland einen Sitz, kann der Antrag nicht bei jedem Landgericht gestellt werden, in dessen Bezirk Niederlassungen bestehen; *OLG Düsseldorf* MMR 2009, 187 ff.

¹²⁵³ *OLG Düsseldorf* MMR 2009, 187; *Hoffmann* MMR 2009, S. 656.

¹²⁵⁴ *OLG Köln* MMR 2009, 547. So auch *Otten* GRUR-RR 2009, S. 372; *Maaßen* MMR 2009, S. 512. Anders die jüngste Rechtsprechung des OLG Köln, die ein Beschwerderecht des betroffenen Anschlussinhabers bejaht, um diesem nachträglich eine gerichtliche Kontrolle gegen die Verwendung seiner Telekommunikationsdaten zu ermöglichen. Vgl. *OLG Köln* MMR 2011, 108 ff.

anordnungen vor; diese sind jedoch aus verfassungsrechtlichen Gründen (Art. 130 Abs. 1 GG) geboten, da der Antragsgegner ansonsten kein rechtliches Gehör erhält.¹²⁵⁵

Die Kosten der Anordnung hat der Verletzte zu tragen (§ 101 Abs. 9 Satz 5 UrhG), zunächst trägt sie naturgemäß der Rechteinhaber, bis er sie vom Verletzten eingefordert hat. Die Kosten betragen nach § 128c Abs. 1 KostO¹²⁵⁶ 200 Euro je Antrag als Festgebühr.¹²⁵⁷ Ob bei einem Auskunftsverfahren über verschiedene IP-Adressen die Festgebühr mehrfach anfällt, richtet sich nach der Anzahl der Anträge. Mehrere Anträge liegen vor, wenn mehrere Lebenssachverhalte zugrunde liegen, was der Fall ist, wenn die Anträge die Verletzungshandlungen mehrerer Personen betreffen oder wenn sie auf die Verletzung unterschiedlicher urheberrechtlich geschützter Werke gestützt sind.¹²⁵⁸ Der Umstand, dass ein Auskunftsverfahren sich auf mehrere IP-Adressen bezieht, genügt für einen mehrfachen Kostenansatz nicht, da aus dem Vorliegen unterschiedlicher IP-Adressen nicht darauf geschlossen werden kann, dass eine, der unterschiedlichen Anzahl von IP-Adressen entsprechende, Anzahl von Anschlussinhabern eine Verletzungshandlung begangen hat.¹²⁵⁹

Offen ist die Diskussion über den Gegenstandswert des Verfahrens. Das *OLG Köln* geht von einem Regelstreitwert von 3.000 Euro je Werk aus, wobei der Wert naturgemäß höher sein kann, wenn es sich um mehrere urheberrechtlich geschützte Werke handelt;¹²⁶⁰ bei einem Musikalbum mit mehreren Titeln wird ein Werk angenommen. Das *OLG Frankfurt* geht bei einem einzelnen Download von einem Gegenstandswert in Höhe von 6.000 Euro aus¹²⁶¹, während das *OLG Zweibrücken* beim Download einer älteren Softwareversion einen Wert von 4.000 Euro angenommen hat.¹²⁶²

dd. Probleme in der Praxis

Das Vorverfahren nach § 101 Abs. 9 UrhG, derzeit einziges (vorgeschaltetes) Mittel zur Bekämpfung von Urheberrechtsverletzungen beim P2P-Filesharing, ist oft nicht zielführend.¹²⁶³

Folgende Aspekte sind beispielhaft zu nennen.

Aus der Auskunftspflicht des § 101 Abs. 9 UrhG folgt nicht zugleich, dass eine Pflicht oder **Berechtigung der Zugangsanbieter zur Speicherung der relevanten Daten** besteht.

¹²⁵⁵ Hoffmann MMR 2009, S. 656; Spindler in Spindler/Schuster § 101 Rn. 25.

¹²⁵⁶ Gesetz über die Kosten in Angelegenheiten der freiwilligen Gerichtsbarkeit (Kostenordnung), BGBl. I S. 1191.

¹²⁵⁷ Wird der Antrag zurückgenommen, bevor eine Entscheidung ergangen ist, betragen die Gerichtskosten nach § 128c Abs. 2 KostO 50 €.

¹²⁵⁸ *OLG Karlsruhe* MMR 2009, 264; *OLG Frankfurt a.M.* MMR 2009, 552.

¹²⁵⁹ Vgl. Weidert/Molle in Ensthaler/Weidert, S. 506.

¹²⁶⁰ *OLG Köln* MMR 2009, 125.

¹²⁶¹ *OLG Frankfurt a.M.* MMR 2009, 542.

¹²⁶² *OLG Zweibrücken* MMR 2009, 702.

¹²⁶³ Der urheberrechtliche Auskunftsanspruch müsste nach einer Auffassung in Anbetracht der datenschutz- und telekommunikationsrechtlichen Vorschriften sogar ins Leere laufen. Vgl. Heinemann, S. 174 ff. Zu Vorschlägen zur Rechtsdurchsetzung *de lege ferenda* vgl. Heinemann, S. 207 ff.

Vielfach werden Daten nur für wenige Tage, z.B. sieben Tage, nach Abwicklung des konkreten Internetzugriffs gespeichert, in manchen Ländern nur für die Dauer der Abwicklung der konkreten Internetverbindung. Daraus ergeben sich in der Praxis Schwierigkeiten, wenn die dem Zugangsanbieter abverlangten Daten nicht bzw. nicht mehr vorliegen, da diese entweder nicht erhoben oder bereits gelöscht wurden. Diese Schwierigkeiten werden – in den Fällen, in denen eine Speicherung von IP-Adressen überhaupt erfolgt – so gelöst, dass zunächst ohne Anhörung des Zuganganbieters der Erlass einer einstweiligen Anordnung beantragt wird, mit der dem Zuganganbieter die Löschung der Verkehrsdaten untersagt wird.¹²⁶⁴ Die Sicherung der Verkehrsdaten gewährleistet einen späteren Zugriff auf die Daten zum Zeitpunkt der Entscheidung über den Auskunftserteilungsantrag. Nachdem dem Zugangsanbieter im Verfahren rechtliches Gehör gewährt wurde, kann über die Zulässigkeit der Verwendung von Verkehrsdaten für die Auskunftserteilung an den Rechteinhaber entschieden werden.

Während Bestandsdaten nach § 95 Abs. 3 TKG erst nach Ende des Vertragsverhältnisses gelöscht werden müssen, sind Verkehrsdaten – und damit auch die dynamischen IP-Adressen – grundsätzlich nach Beendigung einer Verbindung unverzüglich zu löschen (§ 96 Abs. 1 Satz 3 TKG). Ausnahmsweise ist die Speicherung von Verkehrsdaten zu bestimmten Zwecken, wie z.B. zu Abrechnungszwecken (§ 97 TKG) sowie zu Störungsbeseitigung und Missbrauchsbekämpfung (§ 100 TKG) erforderlich. Die Herleitung einer Befugnis der Zugangsanbieter zur Speicherung der Daten aus § 97 Abs. 1 Satz 1 oder § 100 Abs. 1 und 3 TKG wird aber in der Literatur überwiegend abgelehnt. Eine Speicherung der IP-Adresse im Rahmen des urheberrechtlichen Auskunftsanspruch dürfe auf der Grundlage des § 97 Abs. 1 Satz 1 TKG nicht erfolgen, da für die dort genannten Zwecke – die Ermittlung des Entgelts und die Abrechnung – nur eine Speicherung von Zugriffszeit und Nutzerkennung notwendig sei. Keine ausreichende gesetzliche Grundlage bietet auch § 100 Abs. 1 und 3 TKG, da eine Störung bzw. ein Missbrauch die konkrete Beeinträchtigung des Telekommunikationsdienstes durch die Handlung des in Anspruch Genommenen voraussetze.¹²⁶⁵

Als Rechtsgrundlage für die Datenspeicherung ziehen Rechtsprechung¹²⁶⁶ und Literatur¹²⁶⁷ teilweise § 101 Abs. 9 UrhG heran. Die Vorschrift regelt zwar keine ausdrückliche Pflicht zur Speicherung von Daten, enthält aber die Berechtigung, beim Vorliegen einer richterlichen Anordnung, die Verkehrsdaten zur Auskunftserteilung an den Rechteinhaber zu „verwen-

¹²⁶⁴ OLG Köln MMR 2008, 820. Das Gericht vertritt die Auffassung, dass es unzulässig ist, im Rahmen der einstweiligen Anordnung die Gestattung der Auskunftserteilung anzuordnen, da hierdurch die Hauptsache vorweggenommen würde. Anders *Mantz* K&R 2009, S. 22.

¹²⁶⁵ Vgl. dazu *Hennemann*, S. 169 ff.

¹²⁶⁶ OLG Köln MMR 2008, 820.

¹²⁶⁷ *Maaßen* MMR 2009, S. 513; *Ladeur* NJOZ 2010, S. 1605; *Otten* GRUR-RR 2009, S. 370. A.A. *Welp* S. 271 ff., der der Ansicht ist, dass § 101 Abs. 2 und 9 UrhG eine datenschutzrechtliche Erlaubnisnorm für die Auskunftserteilung darstellen kann. Die Vorschrift genügt jedoch nicht den Anforderungen an die Bestimmtheit und Normenklarheit. A.A. auch *Heinemann*, S. 169 ff., der die Meinung vertritt, dass eine hinreichende gesetzliche Grundlage für die Speicherung von Verkehrsdaten im Rahmen des Auskunftsanspruchs bisher nicht besteht.

den“, worunter auch das Speichern im Sinne von Aufbewahren personenbezogener Daten fällt.¹²⁶⁸ Wie oben dargelegt ist nach § 101 Abs. 9 UrhG eine richterliche Anordnung für die Auskunftserteilung erforderlich. Dies bedeutet aber nicht, dass dem Richtervorbehalt nur die Übermittlung von Daten an den Rechteinhaber unterworfen werden, sondern alle Tatbestände der Verwendung von Daten. Soweit eine Speicherung von Daten überhaupt als zulässig zu betrachten ist, ist entsprechend dem Sinn und Zweck der Norm eine richterliche Anordnung nach § 101 Abs. 9 UrhG auch für die Speicherung erforderlich. Nach der Gesetzesbegründung sollte durch diese Regelung der Zugangsanbieter von der Prüfung entlastet werden, ob im Einzelfall eine offensichtliche oder im gewerblichen Ausmaß begangene Rechtsverletzung vorliegt.¹²⁶⁹ Eine Speicherung von Daten mit vorheriger richterlicher Anordnung muss es auch aus datenschutzrechtlichen Gründen geben. Wie oben dargelegt,¹²⁷⁰ soll der Richtervorbehalt dem verfassungsrechtlichen Schutz von Verkehrsdaten (Art. 10 GG) Rechnung tragen.¹²⁷¹ Damit wird der Zweck verfolgt, eine datenschutzrechtliche Absicherung in Bezug auf die Verwendung von Verkehrsdaten für die Auskunftserteilung zu erreichen.¹²⁷²

In den Fällen, in denen die Zugangsanbieter Verkehrsdaten überhaupt nicht speichern, sind die Rechteinhaber dazu übergegangen, vor der Einleitung des Auskunftsverfahrens, eine Speicherung der begehrten Daten zu verlangen. Sie fordern die Zugangsanbieter noch während einer laufenden Internetverbindung, im Rahmen derer eine Rechtsverletzung begangen wird, zur Speicherung der dynamischen IP-Adresse auf und setzen diese davon in Kenntnis, dass ein Auskunftsverfahren nach § 101 Abs. 9 UrhG zur Ermittlung des Rechteinhabers durchgeführt werden soll. Die gespeicherten Daten können somit später genutzt werden, um Rechteinhabern Auskunft über potentielle Urheberrechtsverletzer zu erteilen.

Nicht abschließend geklärt wird, ob ein solcher Anspruch der Rechteinhaber und damit zugleich eine sog. „**Speicherungspflicht auf Zuruf**“ der Zugangsanbieter besteht.

Nach der vom *OLG Hamburg* bestätigten Rechtsprechung des *LG Hamburg*¹²⁷³ sind Zugangsanbieter verpflichtet, die zur Auskunftserteilung erforderlichen Daten während einer Internetverbindung auf Anforderung des Rechteinhabers zu speichern.¹²⁷⁴ Die Hamburger Gerichte stützen die Speicherpflicht auf Zuruf auf § 101 Abs. 2 Nr. 3, Abs. 9 Satz 1 UrhG i.V.m. § 96 Abs. 2 Satz 1 letzter Hs. TKG und § 242 BGB. Im Hinblick auf die Auskunftspflicht nach § 101 Abs. 2 Nr. 3 UrhG bestehe ein gesetzliches Schuldverhältnis zwi-

¹²⁶⁸ Unter „Verwendung“ fallen die Verarbeitung und die Nutzung von Daten im Sinne von § 3 Abs. 4 und 5 BDSG, vgl. *Gola/Schomerus* § 3 Rn. 25; *Dammann in Simitis* § 3 Rn. 193. Davon wird also jede Art des Umgangs mit Daten, außer der Erhebung umfasst, die in § 3 Abs. 3 BDSG definiert ist.

¹²⁶⁹ Vgl. amtliche Begründung des Regierungsentwurfs, BT-Drucks. 16/5048, 40, 63.

¹²⁷⁰ Siehe S. 259.

¹²⁷¹ Vgl. amtliche Begründung des Regierungsentwurfs, BT-Drucks. 16/5048, 40, 63.

¹²⁷² So *Moos/Gosche* CR 2010, S. 502.

¹²⁷³ *OLG Hamburg* ZUM 2010, 893.

¹²⁷⁴ *LG Hamburg* MMR 2009, 570 (572 ff.); kritisch dazu *Schulze zur Wiesche* MMR 2009, S. 574 ff.; *Maaßen* MMR 2009, S. 514 ff.

schen dem Rechteinhaber und dem jeweiligen Zugangsanbieter, aufgrund dessen der Zugangsanbieter ab dem Zeitpunkt der Kenntniserlangung über den konkreten Verbindungsvorgang und die Auskunftserlangungsabsicht verpflichtet sei, die Daten für eine Auskunft vorzuhalten, um seiner Auskunftspflicht nachkommen zu können.¹²⁷⁵ Die Datenspeicherung stehe dabei anders als die Datenübermittlung auch nicht unter dem Richtervorbehalt des § 101 Abs. 9 UrhG, der sich nach dem klaren Wortlaut nur auf die „Verwendung“ beziehe und eine Auskunftserteilung bereits das Vorhandensein der Daten voraussetze.¹²⁷⁶

Andere Oberlandesgerichte¹²⁷⁷ haben eine Speicherungspflicht auf Zuruf mangels Vorliegens einer entsprechenden Rechtsgrundlage abgelehnt. § 101 Abs. 2 Satz 1 Nr. 3 i.V.m. Abs. 9 UrhG regle einen Auskunftsanspruch und nicht eine den Anspruch erst ermöglichende Speicherung.¹²⁷⁸ Auch eine analoge Anwendung der Vorschrift scheidet aus, da dem Gesetzgeber bekannt war, dass die zur Auskunftserteilung nötigen Daten fehlen könnten.¹²⁷⁹ Dass die Erteilung einer Auskunft über Verkehrsdaten von einer richterlichen Gestattung abhängig ist, führe darüber hinaus dazu, dass der Zugangsanbieter erst aufgrund dieser Gestattung nicht mehr sanktionslos die Daten löschen könne, weil er sich ansonsten nach §§ 280 Abs. 1, 281 BGB i.V.m. § 101 UrhG schadensersatzpflichtig mache. Eine – unabhängig von einer Auskunftsverpflichtung – bestehende Speicherungspflicht des Anbieters lasse sich der gesetzlichen Regelung hingegen nicht entnehmen.¹²⁸⁰

In der Literatur wird eine Speicherungspflicht auf Zuruf überwiegend abgelehnt.¹²⁸¹ Sie lasse sich nicht aus § 101 Abs. 2 Satz 1 Nr. 3 i.V.m. Abs. 9 UrhG herleiten.¹²⁸² Geregelt werde ein Anspruch auf Auskunftserteilung, nicht aber auf vorauseilende Speicherung. Erst durch die Gestattung einer Auskunftserteilung werde die datenschutzrechtliche Grundlage dafür geschaffen, dass der Zugangsanbieter berechtigt ist, die Verkehrsdaten nicht zu löschen.¹²⁸³ Für eine solche Speicherung bestehe kein Erlaubnistatbestand, der hierfür aber erforderlich sei, weil eine Speicherungspflicht des Zugangsanbieters mittelbar in das Fernmeldegeheimnis (Art. 10 GG) eingreife.¹²⁸⁴

Eine Übermittlung von Daten seitens der Zugangsanbieter erfolgt im Rahmen des urheberrechtlichen Auskunftsanspruchs nach § 101 Abs. 2 Satz 1 Nr. 3 und Abs. 9 UrhG an die Rechteinhaber. Soweit personenbezogene Daten von den Zugangsanbietern übermittelt

¹²⁷⁵ *LG Hamburg* MMR 2009, 570 (572 ff.); *OLG Hamburg* ZUM 2010, 893 (896).

¹²⁷⁶ *LG Hamburg*, MMR 2009, 570 (573).

¹²⁷⁷ *OLG Frankfurt* MMR 2010, 62; *OLG Frankfurt* MMR 2010, 109; *OLG Hamm* MMR 2011, 194; *OLG Düsseldorf* MMR 2011, 547.

¹²⁷⁸ *OLG Frankfurt* MMR 2010, 62 (63); *OLG Frankfurt* MMR 2010, 109; *OLG Hamm* MMR 2011, 194.

¹²⁷⁹ *OLG Frankfurt* MMR 2010, 62 (63) und *OLG Frankfurt* MMR 2010, 109 jeweils mit Verweis auf BT-Drs. 798/1/07.

¹²⁸⁰ *OLG Frankfurt* MMR 2010, 62 (63); *OLG Frankfurt* MMR 2010, 109.

¹²⁸¹ *Schulze zur Wiesche* MMR 2009, S. 574 ff.; *Maaßen* MMR 2009, S. 514 ff.; *Spindler* in *Spindler/Schuster*, *Recht der elektronischen Medien*, § 101 UrhG, Rn. 23.

¹²⁸² *Spindler* in *Spindler/Schuster*, *Recht der elektronischen Medien*, § 101 UrhG, Rn. 23.

¹²⁸³ *Schulze zur Wiesche* MMR 2009, S. 574 ff.

¹²⁸⁴ *Maaßen* MMR 2009, S. 515.

werden sollen, bedarf es wegen des Personenbezugs nach dem deutschen Datenschutzrecht wiederum eines Erlaubnistatbestands. Nicht klar ist, ob der Auskunftsanspruch gemäß § 101 Abs. 2 und 9 eine taugliche Ermächtigung der Zugangsdiensteanbieter zur Datenübermittlung darstellt.

In der Rechtsprechung wird § 101 Abs. 9 UrhG unter Verweis auf den Willen des Gesetzgebers als hinreichender Erlaubnistatbestand angesehen.¹²⁸⁵ Der besonderen Schutzwürdigkeit der Verkehrsdaten wird dabei durch die richterliche Anordnung Rechnung getragen. Die Literatur sieht teilweise¹²⁸⁶ im Auskunftsanspruch selbst keine hinreichende Ermächtigung der Zugangsanbieter zur Datenübermittlung und fordert - über den geregelten Auskunftsanspruch hinaus - eine gesonderte Befugnis für die Provider, Daten über ihre Kunden herauszugeben. Eine solche bestehe zwar für den Hostprovider in Bezug auf die Herausgabe von Bestandsdaten wegen Verletzung des Rechts am geistigen Eigentum in § 14 Abs. 2 TMG, fehle aber für die Übermittlung von Verkehrsdaten durch die Zugangsanbieter, die im TKG geregelt sein müsse.¹²⁸⁷ Mit der Einführung des § 101 Abs. 2 und Abs. 9 UrhG sei nicht abschließend geklärt, dass nun ein zivilrechtlicher Weg für die Identifizierung des Rechteverletzers und für die Verfolgung der Urheberrechtsverletzungen im Internet bestehe.¹²⁸⁸ Ein Teil dieser in der Literatur vertretenen Ansicht hat wiederum selbst festgestellt, dass es keinen Sinn mache, einerseits ein solches Auskunftsverfahren mit Richtervorbehalt vorzusehen, andererseits aber die Herausgabe der Daten mangels gesonderter Ermächtigung scheitern zu lassen und hat eine solche aus § 96 Abs. 2 Satz 1 TKG a.F. (§ 96 Abs. 1 Satz 2 TKG n.F.) i.V.m. § 101 Abs. 9 UrhG hergeleitet.¹²⁸⁹

Neben diesen datenschutzrechtlichen Problemen sei ferner festgehalten, dass die Anordnung des Gerichts nach § 101 Abs. 9 UrhG zwar zu einer Befugnis, nicht aber zu einer Verpflichtung der Zugangsanbieter führt, die Verkehrsdaten zur Auskunftserteilung zu verwenden.¹²⁹⁰ Verweigert der Zugangsanbieter trotz gerichtlicher Entscheidung die Auskunft, muss der Rechteinhaber Klage auf Auskunftserteilung im zivilrechtlichen Verfahren erheben. Dieses zivilrechtliche Verfahren setzt naturgemäß ein erfolgreiches Auskunftsgestattungsverfahren nach § 101 Abs. 9 UrhG voraus. Von dieser Verweigerung wird aufseiten der Zugangsanbieter durchaus Gebrauch gemacht.

In der Abwicklung gestalten sich schließlich die Auskunftsverfahren für die Zugangsanbieter sehr aufwändig. Größere Zugangsanbieter haben für die Bewältigung solcher Auskunftsersuchen eigens ihre Rechtsabteilung erheblich ausgebaut.

¹²⁸⁵ *OLG Köln MMR 2008, 821.*

¹²⁸⁶ *Spindler in ZUM 2008, 640 (645); Czychowski/Nordemann in NJW 2008, 3095 (3097).*

¹²⁸⁷ *Spindler in ZUM 2008, 640 (645); Czychowski/Nordemann in NJW 2008, 3095 (3097).*

¹²⁸⁸ *Czychowski/Nordemann in NJW 2008, 3095 (3097).*

¹²⁸⁹ *Czychowski/Nordemann in NJW 2008, 3095 (3097), anders Spindler in ZUM 2008, 640 (645), nach dem in § 101 Abs. 9 Satz 8 UrhG allenfalls eine „versteckte Befugnisnorm“ gelesen werden könne.*

¹²⁹⁰ *So Welp S. 351 ff.; Hoffmann MMR 2009, S. 655.*

3. Eignung des Auskunftsanspruchs zur Rechtsdurchsetzung

Der den Unterlassungs- und Schadensersatzanspruch unmittelbar vorbereitende Auskunftsanspruch nach § 101 Abs. 2 und Abs. 9 UrhG stellt im Bereich des P2P-Filesharing sicherlich ein geeignetes Mittel zur Bekämpfung von Urheberrechtsverletzungen, die unter Nutzung dieser Technologie erfolgen, dar. Nach derzeitiger Rechtslage steht auch kein anderes (zivilrechtliches) Mittel zur Verfügung (von strafrechtlichen Mitteln mithin abgesehen). Die Eignung hat sich in praktischer Hinsicht dadurch erhöht, dass der Bundesgerichtshof in der Entscheidung „Sommer unseres Lebens“ die Eignung des benutzten Verfahrens zur Ermittlung der IP-Adresse des Anschlussinhabers nicht infrage gestellt, sondern im Prinzip bestätigt hat, ohne sich mit technischen bzw. fachlichen Einzelheiten des Verfahrens überhaupt zu befassen bzw. befassen zu müssen. Damit sind die – in nicht unerheblichem Umfang vielfach durchaus berechtigten – Einwände der Betroffenen zur Zuverlässigkeit bisher verwendeter Computerprogramme für die forensische Praxis zwar nicht beseitigt, aber erheblich eingeschränkt. Soweit der Einwand, dass derzeit benutzte Verfahren zur Ermittlung der IP-Adresse eines Anschlussinhabers technisch-fachlich von zweifelhafter Zuverlässigkeit sind, vorgebracht werden kann, mag man gar an der Eignung des Auskunftsanspruchs zweifeln.

Inwiefern der Auskunftsanspruch jedoch erforderlich und angemessen ist, erscheint zweifelhaft. Hat man es mit einem hartnäckigen, vorsätzlich handelnden Rechteverletzer zu tun, der im vollen Bewusstsein urheberrechtlich geschützte Werke vervielfältigt, z.B. einen gerade erst gestarteten Kinofilm oder einen eben erst veröffentlichten Musiktitel, so ist nachvollziehbar, dass andere Mittel als solche, die zur Unterlassung zwingen, nicht nur geeignet, sondern auch erforderlich erscheinen. Solche Rechteverletzer würden aber voraussichtlich ohnehin zum Wechsel der Technologie neigen, die sie für die Verletzung einsetzen; jedenfalls ist es angesichts solcher Fallgestaltungen nachvollziehbar, dass – zumindest in letzter Konsequenz – ein Auskunftsanspruch zur Vorbereitung von Unterlassungs- und Schadensersatzansprüchen vorhanden sein muss, von weiter reichenden strafrechtlichen Mitteln abgesehen. Denn anders als über den Auskunftsanspruch ist die Identität des Anschlussinhabers derzeit nicht erlangbar. Ein nicht unerheblicher Teil der vom Auskunftsanspruch und den hernach einsetzenden Abmahnung Betroffenen zählt aber gerade nicht zu diesem Teil der Verletzer, so dass ernstlich fraglich ist, ob ein Auskunftsanspruch nach dem geltenden Recht als derzeit einziges nennenswertes Mittel im Hinblick auf diesen Personenkreis erforderlich ist.

Wenn nicht schon die Erforderlichkeit zweifelhaft ist, so ist jedenfalls ein Auskunftsanspruch als einziges Mittel im Hinblick auf den zuletzt genannten Personenkreis zur Rechtsdurchsetzung wahrscheinlich nicht angemessen. Man wird annehmen dürfen, dass ein erheblicher Teil der fahrlässig handelnden Personen im Grundsatz rechtstreu ist, vielen Personen fehlt die Kenntnis über die technischen und rechtlichen Zusammenhänge der ihnen vorgeworfenen Verletzung. Das darf sicherlich nicht ohne jede Konsequenz bleiben.

Jedoch ist die Belastung solcher Nutzer durch den Auskunftsanspruch und eine auf ihn folgende Abmahnung bzw. gerichtliche Inanspruchnahme erheblich, sie werden schon im ersten Kontakt scharf getroffen, auch im Hinblick auf die Kostenbelastung, denn schon der Erstkontakt durch die Abmahnung ist mit Kosten verbunden.

IV. Rechtsvergleichender Blick auf Auskunftsansprüche

Das französische Recht¹²⁹¹ kennt im Rahmen des neu eingeführten Warnhinweismodells eine Auskunftspflicht des Zugangsanbieters. Diese verpflichtet den Internetzugangsanbieter gegenüber der Rechtsschutzkommission der Hadopi zur Mitteilung über die Identität des Anschlussinhabers. Dem Rechteinhaber gegenüber ist der Diensteanbieter nicht unmittelbar zur Auskunft verpflichtet. Der Rechteinhaber kann Kenntnis über die Identität des Anschlussinhabers regelmäßig nur im Wege der Akteneinsichtnahme im staatsanwaltlichen Ermittlungsverfahren erlangen.

Das englische Urheberrecht¹²⁹² kennt einen Auskunftsanspruch aufgrund richterlicher Anordnung gegen Dritte bereits seit 1974, jedoch nicht aufgrund der ansonsten recht umfassenden Kodifizierung des Urheberrechts, sondern aufgrund der höchstrichterlichen Entscheidung *Norwich Pharmacal Co. & Others v. Customs and Exise Commissioners*¹²⁹³. Damit besteht keine vergleichbare Regelung.

§ 53c des Schwedischen Urheberrechtsgesetzes¹²⁹⁴ kennt einen Auskunftsanspruch der Rechteinhaber u. a. gegen die Zugangsanbieter; dieser ist Gegenstand heftiger Debatten, zumal einige schwedische Zugangsanbieter ihm skeptisch gegenüberstehen und angekündigt hatten, ihn dadurch zu unterlaufen, dass die zu beauskunftenden IP-Daten gelöscht werden. In gerichtlicher Hinsicht ist der Auskunftsanspruch Gegenstand eines Vorabentscheidungsersuchens an den EuGH (*Bonnier Audio AB/ePhone*¹²⁹⁵). Begrenzt wird der Auskunftsanspruch u. a. durch enge datenschutzrechtliche Regelungen, wonach personenbezogene Daten im Grundsatz nur behördlichen Organisationen für deren Zwecke zugänglich gemacht bzw. von diesen verarbeitet werden dürfen. Die Datenschutzbehörde kann hiervon jedoch Ausnahmen zulassen, wenn die verfolgten Zwecke die berechtigten Interessen der verantwortlichen Stelle oder eines Dritten betreffen, sofern diese Interessen schwerer wiegen als das Schutzbedürfnis der betroffenen Person gegen die Verletzung ihrer persönlichen Integrität; die Datenschutzbehörde hat solche Ausnahmen z.B. zugunsten von Musikindustrieverbänden zugelassen, und zwar zeitlich begrenzt auf Einzelfälle. Schon aufgrund der engen datenschutzrechtlichen Maßgaben vermag diese Form des

¹²⁹¹ Zum Auskunftsanspruch in Frankreich s. im Detail S. 76ff.

¹²⁹² Zum Auskunftsanspruch in England S. 111.

¹²⁹³ [1974] AC 133.

¹²⁹⁴ Zum Auskunftsanspruch S. 181.

¹²⁹⁵ Rs C-461/10.

Auskunftsanspruches wohl nicht als Leitbild für eine Verfolgung von Urheberrechtsverletzungen dienen. Nicht zu verkennen ist jedoch, dass nach einer – allerdings auf der Auswertung der reinen Menge des Datenverkehrs beruhenden – Studie der Datenverkehr nach Einführung des Auskunftsanspruchs um ca. 40% zurückging, was als Abnahme illegalen Datenverkehrs gewertet wurde. Dieser Datenverkehr nahm aber nach rund sechs Monaten wieder zu, weil, so der Schluss der Studie, an den Auskunftsanspruch keine hinreichenden Konsequenzen geknüpft waren. Daraus würde jedenfalls folgen - wenn man dies als zutreffend unterstellte - dass ein Auskunftsanspruch, der keine – und sei es über mehrere abgeschichtete Schritte – Konsequenzen für den von der Auskunft Betroffenen hat, in der Praxis mittelfristig wirkungslos ist. Oder umgekehrt: Nur ein Auskunftsanspruch, aus dem auch Folgen für den Betroffenen ableitbar sind, führen zu einer Verhaltensänderung.

In Irland¹²⁹⁶ existiert keine spezielle gesetzliche Regelung zum Auskunftsanspruch von Zugangsanbietern im Zusammenhang mit Urheberrechtsverletzungen, jedoch im Recht der unerlaubten Handlungen der aus UK bekannte Auskunftsanspruch auch gegen Dritte, die – ggf. ohne eigenes Verschulden – eine unerlaubte Handlung ermöglicht oder erleichtert haben. Bei Gewährung dieses Anspruchs sind die Datenschutzbelange des Betroffenen zu berücksichtigen. Mangels einer vergleichbaren Regelung im Urheberrecht ist dieser allgemeine Auskunftsanspruch nicht tauglich für einen Vergleich der Systeme. Der allgemeine Auskunftsanspruch gegen den Zugangsanbieter und das nachfolgende urheberrechtliche Verletzungsverfahren gegen Betroffene haben sich aber nach irischen Vorstellungen als alleiniges Mittel jedenfalls nicht bewährt. Welche Konsequenzen daraus zu ziehen sind, insbesondere im Hinblick auf die künftige Gestaltung des Urheberrechts in Irland, sind nicht abzusehen. Insoweit mag jedoch als Anhaltspunkt dienen, dass der größte irische Zugangsanbieter Eircom im Rahmen einer gerichtlichen Inanspruchnahme auf Auskunft einen Vergleich mit Musikverbänden getroffen hat, der ein Warnhinweismodell impliziert, das bereits einer gerichtlichen Überprüfung standgehalten hat.¹²⁹⁷

¹²⁹⁶ Zum Auskunftsanspruch S. 148.

¹²⁹⁷ Siehe oben S. 161.

2. Teil: Erwägungen zu einem innerstaatlichen Ansatz

A. Vorgerichtliches Mitwirkungsmodell

I. Ausgangsüberlegung

Die Studie beleuchtet die Rahmenbedingungen für die mögliche Umsetzung eines Warnhinweismodells zur Reduzierung von Urheberrechtsverletzungen im Internet. Um die internationalen, die verfassungs- und einfachgesetzlichen Rahmenbedingungen eines Warnhinweismodells nicht abstrakt prüfen zu müssen, sondern konkret erörtern zu können, wird hier ein schlagwortartig als vorgerichtliches Mitwirkungsmodell bezeichneter Lösungsansatz vorgestellt. Diese Ausführungen erfolgen unabhängig von der Projektbeschreibung und können als Ansatz für eine weiterführende Diskussion dienen.

Das eigentliche Spannungsfeld eines solchen Modells liegt dabei zwischen dem Urheber- und Leistungsschutzrecht der **Rechteinhaber**, die ihr geistiges Eigentum wahren wollen und dem Recht der rechtsverletzenden **Nutzer** auf Beachtung von Datenschutzerfordernungen und dem Recht auf Informationsfreiheit bei der Verfolgung von Verletzungshandlungen.

Bei Rechtsverletzungen im Internet sind in dieses Verhältnis aber zwingend die **Zugangsanbieter** als private Dritte eingebunden¹²⁹⁸. Rechteinhaber können Verletzungshandlungen durch Ermittlung einer IP-Adresse ermitteln. Zur Ermittlung von Namen und Anschrift des Rechteinhabers bedarf es aber der Beteiligung des Zugangsanbieters, der die IP-Adresse einem Namen zuordnen kann. Dies berücksichtigt auch das aktuelle deutsche Recht zur Durchsetzung von Urheberrechten im Internet in Form des Auskunftsanspruchs nach § 101 Abs. 9 UrhG.¹²⁹⁹ Es besteht aber Anlass dazu, den Auskunftsanspruch in seiner derzeitigen Ausgestaltung als alleiniges Mittel zur Rechtsdurchsetzung im Internet zu hinterfragen, weil er für einen Nutzer, der ihm sich unvermittelt ausgesetzt sieht, ein zu scharfes erstes Mittel darstellt. Zum anderen ist er aus Sicht der Rechteinhaber aus Gründen des Datenschutzes nur schwer durchsetzbar und darüber hinaus anfällig für als missbräuchlich empfundene Verwendung.

Faktisch streiten in dieser Konstellation aber nicht Rechteinhaber und Nutzer miteinander, sondern die Auseinandersetzung wird zwischen Rechteinhabern und Zugangsanbietern über deren Mitwirkung an einem Modell zum Schutz des Urheberrechts geführt. Diese

¹²⁹⁸ Siehe oben S. 196.

¹²⁹⁹ Siehe oben S. 257

Frage ist insbesondere auch Gegenstand des durch das Bundesministerium für Wirtschaft und Technologie in dieser Angelegenheit moderierten Wirtschaftsdialogs.¹³⁰⁰

Fragen nach der konkreten Ausgestaltung eines Warnhinweismodells sind weder zu stellen noch zu beantworten. Aufgabe der Studie ist es aber, das rechtliche Erfordernis eines Modells unter Mitwirkung von Zugangsanbietern zu untersuchen, das über das reine Modell eines Auskunftsanspruchs hinausgeht und es auf den Prüfstand des internationalen und nationalen Rechts zu stellen. Dieser Ansatz wird hier schlagwortartig als vorgelagertes oder **vorgerichtliches Mitwirkungsmodell** bezeichnet.

Die nachfolgenden Ausführungen in dieser vornehmlich rechtsvergleichenden Studie stellen auftragsgemäß keine abschließende rechtliche Überprüfung eines solchen Ansatzes dar, sondern sie sollen die Möglichkeiten eines Warnhinweismodells, das ohne Sperrungen auskommt, rechtlich in das vorhandene deutsche System einordnen und erste Überlegungen für eine mögliche Umsetzung anstellen.

II. Parameter eines denkbaren Ansatzes

Parameter eines möglichen Ansatzes wären insoweit in Anlehnung an das britische Modell im Rahmen der ersten Stufe des *Digital Economy Acts* eine Inpflichtnahme von Zugangsanbietern zur Mitwirkung an der Versendung von Warnhinweisen zur Vorbereitung eines gerichtlichen Auskunftsanspruchs. Dabei könnte der Zugangsanbieter den Auskunftsanspruch vorbereitende Hinweise an gemeldete Kunden übersenden, entweder geprüft – wie im Vereinigten Königreich – oder ungeprüft – wie nach dem politisch gescheiterten finnischen Gesetzesentwurf. Die an das britische Recht angelehnte Neuerung für das deutsche Recht läge in der Verpflichtung zur Führung einer für den Rechteinhaber anonymen Liste über Verstöße.¹³⁰¹

B. Internationale Rahmenvorgaben für ein vorgerichtliches Mitwirkungsmodell

Bevor die nationalen rechtlichen Voraussetzungen umrissen werden, soll der internationale Rechtsrahmen sowohl für das Urheberrecht als auch für das Datenschutzrecht skizziert und soweit ersichtlich, vorhandene Positionen und Rechtsprechung zu Warnhinweisen, auch im Hinblick auf Anschlussperren, aufgezeigt werden.

¹³⁰⁰ Siehe oben S. 24.

¹³⁰¹ Siehe dazu im einzelnen unten S. 316.

I. Urheberrecht

1. Völkerrechtliche Grundlagen

Völkerrechtliche Gewährleistungen des Rechts am geistigen Eigentum finden sich sowohl im humanitären Völkerrecht als auch im Wirtschaftsvölkerrecht.

a. Vereinte Nationen

Art. 27 der **Erklärung der Menschenrechte der Vereinten Nationen**¹³⁰² gewährt den Schutz des geistigen Eigentums. In derselben Norm werden Informationsfreiheit und Teilhabe an kulturellen Errungenschaften gewährt. Art. 27 AEMR lautet:

„Jeder hat das Recht, am kulturellen Leben der Gemeinschaft frei teilzunehmen, sich an den Künsten zu erfreuen und am wissenschaftlichen Fortschritt und dessen Errungenschaften teilzuhaben“ (Abs. 1).

Absatz 2 nimmt den Rechteinhaber in Bezug, wenn er bestimmt:

„Jeder hat das Recht auf Schutz der geistigen und materiellen Interessen, die ihm als Urheber von Werken der Wissenschaft, Literatur oder Kunst erwachsen.“

Nach Ansicht von Frank La Rue, dem Sonderbeauftragten der UNO für Meinungs- und Pressefreiheit, sind Anschlussperren unverhältnismäßig und verstoßen daher gegen Artikel 19 Absatz 3 des internationalen Pakts über bürgerliche und politische Rechte (International Covenant on Civil and Political Rights, ICCPR). Dies soll unabhängig davon gelten, ob die Sperre wegen Verletzungen des geistigen Eigentums oder aus anderen Gründen erfolgt.

Zwar ohne jegliche rechtliche Bindung liegt der La Rue-Report inhaltlich aber ganz auf der Linie des Menschenrechtsausschusses, welcher unter bestimmten Voraussetzungen in einem quasigerichtlichen Verfahren Verletzungen des ICCPR durch einen Mitgliedstaat feststellen kann. Auch der Ausschuss hält die Sperrung eines Informationssystems für unverhältnismäßig.¹³⁰³

¹³⁰² Resolution 217 A (III) der Generalversammlung vom 10. Dezember 1948, abrufbar unter: <http://www.un.org/depts/german/grunddok/ar217a3.html>.

¹³⁰³ Ausführlich dazu Dr. Tobis O. Keber, ACTA aus internationaler Perspektive, abrufbar unter: <http://politik-digital.de/urheberrecht-three-strikes-auf-pruefstand>.

b. Weltorganisation für geistiges Eigentum (WIPO)

Als erster völkerrechtlicher Vertrag zur Regelung des geistigen Eigentums wurde 1883 die **Konvention von Paris zum Schutz Industriellen Eigentums** (Pariser Verbandsübereinkunft) geschlossen¹³⁰⁴, um Inhabern geistiger Werke in Form von gewerblichen Schutzrechten eines Staates, auch in anderen Staaten Schutz zu gewähren.¹³⁰⁵ Darauf folgte im Jahr 1886 die **Konvention von Bern zum Schutz von Werken der Literatur und der Kunst** (Berner Übereinkunft).¹³⁰⁶ Ziel dieser Übereinkunft war es, den Staatsangehörigen der Mitgliedstaaten, einen internationalen Schutz für ihr Recht zu gewähren, die Nutzung ihrer kreativen Werke zu kontrollieren und für diese ein Entgelt zu erhalten.¹³⁰⁷ Diese Verträge führten zur Gründung des Pariser Verbandes und des Berner Verbandes, aus denen auf Grundlage des **Stockholmer Übereinkommens zur Errichtung der Weltorganisation für geistiges Eigentum**¹³⁰⁸ die WIPO entstand.¹³⁰⁹ Die WIPO ist eine Sonderorganisation der Vereinten Nationen. Sie widmet sich der Entwicklung eines ausgewogenen und zugänglichen internationalen System des geistigen Eigentums, welches Kreativität belohnt, Innovation fördert und einen Beitrag zur Förderung der wirtschaftlichen Entwicklung unter Wahrung des öffentlichen Interesses leistet.¹³¹⁰

Unter dem Dach der WIPO wurden zwei Verträge, der **WIPO-Urheberrechtsvertrag (WCT)**¹³¹¹ und der **WIPO-Vertrag über Darbietungen und Tonträger (WPPT)**¹³¹², angenommen. Mit dem **WCT** wurde im Wesentlichen die Berner Übereinkunft an die Möglichkeiten des Internets und die fortschreitende Digitalisierung angepasst.¹³¹³ Er ist ein Sonderabkommen i.S.d. Art. 20 der Berner Übereinkunft und enthält inhaltliche Ergänzungen und Klarstellungen zu diesem. Der WCT kann das Schutzniveau der Berner Übereinkunft nicht unterlaufen, wohl aber erhöhen (Art. 1 Abs. 2, 4 WCT).¹³¹⁴ Im Hinblick auf den Ausbau des Urheberrechts wegen neuer digitaler Technologien wurde vor allem das neuartige Recht der öffentlichen Zugänglichmachung eingeführt (Art. 8 WCT).¹³¹⁵ Eine Ergänzung des Rom-Abkommens¹³¹⁶ stellt der **WPPT** dar¹³¹⁷, der wiederum die Leistungs-

¹³⁰⁴ Fink/Cole/Keber, Rn. 124.

¹³⁰⁵ WIPO, About WIPO- WIPO Treaties – General Information, abrufbar unter: <http://www.wipo.int/treaties/en/general/>.

¹³⁰⁶ Fink/Cole/Keber, Rn. 124.

¹³⁰⁷ WIPO, About WIPO- WIPO Treaties – General Information, abrufbar unter: <http://www.wipo.int/treaties/en/general/>.

¹³⁰⁸ Text abgedruckt bei Fink/Schwartzmann/Cole/Keber, Europäisches und Internationales Medienrecht – Vorschriftensammlung, B 30.

¹³⁰⁹ Fink/Cole/Keber, Rn. 400.

¹³¹⁰ WIPO, About WIPO- What is WIPO?, abrufbar unter: http://www.wipo.int/about-wipo/en/what_is_wipo.html.

¹³¹¹ WIPO Copyright Treaty v. 20.12.1996, in Kraft getreten am 6.3.2002, ABI 2000 L 89, 8.

¹³¹² WIPO Performances and Phonograms Treaty v. 20.12.1996, in Kraft getreten am 20.5.2002, ABI. 2000 L 89, 15.

¹³¹³ Schwartzmann, Private im Völkerrecht, S. 127.

¹³¹⁴ Schwartzmann, Private im Völkerrecht, S. 128.

¹³¹⁵ Hennemann, S. 61 f.

¹³¹⁶ Siehe S.272.

¹³¹⁷ Schwartzmann, Private im Völkerrecht, S. 128; Katzenberger in Schrickler, Urheberrecht, Vor §§ 120 ff. Rz. 84.

schutzrechte der ausübenden Künstler und der Tonträgerhersteller an das digitale Zeitalter angepasst hat.¹³¹⁸

c. Welturheberrechtsabkommen

Das **Welturheberrechtsabkommen**¹³¹⁹ (WUA), das unter der Organisation der Vereinten Nationen für Bildung, Wissenschaft und Kultur (UNESCO) entstanden ist, hat kaum Bedeutung, da gem. Art. XVII WUA die Berner Übereinkunft unter dessen Mitgliedstaaten Vorrang genießt.¹³²⁰

d. Rom-Abkommen

Das Rom-Abkommen¹³²¹ ist als erste mehrseitige internationale Übereinkunft, die den Leistungsschutz der ausübenden Künstler bezweckt, am 18.5.1964 in Kraft getreten.¹³²² Es ist denjenigen Staaten zugänglich, die Mitglieder des Welturheberrechtsabkommens¹³²³ oder der Berner Übereinkunft¹³²⁴ sind (Art. 23, 24 Abs. 2, 28 Abs. 4 des Rom-Abkommens).¹³²⁵ Derzeit gehören dem Abkommen 91 Staaten an, darunter seit 1966 auch Deutschland.¹³²⁶ Der durch das Abkommen gewährte Schutz beinhaltet eine Inländerbehandlung für ausländische Künstler in Deutschland, d.h., dass diese gemäß Art. 2 Abs. 1 lit. a des Rom-Abkommens grundsätzlich den gleichen Schutz beanspruchen können, der deutschen Staatsangehörigen für ihre hier erfolgten, gesendeten oder erstmals festgelegten Darbietungen gewährt wird.¹³²⁷

e. Welthandelsorganisation (WTO)

Das **TRIPS**-Übereinkommen¹³²⁸ führte erstmals Regeln für geistiges Eigentum in das multilaterale Handelssystem der WTO ein.¹³²⁹ Es enthält vornehmlich Bestimmungen über die Instrumente zur Durchsetzung der Rechte des geistigen Eigentums, die gemeinsame, in-

¹³¹⁸ Hennemann, S. 62.

¹³¹⁹ Welturheberrechtsabkommen vom 6.9.1952. Für Deutschland verbindlich in der revidierten Pariser Fassung v. 24.7.1971, BGBl. 1973 II, S. 1111 ff.

¹³²⁰ Schwartmann, Private im Völkerrecht, S. 124; Fink/Cole/Keber, Rn. 401.

¹³²¹ Internationale Abkommen über den Schutz der ausübenden Künstler, der Hersteller von Tonträgern und der Sendeunternehmen v. 26.10.1961, BGBl. 1965 II, S. 1245.

¹³²² Braun/v. Welser in Wandtke/Bullinger, § 125 Rn. 16.

¹³²³ Dazu S. 272.

¹³²⁴ Dazu S. 271.

¹³²⁵ Schwartmann, Private im Völkerrecht, S. 125.

¹³²⁶ WIPO, About WIPO- Treaties and Contracting Parties, abrufbar unter: http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=17.

¹³²⁷ Braun/v. Welser in Wandtke/Bullinger, § 125 Rn. 23.

¹³²⁸ Übereinkommen über handelsbezogene Aspekte der Rechte am geistigen Eigentum (*Agreement on Trade-Related Aspects of Intellectual Property Rights, TRIPS*).

¹³²⁹ World Trade Organization, *Understanding the WTO: The Agreements, Intellectual property: protection and enforcement*, abrufbar unter: http://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm7_e.htm.

ternational gültige Normen sind und in allen Mitgliedstaaten umgesetzt wurden.¹³³⁰ Deutschland ist nach Art. 41, 45 TRIPS zu einem effektiven Urheberrechtsschutz und der Ermöglichung angemessenen Schadensersatzes bei Rechtsverletzungen verpflichtet.¹³³¹

f. *Anti-Counterfeiting Trade Agreement (ACTA)*

Im Jahr 2007, angestoßen durch die damalige Handelsbeauftragte der USA, die Europäische Kommission und das japanische Außenministerium,¹³³² hat die Europäische Union mit zahlreichen anderen Staaten¹³³³ von Juni 2008 bis Oktober 2011 das Übereinkommen zur Bekämpfung von Produkt- und Markenpiraterie (ACTA)¹³³⁴ ausgehandelt.¹³³⁵ Im November 2010 wurden die Verhandlungen beendet und Anfang Dezember 2010 eine endgültige Version des Abkommens vorgelegt. Seit dem 01. Mai 2011 liegt das Abkommen gemäß Art. 39 ACTA zur Unterzeichnung auf, wobei sechs Ratifikationen nötig sind, bevor die Vereinbarung gem. Art. 40 ACTA in Kraft treten kann.¹³³⁶

Ziel des Übereinkommens ist es, einen multilateralen Vertrag zu schließen, um die globalen Standards für die Durchsetzung der Rechte am geistigen Eigentum und die effektive Bekämpfung des Handels mit gefälschten Waren und Raubkopien, zu verbessern.¹³³⁷ Dieses Ziel soll durch internationale Zusammenarbeit, Durchsetzungsverfahren und Festlegung eines Rechtsrahmens für die Durchsetzung von Rechten des geistigen Eigentums in verschiedenen Bereichen, insbesondere im digitalen Umfeld, erreicht werden.¹³³⁸ Der genaue Inhalt des Abkommens wurde zunächst geheim gehalten und eine erste Stellungnahme zu den Verhandlungen erst im April 2009 veröffentlicht. Daher wurde in der Öffentlichkeit über Regelungen zur Sperrung des Internetzugangs im Sinne eines Three-Strikes-Modells ebenso wie über Regelungen zur Providerhaftung spekuliert¹³³⁹ und das nicht bekannte Abkommen bereits bewertet.¹³⁴⁰ Der im April 2010 veröffentlichte konsolidierte

¹³³⁰ Erwägungsgrund 5 der Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums v. 29.4.2004.

¹³³¹ Hennemann, S. 61.

¹³³² Hennemann, S. 354.

¹³³³ Australien, Kanada, Japan, Korea, Mexiko, Marokko, Neuseeland, Singapur, Schweiz und USA.

¹³³⁴ *Anti-Counterfeiting Trade Agreement*.

¹³³⁵ Uerpman-Witzack, Das Anti-Counterfeiting Trade Agreement (ACTA) als Prüfstein für die Demokratie in Europa, Archiv des Völkerrechts, Bd. 49 (2011), S. 103-123 (103), S. 1.

¹³³⁶ Uerpman-Witzack, Das Anti-Counterfeiting Trade Agreement (ACTA) als Prüfstein für die Demokratie in Europa, Archiv des Völkerrechts, Bd. 49 (2011), S. 103-123 (103).

¹³³⁷ Stellungnahme des Europäischen Datenschutzbeauftragten zu den laufenden Verhandlungen der Europäischen Union über ein Abkommen zur Bekämpfung von Produkt- und Markenpiraterie (*Anti-Counterfeiting Trade Agreement*, ACTA), (2010/C 147/01), Rz.: 6, v. 5.6.2010, abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:147:0001:0013:DE:PDF>.

¹³³⁸ Europäische Kommission „*Intellectual property, Anti-Counterfeiting*“, abrufbar unter: <http://ec.europa.eu/trade/creating-opportunities/trade-topics/intellectual-property/anti-counterfeiting/>.

¹³³⁹ Uerpman-Witzack, Das Anti-Counterfeiting Trade Agreement (ACTA) als Prüfstein für die Demokratie in Europa, S. 103.

¹³⁴⁰ Hennemann, S. 355 m.w.N; siehe v.a. die Stellungnahme des Europäischen Datenschutzbeauftragten zu den laufenden Verhandlungen der Europäischen Union über ein Abkommen zur Bekämpfung von Produkt- und Markenpiraterie (*Anti-Counterfeiting Trade Agreement*, ACTA).

Entwurf des Abkommens¹³⁴¹, sah zwar Vorschriften zur Haftung von Internet Service Providern, nicht aber ein Three-Strikes-Modell vor.¹³⁴²

Seit dem 3. Dezember 2010 liegt der endgültige Vertragstext¹³⁴³ vor, in dem zuvor vorgesehene Regelungen liberalisiert wurden.¹³⁴⁴

Abschnitt 5 des 2. Kapitels regelt die „Durchsetzung der Rechte des geistigen Eigentums im digitalen Umfeld“.¹³⁴⁵ Dort zeigt Art. 27 den Rechtsrahmen der Urheberrechtsdurchsetzung im Internet auf. Nach Abs. 1 soll jede Vertragspartei

„sicherstellen, dass Durchsetzungsverfahren, in dem in den Abschnitten 2 (Zivilrechtliche Durchsetzung) und 4 (Strafrechtliche Durchsetzung) benannten Umfang, unter ihrem nationalen Recht verfügbar sind, um effektive Maßnahmen zu gestatten gegen eine Verletzung von Immaterialgüterrechten, welche im digitalen Umfeld stattfindet, inklusive unmittelbare Rechtsschutzmöglichkeiten, um Rechtsverletzungen zu verhindern, und Rechtsschutzmöglichkeiten, die eine Abschreckung vor zukünftigen Rechtsverletzungen darstellen.“¹³⁴⁶

In Abs. 2 heißt es:

„Unbeschadet von Absatz 1 sollen die Durchsetzungsverfahren jeder Vertragspartei Anwendung finden auf Verletzungen von „copyright“ und verwandten Rechten mittels digitalen Netzwerken, welche den illegalen Einsatz von Maßnahmen eines weitreichenden Vertriebs zum Zwecke von Rechtsverletzungen umfassen können. Diese Verfahren sollen in einer derartigen Weise umgesetzt werden, die die Schaffung von Hindernissen für legale Aktivitäten, inklusive dem elektronischen Handel, verhindert und in Übereinstimmung mit dem Recht der Vertragspartei, elementare Prinzipien, wie etwa Meinungsäußerungsfreiheit, faires Verfahren und Privatsphäre, bewahrt.

In der Fußnote dazu heißt es:

„Zum Beispiel, unbeschadet des {nationalen} Rechts einer Vertragspartei, ein Regime einführen oder beibehalten, das Beschränkungen der Haftung von, oder verfügbaren Rechtsschutz gegen, Internet Service Provider gewährleistet, wobei die legitimen Interessen von Rechtsinhabern gewahrt werden.“¹³⁴⁷

Während der Entwurf in einer Option die Diensteanbieter nur aus einer Haftung entließ, wenn sie Maßnahmen gegen das unerlaubte Speichern und Übertragen urheberrechtlich

¹³⁴¹ *Anti-Counterfeiting Trade Agreement, Consolidated Text, Prepared for Public Release*, abrufbar unter: http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc_146029.pdf.

¹³⁴² Hennemann, S. 356.

¹³⁴³ Abrufbar unter: http://trade.ec.europa.eu/doclib/docs/2011/may/tradoc_147937.pdf.

¹³⁴⁴ Uerpman-Witzack, Das Anti-Counterfeiting Trade Agreement (ACTA) als Prüfstein für die Demokratie in Europa, S. 105.

¹³⁴⁵ Sec. 5 ACTA, „Enforcement of Intellectual Property Rights in the Digital Environment“.

¹³⁴⁶ Übersetzung von Hennemann, S. 356 f.

¹³⁴⁷ Übersetzung von Hennemann, S. 357.

geschützter Inhalte ergreifen, sieht Art. 27 Abs. 3 ACTA nur noch eine allgemeine Pflicht der Vertragsparteien vor, sich um die Förderung einer Zusammenarbeit der Geschäftswelt zum Schutz von Urheberrechten zu bemühen.

Die Norm stellt diese Verpflichtung aber zugleich unter einen Menschenrechtsvorbehalt im Hinblick auf die Wahrung von Meinungsfreiheit, fairem Verfahren und Privatheit.¹³⁴⁸ In Abs. 3 heißt es insoweit:

„Jede Vertragspartei soll anstreben, kooperative Anstrengungen innerhalb der Wirtschaft voranzutreiben, um effizient Verletzungen von {...} „copyright“ und verwandten Rechten zu begegnen, wobei legitimer Wettbewerb, und, in Übereinstimmung mit dem Recht der Vertragspartei, elementare Prinzipien, wie etwa Meinungsäußerungsfreiheit, faires Verfahren und Privatsphäre, gewahrt werden.“¹³⁴⁹

In Art. 27 Abs. 4 ACTA ist eine Regelung enthalten, nach der die Vertragsparteien einen **Auskunftsanspruch** der Rechteinhaber gegen die Diensteanbieter vorsehen können, wobei dieser von einer hinreichend substantiierten Behauptung einer Rechtsverletzung sowie einer gerichtlichen oder behördlichen Anordnung abhängig gemacht wird. Abs. 4 lautet:

„Eine Vertragspartei kann, in Übereinstimmung mit ihren Gesetzen und Verordnungen, ihre zuständigen {staatlichen Einrichtungen} mit der Befugnis ausstatten, einen Internet Service Provider zu verpflichten, unmittelbar gegenüber einem Rechteinhaber Informationen offenzulegen, die erforderlich sind, um einen Kunden zu identifizieren, dessen Nutzerkonto vorgeblich für Rechtsverletzungen genutzt wurde, und der Rechteinhaber eine entsprechende Forderung betreffend eine Verletzung von {...}, „copyright“ oder verwandten Rechten geltend gemacht hat, und die entsprechenden Informationen zu dem Zwecke des Schutzes oder der Durchsetzung der benannten Rechte verlangt wird. Diese Verfahren sollen in einer derartigen Weise umgesetzt werden, die die Schaffung von Hindernissen für legale Aktivitäten, inklusive dem elektronischen Handel, verhindert und, in Übereinstimmung mit dem Recht der Vertragspartei, elementare Prinzipien, wie etwa Meinungsäußerungsfreiheit, faires Verfahren und Privatsphäre, bewahrt.“¹³⁵⁰

Diese „Kann“-Regelung bleibt bereits hinter dem europäischen und deutschen Recht zurück, da hier die Rechteinhaber schon nach § 101 Abs. 2 Nr. 3, Abs. 9 UrhG, der in Umsetzung der Enforcement-Richtlinie¹³⁵¹ erlassen wurde, eine entsprechende gerichtliche Anordnung gegen die Zugangsanbieter erwirken können.¹³⁵²

¹³⁴⁸ *Uerpmann-Witzack*, Das Anti-Counterfeiting Trade Agreement (ACTA) als Prüfstein für die Demokratie in Europa, S. 106 f.

¹³⁴⁹ Übersetzung von *Hennemann*, S. 357.

¹³⁵⁰ Übersetzung von *Hennemann*, S. 357.

¹³⁵¹ Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums v. 29.4.2004, dazu unter II . 3.

¹³⁵² *Uerpmann-Witzack*, Das Anti-Counterfeiting Trade Agreement (ACTA) als Prüfstein für die Demokratie in Europa, S. 106.

g. Europarat

Für die Mitgliedsstaaten des Europarats ist der Schutz des Eigentums in Art. 1 des 1. Zusatzprotokolls zur **Europäischen Menschenrechtskonvention EMRK**¹³⁵³ (1. ZP-EMRK) normiert, wobei nach allgemeiner Auffassung in Rechtsprechung und Literatur davon auch der Schutz des geistigen Eigentums umfasst wird.¹³⁵⁴

2. Recht der Europäischen Union

a. Charta der Grundrechte der europäischen Union (EU-Grundrechtecharta)¹³⁵⁵

Auf unionsrechtlicher Ebene stützt sich der Grundrechtsschutz einerseits auf die Grundrechte, wie sie in der EMRK gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten als allgemeine Grundsätze des Gemeinschaftsrechts ergeben und zum anderen auf die EU-Grundrechtecharta.¹³⁵⁶ Dort ist der Schutz des geistigen Eigentums ausdrücklich in Art. 17 Abs. 2 EU-Grundrechtecharta geschützt, die von EuGH und EuG seit dem Jahr 2000 zunehmend herangezogen werden, um deren Auffassung zu bekräftigen.¹³⁵⁷

b. InfoSoc-Richtlinie (2001/29/EG)¹³⁵⁸

Ziel der InfoSoc-Richtlinie war die Anpassung der Vorschriften für das Urheberrecht und die verwandten Schutzrechte an die technologische Entwicklung und insbesondere die Informationsgesellschaft.¹³⁵⁹ Die EG setzte darin die Verpflichtungen um, die sich für sie aus der Ratifikation der WIPO-Verträge ergaben¹³⁶⁰ Die InfoSoc-Richtlinie hat auch das deut-

¹³⁵³ Zusatzprotokoll zur Konvention zum Schutze der Menschenrechte und Grundfreiheiten SEV-Nr. : 009, v. 20.3.1952, abrufbar unter: <http://conventions.coe.int/Treaty/ger/Treaties/Html/009.htm>.

¹³⁵⁴ Prof. Dr. Peter M. Huber, Geistiges Eigentum und uniales Wettbewerbsrecht, abrufbar unter: http://www.jura.uni-muenchen.de/personen/huber_peter/publikationen/geistigeseigentum.pdf; EKMR Requête No 12633/87, DR 66 (1990), 70/79 – Smith Kline et French Laboratoires Ltd; Chr. Grabenwarter, Europäische Menschenrechtskonvention, 2. Aufl., 2005, § 25 Rdnr. 4; allgemeine zum Eigentumsschutz nach der EMRK: EGMR vom 23. Februar 1995, Serie A, Bd. 306, Nr. 53, S. 46 – Gasus Dosier und Fördertechnik GmbH; EGMR, EuGRZ 1988, 35 van Marle u. a. / Niederlande; W. Peukert, in: Frowein/Peukert, Europäische Menschenrechtskonvention, 2. Aufl., 1996, Art. 1 1.ZP, Rn. 4.

¹³⁵⁵ (2000/C 364/01) v. 7.12.2000, abrufbar unter: http://www.europarl.europa.eu/charter/pdf/text_de.pdf.

¹³⁵⁶ Siehe S. 295.

¹³⁵⁷ Peter M. Huber, Geistiges Eigentum und uniales Wettbewerbsrecht, abrufbar unter: http://www.jura.uni-muenchen.de/personen/huber_peter/publikationen/geistigeseigentum.pdf unter Verweis auf: EuG, Rs. T – 54/99, max.mobil Telekommunikation Service GmbH / Kommission, Slg. 2002, II – 313, Rz. 48, 57; I. Pernice/ F. C. Mayer, in: Grabitz/Hilf (Hrsg.), Das Recht der Europäischen Union, nach Art.6 EUV, Rz. 24 f. (2002) m. w. N. zur Heranziehung der Grundrechtecharta durch die Generalanwälte.

¹³⁵⁸ Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft v. 22.5.2001, abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:167:0010:0019:DE:PDF>.

¹³⁵⁹ Europäische Kommission, Urheberrecht in der Informationsgesellschaft, abrufbar unter: http://ec.europa.eu/internal_market/copyright/copyright-infso/copyright-infso_de.htm.

¹³⁶⁰ Fink/Cole/Keber, Rn. 124.

sche Urheberrecht maßgeblich geprägt¹³⁶¹, welches im Rahmen des sog. ersten und zweiten Korb den europarechtlichen Vorgaben angepasst wurde.¹³⁶²

c. Enforcement-Richtlinie (2004/48/EG)

Die Enforcement-Richtlinie¹³⁶³ enthält die maßgeblichen europarechtlichen Vorgaben für die Durchsetzung des Urheberrechts. Sie sieht diejenigen Maßnahmen, Verfahren und Rechtsbehelfe vor, die zur Sicherstellung der Durchsetzung der Rechte am geistigen Eigentum erforderlich sind (Art. 1 S.1 2004/48/EG). Die wesentliche Regelung der Richtlinie ist das in Art. 8 enthaltene **Recht auf Auskunft**.¹³⁶⁴ Nach diesem haben die Mitgliedstaaten sicherzustellen, dass die zuständigen Gerichte in einem Verfahren wegen Verletzung des geistigen Eigentums eine Anordnung erlassen können, nach der der Rechteverletzer oder an der Rechtsverletzung in bestimmten Formen beteiligte Dritte, Auskunft über den Ursprung und die Vertriebswege der rechtsverletzenden Waren oder Dienstleistungen erteilen müssen. Das Recht auf Auskunft gegen den Internetprovider ist dabei in Art. 8 Abs. 1 lit. c 2004/48/EG verankert¹³⁶⁵, nach dem

„Auskünfte [...], von [...] jeder anderen Person erteilt werden, die nachweislich für rechtsverletzende Tätigkeiten genutzte Dienstleistungen in gewerblichem Ausmaß erbrachte“.

Als Rechtsfolgen einer gerichtlichen Feststellung der Rechtsverletzung sieht die Richtlinie etwa Rückruf, Entfernung und Vernichtung, Schadensersatz und die Veröffentlichung von Gerichtsentscheidungen vor (Art. 10 – 15 2004/48/EG).

d. Telekom-Paket

Noch im April 2008 hat das Europäische Parlament in einer Entschließung zur Kulturwirtschaft in Europa¹³⁶⁶ die Europäische Kommission und die Mitgliedstaaten dazu aufgefordert

„[...] keine Maßnahmen zu ergreifen, die im Widerspruch zu den bürgerlichen Freiheiten und den Menschenrechten sowie den Grundsätzen der Verhältnismäßigkeit, der Effizienz und der Abschreckung stehen, wie z.B. die Unterbrechung des Internet-Zugangs“.¹³⁶⁷

¹³⁶¹ Hennemann, S. 53.

¹³⁶² Fink/Cole/Keber, Rn. 124.

¹³⁶³ Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums v. 29.4.2004.

¹³⁶⁴ Hennemann, S. 51.

¹³⁶⁵ Hennemann, S. 52.

¹³⁶⁶ Entschließung des Europäischen Parlaments vom 10. April 2008 zur Kulturwirtschaft in Europa (2007/2153(INI)), abrufbar unter: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0123+0+DOC+XML+V0//DE>.

¹³⁶⁷ Erwägungsgrund Y Nr. 23 der Entschließung des Europäischen Parlaments vom 10. April 2008 zur Kulturwirtschaft in Europa (2007/2153(INI)), abrufbar unter:

Hingegen wurde in den im November 2009 beschlossenen Richtlinien zu elektronischen Kommunikationsnetzen („Telekom-Paket“¹³⁶⁸) die Einführung von Internetsperren – durch die Festlegung von Mindeststandards – befürwortet.¹³⁶⁹

Art. 1 Abs. 3a S. 1 der Rahmenrichtlinie¹³⁷⁰ sagt insoweit:

„Maßnahmen der Mitgliedstaaten betreffend den Zugang zu oder die Nutzung von Diensten und Anwendungen über elektronische Kommunikationsnetze durch die Endnutzer wahren die in der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten sowie den allgemeinen Grundsätzen des Gemeinschaftsrechts verankerten Grundrechte und -freiheiten natürlicher Personen.“

In Art. 1 Abs. 3a S. 2-5 der Rahmenrichtlinie heißt es weiter:

„Alle diese Maßnahmen betreffend den Zugang zu oder die Nutzung von Diensten und Anwendungen über elektronische Kommunikationsnetze durch die Endnutzer, die diese Grundrechte und -freiheiten einschränken können, dürfen nur dann auferlegt werden, wenn sie im Rahmen einer demokratischen Gesellschaft angemessen, verhältnismäßig und notwendig sind, und ihre Anwendung ist angemessenen Verfahrensgarantien im Einklang mit der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten sowie den allgemeinen Grundsätzen des Gemeinschaftsrechts zu unterwerfen, einschließlich des Rechts auf effektiven Rechtsschutz und ein faires Verfahren. Dementsprechend dürfen diese Maßnahmen nur unter gebührender Beachtung des Grundsatzes der Unschuldsvermutung und des Rechts auf Schutz der Privatsphäre ergriffen werden. Ein vorheriges, faires und unparteiisches Verfahren, einschließlich des Rechts der betroffenen Person(en) auf Anhörung, wird gewährleistet, unbeschadet des Umstandes, dass in gebührend begründeten Dringlichkeitsfällen geeignete Bedingungen und Verfahrensvorkehrungen im Einklang mit der Europäischen Konvention zum Schutze der Menschen-

<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0123+0+DOC+XML+V0//DE>.

¹³⁶⁸ Telekom-Reformpaket zur Schaffung eines neuen Rechtsrahmens für die elektronische Kommunikation: Richtlinie 2009/140/EG zur Änderung der Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, der Richtlinie 2002/19/EG über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung und der Richtlinie 2002/20/EG über die Genehmigung elektronischer Kommunikationsnetze und -dienste v. 25. 11.2009 (Änderungsrichtlinie); Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz Text von Bedeutung für den EWR; Verordnung (EG) Nr. 1211/2009.

¹³⁶⁹ Hennemann, S. 236.

¹³⁷⁰ Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste v. 7.3.2002, geändert durch Richtlinie 2009/140/EG zur Änderung der Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, der Richtlinie 2002/19/EG über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung und der Richtlinie 2002/20/EG über die Genehmigung elektronischer Kommunikationsnetze und -dienste v. 25. 11.2009.

rechte und Grundfreiheiten notwendig sind. Das Recht auf eine effektive und rechtzeitige gerichtliche Prüfung wird gewährleistet.“

Im Ergebnis setzt die Einführung von Internetsperren demnach die Wahrung der Grundrechte sowie die Grundsätze der Verhältnismäßigkeit, des effektiven Rechtsschutzes und des fairen Verfahrens voraus und stellt eine Option dar.¹³⁷¹

Darüber hinaus begrenzt die **Universaldienstrichtlinie**¹³⁷² Urheberrechtsverletzungen durch Verbraucher in kleinem Maßstab. Dazu gehört, dass die Mitgliedstaaten verpflichtet sind, standardisierte Informationen von öffentlichem Interesse zu verschiedenen Themen, insbesondere Urheberrechtsverletzungen und ihre Folgen, zu erstellen, deren Verbreitung sie dann von den Zugangsanbietern verlangen können.¹³⁷³

e. Art. 8 Abs. 1 Rom II-VO¹³⁷⁴

Nach Art. 8 Abs. 1 Rom II-VO ist auf außervertragliche Schuldverhältnisse aus einer Verletzung von Rechten des geistigen Eigentums das Recht des Staates anzuwenden, für den der Schutz beansprucht wird. Damit hat sich der europäische Gesetzgeber für das sog. Schutzlandprinzip entschieden.¹³⁷⁵

f. Rechtsprechung des EuGH – Scarlet Extended

Der Europäische Gerichtshof hat in der Entscheidung Scarlet Extended¹³⁷⁶ seine Rechtsprechung bekräftigt¹³⁷⁷, wonach das geistige Eigentum, das Bestandteil der Eigentumsgarantie¹³⁷⁸ ist, den besonderen Schutz des Europarechts genießt.¹³⁷⁹ Darüber hinaus hat der

¹³⁷¹ Hennemann, S. 237.

¹³⁷² Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten v. 7.3.2002, geändert durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz Text von Bedeutung für den EWR.

¹³⁷³ Stellungnahme des Europäischen Datenschutzbeauftragten zu den laufenden Verhandlungen der Europäischen Union über ein Abkommen zur Bekämpfung von Produkt- und Markenpiraterie (Anti-Counterfeiting Trade Agreement, ACTA), (2010/C 147/01) v. 5.6.2010, Rz. 37; Vgl. Art. 21 Abs. 4 der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten v. 7.3.2002, geändert durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz Text von Bedeutung für den EWR.

¹³⁷⁴ Verordnung (EG) Nr. 864/2007 über das auf außervertragliche Schuldverhältnisse anzuwendende Recht („Rom II“) v. 11.7.2007, abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:199:0040:0049:DE:PDF>.

¹³⁷⁵ Hennemann, S. 57; v. Welser in Wandtke/Bullinger, Vor §§ 120 ff. UrhG Rn. 3.

¹³⁷⁶ EuGH, Urteil v. 24.11.2011, Az.: C- 70/10.

¹³⁷⁷ L’Oreal C-324/09 v. 12.7.2011.

¹³⁷⁸ EuGH, Urteil v. 24.11.2011, Az.: C- 70/10. Art. 17 Abs. 1 GRCh. Zif. 44.

EuGH eine einseitige und umfassende Filterverpflichtung zulasten der Provider für unzulässig erklärt, aber das Erfordernis eines effektiven Urheberrechtsschutzes in den Mitgliedstaaten betont.¹³⁸⁰ Den Vermittlern könnten Maßnahmen aufgegeben werden, die nicht nur begangene Rechtsverletzungen beenden, sondern auch neuen Verletzungen vorbeugen.¹³⁸¹ Der EuGH mahnte zudem eine Abwägung der Eigentümerinteressen der Rechteinhaber mit der unternehmerischen Freiheit der Provider an. Damit wurde eine **einseitige Lösung zugunsten der Rechteinhaber** vom EuGH **abgelehnt**. Nach der Logik der Entscheidung sind aber auch **Provider in der Pflicht**, sich an einem Modell zum Schutz des geistigen Eigentums zu beteiligen, das sowohl präventiv als repressiv ansetzen kann. Den Mitgliedstaaten ist es nach dem Urteil unbenommen, ein System zum Schutz des geistigen Eigentums zu wählen, das Rechteinhaber und Provider in Anspruch nimmt.¹³⁸²

3. Rechtspolitische Initiativen der Europäischen Union

a. *Mitteilung zur „Verbesserung der Durchsetzung von Rechten des geistigen Eigentums im Binnenmarkt“*

Auf europäischer Ebene gibt es eine Reihe rechtspolitischer Diskussionen zur effektiven Durchsetzung von Urheberrechten, die die Bemühungen zeigen, den Urheberrechtsschutz angemessen auszugestalten.¹³⁸³ Hierzu gehört zunächst die von der Europäischen Kommission 2009 veröffentlichte **Mitteilung zur „Verbesserung der Durchsetzung von Rechten des geistigen Eigentums im Binnenmarkt“**¹³⁸⁴, laut der die Kommission Urheberrechtsverletzungen durch nicht legislative Maßnahmen bekämpfen will, wie etwa der Einrichtung einer „EU-Beobachtungsstelle für Marken- und Produktpiraterie“, die auch gegen illegale Downloads im Internet vorgehen soll.¹³⁸⁵

b. *Grünbuch „Erschließung des Potenzials der Kultur- und Kreativindustrien“*

Im April 2010 veröffentlichte die Europäische Kommission darüber hinaus das **Grünbuch „Erschließung des Potenzials der Kultur- und Kreativindustrien“**.¹³⁸⁶ In diesem wies sie darauf hin, dass die EU, um wettbewerbsfähig bleiben zu können, Rahmenbedingungen schaffen müsse,

¹³⁷⁹ EuGH, Urteil v. 24.11.2011, Az.: C- 70/10. Art. 17 Abs. 2 GRCh. Zif. 43.

¹³⁸⁰ EuGH, Urteil v. 24.11.2011, Az.: C- 70/10., Zif. 30.

¹³⁸¹ EuGH, Urteil v. 24.11.2011, Az.: C- 70/10., Zif. 31.

¹³⁸² *Schwartmann*, Provider müssen nicht auf ihre Kosten filtern und sperren, Legal Tribune Online v. 24.11.2011, abrufbar unter: <http://www.lto.de/de/html/nachrichten/4892/eugh-zum-urheberrechtsschutz-provider-muss-nicht-auf-ihre-kosten-filtern-und-sperren/>.

¹³⁸³ *Hennemann*, S. 351.

¹³⁸⁴ KOM (2009) 467.

¹³⁸⁵ *Hennemann*, S. 351.

¹³⁸⁶ KOM (2010) 183, abrufbar unter:

http://ec.europa.eu/culture/documents/greenpaper_creative_industries_de.pdf.

„damit Kreativität und Innovation innerhalb einer neuen unternehmerischen Kultur florieren können“.¹³⁸⁷

Insbesondere müssten die Kultur- und Kreativindustrien *„die Chancen kultureller Diversität, von Globalisierung und Digitalisierung, die die weitere Entwicklung dieser Industrien antreiben, optimal nutzen können“*.¹³⁸⁸ Für diese Industrie-Zweige müsse eine bessere Durchsetzung von Rechten des geistigen Eigentums durch die Rahmenbedingungen gewährleistet werden.¹³⁸⁹

c. Eine digitale Agenda für Europa

Mit der darauffolgend erschienen Mitteilung **„Eine digitale Agenda für Europa“**¹³⁹⁰ hat die Kommission zu Maßnahmen der Urheberrechtsdurchsetzung im digitalen Zeitalter Stellung bezogen und diesbezüglich einen konkreten Zeitplan aufgezeigt. Dabei sieht die Kommission auch eine Überprüfung der Enforcement-Richtlinie unter Berichterstattung *„über die Notwendigkeit zusätzlicher Maßnahmen zur Stärkung des Schutzes vor dauerhaften Verletzungen der Rechte des geistigen Eigentums im Online-Umfeld“*¹³⁹¹ vor.¹³⁹²

d. Gallo-Bericht

Im Juni 2010 nahm der Rechtsausschuss des Europäischen Parlaments und im September 2010 auch das Europäische Parlament den sog. **Gallo-Bericht**¹³⁹³ an, der insbesondere die Problematik von Urheberrechtsverletzungen und – durchsetzungen behandelt. Das Papier betont die Relevanz von Urheberrechtsverletzungen für die europäische Wirtschaft und weist darauf hin, dass die Entwicklung neuer Geschäftsmodelle im Online-Bereich ein erfolgversprechendes Mittel gegen Online-Piraterie sei, so dass legale Downloads gefördert werden sollen. Darüber hinaus sei eine Änderung der Enforcement-Richtlinie in Betracht zu ziehen und der Rechtsausschuss unterstütze die Einrichtung einer Europäischen Beobachtungsstelle für Marken- und Produktpiraterie.¹³⁹⁴

¹³⁸⁷ KOM (2010) 183, S. 2 abrufbar unter:

http://ec.europa.eu/culture/documents/greenpaper_creative_industries_de.pdf.

¹³⁸⁸ KOM (2010) 183, S. 4 abrufbar unter:

http://ec.europa.eu/culture/documents/greenpaper_creative_industries_de.pdf.

¹³⁸⁹ Hennemann, S. 352.

¹³⁹⁰ KOM (2010) 245, abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:DE:PDF>.

¹³⁹¹ KOM 2010, 245 S. 11.

¹³⁹² Hennemann, S. 352.

¹³⁹³ Bericht über die Durchsetzung von Rechten des geistigen Eigentums im Binnenmarkt (2009/2178 (INI)) v. 3.6.2010, Berichterstatterin: Marielle Gallo, abrufbar unter:

http://www.europarl.europa.eu/meetdocs/2009_2014/documents/juri/pr/801/801322/801322de.pdf.

¹³⁹⁴ Hennemann, S. 353.

II. Datenschutzrecht

Die internationalen Rahmenvorgaben für Warnhinweismodelle lassen sich aus der Perspektive des Datenschutzrechts wie folgt umreißen.

1. Völkerrecht

a. Vereinte Nationen und OECD

Im Völkerrecht finden sich allgemeine **Leitsätze des Datenschutzes** in der Richtlinie 45/95 zur Regelung von automatisierten personenbezogenen Dateien der Vereinten Nationen¹³⁹⁵ und den Richtlinien der OECD¹³⁹⁶ über **Datenschutz und grenzüberschreitende Ströme personenbezogener Daten**.¹³⁹⁷ Es handelt sich um unverbindliche Empfehlungen, die aber Rückschlüsse auf einen internationalen Konsens zum Datenschutz zulassen.

b. Europarat

Auf der regionalen Ebene des Europarats gelten das **Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten**¹³⁹⁸ sowie dessen Zusatzprotokoll.¹³⁹⁹ Das Übereinkommen konkretisiert Art. 8 Abs. 1 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) und die dazu ergangene Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR), wonach der Schutz personenbezogener Daten vom Recht auf Achtung des Privatlebens umfasst ist.¹⁴⁰⁰ Die zeichnenden Mitgliedstaaten haben sich im Wege der Datenschutzkonvention verpflichtet, bestimmte Datenschutzgrundsätze, darunter den Grundsatz der Datenverarbeitung nach Treu und Glauben, den Zweckbindungsgrundsatz, das Erforderlichkeitsprinzip sowie den Informationsanspruch des Betroffenen, zu beachten und im nationalen Recht umzusetzen. Besondere Regelungen betreffend das Internet finden sich im 2011 verabschiedeten **Übereinkommen über Computerkriminalität**, das für Deutschland mit Wirkung vom 1. Juli 2009 in Kraft getreten ist. Zielsetzung des Übereinkommens ist eine gemeinsame Strafrechtspolitik zum Schutz der Gesellschaft vor Compu-

¹³⁹⁵ Diese Richtlinie wurde angenommen durch Entschließung der Generalversammlung vom 14.12.1990 und ist abrufbar unter: <http://www.un.org/Depts/german/uebereinkommen/ar45095.pdf>.

¹³⁹⁶ Organisation für wirtschaftliche Zusammenarbeit und Entwicklung.

¹³⁹⁷ Diese Richtlinien traten am 23.09.1980 in Kraft; eine Kurzfassung ist abrufbar unter: <http://www.oecd.org/dataoecd/16/7/15589558.pdf>.

¹³⁹⁸ Vom 28.1.1981, abrufbar unter: <http://conventions.coe.int/treaty/ger/treaties/html/108.htm>.

¹³⁹⁹ Zusatzprotokoll zum Europäischen Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitender Datenverkehr, v. 8.11.2011, abrufbar unter: <http://conventions.coe.int/treaty/ger/treaties/html/181.htm>.

¹⁴⁰⁰ *Keber* in *Schwartzmann*, Praxishandbuch Medienrecht, 18. Kap. Rn. 2.

terkriminalität durch gemeinsame gesetzliche Standards und internationale Zusammenarbeit.¹⁴⁰¹

2. Recht der Europäischen Union

a. Primärrecht

Der unionsrechtliche Grundrechtsschutz stützt sich einerseits auf die Grundrechte, wie sie in der EMRK gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten als allgemeine Grundsätze des Gemeinschaftsrechts ergeben.¹⁴⁰² Mit dem **Vertrag von Lissabon**¹⁴⁰³, der zugleich die Rechtsgrundlage für einen Beitritt der EU zur EMRK enthält,¹⁴⁰⁴ hat die **Charta der Grundrechte der Europäischen Union** (EU-Grundrechtecharta) Verbindlichkeit erlangt.

Datenschutzrechtlich relevante Regelungen finden sich dort in Art. 7 und Art. 8 EU-Grundrechtecharta. Art. 7 EU-Grundrechtecharta normiert das Recht auf **Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation**. Die Vorschrift ist nahezu wortgleich mit Art. 8 EMRK und hat daher die gleiche Bedeutung und Tragweite (Art. 52 Abs. 3 EU-Grundrechtecharta). Das Datenschutzrecht des Art. 8 EU-Grundrechtecharta („Schutz personenbezogener Daten“) ist als konkretere Regelung grundsätzlich *lex specialis*¹⁴⁰⁵ gegenüber Art. 7 EU-Grundrechtecharta und schützt alle Informationen über eine bestimmte oder bestimmbare Person.¹⁴⁰⁶

b. Sekundärrecht

Die Gesetzgebung der EU-Mitgliedstaaten zum Datenschutz wird insbesondere durch **drei Richtlinien** überformt:¹⁴⁰⁷

aa. Allgemeine Datenschutzrichtlinie (95/46/EG)

Die Datenschutzrichtlinie¹⁴⁰⁸ verpflichtet die Mitgliedstaaten, Grundprinzipien für die Verarbeitung personenbezogener Daten in das nationale Recht zu übernehmen, um einen

¹⁴⁰¹ Vgl. hierzu auch die Präambel des Übereinkommens.

¹⁴⁰² *Schwartzmann*, Europäischer Grundrechtsschutz nach dem Verfassungsvertrag AVR 43 (2005), 129 (129 ff.) *Kühling/Seidel/Sivridis*, 1. Kap. B. I. 1., S. 13. Insofern bereits der auf der frühen Rechtsprechung des *EuGH* aufsetzende Art. 6 Abs. 2 EUV a.F.

¹⁴⁰³ In Kraft getreten am 01.12.2009.

¹⁴⁰⁴ Europa Press releases RAPID, Europäische Kommission schlägt Verhandlungsrichtlinien für den Beitritt der Union zur Europäischen Menschenrechtskonvention (EMRK) vor, vom 17.3.2010, abrufbar unter: <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/84&format=HTML&aged=0&language=DE&guiLanguage=en>.

¹⁴⁰⁵ D.h. Art. 8 der EU-Grundrechtecharta ist als spezielleres Gesetz gegenüber Art. 7 EU-Grundrechtecharta vorrangig anzuwenden.

¹⁴⁰⁶ *Kühling/Seidel/Sivridis*, Datenschutzrecht, 1. Kap. B. I. 2 b), S. 17.

¹⁴⁰⁷ *Kühling/Seidel/Sivridis*, Datenschutzrecht, 1. Kap. B. II. 1 a), S. 22.

Ausgleich zwischen dem Schutz der Privatsphäre einerseits und dem freien Verkehr personenbezogener Daten in der EU andererseits zu schaffen.¹⁴⁰⁹ Aufgrund ihrer Anknüpfung an in Deutschland bereits bestehende und auch in der Datenschutzkonvention des Europarats¹⁴¹⁰ bereits enthaltene Regelungsprinzipien, brachte sie für Deutschland keine gravierenden Neuerungen.¹⁴¹¹ Anwendung findet die Richtlinie auf die

„automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen“.¹⁴¹²

Personenbezogene Daten sind gemäß Art. 2 lit. a) der Datenschutzrichtlinie

„alle Informationen über eine bestimmte oder bestimmbare natürliche Person ("betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind“.

Eine **Verarbeitung** dieser Daten ist jeder

„mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten“¹⁴¹³.

Für die Verarbeitung personenbezogener Daten gilt ein **Verbot mit Erlaubnisvorbehalt**. Sie ist nur unter einer der folgenden Voraussetzungen zulässig:¹⁴¹⁴

- wenn der Betroffene eingewilligt hat;
- zur Erfüllung eines Vertrages, wenn der Betroffene Vertragspartei ist oder zur Durchführung vorvertraglicher Maßnahmen auf Antrag des Betroffenen;
- zur Erfüllung einer rechtlichen Verpflichtung, der der für die Verarbeitung Verantwortliche unterliegt;
- zur Wahrung lebenswichtiger Interessen des Betroffenen;

¹⁴⁰⁸ Richtlinie 95/46/EG vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html>.

¹⁴⁰⁹ Vgl. die Zusammenfassung der EU, abrufbar unter: http://europa.eu/legislation_summaries/information_society/l14012_de.htm.

¹⁴¹⁰ Dazu S. 276.

¹⁴¹¹ *Gola/Schomerus* in *Gola/Schomerus*, Bundesdatenschutzgesetz, Einleitung Rn. 10.

¹⁴¹² Art. 3 Abs. 1 der Richtlinie 95/46/EG.

¹⁴¹³ Art. 2 lit. b) der Richtlinie 95/46/EG.

¹⁴¹⁴ Gemäß Art. 7 lit. a)- f) der Richtlinie 95/46/EG.

- zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt;
- zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen wahrgenommen wird.

bb. Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG)¹⁴¹⁵

Eine Ergänzung für den Bereich der Telekommunikation stellt die E-Datenschutzrichtlinie dar, die das **Telekommunikationsgeheimnis** im unionsrechtlichen Sekundärrecht verankert.¹⁴¹⁶ Sie gibt einen Rechtsrahmen für die Verarbeitung personenbezogener Daten im Zusammenhang mit dem Anbieten elektronischer Kommunikationsdienste vor.¹⁴¹⁷ Die Richtlinie unterscheidet im Hinblick auf die Schutzintensität zwischen Verkehrs- (Art. 6) und anderen Standortdaten (Art. 9). Generell dürfen diese Daten nur zu bestimmten Zwecken oder mit Einwilligung des Betroffenen und unter Beachtung besonderer Pflichten verarbeitet werden. Es hat eine Anonymisierung, Sperrung oder Löschung zu erfolgen, sobald der Zweck entfällt.¹⁴¹⁸ Zum Schutz von nationaler und öffentlicher Sicherheit sowie zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten können die Daten, sofern nationale Rechtsvorschriften dies im jeweiligen Mitgliedstaat vorsehen, für eine begrenzte Zeit gespeichert werden (Art. 15 Abs. 1).

cc. Vorratsdatenspeicherungsrichtlinie (2006/24/EG)

Mit der im Frühjahr 2006 in Kraft getretenen **Vorratsdatenspeicherungsrichtlinie**¹⁴¹⁹ soll sichergestellt werden, dass Daten, die von Anbietern öffentlich zugänglicher Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, im Einzelfall zum Zweck der Ermittlung, Feststellung und Verfolgung von schweren Straftaten zur Verfügung stehen.¹⁴²⁰ Dafür normiert die Richtlinie eine Pflicht zur sog. Vorratsdatenspeicherung, d.h. zur **anlasslosen Speicherung bestimmter Kommunikationsdaten**.¹⁴²¹ Ihr Anwendungsbereich bezieht sich auf Verkehrs- und Standortdaten sowie alle damit zusammenhängenden Daten, die der Feststellung des Nutzers dienen (Art. 1 Abs. 2). Nach den Vorgaben der Richtlinie sollen diese Daten für einen Zeitraum von **mindestens sechs Monaten**, im Regelfall jedoch **nicht länger als zwei Jahren** gespei-

¹⁴¹⁵ Richtlinie 2002/58/EG vom 12.07.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (zuletzt geändert durch die Richtlinie 2009/136/EG), abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:DE:PDF> .

¹⁴¹⁶ Kühling/Seidel/Sivridis, Datenschutzrecht, 1. Kap. B. II. 2., S. 39.

¹⁴¹⁷ Vgl. die Zusammenfassung der EU, abrufbar unter:

http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_de.htm .

¹⁴¹⁸ Kühling/Seidel/Sivridis, Datenschutzrecht, 1. Kap. B. II. 3., S. 44.

¹⁴¹⁹ Richtlinie 2006/24/EG vom 15.03.2006 über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:DE:PDF> .

¹⁴²⁰ Vgl. Art. 1 Abs. 1 der Richtlinie 2006/24/EG.

¹⁴²¹ Vgl. Art. 3 der Richtlinie 2006/24/EG.

chert werden (Art. 6). Ein Mitgliedstaat kann diese maximal zulässige Speicherdauer jedoch bei Vorliegen besonderer Gründe überschreiten (Art. 12 Abs. 1).

Die Richtlinie zur Vorratsdatenspeicherung wurde in Deutschland mit Gesetz vom 21. Dezember 2007 in nationales Recht implementiert,¹⁴²² die entsprechenden Vorschriften der §§ 113a und 113b TKG jedoch durch Entscheidung des **Bundesverfassungsgerichts** vom 2. März 2010 für nicht verfassungskonform und damit für nichtig erklärt.¹⁴²³ Eine Neufassung unter Berücksichtigung der Maßgaben des Bundesverfassungsgerichts steht, auch angesichts der von Seiten der Europäischen Kommission mittlerweile eingeleiteten Vorstufe zum Vertragsverletzungsverfahren,¹⁴²⁴ an.

c. Rechtsprechung des Europäischen Gerichtshofs zum Auskunftsanspruch

Der Europäische Gerichtshof hat über den Auskunftsanspruch in der Sache *Promusicae* im Januar 2008 entschieden. In der derzeit anhängigen Rechtssache *Bonnier Audio AB* ebenfalls zum Auskunftsanspruch nach schwedischem Recht liegen seit Oktober 2011 die Schlussanträge des Generalanwalts Jääskiinen vor.

aa. Promusicae

Für den EuGH ist für den effektiven Schutz des Urheberrechts eine Pflicht zur Mitteilung personenbezogener Daten im Rahmen eines zivilrechtlichen **Auskunftsanspruchs** über personenbezogene Daten **gemeinschaftsrechtlich nicht geboten, aber zulässig**.¹⁴²⁵ Er zog neben der E-Commerce-¹⁴²⁶, der Informationsgesellschafts-¹⁴²⁷ und der Durchsetzungsrichtlinie¹⁴²⁸ auf der einen Seite, die Datenschutzrichtlinie¹⁴²⁹ und die Richtlinie zum Datenschutz für elektronische Kommunikation¹⁴³⁰ auf der anderen Seite heran. Die Richtlinie 2002/58 verbiete es den Mitgliedstaaten nicht, im Rahmen eines zivilrechtlichen Verfahrens, zur Mitteilung personenbezogener Daten zu verpflichten. Aus einer Zusammenschau von Art. 15 Abs. 1 RL 2002/58 mit Art. 13 Abs. 1 RL 95/46 ergebe sich, dass Datenschutzregelungen erforderlichenfalls eingeschränkt werden dürfen, um Rechte und Freiheiten Dritter zu schützen. Allerdings bestehe neben dem **Recht** aber **keine** mitgliedstaatliche

¹⁴²² Artikel 2 Nr. 6 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (Bundesgesetzblatt Teil I Seite 3198).

¹⁴²³ Vgl. dazu *BVerfG*, Urteil vom 2.3.2010, abrufbar unter:

http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html.

¹⁴²⁴ Die Europäische Kommission hat mit Schreiben vom 27.10.2011 eine mit Gründen versehene Stellungnahme gemäß Artikel 258 des Vertrags über die Arbeitsweise der Europäischen Union gegenüber der Bundesrepublik Deutschland abgegeben, in der sie die Umsetzung der Vorratsdatenspeicherungsrichtlinie anmahnt (Vertragsverletzung Nr. 2011/2091, K(2011) 7509 endg.).

¹⁴²⁵ 29.1.2008 Urteil Az. C-275/06.

¹⁴²⁶ RL 2000/31/EG.

¹⁴²⁷ RL 2001/29/EG.

¹⁴²⁸ RL 2002/48/EG.

¹⁴²⁹ RL 95/46/EG.

¹⁴³⁰ RL 2002/58/EG.

Pflicht zur Weitergabe personenbezogener Daten im Rahmen eines zivilrechtlichen Verfahrens. Diese ergebe sich weder aus Art. 8 der Durchsetzungsrichtlinie¹⁴³¹, noch aus Art. 15 Abs. 2 und 18 RL 2000/31, noch aus Art. 8 Abs. 1 und 2 RL 2001/29, noch aus Art. 41, 42 und 47 TRIPS. Diese Prüfung obliege den Mitgliedstaaten unter Abwägung von Art. 17 GRCh (Schutz des Eigentums) und Art. 47 GRCh (Recht auf wirksamen Rechtsbehelf) zugunsten des Rechteinhabers und Art. 7, 8 GRCh zum Recht auf Achtung des Privatlebens.

bb. Bonnier Audio AB

Eine Folgeentscheidung wird auf das Vorabentscheidungsersuchen in der Sache *Bonnier Audio AB* zur Auslegung der Datenschutzrichtlinie für elektronische Kommunikation¹⁴³² in der Fassung Vorratsdatenspeicherungsrichtlinie¹⁴³³ sowie der Durchsetzungsrichtlinie¹⁴³⁴ ergehen.¹⁴³⁵ Für den **Generalanwalt** steht die **Vorratsdatenspeicherungsrichtlinie** der **Auskunftspflicht** von Zugangsanbietern nach bei Urheberrechtsverletzungen schon deshalb **nicht entgegen**¹⁴³⁶, weil deren Anwendungsbereich nicht betroffen ist. Sie erfasse nur zur Strafverfolgung sichergestellte Daten und stehe einer Weitergabe von Teilnehmerdaten an einen Empfängerkreis, der über die genannten Behörden hinausgehe nicht entgegen. Im Ergebnis enthalte keine der vorhandenen Datenschutzrichtlinien besondere Normen zur Vorratsspeicherung oder zur Verwendung von Telekommunikationsdaten durch Private. Allerdings geht der Generalanwalt bei Nutzung der Daten in diesem Fall von einer privatrechtliche Rechtsverfolgung aus. Es komme daher im Wesentlichen auf das nationale Recht der Mitgliedstaaten an. Soll die Nutzung von nach der Richtlinie 2006/48/EG gesammelten Daten auch für die privatrechtliche Rechtsverfolgung für Verletzungen des geistigen Eigentums erfolgen, sei dies aber **mitgliedstaatlich** hinreichend detailliert zu regeln.

C. Nationale Vorgaben für ein Warnhinweismodell

Nachdem der internationale Rahmen abgesteckt ist, soll auf nationale Rahmenbedingungen für den Ansatz der vorgerichtlichen Mitwirkung eingegangen werden. Im Folgenden werden zunächst die jeweils betroffenen Grundrechtspositionen aufgezeigt und die rechtlichen Rahmenvorgaben im Spannungsfeld zwischen dem Erfordernis zum Schutz des geistigen Eigentums der Rechteinhaber und dem Recht auf Datenschutz und der Informationsfreiheit der Nutzer auf der anderen Seite sowie den unternehmerischen Interessen der Diensteanbieter beleuchtet.

¹⁴³¹ RL 2004/48/EG.

¹⁴³² RL 2002/58/EG.

¹⁴³³ RL 2006/24/EG.

¹⁴³⁴ RL 2004/48/EG.

¹⁴³⁵ Siehe dazu oben S. 185.

¹⁴³⁶ <http://www.urheberrecht.org/news/4431/>.

I. Rechteinhaber

1. Verfassung

Im Zentrum der grundrechtlichen Positionen des Urhebers¹⁴³⁷ steht für die Rechteinhaber Art. 14 GG.¹⁴³⁸ Als **sonstige Grundrechtspositionen** kommen das bereits erwähnte allgemeine Persönlichkeitsrecht und darüber die Kommunikationsfreiheit aus Art. 5 Abs. 1 GG und gegebenenfalls die Wissenschaftsfreiheit aus Art. 5 Abs. 3 GG sowie Art. 12 GG für künstlerische Berufe in Betracht.

2. Einfaches Recht

Die einfachgesetzlichen Vorgaben¹⁴³⁹ des deutschen Urheberrechts sind im **Urheberrechtsgesetz** vom 9. Mai 1965¹⁴⁴⁰ geregelt, das den Urheber und sein Urheberpersönlichkeitsrecht in das Zentrum stellt. Das Urheberrecht sowie die verwandten Schutzrechte, sind Ausschließungsrechte, d.h. der Berechtigte kann Handlungen in Bezug auf das Werk bzw. das geschützte Gut verbieten. Das Ausschließungsrecht unterliegt aber nicht unerheblichen gesetzlichen Schranken der §§ 44a ff. UrhG, unter anderem der Privatkopierschranke nach § 53 UrhG. Greift ein Nichtberechtigter in Rechte des Rechteinhabers ein, stehen diesem die in §§ 97 ff. UrhG vorgesehenen Rechte, insbesondere der Unterlassungsanspruch und bei schuldhaftem Handeln der Anspruch auf Schadensersatz einschließlich eines dies vorbereitenden Auskunftsanspruchs zu.

II. Nutzer

Den Nutzer schützen die Kommunikationsfreiheit und das allgemeine Persönlichkeitsrecht.

1. Art. 5 GG

Art. 5 Abs. 1 S. 1 2. HS GG gewährt das für die Demokratie wichtige Grundrecht auf Informationsfreiheit.¹⁴⁴¹ Durch die neuen Medien, namentlich die Möglichkeiten des Internet gerät dieses Nebeneinander von Teilhabe an kulturellen Errungenschaften in ein scheinbares Spannungsverhältnis. Berücksichtigt man jedoch, dass Informationsfreiheit nicht den

¹⁴³⁷ Zusammenfassend *Kirchhof*, Gesetzgebungsauftrag zum Schutz des geistigen Eigentums gegenüber modernen Vervielfältigungstechniken, S. 10 f.

¹⁴³⁸ Eingehend *Hennemann*, S. 78 f. und auf Seite 80 zu weiteren tangierten Verfassungspositionen aus Art. 5 Abs. 1 und 3 GG sowie Art. 12.

¹⁴³⁹ Siehe dazu oben S. 226.

¹⁴⁴⁰ BGBl. I, S. 1273.

¹⁴⁴¹ Dazu *Dörr/Schwartzmann*, Medienrecht, Rn. 56.

kostenlosen Zugang zu Informationen schützt¹⁴⁴² und Freiheit von Information und freier Zugang dementsprechend nicht mit Kostenfreiheit verwechselt werden darf¹⁴⁴³, löst sich das oben angesprochene Spannungsverhältnis auf und wird auf die Berücksichtigung des Informationsinteresses der Allgemeinheit im Verhältnis zum Ausschlussinteresse des Urhebers reduziert.¹⁴⁴⁴

2. Art. 10 GG und Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Warnhinweisemodelle erfordern Zugriff auf Daten, die sowohl den Nutzer als auch den Inhaber eines Internetanschlusses betreffen. In Rede stehen insbesondere das Ermitteln, Sammeln, und die Weitergabe von Informationen zum Kommunikationsvorgang und zur Identität des potentiellen Rechteverletzers. Die nahe Lagerung des Sachverhalts am Persönlichkeitsrecht und dem Schutz der Privatheit des Betroffenen macht es erforderlich, die wesentlichen hieraus folgenden verfassungsrechtlichen Berührungspunkte zu beleuchten.

a. Verfassungsrechtliche Parameter

Der Schutz der Privatsphäre jedes Einzelnen findet auf verfassungsrechtlicher Ebene seine Grundlage im allgemeinen Persönlichkeitsrecht, welches von Rechtslehre und –praxis aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hergeleitet und in der ständigen Rechtsprechung des Bundesverfassungsgerichts als eigenständiges, wenngleich anderen Freiheitsverbürgungen des Grundgesetzes nachrangiges Grundrecht anerkannt ist.¹⁴⁴⁵ Das in Art. 10 GG verankerte Fernmeldegeheimnis stellt sich nach der Rechtsprechung des Bundesverfassungsgerichts insofern als speziellere Schutznorm für den Bereich der Telekommunikation dar. Es gewährleistet die Vertraulichkeit individueller Kommunikation.¹⁴⁴⁶ Geschützt sind in erster Linie der Kommunikationsinhalt, darüber hinaus aber auch die Umstände der Kommunikation. Als besondere Ausprägungen des Schutzes der Privatheit hat das Bundesverfassungsgericht in richterlicher Rechtsfortbildung aus dem allgemeinen Persönlichkeitsrecht weitere grundrechtsgleiche Rechte abgeleitet, die insbesondere den Entwicklungen der Digitalisierung Rechnung tragen sollen.

aa. Recht auf informationelle Selbstbestimmung

Als besondere Ausprägung des allgemeinen Persönlichkeitsrechts leitete das Bundesverfassungsgericht erstmals in seinem sog. Volkszählungsurteil¹⁴⁴⁷ aus Art. 2 Abs. 1 i.V.m. Art. 1

¹⁴⁴² Jarras in Jarras/Pieroth, Art. 5 Rn. 16; Hennemann, S. 81.

¹⁴⁴³ Kreuzer, Modell eines deutschen Urheberrechts, S. 159.

¹⁴⁴⁴ Dazu Hoeren, MMR 2000,3 (3); Hennemann, S. 81.

¹⁴⁴⁵ Zur Entwicklung des allgemeinen Persönlichkeitsrechts vgl. Seifert, Postmortaler Schutz des Persönlichkeitsrechts und Schadensersatz - Zugleich ein Streifzug durch die Geschichte des allgemeinen Persönlichkeitsrechts, NJW 1999, S. 1889 ff.

¹⁴⁴⁶ Vgl. Durner in: Maunz/Dürig, Grundgesetz, 62. Ergänzungslieferung 2011, Art. 10 Rn. 85.

¹⁴⁴⁷ BVerfG, Urteil v. 15.12.1984, Az.: 1 BvR 209, 269, 362, 420, 440, 484/83.

Abs. 1 GG das Recht auf informationelle Selbstbestimmung ab. Danach steht jedem Einzelnen die Befugnis zu, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu entscheiden. Die Herleitung des informationellen Selbstbestimmungsrechts durch das Bundesverfassungsgericht folgte als Reaktion auf die fortschreitende Automatisierung der Datenverarbeitung und das dadurch entstehende besondere Schutzbedürfnis von personenbezogenen Daten. Dabei sah das Gericht insbesondere die Gefahr, dass die Bedingungen moderner Informationsverarbeitungstechnologien dazu führen könnten, dass mangels Überschaubarkeit der Datenerhebung, -speicherung und -verwendung für die Bürger, diese auch in der Ausübung anderer Grundrechte, wie etwa der Versammlungsfreiheit, gehemmt werden könnten. Freie Entfaltung setze daher den Schutz des Bürgers vor unbegrenzter Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus.¹⁴⁴⁸

Im überwiegenden Allgemeininteresse darf eine Einschränkung des Rechts auf informationelle Selbstbestimmung erfolgen, soweit diese auf einer verfassungsmäßigen gesetzlichen Grundlage erfolgt, die dem Verhältnismäßigkeitsgrundsatz genügt. Insofern findet das Recht auf informationelle Selbstbestimmung seine konkrete Ausformung wesentlich in den datenschutzrechtlichen Vorgaben des einfachen Rechts.

Der Handlungsspielraum des Gesetzgebers kann dabei auch durch europarechtliche Implikationen begrenzt sein. Aktuelle Rechtsprechung des EuGH deutet jedoch darauf hin, dass gerade im Hinblick auf **Speicher- und Auskunftspflichten** zur Durchsetzung zivilrechtlicher Ansprüche keine zwingenden Maßgaben des europäischen Rechts bestehen.¹⁴⁴⁹ So folgt aus der Entscheidung des EuGH in der Rechtssache *Promusicae/Telefónica*¹⁴⁵⁰, dass es nach bis dato geltender Rechtslage kein Gebot zur Speicherung und Auskunft vonseiten der Internetdiensteanbieter existiert, gleichwohl den Mitgliedstaaten es unbenommen ist, im Rahmen der Beachtung des Grundsatzes der Verhältnismäßigkeit, entsprechende Regelungen im jeweils nationalen Recht vorzusehen.¹⁴⁵¹

Dazu, ob sich die Einschätzung nach Inkrafttreten der Vorratsdatenspeicherungsrichtlinie ändert, hat der EuGH derzeit im Fall *Bonnier Audio AB* zu entscheiden. Insbesondere steht in Frage, ob die Richtlinie einem Auskunftsanspruch gegen Internetzugangsanbieter entgegensteht, nachdem diese potentielle Urheberrechtsverletzer anhand der verwendeten IP-Adressen zu identifizieren und den Rechteinhabern mitzuteilen haben. Nach den bereits vorliegenden Schlussanträgen des Generalanwalts¹⁴⁵² stehen die Vorgaben der Vorratsda-

¹⁴⁴⁸ Vgl. *BVerfGE* 65, 1 – Volkszählung.

¹⁴⁴⁹ In Betracht kommen insbesondere die Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) in der Fassung der Richtlinie über die Vorratsspeicherung von Daten (2006/24/EG) und der Durchsetzungsrichtlinie (2004/48/EG).

¹⁴⁵⁰ *EuGH*, Urteil v. 29.1.2008 – C 275/06 in GRUR 2008, 241 – *Promusicae/Telefónica*; vgl. auch *EuGH* Rs. C-557/07 – LSG.

¹⁴⁵¹ Siehe dazu auch oben S. 287.

¹⁴⁵² Generalanwalt *Jääskiinen*, Schlussanträge in der Rs. C-461/10 - *Bonnier Audio*.

tenspeicherungsrichtlinie einer solchen nationalen Regelung im privatrechtlichen Bereich nicht entgegen.¹⁴⁵³

bb. Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Informationstechnische Systeme, vom Computer bis zum Internet, sieht das Bundesverfassungsgericht als nicht vom informationellen Selbstbestimmungsrecht geschützt an.¹⁴⁵⁴ Ergänzend hat es jedoch, ebenfalls als besondere Ausprägung des allgemeinen Persönlichkeitsrechts, betreffend den heimlichen Zugriff auf informationstechnische Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ein **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme** hergeleitet. Als Auffanggrundrecht schützt dieses vor staatlichen Eingriffen in informationstechnische Systeme, soweit der Schutz nicht bereits durch andere Grundrechte, wie etwa Art. 10 und Art. 13 GG oder das Recht auf informationelle Selbstbestimmung, gewährleistet ist.¹⁴⁵⁵ Dem Staat ist es danach verwehrt, ohne besondere Rechtfertigung mit Hilfe sog. Trojanersoftware Computer zu überwachen und dort Informationen auszulesen.

cc. Fernmeldegeheimnis

Art. 10 GG normiert das Fernmeldegeheimnis, welches den speziellen Bereich der Telekommunikation betrifft.

1) Allgemeine Fragen

Aus ihm leitet sich ein besonderer Schutz für Informationen ab, die durch Eingriffe in das Fernmeldegeheimnis, also durch Kenntnisnahme Dritter von den näheren Umständen elektronischer Kommunikation, erlangt werden.¹⁴⁵⁶ Dem Schutz unterliegen einerseits die Inhalte der Kommunikation, andererseits und darüber hinaus die Vertraulichkeit der näheren Umstände des Kommunikationsvorgangs. Hierzu gehören insbesondere Informationen darüber, „ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist“.¹⁴⁵⁷ Insofern können insbesondere auch Daten, die durch die Nutzung des Internets anfallen oder generiert werden können, in den Schutzbereich des Art. 10 GG fallen. Ausgehend davon, dass sich der Schutz des Fernmeldegeheimnisses auf Individualkommunikation bezieht,¹⁴⁵⁸ steht in der Diskussion, ob jegliche Internetsachverhalte dem Schutz des Fernmeldegeheimnisses unterliegen. Namentlich erstreckte sich der Schutz auf Mail- und Chat-Dienste sowie etwa auf nicht-öffentliche Diskussionsforen. Das Schutzgut des Fernmelde-

¹⁴⁵³ Siehe dazu auch oben S. 287.

¹⁴⁵⁴ Piroth/Schlink, Grundrechte Staatsrecht II, § 8 Rn. 377 c.

¹⁴⁵⁵ BVerfGE 120, 274, 303 – Online-Durchsuchung.

¹⁴⁵⁶ Eingehend hierzu BVerfGE 125, 260 – Vorratsdatenspeicherung.

¹⁴⁵⁷ BVerfGE 125, 260, 309 mit Verweis auf die ständige Rechtsprechung BVerfGE 67, 157, 172; 85, 386, 396; 100, 313, 358; 107, 299, 312 f.; 115, 166, 183; 120, 274, 307.

¹⁴⁵⁸ Vgl. Durner in: Maunz/Dürig, Grundgesetz, 62. Ergänzungslieferung 2011, Art. 10 Rn. 85.

geheimnisses sei nicht technisch zu bestimmen durch die Form der individuellen Verbindung. Vielmehr komme es auf die über diese Verbindung erfolgende Kommunikation einzelner Grundrechtsträger an.¹⁴⁵⁹ Tauschbörsen unter Nutzung von Peer-to-Peer-Netzwerken werden, diese Maßstäbe zugrunde legend, nicht dem Schutzbereich des Art. 10 GG zugeordnet.¹⁴⁶⁰ Soweit hingegen ein umfassender Schutz sämtlicher Internetkommunikation geltend gemacht wird, stützt sich dies maßgeblich darauf, dass sich, technisch gesehen, alle Vorgänge im Internet als Individualkommunikation darstellen und eine Unterscheidung von Individualkommunikation und Kommunikation an die Allgemeinheit nur bei genauerer Betrachtung des kommunizierten Inhalts möglich sei.¹⁴⁶¹

Sofern Sachverhalte dem Schutzbereich des Fernmeldegeheimnisses zuzuordnen sind, müssen Beschränkungen nach Art. 10 Abs. 2 GG die allgemeinen Anforderungen an Grundrechtseingriffe erfüllen, insbesondere dem Gesetzesvorbehalt und dem Grundsatz der Verhältnismäßigkeit gerecht werden. In seiner Rechtsprechung stellt das Bundesverfassungsgericht zudem ergänzende Anforderungen dem Umstand folgend, dass durch Eingriffe in Art. 10 GG gerade personenbezogene Daten erlangt werden. Die im Zusammenhang mit dem Recht auf informationelle Selbstbestimmung entwickelten Gebote der Normenklarheit und der Zweckbindung erhobener Informationen gelten daher auch für das Fernmeldegeheimnis.¹⁴⁶²

2) *Anlasslose Speicherung im Hinblick auf das vorgerichtliche Mitwirkungsmodell*

Geht es – namentlich im Hinblick auf Warnhinweismodelle - um anlasslose Speicherung von Daten wäre maßgeblich die Entscheidung des Bundesverfassungsgerichts im Fall der Vorratsdatenspeicherung zu berücksichtigen.¹⁴⁶³ Der zufolge ist

„eine sechsmonatige, vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten durch private Diensteanbieter (...) mit Art. 10 GG **nicht schlechthin unvereinbar.**“

Jedoch forderte das Gericht,

„dass die **gesetzliche Ausgestaltung** einer solchen Datenspeicherung dem besonderen Gewicht des mit der Speicherung verbundenen Grundrechtseingriffs angemessen Rechnung trägt. Erforderlich sind hinreichend anspruchsvolle und normenklare Regelungen hinsichtlich der **Datensicherheit, der Datenverwendung, der Transparenz und des Rechtsschutzes**“.¹⁴⁶⁴

¹⁴⁵⁹ Hierzu *Durner*, Fernmeldegeheimnis und informationelle Selbstbestimmung als Schranken urheberrechtlicher Sperrverfügungen im Internet?, ZUM 2010, S. 833, 839.

¹⁴⁶⁰ *Hennemann*, S. 80.

¹⁴⁶¹ Zum Streitstand *Hennemann*, S. 82 ff.

¹⁴⁶² Hierzu *Durner* in: Maunz/Dürig, Grundgesetz, 62. Ergänzungslieferung 2011, Art. 10 Rn. 312.

¹⁴⁶³ BVerfGE 125, 260 – Vorratsdatenspeicherung.

¹⁴⁶⁴ Vgl. Leitsätze 1 und 2 der Entscheidung.

Zu berücksichtigen wird im konkreten Fall sein, wie intensiv der jeweils gesetzlich vorgesehene Eingriff zu beurteilen ist, konkret, gemessen am Maßstab der Entscheidung des Bundesverfassungsgerichts, inwieweit Zielsetzung und Ausmaß mit dem der Entscheidung zugrunde liegenden Sachverhalt vergleichbar ist. So wird mit Blick auf das geltende Auskunftsverfahren nach § 101 Abs. 9 UrhG vertreten, dass die Eingriffskriterien, wie sie vom Bundesverfassungsgericht in der genannten Entscheidung angewendet wurden, nicht ohne weiteres auf dieses angewendet werden könnten.¹⁴⁶⁵ Vergleichbares würde, je nach Ausgestaltung, auch für die Speicherung von Daten im Rahmen eines Warnhinweissystems gelten müssen.

b. Einfachgesetzliche Ausgestaltung

Die verfassungsrechtlichen Vorgaben, namentlich den Datenschutz betreffend, hat die Bundesrepublik Deutschland, unter Einbeziehung der europäischen und völkerrechtlichen Verpflichtungen, einfachgesetzlich konkretisiert. Vorgaben zum Fernmeldegeheimnis finden sich maßgeblich im Telekommunikationsgesetz, datenschutzrechtliche Vorgaben in einer Vielzahl weiterer einfachgesetzlicher Rechtsgrundlagen.

aa. Fernmeldegeheimnis

Das Fernmeldegeheimnis findet seine einfachgesetzliche Ausgestaltung in verschiedenen Schutznormen zur Gewährleistung der Vertraulichkeit individueller Kommunikation unter Privaten.¹⁴⁶⁶ Maßgeblich im Umgang mit Kommunikationsdaten durch Telekommunikationsdiensteanbieter ist § 88 TKG. Der Gewährleistung des Fernmeldegeheimnisses unterworfen sind danach alle Diensteanbieter, d.h. insbesondere jedes Unternehmen, das geschäftsmäßig Telekommunikationsdienste erbringt oder hieran mitwirkt (vgl. § 3 Nr. 6 TKG).

Der Diensteanbieter, auch der Zugangsdiensteanbieter, darf sich danach grundsätzlich keine Kenntnisse über den Inhalt eines Telekommunikationsvorgangs, mithin auch über den Inhalt des erfolgten Datenaustauschs verschaffen. Gleiches gilt für die näheren Umstände des Vorgangs, insbesondere bezüglich der Tatsache, wer hieran beteiligt ist oder war bzw. wer wen oder welche Webseite kontaktiert hat.

Ausnahmen von diesem Grundsatz sind zulässig, soweit die Kenntnisnahme zur geschäftsmäßigen Erbringung der Telekommunikationsdienste bzw. des Schutzes technischer Systeme erforderlich ist oder eine andere gesetzliche Vorschrift dies vorsieht. Derartige gesetzliche Ermächtigungstatbestände sind begrenzt.¹⁴⁶⁷ Neben weiteren datenschutzrechtlichen Vorgaben spezifisch für Diensteanbieter sehen das TKG, wie auch das

¹⁴⁶⁵ Hennemann, S. 177 ff.

¹⁴⁶⁶ Vgl. Durner, Fernmeldegeheimnis und informationelle Selbstbestimmung als Schranken urheberrechtlicher Sperrverfügungen im Internet?, ZUM 2010, S. 833, 836.

¹⁴⁶⁷ Nachweise bei Munz in: Taeger/Gabel, § 88 Rn. 17.

TMG, derartige Erlaubnistatbestände vor. Sie ermächtigen den Diensteanbieter, auch ohne Einwilligung des Betroffenen – umfasst sind Teilnehmer und Nutzer der Telekommunikationsleistung - bestimmte Daten zu erheben und zu verwenden. Für Bestandsdaten gelten §§ 95, 100 TKG, für Verkehrsdaten §§ 96, 97, 100 TKG.¹⁴⁶⁸

bb. Datenschutzrecht

Das Datenschutzrecht ist einfachgesetzlich nicht zentral und abschließend normiert. Zur Anwendung kommen, abhängig davon, in welchem Zusammenhang und von wem Daten verwendet werden, sowie davon, um welche Art von Daten es sich handelt, das Bundesdatenschutzgesetz, die Datenschutzgesetze der Länder oder bereichsspezifische Regelungen in anderen Gesetzen.

Das Bundesdatenschutzgesetz (BDSG) ist als grundlegendes Regelwerk einschlägig, sofern Handelnder eine öffentliche Stelle des Bundes oder eine nicht-öffentliche Stelle ist und keine bereichsspezifische Regelung einschlägig ist. Es bezweckt, „den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird“ (§ 1 Abs. 1 BDSG). Die Landesdatenschutzgesetze hingegen gelten für die Verarbeitung personenbezogener Daten durch die jeweiligen Landesbehörden.

Die bereichsspezifischen Regelungen¹⁴⁶⁹ gelangen im Umfang ihres Regelungsgehalts vorrangig vor dem BDSG und den LDSG zur Anwendung. Insbesondere finden sich spezielle Regelungen zum Umgang mit personenbezogenen Daten für die Telemedien im Telemediengesetz (TMG), sowie für die Telekommunikationsdienste im Telekommunikationsgesetz (TKG). Die datenschutzrechtlichen Vorschriften des TMG¹⁴⁷⁰ schützen personenbezogene Daten bei der Nutzung von Telemediendiensten i.S.v. § 1 Abs. 1 TMG, soweit diese Dienste nicht im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken oder innerhalb von oder zwischen nicht öffentlichen Stellen oder öffentlichen Stellen ausschließlich zur Steuerung von Arbeits- oder Geschäftsprozessen bereitgestellt werden (§ 11 Abs. 1 Nr. 1 und 2 TMG). Die im TKG festgeschriebenen Datenschutzregelungen¹⁴⁷¹ bezwecken den Schutz personenbezogener Daten der an der Telekommunikation Beteiligten bei der Erhebung und Verwendung durch Diensteanbieter, also jedem, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt (§ 3 Nr. 6 TKG).

Zu den wichtigsten, nicht aber absolut geltenden, Prinzipien des deutschen Datenschutzrechts zählt, dass Eingriffe in den Datenschutz einem Verbot mit Erlaubnisvorbehalt unter-

¹⁴⁶⁸ Regelungen zu Standorten sind in § 98 TKG enthalten. Sie finden auf Telekommunikationsdienste Anwendung, die für die Öffentlichkeit angeboten werden.

¹⁴⁶⁹ Diese finden sich in zahlreichen anderen Gesetzen, wie etwa dem Einkommensteuergesetz, im Personenstandsgesetz, in der Grundbuchordnung oder dem Bundeszentralregistergesetz.

¹⁴⁷⁰ §§ 11 – 15a TMG.

¹⁴⁷¹ Siehe dort §§ 91 – 107 TKG.

liegen, diese also nur mit Einwilligung oder aufgrund einer gesetzlichen Ermächtigung erfolgen dürfen. Darüber hinaus gelten das Transparenzgebot, der Direkterhebungsgrundsatz, die Grundsätze der Datenvermeidung und Datensparsamkeit sowie der Grundsatz der Zweckbindung. Diese verfassungsrechtlich abgeleiteten Grundprinzipien gilt es bei der Ausgestaltung auch weitergehender einfachgesetzlicher Regelungen zu beachten.

c. Datenschutzrechtlich relevante Aspekte von Warnhinweismodellen

aa. IP-Adresse als personenbezogenes Datum

Ein Warnhinweisverfahren setzt die Ermittlung eines Urheberrechtsverstoßes und damit eines ggf. strafrechtlich relevanten Sachverhalts voraus. Relevante Daten hierfür sind zumindest die Ermittlung der IP-Adresse des Anschlussinhabers sowie der Zugriffszeiten, zu denen eine Rechtsverletzung begangen wurde. Darüber hinaus bedarf es zur Geltendmachung von Ansprüchen im Rahmen der Darlegungslast des Rechteinhabers gegebenenfalls weiterer Informationen, wie etwa zu den Inhalten bzw. Metadaten involvierter Dateien. Diese Daten werden im Rahmen der Rechtsdurchsetzung von den Rechteinhabern bzw. deren Beauftragten, in Frankreich etwa von zertifizierten Bevollmächtigten oder in Irland von Dienstleistern, erhoben.

Unzweifelhaft berührt nicht jede Art von Information das grundrechtlich geschützte Recht des Einzelnen auf Privatsphäre bzw. informationelle Selbstbestimmung. Datenschutzrechtlich relevante Informationen sind insofern nur Einzelangaben über persönliche oder sachliche Verhältnisse, die sich auf eine bestimmte oder zumindest bestimmbare Personen beziehen. Dies setzt zum einen voraus, dass die Information sich auf eine einzelne Person bezieht, zum anderen muss sie diese als solche identifizierbar machen.

Zentral in der datenschutzrechtlichen Diskussion um die Verfolgung von Rechteverletzungen im Internet ist vor diesem Hintergrund die IP-Adresse, die die Identifizierung des Anschlussinhabers als natürliche Person erlaubt. Da die IP-Adresse selbst zunächst nicht unmittelbar den Anschlussinhaber preisgibt, steht ihre Qualität als personenbezogenes Datum in Frage. Ihre Klassifizierung ist insofern jedoch von erheblicher Bedeutung, als sie über die Anwendung datenschutzrechtlicher Vorgaben entscheidet.

1) *Exkurs zum internationalen Recht*

Wie eine Betrachtung der Fragestellung im europäischen Kontext zeigt, ist die Bewertung der IP-Adresse keinesfalls einheitlich. Als Tendenz ist jedoch wahrnehmbar, dass die IP-Adresse grundsätzlich als datenschutzrelevantes Datum anerkannt wird.

In Frankreich wurde, ungeachtet einer etwaigen Einstufung der IP-Adresse durch die Gerichte, eine ausdrückliche gesetzliche Ermächtigung geschaffen, nach der die zugelassenen Bevollmächtigten berechtigt sind, Daten, die die Tat und den Inhaber des Internetanschlusses betreffen, wie u.a. Datum der Urheberrechtsverletzung, IP-Adresse des Nutzers,

Benutzername des Internetnutzers und Name der Datei auf dem Computer des Internetnutzers zu ermitteln,¹⁴⁷² um datenschutzrechtlichen Belangen in jedem Fall Rechnung zu tragen.

a) *Europäische Union*

Eine ausdrückliche Regelung dazu, wie IP-Adressen datenschutzrechtlich zu behandeln sind, gibt es im Europäischen Recht nicht. Der Europäische Datenschutzbeauftragte hat zu dieser Frage in einer „Stellungnahme zu den laufenden Verhandlungen der Europäischen Union über ein Abkommen zur Bekämpfung von Produkt- und Markenpiraterie (Anti-Counterfeiting Trade Agreement, ACTA)“¹⁴⁷³ Stellung bezogen. Er geht danach davon aus, dass - jedenfalls im Fall der Verarbeitung von IP-Adressen für ein Three-Strikes-System - IP-Adressen als personenbezogene Daten zu betrachten seien.¹⁴⁷⁴

Diese Bewertung entspricht dem Ergebnis der sog. „Art. 29-Gruppe“, einer nach Art. 29 der Datenschutzrichtlinie von der Europäischen Union eingesetzten Arbeitsgruppe als unabhängiges EU-Beratungsgremium für Datenschutzfragen. Diese befasste sich mit der Frage im Rahmen einer Stellungnahme. Angesichts der unterschiedlichen Auslegung und Anwendung des Begriffs der „personenbezogenen Daten“ in den einzelnen Mitgliedstaaten sollte hierdurch eine gemeinsame Verständnisgrundlage in diesem Bereich geschaffen werden. Derzufolge sollen auch dynamische IP-Adressen als Daten einzustufen sein, die sich auf eine bestimmbar Person beziehen. In der Begründung heißt es hierzu:

„[...] können **Internet-Zugangsanbieter** und Verwalter von lokalen Netzwerken ohne großen Aufwand Internet-Nutzer identifizieren, denen sie IP-Adressen zugewiesen haben, da sie in der Regel in Dateien systematisch Datum, Zeitpunkt, Dauer und die dem Internet-Nutzer zugeteilte dynamische IP-Adresse einfügen. Dasselbe lässt sich von den Internet-Diensteanbietern sagen, die in ihren HTTP-Servern Protokolle führen. In diesen Fällen besteht kein Zweifel, dass man von personenbezogenen Daten im Sinne von Artikel 2 Buchstabe a) der Richtlinie 95/46/EG reden kann.“¹⁴⁷⁵

Betreffend das Vorgehen von **Rechteinhabern** befand die Datenschutzgruppe weiter, dass:

¹⁴⁷³ (2010/C - 147/01) v. 5.6.2010, abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:147:0001:0013:DE:PDF>.

¹⁴⁷⁴ Stellungnahme des Europäischen Datenschutzbeauftragten zu den laufenden Verhandlungen der Europäischen Union über ein Abkommen zur Bekämpfung von Produkt- und Markenpiraterie (Anti-Counterfeiting Trade Agreement, ACTA)“, (2010/C 147/01) v. 5.6.2010, Rz. 25 ff., abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:147:0001:0013:DE:PDF>.

¹⁴⁷⁵ Stellungnahme der Datenschutzgruppe zum Begriff „personenbezogene Daten“, 4/2007 (01248/DE, WP 136), S. 19.

„vor allem in Fällen, in denen der Zweck der Verarbeitung von IP-Adressen in der Identifizierung der Computernutzer besteht (beispielsweise durch Inhaber von Urheberrechten zur strafrechtlichen Verfolgung von Computernutzern wegen Verletzung von Rechten an geistigem Eigentum), geht der für die Verarbeitung Verantwortliche vom Vorhandensein der Mittel aus, die zur Identifizierung der betreffenden Personen „vernünftigerweise eingesetzt werden könnten“, z. B. von den Gerichten, bei denen Beschwerde eingelegt wurde (andernfalls wäre die Erhebung der Informationen nicht sinnvoll); aus diesem Grund sind die Informationen als personenbezogene Daten anzusehen“.¹⁴⁷⁶

Der Gerichtshof der Europäischen Union hat nunmehr in seiner aktuellen Entscheidung zum Vorabentscheidungsersuchen im Fall Scarlet Extended SA (Rs. C-70/10) vom 24. November 2011 konstatiert, dass es sich bei IP-Adressen um personenbezogene Daten handle.¹⁴⁷⁷ Näher ausgeführt hat der Gerichtshof dieses Ergebnis indes nicht.

b) *Vereinigtes Königreich*

Auf die vorgenannte Stellungnahme der Art. 29-Gruppe bezog sich auch der *High Administrative Court* im Vereinigten Königreich in seiner Spruchpraxis. Seiner Rechtsprechung zufolge stellen die vom Rechteinhaber übermittelten Informationen, darunter auch die IP-Adresse, personenbezogene Daten dar.¹⁴⁷⁸ Diesen Personenbezug sah er nicht nur gegeben im Hinblick auf den Anschlussinhaber, sondern auch bezogen auf den rechteevertzenden Nutzer des Internetzugangs. Zwar könne anhand der IP-Adresse, nur der Anschlussinhaber ermittelt werden, der nicht zwingend identisch mit der Person sei, die das Material rechtswidrig heruntergeladen habe. Der Anschlussinhaber stehe aber zwingend in Verbindung mit dieser Person, so dass es sich auch bei dieser zumindest um eine bestimmbare Person handle.¹⁴⁷⁹

c) *Irland*

Der irische *High Court*, hatte sich bereits in mehreren Verfahren¹⁴⁸⁰ damit auseinanderzusetzen, ob es sich bei den die IP-Adressen umfassenden Daten in den Händen der Musikproduktionsgesellschaften oder ihrer Auftragnehmer unter Berücksichtigung des Zwecks der Datensammlung und der beabsichtigten Weitergabe der Daten an Eircom Ltd. um personenbezogene Daten („*personal data*“¹⁴⁸¹) im Sinne des irischen Datenschutzrechts handelt und ob damit die Sammlung der IP-Adressen durch die Gesellschaften oder ihre Auf-

¹⁴⁷⁶ Stellungnahme der Datenschutzgruppe zum Begriff „personenbezogene Daten“, 4/2007 (01248/DE, WP 136), S. 19f.

¹⁴⁷⁷ *EuGH Scarlet Extended*, Rn. 51.

¹⁴⁷⁸ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 157.

¹⁴⁷⁹ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 157.

¹⁴⁸⁰ Urteil v. 16.04.2010 - [2010] IEHC 108; Urteil v. 11.10.2010 - [2010] IEHC 377.

¹⁴⁸¹ Vgl. Section 1(1) *Data Protection Act*, 1988 as amended: „*personal data* means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller“; vgl. auch § 3 Abs. 1 BDSG.

tragnehmer den besonderen Anforderungen¹⁴⁸² des *Data Protection Act* gerecht werden muss.¹⁴⁸³ Der *High Court* verneinte vor dem Hintergrund der konkreten Ausgestaltung des Warnhinweissystems in Irland diese Frage und entschied, dass die IP-Adressen, die von den Auftragnehmern ermittelt und an die Musikproduktionsunternehmen ausgehändigt werden, keine personenbezogenen Daten seien.¹⁴⁸⁴ Das Gericht begründete seine Entscheidung u.a. damit, dass den Produktionsunternehmen mit diesen Daten lediglich bekannt würde, dass eine bestimmte IP-Adresse in ein urheberrechtswidriges Up- oder Downloading involviert sei. Sie erhielten darüber hinaus aber keine Kenntnis über den Namen und die Anschrift des rechtswidrig Handelnden oder des Inhabers des betreffenden Anschlusses. Nach Ansicht des Gerichts hätten die Musikproduktionsgesellschaften auch keinerlei Interesse daran, mit Hilfe der Regelungen die Rechteverletzer persönlich zu identifizieren. Für den *High Court* war es unwahrscheinlich, dass die Produzenten den Versuch unternehmen, die IP-Adressen hierzu zu benutzen. Der einzig rechtlich zulässige Weg, um an die Namen und Adressen zu gelangen, bestehe darin, den Diensteanbieter wie bisher gerichtlich auf Auskunft in Anspruch zu nehmen. Dass die Musikproduktionsgesellschaften die Absicht hätten, sich illegal zu betätigen, sah das Gericht nicht. Vielmehr gehe es ihnen allein um die Einhaltung des Rechts.

Im Hinblick auf das Verhältnis zwischen dem Diensteanbieter und seinen Kunden sei schließlich allein deren Vertragsbeziehung betroffen und nach Ansicht des Gerichts wirke sich die Durchsetzung des Vertrags in Bezug auf Anti-Piraterie-Regelungen in den Vertragsbedingungen nicht auf die Privatsphäre des Kunden aus.¹⁴⁸⁵

2) *National*

Die Frage, ob IP-Adressen personenbezogene Daten i.S.d. § 3 BDSG und damit datenschutzrechtliche Vorschriften bezüglich deren Verwendung einschlägig sind, war auch in Deutschland bereits Gegenstand der Diskussion.¹⁴⁸⁶ Diese stand in Zusammenhang vor allem mit der Ermittlung von IP-Adressen durch Rechteinhaber im Vorfeld des Auskunfterteilungsverfahrens nach § 101 Abs. 2 und 9 UrhG.¹⁴⁸⁷

Nach der Legaldefinition des § 3 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Bestimmtheit liegt vor, wenn sich die Daten direkt auf eine bestimmte Person beziehen bzw. wenn sie mit dem Namen des Betroffenen verbunden sind.¹⁴⁸⁸ Im Fall der dynamischen IP-Adressen, die bei jedem Internetzugang einer anderen Person

¹⁴⁸² Section 2, 2A, 2B, 2C und 2D des *Data Protection Act*.

¹⁴⁸³ Siehe auch zusammenfassend *McGonagle*, IRIS 2010-6:1/34 (<http://merlin.obs.coe.int/iris/2010/6/article34.de.html>).

¹⁴⁸⁴ *EMI Records (Ireland) Ltd., Sony B. G. Music Entertainment (Ireland) Ltd., Universal Music Ireland Ltd. And Warner Music Ireland Ltd. v Eircom Ltd.*, Charleton J., 16.4.2010, [2010] IEHC 108, Rn. 18 ff.

¹⁴⁸⁵ Urteil v. 11.10.2010 – [2010] IEHC 377.

¹⁴⁸⁶ Vgl. *Meyerdierks* in MMR 2009, 8; *Venzke* in ZD 2011, 114; *Krüger/Maucher* in MMR 2011, 433.

¹⁴⁸⁷ Vgl. oben S. 252ff.

¹⁴⁸⁸ *Gola/Schomerus* § 3 Rn. 10; *Dammann* in *Simitis* § 3 Rn. 22.

zugewiesen sind, lässt sich die Identität einer Person nicht allein anhand der IP-Adresse ermitteln. Bestimmt ist also eine Person nicht bereits durch die Feststellung der von ihr verwendeten IP-Adresse. Bestimmbarkeit ist erst dann gegeben, wenn der Personenbezug ohne unverhältnismäßigen Aufwand herzustellen ist. Es kommt dafür auf die Kenntnis, Mittel und Möglichkeiten der verantwortlichen Stelle zur Herstellung der Verbindung an.¹⁴⁸⁹ Die Bestimmbarkeit der Person ist daher relativ und von den individuellen Kenntnissen des Datenverwenders abhängig.¹⁴⁹⁰ Die dynamischen IP-Adressen sind also nicht per se personenbezogene Daten.¹⁴⁹¹ Es bedarf vielmehr der Differenzierung zwischen den unterschiedlichen Beteiligten.

a) *Personenbezug von IP-Adressen für Internetzugangsanbieter*

Der Internetzugangsanbieter vergibt IP-Adressen an die Nutzer und es ist daher ohne unverhältnismäßigen Aufwand - unter Einblick in sein Datensystem - ermittelbar, welcher Person eine bestimmte dynamische IP-Adresse zugeordnet ist. Er kann den Nutzer also anhand der IP-Adresse identifizieren. Sie stellt damit für den Zugangsanbieter unstreitig ein personenbezogenes Datum dar.¹⁴⁹²

b) *Personenbezug von IP-Adressen für andere Stellen*

Umstritten ist bisher, ob die IP-Adresse für andere Stellen als den Zugangsanbieter - wie z.B. für **Webseitenbetreiber** - ein personenbezogenes Datum ist. Nach herrschender Meinung ist die dynamische IP-Adresse für den Webseitenbetreiber kein personenbezogenes Datum.¹⁴⁹³ Zwar wissen die Webseitenbetreiber, mit welcher IP-Adresse auf die Webseite zugegriffen wurde, sie können aber allein aufgrund der IP-Adresse die Zuordnung zu einer bestimmten Person ohne Hilfe Dritter nicht vornehmen. Die Betreiber können also den Personenbezug mit den ihnen normalerweise zur Verfügung stehenden Hilfsmitteln und mit unverhältnismäßigen Aufwand nicht herstellen, da ihnen besonders aus datenschutzrechtlichen Gründen versagt ist, den hinter einer IP-Adresse stehenden Namen des Nutzers von dem Zugangsanbieter zu fordern.¹⁴⁹⁴

c) *Personenbezug von IP-Adressen für Rechteinhaber*

Vorstehendes gilt auch mit Blick auf die **Rechteinhaber**. Auch für diese ist die IP-Adresse kein personenbezogenes Datum, da sie diese einer bestimmten oder bestimmbar Per-

¹⁴⁸⁹ Gola/Schomerus § 3 Rn. 10.

¹⁴⁹⁰ So Krüger/Maucher MMR 2011, 436 (439); Gola/Schomerus § 3 Rn. 10; Meyerdirks MMR 2009, 8 (9 ff.); Eckhardt K&R 2007, 602; Gabriel/Cornels MMR 11/2008, S. XV; Moos K&R 2008, 139; Wehr/Ujica MMR 2010, 667 (668). Anders z.B. Pahlen-Brandt K&R 2008, 288. Dieser vertritt die objektive Theorie, wonach Daten Personenbezug besitzen, wenn objektiv möglich ist, zwischen dem Datum und der Person einen Bezug herzustellen.

¹⁴⁹¹ Moos K&R 2008, 139; Krüger/Maucher MMR 2011, 433 (439).

¹⁴⁹² Vgl. OLG Karlsruhe MMR 2009, 412 (413), Krüger/Maucher MMR 2011, 433; Meyerdirks MMR 2009, 8 (9); Maaßen MMR 2009, 511 (512).

¹⁴⁹³ So Krüger/Maucher MMR 2011, 433 (433 ff.); Meyerdirks MMR 2009, 8 (9 ff.); Moos K&R 2008, 139.

¹⁴⁹⁴ Vgl. Moos K&R 2008, 139.

son ohne Zuhilfenahme der Zugangsanbieter nicht zuordnen können.¹⁴⁹⁵ Damit ist die Ermittlung der IP-Adressen durch die Rechteinhaber datenschutzrechtlich zunächst unproblematisch.

bb. Datenschutzrechtlich relevantes Handeln

Ausgehend von der Klassifizierung der IP-Adresse als personenbezogenes Datum bedürfte es für alle datenschutzrechtlich relevanten Handlungen einer gesetzlichen Grundlage.

Datenschutzrechtlich bedeutsam ist grundsätzlich jeder Umgang mit personenbezogenen Daten. Ausgehend von der besonderen Gefahrenlage bei automatisierten Verarbeitungsvorgängen nehmen die einfachgesetzlich im BDSG konkretisierten Anforderungen insbesondere auf elektronische Daten Bezug.

Relevantes Handeln ist nach § 3 BDSG das Erheben, d.h. das Beschaffen von Daten. Darüber hinaus relevant ist das Verwenden von Daten, welches synonym steht für das Verarbeiten und Nutzen. Dies umfasst insbesondere das Speichern (Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung), das Verändern (d.h. das inhaltliche Umgestalten gespeicherter Daten), das Übermitteln (d.h. das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten), das Sperren (das Kennzeichnen gespeicherter Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken) und Löschen (das Unkenntlichmachen gespeicherter Daten) von Daten.

Die Ermittlung der IP-Adresse und damit zusammenhängender Informationen stellt insofern datenschutzrechtlich eine Erhebung i.S.d. § 3 Abs. 3 BDSG dar, die Weitergabe an Dritte eine Übermittlung i.S.d. § 3 Abs. 4 Nr. 3 BDSG.

1) Ermittlung von IP-Adressen durch die Rechteinhaber

Ausgehend davon, dass die IP-Adresse aus Perspektive des Rechteinhabers zunächst kein personenbezogenes Datum darstellt, da die Person des Anschlussinhabers damit für ihn nicht feststellbar ist, bedarf es für die Erhebung, Speicherung und Weitergabe dieser IP-Adresse zunächst keiner weiteren ausdrücklichen Ermächtigung.

2) Verwendung der IP-Adresse durch Zugangsdiensteanbieter

Die dargestellten Warnhinweismodelle basieren jedoch wesentlich auf der Mitwirkung der Internetzugangsdiensteanbieter. Die Diensteanbieter wären in diesem Zusammenhang dazu verpflichtet, nicht nur Bestands-, sondern auch Verkehrsdaten, namentlich die IP-Adresse und den Zeitpunkt des Zugriffs, ihrer Anschlusskunden zu speichern und gebe-

¹⁴⁹⁵ So *Hoeren* NJW 2008, 3099; *Kramer* S. 125. Anders *Welp* S. 204 ff., der IP-Adressen aus Sicht der Rechteinhaber als personenbezogene Daten betrachtet, da diese über den Auskunftsanspruch gegen den Zugangsanbieter die rechtliche Handhabe besitzen, um den Nutzer identifizieren zu können. Anders auch *Spindler* ZUM 2008, S. 647; *Maaßen* MMR 2009, S. 512 ff., die generell von einem Personenbezug der IP-Adresse ausgehen.

nenfalls einer berechtigten Person herauszugeben.¹⁴⁹⁶ Datenschutzrechtlich und, soweit einschlägig, vor dem Hintergrund der Gewährleistung des Fernmeldegeheimnisses zulässig ist dies nur dann, wenn eine entsprechende Ermächtigungsgrundlage hierzu vorliegt.

Zudem ist der im Datenschutzrecht geltende Zweckbindungsgrundsatz zu berücksichtigen. Werden Daten über einen Kommunikationsvorgang, etwa im Wege einer Protokollierung, zulässigerweise generiert, ist die Nutzung wie auch die Weitergabe dieser Daten, sofern das Gesetz nicht ausdrücklich Ausnahmen zulässt, an den Zweck der Erhebung gebunden. Rechtmäßig erlangte Kenntnisse dürfen daher nachträglich jeweils nicht auch für andere Zwecke als für diejenigen verwendet werden, für die sie zunächst erhoben wurden.

Ob die derzeit geltenden gesetzlichen Regelungen für die Berechtigung der Internetzugangsdiensteanbieter zur Erhebung und Speicherung von IP-Adressen im Rahmen des Auskunftsanspruchs nach § 101 Abs. 9 UrhG den datenschutzrechtlichen Anforderungen genügen, ist umstritten.¹⁴⁹⁷ So dürfen nach Beendigung der Telekommunikationsverbindung gespeicherte Verkehrsdaten, zu denen Bundesverfassungsgericht und Bundesgerichtshof¹⁴⁹⁸ auch die dynamischen IP-Adressen zählen, nur verwendet werden, soweit sie für bestimmte, im Gesetz festgelegte Zwecke, wie etwa zur Abrechnung (§ 97 TKG) oder zur Störungsbeseitigung sowie Missbrauchsbekämpfung (§ 100 TKG) erforderlich sind (§ 96 Abs. 2 Satz 1 TKG).

Gegenstand zahlreicher gerichtlicher Urteile¹⁴⁹⁹ war diese Erforderlichkeit im Falle der Speicherung dynamischer IP-Adressen bei **Flatrate**-Tarifen. Hier wird eine Erhebung und Speicherung von Verkehrsdaten, einschließlich der dynamischen IP-Adressen, für die Abrechnung i.S.d. § 97 TKG grundsätzlich nicht benötigt, da ein pauschales Entgelt vereinbart ist und damit keine Entgeltermittlung nötig ist.¹⁵⁰⁰ Etwas anderes gilt nur dann, wenn der Anschlussinhaber daneben auch kostenpflichtige Dienste über den zur Verfügung stehenden Anschluss in Anspruch nehmen kann. Dann muss der Zugangsanbieter die Möglichkeit haben, diese Leistungen abzurechnen und kann daher entsprechende Verkehrsdaten des Anschlussinhabers speichern.¹⁵⁰¹

Im Hinblick auf den Erlaubnistatbestand des § 100 Abs. 1 TKG, wonach eine Speicherung von Bestands- und Verkehrsdaten zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen, zulässig ist, wurde eine anlasslose Spei-

¹⁴⁹⁶ Nach höchstrichterlicher Rechtsprechung und h.M. handelt es sich auch bei dynamischen IP-Adressen um Verkehrsdaten. Siehe hierzu S.258.

¹⁴⁹⁷ Vgl. zum Streitstand *Hennemann*, S. 162 ff.

¹⁴⁹⁸ Vgl. dazu oben S. 258.

¹⁴⁹⁹ Jüngst *BGH*, Urteil v. 13.1.2011, Az.: III ZR 146/10 in MMR 2011, 341, zuvor in der Berufungsinstanz *OLG Frankfurt*, Urteil v. 16.6.2010, Az.: 13 U 105/07 in MMR 2010, 645, zuvor erstinstanzlich *LG Darmstadt*, Urteil v. 6.6.2007, Az.: 10 O 562/03; *LG Darmstadt*, Urteil v. 25.1.2006, Az.: 25 S 118/05 in MMR 2006, 330, zuvor *AG Darmstadt*, Urteil v. 30.6.2005, Az.: 300 C 397/04 in MMR 2005, 634; *AG Bonn*, Urteil v. 5.7.2007, Az.: 9 C 177/07 in MMR 2008, 203.

¹⁵⁰⁰ *LG Darmstadt*, Urteil v. 25.1.2006, Az.: 25 S 118/05 in MMR 2006, 330 (331); *AG Bonn*, Urteil v. 5.7.2007, Az.: 9 C 177/07 in MMR 2008, 203 (203).

¹⁵⁰¹ *BGH*, Urteil v. 13.1.2011, Az.: III ZR 146/10 in MMR 2011, 341.

cherung der Daten jedenfalls für einen Zeitraum von **sieben Tagen** nach Beendigung der Nutzung als zulässig angesehen.¹⁵⁰² Diese Rechtsprechung führte in der Praxis dazu, dass Zugangsanbieter ihre bis dahin praktizierte Speicherfrist reduzierten und IP-Adressen nur noch sieben oder weniger Tage und teilweise überhaupt nicht mehr speichern¹⁵⁰³.

III. Zugangsanbieter

Es darf nicht übersehen werden, dass ein vorgerichtliches Mitwirkungsmodell auf Seiten der Zugangsanbieter zu Belastungen führt, die über den Status Quo des reinen Auskunftsanspruchsmodells hinausgehen.

1. Art. 12 GG

Aus Sicht der Zugangsanbieter ist insbesondere das Grundrecht der Berufsfreiheit aus Art. 12 GG betroffen.¹⁵⁰⁴

2. Art. 14 GG

Eine Verpflichtung zur Beteiligung der Provider wäre auch vor dem Hintergrund von Art. 14 GG bedeutsam. Dies wäre etwa dann der Fall, wenn im Hinblick auf die Versendung von Warnhinweisen Anpassungen der Betriebsstruktur erforderlich wären oder Neuanschaffungen von nennenswertem Aufwand von Nöten wären. Art. 14 GG würde je nach Ausgestaltung der Einbindung unterschiedlichen Aufwand verursachen. Die für das Vereinigte Königreich angestellten Berechnungen im *Impact Assessment*¹⁵⁰⁵ zum Aufwand für Zugangsanbieter bei Einbindung in die Warnhinweisversendung nach dem Initial Obligations Code veranschaulichen dies.¹⁵⁰⁶ Insoweit ist der Nutzen, den die Einführung des Modells zur Erfüllung des Zweckes erwarten lässt in das Verhältnis zu den entstehenden Kosten zu setzen, wobei die Frage der Kostentragung nach den Erfahrungen im Vereinigten Königreich¹⁵⁰⁷ ein besonderes Augenmerk verlangen.

¹⁵⁰² BGH, Urteil v. 13.1.2011, Az.: III ZR 146/10 in MMR 2011, 341; OLG Frankfurt, Urteil v. 16.6.2010, Az.: 13 U 105/07 in MMR 2010, 645; LG Darmstadt, Urteil v. 6.6.2007, Az.: 10 O 562/03; AG Bonn, Urteil v. 5.7.2007, Az.: 9 C 177/07 in MMR 2008, 203.

¹⁵⁰³ So speichert etwa AOL IP-Adressen nur 5 Tage, Net Cologne 4 Tage, Versatel Deutschland 3 Tage, während Freenet und Kabel Deutschland die IP-Adressen überhaupt nicht mehr speichern, vgl. den „Leitfaden zum Datenzugriff insbesondere für den Bereich der Telekommunikation“ der Generalstaatsanwaltschaft München v. Juni 2011. Die Telekom hatte ihre Praxis in der Vergangenheit dahingehend geändert, dass IP-Adressen nur noch 7 Tage gespeichert werden, vgl. heise online „T-Com speichert IP-Adressen nur noch sieben Tage“ v. 20.02.2007, abrufbar unter: <http://www.heise.de/newsticker/meldung/T-Com-speichert-IP-Adressen-nur-noch-sieben-Tage-148387.html>.

¹⁵⁰⁴ Siehe dazu sogleich S. 310

¹⁵⁰⁵ Siehe dazu S. 137.

¹⁵⁰⁶ Siehe oben S.138.

¹⁵⁰⁷ Siehe oben S. 128.

D. Vorschlag und Prüfung eines vorgerichtlichen Mitwirkungsmodells in Deutschland

I. Regelungsziel und Mittel des vorgerichtlichen Mitwirkungsmodells

1. Regelungsziel: Urheberrechtsschutz

Das Regelungsziel des vorgerichtlichen Mitwirkungsmodells ist es, Urheberrechtsverstöße im Internet zu verhindern oder zu reduzieren und Bewusstsein für den Wert geistigen Eigentums als zentraler Voraussetzung der kulturellen und wirtschaftlichen Basis des Staates zu schaffen oder wieder herzustellen. Ziel des hier vorgestellten Ansatzes ist es dementsprechend, den Urheberrechtsschutz durch ein Mittel zu stärken, das *nicht* über den vorhandenen Auskunftsanspruch nach geltender Rechtslage *unmittelbar* mit einer rechtlichen Konsequenz verbunden ist, sondern das zunächst insbesondere durch Aufklärung Bewusstsein für die Illegalität von nicht autorisierten Downloads im Internet schafft. Rechtsstaatlich hat das Modell den Vorteil, dass Nutzer, die sich von Rechtsverletzungen abhalten lassen, jedenfalls Geltendmachung eines Auskunftsanspruchs verwarnt werden, so dass eine abschließende rechtliche Konsequenz nicht mehr als unangemessen begriffen werden kann.

Das genannte Bewusstsein hat sich in weiten Teilen der Bevölkerung noch nicht durchgesetzt. Die Ursachen hierfür sind vielschichtig.¹⁵⁰⁸ Ein wesentlicher Grund ist die Komplexität des Urheberrechts. Nutzer können nicht jede Erscheinungsform und jede Handlung sicher rechtlich einordnen. Hinzu kommt der Eindruck beim Nutzer, dass Inhalte im Netz einen geringeren Schutz beanspruchen können, als verkörperte Gegenstände. Strukturprobleme entstehen dadurch, dass anders als in der körperlichen Welt, die Technik massenhaften, unautorisierten und unbezahlten Konsum von Inhalten ermöglicht.¹⁵⁰⁹ Die Grenze zwischen legal und illegal ist im Internet schwer zu ziehen, weil vieles janusköpfig ist: Was technisch gleich funktioniert kann rechtlich unterschiedlich zu bewerten sein und umgekehrt. Der Beitrag der Rechtsprechung in diesem Bereich¹⁵¹⁰ ist wichtig. Er reicht aber gerade im derzeitigen deutschen Modell des Auskunftsanspruchs nicht aus, weil er repressiv ansetzt und den Nutzer mit einem Schuldvorwurf konfrontiert, ohne ihm eine sanktionslose Möglichkeit aufzuzeigen, aufgeklärt zu werden und sich für das Recht zu entscheiden.

¹⁵⁰⁸ Siehe oben S. 43.

¹⁵⁰⁹ Siehe dazu oben S. 50.

¹⁵¹⁰ Dazu *Schwartmann*, K&R 2011, Beihefter zu Heft 11, S. 22.

2. Mittel: Kombination von erklärenden Warnhinweisen und gerichtlichen Auskunftsanspruch unter Mitwirkung der Zugangsanbieter

Mittel des Ansatzes zur Erreichung des Zwecks ist eine **Kombination** aus **aufklärenden Warnungen und Auskunftsanspruch**. Dabei geht es weder darum, internetspezifische Angebote zu kriminalisieren, noch darum Rechtsverstöße zu legalisieren. Vielmehr sollen die vorhandenen urheberrechtlichen Wertungen in Lösungsansätze einfließen, die den Bürger erreichen.

a. Aufklärung und Warnung

Das vorgerichtlichen Mitwirkungsmodell setzt dabei wie in Frankreich, England und Irland auf Warnungen des Nutzers, die zunächst weder eine Kriminalisierung oder eine sonstige Sanktion nach sich ziehen. Dem Nutzer können die Wertungen des Urheberrechtsschutzes zunächst durch einen aufklärenden und zugleich warnenden Hinweis nachvollziehbar gemacht werden, damit er sich dazu entscheiden kann, sie im Netz zu achten. Der Ansatz will dabei nicht nur das Bewusstsein für Rechtsüberschreitungen erzeugen, sondern kann über Hinweise zu legalen Angeboten – wie in allen Referenzstaaten –den Zugang zu Kulturgütern im Internet fördern.¹⁵¹¹

b. Auskunft zur Ermöglichung des zivilrechtlichen Ausgleichs

Für den Fall, dass ein Nutzer sich nach Aufklärung und Warnung gegen die Achtung des Urheberrechts entscheidet, muss aus rechtsstaatlicher Sicht und nach den Erfahrungen in den Referenzstaaten eine Sanktion erfolgen¹⁵¹², weil sanktionslose Warnungen auf Dauer keine Verhaltensänderung bewirken. Diese soll aber nur den zivilrechtlichen Ausgleich zwischen Rechteinhaber und Nutzer ermöglichen, der mit Hilfe des vorhandenen gerichtlichen Auskunftsanspruchs vorbereitet wird. Um dies zu gewährleisten bedarf es der Mitwirkung der Zugangsanbieter, die allein im Stande sind, einer bei einem Download im P2P-Bereich durch die Rechteinhaber ermittelten IP-Adresse einen Anschluss zuzuordnen zu können.¹⁵¹³

c. Mitwirkung der Zugangsanbieter

Eine Mitwirkung der Zugangsanbieter ist aus technischen und strukturellen Gründen¹⁵¹⁴ sowohl aktuell, als auch nach dem hier vorgeschlagenen Modell erforderlich.

¹⁵¹¹ Schwartmann, K&R 2011, Beihefter zu Heft 11, S. 22.

¹⁵¹² Siehe unten S. 320.

¹⁵¹³ Siehe oben S. 196 ff.

¹⁵¹⁴ Siehe oben S.196.

aa. Mitwirkung nach derzeitigem Recht

Nach derzeitigem Recht besteht ein Auskunftsanspruch nach § 101 UrhG. Dieser setzt eine richterliche Anordnung voraus. Die Durchsetzung dieses Anspruchs gegenüber dem Provider ist rechtlich und tatsächlich problematisch.¹⁵¹⁵ Die Verwendung der hierdurch erlangten Information ist wenig zielgerichtet. Der hinter einer IP-Adresse stehende Klarname kann sich auf einen wenig gravierenden Einzelfall beziehen oder einen Mehrfachtäter treffen, insbesondere letzterer ist aber für den Rechteinhaber relevant.

bb. Mitwirkung nach dem vorgerichtlichen Mitwirkungsmodell

Das hier vorgeschlagene Modell effektuiert das bestehende System von Auskunftsanspruch und nachfolgender zivilrechtlicher Durchsetzung des urheberrechtlichen Anspruchs gegenüber dem Nutzer. Dies würde nach britischem Vorbild auf der Stufe des **Initial Obligations Code** geschehen. Im dortigen **Impact Assessment** wird dazu ausgeführt:

„Aus tatsächlichen und technischen Gründen ist es derzeit für Rechteinhaber unmöglich die Rechteverletzer mit den häufigsten und schwerwiegendsten Verstößen zu identifizieren, sodass es sehr schwer ist, gezielte zivilrechtliche Schritte gegen diese einzuleiten. Der Gesetzgeber muss also vom Zugangsanbieter verlangen, Anschlussinhaber auf die potentielle Rechtswidrigkeit ihres Verhaltens hinzuweisen, um es zu überprüfen. Auf der anderen Seite ist es ebenso erforderlich, den Rechteinhaber in die Lage zu versetzen, *gezielt* gegen solche Personen vorzugehen, die am schwerwiegendsten gegen Urheberrecht verstoßen.“¹⁵¹⁶

Die Zugangsanbieter sollte zum einen die Pflicht treffen, Warnhinweise an die Anschlussinhaber zu versenden, deren IP-Adresse im Zusammenhang mit der gemeldeten Rechtsverletzung ermittelt wurde. Sie sollte zum anderen die Pflicht treffen, wie im Vereinigten Königreich eine gegenüber Dritten **anonymisierte Verstoßliste** zu führen und diese ab einer bestimmten Anzahl von festgehaltenen Verstößen, dem Rechteinhaber bekannt zu geben.¹⁵¹⁷ Dieser kann dann, wie bisher, im Wege eines gerichtlichen Auskunftsverlangens Namen und Anschrift des Rechteinhabers heraus verlangen. Ob auch weiterhin, wie bislang nach §101 Abs. 9 S. 3 UrhG die vollbesetzte Zivilkammer des Landgerichts befinden muss, wäre vom Gesetzgeber zu überdenken. Der besondere Nutzen der Verstoßliste liegt darin, dass der Rechteinhaber hieraus ersehen kann, welche für ihn anonyme Person häufig oder gravierend Urheberrecht verletzt hat. Auf dieser Basis kann er seinen Auskunftsanspruch gegen den Provider gezielt mit Blick auf solche Fälle beschränken, die für eine gewerbsmäßige Urheberrechtsverletzung im Sinne von § 101 Abs. 2 Nr. 3 UrhG in Betracht kommen.¹⁵¹⁸

¹⁵¹⁵ Siehe oben S. 252 ff.

¹⁵¹⁶ Vgl. *Impact Assessment*, S. 57, Übersetzung Kölner Forschungsstelle für Medienrecht.

¹⁵¹⁷ Siehe oben S. 124.

¹⁵¹⁸ Siehe dazu oben S. 255.

Das **Modell verbindet** damit die als solche sanktionslose **Warnhinweisregelung** über einen effektuierten **Auskunftsanspruch** mit der zivilrechtlichen Durchsetzung des Anspruchs als Sanktion der Rechtsverletzung. Dabei verzichtet der Ansatz aber auf eine Sanktion, die – wie Sperren oder Drosselung von Anschlüssen in Frankreich und Irland – über das derzeit in Deutschland geltende Recht hinaus geht. Da die Warnhinweisregelung selbst keine unmittelbare Sanktion kennt, ist es auch nicht zwingend, dass dem Zugangsanbieter durch den Rechteinhaber ein gerichtsfester Nachweis einer Rechtsverletzung erbracht wird, der über das zur Identifizierung des Anschlussinhabers und der Feststellung der Verletzung hinaus geht.¹⁵¹⁹

Unabhängig davon erfasst der Ansatz über die Warnhinweise insbesondere auch solche Personen, die in Unkenntnis der Rechtslage Urheberrechte im Netz verletzen.¹⁵²⁰ Aber auch Personen, die bewusst gegen Urheberrecht verstoßen, um eigennützig kostenfrei an Inhalte zu gelangen, würden über die Warnhinweise deutlich gemacht, dass sie auf der Verstoßliste geführt werden und einer zivilrechtlichen Inanspruchnahme entgegensehen.

cc. Datenschutzrechtliche Bedachtnahme

Sowohl für eine Versendung von Warnhinweisen, als auch für die Führung der Verstoßliste stellen sich die angesprochenen Fragen im Zusammenhang mit der Vorratsdatenspeicherung.¹⁵²¹

3. Verfassungsrechtliche Fragen einer Inpflichtnahme der Zugangsanbieter

Beim Ansatz des vorgerichtlichen Mitwirkungsmodells würde letztlich zum Schutz des Urheberrechts eine Inpflichtnahme privater Zugangsanbieter erfolgen, die über deren Verpflichtung im Rahmen des Auskunftsanspruches nach dem status quo hinaus ginge. Eine entsprechende Neuregelung müsste einer verfassungsrechtlichen Prüfung Stand halten.

a. Ausgangslage

Die derzeitige Ausgangslage¹⁵²² zeichnet sich dadurch aus, dass Internetpiraterie ein Massenphänomen darstellt, aufgrund dessen Rechteinhaber Umsatzeinbußen beklagen. Der Vorsitzende Richter des für das Urheberrecht zuständigen I. Zivilsenats am Bundesgerichtshof *Joachim Bornkamm*, der in dieser Eigenschaft einen Einblick in das Spannungsfeld hat, fasst die Situation wie folgt zusammen:

¹⁵¹⁹ Siehe zu den möglichen Angaben oben S. 196.

¹⁵²⁰ Siehe oben S. 40 ff.

¹⁵²¹ Siehe oben S. 292.

¹⁵²² Siehe oben S. 19.

„Das Urheberrecht erlebt durch das Internet eine enorme Herausforderung. Es steht im Feuer der Kritik, und zwar von beiden Seiten. Die Urheber und vor allem die Verwerter beklagen den Ausverkauf des geistigen Eigentums; das Urheberrecht stelle ihnen nicht die erforderlichen Mittel zur Verfügung, um ihre Rechte durchzusetzen. Die Nutzer empfinden das Urheberrecht als Hemmschuh, der der erstrebten freien Information im Netz im Wege steht; sie plädieren für einen möglichst ungehinderten Zugang auch zu urheberrechtlich geschützten Inhalten.“¹⁵²³

Nunmehr – so Bornkamm – gehe es darum,

„den Aderlass (zu) stoppen“.¹⁵²⁴

In einer derartigen Spannungslage kann eine Pflicht des Staates zum Schutz privater Rechtsgüter ausgelöst werden. Nach der **Schutzpflichtenlehre**¹⁵²⁵ ist der Staat wegen des objektiven Gehalts der Grundrechte nicht nur dazu verpflichtet, den Bürger vor staatlichen Eingriffen zu schützen, sondern er ist hierzu auch bei Eingriffen Privater verpflichtet.¹⁵²⁶

„Diese Schutzpflicht schließt die Aufgabe ein, geeignete Maßnahmen zu ergreifen, um die Verletzung von Rechtsgütern zu vermeiden, sie gegebenenfalls aufzuklären, die Verantwortung für sie zuzuweisen und den Rechtsfrieden wieder herzustellen“.¹⁵²⁷

Die Vernachlässigung der Schutzpflicht kann vom Betroffenen mit der Verfassungsbeschwerde geltend gemacht werden.¹⁵²⁸ Vor dem Hintergrund der Schutzpflicht erklären sich die zahlreichen Ansätze zum Urheberrechtsschutz in der digitalen Welt auf internationaler und nationaler Ebene.

b. Die widerstreitenden Grundrechtspositionen

Bei einem vorgerichtlichen Mitwirkungsmodell stehen sich Rechtspositionen der Rechteinhaber auf der einen Seite und der Zugangsanbieter auf der anderen Seite gegenüber, die einen „Streit über den Umgang mit Filesharern“ führen.¹⁵²⁹ Die Standpunkte von Nutzern und Rechteinhabern stimmen unter der Prämisse, dass fremdes geistiges Eigentum grundsätzlich nicht unautorisiert zur kostenfreien Nutzung durch Dritte zur Verfügung steht,

¹⁵²³ Bornkamm, Promedia Heft 11, 2011 S. 10.

¹⁵²⁴ Bornkamm, Den Aderlass stoppen; Interview mit dem Kölner Stadt-Anzeiger v. 3.11.2011, <http://www.ksta.de/html/artikel/1320057515791.shtml>.

¹⁵²⁵ Dazu für den Urheberrechtsschutz passim, Seith, Wie kommt der Urheber zu seinem Recht, 2003.

¹⁵²⁶ BVerfGE 56, 54 (80), ständige Rspr.

¹⁵²⁷ BVerfG – Sondervotum Schluckebier, NJW 2010, 833, 852.

¹⁵²⁸ BVerfG 79, 174, 201 f.

¹⁵²⁹ So deren Vertreter Florian Drücke und Oliver Süme, Pro und Contra Warnhinweismodell, Ein Streit über den Umgang mit Filesharern, <http://www.lto.de/de/html/nachrichten/5062/pro-und-contra-warnhinweismodell-ein-streit-ueber-den-umgang-mit-filesharern/>.

demgegenüber rechtlich überein. Der Nutzer möchte einen möglichst kostengünstigen, schnellen und unkomplizierten Zugang zu urheberrechtlich geschützten Inhalten im Netz. Die Kulturschaffenden und Rechteinhaber haben dasselbe Interesse, soweit es um den verbesserten Zugang zu kulturellen Inhalten über das Internet geht, sind aber darauf angewiesen, dass dies mit ihrem Einverständnis und zu wirtschaftlich tragfähigen Konditionen geschieht.¹⁵³⁰

Aus diesem Grund liegt der rechtliche Fokus im Rahmen dieser Untersuchung in einer Gegenüberstellung der Grundrechtsposition der Rechteinhaber aus der **Eigentumsfreiheit** auf der einen und der Zugangsanbieter aus der **Berufsfreiheit** auf der anderen Seite.

c. Ausgestaltung der Eigentumsfreiheit der Rechteinhaber

Die Bedeutung des geistigen Eigentums als grundrechtliche Position des Rechteinhabers¹⁵³¹ aus Art. 14 GG¹⁵³², zu deren Schutz Zugangsanbieter in die Pflicht genommen würden, fasst das Bundesverfassungsgericht wie folgt zusammen:

„Zu den konstituierenden Merkmalen des Urheberrechts als Eigentum im Sinne der Verfassung gehören die grundsätzliche Zuordnung des vermögenswerten Ergebnisses der schöpferischen Leistung an den Urheber im Wege privatrechtlicher Normierung sowie seine Freiheit, in eigener Verantwortung darüber verfügen zu können. (...) Eingriffe in das Verwertungsrecht des Urhebers können freilich nur durch ein gesteigertes öffentliches Interesse gerechtfertigt werden.“¹⁵³³

Zur wirtschaftlichen Bedeutung tritt das Urheberpersönlichkeitsrecht hinzu, das den Schutz im Hinblick auf Art. 2 GG intensiviert und das in Art. 1 Abs. 1 iVm. Art. 2 Abs. 1 GG verankert und einfachrechtlich in §§ 12 bis 14 UrhG niedergelegt ist. Es ist im Wesentlichen unbestritten, dass im digitalen Zeitalter durch illegales Verhalten im Internet erheblich in das Eigentumsrecht der Urheber eingegriffen wird und dass es hierfür einer rechtlichen Lösung bedarf.¹⁵³⁴

Dabei ist aber zu beachten, dass Urheberrechtsschutz nicht unbegrenzt gilt und vor dem Hintergrund der Sozialpflichtigkeit des Eigentums in den Schranken des Urheberrechts konkretisiert ist.

¹⁵³⁰ *Schwartmann*, K&R 2011, Beihefter zu Heft 11, S. 22.

¹⁵³¹ Zusammenfassend *Kirchhof*, Gesetzgebungsauftrag zum Schutz des geistigen Eigentums gegenüber modernen Vervielfältigungstechniken, S. 10 f.

¹⁵³² Eingehend *Hennemann*, S. 78 f. und auf Seite 80 zu weiteren tangierten Verfassungspositionen aus Art. 5 Abs. 1 und 3 GG sowie Art. 12. Vgl. auch *Schwartmann* in Müller (Hrsg.), Staat und Recht, S. 386.

¹⁵³³ 1 BvR 2742/08 v. 21.12.2010, S. 5 des Entscheidungsabdrucks.

¹⁵³⁴ Siehe oben S. 19.

„Im Einzelnen ist es Sache des Gesetzgebers, im Rahmen der inhaltlichen Ausprägung des Urheberrechts nach Art. 14 Abs. 1 Satz 2 GG sachgerechte Maßstäbe festzulegen, die eine der Natur und der sozialen Bedeutung des Rechts entsprechende Nutzung und angemessene Verwertung sicherstellen.¹⁵³⁵ Dabei hat der Gesetzgeber einen verhältnismäßig weiten Entscheidungsraum.¹⁵³⁶“

Den angesprochenen Entscheidungsspielraum gilt es vor dem Hintergrund der beschriebenen Phänomene von Rechtsverletzungen im Internet bei Erwägung der verfassungsrechtlichen Rahmenbedingungen des vorgerichtlichen Mitwirkungsansatzes auszuloten und in ein **angemessenes Verhältnis** zu anderen Grundrechtspositionen zu setzen.

Im Fokus der Untersuchung steht die Frage, inwieweit Zugangsanbieter im Rahmen einer Lösung zum Schutz des Urheberrechts in die Pflicht genommen werden können. Zugangsanbieter lehnen jede Beteiligung über den aktuellen Stand hinaus ab. Warnhinweismodelle werden als tatsächlich problematisch und rechtlich unzulässig begriffen¹⁵³⁷Der Vorsitzende des Verbandes der deutschen Internetwirtschaft e.V. eco bringt diesen Standpunkt wie folgt auf den Punkt:

„Wenn „Warnhinweise (...) durch die Provider selbst versendet werden sollen, würde sich aus Kundensicht deren Rolle von einem neutralen Kommunikationsdienstleister zu einem parteiischen Überwachungsprovider wandeln. Einen so tiefgreifenden Bruch in der Vertrauensbeziehung zum Verbraucher wollen und können die Provider nicht hinnehmen. Ganz zu schweigen davon, dass dadurch ein Sonderweg für eine einzige Zielgruppe innerhalb der Kreativindustrie eingeschlagen würde.“ (...) Die Problematik illegaler Downloads (habe sich) seit Einführung des Auskunftsanspruches erheblich entschärft (...). Eine Rechtsprivatisierung und die Aufweichung von Datenschutz und Fernmeldegeheimnis ohne richterliche Kontrolle (sein) weder angemessen noch erforderlich.“¹⁵³⁸

Die vorgetragenen Punkte betreffen verfassungsrechtlich die Frage nach der Zulässigkeit einer Inpflichtnahme Privater bei der Bekämpfung von Rechtsverletzungen im Internet, die an der **Berufsfreiheit** der Zugangsanbieter zu messen ist.

¹⁵³⁵ Vgl. BVerfGE 31, 229, 240 f; 79, 1, 25.

¹⁵³⁶ Vgl. BVerfGE 21, 73, 83; 79, 29, 40.

¹⁵³⁷ Süme, <http://www.lto.de/de/html/nachrichten/5062/pro-und-contra-warnhinweismodell-ein-streit-ueber-den-umgang-mit-fileshareern/>.

¹⁵³⁸ Süme, <http://www.lto.de/de/html/nachrichten/5062/pro-und-contra-warnhinweismodell-ein-streit-ueber-den-umgang-mit-fileshareern/>.

d. Inpflichtnahme und Berufsfreiheit der Zugangsanbieter nach Art. 12 GG

Eine Inpflichtnahme der Zugangsanbieter im Rahmen eines vorgerichtlichen Mitwirkungsmodells wirft Fragen hinsichtlich der verfassungsrechtlichen Rechtfertigung eines solchen Eingriffs auf.

Vorab sei darauf hingewiesen, dass eine solche Inpflichtnahme zur Durchsetzung staatlicher oder privater Interessen durchaus üblich ist, wie beispielsweise die umfangreiche Inpflichtnahme Privater im Rahmen der Produktverantwortung im Kreislaufwirtschafts- und Abfallrecht zeigt, die mittlerweile anerkannt ist, aber bei ihrer Einführung sowohl auf Seiten der Abfallwirtschaft – hier namentlich unter Berufung auf die Berufsfreiheit – als auch auf Seiten der Verbraucher auf Widerstand stieß.¹⁵³⁹

aa. Eingriff in den Schutzbereich von Art. 12 Abs. 1 GG

Eine **Inpflichtnahme** von Zugangsanbietern zur Versendung von Warnhinweisen greift in den Schutzbereich von Art. 12 Abs. 1 GG ein.¹⁵⁴⁰

bb. Verfassungsrechtliche Rechtfertigung

1) *Regelung der Berufsausübung*

Dabei ist aber verfassungsrechtlich zu berücksichtigen, dass es sich bei den genannten Maßnahmen in der Terminologie des Bundesverfassungsgerichts um eine sog. **Regelung der Berufsausübung** handelt, die vorliegt, wenn der Eingriff nicht einen Beruf als solchen betrifft, sondern „die eigentliche Berufstätigkeit als Grundlage der Lebensführung unberührt lässt“.¹⁵⁴¹ Bei gesetzlicher Implementierung eines vorgerichtlichen Mitwirkungsmodells stellt sich die Frage, ob eine Indienstnahme privater Zugangsanbieter für die Erfüllung der aus Art. 14 GG gebotenen Aufgabe zum Schutz des geistigen Eigentums verfassungsrechtlich zulässig wäre. Ob es sich dabei um eine staatliche oder private Aufgabe handelt kann dahin stehen, weil die Verfassung keine kategorische Trennung von „Staatsaufgaben“ und „privaten Aufgaben“ kennt und dem Gesetzgeber einen weiten Gestaltungsspielraum zuerkennt,

„welche Pflichten zur Sicherstellung von Gemeinwohlbelangen er Privaten im Rahmen ihrer Berufstätigkeit auferlegt (vgl. BVerfGE 109, 64, 85).“¹⁵⁴²

Bei der Entscheidung, welche Private er in Dienst nimmt, hat der Staat ebenfalls einen weiten Beurteilungsspielraum. Zur Auferlegung der Pflicht auf Anbieter öffentlich zugänglicher Telekommunikationsdienste, Telekommunikationsdaten ihrer Kunden für sechs Monate zu speichern hat das Bundesverfassungsgericht entschieden, dass insoweit

¹⁵³⁹ Dazu *Schwartmann/Pabst*, Umweltrecht, Rn. 445 ff.

¹⁵⁴⁰ Siehe oben S. 302.

¹⁵⁴¹ BVerfGE 75, 246, 274.

¹⁵⁴² BVerfGE 125, 260, 261 f.

„eine hinreichende Sach- und Verantwortungsnähe zwischen der beruflichen Tätigkeit und der auferlegten Verpflichtung“ (vgl. BVerfGE 95, 173, 187)

insoweit reicht.¹⁵⁴³ Die Frage der Entschädigung¹⁵⁴⁴ und Kostenverteilung im Rahmen der Indienstnahme bedürfte einer eingehenden Prüfung, nachdem eine Abschätzung der Kosten möglich ist.

2) *Verhältnismäßigkeit einer Inpflichtnahme der Zugangsanbieter*

Ein Eingriff in die Berufsausübungsfreiheit unterliegt nach der Stufentheorie des Bundesverfassungsgerichts¹⁵⁴⁵ der Schranke des Übermaßverbotes. Er ist zulässig, wenn er in einem vernünftigen Verhältnis zu dem gegebenen Anlass und dem damit verbundenen Zweck steht.¹⁵⁴⁶ Das ist bei einer Berufsausübungsregelung der Fall, wenn sich

„vernünftige Gründe des Gemeinwohls dafür finden lassen. Gesichtspunkte der Zweckmäßigkeit sind ausreichend, wenn die Regelung für die Betroffenen zumutbar und nicht übermäßig belastend ist (vgl. BVerfGE 7, 377, 406).“¹⁵⁴⁷

Es käme also auf die verhältnismäßige Ausgestaltung der Inpflichtnahme im konkreten Fall an. Damit ist nach Legitimität des möglichen staatlichen Handelns, sowie nach seiner Eignung zur Erreichung des Zwecks, nach seiner Erforderlichkeit und seiner Angemessenheit zu fragen.

a) *Legitimer Zweck*

Wenn die staatliche Bekämpfung von Internetpiraterie ein Ziel verfolgen würde, das legitim nicht angestrebt werden darf, würden sich staatliche Eingriffe zu diesem Zweck von vornherein verbieten. Das wäre dann der Fall, wenn Internetpiraterie aus gesamtwirtschaftlichen Gründen nicht unerwünscht wäre und dies sich auf die rechtliche Beurteilung auswirken würde.

Bisweilen wird die gesamtwirtschaftliche Schädlichkeit von Rechtsverletzungen im Internet in Abrede gestellt, so dass ein staatlicher Eingriff aus ökonomischen Gründen insgesamt für nicht erforderlich gehalten wird.¹⁵⁴⁸ So verhält es sich auch mit der Frage, inwiefern die Anzahl illegaler Downloads unmittelbar für verlorene entgeltliche Vorgänge steht und ob jeder illegale Download zu einem verlorenen entgeltlichen Geschäft führt, weil der

¹⁵⁴³ BVerfGE 125, 260, 361 f.

¹⁵⁴⁴ BVerfGE 30, 292, 311; 125, 260, 362.

¹⁵⁴⁵ BVerfGE 7, 377, 405 ff.

¹⁵⁴⁶ BVerfGE 15, 226, 234.

¹⁵⁴⁷ BVerfGE 16, 286, 297.

¹⁵⁴⁸ In diesem Sinne das Parteiprogramm der Piratenpartei: „Wir sind der Überzeugung, dass die nichtkommerzielle Vervielfältigung und Nutzung von Werken als natürlich betrachtet werden sollte und die Interessen der Urheber entgegen anders lautender Behauptungen von bestimmten Interessengruppen nicht negativ tangiert. Es konnte in der Vergangenheit kein solcher Zusammenhang schlüssig belegt werden. In der Tat existiert eine Vielzahl von innovativen Geschäftskonzepten, welche die freie Verfügbarkeit bewusst zu ihrem Vorteil nutzen und Urheber unabhängiger von bestehenden Marktstrukturen machen können.“
<http://www.piratenpartei.de/navigation/politik/urheberrecht-und-nicht-kommerzielle-vervielfaeltigung>.

Nutzer dasselbe Produkt vielleicht nicht legal erworben hätte¹⁵⁴⁹. Ob diese Argumentation zutrifft kann hier dahinstehen, weil diese Fragen im Hinblick auf Rechtsverletzungen in konkreten Fällen belanglos sind. Die Handlungspflicht des Staates zum Schutz von Grundrechtspositionen kann aus ökonomischen Gründen nicht verzichtbar werden. Die in Studien gestellte Frage, inwiefern die Anzahl illegaler Downloads unmittelbar für verlorene entgeltliche Vorgänge steht und ob jeder illegale Download zu einem verlorenen entgeltlichen Geschäft führt, weil der Nutzer dasselbe Produkt vielleicht nicht legal erworben hätte¹⁵⁵⁰ ist für die Erfüllung des staatlichen Schutzauftrags unbeachtlich. Der Staat muss Rechtsverletzungen auch dann entgegenwirken, wenn die entsprechende Handlung volkswirtschaftlich betrachtet sinnvoll wäre.¹⁵⁵¹ Die ökonomische Betrachtung der Onlinepiraterie ist lediglich von Bedeutung, um die Rahmenbedingungen der Kreativwirtschaft für Innovation, Wachstum und Beschäftigung¹⁵⁵² einschätzen zu können. Sie kann das wirtschaftliche Ausmaß des Problems erfassen und dem Gesetzgeber einen Indikator für die Dringlichkeit und volkswirtschaftliche Relevanz seines Handelns oder Unterlassens zu geben. Das staatliche Handeln im Wege eines vorgerichtlichen Mitwirkungsmodell würde also einen legitimen Zweck allein deswegen verfolgen, weil Urheberrechtsverletzungen im Internet urheberrechtswidrig sind.

b) Eignung des vorgerichtlichen Mitwirkungsmodells

aa) Einschätzungsspielraum des Gesetzgebers bei Beurteilung der Eignung

Will der Gesetzgeber zur Ausgestaltung des Spielraums zwischen kollidierenden Grundrechten tätig werden, liegen dem entsprechende Wertungen darüber zugrunde, ob und inwieweit eine Maßnahme **geeignet** ist, das gesteckte Ziel zu erreichen. Im Rahmen dieser Bewertung hat der Gesetzgeber auf der Basis einer Einschätzung der Gefahrenlage eine Prognose zur Wirksamkeit möglicher Gegenmaßnahmen vorzunehmen. Hierbei wird dem Gesetzgeber ein deutlicher Spielraum zugestanden, dessen Ausmaß im Einzelfall von der Eigenart des jeweiligen Sachbereichs, von der Möglichkeit einer Beurteilung der Sachlage auf sicherer, empirisch abgestützter Grundlage und von der Bedeutung der im Einzelfall betroffenen Rechtsgüter abhängt.¹⁵⁵³ Die Grenze zur Verfassungswidrigkeit ist dabei erst dann überschritten, wenn eine vom Gesetzgeber ergriffene Maßnahme sich als **offensichtlich oder schlechthin ungeeignet darstellt**.¹⁵⁵⁴

¹⁵⁴⁹ So auch *Hargreaves*, S. 73.

¹⁵⁵⁰ So auch *Hargreaves*, S. 73.

¹⁵⁵¹ Auch wenn der Spender einer Niere gesundheitlich keinen Schaden nimmt und das zur Verfügung gestellte Organ den Empfänger lebens- und damit arbeitsfähig erhält und der Organhandel damit volkswirtschaftlich sinnvoll ist, bleibt er illegal. Prostitution ist zivilrechtlich sittenwidrig und gewerberechtlich nicht vom Schutz der Berufs- und Gewerbefreiheit erfasst, obwohl sie volkswirtschaftlich nutzt.

¹⁵⁵² *Mundelius*, S. 4.

¹⁵⁵³ Vgl. *BVerfGE* 83, 130, 141 - Josephine Mutzenbacher. Auch *Grzeszick* in: Maunz/Dürig, Grundgesetz, 62. Ergänzungslieferung 2011, Art. 20 Rn. 122 m.w.N. zur Rechtsprechung.

¹⁵⁵⁴ Hierzu *Grzeszick* in: Maunz/Dürig, Grundgesetz, 62. Ergänzungslieferung 2011, Art. 20 Rn. 122.

Gerade im Hinblick auf neuere Entwicklung und damit verbundene Unwägbarkeiten ist es dem Gesetzgeber von daher auch gestattet, Maßnahmen zu erproben. Der Prognosespielraum kann in diesen wie auch in anderen Fällen zur Folge haben, dass die gesetzten Ziele entgegen der Erwartung des Gesetzgebers nicht oder nicht gänzlich erreicht werden. Insofern verlangt die Bindung des Gesetzgebers an das Gebot der Geeignetheit nicht absolute Zielgenauigkeit, so aber doch Korrekturen, sobald mögliche Fehleinschätzungen sichtbar werden. Seine Prognose muss im Zeitpunkt des gesetzgeberischen Handelns sachgerecht und vertretbar sein.¹⁵⁵⁵ Auch wenn Wirkung und Wirksamkeit von Warnhinweisen noch nicht abschließend geklärt sind, so lässt sie sich jedenfalls nicht ausschließen. Grundsätzlich ist ein Modell unter Einbindung von Warnhinweisen also von der dem Gesetzgeber eingeräumten Einschätzungsprärogative umfasst.¹⁵⁵⁶

bb) Effizienz von Warnhinweisen

Unter Berücksichtigung dieses Beurteilungsspielraums ist die Frage nach der Wirksamkeit von Warnhinweisen im Hinblick auf eine Reduzierung von Urheberrechtsverletzungen zu beantworten. An dieser Stelle kann für Deutschland auf die Erfahrungen in den Referenzstaaten zurück gegriffen werden, in denen ein Warnhinweismodell bereits Anwendung findet, nämlich Frankreich und Irland. Zudem können Erhebungen im Vereinigten Königreich ausgewertet werden, wo das Warnhinweismodell bereits gesetzlich verankert, aber noch nicht umgesetzt ist.

(1) Frankreich

Betrachtet aus der Perspektive der Rechteinhaber hat die Einführung des Warnhinweissystems im französischen Rechtssystem zu einer Ergänzung ihres Handlungsspielraums beigetragen. Durch die Neuregelung werden die Rechteinhaber bzw. deren Beauftragte ermächtigt, IP-Adressen von potentiellen Rechteinverletzern zu sammeln. Ein eigener Auskunftsanspruch gegenüber den Internetzugangsanbietern steht ihnen auch nach dem neuen System nicht zu und Kenntnis über den Anschlussinhaber bzw. potentiellen Täter kann weiterhin nur mittels Akteneinsicht im Strafverfahren erlangt werden. Über die Initiierung des Warnhinweisverfahrens vor der Hadopi ist es den Rechteinhaber jedoch möglich, auf den potentiellen Rechteinverletzer bzw. den Anschlussinhaber als diesem näher stehende Person, einzuwirken. Die Einführung des Fahrlässigkeitstatbestandes in Art. R.335-5 Gesetzbuch über das geistige Eigentum hat zudem dazu geführt, dass der Anschlussinhaber in die Verantwortung genommen wird. Die schwer nachweisbare Frage der Täterschaft bei einer Urheberrechtsverletzung ist damit auf eine zweite Stufe gerückt. In erster Linie kann bereits erreicht werden, dass der Zugriff auf das Tatmittel, nämlich das Internet, durch Sperrung des Zugangs verhindert wird.

¹⁵⁵⁵ Vgl. grundlegend *BVerfGE* 30, 250, 263.

¹⁵⁵⁶ An diesem Maßstab *BVerfGE* 83, 130, 140 ff. - Josephine Mutzenbacher.

Als ein Manko in der Wirksamkeit des französischen Modells stellt sich die Begrenzung des Handlungsspielraums auf **Peer-to-Peer-Netzwerke** dar. Da die Initiierung des Hinweisverfahrens der Ermittlung der IP-Adresse durch die Rechteinhaber bzw. deren Bevollmächtigten bedarf, werden andere Techniken, etwa Abruf- und Streamingdienste, nicht vom System erfasst. Die Hadopi ist hier bestrebt, die technischen und juristischen Rahmenbedingungen im Hinblick auf eine Ausweitung des Handlungsspielraums auszuloten.¹⁵⁵⁷

Angesichts der großen Zahl an Verfahrensanträgen vor der Rechtsschutzkommission erscheint die Feststellung gerechtfertigt, dass das System von Seiten der Rechteinhaber grundsätzlich angenommen wurde. Die neu per Gesetz verankerte Verantwortlichkeit des Anschlussinhabers für die über seinen Internetzugang begangenen Urheberrechtsverletzungen ermöglichen den Rechteinhabern einen mittelbaren Zugriff auf den potentiellen Rechteverletzer außerhalb des strafrechtlichen bzw. zivilrechtlichen Verfahrens. Die Durchsetzung von insbesondere Schadensersatzansprüchen gegenüber dem Rechteverletzer ist von der Weiterleitung des Falles an die Staatsanwaltschaft abhängig. Die vergleichsweise geringe Anzahl an Anhörungen, die nunmehr in der dritten Verfahrensstufe und damit vor Weiterleitung an die Staatsanwaltschaft, durchgeführt werden,

- weist darauf hin, dass nur eine vergleichsweise geringe Anzahl an Anschlussinhabern mehrfach, d.h. ein drittes Mal innerhalb eines Jahres, bei Urheberrechtsverstößen ermittelt wurde;
- relativiert sich jedoch aufgrund des erzieherischen Ansatzes und der damit einhergehenden Praxis der Hadopi, einzelne Fälle von Urheberrechtsverletzungen als einheitlichen Sachverhalt zu behandeln, so dass nicht jeder begründete Antrag in einen Warnhinweis mündet;
- ist insofern noch nicht gänzlich aussagekräftig, als eine Anzahl von Verfahren noch in der Bearbeitung und nicht abschließend behandelt sind.

(2) Irland

Im Hinblick auf die **Wahrung und Durchsetzung von Urheberrechten** im Internet ist die *Wirkung* der Warnhinweis-Regelung zunächst durch ihren Anwendungsbereich beschränkt.¹⁵⁵⁸ Die Auswirkungen des „*Graduated Response*“-Verfahrens wirken nur auf den Teil der P2P-Nutzer in Irland, die Kunden von Eircom sind. Darüber hinaus hat das Programm keinen messbaren positiven Effekt im Sinne einer Reduzierung von Urheberrechtsverletzungen.¹⁵⁵⁹

Neben dem Auskunftsanspruch, den auch bisher schon der Rechteinhaber gegenüber dem Zugangsprovider zur individuellen Verfolgung seiner Rechte gerichtlich geltend machen

¹⁵⁵⁷ Vgl. *Rapport d'activité 2010*, Tätigkeitsbericht der Hadopi über ihre Aktivitäten in den ersten eineinhalb Jahren ihres Bestehens, September 2011, abrufbar unter:

<http://www.hadopi.fr/sites/default/files/page/pdf/rapport-d-activite-hadopi.pdf>, S. 8.

¹⁵⁵⁸ Siehe oben S. 154 ff.

¹⁵⁵⁹ Vgl. oben zur nicht gestatteten Freigabe der zugrunde liegenden Daten.

konnte, der darüber hinaus aber indirekt auch eine abschreckende Wirkung bei den Nutzern entfaltet, tritt damit ein weiteres präventiv-verhaltenssteuerndes Mittel zur Rechterhaltung. Dabei kommt der **Warnhinweis-Regelung** in zweifacher Hinsicht gegenüber dem Auskunftsanspruch ein „Mehrwert“ zu. Zum einen ist der Effekt der Verhaltenssteuerung bei der Warnhinweis-Regelung mit ihrem mehrstufigen Verfahren konkreter und **„zielgenauer“**. Während nämlich der Nutzer bei dem Auskunftsanspruch die eher abstrakte Gefahr gewärtigen muss, dass der Rechteinhaber, nachdem er erst einmal im Prozesswege von dem Provider Auskunft erlangt hat, gegen ihn vorgeht, wird er im Rahmen der Warnhinweis-Regelung wiederholt individuell aufgeklärt und ver- bzw. gewarnt sowie mit einer rechtlichen Konsequenz konfrontiert. Zum anderen erfordert die Warnhinweis-Regelung kein – für alle Beteiligten zeit- und kostenaufwendiges – Gerichtsverfahren. Soweit das „*Graduated Response*“-Verfahren Wirkung zeigt, ist anzunehmen, dass die Anzahl von Gerichtsverfahren zur Auskunftserlangung abnimmt. Denn die Rechteinhaber sind in der Regel eher an dem präventiv-verhaltenssteuernden Effekt interessiert, der mit der *Möglichkeit* der Rechtsdurchsetzung verbunden ist, als daran, tatsächlich einzelne Urheberrechteverletzer repressiv auf Unterlassung und Ersatz des – meist schwierig zu beziffernden – Schadens in Anspruch zu nehmen.¹⁵⁶⁰ Ansonsten hat das „*Graduated Response*“-Verfahren keinen Nutzen im Hinblick auf die Geltendmachung eines Auskunftsanspruchs bzw. ihre Vorbereitung. **Warnhinweis-Regelung und Auskunftsanspruch** stehen insoweit **unverbunden nebeneinander**.¹⁵⁶¹ Im Rahmen des Verfahrens werden auf Seiten des Zugangsanbieters offenbar keine Listen o. ä. geführt, in denen besonders auffällig gewordenen IP-Adressen zusammengefasst sind, auf die sich dann ein Auskunftsverlangen konzentrieren könnte.

Negative Effekte¹⁵⁶² in rechtlicher Hinsicht bestehen darin, dass der adressierte, mit dem Vorwurf einer Urheberrechtsverletzung konfrontierte Kunde, nicht auch der Nutzer des Anschlusses und Rechteverletzer sein muss und dass im Übrigen Fehlversendungen sowie Anschlussunterbrechungen oder –sperrungen „unschuldige“ Kunden in ihren Rechten beeinträchtigen können. Ansonsten sind unter rechtlichen Gesichtspunkten keine nachteiligen Wirkungen des „*Graduated Response*“-Verfahrens ersichtlich. Insbesondere sind mit dem Verfahren für die Kunden in Irland insoweit keine negativen datenschutzrechtlichen oder unangemessen ihre Verfassungsrechte einschränkende Auswirkungen verbunden,

¹⁵⁶⁰ So sind denn auch im Anschluss an die gerichtlichen Auskunftsverfahren in den Jahren 2005 – 2007 nur in drei Fällen Verfahren gegen die mutmaßlichen Rechteverletzer eingeleitet und im Übrigen einzelne Vergleiche abgeschlossen worden. Nach Aussage des High Court sind dabei zur Identifizierung der Personen im Wege gerichtlicher Anordnungen (2005 – 2007) Anwaltskosten in Höhe von insgesamt € 680.000 angefallen, während auf der Grundlage von Vergleichsabschlüssen lediglich ein Betrag in Höhe von € 80.000 „eingewonnen“ wurde.

¹⁵⁶¹ Der von einer Musikproduktionsgesellschaft gegenüber Eircom im Rahmen des Warnhinweisverfahrens zu erbringenden „Nachweis“ muss freilich dem Standard eines Beweises entsprechen, der in der Vergangenheit erbracht worden ist und in Zukunft verlangt werden dürfte, um im Rahmen eines Prozesses vor einem irischen Gericht „*Norwich Pharmacal Orders*“ („*Disclosure Orders*“) zur Auskunftserteilung zu erhalten.

¹⁵⁶² Diese berühren im eigentlichen Sinne nicht die Wirksamkeit des „*Graduated Response*“-Verfahrens, die an dem beabsichtigten Regelungsziel zu messen ist.

als der irische High Court eben dies in seiner Entscheidung vom 16. April 2010 verneint hat.¹⁵⁶³ In diesem Zusammenhang ist namentlich zu berücksichtigen, dass die Sanktionen der Warnhinweis-Regelungen auch in dem Provider-Vertrag vorgesehen sind, den der Nutzer freiwillig mit dem Diensteanbieter abschließt.

(3) *Vereinigtes Königreich*

Im Vereinigten Königreich werden nach dem Regelungssystem des Digital Economy Act (DEA) alle Anschlussinhaber, denen eine wiederholte Rechtsverletzung vorgeworfen wird, systematisch in einer **Liste gemeldeter Rechtsverstöße** erfasst. Die anonymisierte Liste ist insofern Indikator für das Ausmaß begangener Rechtsverletzungen, da sie die einzelnen Rechtsverstöße aufführt. Dem Rechteinhaber ist es auf diese Weise möglich, Mehrfachtäter oder Fälle größeren Ausmaßes zu identifizieren, ohne dass ihm bis zu diesem Zeitpunkt jedoch die genaue Identität des Anschlussinhabers bekannt ist. Die gerichtliche Verfolgung und Geltendmachung von Ansprüchen kann er hierdurch auf **besonders signifikante Fälle beschränken** und die Erfolgchancen einer kostenintensiven Rechtsverfolgung wegen der günstigeren Beweislage ungleich erhöhen. Entscheidet er sich zur Rechtsverfolgung bedarf es einer richterlichen Anordnung zur Auskunftserteilung über die Identität des Anschlussinhabers, wodurch datenschutzrechtliche Interessen Berücksichtigung finden.¹⁵⁶⁴ Im Unterschied zu Irland sind **Warnhinweisversendung und Auskunftsanspruch also miteinander verbunden**.

Für den Anschlussinhaber trägt das Verfahren nach dem DEA vor allem aus Gründen der Aufklärung zur Verbesserung bei. Bevor gerichtliche Schritte gegen den Anschlussinhaber eingeleitet werden, erhält er nun zuvor mehrfach Warnhinweise und hat hinreichend Gelegenheit, sein Verhalten hieran auszurichten. Rechteverletzer, die nach geltender Rechtslage vor Inkrafttreten des DEA hätten unmittelbar rechtlich verfolgt werden können, sind nun angehalten, ihr rechtswidriges Verhalten aufzugeben, bevor sie auf der Liste der gemeldeten Rechtsverstöße geführt werden. Die Rechtslage mit Verabschiedung des DEA sieht insofern sowohl aus Perspektive des Anschluss- als auch des Rechteinhabers ein effektiveres, zielgerichteteres und gerechteres System vor. Zudem wird durch das neue System die Justiz entlastet.¹⁵⁶⁵

cc) Beschränkung auf P2P

Der Eignung des vorgerichtlichen Mitwirkungsmodells könnte entgegen stehen, dass sich dieses aus technischen und datenschutzrechtlichen Gründen – wie auch die Modelle in allen Referenzstaaten – nur auf die Bekämpfung von Rechtsverletzungen beschränkt, die über P2P-Netzwerke begangen werden. Dabei ist zu berücksichtigen, dass über illegale P2P-Nutzung absolut betrachtet **weltweit mit 16,37 Prozent** die mit Abstand meisten

¹⁵⁶³ Siehe oben S. 161.

¹⁵⁶⁴ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 228.

¹⁵⁶⁵ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 228.

unautorisierten Downloads erfolgen.¹⁵⁶⁶ In Deutschland ist davon auszugehen, dass etwa 20 Prozent der illegalen Nutzung über P2P-Netzwerke erfolgen.¹⁵⁶⁷ Die mangelnde Eignung wegen der Beschränkung auf P2P-Netzwerke war auch Gegenstand, des Verfahrens im Vereinigten Königreich gegen den Digital Economy Act (DEA) vor dem High Administrative Court, wo die klagenden Zugangsanbieter vortrugen, dass im Vereinigten Königreich **37 Prozent** der Urheberrechtsverletzungen im Internet durch illegales P2P-Filesharing verursacht würden und das alleinige Vorgehen gegen diese Nutzungsart ungeeignet sei, Internetpiraterie zu bekämpfen. Mit dem High Court ist insofern zu berücksichtigen, dass es eine flächendeckende und umfassende Lösung für die Bekämpfung von Rechtsverletzungen im Internet nicht geben kann, sondern dass es auf die Möglichkeit einer nennenswerten Verbesserung des Status Quo ankommt, was bei einer Lösung, die 37 Prozent des Problems ins Auge fassen kann der Fall ist.¹⁵⁶⁸ Auch, dass die Migration von Rechteinhaltern zu alternativen Pirateriemitteln möglich ist, ist im Hinblick auf die Eignung insofern unbeachtlich, als die Möglichkeiten der Umgehung dem Recht immanent ist. Ohnedies würde eine Umgehung nur den Anteil der Nutzer interessieren, die nachhaltig Rechtsverletzungen begehen. Diese sind indes insgesamt nicht so sehr im Fokus des auf Aufklärung setzenden vorgerichtlichen Mitwirkungsmodells wie die Anschlussinhaber, die sich entweder der Illegalität ihres eigenen Handelns ohne aufklärenden Warnhinweis nicht bewusst sind, oder ihren Anschluss aus Unwissen oder Unachtsamkeit nicht hinreichend gegenüber dessen missbräuchlicher Nutzung etwa durch Angehörige schützen. Diese für Aufklärung offene Gruppe würde ein Warnhinweis zu einem hohen Prozentsatz mit seiner Aussage erreichen. Dass der Ansatz erfolgt verspricht ergeben Daten der IFPI für Frankreich. Danach ist die P2P-Nutzung dort im Zeitraum zwischen April 2010 und April 2011 um insgesamt **31 Prozent** gesunken und zwar mit einem deutlichen Einbruch zum Zeitpunkt der Versendung der ersten Warnhinweise.¹⁵⁶⁹

dd) Zwischenergebnis

Auch wenn die Effizienz von Warnhinweisen in den Referenzstaaten nicht zur vollen Überzeugung nachgewiesen ist, so sprechen jedenfalls keine Gründe gegen die Eignung eines Warnhinweismodells zur Vorbereitung eines Auskunftsanspruchs. Absolut gesehen ist es ein Manko, dass ein Warnhinweismodell nur P2P-Nutzer erfasst. Auf der anderen Seite kann der Gesetzgeber – wenn er aus datenschutzrechtlichen und technischen Gründen keine flächendeckende Lösung ermöglichen kann – nicht auf Untätigkeit verfallen, wenn ein erfolgversprechendes Mittel eine Teillösung ermöglicht. Das Absinken der P2P-Nutzung in Frankreich nach Versendung der Warnhinweise deutet auf Effizienz in diesem

¹⁵⁶⁶ *Envisional*, S. 51ff. Siehe dazu oben S. 74.

¹⁵⁶⁷ Eigene Berechnung auf Grundlage der Zahlen der DCN- Studie, S.18. Wert berechnet sich aus den Angaben zu Sharehostern, BitTorrent und Verzeichnungsdienste (P2P) und Streaming- Portale für Filme, für welche eine illegal Nutzung unterstellt wird.

¹⁵⁶⁸ *High Administrative Court*, [2011] EWHC 1021 (Admin), par. 230.

¹⁵⁶⁹ *IFPI*, *Measuring the Impact of Graduate Response*, July 2011, S. 2.

Bereich hin. Gerade ein Ansatz, der sich auf P2P-Nutzung konzentriert, ist insofern ein geeigneter, als hier nach bisherigen Erkenntnissen, eine erhebliche Gruppe von Rechteverletzern erreicht werden kann.

c) Erforderlichkeit des vorgerichtlichen Mitwirkungsmodells

Das Übermaßverbot verpflichtet den Staat dazu, sich bei den Bürger belastenden Maßnahmen auf das Notwendige zu beschränken. Im Rahmen der Erforderlichkeitsprüfung ist nach Mitteln zu suchen, die den Betroffenen bei der Erreichung des Zieles des Staates bei gleicher Wirksamkeit weniger belasten.¹⁵⁷⁰ Folgende Handlungsvarianten können erwogen werden.

aa) Vorgehen ohne Mitwirkung der Zugangsanbieter

Ein Vorgehen ohne Mitwirkung der Zugangsanbieter würde diese nicht belasten, ist aber im Zusammenhang mit Warnhinweismodellen unmöglich, da die Zuordnung von durch die Rechteinhaber ermittelten Daten allein durch die Zugangsanbieter erfolgen kann.

bb) Vorgehen nur im Rahmen des Auskunftsanspruchs

Zu erwägen ist, ob das bisherige Vorgehen im Rahmen des Auskunftsanspruchs ein milderes und für die Erreichung des Zweckes ebenso effektives Mittel darstellt, wie der mit einem Warnhinweismodell kombinierte Auskunftsanspruch. Dazu wäre zunächst erforderlich, dass der Auskunftsanspruch als alleiniges Mittel gegenüber einem Auskunftsanspruch im Rahmen des vorgelagerten Mitwirkungsmodells, dem Warnhinweise voraus gehen müßte, um Rechtsverletzungen im Internet insbesondere auch durch Aufklärung und Schaffung von Rechtsbewusstsein zu bekämpfen.

(1) Probleme bei der Geltendmachung des Auskunftsanspruchs

In diesem Zusammenhang ist zunächst auf die beschriebenen **Probleme bei der Geltendmachung** des Anspruchs im Verfahren nach § 101 Abs. 9 UrhG und die nach wie vor offenen Rechtsfragen hinzuweisen,¹⁵⁷¹ die an der Effektivität des Auskunftsanspruchs zwar nicht generell zweifeln lassen, wohl aber an seiner Eignung zu einer verhältnismäßigen Aufklärung. Das liegt daran, dass der Auskunftsanspruch dann, wenn ihm stattgegeben wird, den Betroffenen mit einer drastischen rechtlichen Konsequenz konfrontiert. Er entfaltet seine aufklärende Wirkung erst im Zusammenhang mit einer gerichtlichen Inanspruchnahme und ist damit so gesehen nicht präventiv.

(2) Auskunftsanspruch als milderes Mittel

Fraglich ist aber, ob der isolierte Auskunftsanspruch im Vergleich zum vorgelagerten Mitwirkungsmodell ein milderes Mittel darstellt. Dies ist insbesondere vor dem Hintergrund

¹⁵⁷⁰ Dazu *Pieroth/Schlink*, Grundrechte Staatsrecht II, Rn. 285.

¹⁵⁷¹ Siehe oben S. 252.

des nicht auf Warnung sondern sogleich auf Abschreckung und Sanktion gerichteten Zwecks des Auskunftsanspruchs zu sehen.

Diese scharfe Sanktion im ersten Kontakt mag im Verhältnis zu Nutzern des Internet, die sich der Illegalität ihres Handelns bewusst sind, als angemessen betrachtet werden, auch wenn sie sich auch insofern dem Vorwurf aussetzen muss, es nicht zuerst „im Guten“ versucht zu haben. Unangemessen ist die rechtliche Konsequenz des unmittelbaren Auskunftsanspruchs aber gegenüber unaufgeklärten Nutzern, die das vorgerichtliche Mitwirkungsmodell in besonderem Maße im Auge hat.¹⁵⁷² Der Auskunftsanspruch in seiner heutigen Form führt dazu, dass ein Anschlussinhaber allein aufgrund dieser Eigenschaft in die Haftung genommen wird, wenn ein Dritter ohne sein Wissen den Anschluss mißbraucht. Würden dem Auskunftsanspruch Warnhinweise vorausgehen, so wäre dies nicht mehr möglich.

Es ist ferner zu berücksichtigen, dass eine erhebliche Anzahl von Anschlussinhabern über die technischen und rechtlichen Grundlagen der Internetbenutzung noch nicht hinreichend aufgeklärt ist. Diese Personen werden von direkter Rechtsverfolgung über den Auskunftsanspruch, teilweise in Form von massenhaft versandten kostenpflichtigen Abmahnungen, die auf Betreiben der Rechteinhaber auf die Auskunftserteilung folgen, unmittelbar und scharf getroffen. Das geht insbesondere die mittlere und die ältere Generation an, d.h. die Generation derjenigen, die selbst nicht mit dem Internet aufgewachsen sind, deren Kinder jedoch „digital Natives“ sind, sowie die noch älteren Personen. Die technischen Kenntnisse dieser Elterngeneration, die i.d.R. die Anschlussinhaber stellen und ihre minder- und volljährigen Verwandten den Anschluss mitbenutzen lassen, ist gegenüber den Kenntnissen der jüngeren Generation, d.h. etwa unter 25 -Jährigen, in erheblichem Maße unterentwickelt. Viele der gängigen Technologien für Urheberrechtsverletzungen¹⁵⁷³ sind ihnen überhaupt nicht bekannt. Personen dieser Altersgruppe haben ihr Mediennutzungsverhalten vor dem Aufkommen des Internet, jedenfalls vor der Verbreitung von Technologien zum massenhaften Download erworben und dieses Verhalten seither nicht oder kaum geändert. Viele begreifen das Internet in erster Linie als Informationsmedium und die aktuellen Erscheinungen und Möglichkeiten des Web 2.0 gehen in erheblichen Teilen an diesen Personen vorbei. Internet-Technologien als Mittel für die Begehung von Urheberrechtsverletzungen sind ihnen fremd.

Dieser Personenkreis wird über die auf das durchgeführte Auskunftsersuchen folgende Abmahnung vielfach erstmals konkret damit konfrontiert, dass Möglichkeiten zum illegalen Download zur Verfügung stehen. Der Wunsch zur Rechtstreue ist bei diesen Menschen aufgrund des erlernten Mediennutzungsverhaltens durchaus hinreichend ausgeprägt, und es erscheint daher äußerst fraglich ob es notwendig oder gar angemessen erscheint, diese Zielgruppe von erheblicher Größe nach einem ersten Rechtsverstoß in unmittelbarer Folge

¹⁵⁷² Siehe oben S. 43.

¹⁵⁷³ Siehe oben S. 34 ff.

eines Auskunftersuchens nach § 101 Abs. 9 UrhG mit einer kostenpflichtigen Abmahnung zu belegen.

Im Ergebnis mag das isolierte Vorgehen im Rahmen des Auskunftsanspruchs im Verhältnis zum Zugangsanbieter zwar milder sein; es ist aber nicht ebenso effektiv wie das hier vorgeschlagene Modell und im Verhältnis zu den Nutzern sogar schärfer.

cc) Sanktionslose Versendung von Warnhinweisen

Als Alternative zum vorgerichtlichen Mitwirkungsmodell ist auch ein Modell denkbar, das ohne Einbindung des Auskunftsanspruchs auskommt. Hier könnten Warnhinweise versendet werden, ohne dass dem Rechteinhaber über die Mitteilung einer Verstoßliste¹⁵⁷⁴ potentielle relevante Nutzer, die nachhaltig illegal handeln zur Kenntnis gebracht würden. Dieser Ansatz wäre sowohl im Verhältnis zum Provider als auch im Verhältnis zum Nutzer weniger eingreifend, verspräche aber weit weniger Effektivität. Dies zeigte sich etwa in Schweden im Hinblick auf den zunächst dem EuGH vorgelegten und insofern außer Kraft gesetzten Auskunftsanspruch.¹⁵⁷⁵ Auch in Finnland stand das nicht weiter verfolgte Warnhinweismodell wegen seiner Sanktionslosigkeit in der Kritik.¹⁵⁷⁶

dd) Anlasslose Warnhinweise

In Betracht zu ziehen wäre auch das anlasslose Versenden von standardisierten Informationen durch die Zugangsprovider an ihre Kunden, in denen auf das Verbot von Urheberrechtsverstößen ohne konkreten Anlass hingewiesen würde.¹⁵⁷⁷ Ein solcher anlassloser Hinweis wäre für den Nutzer mit so gut wie keinem Eingriff verbunden. Aus Sicht der Provider wäre auch die Inpflichtnahme zur Versendung an Art. 12 GG zu messen und sicher milder als die Beteiligungspflicht im Rahmen des vorgerichtlichen Mitwirkungsmodells. Ob ein anlassloser Warnhinweis, der wahllos an jeden Kunden gerichtet würde, angesichts der Vielzahl der täglich eingehenden Emails überhaupt die Wahrnehmungsebene des Nutzers erreichen würde, ist fraglich, so dass bereits die Eignung dieses Mittels in Frage gestellt werden kann, um einen nennenswerten Auflärungs- oder gar Warnungserfolg herbeizuführen. In jedem Fall wäre ein anlassloser Warnhinweis hinsichtlich seiner Effektivität nicht mit einem gezielten Hinweis nach dem hier vorgeschlagenen Ansatz vergleichbar.

ee) Netzsperrern

Die Bundesregierung hat sich gegen Netzsperrern ausgesprochen, die nicht Gegenstand der vorliegenden Studie sind. Gleichwohl soll im Rahmen der Erforderlichkeit der Vollstän-

¹⁵⁷⁴ Siehe oben S. 316.

¹⁵⁷⁵ Siehe oben S. 180.

¹⁵⁷⁶ Siehe oben S. 169.

¹⁵⁷⁷ Vgl. zu dieser Möglichkeit Art. 21 Abs. 4 RiLi 2009/136/EG. Dazu auch Stellungnahme des Europäischen Datenschutzbeauftragten zu den laufenden Verhandlungen der Europäischen Union über ein Abkommen zur Bekämpfung von Produkt- und Markenpiraterie (Anti-Counterfeiting Trade Agreement, ACTA), (2010/C 147/01), Rz. 37, v. 5.6.2010, abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:147:0001:0013:DE:PDF>.

digkeit halber gefragt werden, ob Netzsperrern keine schonendere Handlungsalternative im Vergleich zum vorgerichtlichen Mitwirkungsmodell darstellen. Insoweit ist zwischen Sperrern von **Inhalten** und Sperrern von **Zugängen** zu unterscheiden.¹⁵⁷⁸

Das Sperrern von Internetinhalten beschränkt den Zugriff auf ausgewählte Webseiten und unterbindet die Übermittlung von Daten.¹⁵⁷⁹ Sperrern können auf verschiedenen Ebenen ansetzen. Über die sog. „**IP-Schicht**“ können IP-Adressen mit der Folge gesperrt werden, dass der Nutzer sämtliche unter der IP-Adresse abrufbare Webseiten nicht mehr laden kann. Augenfällig ist hier das Problem des sog. „Overblocking“, das dazu führt, dass auf Seiten mit legalen und illegalen Inhalten auch legale Inhalte unzugänglich gemacht würden.¹⁵⁸⁰ Eine andere technische Möglichkeit setzt dabei an, den Transport von Inhalten durch das **Trennen des Transmission Transport Protocols** zu unterbinden, so dass etwa der Port für das http-Protokoll, nicht aber der für den Empfang von Emails gesperrt ist. Diese Sperrern setzen einen erhöhten Zugriff auf Daten voraus.¹⁵⁸¹ Eine weitere Möglichkeit setzt bei der Kanalisierung und damit Überwachung des Datenverkehrs durch sog. **Proxys**¹⁵⁸² oder im Wege der sog. **Deep Packet Inspection** auf der Anwendungsschicht an. Sie sind zum einen nicht vom Willen der Bundesregierung erfasst und zum anderen nach der jüngsten Rechtsprechung des Europäischen Gerichtshofes in der Rechtssache *Scarlet Extended*¹⁵⁸³ unzulässig. Schließlich besteht die Möglichkeit Internetinhalte über das **Domain Name System** (DNS) zu **sperrern**. Hier wird einer Domain (www.inhalt.de) eine IP-Adresse zugeordnet. Bei Eingabe der Domain ist der Aufruf der gesperrten Seite nicht möglich oder es wird ein Hinweis gegeben.¹⁵⁸⁴ Das Problem bei diesen Sperrern liegt darin, dass hier zum einen eine Festlegung auf verbotene Inhalte erfolgen müsste und unklar ist, wer über die Aufnahme von Inhalten in eine Liste zu sperrender Seiten entscheiden soll und welche Inhalte aufgenommen werden sollen. Die sog. „Labelisierung“ hat sich jedenfalls in Frankreich als nicht sehr effektiv erwiesen.¹⁵⁸⁵ Auch hier besteht das Problem des sog. „Overblocking“.¹⁵⁸⁶

Die genannten Sperrmaßnahmen wären zwar möglicherweise ein effektiveres Mittel zur Aufklärung über und die Bekämpfung von Rechtsverletzungen im Internet. Wegen der mit

¹⁵⁷⁸ Dazu Hennemann, S. 231 ff.

¹⁵⁷⁹ Dazu Hennemann, S. 238 ff.

¹⁵⁸⁰ Dazu Hennemann, S. 239.

¹⁵⁸¹ Dazu Hennemann, S. 240.

¹⁵⁸² Dazu Hennemann, S. 241.

¹⁵⁸³ Dazu Schwartmann, Provider müssen nicht auf ihre Kosten filtern und sperren, LTO, abrufbar unter: <http://www.lto.de/de/html/nachrichten/4892/eugh-zum-urheberrechtsschutz-provider-muessen-nicht-auf-ihre-kosten-filtern-und-sperren/>.

¹⁵⁸⁴ Unter <http://www.kino.to/> erscheint etwa bei Abruf am 5. November 2011 folgender Warnhinweis: „Die Kriminalpolizei weist auf Folgendes hin: Die Domain zur von Ihnen ausgewählten Webseite wurde wegen des Verdachts der Bildung einer kriminellen Vereinigung zur gewerbsmäßigen Begehung von Urheberrechtsverletzungen geschlossen. Mehrere Betreiber von KINO.TO wurden festgenommen. Internetnutzer, die widerrechtlich Raubkopien von Filmwerken hergestellt oder vertrieben haben, müssen mit einer strafrechtlichen Verfolgung rechnen.“

¹⁵⁸⁵ Siehe oben S. 220.

¹⁵⁸⁶ Dazu Hennemann, S. 243 f.

ihnen verbundenen Probleme in Hinblick auf die inhaltliche Zensur von Inhalten und die mit ihnen verbundenen datenschutzrechtliche Eingriffsintensität wären sie aber keineswegs grundrechtsschonender und damit im Verhältnis zum vorgerichtlichen Mitwirkungsmodell **kein milderes Mittel** zur Erreichung des Zwecks.¹⁵⁸⁷

d) *Angemessenheit des vorgerichtlichen Mitwirkungsmodells*

Nach Rechtsprechung und herrschender Lehre ist das abschließende Kriterium des Verhältnismäßigkeitsgrundsatzes die Frage der Angemessenheit oder auch der Verhältnismäßigkeit im engeren Sinne. Bisweilen werden auch die Begriffe der Proportionalität oder Zumutbarkeit verwendet.¹⁵⁸⁸ Kriterien im Rahmen der Zumutbarkeit sind die Nähe zur Rechtsverletzung und die vertraglichen Befugnisse im Verhältnis zum Anschlussinhaber als Kunde im Falle des Rechtsmissbrauchs.

aa) *Nähe zur Rechtsverletzung*

Stellt man die Frage nach der Zumutbarkeit eines vorgerichtlichen Beteiligungsmodells für Zugangsanbieter, so ist zunächst deren **Nähe zur Rechtsverletzung** zu beachten, die zwar nicht mit deren Zutun geschieht, die aber ohne sie nicht denkbar wäre. Zu berücksichtigen ist dabei auch, dass Zugangsanbieter an dem für illegale Downloadvorgänge erforderlichen Datendurchsatz insofern verdienen, als hierfür große Bandbreiten genutzt werden müssen, die über die Tarife abgegolten werden. Diese Nähe zur Rechtsverletzung drückt sich bereits heute im Vorhandensein des Auskunftsanspruchs sowie in der Rechtsprechung zur Providerhaftung aus, die jedoch die Verletzung einer Rechtspflicht durch die Zugangsanbieter voraussetzt.¹⁵⁸⁹ In der jüngsten Rechtsprechung des Bundesgerichtshofes wird diese Pflicht jedenfalls in Bezug auf Hostprovider intensiviert. Sowohl der I.¹⁵⁹⁰ als auch der VI. Senat¹⁵⁹¹ nehmen im Rahmen der Störerhaftung eine Pflicht des Hostproviders an, mit einem für Inhalte verantwortlichen Nutzer in Kontakt zu treten. Ihn trifft also unabhängig von einem Auskunftsverlangen nach § 101 UrhG die Pflicht, kommunikativ-vermittelnd zwischen Rechteinhabern und Kunden tätig zu werden und unter Umständen sogar auf diese einzuwirken, um künftigen Rechtsverletzungen zu begegnen.

bb) *Vertragliche Befugnisse des Zugangsanbieters bei Rechtsmissbrauch*

Ein wesentlicher Punkt, auf den die Zugangsanbieter hinweisen, ist deren Vertrauensverhältnis zu den Kunden. In der Tat wäre es unzumutbar, wenn die Zugangsanbieter zu „par-

¹⁵⁸⁷ Vgl. kritisch zu Sperren und zu einer Aufforderung mildere Maßnahmen zu prüfen die Stellungnahme des Europäischen Datenschutzbeauftragten im Vorfeld des im Rahmen von ACTA diskutierten Three-Strikes-Modell Zif. 30 ff.

¹⁵⁸⁸ Dazu *Pieroth/Schlink*, Grundrechte Staatsrecht II, Rn. 289.

¹⁵⁸⁹ Dazu eingehend *Schwartmann*, K&R 2011, Beihefter zu Heft 11; *Gennen*, in Schwartmann, Praxishandbuch Medienrecht, 20. Kap. Rn. 151 ff.

¹⁵⁹⁰ *BGH v. 17.8.2011 – I ZR 57/09 (Stiftparfüm)*.

¹⁵⁹¹ *BGH v. 25.10.2011 – VI ZR 93/10*.

teischen Überwachungsprovider wandeln“ würden.¹⁵⁹² Allerdings sieht das hier vorgeschlagene Modell in Übereinstimmung mit der Rechtsprechung des EuGH in der Sache *Scarlet Extended* gerade keine Überwachung durch den Provider vor, sondern das Versenden einen aufklärenden und warnenden Hinweises und das Führen einer Liste. Diese Obliegenheit kann aus technischen und datenschutzrechtlichen Gründen allein die Zugangsanbieter treffen, deren Geschäftsmodell bei aller Neutralität nicht in einem Wegsehen und faktischen Profitieren an Urheberrechtsverletzungen in Verbindung gebracht werden darf. Hinzu kommt, dass die Versendung von Hinweisen an die Kunden und auch Drosselungen von Bandbreiten etwa bei Überschreiten des vertraglich eingeräumten Datenvolumens an der Tagesordnung sind. Selbst Sperrungen und einseitige Kündigung von Anschlüssen sind im Falle unter anderem von Urheberrechtsverletzungen vorgesehen, ohne dass darin ein „tiefgreifende(r) Bruch in der Vertrauensbeziehung zum Verbraucher“¹⁵⁹³ gesehen wird. Die rechtlichen Möglichkeiten erlauben den Zugangsanbietern zur Kontrolle von Rechtsmissbrauch bereits jetzt mehr, als das hier vorgeschlagene Modell vorsieht. Bei der Abwägung der Frage, was einem Zugangsanbieter im Rahmen einer Inpflichtnahme gerade im Verhältnis zu den Anschlussinhabern als seinen Kunden zumutbar ist, sollen deshalb die vertraglich vereinbarten Maßnahmen als Referenz dienen. Nach den im Privatkundengeschäft geltenden AGB¹⁵⁹⁴ der großen in Deutschland tätigen Internet-Service-Provider sind die Kunden diesem gegenüber vertraglich dazu verpflichtet, bei Inanspruchnahme der Leistung bestehende Gesetze, insbesondere Urheberrechte bzw. Rechte Dritter einzuhalten.¹⁵⁹⁵ Die Vertragsbedingungen sehen vor, dass der Provider im Falle einer Pflichtverlet-

¹⁵⁹² *Süme*, <http://www.lto.de/de/html/nachrichten/5062/pro-und-contra-warnhinweismodell-ein-streit-ueber-den-umgang-mit-fileshareern/>.

¹⁵⁹³ *Süme*, <http://www.lto.de/de/html/nachrichten/5062/pro-und-contra-warnhinweismodell-ein-streit-ueber-den-umgang-mit-fileshareern/>.

¹⁵⁹⁴ Alle nachstehend angeführten AGB (Auswahl!) sind am 2.12.2011 im Internet abgerufen worden.

¹⁵⁹⁵ Siehe Allgemeine Geschäftsbedingungen – Internet Zugangstarife / Call & Surf der **Telekom Deutschland GmbH** Ziff. 4.1 b): „Die überlassenen Leistungen dürfen nicht missbräuchlich genutzt werden, insbesondere [...] sind die nationalen und internationalen Urheber- und Marken-, Patent-, Namens- und Kennzeichenrechte sowie sonstigen gewerblichen Schutzrechte und Persönlichkeitsrechte Dritter zu beachten“; Allgemeine Geschäftsbedingungen der **1 & 1 Telecom GmbH** Ziff. A. 6.1.: „Der Kunde ist verpflichtet, die Dienstleistungen der 1&1 in Übereinstimmung mit den geltenden Gesetzen und unter Berücksichtigung Rechte Dritter zu nutzen“; Allgemeine Geschäftsbedingungen für **Vodafone D2-Dienstleistungen** (AGB) Ziff. 6.5.: „Der Kunde verpflichtet sich, den Zugang zu den Diensten sowie die Dienste selbst nicht missbräuchlich zu nutzen, insbesondere [...] keine Rechte Dritter, insbesondere Schutzrechte (z. B. Urheber- und Markenrechte) zu verletzen“; Allgemeine Geschäftsbedingungen Geschäftskunden der **QSC AG** Ziff. I 11.5: „Der Kunde ist verpflichtet, die Dienstleistungen sachgerecht und im Rahmen der geltenden Gesetze zu nutzen. Der Kunde ist insbesondere dazu verpflichtet, den von QSC bereitgestellten Zugang zur Dienstleistung sowie die genutzten Dienstleistungen selbst nicht missbräuchlich zu nutzen, insbesondere keine rechtswidrigen Handlungen im Rahmen der Nutzung gegenüber Dritten zu begehen und insbesondere Schutzrechte Dritter nicht zu verletzen“; Allgemeine Geschäftsbedingungen Alice Comfort und Allgemeine Geschäftsbedingungen für Alice Privatkundenprodukte von **Telefónica Germany** Ziff. 4.1.2: „Der Kunde darf die zur Verfügung gestellten Leistungen nicht missbräuchlich, sondern nur bestimmungsgemäß und nach Maßgabe der geltenden Gesetze und Verordnungen nutzen. Er hat insbesondere jede Maßnahme zu unterlassen, die zu einer Bedrohung, Belästigung, Schädigung oder anderweitigen Verletzung der Rechte Dritter (einschl. Urheberrechte) führt oder eine solche unterstützt.“; Allgemeine Geschäftsbedingungen der **Telefónica Germany GmbH & Co. OHG für O2 DSL** Ziff. 5.3 a): „Der Kunde darf die Leistungen von Telefónica Germany nicht missbräuchlich nutzen, insbesondere keine sitten- oder gesetzeswidrigen Inhalte verbreiten, nicht gegen strafrechtliche Vorschriften oder Vorschriften zum Schutz der Jugend verstoßen und keine Rechte Dritter

zung berechtigt ist, den Zugang zum Internet zu **sperr**en und / oder den Vertrag fristlos zu **kündigen**. Die Voraussetzungen für ein solches Recht variieren dabei im Einzelnen.¹⁵⁹⁶ Ist für die Internetnutzung eine Flatrate vereinbart, dann steht nach den Vertragsbedingungen dem Provider – aus wirtschaftlichen Gründen – vielfach das Recht zu, die Geschwindigkeit der Datenübertragung für den Rest des Abrechnungszeitraums zu **drosseln**, falls der Kunde das ihm nach dem Tarif für diesen Zeitraum zustehende Datenvolumen überschritten hat.¹⁵⁹⁷ Ein Sonderkündigungsrecht des Kunden oder eine Reduzierung des zu

verletzen.“; Besondere Geschäftsbedingungen Internet und Telefonie der **Unitymedia NRW GmbH** Ziff. A. 3.1: „Der Kunde darf die Internetdienste nur in dem vereinbarten Umfang und im Rahmen der jeweils geltenden gesetzlichen Bestimmungen nutzen.“

¹⁵⁹⁶ Allgemeine Geschäftsbedingungen – Internet Zugangstarife / Call & Surf der **Telekom Deutschland GmbH** Ziff.4.2: „Die Telekom ist berechtigt, bei schwerwiegenden Verstößen gegen die dem Kunden obliegenden Pflichten sowie bei begründeten erheblichen Verdachtsmomenten für eine Pflichtverletzung nach Ziffer 4.1, Buchstabe b und c, die jeweilige Leistung auf Kosten des Kunden zu sperren. Der Kunde bleibt in diesem Fall verpflichtet, die monatlichen Preise zu zahlen“ und Ziff. 11.4: „Das Recht, aus wichtigem Grund fristlos zu kündigen, bleibt unberührt. Ein wichtiger Grund ist für die Telekom insbesondere in den Fällen gegeben, in denen der Kunde die ihm nach diesen Allgemeinen Geschäftsbedingungen obliegenden Pflichten erheblich verletzt.“; Allgemeine Geschäftsbedingungen der **1 & 1 Telecom GmbH** Ziff. A. 5.6: „Unberührt bleibt das Recht beider Parteien zur fristlosen Kündigung aus wichtigem Grund. Ein wichtiger Grund liegt für 1&1 insbesondere dann vor, wenn der Kunde schuldhaft gegen eine der in den Ziffern A. 4. und 6. geregelten Pflichten verstößt“ (aber keine Berechtigung zur Aussetzung oder Sperrung des *generellen* Internetzugangs, sondern nur Recht zur Abschaltung des Zugriffs auf einzelne Websites; vgl. Ziff. B 1.4: „1&1 ist berechtigt, den Zugriff auf Webseiten des Kunden oder Dritter, Internet-Newsgroups oder IRCkanäle abzuschalten, sofern deren Inhalte gegen geltendes Recht, gesetzliche oder behördliche Verbote oder die guten Sitten verstoßen. Ansprüche des Kunden entstehen in solchen Fällen nicht.“); Allgemeine Geschäftsbedingungen für **Vodafone D2-Dienstleistungen** (AGB) Ziff. 6.6: „Bei schuldhafter Pflichtverletzung haftet der Kunde gegenüber Vodafone auf Schadensersatz, und Vodafone ist zur außerordentlichen Kündigung des Vertrages berechtigt.“ (aber keine konkrete Berechtigung zur Anschlussperre, sondern nur generelles Eingriffsbefugnis nach Ziff. 6.6: „Verstößt der Kunde gegen die Pflichten gemäß Ziff. 6.5 ist Vodafone berechtigt, alle erforderlichen Maßnahmen zur Beseitigung des Missbrauchs zu ergreifen“); Allgemeine Geschäftsbedingungen Geschäftskunden der **QSC AG** Ziff. I 6.3: „[...] kann QSC die Dienstleistung jederzeit aussetzen und/oder die Übermittlung der vom Kunden bzw. Nutzer bereitgestellten Inhalte einstellen, wenn [...] die Nutzung offensichtlich rechtswidrig oder missbräuchlich ist“ (aber ohne spezielles Kündigungsrecht; vgl. Ziff. I 12.2: „Das Recht zur außerordentlichen Kündigung bleibt unberührt.“); Allgemeine Geschäftsbedingungen Alice Comfort und Allgemeine Geschäftsbedingungen für Alice Privatkundenprodukte von **Telefónica Germany GmbH & Co. OHG** Ziff. 7.3.3: „Der Anbieter ist weiter berechtigt, die von dem Kunden in Anspruch genommenen Internet-Dienstleistungen zu sperren, wenn der Kunde gegen die sich aus Ziffer 4.1.2 oder 4.4.2 ergebenden Pflichten verstößt.“ und Ziff. 14.1: „Das Vertragsverhältnis kann von jedem Vertragspartner aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist nach den gesetzlichen Bestimmungen gekündigt werden.“ i. V. m. Ziff. 14.2: „Ein wichtiger Grund liegt für den Anbieter insbesondere vor bei [...] einer missbräuchlichen Nutzung des Internetzuganges im Sinne der Ziffern 4.1.2 [...]“; Allgemeine Geschäftsbedingungen der **Telefónica Germany GmbH & Co. OHG für O2 DSL** Ziff. 9.4: „Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt für Telefónica Germany insbesondere vor, wenn der Kunde [...] b) bei der Nutzung gegen Strafvorschriften verstößt. c) gegen die Pflichten aus Ziffern 5.2 c, 5.3 a, 5.3 b, 5.3 c und 5.3 d verstößt.“ (aber Recht zur Sperre des Anschlusses nur „unbeschadet anderer gesetzlicher Vorschriften nach näherer Maßgabe des Telekommunikationsgesetzes (TKG); Ziff. 11.1); Besondere Geschäftsbedingungen Internet und Telefonie der **Unitymedia NRW GmbH** Ziff. A. 3.7: „Bei missbräuchlicher Nutzung des Internetdienstes gemäß den vorstehenden Regelungen und/oder bei Verstößen gegen geltendes Recht ist der Kabelnetzbetreiber zur Sperrung bzw. Löschung der Inhalte oder fristlosen Kündigung des Vertragsverhältnisses berechtigt. Das gleiche Recht steht dem Kabelnetzbetreiber auch in begründeten Verdachtsfällen sowie bei einer Gefährdung des Netzes des Kabelnetzbetreibers oder des Internets zu.“ und Ziff. C 3.2: „Der Kabelnetzbetreiber behält sich das Recht vor, den Internet- bzw. den Telefonanschluss des Kunden ohne Ankündigung und ohne Einhaltung einer Wartefrist zu sperren, wenn 1. der Kunde Veranlassung zu einer fristlosen Kündigung des Vertragsverhältnisses gegeben hat.“

¹⁵⁹⁷ Ob und inwieweit der Provider zur Drosselung der Übertragungsgeschwindigkeit befugt ist, ist abhängig von der vereinbarten Leistung bzw. dem vereinbarten Tarif. Vgl. etwa Leistungsbeschreibung Call & Surf mit Standard- und Universal-Anschluss der **Deutsche Telekom GmbH** Ziff. 1.2.1.1 sowie Leistungsbeschreibung

leistenden Entgelts ist für den Fall einer solchen Sperre des Anschlusses oder Drosselung der Übertragungsgeschwindigkeit offenbar nicht vorgesehen.¹⁵⁹⁸

Vor dem Hintergrund dieser Geschäftsbedingungen erschiene es sogar **zumutbar**, weil im Verhältnis zum Kunden nicht überraschend und vereinbart wäre, dem Zugangsanbieter aufzuerlegen, bei Urheberrechtsverstößen im Internet Sperren anzuordnen, zu der er nach dem Vertrag gegenüber seinem Kunden auch bisher schon *berechtigt* ist, die der EuGH in Scarlet Extended – anders als Überwachung und Filterung – nicht für unzulässig erklärt und damit in das Ermessen der Mitgliedstaaten gestellt hat.¹⁵⁹⁹ Auf der anderen Seite ist dem Kunden ohne weiteres die Ausübung der vertraglichen Rechte durch den Provider zuzumuten, wenn deren Voraussetzungen vorliegen; denn der Nutzer hat den Vertrag in Kenntnis der Sanktionen abgeschlossen und sich dadurch mit dessen Bedingungen einverstanden erklärt.

Nach dem hier vorgeschlagenen Ansatz stehen derartige vertraglich vorgesehene und im Vergleich zum vorgerichtlichen Mitwirkungsmodell schärfere Maßnahmen wie Sperrung, Kündigung oder Drosselung durch den Zugangsanbieter in Folge von Urheberrechtsverletzungen nicht in Rede. Aus einem Schluss von größeren auf das kleinere ist die Inpflichtnahme von Zugangsanbietern zur Mitwirkung im Rahmen eines vorgerichtlichen Mitwirkungsmodells zumutbar. Dies gilt umso mehr, als dieses – etwa nach dem gescheiterten finnischen Ansatz¹⁶⁰⁰ ohne Prüfungspflicht des Providers oder nach dem bevorstehenden britischen Ansatz mit Prüfungspflicht des Providers - vom Gesetzgeber unterschiedlich ausgestaltet werden könnte.

Call & Surf IP der Deutsche Telekom GmbH; Leistungsbeschreibung Call & Surf Comfort via Funk/Standard und Call & Surf Comfort via Funk/Universal der Deutsche Telekom GmbH Ziff. 1.2.1.1 („Ab einem übertragenen Datenvolumen von 10 GB pro Monat wird die Übertragungsgeschwindigkeit für den Rest des jeweiligen Monats auf max. 384 Kbit/s im Download und 64 kbit/s im Upload begrenzt. Darüber hinaus ist ein Peer-to-Peer-Verkehr in diesem Zeitraum nicht mehr möglich. Die Berechnung des Datenvolumens erfolgt im 100-KB-Daten-block. Am Ende jeder Verbindung, mindestens jedoch einmal täglich, wird auf den begonnenen Datenblock aufgerundet. Die Telekom behält sich vor, nach 24.00 Uhr jeweils eine automatische Trennung der Verbindung durchzuführen.“); Leistungsbeschreibung **1&1** DSL und Telefonie Ziff. 2.6; Leistungsbeschreibung 1&1 LTE Ziff. 3; Leistungsbeschreibung 1&1 Doppel-Flat 6.000 HSDPA Ziff. 3.1; Preisliste **Vodafone** DSL & Festnetz Pakete inkl. Surf-Sofort und LTE Zuhause 3.1.2.2 (Mobiles Surfen mit UMTS) und insbesondere FAQ 7.2.6; Leistungsbeschreibung QSC-Internet-Produkte Leistungsbeschreibung der Alice Comfort und Alice Comfort Office Produkte der **Telefónica Germany GmbH & Co. OHG** Ziff. 3.8; Leistungsbeschreibung der Produkte Alice Fun Max, Alice Light Max, Alice Fun Speed und Alice Light Speed der **Telefónica Germany GmbH & Co. OHG** Ziff. 3.2; Leistungsbeschreibung der **Telefónica Germany GmbH & Co. OHG für O2** Ziff. 7. und 8.

¹⁵⁹⁸ Zum Teil ist dies ausdrücklich in den Geschäftsbedingungen so geregelt: Vgl. für den Fall der Sperre Allgemeine Geschäftsbedingungen – Internet Zugangstarife / Call & Surf der Telekom Deutschland GmbH Ziff. 4.2; Allgemeine Geschäftsbedingungen der Telefónica Germany GmbH & Co. OHG für O2 DSL Ziff. 11.2.

¹⁵⁹⁹ Dazu *Schwartzmann*, Provider müssen nicht auf ihre Kosten filtern und sperren, Legal Tribune Online v. 24.11.2011, abrufbar unter: <http://www.lto.de/de/html/nachrichten/4892/eugh-zum-urheberrechtsschutz-provider-muessen-nicht-auf-ihre-kosten-filtern-und-sperren/>.

¹⁶⁰⁰

cc. Zwischenergebnis

Nach alledem wäre der Eingriff in das Grundrecht der Berufsfreiheit der Zugangsanbieter mit der im Rahmen des vorgerichtlichen Mitwirkungssystem vorgeschlagenen Inpflichtnahme vor dem Hintergrund von Art. 12 GG verfassungsrechtlich nicht zu beanstanden.

E. Ergebnis

Das vorgeschlagene Modell der vorgerichtlichen Mitwirkung der Zugangsanbieter, das ein aufklärendes Warnhinweismodell mit einer Effektivierung des Auskunftsanspruchs verbindet, der weiterhin eine richterliche Anordnung voraussetzt, erscheint vor dem Hintergrund des internationalen Rechtsrahmens zulässig. Insbesondere die Rechtsprechung des Europäischen Gerichtshofs legt ein Prävention und Repression verbindendes Modell zum Urheberrechtsschutz nahe.¹⁶⁰¹ Verfassungsrechtlich ist eine aus technischen Gründen unabdingbare Inpflichtnahme der Zugangsanbieter vor dem Hintergrund der Berufsfreiheit nicht zu beanstanden und stellt mit einer Kombination aus Aufklärung und Warnhinweis ein verhältnismäßiges Mittel beim Vorgehen gegen Urheberrechtsverletzungen im Internet dar. Im Hinblick auf den Datenschutz käme es auf die konkrete Ausgestaltung der Maßnahme an, die dem Gesetzgeber obläge. Insbesondere sind hier die Anforderungen an eine verfassungskonforme Vorratsdatenspeicherung zu beachten, die hier aufgezeigt wurden.

¹⁶⁰¹ *EuGH C 70/10* v. 24.10.2011, Rn. 31. „Sodann ergibt sich aus der Rechtsprechung des Gerichtshofs, dass die den nationalen Gerichten nach diesen Bestimmungen zugewiesene Zuständigkeit ihnen ermöglichen muss, den Vermittlern Maßnahmen aufzugeben, die nicht nur mittels ihrer Dienste der Informationsgesellschaft bereits begangene Verletzungen an Rechten des geistigen Eigentums beenden, sondern auch **neuen Verletzungen vorbeugen sollen** (vgl. in diesem Sinne Urteil vom 12. Juli 2011, *L'Oréal u. a.*, C-324/09, Slg. 2011, I-0000, Randnr. 131).“ <http://curia.europa.eu/juris/document/document.jsf?jsessionid=9ea7d2dc30dd8b9efd6ee12940c9bc6ef3cb2bf8ae67.e34KaxiLc3qMb40Rch0SaxqTbxb0?text=&docid=115202&pageIndex=0&doclang=de&mode=doc&dir=&occ=first&part=1&cid=212480>

3. Teil Kurzfassung

Vor dem Hintergrund des „erheblichen Ausmaßes an Urheberrechtsverletzungen im Internet und dem dadurch entstehenden volkswirtschaftlichen Schaden“ hat das Bundesministerium für Wirtschaft und Technologie (BMWi) eine wissenschaftliche Studie vergeben. Konkret geht es in der vergleichenden Studie um Modelle zur Versendung von Warnhinweisen durch Internet-Zugangsanbieter an Nutzer bei Urheberrechtsverletzungen in anderen EU-Staaten.¹⁶⁰² Unabhängig von der Projektbeschreibung schlägt die Studie einen schlagwortartig als vorgerichtliches Mitwirkungsmodell bezeichneten Ansatz vor. Dies geschieht, um die internationalen, die verfassungs- und einfachgesetzlichen Rahmenbedingungen nicht abstrakt, sondern anhand eines konkreten Vorschlags prüfen zu können. Zugleich kann dieser als Ansatz für eine weiterführende Diskussion dienen.

A. 1. Teil: Rechtsvergleichende Untersuchung zu Warnhinweismodellen bei Urheberrechtsverletzungen im Internet

I. Ausgangssituation

1. Erscheinungsformen von Rechtsverletzungen im Internet

Urheberrechtsverletzungen im Internet erfolgen überwiegend über das Usenet, Sharehosting- und Streamhostingdienste, mittels Aufnahmesoftware sowie insbesondere beim P2P-Filesharing¹⁶⁰³. Die Ursachen für solche Rechtsverletzungen liegen im technologischen Fortschritt und im mangelnden Rechts- bzw. Unrechtsbewusstsein der Nutzer begründet. Letztgenannte Ursache umfasst sowohl Verletzungshandlungen in Unkenntnis der Rechtslage oder der tatsächlichen Umstände als auch die bewusste Normüberschreitung bei fehlender Akzeptanz oder Respektierung des Urheberrechts¹⁶⁰⁴.

¹⁶⁰² Siehe oben, S. 19.

¹⁶⁰³ Siehe oben, S. 34.

¹⁶⁰⁴ Siehe oben, S. 40.

2. Betroffene Branchen

Das Problem betrifft verschiedene Branchen der Kultur- und Kreativwirtschaft, die ihre Produkte zunehmend in digitaler Form vertreiben. Hierzu zählen die Musik-, die Film- und Fernsehbranche, der Bereich Software, Games (Computer- und Videospielsoftware), Bücher sowie Zeitungen und Zeitschriften.¹⁶⁰⁵

3. Umsatzrückgänge

Durch Piraterie verursachte Umsatzrückgänge der betroffenen Branchen lassen sich bei einer Betrachtung eines gesamten Industriezweiges kaum feststellen. Für einzelne Bereiche sind andauernde Umsatzrückgänge zu verzeichnen und Piraterie als Mitursache hierfür sehr wahrscheinlich. Nachweise sind insoweit nur bedingt erbracht. Die Urheberrechtsverletzungen wirken sich volkswirtschaftlich insgesamt kaum aus. In einzelnen Branchen der Kreativwirtschaft deuten sich Auswirkungen an, die sich aber nicht konkret beziffern lassen.¹⁶⁰⁶

4. Zusammenhang zwischen Umsatz und illegaler Nutzung

Ein direkter Zusammenhang zwischen der Nutzung illegaler Kopien und dem Rückgang der Umsatzzahlen liegt nahe, ist aber nur sehr schwer nachzuweisen. Belastbare Anhaltspunkte liefert eine Studie von 2010 für Schweden. Es wurde der Internetverkehr vor und nach Einführung einer Gesetzesänderung zur besseren Verfolgung von Urheberrechtsverletzungen im Internet über einen Zeitraum von 9 Monaten gemessen. Nach Inkrafttreten der Gesetzesreform wurde ein Rückgang des Internetverkehrs um 18 Prozent für die folgenden sechs Monate gemessen. In den Vergleichsländern Norwegen und Finnland war im gleichen Zeitraum kein derartiger Rückgang festzustellen. Daraus wird gefolgert, dass es sich bei den eingestellten Internetaktivitäten um illegales Nutzungsverhalten handelte, welches in Ansehung drohender Rechtsverfolgung aufgegeben wurde. Im selben Zeitraum stieg die Anzahl der physischen Musikverkäufe um 27 Prozent und der digitalen Musikverkäufe um 48 Prozent. Wäre dieser Effekt konstant, so wären physische Musikverkäufe in Schweden um 72 Prozent höher und im Bereich digitaler Musikverkäufe sogar 131 Prozent höher. Die festgestellten Effekte des Rückgangs des Piraterieverhaltens endeten nach sechs Monaten. Als Ursache wird vermutet, dass es nicht zu einer tatsächlichen Rechtsverfolgung aufgrund der neuen Gesetzeslage kam. Die Nachfrage nach legaler Musik sank ab diesem Zeitpunkt, vor allem bei physischen Musikverkäufen. Bei digitalen Musikverkäufen blieb die Umsatzsteige-

¹⁶⁰⁵ Siehe oben, S. 51.

¹⁶⁰⁶ Siehe oben, S. 60.

rung konstant, was den Schluss zulässt, dass die Migration zur Legalität in diesem Bereich langfristig war und die Nutzer Geschäftsmodelle der legalen, digitalen Musiknutzung als echtes Substitut für die illegale Nutzung entdeckten.¹⁶⁰⁷

5. Auswirkungen

Methodische Schwierigkeiten bei der Ermittlung von Beeinträchtigungen bestehen darin, dass Berechnungen auf einem hypothetischen Alternativverhalten der Nutzer beruhen und dass Effekte von Piraterie schwer zu bestimmen, geschweige denn zahlenmäßig anzugeben sind.¹⁶⁰⁸ Trotz dieser Schwierigkeiten wurden konkrete Zahlen zu den Auswirkungen von Piraterie von staatlicher Seite im Vereinigten Königreich vorgelegt¹⁶⁰⁹ und auch im Hinblick auf das wirtschaftliche Wachstum in der Europäischen Union festgestellt. Zugleich wird Onlinepiraterie als Hemmnis für Anreize zu Investitionen der Industrie zur Schaffung neuer, kreativer Werke beklagt. Für eine künftige Zunahme der Onlinepiraterie sprechen die Ausweitung des Zugangs zu Breitbandanschlüssen und die Ausbreitung mobiler Technologien, die Diversifizierung der technischen Möglichkeiten zur Rechtsverletzung sowie die fortschreitende Digitalisierung kreativer Erzeugnisse¹⁶¹⁰.

6. P2P

Alle diese Modelle erfassen allein Urheberrechtsverletzungen, die über das Hoch- und Herunterladen von Daten in P2P-Netzwerken erfolgen. Diese Eingrenzung ist erforderlich, weil nach dem aktuellen Stand der Technik nur Rechtsverletzungen über P2P-Netzwerke erfasst werden können. P2P-Nutzung macht einen wesentlichen Anteil der Verletzungen aus.¹⁶¹¹

II. Rechtsvergleichende Untersuchung

Warnhinweismodelle sind derzeit in Frankreich auf gesetzlicher Grundlage und in Irland auf Basis eines privaten Vergleichs zwischen dem größten Zugangsanbieter und verschiedenen Musikunternehmen etabliert. Im Vereinigten Königreich ist steht ein Warnhinweismodell vor der Einführung, ist aber derzeit noch Gegenstand einer gerichtlichen Überprüfung.

¹⁶⁰⁷ Siehe oben, S. 61.

¹⁶⁰⁸ Siehe oben, S. 65.

¹⁶⁰⁹ Siehe oben, S. 137.

¹⁶¹⁰ Siehe oben, S. 73.

¹⁶¹¹ Siehe oben, S. 219.

1. Frankreich¹⁶¹²

- Rahmen

Frankreich hat mit den sog. Hadopi-Gesetzen und den dazu gehörigen Verordnungen im Rahmen einer Gesetzesnovelle in 2009/2010 ein Warnhinweismodell zur Bekämpfung von Urheberrechtsverletzungen im Internet geschaffen. Kern ist ein mehrstufiges Warnhinweisverfahren, bei dem die neu errichtete **Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (Hadopi)** als unabhängige staatliche Behörde mit weitreichenden Befugnissen zur Verfolgung und Sanktionierung von Urheberrechtsverletzungen im Internet eine zentrale Rolle einnimmt.

- Verfahren

Das Verfahren wird von der Hadopi durchgeführt und ermöglicht die Versendung von Warnhinweisen an Inhaber von Internetanschlüssen, über die Urheberrechtsverletzungen begangen wurden. Nach zwei Warnhinweisen innerhalb eines Zeitraums von zwei Monaten und einem weiteren Verstoß innerhalb des darauffolgenden Jahres kann die Hadopi den Sachverhalt an die Staatsanwaltschaft abgeben und so in ein strafrechtliches Verfahren überleiten.

Der Anschlussinhaber hat, unabhängig davon, ob er selbst die Urheberrechtsverletzungen begangen hat, nach dem Gesetz die Pflicht, für eine ausreichende Sicherung seines Internetanschlusses zu sorgen. Kommt er dem nicht nach, kann im strafrechtlichen Verfahren gegen ihn eine Geldbuße in Höhe von bis zu 1.500 Euro verhängt und sein Internetanschluss für bis zu einem Monat gesperrt werden. Die Ermittlung der Urheberrechtsverletzung erfolgt durch Bevollmächtigte der Rechteinhaber. Sie teilen der Hadopi die IP-Adresse des potentiellen Urheberrechtsverletzers mit. Die Zuordnung der IP-Adresse zum jeweiligen Anschlussinhaber erfolgt durch die betreffenden Internetzugangsdiensteanbieter, welche gegenüber der Hadopi zur Auskunft verpflichtet sind. Verstöße gegen diese Mitteilungspflicht sind mit Geldbußen belegt. Die Hadopi ist zur automatischen Verarbeitung personenbezogener Daten bevollmächtigt, sofern und soweit dies erforderlich ist, um die Durchführung des Verfahrens durch die bei der Behörde eingerichtet Rechtsschutzkommission zu ermöglichen. Die Daten dürfen nur eine begrenzte Zeit gespeichert werden, und unmittelbaren Zugang hierzu haben nur vereidigte und zugelassene Bevollmächtigte der Rechteinhaber sowie Mitglieder der Rechtsschutzkommission der HADOPI.

¹⁶¹² Siehe oben, S. 76.

Außerhalb des (straf-)gerichtlichen Verfahrens soll das Warnhinweissystem zur Eindämmung von Urheberrechtsverstößen im Internet beitragen und für einen gerechten Interessenausgleich zwischen den Beteiligten unter Beachtung rechtsstaatlicher Maßgaben sorgen. Das Modell ist insofern in Zusammenhang mit den weiteren Maßnahmen zu sehen, die durch die Hadopi-Gesetze initiiert wurden und die weitere Aufklärung sowie die Förderung von legalen kulturellen Angeboten im Internet zum Gegenstand haben

- Effekte

Die Peer-to-Peer-Nutzung in Frankreich ist nach Aufnahme der Warnhinweisversendung zwischen April 2010 und April 2011 um insgesamt **31 Prozent** gesunken, wobei ein deutlicher Einbruch zum Zeitpunkt der Versendung der ersten Warnhinweise zu verzeichnen war.

2. Vereinigtes Königreich¹⁶¹³

- Rahmen

Das Warnhinweismodell ist mit Erlass des Digital Economy Act (DEA) im April 2010 im britischen Recht verankert worden und wird derzeit auf Betreiben zweier britischer Diensteanbieter gerichtlich in zweiter Instanz überprüft. Die Durchführung der Warnhinweisversendung hängt vom Erlass behördlicher Ausführungsvorschriften ab, welcher bis zum Abschluss des Gerichtsverfahrens ausgesetzt ist.

- Verfahren

Der DEA normiert ein zweistufiges Warnhinweismodell.

Die erste Stufe soll einen Anspruch auf Auskunftserteilung über die Identität des Rechtsverletzers vorbereiten. Das Gesetz regelt die Meldung von Urheberrechtsverstößen, die Versendung von Warnhinweisen an Anschlussinhaber, die Festlegung einer Anzahl von Verstößen, ab der ein Anwender als besonders relevant gilt, und ab welchem Zeitpunkt der Rechteinhaber anhand einer über den Anschlussinhaber anonym geführten Liste gerichtlich Auskunft über dessen Identität verlangen kann. Außerdem enthält es Regelungen zur Speicherung von Anschlussinhaberdaten und Kostenregelungen zur Durchführung des Verfahrens. Dem *Office of Communications* (OFCOM) wurde als zur Medienaufsicht berufener Behörde übertragen, die **Durchführung** der Maßnahmen des DEA im Einzelnen in einem *Initial Obligations Code* zu normieren und zu überwachen.

Die zweite Stufe des britischen Modells setzt den Erlass eines *Technical Obligations Code* voraus. Dieser soll die Anordnung von technischen Sanktionen, wie Sperrun-

¹⁶¹³ Siehe oben, S. 110.

gen und Drosselungen von Internetanschlüssen, als Folge von Verletzungshandlungen regeln. Er ist gegebenenfalls von der OFCOM vorzulegen, was noch nicht geschehen ist, weil zunächst abgewartet werden soll, ob sich das Warnhinweismodell auch ohne Sanktionen als hinreichend effizient erweist.

- Nutzen

Um das Gesetzgebungsverfahren und die damit verbundenen Eingriffe in die jeweiligen Rechtspositionen abzusichern und zu legitimieren, wurde durch Regierungsstellen eine Kosten-Nutzen-Analyse („Impact Assessment“) erstellt, die den ökonomischen Nutzen des neuen Modells ermittelt. Konkret wurde unter Zugrundelegung der Preisbasis des Jahres 2008 über einen Zeitraum von zehn Jahren ein Netto-Nutzen des Warnhinweismodells von £1,2 Mrd. ermittelt.

3. Republik Irland¹⁶¹⁴

- Rahmen

In Irland existiert ein Vergleich zwischen dem führenden Zugangsanbieter und vier großen irischen Musikproduktionsgesellschaften, der eine Warnhinweis-Regelung vorsieht, die in der Abschaltung des Internetanschlusses enden kann. Ferner existiert auf der Grundlage des Vergleichs ein Protokoll zur Umsetzung der Regelungen. Mit den Warnhinweisen soll verhaltenssteuernd auf die Nutzer eingewirkt werden. Die Wirkung soll mit drei Schritten erzielt werden, nämlich zunächst durch erzieherische Aufklärung über die Urheberrechtsverletzung, dann abschreckend durch die Androhung einer Sanktion und schließlich durch Sanktionsverhängung selbst.

- Verfahren

Ausgangspunkt des irischen Modells ist, dass die Rechteinhaber eine Urheberrechtsverletzung im Internet ermitteln und dem Provider unter Angabe der betreffenden IP-Adresse in bestimmter Form „nachweisen“. Der Provider versendet dann an den Anschlussinhaber zunächst eine Nachricht mit dem Hinweis auf die Rechtsverletzung. Im Falle eines weiteren Urheberrechtsverstoßes ergeht eine Warnung, dass der Anschluss bei einer erneuten Verletzungshandlung für eine Woche unterbrochen wird. Gegebenenfalls wird sodann der Internetanschluss für diesen Zeitraum gesperrt. Findet danach wieder eine Urheberrechtsverletzung über den betreffenden Anschluss statt, dann kann dieser für ein Jahr abgeschaltet werden. Auf allen Stufen des Verfahrens hat der Anschlussinhaber die Möglichkeit der Beschwerde gegenüber dem Provider. Der Auskunftsanspruch nach irischem Recht

¹⁶¹⁴ Siehe oben, S. 146.

steht anders als im Vereinigten Königreich unverbunden neben dem Warnhinweismodell.

Der irische High Court hat die Vergleichsregelung im Hinblick auf datenschutzrechtliche Anforderungen überprüft und nicht beanstandet. Der irische Datenschutzbeauftragte hat gegenüber betroffenen irischen Provider angeordnet, die Anwendung der Warnhinweis-Regelung zu stoppen.

- Effekte

Daten zu messbaren Auswirkungen des Modells auf die Internetpiraterie liegen vor, sind aber nicht zur Veröffentlichung freigegeben.

4. Ausgewählte weitere Europäische Staaten¹⁶¹⁵

In verschiedenen weiteren EU-Staaten existieren Gesetzesentwürfe zu Warnhinweismodellen, die aber bislang nicht umgesetzt worden sind. In Finnland wurde der Gesetzesentwurf einer Warnhinweis-Regelung nach Parlamentsneuwahlen und einem Regierungswechsel nicht weiter verfolgt. Auch in Belgien existiert ein Gesetzesvorschlag, der aber nicht in das Parlament eingebracht wurde.

III. Effizienz von Warnhinweismodellen¹⁶¹⁶

Die Effizienz von Warnhinweisen wurde aus technischer, pädagogischer, informationeller und wirtschaftlicher Perspektive untersucht.

1. Technische Perspektive¹⁶¹⁷

Aus **technischer Sicht** stellt sich die Frage nach einer sicheren Identifikation sowohl der Rechtsverletzung als auch des hierfür Verantwortlichen. Besonderes Augenmerk liegt auf der Speicherung von Daten. Soweit nicht unter einem Klarnamen gehandelt wird, ist das Identifizierungsmerkmal im Internet die IP-Adresse. Diese gibt jedoch keinen Aufschluss über die handelnde Person sondern nur über den Inhaber des Anschlusses, über den eine mögliche Rechtsverletzung begangen wurde. Die Zuordnung ist nur über die Internetdiensteanbieter unter Rückgriff auf Verkehrs- und Bestandsdaten technisch möglich. Für die Effektivität des Warnhinweismodells ist es entscheidend, wie sicher eine Urheberrechtsverletzung festgestellt und einer IP-Adresse zugeordnet sowie der Anschlussinhaber identifiziert

¹⁶¹⁵ Siehe oben, S. 168 ff.

¹⁶¹⁶ Siehe oben, S. 196.

¹⁶¹⁷ Siehe oben, S. 196.

werden kann. Wichtig sind die Qualität der eingesetzten Software, insbesondere durch Ergänzung der Such- und Identifizierungsparameter für die urheberrechtlich relevanten Dateien.

Soweit vom Rechteinhaber der Nachweis einer konkreten Rechtsverletzung abverlangt wird, beschränken sich nach derzeitigem Stand der Technik die Möglichkeiten der Verfolgung auf Rechtsverletzungen in Peer-to-Peer -Netzwerken. Andere Technologien bleiben derzeit aus technischen Gründen außen vor, so dass unrechtmäßiges Verhalten im Internet von vorne herein nur in begrenztem Rahmen überhaupt erfasst werden kann. Allerdings stellt Peer-to-Peer-Nutzung nach wie vor einen wesentlichen Anteil der illegalen Nutzun dar.

2. Pädagogische Perspektive¹⁶¹⁸

Aus **pädagogischer Sicht** stellt sich die Frage nach der Neigung von Nutzern, in Folge einer Sanktion oder Sanktionsandrohung im Rahmen eines Peer-to-Peer-Filesharing auf andere Formen illegaler Nutzung zu wechseln, die aus technischen Gründen nicht ermittel- und damit nicht sanktionierbar ist. Zugleich ist relevant, ob Nutzer sich nach Warnungen und gegebenenfalls Sanktionen legalen Nutzungsformen zuwenden. Die Erhebungen aus Schweden zeigen, dass die sich im Bereich Musik, das Nutzerverhalten und auch der Umsatz mit digitalem Content unmittelbar in Richtung legaler Angebote ändern, wenn Nutzer mit einer Rechtsfolge rechnen müssen. Sobald eine Rechtsverfolgung nicht mehr droht, findet teilweise wieder eine Abkehr von der Legalität statt, wobei da, wo legale Substitute zu den Piraterieangeboten existierten, die Abkehr von der Illegalität dauerhaft war. Exakte Voraussagen dazu, wie die Reaktionen auf die Anwendung eines Warnhinweisverfahrens sein werden, lassen sich nicht treffen. Insbesondere die Erfahrungen mit dem französischen und irischen Modell sind noch nicht abschließend bzw. nicht hinreichend aussagekräftig. Es gibt Anzeichen dafür, dass die Gründe für eine Verhaltensänderung der Nutzer von vielen Faktoren abhängen. Dies können neben kulturellen Besonderheiten die Zugänglichkeit und Erschwinglichkeit legaler Angebote, deren Kennzeichnung, die Aufklärung der Verbraucher sowie die Rechtsverfolgung und Sanktionierung von Verstößen sein. Der tatsächliche zu erzielende Effekt wird daher immer auch von den konkreten Umständen des nationalen Regelungssystems und der Akzeptanz der Nutzer abhängen. Jedenfalls aber führen die Betrachtungen der verschiedenen Länder nicht zu dem Ergebnis, dass diese Maßnahmen ineffizient seien. Eine aktuelle Studie aus den USA kommt vielmehr für das Warnhinweismodell in Frankreich zu dem Ergebnis, dass die Kombination aus Sanktionsandrohung, Medienaufmerksamkeit und Aufklärung über die Rechtswidrigkeit

¹⁶¹⁸ Siehe oben, S. 203.

von Filesharing sowie der Hinweis auf legale Alternativen den Nutzern den Weg in die Legalität geöffnet hat. So kam es in Frankreich schon in Ansehung der Einführung des Warnhinweissystems zu einer Umsatzsteigerung bei den Musikverkäufen über die Online-Vertriebsplattform iTunes.

3. Informationelle Perspektive¹⁶¹⁹

Im Zusammenhang mit der **informationellen Perspektive** geht es um die Medienkompetenz der Nutzer bei der Einordnung von Angeboten und die Funktion der Aufklärungsarbeit. Auch wenn nicht abschließend geklärt ist, inwieweit Aufklärung zu einer Veränderung des Nutzerverhaltens beiträgt, sind positive Effekte wahrscheinlich. Unabhängig von jeder gezielten Einwirkung auf die Nutzer und deren Verhaltensschemen kann Aufklärung dazu beitragen, die offenbar nicht immer klar umrissenen rechtlichen Rahmenbedingungen und die Konsequenzen rechtswidrigen Handelns zu vermitteln. Die vorliegenden Daten zeigen, dass einerseits ein Bedürfnis besteht, dem Nutzer die Unterscheidung von legalen und illegalen Angeboten zu vereinfachen. Dazu können Kennzeichnungen legaler Angebote beitragen. Es zeigt sich aber, dass die Handlungsmöglichkeiten des aktiven Internetnutzers nicht immer der rechtlich richtigen Bewertung zugeordnet werden. Auch hier besteht Aufklärungsbedarf. Kenntnis der Rechtslage, der zu erwartender Folgen bzw. Sanktionen des Handelns sowie Auswirkungen des eigenen Handelns auf Dritte und die Allgemeinheit setzen dabei im Rahmen der Aufklärung unterschiedliche Impulse, indem sie Rechtskenntnis, Unrechtsbewusstsein und Gerechtigkeitsempfinden fördern. Positive Auswirkungen im Sinne einer Verhaltensänderung sind nicht nachgewiesen, aber auch nicht auszuschließen. Jedenfalls können durch Aufklärung Sachverhalte vermieden werden, die nach derzeitiger Rechtslage als ungerecht empfunden werden. Ein Warnhinweissystem kann verhindern, dass ein Rechtsverletzer in Unkenntnis der rechtlichen Konsequenzen sanktioniert wird, wenn er etwa Peer-to-Peer-Filesharing zum ersten Mal durchführt. Dies gilt auch für den in Anspruch genommenen Anschlussinhaber, dem die über seinen Anschluss begangenen Rechtsverletzungen unbekannt sind.

4. Wirtschaftliche Perspektive¹⁶²⁰

Bei der Bewertung der Effizienz aus **wirtschaftlicher Perspektive** geht es um die Kosten-Nutzen-Analyse bei Einführung eines Warnhinweissystems. Nach staatlichen Erhebungen für das Vereinigte Königreich entstehen für die Diensteanbieter über einen Zeitraum von 10 Jahren Gesamtkosten in Höhe von £290 - 500 Mio. Für

¹⁶¹⁹ Siehe oben, S. 219.

¹⁶²⁰ Siehe oben, S. 223.

die Rechteinhaber wird der Gesamtnutzen über denselben Zeitraum auf £1,7 Mrd. beziffert. Der französischen Hadopi stand zur Aufgabenerfüllung für 2011 ein Budget in Höhe von 13,79 Millionen Euro zur Verfügung (im Jahr 2010 waren es 10,85 Millionen Euro). Wesentlicher Kostenfaktor ist das Warnhinweisverfahren. Zuverlässige Daten dazu, welcher zahlenmäßige Aufwand auf Seiten der Internetdiensteanbieter und der Rechteinhaber im Rahmen des Verfahrens in Frankreich entsteht, liegen nicht vor. Für Irland ist nach der Datenlage unklar, welche der Kosten das Warnhinweisverfahren für Zugangsanbieter und Musikproduktionsgesellschaften verursachen und ob sie im Ergebnis wirtschaftlich nutzen.

IV. Rechtsdurchsetzung nach deutschem Urheberrecht¹⁶²¹

Die zivilrechtliche Verfolgung von Urheberrechtsverletzungen im Internet erfolgt in Deutschland über die Geltendmachung eines gerichtlichen Auskunftsanspruchs gegenüber dem Zugangsanbieter, mit dem der Rechteinhaber die Identität des Anschlussinhabers in Erfahrung bringen kann. Er wird bei offensichtlicher Rechtsverletzung und gewerblichem Ausmaß der rechtswidrigen Zugangsvermittlung gewährt. Die Auskunftserteilung erstreckt sich auf Verkehrsdaten und steht unter Richtervorbehalt. Die praktischen Probleme des Anspruchs bestehen in der Gefahr seines rechtsmissbräuchlichen Einsatzes sowie darin, dass er unvermittelt und ohne Vorwarnung Anschlussinhaber trifft, über deren Anschlüsse Rechtsverstöße durch Dritte begangen wurden. Nach Auskunftserteilung kann der Rechteinhaber zivilrechtliche Ansprüche gegenüber dem Anschlussinhaber geltend machen.

B. 2. Teil: Erwägungen zu einem innerstaatlichen Ansatz

Die Studie skizziert die rechtlichen Rahmenbedingungen für die mögliche Umsetzung eines Warnhinweismodells zur Reduzierung von Urheberrechtsverletzungen im Internet. Um die internationalen, die verfassungs- und einfachgesetzlichen Rahmenbedingungen eines Warnhinweismodells nicht abstrakt prüfen zu müssen, sondern konkret erörtern zu können, wird ein hier ein schlagwortartig als vorgeordnetes Mitwirkungsmodell bezeichneter Lösungsansatz vorgestellt. Diese Ausführungen erfolgen unabhängig von der Projektbeschreibung und können als Ansatz für eine weiterführende Diskussion dienen. Das eigentliche Spannungsfeld eines solchen Modells liegt dabei zwischen dem Urheberrecht der Rechteinhaber, die die Rechte an ihrem geistigen Eigentum wahren wollen und dem Recht der rechts-

¹⁶²¹ Siehe oben, S. 226.

verletzenden Nutzer darauf, dass bei der Verfolgung ihrer Verletzungshandlungen Belange des Datenschutzes und der Informationsfreiheit beachtet werden. Im Internet sind in dieses Verhältnis aber zwingend die Zugangsanbieter als private Dritte eingebunden. Rechteinhaber können potentielle Verletzungshandlungen durch Ermittlung einer IP-Adresse feststellen, Namen und Anschrift des Rechteverletzers kennt aber nur der Zugangsanbieter.

I. **Vorgerichtliches Mitwirkungsmodell**¹⁶²²

Das Mittel im Rahmen des hier vorgeschlagenen Modells zur Reduzierung von Rechtsverletzungen im Internet ist eine Kombination aus aufklärenden Warnungen und Auskunftsanspruch. Dabei geht es weder darum, internetspezifische Angebote zu kriminalisieren noch darum Rechtsverstöße zu legalisieren. Vielmehr sollen die vorhandenen urheberrechtlichen Wertungen in Lösungsansätze einfließen, die den Bürger erreichen. Das Modell verbindet die als solche rechtsfolgenlose Warnhinweisregelung über einen effektuierten Auskunftsanspruch mit der zivilrechtlichen Durchsetzung des Anspruchs als Sanktion im Rahmen der zivilrechtlichen Rechtsverletzung. Dabei wird auf Sanktionen verzichtet, die wie Sperren oder Drosselung von Anschlüssen über das derzeit in Deutschland geltende Recht hinaus gehen. Rechtsstaatlich ist der Ansatz von Vorteil, weil er vor einer Abmahnung auf aufklärende Warnungen setzt.

II. **Verfahrensablauf**

Nach Feststellung eines Rechtsverstoßes unter Ermittlung der IP-Adresse des Anschlussinhabers durch den Rechteinhaber übermittelt diese die IP-Adresse an den betreffenden Zugangsanbieter. Dieser versendet eine aufklärende Warnung an den Anschlussinhaber, dessen Klarnamen und Anschrift er als dessen Vertragspartner hat. Zugleich legt er den Namen und den Verstoßvorwurf in einer intern geführten Liste ab und informiert den Anschlussinhaber darüber. Ab einer bestimmten Zahl von festgehaltenen Verstößen ist die anonymisierte, also um den Klarnamen des Anschlussinhabers bereinigte Verstoßliste, dem Rechteinhaber bekannt zu geben und der Anschlussinhaber darüber zu informieren. Der Rechteinhaber kann dann, wie nach derzeit geltendem Recht, im Wege eines gerichtlichen Auskunftsverlangens Namen und Anschrift des Rechteinhabers heraus verlangen. Der besondere Nutzen der Verstoßliste liegt darin, dass der Rechteinhaber hieraus ersehen kann, welche für ihn anonyme Person häufig oder gravierend Urheberrecht verletzt ha-

¹⁶²² Siehe oben, S. 268.

ben soll. Auf dieser Basis kann er seinen Auskunftsanspruch gegen den Provider gezielt mit Blick auf solche Fälle beschränken, die für eine gewerbsmäßige Urheberrechtsverletzung in Betracht kommen.

III. Vorteil des Modells

Das vorgerichtliche Mitwirkungsmodell setzt wie in Frankreich, England und Irland auf Warnungen des Nutzers. Diese ziehen zunächst keine Sanktion und kein Unwerturteil nach sich. Die Hinweise können dem Nutzer die Wertungen des Urheberrechtsschutzes durch einen aufklärenden und zugleich warnenden Hinweis nachvollziehbar machen, damit er sich dazu entscheiden kann, sie im Internet zu achten. Der Ansatz will dabei nicht nur das Bewusstsein für Rechtsüberschreitungen erzeugen, sondern kann über Hinweise zu legalen Angeboten – wie in allen Referenzstaaten - den Zugang zu Kulturgütern im Internet fördern.

Mit diesen Warnungen werden Personen aufgeklärt, die in Unkenntnis der Rechtslage Urheberrechte im Internet verletzen. Nutzer, die bewusst gegen Urheberrecht verstoßen um eigennützig kostenfrei an Inhalte zu gelangen, würden über die Warnhinweise deutlich gemacht, dass sie auf einer Verstoßliste geführt werden und einer zivilrechtlichen Inanspruchnahme entgegensehen. Kommt es nicht zu einer dritten Verwarnung, drohen grundsätzlich keine rechtlichen Konsequenzen.

IV. Erfordernis rechtlicher Konsequenzen bei mehrfachen Verstößen

Für den Fall, dass ein Nutzer sich nach Aufklärung und Warnung gegen die Achtung des Urheberrechts entscheidet, muss dies aus rechtstaatlicher Sicht und nach den Erfahrungen in den Referenzstaaten eine rechtliche Konsequenz nach sich ziehen. Diese stellen aber keine Verschärfung des geltenden Rechts dar. Sie mildern im Gegenteil dessen Härte, weil der betreffende Nutzer auch über die drohenden Rechtsfolgen aufgeklärt und sich nicht mehr auf Unkenntnis der Illegalität seines Handles berufen kann.

V. Unterschied gegenüber dem reinen Auskunftsanspruch

Im aktuellen deutschen Recht zur Durchsetzung von Urheberrechten durch den Auskunftsanspruch nach dem UrhG sieht sich der Nutzer unvermittelt einer Abmahnung ausgesetzt, die ein sehr scharfes erstes Mittel darstellt, das zudem anfällig für als missbräuchlich empfundene Verwendung ist. Der Vorteil des vorgeschlage-

nen Modells gegenüber dem aktuellen Recht bestünde darin, dass der Auskunftsanspruch zielgenauer und Vorwarnung geltend gemacht würde. Der hinter einer IP-Adresse stehende Klarname kann sich auf einen Einzelfall beziehen oder einen Mehrfachtäter treffen, insbesondere letzterer ist aber für den Rechteinhaber relevant. Aus der Verstoßliste könnte der Rechteinhaber ersehen, welche für ihn anonyme Person häufig oder gravierend Urheberrecht verletzt. Auf dieser Basis könnte er seinen Auskunftsanspruch gegen den Provider gezielt auf Fälle beschränken, die für eine gewerbsmäßige Urheberrechtsverletzung in Betracht kommen. So würde das bestehende System von Auskunftsanspruch und nachfolgender zivilrechtlicher Durchsetzung des urheberrechtlichen Anspruchs gegenüber dem Nutzer effektiviert und die Gerichte entlastet.

VI. Rechtlicher Rahmen¹⁶²³

1. Internationaler urheber- und datenschutzrechtlicher Rahmen¹⁶²⁴

Der Vorschlag bewegt sich im Rahmen des internationalen und europäischen Rechts und berücksichtigt insbesondere die urheber- und datenschutzrechtlichen Vorgaben. Er beachtet insbesondere die aktuelle Rechtsprechung des Europäischen Gerichtshofs (Scarlet Extended), wonach das geistige Eigentum besonderen Schutz des Europarechts genießt. Der EuGH hat zu dessen Schutz eine einseitige und umfassende Filterverpflichtung zulasten von Zugangsanbietern für unzulässig erklärt. Zugleich hat er das Erfordernis eines effektiven Urheberrechtsschutzes in den Mitgliedstaaten betont. Den Vermittlern könnten Maßnahmen aufgegeben werden, die nicht nur begangene Rechtsverletzungen beenden sondern auch neuen Verletzungen vorbeugen. Insbesondere erfolgt eine Abwägung der Eigentümerinteressen der Rechteinhaber mit der unternehmerischen Freiheit der Provider in deren Ergebnis der EuGH eine einseitige Lösung zugunsten der Rechteinhaber ablehnt. Nach der Logik der Entscheidung sind damit auch Provider in der Pflicht, sich an einem Modell zum Schutz des geistigen Eigentums zu beteiligen, das sowohl präventiv als repressiv ansetzen kann.

2. Nationaler Rechtsrahmen

Aus Sicht des **nationalen Rechts** sind der Schutz des geistigen Eigentums der Rechteinhaber mit den Anforderungen des **Datenschutzes** und der Informationsfreiheit der Nutzer sowie die unternehmerischen Interessen der Provider zu be-

¹⁶²³ Siehe oben, S. 269.

¹⁶²⁴ Siehe oben, S. 270.

leuchten. Den Nutzer schützen die Kommunikationsfreiheit und das allgemeine Persönlichkeitsrecht.

a. Datenschutzrecht¹⁶²⁵

Warnhinweismodelle erfordern Zugriff auf Daten durch das Ermitteln, Sammeln, und Weitergabe von Informationen zum Kommunikationsvorgang und zur Identität eines potentiellen Rechteverletzers. Das Bundesverfassungsgericht hält eine sechsmonatige, vorsorgliche anlasslose Speicherung von Telekommunikationsverkehrsdaten bei entsprechender gesetzlicher Ermächtigung durch private Diensteanbieter für „mit Art. 10 GG nicht schlechthin unvereinbar.“ „Erforderlich sind hinreichend anspruchsvolle und normenklare Regelungen hinsichtlich der Datensicherheit, der Datenverwendung, der Transparenz und des Rechtsschutzes“.

Ein Warnhinweisverfahren setzt die Ermittlung eines Urheberrechtsverstoßes und damit eines ggf. strafrechtlich relevanten Sachverhalts voraus. Relevante Daten hierfür sind zumindest die Ermittlung der IP-Adresse des Anschlussinhabers sowie der Zugriffszeiten, zu denen eine Rechtsverletzung begangen wurde. Darüber hinaus bedarf es zur Geltendmachung von Ansprüchen im Rahmen der Darlegungslast des Rechteinhabers gegebenenfalls weiterer Informationen, wie etwa zu den Inhalten bzw. Metadaten involvierter Dateien. Diese Daten werden im Rahmen der Rechtsdurchsetzung von den Rechteinhabern bzw. deren Beauftragten, in Frankreich etwa von zertifizierten Bevollmächtigten oder in Irland von Dienstleistern, erhoben. Nicht jede Art von Information berührt das grundrechtlich geschützte Recht des Einzelnen auf Privatsphäre bzw. informationelle Selbstbestimmung. Datenschutzrechtlich relevante Informationen sind insofern nur Einzelangaben über persönliche oder sachliche Verhältnisse, die sich auf eine bestimmte oder zumindest bestimmbare Personen beziehen. Dies setzt zum einen voraus, dass die Information sich auf eine einzelne Person bezieht, zum anderen muss sie diese als solche identifizierbar machen.

Datenschutzrechtlich zentral ist bei der Verfolgung von Rechteverletzungen im Internet die IP-Adresse, welche die Identifizierung des Anschlussinhabers erlaubt. Die Einordnung der IP-Adresse als personenbezogen ist nicht einheitlich; sie wird aber tendenziell grundsätzlich als datenschutzrelevantes Datum anerkannt. Der EuGH hat sie jüngst ohne Begründung als personenbezogenes Datum bezeichnet (Scarlet Extended). Nach deutschem Recht stellt die Ermittlung der IP-Adresse und damit zusammenhängender Informationen eine Erhebung und ihre Weitergabe an Dritte eine Übermittlung dar.

¹⁶²⁵ Siehe oben, S. 294.

Aus der Perspektive des Rechteinhabers ist die IP-Adresse zunächst kein personenbezogenes Datum, weil die Person des Anschlussinhabers für ihn nicht feststellbar ist. Für die auch derzeit praktizierte Feststellung eines Verstoßes mit Erhebung, Speicherung sowie mit der Weitergabe der IP-Adresse an den Zugangsanbieter bedarf es also keiner weiteren ausdrücklichen Ermächtigung.

Warnhinweismodelle basieren auf der **Mitwirkung** der **Zugangsdiensteanbieter**, die dazu verpflichtet würden, nicht nur Bestands-, sondern auch Verkehrsdaten, namentlich die IP-Adresse und den Zeitpunkt des Zugriffs, ihrer Anschlusskunden zu speichern und in eine Liste aufzunehmen, um sie dann in anonymisierter Form einer berechtigten Person herauszugeben. Datenschutzrechtlich und vor dem Hintergrund der Gewährleistung des Fernmeldegeheimnisses ist dies nur bei Vorliegen einer entsprechenden Ermächtigung möglich. Nach dem im Datenschutzrecht geltenden Zweckbindungsgrundsatz dürfen erlangte Kenntnisse nachträglich nicht auch für andere Zwecke als für diejenigen verwendet werden, für die sie zunächst erhoben wurden. Im Hinblick auf den für den Auskunftsanspruch relevanten Erlaubnistatbestand des § 100 Abs. 1 TKG, wonach eine Speicherung von Bestands- und Verkehrsdaten zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an TK-Anlagen zulässig ist, lässt die Rechtsprechung eine anlasslose Speicherung der Daten durch Zugangsdiensteanbieter jedenfalls für einen Zeitraum von sieben Tagen nach Beendigung der Nutzung zu.

b. Verfassungsrechtliche Vorgaben¹⁶²⁶

Während der Schutz des geistigen Eigentums über Art. 14 Abs. 1 GG gewährt wird, ist ein Warnhinweismodell unter Mitwirkung der Zugangsanbieter insbesondere an deren Berufsfreiheit aus Art. 12 Abs. 1 GG zu messen. Verfassungsrechtlich betrachtet, handelt es sich um eine Inpflichtnahme Privater zur Aufgabenerfüllung.

- Voraussetzungen einer Inpflichtnahme Privater

Die Verpflichtung zur Versendung von Warnhinweisen durch Zugangsanbieter ist als Berufsausübungsregelung einzuordnen, weil sie „die eigentliche Berufstätigkeit als Grundlage der Lebensführung unberührt lässt“ (BVerfGE 75, 246, 274) und in den Schutzbereich von Art. 12 Abs. 1 GG einzuordnen ist. Ob es sich bei der Versendung von Warnhinweisen um eine staatliche oder private Aufgabe handelt kann dahin stehen, weil die Verfassung keine kategorische Trennung von „Staatsaufgaben“ und „privaten Aufgaben“ kennt und dem Gesetzgeber einen weiten Gestaltungsspielraum zuerkennt, „welche Pflichten zur Sicherstellung von Gemeinwohlbelangen er Privaten im Rahmen ihrer Berufstätigkeit auferlegt (vgl. BVerfGE 109, 64, 85)“ (BVerfGE 125, 260, 261 f.). Bei der Entscheidung welche Private er in Dienst

¹⁶²⁶ Siehe oben, S. 303.

nimmt, hat der Staat einen weiten Beurteilungsspielraum. Anbieter öffentlich zugänglicher Telekommunikationsdienste können etwa verpflichtet werden, (die Daten ihrer Kunden für sechs Monate zu speichern (vgl. BVerfGE 95, 173, 187). Die Frage der Entschädigung und Kostenverteilung im Rahmen der Indienstnahme bedürfte einer eingehenden Prüfung, nachdem eine Abschätzung der Kosten möglich ist.

- Eingriff in die Berufsfreiheit

Ein Eingriff in die Berufsausübungsfreiheit unterliegt nach der Dreistufentheorie des Bundesverfassungsgerichts der Schranke des Übermaßverbotes. Er ist zulässig, wenn er in einem vernünftigen Verhältnis zu dem gegebenen Anlass und dem damit verbundenen Zweck steht. Das ist bei einer Berufsausübungsregelung der Fall, wenn sich „vernünftige Gründe des Gemeinwohls dafür finden lassen. Gesichtspunkte der Zweckmäßigkeit sind ausreichend, wenn die Regelung für die Betroffenen zumutbar und nicht übermäßig belastend ist. (vgl. BVerfGE 7, 377, 406).“

Bei der Abwägung ist nach einem legitimen Zweck des Eingriffs, sowie nach seiner Eignung und Erforderlichkeit zur Erreichung des Zwecks zu fragen, so wie nach dessen Zumutbarkeit für den Betroffenen.

Einen **legitimen Zweck** würde das staatliche Handeln im Wege eines vorgerichtlichen Mitwirkungsmodells allein deswegen verfolgen, weil Urheberrechtsverletzungen im Internet urheberrechtswidrig sind.

Bei der Frage nach der **Eignung** eines Eingriffs in Rechtsgüter hat der Gesetzgeber einen weiten Entscheidungsspielraum. Die Grenze zur Verfassungswidrigkeit ist überschritten, wenn Maßnahme sich als offensichtlich oder schlechthin ungeeignet darstellt. Auch wenn die Wirksamkeit von Warnhinweisen noch nicht abschließend geklärt ist, lässt diese sich jedenfalls grundsätzlich nicht ausschließen. Die Eignung der Maßnahme ist danach zu beurteilen, ob das Mittel einen Schritt in die richtige Richtung weist. Die kurzzeitigen Erfahrungen aus Frankreich und Irland erlauben nur begrenzt Rückschlüsse auf die Effizienz von Warnhinweisen. Während für Irland keine Daten verfügbar sind, ist die Peer-to-Peer-Nutzung in Frankreich zwischen April 2010 und April 2011 um insgesamt 31 Prozent gesunken, wobei ein deutlicher Einbruch zum Zeitpunkt der Versendung der ersten Warnhinweise zu verzeichnen war. Eine Untersuchung für Schweden hat ergeben, dass die Furcht vor Sanktionen von Internetpiraterie zu einem Rückgang von Urheberrechtsverletzungen im Internet führt, mit der ein Anstieg des Umsatzes legaler Angebote einher ging. Dieser Effekt ließ nach, nachdem von einer Durchsetzung von Sanktionen abgesehen wurde. Der Eignung des vorgerichtlichen Mitwirkungsmodells steht eine Beschränkung auf P2P-Netzwerke nicht entgegen, weil über diese Nutzungsform weltweit mit 16,37 Prozent die mit Abstand meisten unautorisierten Downloads erfolgen. Im

Vereinigten Königreich geht man von 37 Prozent der Urheberrechtsverletzungen im Internet durch illegales P2P-Filesharing aus während in Deutschland von etwa 20 Prozent ausgegangen werden kann.

Das Übermaßverbot verpflichtet den Staat dazu, sich bei den Bürger belastenden Maßnahmen auf das Notwendige zu beschränken. Im Rahmen der **Erforderlichkeitsprüfung** ist nach Mitteln zu suchen, die das Ziel des Staates bei gleicher Wirksamkeit weniger belasten. Als Handlungsvarianten kommen ein Vorgehen ohne Mitwirkung der Zugangsanbieter, ein Agieren nur im Rahmen des Auskunftsanspruchs, eine sanktionslose Versendung von Warnhinweisen sowie eine anlasslose Warnhinweise und Netzsperrern in Betracht.

Ein Vorgehen im Wege von Warnhinweisen ohne Mitwirkung der Zugangsanbieter wäre tatsächlich unmöglich, da die Zuordnung von durch die Rechteinhaber ermittelten Daten allein durch die Zugangsanbieter erfolgen kann. Ein Auskunftsanspruch als alleiniges Mittel entfaltet seine aufklärende Wirkung erst im Zusammenhang mit einer gerichtlichen Inanspruchnahme und ist damit nicht präventiv. Zudem ist dieses Mittel schärfer als das hier vorgeschlagene Mittel, weil es nicht auf Warnung zielt. Das Vorgehen im Rahmen des Auskunftsanspruchs mag zwar im Verhältnis zum Zugangsanbieter milder sein; es ist aber mit Blick auf das Regelungsziel nicht ebenso effektiv wie das hier vorgeschlagene Modell und im Verhältnis zum Nutzer schärfer. Ein völlig ohne Blick auf eine Konsequenz – also den Auskunftsanspruch - gerichtetes Warnhinweismodell wäre zwar milder, aber nicht effektiv. Auch das anlasslose Versenden von standardisierten Informationen durch die Zugangsprovider an ihre Kunden, in denen auf das Verbot von Urheberrechtsverstößen ohne konkreten Anlass hingewiesen wäre nicht effektiv, weil es für den Nutzer allein mit einer „Belästigung“ verbunden wäre. Ob eine anlasslose Warnung angesichts einer Vielzahl täglich eingehender Emails überhaupt die Wahrnehmungsebene des Nutzers erreichen würde ist fraglich. Netzsperrern sind nicht vom Gegenstand der vorliegenden Studie. Sie würden zwar möglicherweise ein effektiveres Mittel zur Aufklärung über und die Bekämpfung von Rechtsverletzungen im Internet sein, sind aber wegen der mit ihnen verbundenen rechtlichen Härten in Hinblick auf inhaltliche Zensur von Inhalten und ihre datenschutzrechtliche Eingriffsintensität keineswegs grundrechtsschonender und damit im Verhältnis zum vorgerichtlichen Mitwirkungsmodell kein milderes Mittel.

Abschließendes Kriterium des Verhältnismäßigkeitsgrundsatzes ist die **Angemessenheit** oder auch der Verhältnismäßigkeit im engeren Sinne, die auch Zumutbarkeit genannt wird. In deren Rahmen werden Zweck und Mittel in Relation gestellt. Bei der Frage nach der Zumutbarkeit des mit dem hier vorgeschlagenen Modell verbundenen Eingriff in die Kundenbeziehung zwischen Zugangsanbieter und Nutzer sind die Nähe der in die Pflicht genommenen Zugangsanbieter zur Rechtsver-

letzung und deren vertraglichen Befugnisse im Verhältnis zum Anschlussinhaber im Falle des Rechtsmissbrauchs zu berücksichtigen. Eine besondere Nähe der Zugangsanbieter zur Rechtsverletzung liegt insofern auf der Hand, als sie diese technisch über ihr Angebot ermöglichen. Das Vertrauensverhältnis zum Kunden würde durch ein Warnhinweismodell deshalb nicht in unzumutbarer Weise gestört, als nach den im Privatkundengeschäft geltenden AGB der großen in Deutschland tätigen Internet-Service-Provider die Kunden diesem gegenüber vertraglich dazu verpflichtet, bei Inanspruchnahme der Leistung bestehende Gesetze, insbesondere Urheberrechte bzw. Rechte Dritter einzuhalten. Die Vertragsbedingungen sehen vor, dass der Provider im Falle einer Pflichtverletzung berechtigt ist, den Zugang zum Internet zu sperren und/oder den Vertrag fristlos zu kündigen. Die Voraussetzungen für ein solches Recht variieren dabei im Einzelnen. Ist für die Internetnutzung eine Flatrate vereinbart, steht nach dem Provider vielfach das Recht zu, die Geschwindigkeit der Datenübertragung für den Rest des Abrechnungszeitraums zu drosseln, falls der Kunde das ihm nach dem Tarif für diesen Zeitraum zustehende Datenvolumen überschritten hat. Ein Sonderkündigungsrecht des Kunden oder eine Reduzierung des zu leistenden Entgelts ist für den Fall einer solchen Sperre des Anschlusses oder Drosselung der Übertragungsgeschwindigkeit nicht vorgesehen. Nach dem hier vorgeschlagenen Ansatz stehen derartige vertraglich vorgesehene und im Vergleich zum vorgerichtlichen Mitwirkungsmodell schärferen Maßnahmen wie Sperrung, Kündigung oder Drosselung durch den Zugangsanbieter in Folge von Urheberrechtsverletzungen nicht in Rede. Die Inpflichtnahme von Zugangsanbietern zur Mitwirkung im Rahmen eines vorgerichtlichen Mitwirkungsmodells in diesem Rahmen ist daher zumutbar.

Insgesamt wäre der Eingriff in das Grundrecht der Berufsfreiheit der Zugangsanbieter mit der im Rahmen des vorgerichtlichen Mitwirkungssystem vorgeschlagenen Inpflichtnahme vor dem Hintergrund von Art. 12 GG verfassungsrechtlich nicht zu beanstanden.

C. Fazit¹⁶²⁷

Das Modell der vorgerichtlichen Mitwirkung der Zugangsanbieter, das ein aufklärendes Warnhinweismodell mit einer Effektivierung des Auskunftsanspruchs verbindet, erscheint vor dem Hintergrund des internationalen und europäischen Rechtsrahmens zulässig. Insbesondere die Rechtsprechung des Europäischen Gerichtshofs legt ein Prävention und Repression verbindendes Modell zum Urheberrechtsschutz nahe. Verfassungsrechtlich ist eine aus technischen Gründen unab-

¹⁶²⁷ Siehe oben, S. 326.

dingbare Inpflichtnahme der Zugangsanbieter vor dem Hintergrund der Berufsfreiheit nicht zu beanstanden und stellt mit einer Kombination aus Aufklärung und Warnhinweis ein verhältnismäßiges Mittel beim Vorgehen gegen Urheberrechtsverletzungen im Internet dar. Im Hinblick auf den Datenschutz käme es auf die konkrete Ausgestaltung der Maßnahme an. Wegen seiner Einbindung des Vorgeschlagenen in die derzeit geltende Rechtslage zum Auskunftsanspruch, ist es datenschutzrechtlich schonend konstruiert.

ENTWURF / VERTRAULICH

Anhang (Gesetzestexte und Quellen)

Code de la Propriété Intellectuelle

in der konsolidierten Fassung vom 11.09.2011¹⁶²⁸

Auszug

GESETZBUCH ÜBER DAS GEISTIGE EIGENTUM

Artikel L.331-1

Für Zivilklagen und Forderungen in Bezug auf Urheberrechte an Werken der Literatur und Kunst, einschließlich jener, die Fragen des unlauteren Wettbewerb betreffen, sind ausschließlich die gesetzlich bestimmten Tribunaux de grande instance [dt.: Landgerichte] zuständig.

Die zum Schutz von Urheberrechten ordentlich gegründeten Berufsverbände sind befähigt vor Gericht aufzutreten, um Interessen, zu deren Vertretung sie satzungsmäßig beauftragt sind, zu verteidigen.

Der Begünstigte, der wirksam und exklusiv gemäß den Bestimmungen des Buchs II ein ausschließliches Nutzungsrecht verliehen bekommen hat, das einem Hersteller von Ton- oder Bildträgern gehört, darf, soweit der Lizenzvertrag nicht anders bestimmt, aufgrund dieses Rechts eine Klage anstrengen. Die Geltendmachung dieses Rechts wird dem Hersteller mitgeteilt.

Die vorstehenden Bestimmungen bilden gemäß den Bedingungen der Artikel 2059 und 2060 des französischen Bürgerlichen Gesetzbuches für die Inanspruchnahme eines Schiedsgerichts kein Hindernis.

Artikel L.331-2

Neben den Protokollen von Beamten oder Angestellten der Kriminalpolizei kann der Beweis der Substanzhaltigkeit eines Versto-

CODE DE LA PROPRIÉTÉ INTELLECTUELLE

Article L.331-1

Les actions civiles et les demandes relatives à la propriété littéraire et artistique, y compris lorsqu'elles portent également sur une question connexe de concurrence déloyale, sont exclusivement portées devant des tribunaux de grande instance, déterminés par voie réglementaire.

Les organismes de défense professionnelle régulièrement constitués ont qualité pour ester en justice pour la défense des intérêts dont ils ont statutairement la charge.

Le bénéficiaire valablement investi à titre exclusif, conformément aux dispositions du livre II, d'un droit exclusif d'exploitation appartenant à un producteur de phonogrammes ou de vidéogrammes peut, sauf stipulation contraire du contrat de licence, exercer l'action en justice au titre de ce droit. L'exercice de l'action est notifié au producteur.

Les dispositions qui précèdent ne font pas obstacle au recours à l'arbitrage, dans les conditions prévues aux articles 2059 et 2060 du code civil.

Article L.331-2

Outre les procès-verbaux des officiers ou agents de police judiciaire, la preuve de la matérialité de toute infraction aux dispositions des livres Ier, II et III du présent code

¹⁶²⁸ Deutsche Übersetzung im Wesentlichen: tolingo GmbH, 2011.

ßes nach den Bestimmungen der Bücher I, II und III dieses Gesetzes durch Feststellung seitens beeidigter Bedienstete erfolgen, die je nach Fall entweder vom Centre national du cinéma et de l'image animée (staatl. französische Filmförderungsbehörde) oder von den in Artikel L.331-1 erwähnten Berufsverbänden zum Schutz von Urheberrechten oder durch die in Titel II dieses Buches genannten Gesellschaften bestellt werden. Diese Bedienstete werden durch den Kultusminister gemäß den Bedingungen, die der Staatsrat durch Erlass vorgibt, zugelassen.

Artikel L.331-5

Die technisch wirksamen Maßnahmen, die dazu bestimmt sind, die vom Rechtsinhaber nicht genehmigte Nutzung eines Urheberrechtes oder eines verwandten Schutzrechtes an einem Werk, jedoch keine Software, an einer Interpretation, an einem Tonträger, Bildträger oder an einem Programm zu verhindern oder zu beschränken, sind nach den in diesem Titel genannten Bedingungen geschützt.

Im Sinne des ersten Absatzes bezeichnet der Ausdruck technische Maßnahme alle Technologien, Vorrichtungen oder Bestandteile, die im normalen Betrieb die in diesem Absatz beschriebene Funktion erfüllen. Diese technischen Maßnahmen sind als wirksam anzusehen, soweit die im gleichen Absatz genannte Nutzung von den Rechtsinhabern durch eine Zugangskontrolle oder einen Schutzmechanismus wie Verschlüsselung, Verzerrung oder sonstige Wandlung des Werks oder sonstigen Schutzgegenstands oder einen Mechanismus zur Kontrolle der Vervielfältigung, die die Erreichung des Schutzziels sicherstellen, unter Kontrolle gehalten wird.

Ein Protokoll, ein Format, ein Verschlüsselungs-, Verzerrungsverfahren oder die Wandlung des Werkes bilden an sich keine technische Maßnahme im Sinne dieses Artikels.

Die technischen Maßnahmen dürfen, unter Wahrung des Urheberrechts, nicht die effektive Umsetzung der Interoperabilität verhindern. Die Lieferanten der technischen Maßnahmen machen unter den unter Punkt 1 des Artikels L.333-31 und Artikel

peut résulter des constatations d'agents assermentés désignés selon les cas par le Centre national du cinéma et de l'image animée, par les organismes de défense professionnelle visés à l'article L. 331-1 et par les sociétés mentionnées au titre II du présent livre. Ces agents sont agréés par le ministre chargé de la culture dans les conditions prévues par un décret en Conseil d'Etat.

Article L.331-5

Les mesures techniques efficaces destinées à empêcher ou à limiter les utilisations non autorisées par les titulaires d'un droit d'auteur ou d'un droit voisin du droit d'auteur d'une œuvre, autre qu'un logiciel, d'une interprétation, d'un phonogramme, d'un vidéogramme ou d'un programme sont protégées dans les conditions prévues au présent titre.

On entend par mesure technique au sens du premier alinéa toute technologie, dispositif, composant qui, dans le cadre normal de son fonctionnement, accomplit la fonction prévue par cet alinéa. Ces mesures techniques sont réputées efficaces lorsqu'une utilisation visée au même alinéa est contrôlée par les titulaires de droits grâce à l'application d'un code d'accès, d'un procédé de protection tel que le cryptage, le brouillage ou toute autre transformation de l'objet de la protection ou d'un mécanisme de contrôle de la copie qui atteint cet objectif de protection.

Un protocole, un format, une méthode de cryptage, de brouillage ou de transformation ne constitue pas en tant que tel une mesure technique au sens du présent article.

Les mesures techniques ne doivent pas avoir pour effet d'empêcher la mise en oeuvre effective de l'interopérabilité, dans le respect du droit d'auteur. Les fournisseurs de mesures techniques donnent l'accès aux informations essentielles à l'interopérabilité dans les conditions définies au 1° de l'article L. 331-31 et à l'article L. 331-32.

L.331-32 festgelegten Bedingungen wesentliche Informationen für die Interoperabilität zugänglich.

Die Bestimmungen dieses Kapitels stellen den Rechtsschutz nicht in Frage, der in den Artikeln 79-1 bis 79-6 und im Artikel 95 des Gesetzes Nr. 86-1067 vom 30. September 1986 über die Kommunikationsfreiheit verankert ist.

Die technischen Maßnahmen dürfen der freien Nutzung des Werkes oder Schutzgegenstandes im Rahmen der in diesem Gesetzbuch genannten Rechte sowie im Rahmen jener Rechte, die unter den Rechtsinhabern vereinbart wurden, nicht entgegenstehen.

Die Bestimmungen dieses Artikels gelten unbeschadet der Bestimmungen des Artikels L.122-6-1 dieses Gesetzbuches.

Artikel L.331-12

Die Hohe Behörde für die Verbreitung von Werken und den Schutz von Rechten im Internet ist eine öffentliche unabhängige Behörde. Demnach besitzt sie Rechtspersönlichkeit.

Artikel L.331-13

Die Hohe Behörde stellt folgende Aufgaben sicher:

1. Unterstützung der Förderung des legalen Angebots und Beobachtung der erlaubten und unerlaubten Nutzung von Werken und Gegenständen, für die ein Urheberrecht oder ein verwandtes Schutzrecht in den elektronischen Kommunikationsnetzen, die für die Erbringung von öffentlichen Online-Kommunikationsdiensten benutzt werden, existiert;
2. Schutz dieser Werke und Gegenstände gegen Verletzungen dieser Rechte, die in den elektronischen Kommunikationsnetzen, die für die Erbringung von öffentlichen Online-Kommunikationsdiensten benutzt werden, begangen werden;
3. Regulierung und Überwachung im Bereich der technischen Schutz- und Identifizierungsmaßnahmen für Werke und Gegenstände, die durch ein Urheberrecht bzw. durch ein verwandtes Schutzrecht ge-

Les dispositions du présent chapitre ne remettent pas en cause la protection juridique résultant des articles 79-1 à 79-6 et de l'article 95 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

Les mesures techniques ne peuvent s'opposer au libre usage de l'oeuvre ou de l'objet protégé dans les limites des droits prévus par le présent code, ainsi que de ceux accordés par les détenteurs de droits.

Les dispositions du présent article s'appliquent sans préjudice des dispositions de l'article L. 122-6-1 du présent code.

Article L.331-12

La Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet est une autorité publique indépendante. A ce titre, elle est dotée de la personnalité morale.

Article L.331-13

La Haute Autorité assure :

- 1° Une mission d'encouragement au développement de l'offre légale et d'observation de l'utilisation licite et illicite des œuvres et des objets auxquels est attaché un droit d'auteur ou un droit voisin sur les réseaux de communications électroniques utilisés pour la fourniture de services de communication au public en ligne ;
- 2° Une mission de protection de ces œuvres et objets à l'égard des atteintes à ces droits commises sur les réseaux de communications électroniques utilisés pour la fourniture de services de communication au public en ligne ;
- 3° Une mission de régulation et de veille dans le domaine des mesures techniques de protection et d'identification des œuvres et des objets protégés par un droit d'auteur ou par un droit voisin.

Au titre de ces missions, la Haute Autorité peut recommander toute modification légi-

schützt sind.

Im Rahmen dieser Aufgaben kann die Hohe Behörde alle Änderungen von Gesetzen und Vorschriften empfehlen. Sie kann von der Regierung über jeden Gesetz- oder Dekretentwurf konsultiert werden, der für den Schutz der Urheberrechte an Werken der Literatur und Kunst von Bedeutung ist. Desgleichen kann sie von der Regierung oder von den Parlamentsausschüssen zu Fragen, die in ihrem Zuständigkeitsbereich fallen, konsultiert werden.

Artikel L.331-15

Die Hohe Behörde besteht aus einem Kollegium und aus einer Rechtsschutzkommission. Den Vorsitz des Kollegiums hat der Präsident der Hohen Behörde inne.

Die der Hohen Behörde anvertrauten Aufgaben führt das Kollegium aus, soweit die Gesetzgebung nicht anders bestimmt.

Bei der Erfüllung ihrer Aufgaben erhalten die Mitglieder des Kollegiums und der Rechtsschutzkommission keine Anweisungen von anderen Behörden.

Artikel L.331-21

Für die Erfüllung der Aufgaben durch die Rechtsschutzkommission verfügt die Hohe Behörde über vereidigte öffentliche Bedienstete, die von der Hohen Behörde nach den in einem Staatsratserlass festgelegten Bedingungen ermächtigt sind. Diese Ermächtigung entbindet nicht von der Anwendung der Bestimmungen, in denen die Verfahren festgelegt sind, die den Zugang zu gesetzlich geschützten Geheimnissen erlauben.

Die Mitglieder der Rechtsschutzkommission und die im ersten Absatz genannten Bedienstete erhalten die Anrufungen, die an diese Kommission nach den in Artikel L.331-24 festgelegten Bedingungen gerichtet sind. Sie untersuchen den Sachverhalt [Bestimmungen durch Beschluss des Verfassungsrates Nr. 2009-580 DC vom 10. Juni 2009 als nicht verfassungskonform erklärt].

Sie können sich unabhängig vom Datenträger alle für das Verfahren erforderliche Dokumente beschaffen, einschließlich der vom Betreiber im Bereich der elektroni-

slative ou réglementaire. Elle peut être consultée par le Gouvernement sur tout projet de loi ou de décret intéressant la protection des droits de propriété littéraire et artistique. Elle peut également être consultée par le Gouvernement ou par les commissions parlementaires sur toute question relative à ses domaines de compétence.

Article L.331-15

La Haute Autorité est composée d'un collège et d'une commission de protection des droits. Le président du collège est le président de la Haute Autorité.

Sauf disposition législative contraire, les missions confiées à la Haute Autorité sont exercées par le collège.

Dans l'exercice de leurs attributions, les membres du collège et de la commission de protection des droits ne reçoivent d'instruction d'aucune autorité.

Article L.331-21

Pour l'exercice, par la commission de protection des droits, de ses attributions, la Haute Autorité dispose d'agents publics assermentés habilités par le président de la Haute Autorité dans des conditions fixées par un décret en Conseil d'Etat. Cette habilitation ne dispense pas de l'application des dispositions définissant les procédures autorisant l'accès aux secrets protégés par la loi.

Les membres de la commission de protection des droits et les agents mentionnés au premier alinéa reçoivent les saisines adressées à ladite commission dans les conditions prévues à l'article L. 331-24. Ils procèdent à l'examen des faits [Dispositions déclarées non conformes à la Constitution par la décision du Conseil constitutionnel n° 2009-580 DC du 10 juin 2009].

Ils peuvent, pour les nécessités de la procédure, obtenir tous documents, quel qu'en soit le support, y compris les données conservées et traitées par les opérateurs de communications électroniques en application de l'article L. 34-1 du code des postes

schen Kommunikation in Anwendung des Artikels L.34-1 des französischen Gesetzbuches über das Postwesen und elektronische Medien gespeicherten oder verarbeiteten Daten sowie die Daten der Dienstleister die unter I.-1 und 2 des Artikels 6 des Gesetzes Nr. 2004-575 vom 21. Juni 2004 über das Vertrauens in die digitale Wirtschaft genannt sind.

Sie können sich auch Kopien der im vorigen Absatz genannten Dokumente beschaffen. Sie können sich insbesondere von den Betreibern im Bereich der elektronischen Kommunikation die Identität, die Postanschrift, die elektronische Adresse und die Telefondaten des Internetteilnehmers beschaffen, dessen Zugang zu öffentlichen Online-Kommunikationsdiensten benutzt wurde zum Zwecke der Vervielfältigung, Darbietung, Bereitstellung oder öffentliche Wiedergabe von Werken oder sonstigen geschützten Werken ohne dabei über die Genehmigung der Rechtsinhaber gemäß den Büchern I und II zu verfügen, wenn eine solche vorgeschrieben ist.

Artikel L.331-21-1

Die Mitglieder der Rechtsschutzkommission sowie die befugten und von der in Artikel L.331-21 genannten Justizbehörde vereidigten Bediensteten dürfen Tatsachen feststellen, die Verstöße gemäß diesem Titel darstellen können, wenn die Verstöße mit der zusätzlichen Strafe der Zugangssperre zu einem öffentlichen Online-Kommunikationsdienst gemäß Artikel L.335-7 und L.335-7-1 geahndet wird.

Sie dürfen außerdem Äußerungen der betreffenden Personen einholen. Im Einladungsschreiben wird auf dieses Recht hingewiesen.

Verlangen die betreffenden Personen angehört zu werden, werden sie eingeladen und angehört. Jede Person hat bei der Anhörung das Recht auf einen Beistand ihrer Wahl.

Der betreffenden Person wird eine Abschrift des Vernehmungsprotokolls ausgehändigt.

et des communications électroniques et les prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

Ils peuvent également obtenir copie des documents mentionnés à l'alinéa précédent.

Ils peuvent, notamment, obtenir des opérateurs de communications électroniques l'identité, l'adresse postale, l'adresse électronique et les coordonnées téléphoniques de l'abonné dont l'accès à des services de communication au public en ligne a été utilisé à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise.

Article L.331-21-1

Les membres de la commission de protection des droits, ainsi que ses agents habilités et assermentés devant l'autorité judiciaire mentionnés à l'article L. 331-21, peuvent constater les faits susceptibles de constituer des infractions prévues au présent titre lorsqu'elles sont punies de la peine complémentaire de suspension de l'accès à un service de communication au public en ligne mentionnée aux articles L. 335-7 et L. 335-7-1.

Ils peuvent en outre recueillir les observations des personnes concernées. Il est fait mention de ce droit dans la lettre de convocation.

Lorsque les personnes concernées demandent à être entendues, ils les convoquent et les entendent. Toute personne entendue a le droit de se faire assister d'un conseil de son choix.

Une copie du procès-verbal d'audition est remise à la personne concernée.

Artikel L.331-24

Die Rechtsschutzkommission handelt auf Anrufung der unter den in Artikel L.331-2 genannten Bedingungen vereidigten und zugelassenen Bediensteten, die von folgenden Einrichtungen bestellt werden:

- ordnungsgemäß gegründete Berufsverbände zum Schutz von Urheberrechten;
- Verwertungsgesellschaften;
- Centre national de la cinématographie (staatl. franz. Filmförderungsbehörde)

Die Rechtsschutzkommission kann auch aufgrund von Informationen handeln, die ihm vom Oberstaatsanwalt übermittelt werden.

Die Kommission darf nicht für Fälle, die länger als sechs Monate zurückliegen, angerufen werden.

Artikel L.331-25

Wird die Rechtsschutzkommission wegen Tatsachen angerufen, die eine Nichterfüllung der in Artikel L.336-3 genannten Pflicht darstellen können, kann die Kommission dem Internetteilnehmer auf seine Kosten auf elektronischem Weg und durch die Person, deren Tätigkeit das Anbieten eines Zugangs zu öffentlichen Online-Kommunikationsdiensten ist, und die mit dem Internetteilnehmer einen Vertrag abgeschlossen hat, ein Schreiben zukommen lassen, in dem der Internetteilnehmer auf die Bestimmungen des Artikels L.336-3 hingewiesen und aufgefordert wird, die in diesen Bestimmungen genannte Pflicht einzuhalten, und zudem wird der Internetteilnehmer über die in Artikel L.335-7 und L.335-7-1 angedrohten Strafmaßnahmen in Kenntnis gesetzt. Dieses Schreiben enthält auch eine Information an den Internetteilnehmer über das legale Angebot an kulturellen Online-Inhalten, über bestehende Sicherungsmaßnahmen, die die Vermeidung der Nichterfüllung der in Artikel L.336-3 genannten Pflicht ermöglicht, sowie über die Gefahren, die Handlungen für die Erneuerung des künstlerischen Schaffens und für die Wirtschaft des kulturellen Sektors bergen, bei denen das Urheberrecht und verwandte Schutzrechte nicht eingehalten werden.

Liegen nach einem Zeitraum von sechs

Article L.331-24

La commission de protection des droits agit sur saisine d'agents assermentés et agréés dans les conditions définies à l'article L. 331-2 qui sont désignés par :

- les organismes de défense professionnelle régulièrement constitués ;
- les sociétés de perception et de répartition des droits ;
- le Centre national de la cinématographie.

La commission de protection des droits peut également agir sur la base d'informations qui lui sont transmises par le procureur de la République.

Elle ne peut être saisie de faits remontant à plus de six mois.

Article L.331-25

Lorsqu'elle est saisie de faits susceptibles de constituer un manquement à l'obligation définie à l'article L. 336-3, la commission de protection des droits peut envoyer à l'abonné, sous son timbre et pour son compte, par la voie électronique et par l'intermédiaire de la personne dont l'activité est d'offrir un accès à des services de communication au public en ligne ayant conclu un contrat avec l'abonné, une recommandation lui rappelant les dispositions de l'article L. 336-3, lui enjoignant de respecter l'obligation qu'elles définissent et l'avertissant des sanctions encourues en application des articles L. 335-7 et L. 335-7-1. Cette recommandation contient également une information de l'abonné sur l'offre légale de contenus culturels en ligne, sur l'existence de moyens de sécurisation permettant de prévenir les manquements à l'obligation définie à l'article L. 336-3 ainsi que sur les dangers pour le renouvellement de la création artistique et pour l'économie du secteur culturel des pratiques ne respectant pas le droit d'auteur et les droits voisins.

En cas de renouvellement, dans un délai de six mois à compter de l'envoi de la recommandation visée au premier alinéa, de faits susceptibles de constituer un manquement à l'obligation définie à l'article L. 336-3, la commission peut adresser une nouvelle recommandation comportant les mêmes

Monaten nach Versendung des im ersten Absatz genannten Schreibens die Tatsachen wieder vor, die eine Nichterfüllung der in Artikel L.336-3 genannten Pflicht darstellen, kann die Kommission erneut ein Schreiben auf elektronischem Wege und unter den im ersten Absatz genannten Bedingungen versenden, in dem die gleichen Informationen enthalten sind, wie im ersten Schreiben. Dieses Schreiben ist zusammen mit einem Einschreiben zuzustellen oder mit jedem anderen Mittel, das geeignet ist, das Zustellungsdatum dieses Schreibens nachzuweisen.

In den aufgrund dieses Artikels verschickten Schreiben werden das festgestellte Datum und die festgestellte Uhrzeit des Sachverhalts angezeigt, das eine Nichterfüllung der in Artikel L.336-3 genannten Pflicht darstellen kann. Diese Schreiben geben allerdings den Inhalt der von dieser Nichterfüllung betroffenen Werke oder Schutzgegenstände nicht bekannt. Angegeben werden die Telefondaten, die Postanschrift und die elektronische Adresse, an die der Empfänger, falls er es wünscht, seine Stellungnahme gegenüber der Rechtsschutzkommission richten kann und wo der Empfänger, sofern er es ausdrücklich beantragt, genaue Angaben über den Inhalt der Werke oder Schutzgegenstände, die die ihm zur Last gelegte Verfehlung betreffen, erhalten kann.

Artikel L.331-29

Die Hohe Behörde ist befugt, eine automatische Verarbeitung von personenbezogenen Daten für Personen durchzuführen, die im Sinne dieses Unterabschnitts Gegenstand eines Verfahrens sind.

Zweck dieser Datenverarbeitung ist die Umsetzung der in diesem Unterabschnitt genannten Maßnahmen durch die Rechtsschutzkommission sowie die Durchführung aller damit verbundenen Prozesshandlungen und die Umsetzung der Modalitäten der Unterrichtung der Berufsverbände zum Schutz von Urheberrechten und der Verwertungsgesellschaften über eventuelle Anrufungen der Justizbehörde sowie die Durchführung der Zustellungen gemäß Absatz 5 des Artikels L.335-7.

informations que la précédente par la voie électronique dans les conditions prévues au premier alinéa. Elle doit assortir cette recommandation d'une lettre remise contre signature ou de tout autre moyen propre à établir la preuve de la date de présentation de cette recommandation.

Les recommandations adressées sur le fondement du présent article mentionnent la date et l'heure auxquelles les faits susceptibles de constituer un manquement à l'obligation définie à l'article L. 336-3 ont été constatés. En revanche, elles ne divulguent pas le contenu des œuvres ou objets protégés concernés par ce manquement. Elles indiquent les coordonnées téléphoniques, postales et électroniques où leur destinataire peut adresser, s'il le souhaite, des observations à la commission de protection des droits et obtenir, s'il en formule la demande expresse, des précisions sur le contenu des œuvres ou objets protégés concernés par le manquement qui lui est reproché.

Article L.331-29

Est autorisée la création, par la Haute Autorité, d'un traitement automatisé de données à caractère personnel portant sur les personnes faisant l'objet d'une procédure dans le cadre de la présente sous-section.

Ce traitement a pour finalité la mise en œuvre, par la commission de protection des droits, des mesures prévues à la présente sous-section, de tous les actes de procédure afférents et des modalités de l'information des organismes de défense professionnelle et des sociétés de perception et de répartition des droits des éventuelles saisines de l'autorité judiciaire ainsi que des notifications prévues au cinquième alinéa de l'article L. 335-7.

Un décret en Conseil d'Etat, pris après avis

Ein Erlass des Staatsrats legt nach Stellungnahme der nationalen Kommission für Informatik und Freiheiten die Durchführungsbestimmungen zu diesem Artikels fest. Insbesondere wird Folgendes festgelegt:

- die Kategorien der gespeicherten Daten und wie lange die Daten gespeichert bleiben;
- die Empfänger, die berechtigt sind, diese Daten zu erhalten, insbesondere die Personen, deren Tätigkeit das Anbieten eines Zugangs zu öffentlichen Online-Kommunikationsdiensten ist;
- die Bedingungen, unter denen die betreffenden Personen bei der Hohen Behörde ihr Recht auf Zugang zu den Daten, die sie betreffen, ausüben können gemäß Gesetz Nr. 78-17 vom 6. Januar 1978 über Informatik, Dateien und Freiheiten.

Artikel L.335-2

Jede Herausgabe von Schriften, Musikkompositionen, Zeichnungen, Bildern aller Art oder sonstigen Produktionen, ganz oder teilweise gedruckt bzw. gebrannt, unter Missachtung der Gesetze und Vorschriften über das Eigentum von Urhebern stellt eine Raubkopie dar und jede Raubkopie ist eine Straftat.

Die Raubkopie von in Frankreich oder im Ausland veröffentlichten Werken wird in Frankreich mit einer Gefängnisstrafe von drei Jahren und einer Geldstrafe in Höhe von 300.000 Euro geahndet.

Mit dem gleichen Strafmaß werden der Verkauf, der Ex- und Import von gefälschten Werken geahndet.

Werden die hier genannten Straftaten durch eine organisierte Bande begangen, beträgt das Strafmaß fünf Jahre Haft und 500.000 Euro Geldstrafe.

Artikel L.335-7

Wird der Verstoß über einen öffentlichen Online-Kommunikationsdienst begangen, können die nach Maßgabe der Artikel L.335-2, L.335-3 und L.335-4 schuldigen Personen zudem zu einer zusätzlichen Strafe in Form einer Zugangssperre zu einem öffentlichen Online-Kommunikationsdienst für die Höchstdauer von einem Jahr verur-

de la Commission nationale de l'informatique et des libertés, fixe les modalités d'application du présent article. Il précise notamment :

- les catégories de données enregistrées et leur durée de conservation ;
- les destinataires habilités à recevoir communication de ces données, notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne ;
- les conditions dans lesquelles les personnes intéressées peuvent exercer, auprès de la Haute Autorité, leur droit d'accès aux données les concernant conformément à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Article L.335-2

Toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production, imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon et toute contrefaçon est un délit.

La contrefaçon en France d'ouvrages publiés en France ou à l'étranger est punie de trois ans d'emprisonnement et de 300 000 euros d'amende.

Seront punis des mêmes peines le débit, l'exportation et l'importation des ouvrages contrefaisants.

Lorsque les délits prévus par le présent article ont été commis en bande organisée, les peines sont portées à cinq ans d'emprisonnement et à 500 000 euros d'amende.

Article L.335-7

Lorsque l'infraction est commise au moyen d'un service de communication au public en ligne, les personnes coupables des infractions prévues aux articles L. 335-2, L. 335-3 et L. 335-4 peuvent en outre être condamnées à la peine complémentaire de suspension de l'accès à un service de communication au public en ligne pour une

teilt werden, wobei es diesen Personen während dieses Zeitraums verboten ist, einen Vertrag mit einem Betreiber einer Dienstleistung der gleichen Art abzuschließen.

Wird diese Dienstleistung im Rahmen von kombinierten Geschäftsangeboten erworben, die weitere Arten von Dienstleistungen umfassen, wie Telefon- und Fernsehdienste, gelten die Beschlüsse über die Sperrung nicht für diese Dienste.

Die Zugangssperre selbst hat keinen Einfluss auf die Bezahlung des Preises für die Dienstleistung an den Dienstleister. Artikel L.121-84 des französischen Verbraucherschutzgesetzes ist während der Sperrzeit nicht anwendbar.

Die Kosten aufgrund einer eventuellen Kündigung des Nutzervertrags während der Sperrzeit trägt der Internetteilnehmer.

Ist der Beschluss vollstreckbar, wird die Hohe Behörde für die Verbreitung von Werken und den Schutz von Rechten im Internet über die in diesem Artikel genannte zusätzliche Strafe in Kenntnis gesetzt, die ihrerseits den Beschluss der Person zustellt, deren Tätigkeit das Anbieten eines Zugangs zu öffentlichen Online-Kommunikationsdiensten ist, damit die Person bis spätestens fünfzehn Tage nach der Zustellung die Zugangssperre für den betreffenden Internetteilnehmer einrichten kann.

Die Tatsache, dass die Person, deren Tätigkeit das Anbieten eines Zugangs zu öffentlichen Online-Kommunikationsdiensten ist, die Zugangssperre, über die sie informiert wurde, nicht durchführt, wird mit einer Strafe von 5.000 Euro geahndet.

Punkt 3 des Artikels 777 der französischen Strafprozessordnung ist auf die in diesem Artikel genannte zusätzliche Strafe nicht anwendbar.

Artikel L.335-7-1

Bei Übertretungen der fünften Kategorie, gemäß diesem Gesetzbuch, und wenn die Regelung dies vorsieht, kann die in Artikel L. 335-7 genannte zusätzliche Strafe nach den gleichen Modalitäten bei grober Fahrlässigkeit gegen den Inhaber des Zugangs zu einem öffentlichen Online-

durée maximale d'un an, assortie de l'interdiction de souscrire pendant la même période un autre contrat portant sur un service de même nature auprès de tout opérateur.

Lorsque ce service est acheté selon des offres commerciales composites incluant d'autres types de services, tels que services de téléphonie ou de télévision, les décisions de suspension ne s'appliquent pas à ces services.

La suspension de l'accès n'affecte pas, par elle-même, le versement du prix de l'abonnement au fournisseur du service. L'article L. 121-84 du code de la consommation n'est pas applicable au cours de la période de suspension.

Les frais d'une éventuelle résiliation de l'abonnement au cours de la période de suspension sont supportés par l'abonné.

Lorsque la décision est exécutoire, la peine complémentaire prévue au présent article est portée à la connaissance de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet, qui la notifie à la personne dont l'activité est d'offrir un accès à des services de communication au public en ligne afin qu'elle mette en œuvre, dans un délai de quinze jours au plus à compter de la notification, la suspension à l'égard de l'abonné concerné.

Le fait, pour la personne dont l'activité est d'offrir un accès à des services de communication au public en ligne, de ne pas mettre en œuvre la peine de suspension qui lui a été notifiée est puni d'une amende maximale de 5 000 €.

Le 3° de l'article 777 du code de procédure pénale n'est pas applicable à la peine complémentaire prévue par le présent article.

Article L.335-7-1

Pour les contraventions de la cinquième classe prévues par le présent code, lorsque le règlement le prévoit, la peine complémentaire définie à l'article L. 335-7 peut être prononcée selon les mêmes modalités, en cas de négligence caractérisée, à l'encontre du titulaire de l'accès à un service de com-

Kommunikationsdienst verhängt werden, dem die Rechtsschutzkommission in Anwendung des Artikels L.331-25 vorab ein Einschreiben oder ein anderes Mittel, das geeignet ist, das Zustellungsdatum nachzuweisen, zugestellt hat, und damit den Inhaber aufgefordert hat, eine Maßnahme zur Sicherung seines Zugangs zum Internet durchzuführen.

Die grobe Fahrlässigkeit wird anhand der begangenen Tatsachen spätestens ein Jahr nach Zustellung des in vorigem Absatz genannten Schreibens festgestellt.

In diesem Fall beträgt die Höchstdauer für die Sperre einen Monat.

Die Tatsache, dass die Person, gegenüber der die in diesem Artikel genannte zusätzliche Strafe verhängt wurde, das Verbot missachtet, mit einem anderen Anbieter einen Nutzungsvertrag für einen öffentlichen Online-Kommunikationsdienst während der Zugangssperre abzuschließen, wird mit einer Geldstrafe in Höhe von maximal 3.750 Euro geahndet.

Artikel L.336-3

Der Inhaber eines Zugangs zu öffentlichen Online-Kommunikationsdiensten hat die Pflicht, dafür Sorge zu tragen, dass dieser Zugang nicht dazu benutzt wird, um Vielfältigungen, Darbietungen, Bereitstellungen oder öffentliche Wiedergaben von Werken oder sonstigen urheberrechtlich oder anders geschützten Gegenständen zu tätigen, ohne dabei über die Genehmigung der Rechtsinhaber gemäß den Büchern I und II, sofern eine Genehmigung vorgeschrieben ist, zu verfügen.

Die Nichterfüllung durch den Inhaber des Zugangs der im ersten Absatz genannten Pflicht führt nicht zur strafrechtlichen Haftbarmachung des Betreffenden, vorbehaltlich der Artikel L.335-7 und L.335-7-1.

Artikel R331-35

Für die Zulässigkeit der an die Rechtsschutzkommission der Hohen Behörde gerichteten Anrufungen durch Berufsverbände, Verwertungsgesellschaften und durch die Filmförderungsbehörde ist es erforderlich, dass die Anrufungen unter den in Artikel L.331-24 genannten Bedingungen Fol-

munication au public en ligne auquel la commission de protection des droits, en application de l'article L. 331-25, a préalablement adressé, par voie d'une lettre remise contre signature ou de tout autre moyen propre à établir la preuve de la date de présentation, une recommandation l'invitant à mettre en œuvre un moyen de sécurisation de son accès à internet.

La négligence caractérisée s'apprécie sur la base des faits commis au plus tard un an après la présentation de la recommandation mentionnée à l'alinéa précédent.

Dans ce cas, la durée maximale de la suspension est d'un mois.

Le fait pour la personne condamnée à la peine complémentaire prévue par le présent article de ne pas respecter l'interdiction de souscrire un autre contrat d'abonnement à un service de communication au public en ligne pendant la durée de la suspension est puni d'une amende d'un montant maximal de 3 750 €.

Article L.336-3

La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise.

Le manquement de la personne titulaire de l'accès à l'obligation définie au premier alinéa n'a pas pour effet d'engager la responsabilité pénale de l'intéressé, sous réserve des articles L. 335-7 et L. 335-7-1.

Article R.331-35

Pour être recevables, les saisines adressées à la commission de protection des droits de la Haute Autorité par les organismes de défense professionnelle régulièrement constitués, les sociétés de perception et de répartition des droits et le Centre national du cinéma et de l'image animée dans les

gendes enthalten:

1. Die personenbezogenen Daten und die Informationen, die unter 1. im Anhang des Erlasses Nr.2010-236 vom 5. März 2010 über die automatische Verarbeitung von personenbezogenen Daten genannt werden, genehmigt durch den Artikel L.331-29 des Urheberrechtsgesetzbuchs bezeichnet als „Verwaltungssystem für Maßnahmen zum Schutz von Werken im Internet“;
2. Eine eidesstattliche Erklärung darüber, dass der Urheber der Anrufung berechtigt ist, im Namen des Inhabers der Rechte am Werk oder an dem Schutzgegenstand, das vom Sachverhalt betroffen ist, zu handeln. Nach Erhalt der Anrufung erteilt die Rechtsschutzkommission eine elektronische Empfangsbestätigung.

Artikel R.331-37

Die in Artikel L.34-1 des französischen Gesetzbuches über das Postwesen und elektronische Medien genannten Betreiber im Bereich der elektronischen Kommunikation sowie die unter I-1 und 2 des Artikels 6 des Gesetzes Nr. 2004-575 vom 21. Juni 2004 über das Vertrauen in die digitale Wirtschaft genannten Dienstleister sind gehalten, die personenbezogenen Daten und die Informationen, die unter 2. im Anhang des Dekrets Nr.2010-236 vom 5. März 2010 genannt werden, innerhalb einer Frist von acht Tagen nach Erhalt der für die Identifizierung des Internetteilnehmers erforderlichen technischen Angaben durch die Rechtsschutzkommission mitzuteilen, wenn der Zugang des Internetteilnehmers zu öffentlichen Online-Kommunikationsdiensten dazu benutzt wurde, um Vervielfältigungen, Darbietungen, Bereitstellungen oder öffentliche Wiedergaben von Werken oder sonstigen Schutzgegenständen zu tätigen, ohne dabei über die Genehmigung der Rechtsinhaber gemäß den Büchern I und II, sofern eine Genehmigung vorgeschrieben ist, zu verfügen.

Die Betreiber und Dienstleister sind auch gehalten, innerhalb von einer Frist von fünfzehn Tagen nach Aufforderung durch die Rechtsschutzkommission die Unterlagen und Kopien von Unterlagen beizubrin-

conditions prévues à l'article L. 331-24 doivent comporter :

1° Les données à caractère personnel et les informations mentionnées au 1° de l'annexe du décret n° 2010-236 du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé " Système de gestion des mesures pour la protection des œuvres sur internet " ;

2° Une déclaration sur l'honneur selon laquelle l'auteur de la saisine a qualité pour agir au nom du titulaire de droits sur l'œuvre ou l'objet protégé concerné par les faits.

Dès réception de la saisine, la commission de protection des droits en accuse réception par voie électronique.

Article R.331-37

Les opérateurs de communications électroniques mentionnés à l'article L. 34-1 du code des postes et des communications électroniques et les prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique sont tenus de communiquer les données à caractère personnel et les informations mentionnées au 2° de l'annexe du décret n° 2010-236 du 5 mars 2010 dans un délai de huit jours suivant la transmission par la commission de protection des droits des données techniques nécessaires à l'identification de l'abonné dont l'accès à des services de communication au public en ligne a été utilisé à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise.

Ces opérateurs et prestataires sont également tenus de fournir les documents et les copies des documents mentionnés aux troisième et quatrième alinéas de l'article L. 331-21 dans un délai de quinze jours suivant la demande qui leur en est faite par la commission de protection des droits.

Les opérateurs sont tenus d'adresser par voie électronique à l'abonné chacune des

gen, die im dritten und vierten Absatz des Artikels L.331-21 genannt werden.

Die Betreiber sind gehalten, dem Internetteilnehmer auf elektronischen Wege alle im ersten bzw. zweiten Absatz des Artikels L.331-25 genannten Schreiben innerhalb von vierundzwanzig Stunden nach der Übertragung durch die Rechtsschutzkommission zukommen zu lassen.

Artikel R.331-38

Der Verstoß gegen die Bestimmungen des Artikels R.331-37 wird mit der für Übertretungen der fünften Kategorie vorgesehenen Geldstrafe geahndet.

Im Fall der Wiederholung eines der in diesem Artikel genannten Rechtsverstöße wird nach Maßgabe der Artikel 132-11 und 132-15 des Strafgesetzbuchs bestraft.

Artikel R.331-40

Wird nach einer Frist von einem Jahr nach Zustellung des im ersten Absatz des Artikels L.335-7-1 genannten Schreibens die Rechtsschutzkommission erneut wegen Tatsachen angerufen, die eine grobe Fahrlässigkeit nach Artikel R.335-5 darstellen können, teilt die Kommission dem Internetteilnehmer durch ein Einschreiben mit, dass diese Tatsachen strafrechtlich verfolgt werden können. Dieses Schreiben fordert die betreffende Person auf, innerhalb von fünfzehn Tagen Stellung zu nehmen. Weiterhin wird angegeben, dass die Person innerhalb der gleichen Frist gemäß Artikel L.331-21 eine Anhörung beantragen kann und, dass sie das Recht auf einen Beistand hat. Im Schreiben wird die Person auch aufgefordert, ihre finanzielle Belastung durch die Familie und ihre Einnahmen anzugeben.

Die Kommission kann aus eigener Initiative die betreffende Person zur Anhörung laden. Im Einladungsschreiben wird darauf hingewiesen, dass ein Recht auf Beistand besteht.

Artikel R.331-43

Die Entscheidung der Kommission, mit der festgestellt wird, dass der Sachverhalt eine Gesetzesübertretung darstellen kann, wird dem Oberstaatsanwalt beim zuständigen Landgericht zusammen je nach Fall mit ei-

recommandations mentionnées respectivement au premier et au deuxième alinéa de l'article L. 331-25, dans un délai de vingt-quatre heures suivant sa transmission par la commission de protection des droits.

Article R.331-38

Est puni de l'amende prévue pour les contraventions de cinquième classe le fait de contrevenir aux dispositions de l'article R. 331-37.

La récidive des contraventions prévues au présent article est réprimée conformément aux articles 132-11 et 132-15 du code pénal.

Article R.331-40

Lorsque, dans le délai d'un an suivant la présentation de la recommandation mentionnée au premier alinéa de l'article L. 335-7-1, la commission de protection des droits est saisie de nouveaux faits susceptibles de constituer une négligence caractérisée définie à l'article R. 335-5, elle informe l'abonné, par lettre remise contre signature, que ces faits sont susceptibles de poursuite. Cette lettre invite l'intéressé à présenter ses observations dans un délai de quinze jours. Elle précise qu'il peut, dans le même délai, solliciter une audition en application de l'article L. 331-21-1 et qu'il a droit de se faire assister par un conseil. Elle l'invite également à préciser ses charges de famille et ses ressources.

La commission peut de sa propre initiative convoquer l'intéressé aux fins d'audition. La lettre de convocation précise qu'il a droit de se faire assister par un conseil.

Article R.331-43

La délibération de la commission constatant que les faits sont susceptibles de constituer une infraction, à laquelle sont joints, selon les cas, un procès-verbal récapitulatif de l'ensemble des faits et procédure ainsi

nem Protokoll, das alle Tatsachen und das Verfahren zusammenfasst sowie mit allen zweckdienlichen Schriftstücken übermittelt. Die Rechtsschutzkommission informiert die Urheber der Anrufungen, die der Kommission unter den in Artikel L.331-24 genannten Bedingungen zugeschickt wurden, über die Weiterleitung des Verfahrens an den Oberstaatsanwalt.

Artikel R.335-5

I. Eine grobe Fahrlässigkeit, die mit der für Übertretungen der fünften Kategorie vorgesehenen Geldstrafe geahndet wird, liegt vor, wenn für den Inhaber eines Zugangs zu öffentlichen Online-Kommunikationsdiensten ohne berechtigten Grund folgender Tatbestand besteht, sofern die Voraussetzungen unter II erfüllt sind:

1. Der Inhaber hat für diesen Zugang keine Maßnahme zu Sicherung getroffen;
2. Der Inhaber hat bei der Durchführung dieser Maßnahme keine Sorgfalt walten lassen.

II. Die Bestimmungen unter I gelten nur, wenn die beiden nachfolgenden Voraussetzungen erfüllt sind:

1. Dem Inhaber des Zugangs wurde in Anwendung des Artikels L.331-25 und in den Formen, die dieser Artikel vorsieht, durch die Rechtsschutzkommission empfohlen, seinen Zugang derart zu schützen, dass bei einer erneuten Nutzung des Zugangs keine Vervielfältigungen, Darbietungen, Bereitstellungen oder öffentliche Wiedergaben von Werken oder sonstigen urheberrechtlich oder anders geschützten Gegenständen getätigt werden können, ohne dabei über die Genehmigung der Rechtsinhaber gemäß den Büchern I und II, sofern eine Genehmigung vorgeschrieben ist, zu verfügen;

2. Im Verlauf des Jahres nach der Zustellung dieser Empfehlung wurde dieser Zugang erneut für die unter II.1. genannten Zwecke benutzt.

III. Die Personen, die sich gemäß Punkt I strafbar gemacht haben, können gemäß den Bestimmungen des Artikels L.335-7-1 zudem zu einer zusätzlichen Strafe in Form einer Zugangssperre zu einem öffentlichen

que toutes pièces utiles, est transmise au procureur de la République près le tribunal de grande instance compétent.

La commission de protection des droits avise les auteurs des saisines qui lui ont été adressées dans les conditions prévues à l'article L. 331-24 de la transmission de la procédure au procureur de la République.

Article R.335-5

I.-Constitue une négligence caractérisée, punie de l'amende prévue pour les contraventions de la cinquième classe, le fait, sans motif légitime, pour la personne titulaire d'un accès à des services de communication au public en ligne, lorsque se trouvent réunies les conditions prévues au II :

- 1° Soit de ne pas avoir mis en place un moyen de sécurisation de cet accès ;
- 2° Soit d'avoir manqué de diligence dans la mise en œuvre de ce moyen.

II.-Les dispositions du I ne sont applicables que lorsque se trouvent réunies les deux conditions suivantes :

- 1° En application de l'article L. 331-25 et dans les formes prévues par cet article, le titulaire de l'accès s'est vu recommander par la commission de protection des droits de mettre en œuvre un moyen de sécurisation de son accès permettant de prévenir le renouvellement d'une utilisation de celui-ci à des fins de reproduction, de représentation ou de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise ;

- 2° Dans l'année suivant la présentation de cette recommandation, cet accès est à nouveau utilisé aux fins mentionnées au 1° du présent II.

III.-Les personnes coupables de la contravention définie au I peuvent, en outre, être condamnées à la peine complémentaire de suspension de l'accès à un service de communication au public en ligne pour une durée maximale d'un mois, conformément aux dispositions de l'article L. 335-7-1.

Online-Kommunikationsdienst für die
Höchstdauer von einem Jahr verurteilt
werden.

Digital Economy Act 2010

in der Fassung vom 08.04.2010¹⁶²⁹

Auszug

Gesetz über die digitale Wirtschaft 2010

Digital Economy Act 2010

Verletzung von Urheberrechten im Internet

Online infringement of copyright

3 Verpflichtung zur Versendung eines Warnhinweises an den Anschlussinhaber über gemeldete Verstöße gegen das Urheberrecht

3 Obligation to notify subscribers of reported infringements

Im Anschluss an Artikel 124 des Communications Act 2003 einfügen –

After section 124 of the Communications Act 2003 insert—

„Verletzung von Urheberrechten im Internet: Verpflichtungen der Anbieter von Internetdiensten

“Online infringement of copyright: obligations of internet service providers

124A Verpflichtung zur Versendung eines Warnhinweises an den Anschlussinhaber über gemeldete Verstöße gegen das Urheberrecht

124A Obligation to notify subscribers of copyright infringement reports

(1) Die Bestimmungen dieses Abschnitts finden Anwendung wenn ein Inhaber von Urheberrechten der Meinung ist, dass

(1) This section applies if it appears to a copyright owner that—

(a) ein Anschlussinhaber eines Internet-Zugangsdienstes durch die Nutzung dieses Dienstes seine Urheberrechte verletzt hat;

(a) a subscriber to an internet access service has infringed the owner’s copyright by means of the service; or

(b) ein Anschlussinhaber eines Internet-Zugangsdienstes die Nutzung des Dienstes Dritten gestattet hat, die unter Verwendung des Dienstes seine Urheberrechte verletzt haben;

(b) a subscriber to an internet access service has allowed another person to use the service, and that other person has infringed the owner’s copyright by means of the service.

(2) Der Rechteinhaber kann die Verletzung seiner Rechte bei dem Internet-Diensteanbieter, der den Zugang bereitgestellt hat, anzeigen, sofern ein geltendes

(2) The owner may make a copyright infringement report to the internet service provider who provided the internet access service if a code in force under section 124C

¹⁶²⁹ Deutsche Übersetzung im Wesentlichen: tolingo GmbH, 2011.

Regelwerk im Sinne der Abschnitte 124C oder 124D („Initial Obligation Code“) vorliegt, dass dem Rechteinhaber ein solches Recht einräumt.

(3) Eine „Meldung eines Verstoßes gegen das Urheberrecht“ ist eine Meldung,

(a) die besagt, dass offenkundig eine Urheberrechtsverletzung vorliegt;

(b) die eine Beschreibung der offenkundig vorliegenden Verletzung enthält;

(c) die Beweise für die offenkundige Verletzung enthält, aus denen die IP-Adresse des Nutzers hervorgeht sowie der Zeitpunkt, zu dem die Beweise gesichert wurden;

(d) die innerhalb eines Monats nach Sicherung der entsprechenden Beweise an den Anbieter des Internetdienstes geschickt wird; und

(e) die alle anderen Anforderungen des Initial Obligations Code erfüllt.

(4) Erhält ein Internet-Diensteanbieter eine Meldung über einen Verstoß gegen das Urheberrecht, muss er dem betreffenden Anschlussinhaber einen Warnhinweis senden, sofern dies nach dem Initial Obligation Code vorgeschrieben ist.

(5) Dieser Warnhinweis gemäß Punkt (4) muss dem Anschlussinhaber vom Anbieter des Internetdienstes innerhalb eines Monats nach Eingang der Meldung übermittelt werden.

(6) Dieser Warnhinweis gemäß Punkt (4) muss enthalten:

(a) einen Vermerk, dass die Benachrichtigung gemäß diesem Abschnitt und infolge eines gemeldeten Verstoßes gegen das Urheberrecht erfolgt;

(b) den Namen des Rechteinhabers, der den Verstoß gemeldet hat;

(c) eine Beschreibung des offenkundigen Verstoßes;

(d) einen Beweis für den Verstoß, aus dem die IP-Adresse des Anschlussinhabers hervorgeht sowie Informationen dazu, wann genau der betreffende Beweis gesichert wurde;

(e) Informationen über das Widerspruchsrecht des Nutzers und die Gründe aus denen ein solcher Widerspruch erhoben werden kann;

(f) Informationen über das Urheberrecht und seinen Sinn und Zweck;

or 124D (an “initial obligations code“) allows the owner to do so.

(3) A “copyright infringement report“ is a report that—

(a) states that there appears to have been an infringement of the owner’s copyright;

(b) includes a description of the apparent infringement;

(c) includes evidence of the apparent infringement that shows the subscriber’s IP address and the time at which the evidence was gathered;

(d) is sent to the internet service provider within the period of 1 month beginning with the day on which the evidence was gathered; and

(e) complies with any other requirement of the initial obligations code.

(4) An internet service provider who receives a copyright infringement report must notify the subscriber of the report if the initial obligations code requires the provider to do so.

(5) A notification under subsection (4) must be sent to the subscriber within the period of 1 month beginning with the day on which the provider receives the report.

(6) A notification under subsection (4) must include—

(a) a statement that the notification is sent under this section in response to a copyright infringement report;

(b) the name of the copyright owner who made the report;

(c) a description of the apparent infringement;

(d) evidence of the apparent infringement that shows the subscriber’s IP address and the time at which the evidence was gathered;

(e) information about subscriber appeals and the grounds on which they may be made;

(f) information about copyright and its purpose;

(g) Informationen über Möglichkeiten des legalen Zugriffs auf urheberrechtlich geschützte Werke bzw. einen Hinweis, wo entsprechende Informationen erhältlich sind;

(h) Informationen über die Möglichkeiten des Anschlussinhabers, seinen Internetzugang vor unberechtigtem Zugriff zu schützen bzw. einen Hinweis, wo entsprechende Informationen erhältlich sind; und

(i) alle anderen Angaben, die laut Initial Obligations Code in der Benachrichtigung enthalten sein müssen.

(7) Bei der Anwendung von Punkt (6)(h) muss der Anbieter des Internetdienstes berücksichtigen, dass abhängig von den Umständen für Anschlussinhaber verschiedene Schutzmöglichkeiten geeignet sein können.

(8) Zu den Informationen, die gemäß Punkt (6)(i) in der Benachrichtigung enthalten sein müssen, ob allgemein oder im Einzelfall, gehören insbesondere:

(a) der Vermerk, dass der Anbieter des Internetdienstes Informationen über die vorliegende Urheberrechtsverletzung speichern kann;

(b) der Vermerk, dass der Rechteinhaber den Anbieter des Internetdienstes dazu auffordern kann offenzulegen, welche der von ihm gemeldeten Urheberrechtsverletzungen von dem Anschlussinhaber begangen wurden;

(c) der Vermerk, dass der Rechteinhaber nach Offenlegung dieser Informationen die Identität des Anschlussinhabers mithilfe einer gerichtlichen Verfügung ermitteln und eine Klage wegen Verletzung des Urheberrechts gegen den Nutzer anstrengen kann; und

(d) der Vermerk dass, falls die Verpflichtung zur Versendung der Benachrichtigung daraus resultiert, dass zuvor bereits ein anderer Verstoß nach Punkt (4) gemeldet wurde, die Anzahl der vom Anschlussinhaber begangenen Urheberrechtsverletzungen herangezogen werden kann für eine Entscheidung über die Anwendung technischer Maßnahmen.

(9) In diesem Abschnitt bedeutet „Versendung eines Warnhinweises“ im Zusammenhang mit dem Anschlussinhaber, dass der

(g) advice, or information enabling the subscriber to obtain advice, about how to obtain lawful access to copyright works;

(h) advice, or information enabling the subscriber to obtain advice, about steps that a subscriber can take to protect an internet access service from unauthorised use; and

(i) anything else that the initial obligations code requires the notification to include.

(7) For the purposes of subsection (6)(h) the internet service provider must take into account the suitability of different protection for subscribers in different circumstances.

(8) The things that may be required under subsection (6)(i), whether in general or in a particular case, include in particular—

(a) a statement that information about the apparent infringement may be kept by the internet service provider;

(b) a statement that the copyright owner may require the provider to disclose which copyright infringement reports made by the owner to the provider relate to the subscriber;

(c) a statement that, following such a disclosure, the copyright owner may apply to a court to learn the subscriber's identity and may bring proceedings against the subscriber for copyright infringement; and

(d) where the requirement for the provider to send the notification arises partly because of a report that has already been the subject of a notification under subsection (4), a statement that the number of copyright infringement reports relating to the subscriber may be taken into account for the purposes of any technical measures.

(9) In this section “notify”, in relation to a subscriber, means send a notification to the electronic or postal address held by the

Internet-Dienstanbieter eine Benachrichtigung an die ihm vorliegende elektronische Adresse oder Postanschrift des Nutzers schickt (und dass die Abschnitte 394 bis 396 keine Anwendung finden).“

4 Verpflichtung zur Bereitstellung einer Liste der gemeldeten Urheberrechtsverstöße für den Rechteinhaber

Im Anschluss an Artikel 124A des Communications Act 2003 einfügen –

„124B Verpflichtung zur Bereitstellung einer Liste der gemeldeten Urheberrechtsverstöße für den Rechteinhaber

(1) Der Anbieter des Internetdienstes muss dem Rechteinhaber eine Liste über die innerhalb eines bestimmten Zeitraums gemeldeten Urheberrechtsverletzungen zur Verfügung stellen, wenn

(a) ein Rechteinhaber eine solche Liste für den Zeitraum angefordert hat; und
(b) sofern dies nach dem Initial Obligations Code vorgeschrieben ist.

(2) Eine „Liste der gemeldeten Urheberrechtsverstöße“ ist eine Liste,

(a) aus der in Bezug auf jeden relevanten Anschlussinhaber hervorgeht, welche der vom Rechteinhaber angezeigten Urheberrechtsverletzungen von dem betreffenden Anschlussinhaber begangen wurden,
(b) die jedoch keinen Aufschluss über die persönlichen Daten des Nutzers gibt.

(3) In Bezug auf den Rechteinhaber und den Anbieter des Internetdienstes ist ein Anschlussinhaber dann ein „relevanter Anschlussinhaber“, wenn die Anzahl der vom Rechteinhaber beim Anbieter des Internetdienstes gemeldeten Urheberrechtsverletzungen durch diesen Anschlussinhaber die Mindestgrenze überschritten hat, die im Initial Obligation Code festgelegt wurde.“

5 Anerkennung des Initial Obligation Code

Im Anschluss an Artikel 124B des Communications Act 2003 einfügen –

internet service provider for the subscriber (and sections 394 to 396 do not apply).“

4 Obligation to provide infringement lists to copyright owners

After section 124A of the Communications Act 2003 insert—

“124B Obligation to provide copyright infringement lists to copyright owners

(1) An internet service provider must provide a copyright owner with a copyright infringement list for a period if—

(a) the owner requests the list for that period; and

(b) an initial obligations code requires the internet service provider to provide it.

(2) A “copyright infringement list” is a list that—

(a) sets out, in relation to each relevant subscriber, which of the copyright infringement reports made by the owner to the provider relate to the subscriber, but

(b) does not enable any subscriber to be identified.

(3) A subscriber is a “relevant subscriber” in relation to a copyright owner and an internet service provider if copyright infringement reports made by the owner to the provider in relation to the subscriber have reached the threshold set in the initial obligations code.”

5 Approval of code about the initial obligations

After section 124B of the Communications Act 2003 insert—

„124 C Anerkennung des Initial Obligation Code

(1) Die Verpflichtungen des Internet-Diensteanbieters i. S. d. Abschnitte 124A und 124B sind die „grundlegenden Verpflichtungen“.

(2) Ist die OFCOM der Auffassung,

(a) dass zum Zweck einer Regulierung der grundlegenden Verpflichtungen ein Regelwerk verfasst wurde; und

(b) dass es sinnvoll ist, dieses Regelwerk anzuerkennen, kann sie ihre Anerkennung mit sofortiger Wirkung per Anordnung gewähren.

(3) Die Bestimmungen, die in diesem Regelwerk enthalten sein können und die die OFCOM nach diesem Abschnitt anerkennen kann, sind solche Bestimmungen,

(a) welche die Bedingungen erläutern, die im Einzelfall erfüllt sein müssen, um Rechte und Verpflichtungen nach den Bestimmungen zur Verletzung von Urheberrechten oder dem Regelwerk im konkreten Fall geltend machen zu können;

(b) die sowohl den Internet-Diensteanbieter als auch den Rechteinhaber dazu verpflichten, alle notwendigen Informationen bereitzustellen oder sonstige angemessene Unterstützung zu leisten, damit festgestellt werden kann, ob die Bedingungen aus Absatz (a) erfüllt sind.

(4) Die in Unterpunkt (3)(a) genannten Bedingungen müssen insbesondere festlegen, dass dem Rechteinhaber keinerlei Rechte und Verpflichtungen entstehen, es sei denn er hat eine Vereinbarung mit dem Internet-Diensteanbieter getroffen bezüglich

(a) der Anzahl von Meldungen über Urheberrechtsverletzungen, die der Rechteinhaber innerhalb eines bestimmten Zeitraums erstatten kann; und

(b) einer im Voraus zu entrichtenden Beteiligung durch den Rechteinhaber an den entstehenden Kosten für den Internet-Diensteanbieter.

(5) Die in Unterpunkt (3)(a) genannten Bestimmungen müssen insbesondere festlegen,

(a) dass, sofern nichts anderes im Regelwerk

“124C Approval of code about the initial obligations

(1) The obligations of internet service providers under sections 124A and 124B are the “initial obligations”.

(2) If it appears to OFCOM—

(a) that a code has been made by any person for the purpose of regulating the initial obligations; and

(b) that it would be appropriate for them to approve the code for that purpose, they may by order approve it, with effect from the date given in the order.

(3) The provision that may be contained in a code and approved under this section includes provision that—

(a) specifies conditions that must be met for rights and obligations under the copyright infringement provisions or the code to apply in a particular case;

(b) requires copyright owners or internet service providers to provide any information or assistance that is reasonably required to determine whether a condition under paragraph (a) is met.

(4) The provision mentioned in subsection (3)(a) may, in particular, specify that a right or obligation does not apply in relation to a copyright owner unless the owner has made arrangements with an internet service provider regarding—

(a) the number of copyright infringement reports that the owner may make to the provider within a particular period; and

(b) payment in advance of a contribution towards meeting costs incurred by the provider.

(5) The provision mentioned in subsection (3)(a) may also, in particular, provide that—

(a) except as provided by the code, rights

vorgesehen ist, die Rechte und Verpflichtungen aus dem Regelwerk auf den Internet-Diensteanbieter nicht anwendbar sind, sofern die Anzahl der Meldungen, die innerhalb eines bestimmten Zeitraums bei ihm eingehen, nicht die im Regelwerk festgeschriebene Mindestgrenze überschreiten; und

(b) dass, sobald die Mindestgrenze überschritten wird, die Rechte und Verpflichtungen aus dem Regelwerk von dem Zeitpunkt an gelten, an dem diese überschritten wurde oder ab einem späteren Zeitpunkt.

(6) Die OFCOM darf keinem Regelwerk i. S. d. Abschnitts zustimmen, das nicht die Kriterien in Abschnitt 124E erfüllt.

(7) Es kann zu einem gegebenen Zeitpunkt immer nur ein verbindliches Regelwerk in Kraft sein.

(8) Die OFCOM muss ein anerkanntes Regelwerk regelmäßig überprüfen.

(9) Die OFCOM kann jederzeit durch entsprechende Anordnung zu den in Punkt (2) genannten Zwecken

(a) Änderungen an einem anerkannten Regelwerk zustimmen; oder

(b) die Zustimmung zu einem zuvor von ihr anerkannten Regelwerk zurückziehen. Eine solche Anordnung ist mit sofortiger Wirkung gültig. Die OFCOM ist verpflichtet, ihre Zustimmung zurückziehen, falls das Regelwerk die Kriterien in Abschnitt 124E nicht länger erfüllt.

(10) Für die Anerkennung eines Regelwerks oder Änderungen an einem bestehenden Regelwerk ist die Genehmigung des Secretary of State (Minister) erforderlich.

(11) In einer Anordnung der OFCOM i. S. d. Abschnitts, durch die ein Regelwerk oder eine Änderung an einem bestehenden Regelwerk anerkannt wird, muss das betreffende Regelwerk oder die betreffende Änderung genannt werden.

(12) Abschnitt 403 regelt die Befugnis der OFCOM, eine Anordnung i. S. d. Abschnitts zu erlassen.

(13) Ein Rechtsinstrument, dem die OFCOM gem. dieses Abschnitts durch eine Anordnung zugestimmt hat, kann durch den Beschluss jedes der Houses of Parliament außer Kraft gesetzt werden."

and obligations do not apply in relation to an internet service provider unless the number of copyright infringement reports the provider receives within a particular period reaches a threshold set in the code; and

(b) if the threshold is reached, rights or obligations apply with effect from the date when it is reached or from a later time.

(6) OFCOM must not approve a code under this section unless satisfied that it meets the criteria set out in section 124E.

(7) Not more than one approved code may have effect at a time.

(8) OFCOM must keep an approved code under review.

(9) OFCOM may by order, at any time, for the purpose mentioned in subsection (2)—

(a) approve modifications that have been made to an approved code; or

(b) withdraw their approval from an approved code, with effect from the date given in the order, and must do so if the code ceases to meet the criteria set out in section 124E.

(10) The consent of the Secretary of State is required for the approval of a code or the modification of an approved code.

(11) An order made by OFCOM under this section approving a code or modification must set out the code or modification.

(12) Section 403 applies to the power of OFCOM to make an order under this section.

(13) A statutory instrument containing an order made by OFCOM under this section is subject to annulment in pursuance of a resolution of either House of Parliament."

6 Initial Obligations Code der OFCOM in Ermangelung eines anzuerkennenden Regelwerks

Im Anschluss an Artikel 124C des Communications Act 2003 einfügen –

„124D Initial Obligations Code der OFCOM in Ermangelung eines anzuerkennenden Regelwerks

(1) Sind die Abschnitte 124A und 124B in Kraft, ohne dass ein anerkannter Initial Obligations Code gemäß Abschnitt 124C vorliegt, muss die OFCOM per Anordnung ein entsprechendes Regelwerk beschließen.

(2) Die OFCOM hat die Befugnis, ist jedoch nicht dazu verpflichtet, ein Regelwerk i. S. d. Unterabschnitts (1) zu erstellen für den Zeitraum bis zum Ablauf von

(a) sechs Monaten ab Inkrafttreten der Abschnitte 124A und 124B, oder

(b) einen längeren Zeitraum, der vom Secretary of State festgelegt und der OFCOM mitgeteilt wird.

(3) Der Secretary of State wird die in Unterpunkt (2)(b) genannte Mitteilung nur dann vornehmen, wenn er der Auffassung ist, dass die Erstellung eines Regelwerks durch die OFCOM mit Wirkung zum Ende des in Unterpunkt (2)(a) genannten oder eines längeren Zeitraums gemäß Unterpunkt (2)(b) nicht realisierbar ist.

(4) Ein Regelwerk i. S. d. Abschnitts kann alle Sachverhalte regeln, die in den Abschnitten 124C(3) bis (5) Erwähnung finden.

(5) Ein Regelwerk i. S. d. Abschnitts kann unter anderem:

(a) der OFCOM selbst die Entscheidungsgewalt für bestimmte Angelegenheiten übertragen (außer über die Entscheidungsgewalt hinsichtlich eines Widerspruchs durch den Anschlussinhaber);

(b) der OFCOM die Befugnis erteilen, im Rahmen ihrer Zuständigkeit Entschädigungen festzulegen, die Erstattung von Kosten zu regeln oder beides;

(c) der OFCOM die Befugnis erteilen, durch das Regelwerk festgelegte Entschädigungen oder Vorschriften durchzusetzen oder

6 Initial obligations code by OFCOM in the absence of an approved code

After section 124C of the Communications Act 2003 insert—

“124D Initial obligations code by OFCOM in the absence of an approved code

(1) For any period when sections 124A and 124B are in force but for which there is no approved initial obligations code under section 124C, OFCOM must by order make a code for the purpose of regulating the initial obligations.

(2) OFCOM may but need not make a code under subsection (1) for a time before the end of—

(a) the period of six months beginning with the day on which sections 124A and 124B come into force, or

(b) such longer period as the Secretary of State may specify by notice to OFCOM.

(3) The Secretary of State may give a notice under subsection (2)(b) only if it appears to the Secretary of State that it is not practicable for OFCOM to make a code with effect from the end of the period mentioned in subsection (2)(a) or any longer period for the time being specified under subsection (2)(b).

(4) A code under this section may do any of the things mentioned in section 124C(3) to (5).

(5) A code under this section may also—

(a) confer jurisdiction with respect to any matter (other than jurisdiction to determine appeals by subscribers) on OFCOM themselves;

(b) provide for OFCOM, in exercising such jurisdiction, to make awards of compensation, to direct the reimbursement of costs, or to do both;

(c) provide for OFCOM to enforce, or to participate in the enforcement of, any awards or directions made under the code;

sich an Maßnahmen zu deren Durchsetzung zu beteiligen;

(d) andere Bestimmungen zur Durchsetzung solcher Entschädigungen und Vorschriften festzulegen;

(e) eine Körperschaft zu gründen, welche die Befugnis hat, eigene Regeln und Verfahrensabläufe festzulegen um Widersprüche der Anschlussinhaber zu bearbeiten;

(f) einer Person die Aufgabe übertragen, als Rechtsbehelfsinstanz die von ihr angeordneten Entschädigungen und Vorschriften durchzusetzen oder sich an Maßnahmen zu deren Durchsetzung zu beteiligen;

(g) andere Bestimmungen zur Durchsetzung solcher Entschädigungen und Vorschriften festzulegen; und

(h) andere Bestimmungen zur Regelung der Erstverpflichtungen festzulegen.

(6) Die OFCOM darf kein Regelwerk i. S. d. Abschnitts aufsetzen, das nicht die Kriterien in Abschnitt 124E erfüllt.

(7) Die OFCOM muss

(a) das Regelwerk i. S. d. Abschnitts regelmäßig überprüfen; und

(b) mittels Anordnungen Erweiterungen des Regelwerks veranlassen, die erforderlich sind, um die Erfüllung der Kriterien nach Abschnitt 124E für die gesamte Dauer seiner Wirksamkeit zu gewährleisten.

(8) Für die Erstellung und Erweiterung des Regelwerks i. S. d. Abschnitts durch die OFCOM ist die Genehmigung des Secretary of State erforderlich.

(9) Abschnitt 403 regelt die Befugnis der OFCOM, eine Anordnung i. S. d. Abschnitts zu erlassen.

(10) Ein Rechtsinstrument, dem die OFCOM i. S. d. Abschnitts durch eine Anordnung zugestimmt hat, kann durch den Beschluss jedes der Houses of Parliament außer Kraft gesetzt werden."

(d) make other provision for the enforcement of such awards and directions;

(e) establish a body corporate, with the capacity to make its own rules and establish its own procedures, for the purpose of determining subscriber appeals;

(f) provide for a person with the function of determining subscriber appeals to enforce, or to participate in the enforcement of, any awards or directions made by the person;

(g) make other provision for the enforcement of such awards and directions; and

(h) make other provision for the purpose of regulating the initial obligations.

(6) OFCOM must not make a code under this section unless they are satisfied that it meets the criteria set out in section 124E.

(7) OFCOM must—

(a) keep a code under this section under review; and

(b) by order make any amendment of it that is necessary to ensure that while it is in force it continues to meet the criteria set out in section 124E.

(8) The consent of the Secretary of State is required for the making or amendment by OFCOM of a code under this section.

(9) Section 403 applies to the power of OFCOM to make an order under this section.

(10) A statutory instrument containing an order made by OFCOM under this section is subject to annulment in pursuance of a resolution of either House of Parliament."

7 Inhalt des Initial Obliations Code

Im Anschluss an Artikel 124D des Communications Act 2003 einfügen –

„124E Inhalt des Initial Obliations Code

(1) Die in den Abschnitten 124C(6) und

7 Contents of initial obligations code

After section 124D of the Communications Act 2003 insert—

“124E Contents of initial obligations code

(1) The criteria referred to in sections

124D(6) genannten Kriterien sind:

- (a) dass das Regelwerk die erforderlichen Bestimmungen für die Meldung von Urheberrechtsverletzungen enthalten muss (siehe Unterpunkt (2));
- (b) dass das Regelwerk die erforderlichen Bestimmungen für die Benachrichtigung des Anschlussinhabers enthalten muss (siehe Unterpunkte (3) und (4));
- (c) dass es eine Mindestgrenze von Verstößen festlegen muss, ab der ein Anschlussinhaber als „relevanter Anschlussinhaber“ i. S. d. Abschnitts 124B(3) einzustufen ist (siehe Unterpunkte (5) und (6));
- (d) dass es Bestimmungen dazu enthalten muss, in welcher Form die Anbieter von Internetdiensten Informationen über ihre Anschlussinhaber aufbewahren;
- (e) dass es den Zeitraum für die Aufbewahrung von Anschlussinhaberdaten begrenzt;
- (f) dass es alle erforderlichen Bestimmungen bezüglich der Kostenbeteiligung enthält, die per Anordnung gemäß Abschnitt 124M festzulegen sind;
- (g) dass die Anforderungen betreffend die Verwaltung und die Durchsetzung des Regelwerks erfüllt werden (siehe Unterpunkte (7) und (8));
- (h) dass die Anforderungen betreffend den Einspruch durch Nutzer in Zusammenhang mit dem Regelwerk erfüllt werden (siehe Abschnitt 124K);
- (i) dass die Bestimmungen des Regelwerks in Bezug auf den zu regelnden Sachverhalt objektiv zu rechtfertigen sind;
- (j) dass die Bestimmungen keine Personen oder Personengruppen diskriminieren;
- (k) dass die Bestimmungen in Bezug auf ihren Zweck verhältnismäßig sind; und
- (l) dass die Bestimmungen in Bezug auf ihren Zweck transparent sind.

(2) Die erforderliche Bestimmung bezüglich der Meldung von Urheberrechtsverletzungen legt Folgendes fest:

- (a) Anforderungen an die zulässigen Mittel für die Sicherung von Beweisen für den Verstoß, welche der Meldung beizufügen sind;
- (b) das zu erfüllende Beweismaß; und

124C(6) and 124D(6) are—

- (a) that the code makes the required provision about copyright infringement reports (see subsection (2));
 - (b) that it makes the required provision about the notification of subscribers (see subsections (3) and (4));
 - (c) that it sets the threshold applying for the purposes of determining who is a relevant subscriber within the meaning of section 124B(3) (see subsections (5) and (6));
 - (d) that it makes provision about how internet service providers are to keep information about subscribers;
 - (e) that it limits the time for which they may keep that information;
 - (f) that it makes any provision about contributions towards meeting costs that is required to be included by an order under section 124M;
 - (g) that the requirements concerning administration and enforcement are met in relation to the code (see subsections (7) and (8));
 - (h) that the requirements concerning subscriber appeals are met in relation to the code (see section 124K);
 - (i) that the provisions of the code are objectively justifiable in relation to the matters to which it relates;
 - (j) that those provisions are not such as to discriminate unduly against particular persons or against a particular description of persons;
 - (k) that those provisions are proportionate to what they are intended to achieve; and
 - (l) that, in relation to what those provisions are intended to achieve, they are transparent.
- (2) The required provision about copyright infringement reports is provision that specifies—
- (a) requirements as to the means of obtaining evidence of infringement of copyright for inclusion in a report;
 - (b) the standard of evidence that must be

- (c) die erforderliche Form der Meldung;
- (3) Die erforderliche Bestimmung betreffend die Versendung eines Warnhinweises an einen Anschlussinhaber, die durch eine oder mehrere Meldungen von Urheberrechtsverletzungen aufgefallen sind, enthält
- (a) eine Festlegung der Mittel, die der Anbieter des Internetdienstes einsetzen kann, um den Anschlussinhaber zu identifizieren;
- (b) eine Bestimmung dahingehend, über welche der gemeldeten Verstöße der Anbieter des Internetdienstes den Anschlussinhaber informieren muss; und
- (c) eine Festlegung der Form, des Inhalts und der ordnungsgemäßen Übermittlung der einzelnen Benachrichtigungen.
- (4) Die Regelung nach Punkt (3) muss festlegen, dass die Meldung einer Urheberrechtsverletzung, welche beim Anbieter des Internetdienstes mehr als 12 Monate vor der Benachrichtigung eines Anschlussinhabers eingegangen ist, nicht länger berücksichtigt werden darf.
- (5) Die gemäß Unterpunkt (1)(c) geltende Mindestgrenze kann unter Beachtung der Bestimmungen in Punkt (6) für jeden beliebigen Sachverhalt festgelegt werden, insbesondere für einen oder mehrere der folgenden:
- (a) für die Anzahl der gemeldeten Urheberrechtsverletzungen;
- (b) für den Zeitraum, in dem die Meldungen beim Anbieter des Internetdienstes eingehen; und
- (c) für den Zeitpunkt der offenkundige Verletzung, auf den sie sich beziehen;
- (6) Die gemäß Unterpunkt (1)(c) geltende Mindestgrenze ist in der Weise zu handhaben, dass eine Meldung, die beim Anbieter des Internetdienstes mehr als 12 Monate vor einem bestimmten Zeitpunkt eingegangen ist, nicht bei Feststellung einer möglichen Überschreitung der Mindestgrenze zum maßgeblichen Zeitpunkt berücksichtigt wird; eine gemäß Abschnitt 124B erstellte und bereitgestellte Liste der gemeldeten Urheberrechtsverletzungen darf eine solche Meldung nicht enthalten.
- (7) Die Anforderungen betreffend Verwaltung und Durchsetzung sind

- included; and
- (c) the required form of the report.
- (3) The required provision about the notification of subscribers is provision that specifies, in relation to a subscriber in relation to whom an internet service provider receives one or more copyright infringement reports—
- (a) requirements as to the means by which the provider identifies the subscriber;
- (b) which of the reports the provider must notify the subscriber of; and
- (c) requirements as to the form, contents and means of the notification in each case.
- (4) The provision mentioned in subsection (3) must not permit any copyright infringement report received by an internet service provider more than 12 months before the date of a notification of a subscriber to be taken into account for the purposes of the notification.
- (5) The threshold applying in accordance with subsection (1)(c) may, subject to subsection (6), be set by reference to any matter, including in particular one or more of—
- (a) the number of copyright infringement reports;
- (b) the time within which the reports are made; and
- (c) the time of the apparent infringements to which they relate.
- (6) The threshold applying in accordance with subsection (1)(c) must operate in such a way that a copyright infringement report received by an internet service provider more than 12 months before a particular date does not affect whether the threshold is met on that date; and a copyright infringement list provided under section 124B must not take into account any such report.
- (7) The requirements concerning administration and enforcement are—

(a) dass die OFCOM im Rahmen des Regelwerks die Funktion einer verwaltenden und durchsetzenden Behörde übernimmt und unter anderem bei Meinungsverschiedenheiten zwischen Rechteinhaber und Internet-Diensteanbieter als vermittelnde Instanz tätig wird;

(b) dass das Regelwerk angemessene Bestimmungen und Maßnahmen enthält, durch die sichergestellt wird, dass die OFCOM von den Anbietern der Internetdienste sowie von den Rechteinhabern alle Informationen und jede Unterstützung erhält, welche die Behörde nach vernünftigem Ermessen benötigt, um das Regelwerk zu verwalten und über seine Einhaltung zu wachen zu können; und

(c) dass das Regelwerk angemessene Bestimmungen und Maßnahmen enthält, durch die sichergestellt wird, dass der OFCOM die Kosten aus der Verwaltung und Durchsetzung des Regelwerks von den Anbietern der Internetdienste und den Rechteinhabern erstattet werden.

(8) Die in Punkt (7) genannten Bestimmungen müssen insbesondere enthalten:

(a) die Zahlung einer Geldbuße, an eine im Regelwerk bestimmte Person, die keinesfalls die Höchstsumme für den in Abschnitt 124L(2) festgelegten Zeitraum überschreiten darf;

(b) die Verpflichtung des Rechteinhabers zur Zahlung einer Entschädigung an den Anbieter des Internetdienstes für Verluste und Schäden, die daraus resultieren, dass der Rechteinhaber das Regelwerk nicht befolgt oder die Bestimmungen zum Schutz des Urheberrechts missachtet hat.

(9) Die Bezeichnung „Streitigkeiten zwischen Rechteinhabern und Internetdienst-Anbietern“ in diesem Abschnitt bezieht sich auf Streitfragen

(a) zwischen Rechteinhabern und Anbietern von Internetdiensten; und

(b) auf ein Handeln oder Unterlassen im Zusammenhang mit den grundlegenden Verpflichtungen oder dem Initial Obligation Code.“

8 Fortschrittsberichte

Im Anschluss an Artikel 124E des Commu-

(a) that OFCOM have, under the code, the functions of administering and enforcing it, including the function of resolving owner-provider disputes;

(b) that there are adequate arrangements under the code for OFCOM to obtain any information or assistance from internet service providers or copyright owners that OFCOM reasonably require for the purposes of administering and enforcing the code; and

(c) that there are adequate arrangements under the code for the costs incurred by OFCOM in administering and enforcing the code to be met by internet service providers and copyright owners.

(8) The provision mentioned in subsection (7) may include, in particular—

(a) provision for the payment, to a person specified in the code, of a penalty not exceeding the maximum penalty for the time being specified in section 124L(2);

(b) provision requiring a copyright owner to indemnify an internet service provider for any loss or damage resulting from the owner's failure to comply with the code or the copyright infringement provisions.

(9) In this section “owner-provider dispute” means a dispute that—

(a) is between persons who are copyright owners or internet service providers; and

(b) relates to an act or omission in relation to an initial obligation or an initial obligations code.”

8 Progress reports

After section 124E of the Communications

nications Act 2003 einfügen –

„124F Fortschrittsberichte

(1) Die OFCOM muss für den Secretary of State die nachstehend genannten Berichte über Verstöße gegen das Urheberrecht durch Nutzer von Internetdiensten erstellen.

(2) Die OFCOM muss einen vollständigen Bericht vorlegen für

(a) den Zeitraum von 12 Monaten nach Inkrafttreten eines Initial Obligations Code; und

(b) jeden darauffolgenden Zeitraum von 12 Monaten.

(3) Die OFCOM muss einen Zwischenbericht vorlegen für

(a) den Zeitraum von 3 Monaten nach Inkrafttreten des Initial Obligations Code; und

(b) jeden darauffolgenden Zeitraum von 3 Monaten, sofern dessen Ende nicht mit dem Ende eines 12-Monatszeitraums nach Punkt (2) zusammenfällt. Dies richtet sich jedoch nach den Maßgaben des Secretary of State gemäß Punkt (4).

(4) Der Secretary of State kann Punkt (3) durch eine entsprechende Anordnung mit sofortiger Wirkung außer Kraft setzen.

(5) Ein vollständiger Bericht i. S. d. Abschnitts muss enthalten:

(a) eine Bewertung des gegenwärtigen Ausmaßes des Missbrauchs von Internetdiensten für Verstöße gegen das Urheberrecht;

(b) eine Beschreibung der von den Rechteinhabern ergriffenen Maßnahmen, um Internetnutzern den legalen Zugriff auf urheberrechtlich geschützten Werke zu ermöglichen;

(c) eine Beschreibung der von den Rechteinhabern ergriffenen Maßnahmen, um die Öffentlichkeit über die Verletzung des Urheberrechts zu informieren und sie dafür zu sensibilisieren;

(d) eine Bewertung des Ausmaßes der in den Absätzen (b) und (c) aufgeführten Maßnahmen;

(e) eine Bewertung des Ausmaßes, in dem Rechteinhaber von der Möglichkeit der

Act 2003 insert—

“124F Progress reports

(1) OFCOM must prepare the following reports for the Secretary of State about the infringement of copyright by subscribers to internet access services.

(2) OFCOM must prepare a full report for—

(a) the period of 12 months beginning with the first day on which there is an initial obligations code in force; and

(b) each successive period of 12 months.

(3) OFCOM must prepare an interim report for—

(a) the period of 3 months beginning with the first day on which there is an initial obligations code in force; and

(b) each successive period of 3 months, other than one ending at the same time as a period of 12 months under subsection (2). But this is subject to any direction by the Secretary of State under subsection (4).

(4) The Secretary of State may direct that subsection (3) no longer applies, with effect from the date given in the direction.

(5) A full report under this section must include—

(a) an assessment of the current level of subscribers' use of internet access services to infringe copyright;

(b) a description of the steps taken by copyright owners to enable subscribers to obtain lawful access to copyright works;

(c) a description of the steps taken by copyright owners to inform, and change the attitude of, members of the public in relation to the infringement of copyright;

(d) an assessment of the extent of the steps mentioned in paragraphs (b) and (c);

(e) an assessment of the extent to which copyright owners have made copyright

- Meldung von Urheberrechtsverletzungen Gebrauch machen;
- (f) eine Bewertung des Ausmaßes, in welchem gerichtliche Prozesse gegen Anschlussinhaber wegen Urheberrechtsverletzungen angestrengt wurden in Bezug zur Anzahl der Meldungen;
- (g) eine Bewertung des Ausmaßes in dem gerichtliche Prozesse gegen Nutzer angestrengt wurden, die besonders häufig wegen Urheberrechtsverletzungen gemeldet wurden; und
- (h) alle anderen Informationen, welche die OFCOM nach Maßgabe des Secretary of State in den Bericht aufnehmen soll.
- (6) Ein Zwischenbericht i. S. d. Abschnitts muss enthalten:
- (a) die in den Unterpunkten (5)(a), (e) und (f) genannten Bewertungen; und
- (b) alle anderen Informationen, welche die OFCOM nach Maßgabe des Secretary of State in den Bericht aufnehmen soll.
- (7) Die OFCOM muss die in diesem Abschnitt genannten Berichte dem Secretary of State so bald wie möglich nach Ablauf des jeweiligen Berichtszeitraums zukommen lassen.
- (8) Die OFCOM muss alle in diesem Abschnitt genannten vollständigen Berichte
- (a) so bald wie möglich nach Übersendung an den Minister veröffentlichen, und
- (b) in einer Art und Weise veröffentlichen, welche nach ihrer Auffassung geeignet ist, um die Inhalte interessierten Personen zur Kenntnis zu bringen.
- (9) Die OFCOM kann bestimmte Informationen von der Veröffentlichung des Berichts gemäß Punkt (8) ausschließen, falls sie die Auffassung vertritt, dass es sich dabei um Informationen handelt, deren Veröffentlichung sie aufgrund eines Antrags gemäß des Freedom of Information Act 2000 ablehnen könnte."
- infringement reports;
- (f) an assessment of the extent to which they have brought legal proceedings against subscribers in relation to whom such reports have been made;
- (g) an assessment of the extent to which any such proceedings have been against subscribers in relation to whom a substantial number of reports have been made; and
- (h) anything else that the Secretary of State directs OFCOM to include in the report.
- (6) An interim report under this section must include—
- (a) the assessments mentioned in subsection (5)(a), (e) and (f); and
- (b) anything else that the Secretary of State directs OFCOM to include in the report.
- (7) OFCOM must send a report prepared under this section to the Secretary of State as soon as practicable after the end of the period for which it is prepared.
- (8) OFCOM must publish every full report under this section—
- (a) as soon as practicable after they send it to the Secretary of State, and
- (b) in such manner as they consider appropriate for bringing it to the attention of persons who, in their opinion, are likely to have an interest in it.
- (9) OFCOM may exclude information from a report when it is published under subsection (8) if they consider that it is information that they could refuse to disclose in response to a request under the Freedom of Information Act 2000."

9 Verpflichtung zur Beschränkung des Internetzugangs: Bewertung und Vorbereitung

Im Anschluss an Artikel 124F des Commu-

9 Obligations to limit internet access: assessment and preparation

After section 124F of the Communications

nications Act 2003 einfügen –

Act 2003 insert—

„124G Verpflichtung zur Beschränkung des Internetzugangs: Bewertung und Vorbereitung

“124G Obligations to limit internet access: assessment and preparation

(1) Der Secretary of State kann die OFCOM anweisen

(1) The Secretary of State may direct OFCOM to—

(a) darüber zu beraten, ob den Anbietern von Internetdiensten eine oder mehrere Verpflichtungen zur Durchführung technischer Maßnahmen auferlegt werden sollten;

(a) assess whether one or more technical obligations should be imposed on internet service providers;

(b) geeignete Schritte zur Vorbereitung dieser Verpflichtungen zu ergreifen;

(b) take steps to prepare for the obligations;

(c) für ihn einen Bericht über das Beratungsergebnis oder die Schritte zu verfassen.

(c) provide a report on the assessment or steps to the Secretary of State.

(2) Eine „Verpflichtung zur Durchführung technischer Maßnahmen“ bezogen auf den Anbieter eines Internetdienstes bedeutet dessen Verpflichtung, technische Maßnahmen gegen einige oder alle relevanten Anschlusshaber seines Dienstes zu ergreifen, die dem Zweck dienen, Verstöße gegen das Urheberrecht im Internet zu reduzieren oder zu verhindern.

(2) A “technical obligation”, in relation to an internet service provider, is an obligation for the provider to take a technical measure against some or all relevant subscribers to its service for the purpose of preventing or reducing infringement of copyright by means of the internet.

(3) Eine „technische Maßnahme“ kann Folgendes beinhalten:

(3) A “technical measure” is a measure that—

(a) Herabsetzung der Übertragungsgeschwindigkeit oder anderer Leistungen, die dem Anschlussinhaber zur Verfügung gestellt werden;

(a) limits the speed or other capacity of the service provided to a subscriber;

(b) Verweigerung oder Beschränkung der Nutzung des Dienstes für den Zugriff auf bestimmte Inhalte;

(b) prevents a subscriber from using the service to gain access to particular material, or limits such use;

(c) Aussetzung der Dienstleistung für den Anschlussinhaber; oder

(c) suspends the service provided to a subscriber; or

(d) sonstige Beschränkungen der Nutzung des Dienstes.

(d) limits the service provided to a subscriber in another way.

(4) Der Anschlussinhaber eines Internetdienstes gilt in Bezug auf den Anbieter des Internetdienstes und einen oder mehrere Rechteinhaber als „relevant“, wenn es sich bei ihm um einen „relevanten Anschlussinhaber“ im Sinne der Definition in Abschnitt 124B(3) handelt.

(4) A subscriber to an internet access service is “relevant” if the subscriber is a relevant subscriber, within the meaning of section 124B(3), in relation to the provider of the service and one or more copyright owners.

(5) Die Durchführung der Beratungen und Schritte, welche der Secretary of State der OFCOM nach Punkt (1) auftragen kann, beinhaltet insbesondere

(5) The assessment and steps that the Secretary of State may direct OFCOM to carry out or take under subsection (1) include, in particular—

- (a) eine Befragung der Rechteinhaber, der Anbieter von Internetdiensten, der Anschlussinhaber und anderer Personen;
- (b) eine Bewertung der zu erwartenden Effektivität einer technischen Maßnahme im Hinblick auf eine bestimmten Art von Internetdienst; und
- (c) Schritte zur Vorbereitung eines Technical Obligations Code;
- (6) Anbieter von Internetdiensten und Rechteinhaber sind dazu verpflichtet, der OFCOM jede Unterstützung zu leisten, welche die Behörde vernünftigerweise benötigt, um ihre Verpflichtungen aus diesem Abschnitt erfüllen zu können.
- (7) Der Secretary of State muss jede gemäß diesem Abschnitt getroffene Anordnung dem britischen Parlament zur Genehmigung vorlegen.
- (8) Die OFCOM muss Berichte gemäß diesem Abschnitt
- (a) schnellstmöglich nach Übersendung an den Secretary of State veröffentlichen, und
- (b) in einer Art und Weise veröffentlichen, welche nach ihrer Auffassung geeignet ist, um die Inhalte interessierten Personen zur Kenntnis zu bringen.
- (9) Die OFCOM kann bestimmte Informationen von der Veröffentlichung des Berichts nach Punkt (8) ausschließen, falls sie die Auffassung vertritt, dass es sich um Informationen handelt, deren Veröffentlichung sie aufgrund eines Antrags gemäß Freedom of Information Act 2000 ablehnen könnte."

10 Verpflichtung zur Beschränkung des Internetzugangs

Im Anschluss an Artikel 124G des Communications Act 2003 einfügen –

„124H Verpflichtung zur Beschränkung des Internetzugangs

- (1) Der Secretary of State kann einem Internet-Diensteanbieter durch Verfügung die Verpflichtung zur Durchführung einer technischen Maßnahme auferlegen, sofern
- (a) die OFCOM darüber beraten hat, ob dem Anbieter eine oder mehrere Verpflichtungen zur Durchführung technischer Maßnahmen auferlegt werden sollen; und

- (a) consultation of copyright owners, internet service providers, subscribers or any other person;
- (b) an assessment of the likely efficacy of a technical measure in relation to a particular type of internet access service; and
- (c) steps to prepare a proposed technical obligations code.
- (6) Internet service providers and copyright owners must give OFCOM any assistance that OFCOM reasonably require for the purposes of complying with any direction under this section.

(7) The Secretary of State must lay before Parliament any direction under this section.

(8) OFCOM must publish every report under this section—

- (a) as soon as practicable after they send it to the Secretary of State, and
- (b) in such manner as they consider appropriate for bringing it to the attention of persons who, in their opinion, are likely to have an interest in it.

(9) OFCOM may exclude information from a report when it is published under subsection (8) if they consider that it is information that they could refuse to disclose in response to a request under the Freedom of Information Act 2000."

10 Obligations to limit internet access

After section 124G of the Communications Act 2003 insert—

“124H Obligations to limit internet access

- (1) The Secretary of State may by order impose a technical obligation on internet service providers if—
- (a) OFCOM have assessed whether one or more technical obligations should be imposed on internet service providers; and

- (b) der Secretary of State aufgrund der Einschätzung und der Berichte der OFCOM nach Abschnitt 124F und nach Bewertung aller anderen seiner Auffassung nach relevanten Fakten zu dem Schluss kommt, dass eine solche Verfügung angemessen ist.
- (2) Eine Verfügung i. S. d. Abschnitts darf nicht innerhalb der ersten 12 Monate nach Inkrafttreten des Initial Obligations Code ergehen.
- (3) Eine Verfügung i. S. d. Abschnitts muss das Datum angeben, von dem an eine Verpflichtung zur Anwendung technischer Maßnahmen besteht oder Regelungen zu dessen Festlegung beinhalten.
- (4) Die Verfügung muss darüber hinaus enthalten:
- (a) Kriterien für die Anwendung technischer Maßnahme gegen den Nutzer;
- (b) erforderliche Schritte im Rahmen einer Maßnahme und Informationen darüber, wann die einzelnen Schritte erfolgen sollen.
- (5) Eine Verfügung i. S. d. Abschnitts darf erst dann ergehen,
- (a) wenn der Secretary of State den Anforderungen der Punkte (6) bis (10) nachgekommen ist; und
- (b) wenn dem Parlament ein Entwurf für die Verfügung vorgelegt wurde und dieser von beiden Houses of Parliament per Beschluss genehmigt wurde.
- (6) Falls der Secretary of State eine Verfügung nach diesem Abschnitt beantragen möchte, muss er dem britischen Parlament ein Dokument vorlegen, das
- (a) eine Begründung für den Antrag enthält, und
- (b) diese Begründung in Form eines Verfügungsentwurfs darlegt.
- (7) Ab dem Tag, an dem das Dokument gemäß Punkt (6) dem Parlament vorgelegt wurde, darf der Secretary of State dem Parlament 60 Tage lang (die „60-Tage-Frist“) keinen Verfügungsentwurf vorlegen, durch dessen Annahme sein Antrag wirksam würde (mit oder ohne Änderungen).
- (8) Bei der Vorbereitung eines Verfügungsentwurfs gemäß diesem Abschnitt, durch dessen Annahme der vorgenannte Antrag in Kraft gesetzt würde, muss der Secretary of State während der 60-Tage-Frist Folgen
- (b) taking into account that assessment, reports prepared by OFCOM under section 124F, and any other matter that appears to the Secretary of State to be relevant, the Secretary of State considers it appropriate to make the order.
- (2) No order may be made under this section within the period of 12 months beginning with the first day on which there is an initial obligations code in force.
- (3) An order under this section must specify the date from which the technical obligation is to have effect, or provide for it to be specified.
- (4) The order may also specify—
- (a) the criteria for taking the technical measure concerned against a subscriber;
- (b) the steps to be taken as part of the measure and when they are to be taken.
- (5) No order is to be made under this section unless—
- (a) the Secretary of State has complied with subsections (6) to (10), and
- (b) a draft of the order has been laid before Parliament and approved by a resolution of each House.
- (6) If the Secretary of State proposes to make an order under this section, the Secretary of State must lay before Parliament a document that—
- (a) explains the proposal, and
- (b) sets it out in the form of a draft order.
- (7) During the period of 60 days beginning with the day on which the document was laid under subsection (6) (“the 60-day period”), the Secretary of State may not lay before Parliament a draft order to give effect to the proposal (with or without modifications).
- (8) In preparing a draft order under this section to give effect to the proposal, the Secretary of State must have regard to any of the following that are made with regard to the draft order during the 60-day period—

des berücksichtigen:

(a) sämtliche Einwände und
(b) Empfehlungen der Ausschüsse beider Houses of Parliament, die dem Parlament über diesen Verfügungsentwurf berichten.

(9) Legt der Secretary of State dem Parlament einen Verfügungsentwurf vor, durch dessen Annahme sein Antrag in Kraft gesetzt würde (mit oder ohne Änderungen), muss er gegebenenfalls ein Dokument vorlegen, in dem alle Änderungen an dem Antrag, der dem Parlament gemäß Unterpunkt (6) vorgelegt wurde, erläutert werden.

(10) Bei der Bestimmung des Datums, an dem die 60-Tage-Frist abläuft, werden Zeiträume, in denen das Parlament aufgelöst oder vertagt ist, oder in denen die Sitzungsperiode in einer der beiden Houses of Parliament für länger als 4 Tage unterbrochen ist, nicht berücksichtigt.“

11 Regelwerk der OFCOM über die Verpflichtung zur Beschränkung des Internetzugangs

Im Anschluss an Artikel 124H des Communications Act 2003 einfügen –

„124I Regelwerk der OFCOM über die Verpflichtung zur Beschränkung des Internetzugangs

(1) Befinden sich während eines Zeitraums eine oder sind mehrere Verpflichtungen zur Durchführung technischer Maßnahmen gemäß Abschnitt 124H in Anwendung, muss die OFCOM durch Verfügung einen entsprechenden Technical Obligations Code zur Durchführung technischer Maßnahmen erstellen.

(2) Dieses Regelwerk kann unabhängig von oder in Kombination mit dem Initial Obligations Code i. S. d. Abschnitts 124D aufgesetzt werden.

(3) Ein Regelwerk i. S. d. Abschnitts muss
(a) alle Sachverhalte regeln, die in den Abschnitten 124C(3) bis (5) oder 124D(5)(a) bis (g) Erwähnung finden; und
(b) sonstige Bestimmungen zur Regelung der Verpflichtung zur Durchführung technischer Maßnahmen festlegen.

(a) any representations, and
(b) any recommendations of a committee of either House of Parliament charged with reporting on the draft order.

(9) When laying before Parliament a draft order to give effect to the proposal (with or without modifications), the Secretary of State must also lay a document that explains any changes made to the proposal contained in the document laid before Parliament under subsection (6).

(10) In calculating the 60-day period, no account is to be taken of any time during which Parliament is dissolved or prorogued or during which either House is adjourned for more than 4 days.”

11 Code by OFCOM about obligations to limit internet access

After section 124H of the Communications Act 2003 insert—

“124I Code by OFCOM about obligations to limit internet access

(1) For any period during which there are one or more technical obligations in force under section 124H, OFCOM must by order make a technical obligations code for the purpose of regulating those obligations.

(2) The code may be made separately from, or in combination with, any initial obligations code under section 124D.

(3) A code under this section may—
(a) do any of the things mentioned in section 124C(3) to (5) or section 124D(5)(a) to (g); and
(b) make other provision for the purpose of regulating the technical obligations.

- | | |
|--|---|
| <p>(4) Die OFCOM darf kein Regelwerk i. S. d. Abschnitts erstellen, das nicht die Kriterien in Abschnitt 124J erfüllt.</p> <p>(5) Die OFCOM muss</p> <p>(a) ein Regelwerk i. S. d. Abschnitts regelmäßig überprüfen; und</p> <p>(b) auf Anordnung Erweiterungen des Regelwerks veranlassen, die erforderlich sind, um die Erfüllung der Kriterien aus Abschnitt 124J für die Dauer seiner Wirksamkeit zu gewährleisten.</p> <p>(6) Für die Verabschiedung und Erweiterung des Regelwerks i. S. d. Abschnitts durch die OFCOM ist eine Genehmigung durch den Secretary of State erforderlich.</p> <p>(7) Abschnitt 403 regelt die Befugnis der OFCOM zur Beschlussfassung i. S. d. Abschnitts.</p> <p>(8) Ein Rechtsinstrument, dem die OFCOM i. S. d. Abschnitts durch einen Beschluss zugestimmt hat, kann durch den Beschluss einer der beiden Houses of Parliament außer Kraft gesetzt werden."</p> | <p>(4) OFCOM must not make a code under this section unless they are satisfied that it meets the criteria set out in section 124J.</p> <p>(5) OFCOM must—</p> <p>(a) keep a code under this section under review; and</p> <p>(b) by order make any amendment of it that is necessary to ensure that while it is in force it continues to meet the criteria set out in section 124J.</p> <p>(6) The consent of the Secretary of State is required for the making or amendment by OFCOM of a code under this section.</p> <p>(7) Section 403 applies to the power of OFCOM to make an order under this section.</p> <p>(8) A statutory instrument containing an order made by OFCOM under this section is subject to annulment in pursuance of a resolution of either House of Parliament."</p> |
|--|---|

12 Inhalt des Regelwerks über die Verpflichtung zur Beschränkung des Internetzugangs

Im Anschluss an Artikel 124I des Communications Act 2003 einfügen –

„124J Inhalt des Regelwerks über die Verpflichtung zur Beschränkung des Internetzugangs

- (1) Die in Abschnitt 124I(4) genannten Kriterien sind:
- (a) dass die Anforderungen bezüglich der Verwaltung und Durchsetzung des Regelwerks sowie weitere Bedingungen in Zusammenhang mit dem Regelwerk erfüllt werden (siehe Punkte (2) und (3));
- (b) dass die Anforderungen betreffend das Widerspruchsrecht des Anschlussinhabers erfüllt werden (siehe Abschnitt 124K);
- (c) dass eine Regelung bezüglich der Beteiligung am Kostenaufwand enthalten ist, die durch eine Verfügung gemäß Abschnitt 124M hinzugefügt werden muss;
- (d) dass das Regelwerk alle sonstigen vom Secretary of State geforderten Bestimmun-

12 Contents of code about obligations to limit internet access

After section 124I of the Communications Act 2003 insert—

“124J Contents of code about obligations to limit internet access

- (1) The criteria referred to in section 124I(4) are—
- (a) that the requirements concerning enforcement and related matters are met in relation to the code (see subsections (2) and (3));
- (b) that the requirements concerning subscriber appeals are met in relation to the code (see section 124K);
- (c) that it makes any provision about contributions towards meeting costs that is required to be included by an order under section 124M;
- (d) that it makes any other provision that the Secretary of State requires it to make;

gen vorsieht;

(e) dass die Bestimmungen des Regelwerks in Bezug auf den zu regelnden Sachverhalt objektiv zu rechtfertigen sind;

(f) dass die Bestimmungen keine Personen oder Personengruppen diskriminieren;

(g) dass die Bestimmungen in Bezug auf ihren Zweck verhältnismäßig sind; und

(h) dass die Bestimmungen in Bezug auf ihren Zweck transparent sind.

(2) Die Anforderungen bezüglich der Durchsetzung von Regelungen und den damit zusammenhängenden Angelegenheiten sind:

(a) dass die OFCOM im Rahmen des Regelwerks die Funktion einer verwaltenden und durchsetzenden Behörde übernimmt und unter anderem bei Meinungsverschiedenheiten zwischen Rechteinhaber und Internet-Dienstanbieter als vermittelnde Instanz tätig wird;

(b) dass das Regelwerk angemessene Bestimmungen und Maßnahmen enthält, durch die sichergestellt wird, dass die OFCOM von den Anbietern von Internetdiensten sowie von den Rechteinhabern alle Informationen und jede Unterstützung erhält, welche die Behörde nach vernünftigem Ermessen benötigt, um das Regelwerk zu verwalten und über seine Einhaltung wachen zu können; und

(c) dass das Regelwerk angemessene Bestimmungen und Maßnahmen enthält, durch die sichergestellt wird, dass die der OFCOM entstehenden Kosten für die Verwaltung und Durchsetzung des Regelwerks durch die Anbieter von Internetdiensten und die Rechteinhaber erstattet werden.

(3) Die Regelung betreffend die Durchsetzung von Regelungen und damit zusammenhängenden Verwaltung müssen insbesondere enthalten (sofern vom Secretary of State nicht anders angeordnet):

(a) eine Bestimmung, welche die Zahlung einer Strafe an eine im Regelwerk benannte Person vorsieht, die für den in Abschnitt 124L(2) festgelegten Zeitraum keinesfalls die Höchstsumme überschreiten darf;

(b) eine Bestimmung, welche vorsieht, dass

(e) that the provisions of the code are objectively justifiable in relation to the matters to which it relates;

(f) that those provisions are not such as to discriminate unduly against particular persons or against a particular description of persons;

(g) that those provisions are proportionate to what they are intended to achieve; and

(h) that, in relation to what those provisions are intended to achieve, they are transparent.

(2) The requirements concerning enforcement and related matters are—

(a) that OFCOM have, under the code, the functions of administering and enforcing it, including the function of resolving owner-provider disputes;

(b) that there are adequate arrangements under the code for OFCOM to obtain any information or assistance from internet service providers or copyright owners that OFCOM reasonably require for the purposes of administering and enforcing the code; and

(c) that there are adequate arrangements under the code for the costs incurred by OFCOM in administering and enforcing the code to be met by internet service providers and copyright owners.

(3) The provision made concerning enforcement and related matters may also (unless the Secretary of State requires otherwise) include, in particular—

(a) provision for the payment, to a person specified in the code, of a penalty not exceeding the maximum penalty for the time being specified in section 124L(2);

(b) provision requiring a copyright owner to

der Rechteinhaber den Anbieter des Internetdienstes für Verluste und Schäden entschädigen muss, die daraus entstanden sind, dass der Rechteinhaber das Regelwerk nicht befolgt oder die Bestimmungen zum Urheberrecht missachtet hat.

(4) Die Bezeichnung „Streitigkeiten zwischen Rechteinhaber und Internetdienst-Anbieter“ in diesem Abschnitt bezieht sich auf Streitfälle

(a) zwischen den Rechteinhabern und Anbietern von Internetdiensten; und

(b) die mit einem Handeln oder Unterlassen i. S. d. Regelwerks über die Verpflichtung zur Durchführung technischer Maßnahmen in Zusammenhang stehen.“

13 Widerspruchsrecht des Anschlussinhabers

Im Anschluss an Artikel 124J des Communications Act 2003 einfügen –

„124K Widerspruchsrecht des Anschlussinhabers

(1) Die Anforderungen betreffend das Widerspruchsrecht des Anschlussinhabers sind:

(a) zu den in Abschnitt 124E(1)(h) genannten Zwecken die Anforderungen der Unterpunkte (2) bis (8); und

(b) zu den in Abschnitt 124E(1)(b) genannten Zwecken die Anforderungen der Unterpunkte (2) bis (11).

(2) Die Anforderungen dieses Unterpunkts sind:

(a) dass das Regelwerk dem Anschlussinhaber das Recht einräumt, Widerspruch zu erheben und, im Falle des Erlasses eines Technical Obligations Code, das Recht eine weitere Beschwerde beim First-tier Tribunal (britisches Verwaltungsgericht) einzulegen;

(b) dass einer Person die Aufgabe übertragen wird, über Widersprüche von Anschlussinhabern zu entscheiden;

(c) dass diese Person aus praktischen Gründen unabhängig von Internetdienst-Anbietern, Rechteinhabern und der OFCOM agiert (bei der Entscheidung über Widersprüche des Anschlussinhabers); und

indemnify an internet service provider for any loss or damage resulting from the owner’s infringement or error in relation to the code or the copyright infringement provisions.

(4) In this section “owner-provider dispute” means a dispute that—

(a) is between persons who are copyright owners or internet service providers; and

(b) relates to an act or omission in relation to a technical obligation or a technical obligations code.”

13 Subscriber appeals

After section 124J of the Communications Act 2003 insert—

“124K Subscriber appeals

(1) The requirements concerning subscriber appeals are—

(a) for the purposes of section 124E(1)(h), the requirements of subsections (2) to (8); and

(b) for the purposes of section 124J(1)(b), the requirements of subsections (2) to (11).

(2) The requirements of this subsection are—

(a) that the code confers on subscribers the right to bring a subscriber appeal and, in the case of a technical obligations code, a further right of appeal to the First-tier Tribunal;

(b) that there is a person who, under the code, has the function of determining subscriber appeals;

(c) that that person is for practical purposes independent (so far as determining subscriber appeals is concerned) of internet service providers, copyright owners and OFCOM; and

(d) dass das Regelwerk angemessene Bestimmungen und Maßnahmen enthält, durch die sichergestellt wird, dass diese Person eine Erstattung der ihr bei der Entscheidung über Widersprüche entstehenden Kosten durch die betroffenen Internet-Diensteanbieter und die Rechteinhaber erhält.

(3) Das Regelwerk muss folgende Widerspruchsgründe festlegen (sofern ein Widerspruch gegen oder im Zusammenhang mit einem gemeldeten Regelverstoß vorgebracht wird):

(a) bei dem offenkundigen Verstoß, auf den sich die Meldung bezieht, handelte es sich nicht um eine Urheberrechtsverletzung;

(b) der gemeldete Verstoß sowie der Zeitpunkt des Verstoßes lassen sich nicht mit der IP-Adresse des Anschlussinhabers in Zusammenhang bringen.

(4) Das Regelwerk muss Widerspruchsgründe festlegen für den Fall, dass ein Rechteinhaber oder Internet-Diensteanbieter Verpflichtungen aus dem Regelwerk nicht erfüllt oder gegen das Regelwerk verstoßen hat.

(5) Das Regelwerk muss vorsehen, dass bei einem Einspruch stets zugunsten des Anschlussinhabers entschieden werden muss, es sei denn der Rechteinhaber bzw. der Anbieter des Internetdienstes weist nach, dass die entsprechende Meldung (oder falls mehrere Meldungen vorliegen, jede dieser Meldungen) gerechtfertigt ist und dass

(a) bei dem offenkundigen Verstoß eine Verletzung des Urheberrechts vorlag;

(b) der angezeigte Verstoß sowie der Zeitpunkt des Verstoßes sich mit der IP-Adresse des Anschlussinhabers in Zusammenhang bringen lassen.

(6) Das Regelwerk muss vorsehen, dass bei einem Widerspruch aufgrund eines der in Punkt (3) genannten Gründe stets zugunsten des Anschlussinhabers entschieden werden muss, sofern dieser nachweisen kann, dass

(a) der offenkundige Verstoß, auf den sich die Meldung bezieht, nicht durch ihn begangen wurde, und

(b) der Anschlussinhaber angemessene Schritte ergriffen hat um zu verhindern,

(d) that there are adequate arrangements under the code for the costs incurred by that person in determining subscriber appeals to be met by internet service providers, copyright owners and the subscriber concerned.

(3) The code must provide for the grounds of appeal (so far as an appeal relates to, or to anything done by reference to, a copyright infringement report) to include the following—

(a) that the apparent infringement to which the report relates was not an infringement of copyright;

(b) that the report does not relate to the subscriber's IP address at the time of the apparent infringement.

(4) The code must provide for the grounds of appeal to include contravention by the copyright owner or internet service provider of the code or of an obligation regulated by the code.

(5) The code must provide that an appeal on any grounds must be determined in favour of the subscriber unless the copyright owner or internet service provider shows that, as respects any copyright infringement report to which the appeal relates or by reference to which anything to which the appeal relates was done (or, if there is more than one such report, as respects each of them)—

(a) the apparent infringement was an infringement of copyright, and

(b) the report relates to the subscriber's IP address at the time of that infringement.

(6) The code must provide that, where a ground mentioned in subsection (3) is relied on, the appeal must be determined in favour of the subscriber if the subscriber shows that—

(a) the act constituting the apparent infringement to which the report relates was not done by the subscriber, and

(b) the subscriber took reasonable steps to prevent other persons infringing copyright

dass andere Personen mit Hilfe des betreffenden Internetdienst eine Verletzung des Urheberrechts begehen.

(7) Die Befugnisse der Person, die über Widersprüche von Anschlussinhabern entscheidet, müssen

(a) dazu geeignet sein, so weit wie möglich sicherzustellen, dass kein Anschlussinhaber bei der Durchsetzung der Bestimmungen zum Schutz des Urheberrechts durch ein Handeln oder Unterlassen im Zusammenhang mit einem Widerspruch, der zugunsten des Anschlussinhabers zu entscheiden ist, beeinträchtigt wird;

(b) dazu geeignet sein, eine Entschädigung festzulegen, die der Rechteinhaber bzw. der Anbieter des Internetdienstes an den Anschlussinhaber zahlen muss, der durch ein solches Handeln oder Unterlassen beeinträchtigt wurde; und

(c) dazu geeignet sein, dem Rechteinhaber oder dem Internet-Diensteanbieter in vertretbarem Umfang eine Übernahme der dem Anschlussinhaber entstandenen Kosten aufzuerlegen, falls in der Sache zugunsten des Anschlussinhabers entschieden wurde.

(8) Das Regelwerk muss festlegen, dass die Befugnis zur Veranlassung einer Kostenübernahme gemäß Unterpunkt (7)(c) ausgeübt werden soll, um den Anschlussinhaber, der erfolgreich Widerspruch eingelegt hat, für entstandene Kosten zu entschädigen, sofern die Person, die über den Widerspruch entscheidet, nicht nach Abwägung aller Fakten und Umstände sowie des Verhaltens der Parteien vor und während des Verfahrens zu dem Schluss kommt, dass eine solche Entschädigung nicht gerechtfertigt wäre.

(9) Die Befugnisse der Person, die im Fall eines Technical Obligations Code zur Durchführung technischer Maßnahmen über die Widersprüche der Anschlussinhaber entscheidet, müssen unter anderem umfassen

(a) bei einem Widerspruch gegen eine tatsächlich angewandte oder in Erwägung gezogene technische Maßnahme

(i) die Befugnis, die Maßnahme zu bestätigen;

(ii) die Befugnis, die Maßnahme nicht anzu-

by means of the internet access service.

(7) The powers of the person determining subscriber appeals must include power—

(a) to secure so far as practicable that a subscriber is not prejudiced for the purposes of the copyright infringement provisions by an act or omission in respect of which an appeal is determined in favour of the subscriber;

(b) to make an award of compensation to be paid by a copyright owner or internet service provider to a subscriber affected by such an act or omission; and

(c) where the appeal is determined in favour of the subscriber, to direct the copyright owner or internet service provider to reimburse the reasonable costs of the subscriber.

(8) The code must provide that the power to direct the reimbursement of costs under subsection (7)(c) is to be exercised to award reasonable costs to a subscriber whose appeal is successful, unless the person deciding the appeal is satisfied that it would be unjust to give such a direction having regard to all the circumstances including the conduct of the parties before and during the proceedings.

(9) In the case of a technical obligations code, the powers of the person determining subscriber appeals must include power—

(a) on an appeal in relation to a technical measure or proposed technical measure—

(i) to confirm the measure;

(ii) to require the measure not to be taken

ordnen oder zurückzuziehen;

(iii) die Befugnis, eine technische Maßnahme durch eine andere, für den Anbieter des Internetdienstes durchführbare Maßnahme zu ersetzen;

(b) die Ausübung der vorstehend in den Unterpunkten (a)(ii) oder (iii) genannten Befugnisse, für den Fall dass ein Widerspruch nicht aufrecht erhalten werden kann, die entscheidungsbefugte Person jedoch davon überzeugt ist, dass außergewöhnliche Umstände vorliegen, die eine Ausübung dieser Befugnisse rechtfertigen;

(c) die Einleitung von Schritten, die auch die OFCOM ergreifen könnte in Bezug auf das Handeln oder Unterlassen, welches zu der Anwendung der technischen Maßnahme geführt hat; und

(d) Entscheidungen über die Bestätigung einer technischen Maßnahme bzw. aller anderen Angelegenheiten im Zusammenhang mit einer solchen Entscheidung an die OFCOM zu verweisen.

(10) Im Fall eines Technical Obligations Code müssen folgende Bestimmungen enthalten sein:

(a) die Möglichkeit zur Anfechtung eines Widerspruchsbescheides, vor dem First-tier Tribunal, für den Fall dass die Entscheidung auf einem Tatsachenfehler beruht, rechtsfehlerhaft oder unbillig ist;

(b) dem First-tier Tribunal müssen für den Fall einer Anrufung Befugnisse nach den Punkten (7) und (9) eingeräumt werden; und

(c) eine Bestimmung zur Erstattung der Kosten wie durch das Tribunal zuerkannt;

(11) Im Fall eines Technical Obligations Code müssen Bestimmungen enthalten sein, die sicherstellen, dass die technische Maßnahme nicht gegen den Anschlussinhaber eingesetzt wird, bis

(a) die Widerspruchsfrist oder für die Frist zur weiteren Beschwerde zum First-tier Tribunal bezüglich der anzuwendenden Maßnahme abgelaufen ist (bzw. der Anschlussinhaber auf Rechtsbehelfe verzichtet hat); und

(b) derartige Widersprüche bzw. weitere Beschwerden des Nutzers entschieden, abgelehnt oder anderweitig abgewehrt wurden.“

or to be withdrawn;

(iii) to substitute any other technical measure that the internet service provider has power to take;

(b) to exercise the power mentioned in paragraph (a)(ii) or (iii) where an appeal is not upheld but the person determining it is satisfied that there are exceptional circumstances that justify the exercise of the power;

(c) to take any steps that OFCOM could take in relation to the act or omission giving rise to the technical measure; and

(d) to remit the decision whether to confirm the technical measure, or any matter relating to that decision, to OFCOM.

(10) In the case of a technical obligations code, the code must make provision—

(a) enabling a determination of a subscriber appeal to be appealed to the First-tier Tribunal, including on grounds that it was based on an error of fact, wrong in law or unreasonable;

(b) giving the First-tier Tribunal, in relation to an appeal to it, the powers mentioned in subsections (7) and (9); and

(c) in relation to recovery of costs awarded by the Tribunal.

(11) In the case of a technical obligations code, the code must include provision to secure that a technical measure is not taken against a subscriber until—

(a) the period for bringing a subscriber appeal, or any further appeal to the First-tier Tribunal, in relation to the proposed measure has ended (or the subscriber has waived the right to appeal); and

(b) any such subscriber appeal or further appeal has been determined, abandoned or otherwise disposed of.”

14 Durchsetzung der Verpflichtungen

Im Anschluss an Artikel 124K des Communications Act 2003 einfügen –

„124L Durchsetzung der Verpflichtungen

(1) Die Abschnitte 94 bis 96 finden bei einer Zuwiderhandlung gegen die grundlegenden Verpflichtungen, gegen die Verpflichtung zur Durchführung einer technischen Maßnahme oder gegen eine Verpflichtung aus Abschnitt 124G(6) ebenso Anwendung wie bei Nichtbeachtung einer Bedingung aus Abschnitt 45.

(2) Die in Abschnitt 96 festgelegte und in diesem Abschnitt angewendete Geldbuße darf £250.000 nicht überschreiten und wird von der OFCOM festgelegt je nach

(a) Angemessenheit; und
(b) Verhältnismäßigkeit in Hinblick auf den begangenen Verstoß.

(3) Bei dieser Entscheidung muss die OFCOM folgende Punkte berücksichtigen:

(a) sämtliche Einwände, die der OFCOM vorliegen, seitens des Internetdienst-Anbieters oder Rechteinhabers, gegen den eine Geldbuße verhängt werden soll;

(b) alle Maßnahmen, die ein Anbieter oder Rechteinhaber ergriffen hat, um den Verpflichtungen nachzukommen, gegen die ihm gemäß Abschnitt 94 (wie angewandt) Verstöße gemeldet wurden; und

(c) alle Maßnahmen, die der Anbieter oder Rechteinhaber ergriffen hat, um die Auswirkungen dieser Verstöße zu begrenzen oder zu beseitigen.

(4) Der Secretary of State kann diesen Abschnitt durch Verfügung dahingehend erweitern, dass eine andere Höchststrafe für den in Punkt (2) festgelegten Zeitraum gelten soll;

(5) Es darf keine Verfügung über eine Änderung der Bestimmung nach Punkt (4) ergehen, bis dem Parlament ein Entwurf für die Verfügung vorgelegt wurde und dieser durch einen Beschluss beider Kammern genehmigt wurde.“

14 Enforcement of obligations

After section 124K of the Communications Act 2003 insert—

“124L Enforcement of obligations

(1) Sections 94 to 96 apply in relation to a contravention of an initial obligation or a technical obligation, or a contravention of an obligation under section 124G(6), as they apply in relation to a contravention of a condition set out under section 45.

(2) The amount of the penalty imposed under section 96 as applied by this section is to be such amount not exceeding £250,000 as OFCOM determine to be—

(a) appropriate; and
(b) proportionate to the contravention in respect of which it is imposed.

(3) In making that determination OFCOM must have regard to—

(a) any representations made to them by the internet service provider or copyright owner on whom the penalty is imposed;

(b) any steps taken by the provider or owner towards complying with the obligations contraventions of which have been notified to the provider or owner under section 94 (as applied); and

(c) any steps taken by the provider or owner for remedying the consequences of those contraventions.

(4) The Secretary of State may by order amend this section so as to substitute a different maximum penalty for the maximum penalty for the time being specified in subsection (2).

(5) No order is to be made containing provision authorised by subsection (4) unless a draft of the order has been laid before Parliament and approved by a resolution of each House.”

15 Aufteilung der Kosten

Im Anschluss an Artikel 124L des Communications Act 2003 einfügen –

„124M Aufteilung der Kosten

(1) Der Secretary of State kann per Verfügung eine Regelung betreffend die Übernahme von Kosten festlegen, die bei der Durchsetzung der Bestimmungen zum Schutz des Urheberrechts entstanden sind. Diese Regelung ist in den Initial Obligations Code bzw. in den Technical Obligations Code aufzunehmen.

(2) Eine Regelung nach Punkt (1) muss den Kostenanteil festlegen, der von einer oder mehreren der folgenden Parteien zu tragen ist:

- (a) vom Rechteinhaber;
- (b) vom Anbieter des Internetdienstes;
- (c) vom Anschlussinhaber (im Fall eines Widerspruchs durch den Anschlussinhaber und einer weiteren Beschwerde zum dem First-tier Tribunal).

(3) Die in Punkt (1) genannte Regelung muss insbesondere Folgendes regeln:

- (a) die anteilige Übernahme der dem Internet-Diensteanbieter entstandenen Kosten durch den Rechteinhaber;
- (b) die anteilige Übernahme der Kosten, die der OFCOM entstanden sind, durch den Rechteinhaber oder den Anbieter des Internetdienstes.

(4) Die in Punkt (1) genannte Regelung muss insbesondere

- (a) eine Regelung betreffend die Kosten enthalten, die anfallen, bevor die Regelung in den Initial Obligations Code bzw. in den Technical Obligations Code aufgenommen wird;
- (b) eine Regelung betreffend die Vorauszahlung der zu erwartenden Kosten (und die Rückzahlung zu viel gezahlter Beträge, falls die Kosten letztendlich geringer ausfallen als erwartet) beinhalten;
- (c) eine Regelung betreffend die Berechnung der Kosten und Kostenanteile enthalten;
- (d) weitere Regelungen dazu enthalten, wann und wie die Kostenanteile gezahlt werden müssen.

15 Sharing of costs

After section 124L of the Communications Act 2003 insert—

“124M Sharing of costs

(1) The Secretary of State may by order specify provision that must be included in an initial obligations code or a technical obligations code about payment of contributions towards costs incurred under the copyright infringement provisions.

(2) Any provision specified under subsection (1) must relate to payment of contributions by one or more of the following only—

- (a) copyright owners;
- (b) internet service providers;
- (c) in relation to a subscriber appeal or a further appeal by a subscriber to the First-tier Tribunal, the subscriber.

(3) Provision specified under subsection (1) may relate to, in particular—

- (a) payment by a copyright owner of a contribution towards the costs that an internet service provider incurs;
- (b) payment by a copyright owner or internet service provider of a contribution towards the costs that OFCOM incur.

(4) Provision specified under subsection (1) may include, in particular—

- (a) provision about costs incurred before the provision is included in an initial obligations code or a technical obligations code;
- (b) provision for payment in advance of expected costs (and for reimbursement of overpayments where the costs incurred are less than expected);
- (c) provision about how costs, expected costs or contributions must be calculated;
- (d) other provision about when and how contributions must be paid.

(5) Es darf keine Verfügung i. S. d. Abschnitts ergehen, bis dem Parlament ein Entwurf für die Verfügung vorgelegt wurde und dieser durch einen Beschluss beider Houses of Parliament genehmigt wurde.“

16 Auslegung und Folgebestimmungen

(1) Im Anschluss an Artikel 124M des Communications Act 2003 einfügen –

„124N Auslegung

In den Abschnitten 124A bis 124M sowie in diesem Abschnitt bezeichnet der Begriff „offenkundige Verletzung“, bezogen auf die Meldung eines Urheberrechtsverstoßes die Verletzung des Urheberrechts, die laut Meldung offenkundig stattgefunden hat; „Liste der gemeldeten Urheberrechtsverletzungen“ ist eine Liste i. S. d. Abschnitts 124B(2);

„Bestimmungen zur Verletzungen des Urheberrechts“ sind die Abschnitte 124A bis 124M sowie der vorliegende Abschnitt;

„Meldung einer Urheberrechtsverletzung“ ist eine Meldung i. S. d. Abschnitts 124A(3);

„Rechteinhaber“ bedeutet

(a) ein Inhaber von Urheberrechten im Sinne von Teil 1 des Copyright, Designs and Patents Act 1988 (siehe Paragraph 173 des Gesetzes); oder

(b) ein vom Rechteinhaber bevollmächtigter Stellvertreter;

„urheberrechtlich geschütztes Werk“ ist ein Werk im Sinne von Teil 1 des Copyright, Designs and Patents Act 1988 (siehe Paragraph 1(2) dieses Gesetzes);

„Grundlegende Verpflichtungen“ sind die Verpflichtungen i. S. d. Abschnitts 124C(1);

„Initial Obligations Code“ bedeutet ein Regelwerk i. S. d. Abschnitts 124A(2);

„Internet-Dienst“ ist einen elektronischen Kommunikationsdienst, der

(a) einem Anschlussinhaber zur Verfügung gestellt wird;

(b) vollständig oder überwiegend darin besteht, einen Zugang zum Internet bereitzustellen; und

(c) dem Anschlussinhaber eine oder mehre-

(5) No order is to be made under this section unless a draft of the order has been laid before Parliament and approved by a resolution of each House.“

16 Interpretation and consequential provision

(1) After section 124M of the Communications Act 2003 insert—

“124N Interpretation

In sections 124A to 124M and this section— “apparent infringement”, in relation to a copyright infringement report, means the infringement of copyright that the report states appears to have taken place;

“copyright infringement list” has the meaning given in section 124B(2);

“copyright infringement provisions” means sections 124A to 124M and this section;

“copyright infringement report” has the meaning given in section 124A(3);

“copyright owner” means—

(a) a copyright owner within the meaning of Part 1 of the Copyright, Designs and Patents Act 1988 (see section 173 of that Act); or

(b) someone authorised by that person to act on the person’s behalf;

“copyright work” has the same meaning as in Part 1 of the Copyright, Designs and Patents Act 1988 (see section 1(2) of that Act);

“initial obligations” has the meaning given in section 124C(1);

“initial obligations code” has the meaning given in section 124A(2);

“internet access service” means an electronic communications service that—

(a) is provided to a subscriber;

(b) consists entirely or mainly of the provision of access to the internet; and

(c) includes the allocation of an IP address or IP addresses to the subscriber to enable

re IP-Adressen zuweist, um den Zugang zu ermöglichen;

„Internet-Dienstanbieter“/„Anbieter eines Internetdienstes“ bedeutet eine Person, die einen Internet-Dienst bereitstellt;

„IP-Adresse“ ist eine Internetprotokolladresse;

„Anschlussinhaber“, bezogen auf einen Internet-Zugangsdienst, ist eine Person, die (a) den Dienst im Rahmen eines Vertrages zwischen der Person und dem Anbieter des Dienstes nutzt; und

(b) den Dienst nicht als Kommunikationsanbieter nutzt;

„Widerspruch des Anschlussinhabers“ bedeutet

(a) in Bezug auf den Initial Obligations Code den Widerspruch des Nutzers aufgrund eines Widerspruchsgrundes, der im Regelwerk genannt ist und der sich bezieht auf

(i) die Meldung einer Urheberrechtsverletzung;

(ii) die Versendung eines Warnhinweises i. S. d. Abschnitts 124A(4);

(iii) die tatsächliche oder vorgeschlagene Eintragung in eine Liste über gemeldete Urheberrechtsverstöße; oder

(iv) jedes Handeln oder Unterlassen im Zusammenhang mit den grundlegenden Verpflichtungen oder dem Initial Obligations Code;

(b) in Bezug auf den Technical Obligations Code den Widerspruch eines Anschlussinhabers aufgrund eines Widerspruchsgrundes, der in dem Regelwerk genannt ist und der sich bezieht auf

(i) die geplante Anwendung einer technischen Maßnahme; oder

(ii) ein Handeln oder Unterlassen im Zusammenhang mit dem Technical Obligations Code oder einer technischen Verpflichtung;

„technische Maßnahme“ ist eine Maßnahme i. S. d. Abschnitts 124G(3);

„Verpflichtung zur Durchführung technischer Maßnahmen“ ist die Verpflichtung i. S. d. Abschnitts 124G(2);

„Regelwerk über die Verpflichtung zur Durchführung technischer Maßnahmen“ bedeutet das Regelwerk i. S. d. Abschnitts 124I;

that access;

“internet service provider” means a person who provides an internet access service;

“IP address” means an internet protocol address;

“subscriber”, in relation to an internet access service, means a person who—

(a) receives the service under an agreement between the person and the provider of the service; and

(b) does not receive it as a communications provider;

“subscriber appeal” means—

(a) in relation to an initial obligations code, an appeal by a subscriber on grounds specified in the code in relation to—

(i) the making of a copyright infringement report;

(ii) notification under section 124A(4);

(iii) the inclusion or proposed inclusion of an entry in a copyright infringement list; or

(iv) any other act or omission in relation to an initial obligation or an initial obligations code;

(b) in relation to a technical obligations code, an appeal by a subscriber on grounds specified in the code in relation to—

(i) the proposed taking of a technical measure; or

(ii) any other act or omission in relation to a technical obligation or a technical obligations code;

“technical measure” has the meaning given in section 124G(3);

“technical obligation” has the meaning given in section 124G(2);

“technical obligations code” means a code in force under section 124I.”

(2) In section 135(3) of that Act (information

(2) In Abschnitt 135(3) des Gesetzes (erforderliche Informationen zum Zweck der Funktion des Kapitels 1), nach Paragraph (i) einfügen:

„(ia) Erstellung einer Meldung gemäß 124F; (ib) die Ausführung einer Bewertung, die Einleitung von Schritten oder die Einreichung einer Meldung gemäß Abschnitt 124G;“.

(3) In Anhang 8 zu diesem Gesetz (Entscheidungen, gegen die kein Einspruch vor dem Competition Appeal Tribunal erhoben wurde), nach Paragraph 9 einfügen:

„9A Eine Entscheidung in Zusammenhang mit den Abschnitten 124A bis 124N oder in Zusammenhang mit einer Maßnahme die aus diesen Abschnitten folgt.“

17 Befugnis zum Erlass von gerichtlichen Verfügungen zur Sperrung von Speicherorten im Internet

(1) Der Secretary of State kann per Verordnung festlegen, dass ein Gericht die Sperrung eines Speicherorts im Internet anordnen kann, wenn es zu der Überzeugung gelangt, dass dieser für Verstöße gegen das Urheberrecht genutzt wurde, derzeit genutzt wird oder voraussichtlich genutzt werden wird.

(2) „Anordnung einer Sperrung“ bezeichnet in diesem Zusammenhang eine Verfügung, nach der ein Dienstanbieter verpflichtet wird, zu verhindern, dass sein Dienst genutzt wird, um Zugang zu einem Speicherort im Internet zu erhalten.

(3) Der Secretary of State darf keine Verordnung i. S. d. Abschnitts erlassen, bis zweifelsfrei feststeht,

(a) dass die Nutzung des Internets für Aktivitäten, die eine Urheberrechtsverletzung darstellen, erhebliche negative Auswirkungen auf Unternehmen oder Verbraucher hat,

(b) dass die Verordnung ein geeignetes Mittel ist, um diese Auswirkungen zu verhindern, und

(c) dass durch die Verordnung die nationale Sicherheit nicht gefährdet oder die Aufdeckung von Straftaten verhindert wird.

(4) Die Verordnung muss festlegen, dass ein Gericht erst dann eine Sperrung anordnen

required for purposes of Chapter 1 functions), after paragraph (i) insert—

“(ia) preparing a report under section 124F; (ib) carrying out an assessment, taking steps or providing a report under section 124G;“.

(3) In Schedule 8 to that Act (decisions not subject to appeal to the Competition Appeal Tribunal), after paragraph 9 insert—

“9A A decision relating to any of sections 124A to 124N or to anything done under them.”

17 Power to make provision about injunctions preventing access to locations on the internet

(1) The Secretary of State may by regulations make provision about the granting by a court of a blocking injunction in respect of a location on the internet which the court is satisfied has been, is being or is likely to be used for or in connection with an activity that infringes copyright.

(2) “Blocking injunction” means an injunction that requires a service provider to prevent its service being used to gain access to the location.

(3) The Secretary of State may not make regulations under this section unless satisfied that—

(a) the use of the internet for activities that infringe copyright is having a serious adverse effect on businesses or consumers,

(b) making the regulations is a proportionate way to address that effect, and

(c) making the regulations would not prejudice national security or the prevention or detection of crime.

(4) The regulations must provide that a court may not grant an injunction unless

darf, wenn es zu der Überzeugung gelangt ist, dass der Speicherort

(a) ein Speicherort ist, über den eine erhebliche Menge an geschütztem Material widerrechtlich erlangt wurde, derzeit erlangt wird oder voraussichtlich erlangt werden wird,

(b) ein Speicherort ist, an dem eine erhebliche Menge an geschütztem Material widerrechtlich zur Verfügung gestellt wurde, derzeit gestellt wird oder voraussichtlich zur Verfügung gestellt werden wird, oder

(c) ein Speicherort ist, der dazu genutzt wurde, derzeit genutzt wird oder wahrscheinlich in Zukunft dazu genutzt werden wird, Zugang zu einem Speicherort i. S. d. Unterpunkte (a) oder (b) zu erhalten.

(5) Die Verordnung muss festlegen, dass ein Gericht bei der Entscheidung über die Verhängung einer Sperre Folgendes berücksichtigen muss:

(a) alle Nachweise zu ergriffenen Maßnahmen des Internet-Diensteanbieters oder des Betreibers des Speicherorts zur Verhinderung von Verstößen gegen das Urheberrecht,

(b) alle Nachweise zu ergriffenen Maßnahmen des Rechteinhabers oder eines Inhabers von Lizenzrechten an dem qualifizierten Material, um einen legalen Zugang zu dem qualifizierten Material zu ermöglichen,

(c) sämtliche Einwände eines Minister of the Crown,

(d) die Frage, ob sich eine solche Verfügung in unverhältnismäßiger Weise auf die berechtigten Interessen Dritter auswirken würde, und

(b) die Wichtigkeit der freien Meinungsäußerung.

(6) Die Bestimmungen müssen festlegen, dass ein Gericht keine Sperrung anordnen darf, bis eine Benachrichtigung über die Beantragung einer solchen in der festgelegten Form übermittelt wurde an

(a) den Internet-Diensteanbieter und

(b) die Betreiber des Speicherorts im Internet.

(7) Die Verordnung muss außerdem

(a) eine Definition enthalten, wann ein Speicherort als ein Speicherort einzustufen ist, über den Zugriff auf einen anderen

satisfied that the location is—

(a) a location from which a substantial amount of material has been, is being or is likely to be obtained in infringement of copyright,

(b) a location at which a substantial amount of material has been, is being or is likely to be made available in infringement of copyright, or

(c) a location which has been, is being or is likely to be used to facilitate access to a location within paragraph (a) or (b).

(5) The regulations must provide that, in determining whether to grant an injunction, the court must take account of—

(a) any evidence presented of steps taken by the service provider, or by an operator of the location, to prevent infringement of copyright in the qualifying material,

(b) any evidence presented of steps taken by the copyright owner, or by a licensee of copyright in the qualifying material, to facilitate lawful access to the qualifying material,

(c) any representations made by a Minister of the Crown,

(d) whether the injunction would be likely to have a disproportionate effect on any person's legitimate interests, and

(e) the importance of freedom of expression.

(6) The regulations must provide that a court may not grant an injunction unless notice of the application for the injunction has been given, in such form and by such means as is specified in the regulations, to—

(a) the service provider, and

(b) operators of the location.

(7) The regulations may, in particular—

(a) make provision about when a location is, or is not, to be treated as being used to facilitate access to another location,

Speicherort erlangt wird,

(b) festlegen, dass die Benachrichtigung der Betreiber des Speicherorts über den Antrag auf Sperre durch Veröffentlichung i. S. d. Bestimmungen erfolgen soll,

(c) festlegen, dass ein Gericht keine Kostenübernahme durch den Internet-Dienstanbieter verfügen kann,

(d) verschiedene Regelungen für verschiedene Zwecke festlegen, und

(e) Nebenbestimmungen, ergänzende Bestimmungen, Folgebestimmungen, Übergangsbestimmungen, temporäre Bestimmungen oder Schutzbestimmungen festlegen.

(8) Die Verordnung kann

(a) Kapitel 6 des 1. Teils des Copyright, Designs and Patents Act 1988 abändern, und

(b) Folgebestimmungen zur Abänderung von Gesetzen und untergeordneten Gesetzen festlegen.

(9) Verordnungen i. S. d. Abschnitts dürfen ohne Zustimmung des Lord Chancellor keine Regelungen zum Verfahren vor einem Gericht in England oder Wales vorsehen.

(10) Die Verordnungen i. S. d. Abschnitts müssen durch ein Rechtsinstrument festgelegt werden.

(11) Ein Rechtsinstrument, das Verordnungen i. S. d. Abschnitts enthält, darf erst dann eingesetzt werden, wenn

(a) der Secretary of State den Anforderungen gemäß Abschnitt (18) Folge geleistet hat; und

(b) dem Parlament ein Entwurf für das Instrument vorgelegt wurde und dieser durch einen Beschluss beider Kammern genehmigt wurde.

(12) In diesem Abschnitt hat die Bezeichnung

„Rechteinhaber“ dieselbe Bedeutung wie in Teil 1 des Copyright, Designs and Patents Act 1988;

„Minister of the Crown“ dieselbe Bedeutung wie im Ministers of the Crown Act 1975;

„abändern“ auch die Bedeutung erweitern, widerrufen oder aufheben;

„Betreiber“ bezogen auf einen Internetstandort die Bedeutung einer Person, die die redaktionelle Kontrolle über die Inhalte hat, die über den Speicherort abrufbar sind;

„qualifiziertes Material“ in Bezug auf die

(b) provide that notice of an application for an injunction may be given to operators of a location by being published in accordance with the regulations,

(c) provide that a court may not make an order for costs against the service provider,

(d) make different provision for different purposes, and

(e) make incidental, supplementary, consequential, transitional, transitory or saving provision.

(8) The regulations may—

(a) modify Chapter 6 of Part 1 of the Copyright, Designs and Patents Act 1988, and

(b) make consequential provision modifying Acts and subordinate legislation.

(9) Regulations under this section may not include provision in respect of proceedings before a court in England and Wales without the consent of the Lord Chancellor.

(10) Regulations under this section must be made by statutory instrument.

(11) A statutory instrument containing regulations under this section may not be made unless—

(a) the Secretary of State has complied with section 18, and

(b) a draft of the instrument has been laid before and approved by a resolution of each House of Parliament.

(12) In this section—

“copyright owner” has the same meaning as in Part 1 of the Copyright, Designs and Patents Act 1988;

“Minister of the Crown” has the same meaning as in the Ministers of the Crown Act 1975;

“modify” includes amend, repeal or revoke;

“operator”, in relation to a location on the internet, means a person who has editorial control over material available at the location;

“qualifying material”, in relation to an injunction, means the material taken into

Anordnung einer Sperre die Bedeutung von Material, das vom Gericht zum Zwecke der Entscheidung über eine Verfügung gemäß Unterabschnitt (4) bewertet wird;

„Dienstanbieter“ dieselbe Bedeutung wie in Abschnitt 97A des Copyright, Designs and Patents Act 1988;

„untergeordnete Gesetze“ die gleiche Bedeutung wie im Interpretation Act 1978.

(13) Bei der Anwendung dieses Abschnitts in Schottland

sind „Kosten“ gleichbedeutend mit Aufwendungen;

ist „Verfügung“ gleichbedeutend mit Interdikt;

18 Beratung und parlamentarische Überprüfung

(1) Der Secretary of State muss im Vorfeld der Verordnung nach Abschnitt 17 folgende Gremien zu Rate ziehen:

(a) den Lord President of the Court of Session (Nordirland) und den Lord Chief Justice von Nordirland,

(b) Personen, die nach Auffassung des Secretary of State wahrscheinlich von der Verordnung betroffen sein werden (oder deren Vertreter), und

(c) andere Personen, nach Ermessen des Secretary of State.

(2) Wenn der Secretary of State nach Beratung gemäß Punkt (1) die Verabschiedung einer Verordnung nach Abschnitt 17 beantragt, muss er dem Parlament ein Dokument vorlegen, das

(a) den Antrag begründet und einen Entwurf für die Verordnung enthält;

(b) eine Begründung enthält, weshalb der Secretary of State von der Erfüllung der Bedingungen nach Unterpunkten 17(3)(a) bis (c) überzeugt ist, und

(c) eine Zusammenfassung der Einwände enthält, die während der Beratungen gemäß Abschnitt (1) erhoben wurden.

(3) Ab dem Tag, an dem das Dokument gemäß Punkt (2) dem Parlament vorgelegt wurde, darf der Secretary of State dem Parlament 60 Tage lang (die „60-Tage-Frist“)

account by the court for the purposes of provision made under subsection (4);

“service provider” has the same meaning as in section 97A of the Copyright, Designs and Patents Act 1988;

“subordinate legislation” has the same meaning as in the Interpretation Act 1978.

(13) In the application of this section to Scotland—

“costs” means expenses;

“injunction” means interdict.

18 Consultation and Parliamentary scrutiny

(1) Before making regulations under section 17 the Secretary of State must consult—

(a) the Lord President of the Court of Session and the Lord Chief Justice of Northern Ireland,

(b) the persons that the Secretary of State thinks likely to be affected by the regulations (or persons who represent such persons), and

(c) such other persons as the Secretary of State thinks fit.

(2) If, following the consultation under subsection (1), the Secretary of State proposes to make regulations under section 17, the Secretary of State must lay before Parliament a document that—

(a) explains the proposal and sets it out in the form of draft regulations,

(b) explains the reasons why the Secretary of State is satisfied in relation to the matters listed in section 17(3)(a) to (c), and

(c) contains a summary of any representations made during the consultation under subsection (1).

(3) During the period of 60 days beginning with the day on which the document was laid under subsection (2) (“the 60-day period”), the Secretary of State may not lay

keinen Verfügungsentwurf vorlegen, durch dessen Annahme sein Antrag wirksam würde (mit oder ohne Änderungen).

(4) Bei der Vorbereitung des Entwurfs nach Abschnitt 17, durch dessen Annahme der vorgenannte Antrag in Kraft gesetzt würde, muss der Secretary of State während der 60-Tage-Frist Folgendes berücksichtigen:

(a) sämtliche Einwände und
(b) Empfehlungen von Ausschüssen beider Houses of Parliament, die dem Parlament über diesen Verordnungsentwurf berichten.

(5) Legt der Minister dem Parlament einen Entwurf für ein Rechtsinstrument vor, durch dessen Annahme der vorgenannte Antrag in Kraft gesetzt würde (mit oder ohne Änderungen), muss er gegebenenfalls ein Dokument vorlegen, in dem alle Änderungen an dem Antrag, der dem Parlament gemäß Unterpunkt (2) vorgelegt wurde, erläutert werden.

(6) Bei der Bestimmung des Datums, an dem die 60-Tage-Frist abläuft, werden Zeiträume, in denen das Parlament aufgelöst oder vertagt ist oder in denen die Sitzungsperiode der Houses of Parliament länger als 4 Tage unterbrochen ist, nicht berücksichtigt.

...

before Parliament a draft statutory instrument containing regulations to give effect to the proposal (with or without modifications).

(4) In preparing draft regulations under section 17 to give effect to the proposal, the Secretary of State must have regard to any of the following that are made with regard to the draft regulations during the 60-day period—

(a) any representations, and
(b) any recommendations of a committee of either House of Parliament charged with reporting on the draft regulations.

(5) When laying before Parliament a draft statutory instrument containing regulations to give effect to the proposal (with or without modifications), the Secretary of State must also lay a document that explains any changes made to the proposal contained in the document laid before Parliament under subsection (2).

(6) In calculating the 60-day period, no account is to be taken of any time during which Parliament is dissolved or prorogued or during which either House is adjourned for more than 4 days.

...

Quellenverzeichnis

1. Literatur

- Adermon, Adrian / Liang, Che-Yuan**, Piracy, Music, and Movies: A Natural Experiment, 40452, Uppsala Center for Fiscal Studies, Department of Economics, Uppsala University.
- Adolphsen, Jens / Mayer, Dominik / Möller, Frederik**, Massenabmahnungen im Urheberrecht - Ein Geschäftsmodell auf dem Prüfstand, NJOZ 2010, 2395 ff.
- Bäcker, Kerstin**, Starkes Recht und schwache Durchsetzung, ZUM 2008, 391 ff.
- Beatson, Jack (etd.)**, Human Rights: Judicial Protection in the United Kingdom, 2008, Sweet & Maxwell.
- Blocman, Amélie**, Gesetz über das Urheberrecht und die verwandten Schutzrechte in der Informationsgesellschaft verabschiedet, IRIS 2006-7, 2006, Europäische Audiovisuelle Informationsstelle.
- Blocman, Amélie**, Verfassungsrat kritisiert Gesetz über Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft, IRIS 2006/8, 2006, Europäische Audiovisuelle Informationsstelle.
- Bohne, Daniel**, Zum Erfordernis eines gewerblichen Ausmaßes der Rechtsverletzung in § 101 Abs. 2 UrhG, CR 2010, 104 ff.
- Borges, Georg**, Pflichten und Haftung beim Betrieb privater WLAN, NJW 2010, 2624 ff.
- Brand, Oliver**, Grundfragen der Rechtsvergleichung - Ein Leitfadens für die Wahlfachprüfung, Jus 2003, 1082 ff.
- Breyer, Patrick**, Verkehrssicherungspflichten von Internetdiensten im Lichte der Grundrechte, MMR 2009, 14 ff.
- Cannie, Hannes**, Gesetzesentwurf für besseren Schutz kultureller Werke im Internet, IRIS 2011-5: 1/7, 2011, Europäische Audiovisuelle Informationsstelle.
- Cichon, Caroline**, LG Hamburg: Accessprovider hat keine zivilrechtlichen Filter- oder Sperrpflichten, GRUR-Prax 2010, 345.
- Clark, Robert / Shúilleabháin, Maire Ni**, Intellectual Property Law in Ireland, 2010.
- Czychowski, Christian / Nordemann, Jan-Bernd**, Vorratsdaten und Urheberrecht - Zulässige Nutzung gespeicherter Daten, NJW 2008, 3095 ff.
- Dörr, Dieter / Schwartmann, Rolf**, Medienrecht, 3. Aufl., Heidelberg, 2010.
- Dreier, Thomas / Schulze, Gernot**, Urheberrechtsgesetz. Kommentar, 3. Aufl., München, 2008.
- Durie, Robin**, Der englische Copyright, Designs and Patents Act von 1988, GRUR Int. 1990, 832 ff.
- Durner, Wolfgang**, Fernmeldegeheimnis und informationelle Selbstbestimmung als Schranken urheberrechtlicher Sperrverfügungen im Internet?, ZUM 2010, 833 ff.
- Eckhardt, Jens**, Anmerkung zum Urteil des LG Berlin vom 6.9.2007 – 23 S 3/07, K&R &, 2007, 601 f., K&R 2007, 602 ff.
- Ensthaler, Jürgen / Weidert, Stefan** (Hrsg.), Handbuch Urheberrecht und Internet, 2. Aufl., Frankfurt a. M., 2010.
- Ewert, Jonas / Hartz, Nikolaus**, Neue kostenrechtliche Herausforderungen bei der Abmahnung im Urheberrecht, MMR 2009, 84 ff.
- Faustmann, Jörg / Ramsperger, Gabriel**, Abmahnkosten im Urheberrecht – Zur Anwendbarkeit des § 97a Abs. 2 UrhG, MMR 2010, 664.
- Feldmann, Thorsten**, Die Unterlassungsverpflichtung des Access-Providers als Störer, K&R 2011, 225 ff.
- Fink, Udo / Cole, Marc / Keber, Tobias**, Europäisches und Internationales Medienrecht, Heidelberg, 2008.
- Fink, Udo / Schwartmann, Rolf / Cole, Marc / Keber, Tobias**, Europäisches und Internationales Medienrecht – Vorschriftensammlung, Heidelberg, 2007.
- Frey, Dieter**: Netzsperrern: Werden Access-Provider die neuen Gatekeeper des Rechts? In: MMR, 2009, 221.

- Fromm, Friedrich Karl / Nordemann, Wilhelm** (Begr.), Urheberrecht.Kommentar zum Urheberrechtsgesetz, zum Verlagsgesetz und zum Urheberrechtswahrnehmungsgesetz, 10. Aufl., Stuttgart, 2008.
- Frowein Jochen A. / Peukert, Wolfgang**, Europäische Menschenrechtskonvention, EMRK-Kommentar, 3. Aufl., Berlin, 2009.
- Gabriel /, Ulrich / Albrecht, Stefanie**, Filesharing-Dienste, Grundrechte und (k)eine Lösung?, ZUM 2010, 392 ff.
- Gabriel, Ulrich / Cornels, Lars C.**, Webtracking and Datenschutz – ein “hidden problem”, MMR 11/2008 S. XIV.
- Gelles, David / Edgecliffe-Johnson, Andrew**, Publishers rush to erect defence against piracy, Financial Times, vom 15.04.2011.
- Gietl, Andreas**, Störerhaftung aufgrund ungeschützter WLAN-Verbindung, ZUM 2007, 407.
- Gietl, Andreas / Manz, Reto**, Die IP-Adresse als Beweismittel im Zivilprozess, CR 2008, 810 ff.
- Gola, Peter / Schomerus, Rudolph**, Bundesdatenschutzgesetz, Kommentar, 10. Aufl., München, 2010.
- Grabitz, Eberhard / Hilf, Meinhard**, Das Recht der Europäischen Union, München, 40. Ergänzungslieferung – Stand Oktober 2009, München.
- Härting, Niko**, Internetrecht, 4. Aufl., Köln, 2010.
- Hennemann, Moritz**, Urheberrechtsdurchsetzung und Internet, Baden- Baden, 2011.
- Hoeren, Thomas**, Urheberrecht 2000 - Thesen für eine Reform des Urheberrechts, MMR, 2000, 3.
- Hoeren, Thomas**, Vorratsdaten und Urheberrecht – Keine Nutzung gespeicherter Daten, NJW 2008, 3099 ff.
- Hoeren, Thomas / Sieber, Ulrich** (Hrsg.), Handbuch Multimedia-Recht, Stand: August 2011 (29. Ergänzungslieferung), München.
- Hoffmann, Helmut**, Das Auskunftsverfahren nach § 101 Abs. 9 UrhG n.F., MMR 2009, 655 ff.
- Hofmann, Ruben A.**, Virtuelle Personal Video Recorder vor dem Aus? – Kritische Analyse der bisherigen Rechtsprechung zu virtuellen PVR, MMR, 2006, 793.
- Jarras, Hans / Pieroth, Bodo**, Grundgesetz für die Bundesrepublik Deutschland: GG, Kommentar, 11. Aufl., München, 2011.
- Jüngel, Marc / Geißler, Tim**, Der neue Auskunftsanspruch aus § 101 UrhG unter Berücksichtigung der bisherigen Rechtsprechung, MMR 2008, 787 ff.
- Karger, Michael**, Praktische Hinweise zum Parteivortrag nach der BGH-Entscheidung zur Störerhaftung des WLAN-Betreibers, GRUR- Prax 2010, 305.
- Kindt, Anne**, Grundrechtsschutz für Raubkopierer und Musikpiraten?, MMR 2009, 147 ff.
- Kirchhof, Paul**: Gesetzgebungsauftrag zum Schutz des geistigen Eigentums gegenüber modernen Vervielfältigungstechniken. Rechtswissenschaftliches Gutachten, Heidelberg, 1998.
- Kitz, Volker**, Rechtsdurchsetzung im geistigen Eigentum – die neuen Regeln, NJW 2008, 2374 ff.
- Kondziela, Andreas**, Staatsanwälte als Erfüllungsgehilfen der Musik- und Pornoindustrie?, MMR 2009, 295 ff.
- Kramer, Andreas**, Zivirechtlicher Auskunftsanspruch gegenüber Access-Provider. Verpflichtung zur Herausgabe der Nutzerdaten von Urheberrechtsverletzern unter Berücksichtigung der Enforcement-Richtlinie (RL 3004/48/EG), Diss. Hamburg, 2007).
- Kreutzer, Till**, Das Modell eines deutschen Urheberrechts und Regelungsalternativen, Baden- Baden, 2008.
- Krüger, Stefan / Maucher, Svenja- Ariane**, Ist die IP-Adresse wirklich ein personenbezogenes Datum? Ein falscher Trend mit großen Auswirkungen auf die Praxis, MMR, 2011, 433.
- Kühling, Jürgen / Seidel, Christian / Sivridis, Anastasios**: Datenschutzrecht, 1. Aufl., Stuttgart, 2008.
- Kuhr, Martin**, Verwertungsfenster im Wandel, IRIS plus 2008-4, 2008, Europäische Audiovisuelle Informationsstelle.
- Ladeur, Karl-Heinz**, Der Auskunftsanspruch aus § 101 UrhG und seine Durchsetzung Zivilrechtsanwendung ohne Methode und jenseits der Drittwirkung der Grundrechte?, NJOZ 2010, 1606 ff.

- Lampe, Ernst- Joachim** (Hrsg.), Zur Entwicklung von Rechtsbewusstsein, Berlin, 1997.
- Leupold, Andreas / Glossner, Silke** (Hrsg.), Münchener Anwaltshandbuch IT-Recht, 2. Aufl., München, 2011.
- Lindner, Brigitte**, Alternative Modelle zur Begegnung von Urheberrechtsverstößen im Internet, zusammenfassende Übersicht vom 25.11.2011.
- Loewenheim, Ulrich** (Hrsg.), Handbuch des Urheberrechts, 2. Aufl., München, 2010.
- Lutz, Stefan**, Verteidigungsstrategien bei Filesharing-Abmahnungen, VuR 2010, 337 ff.
- Maaßen, Stefan**: Urheberrechtlicher Auskunftsanspruch und Vorratsdatenspeicherung, MMR 2009, 511 ff.
- Malkus, Martin**, Harry Potter und die Abmahnung des Schreckens, MMR 2010, 382 ff.
- Mansala, Marja-Leena**: Torrent-Dateien, Filesharing und Urheberrecht im Fall Finreactor, IRIS 2010-7:1/104, 2010, Europäische Audiovisuelle Informationsstelle.
- Mantz, Reto**, Zur Schadensersatzpflicht und Störerhaftung von WLAN-Betreibern, MMR 2010, 568 ff.
- Maunz, Theodor / Dürig, Günter** (Begr.), Grundgesetz, Kommentar, 62. EL 2011, München.
- Meyerdierks, Per**, Sind IP-Adressen personenbezogene Daten?, MMR 2009, 8.
- Moos, Flemming**, Die Entwicklung des Datenschutzrechts im Jahr 2007, K&R 2008, 137 ff.
- Moos, Flemming / Gosche, Anna**, Datenspeicherung auf Zuruf, CR 2010, 499 ff.
- Musiol, Christian**, Erste Erfahrungen mit der Anwendung des § 101 IX UrhG – wann erreicht die Verletzung ein „gewerbliches Ausmaß“?, GRUR-RR, 2009, 1.
- Nordemann, Jan Bernd**, Störerhaftung für Urheberrechtsverletzungen – Welche konkreten Prüfpflichten haben Hostprovider (Contentprovider), CR 2010, 653 ff.
- Nümann, Peter / Mayer, Markus A.**, Rechtfertigung und Kritik von Massenabmahnungen gegen Urheberrechtsverletzungen in Filesharing-Netzwerken, ZUM 2010, 321 ff.
- Otten, Wolfgang**, Die auskunftsrechtliche Anordnung nach § 101 IX UrhG in der gerichtlichen Praxis, GRUR-RR 2009, 369 ff.
- Paal, Boris / Hennemann, Moritz**, Privates Medien- und Informationsrecht im Koalitionsvertrag, ZRP 2010, 40 ff.
- Pahlen-Brandt, Ingrid**, Zur Personenbezogenheit von IP-Adressen, K&R 2008, 288 ff.
- Pieroth, Bodo / Schlink, Bernhard**, Grundrechte Staatsrecht II, 26. Aufl., Heidelberg, 2010.
- Röhl, Andreas / Bosch, Christoph**, Musiktaschbörsen im Internet – Eine Analyse der aktuellen tatsächlichen und rechtlichen Entwicklungen, NJOZ, 2008, 1197.
- Rösler, Hannes**, Rechtsvergleichung als Erkenntnisinstrument in Wissenschaft, Praxis und Ausbildung (Teil 2), JuS 1999, 1186 ff.
- Rössel, Markus / Rössel, Martina**, Filterpflichten des Providers, CR 2005, 809 ff.
- Rüther, Bernd / Fischer, Christian**, Rechtstheorie. Begriff, Geltung und Anwendung des Rechts, 5. Aufl., München, 2010.
- Sacco, Rodolfo**, Einführung in die Rechtsvergleichung, 2. Aufl., Baden-Baden, 2011.
- Schirmacher, Frank**: Was passiert, wenn der Kopf nicht mehr mitkommt, in: Schwartmann (Hrsg.), Leben im Schwarm – Wie das Internet uns verändert, 2010.
- Schmidt, Heiner Christian**, Anmerkungen zur Diskussion um die Beschränkung des Akteneinsichtsrechts in den Filesharingverfahren, GRUR 2010, 673 ff.
- Schnabel, Christoph**, Porn not found – Die Arcor-Sperre, K&R 2008, 26 ff.
- Schricker, Gerhard / Loewenheim, Ulrich**, Urheberrecht, Kommentar, 4. Aufl., München, 2010.
- Schulz zur Wiesche, Jens**, Anmerkung zum Urteil des LG Hamburg vom 11.3.2009 – 308 O 75/09, MMR 2009, 570, MMR 2009, 574 f.
- Schwartmann, Rolf** (Hrsg.), Praxishandbuch Medien-, IT- und Urheberrecht, 2. Aufl., Heidelberg, 2011.
- Schwartmann, Rolf**, Filesharing, Sharehosting & Co., K&R Beihefter 2/2011.

- Schwartzmann, Rolf**, Europäischer Grundrechtsschutz nach dem Verfassungsvertrag, Archiv des Völkerrechts AVR (43), 2005, 129 ff.
- Schwartzmann, Rolf**, Meins bleibt Meins, in: Müller, Reinhard, Staat und Recht, 100 Beiträge aus der F.A.Z.-Rubrik >Staat und Recht<, Frankfurt, 2011, S. 386.
- Schwartzmann, Rolf**: Private im Wirtschaftsvölkerrecht, Tübingen, 2005.
- Schwartzmann, Rolf / Kocks, Sebastian**, Haftung für den Missbrauch offener WLAN-Anschlüsse, K&R 2010, 433 ff.
- Schwartzmann, Rolf / Pabst, Heinz-Joachim**, Umweltrecht, 2. Aufl. 2011.
- Schwarz, Matthias / Brauneck, Anja**, Verbesserung des Rechtsschutzes gegen Raubkopierer auf der Grundlage der EU- Enforcement- Richtlinie und deren Umsetzung in deutsches Recht, ZUM 2006, 701.
- Seifert, Fedor**, Postmortaler Schutz des Persönlichkeitsrechts und Schadensersatz – Zugleich ein Streifzug durch die Geschichte des allgemeinen Persönlichkeitsrechts, NJW 1999, 1889 ff.
- Seith, Sebastian**, Wie kommt der Urheber zu seinem Recht? Heidelberg, 2003.
- Simitis, Spiros** (Hrsg.), Bundesdatenschutzgesetz, 7. Aufl., Baden- Baden, 2011.
- Sollmecke, Christian**: Rechtliche Beurteilung der Nutzung von Musiktaschbörsen, In: K&R- Kommunikation und Recht, 2007, Verlag Recht und Wirtschaft.
- Solmecke, Christian**, Anmerkung zu LG Mannheim, Urteil vom 29.9.2006 - 7 O 76/06, MMR 2007, 267, MMR 2007, 268 f.
- Solmecke, Christian / Dierking, Laura**, Die Rechtsmissbräuchlichkeit von Abmahnungen, MMR 2009, 727 ff.
- Sommermann, Karl- Peter**, Die Bedeutung der Rechtsvergleichung für die Fortentwicklung des Staats- und Verwaltungsrechts in Europa, DöV, 1999, 1019 ff.
- Spindler, Gerald**, Der Auskunftsanspruch gegen Verletzer und Dritte im Urheberrecht nach neuem Recht, ZUM 2008, 640 ff.
- Spindler, Gerald / Schuster, Fabian**, Recht der elektronischen Medien. Kommentar, 2. Auflage, München, 2011.
- Spittgerber, Andreas / Klytta, Joanna**, Auskunftsansprüche gegen InternetproviderIn, K&R 2007, 78 ff.
- Stang, Felix / Hühner, Sebastian**, Haftung des Anschlussinhabers für fremde Rechtsverletzungen beim Betrieb eines ungesicherten WLAN- Funknetzes, GRUR-RR 2008, 273 ff.
- Taeger, Jürgen / Gabel, Detlev**, Kommentar zum BDSG und den einschlägigen Vorschriften des TMG und TKG, Frankfurt a.M., 2010.
- Tyra, Frank**, Ausgewählte Probleme aus der Abmahnpraxis bei Privatnutzungen in Musiktaschsystemen, ZUM 2009, 934 ff.
- Uerpmann- Witzack, Robert**, Das Anti- Counterfeiting Trade Agreement (ACTA) als Prüfstein für die Demokratie in Europa, Archiv des Völkerrechts AVR (43), 2011, 103 ff.
- van Eimeren, Birgit / Frees, Beate**, Drei von vier Deutschen im Netz – ein Ende des digitalen Grabens in Sicht?, Ergebnisse der ARD/ZDF-Onlinestudie 2011, Media Perspektiven 7-7/2011, S. 334.
- v. Zimmermann, Georg**, Recording-Software für Internetradios, MMR 2007, 553 ff.
- Venzke, Sven**, Die Personenbezogenheit der IP-Adresse – Lange diskutiert und immer noch umstritten?, ZD 2011, 114 ff.
- Volkman, Christian**, Verkehrspflichten für Internet-Provider, CR 2008, 232 ff.
- Wandtke, Artur-Axel / Bullinger, Winfried**, Praxiskommentar zum Urheberrecht, , 3. Aufl., München, 2009.
- Waldfoegel, Joel**, Bye, Bye, Miss American Pie? The Supply of New Recorded Music since Napster, The Carlson School and Department of Economics, University of Minnesota and NBER, January 3, 2011.
- Wehr, Christina / Ujjica, Matei**, „Alles muss raus!“, MMR 2010, 667 ff.
- Welp, Kai**, Die Auskunftspflicht von Access-Providern nach dem Urheberrechtsgesetz, 2009.
- Werner, Marcus / Jaeger, Henning**, AnwaltFormulare EDV- und Internetrecht, Bonn, 2007.

- Widmaier, Gunter** (Hrsg.), Münchener Anwalts Handbuch Strafverteidigung, 1. Aufl., München, 2006.
- Wilhelmi, Rüdiger**, Das gewerbliche Ausmaß als Voraussetzung der Auskunftsansprüche nach dem Durchsetzungsgesetz, ZUM, 2008, 942.
- Wilmer, Thomas**, Überspannte Prüfpflichten für Host-Provider?, NJW 2008, 1845 ff.
- Zweigert, Konrad / Kötz, Hein**, Einführung in die Rechtsvergleichung auf dem Gebiete des Privatrechts, 3. Aufl., Tübingen, 1996.

2. Studien*

- Adermon, Adrian / Liang, Che Yuan**, Universität Uppsala, Piracy, Music, and Movies: A Natural Experiment, Oktober 2010.
- The British Recorded Music Industry (BPI)**, Digital Music Nation 2010 – The UK's legal and illegal digital music landscape, December 2010.
- Bundesverband der Dienstleistungswirtschaft (BDWi), Interessenverband des Video- und Medienfachhandels in Deutschland (iVD), WEB-Guard Verein zur Förderung der Rechte im Internet e. V.**, Internet-Report I/2011.
- Bundesverband der Dienstleistungswirtschaft (BDWi), Interessenverband des Video- und Medienfachhandels in Deutschland (iVD), WEB-Guard Verein zur Förderung der Rechte im Internet e. V.**, Internet-Report II/2011.
- Bundesverband der Musikindustrie (BVMI)**, Musikindustrie in Zahlen 2010, April 2011.
- Bundesministerium für Wirtschaft und Technologie (BMWi)**, Forschungsbericht Nr. 577, Gesamtwirtschaftliche Perspektiven der Kultur- und Kreativwirtschaft in Deutschland, Februar 2009.
- Bundesministerium für Wirtschaft und Technologie (BMWi)**, Forschungsbericht Nr. 594, Monitoring zu wirtschaftlichen Eckdaten der Kultur und Kreativwirtschaft 2009, Dezember 2010.
- Bundesministeriums für Wirtschaft und Technologie (BMWi)**, Bericht zum Breitbandatlas 2010, Teil 1, 2010.
- Bundesministerium für Wirtschaft und Technologie (BMWi) / TNS Infratest Business Intelligence**, Monitoring-Report Deutschland Digital, Der IKT-Standort im internationalen Vergleich 2010.
- Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM)**, Symposium: Piraterie auf Informationsmärkten, Internetpiraterie aus Sicht der ITK-Industrie, 29. Oktober 2010.
- Business Software Alliance (BSA)**, Eighth Annual BSA Global Software 2010 Piracy Study, Mai 2011.
- Cicso Systems, Inc.**, Visual Networking Index: Forecast and Methodology, 2010-2015, Juni 2011.
- Departement for Culture, Media and Sport (dcms)**, Next Steps for implementation of the Digital Economy Act, August 2011.
- Department for Business, Innovation and Skills (BIS) / Departement for Culture, Media and Sport (dcms)**, Digital Britain – Final Report, Juni 2009.
- Department for Business, Innovation and Skills (BIS) / Departement for Culture, Media and Sport (dcms) / Intellectual Property Office**, Impact Assessments for the Digital Economy Act 2010, April 2010.
- Economic Consulting**, The Costs and Benefits to ISPs of Proposed Measures to Curb Illegal File Sharing, Dezember 2009.
- Envisional**, im Auftrag von NBC Universal, Techniacal report: An Estimate of Infringing Use of the Internet, Januar 2011.
- US Government Accountability Office (GAO)**, Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods, GAO-10-423, April 2010.

* Siehe auch Internetquellen mit weiteren Studien.

- GfK (Gesellschaft für Konsumforschung), im Auftrag des Bundesverbandes der Musikindustrie e.V. in Zusammenarbeit mit der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e.V. und dem Börsenverein des Deutschen Buchhandels:** Studie zur digitalen Content- Nutzung (DCN- Studie für die Jahre 2005- 2010: Brennerstudien) 2011, August 2011.
- GfK (Gesellschaft für Konsumforschung), im Auftrag des Bundesverbandes der Musikindustrie e.V.:** Brenner-Studie 2010, Januar 2010.
- Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e. V. (GVU),** Jahresbericht 2009, Oktober 2010.
- Hargreaves, Ian,** Digital Opportunity- A Review of Intellectual Property and Growth, Mai 2011.
- Harris Interactive / The British Recorded Music Industry (BPI),** Digital Music Survey, digital music nation 2010, 2010.
- Huygen, im Auftrag der niederländischen Regierung,** Ups and Downs: Economic and Cultural Effects of Filesharing on Music, Film and Games, 2009.
- Institut für Europäisches Medienrecht (EMR) in Zusammenarbeit mit der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel,** Die Zulässigkeit einer Kulturfltrate nach nationalem und europäischem Recht, Kurzgutachten vom 13.03.2009 im Auftrag von: Bundestagsfraktion BÜNDNIS 90/DIE GRÜNEN und der Fraktion der Grünen / Freie Europäische Allianz im Europäischen Parlament.
- International Chamber of Commerce (ICC), Business Action to Stop Counterfeiting and Piracy (BASCAP),** Estimating the global economic and social impacts of counterfeiting and piracy, a report commissioned by business action to stop counterfeiting and piracy, Februar 2011.
- International Chamber of Commerce (ICC), Business Action to Stop Counterfeiting and Piracy (BASCAP) / StrategyOne,** Research Report on Consumer Attitudes and Perceptions on Counterfeiting and Piracy (www.iccwbo.org/bascap), November 2009.
- International Data Corporation (IDC), Ipsos, im Auftrag des Business Software Alliance (BSA),** Eighth Annual BSA Global Software 2010 Piracy Study, Mai 2011.
- International Federation of the Phonographic Industry (IFPI),** Digital Music Report (DRM) 2011- Music at the touch of a button, 2011.
- International Federation of the Phonographic Industry (IFPI),** ISP Cooperation – Update vom Mai 2011, Mai 2011.
- Karaganis, Joe, im Auftrag des Social Science Research Council (SSRC),** Media Piracy in Emerging Economies, 2011.
- Liebowitz, Stan J. (ed.):** Testing File-Sharing's Impact by Examining Record Sales in Cities, CAPRI Publication 05-02.
- MidemNet / Music Matters / Synovate:** Global Music Study – An exclusive MidemNet/ Music Matters survey into music consumption around the world, Januar 2010.
- Mundelius, Marco,** Friedrich Ebert Stiftung, Schriftenreihe Moderne Industriepolitik 4/2009: Braucht die Kultur- und Kreativwirtschaft eine industriepolitische Förderung?, 2009.
- NERA Economic Consulting,** The Costs and Benefits to ISPs of Proposed Measures to Curb Illegal File Sharing, Dezember 2009.
- The Nielsen Company, im Auftrag von Midem,** The Hyper-Fragmented World of Music: Marketing considerations and revenue maximisation, März 2011.
- Oberholzer- Gee, Felix / Strumpf, Koleman,** Harvard Business School, File Sharing and Copyright, Working Paper 09-132, Mai 2009.
- Opinionway, rapport au premier ministre: Pratiques et attentes des internautes: la consommation de contenus culturels sur Internet, septembre 2009.**
- TERA Consultants, im Auftrag der Internationalen Handelskammer (ICC) / Business Action to Stop Counterfeiting and Piracy (BASCAP),** Aufbau einer digitalen Wirtschaft: Die Bedeutung der Sicherung von Arbeitsplätzen in der Kreativwirtschaft der europäischen Union, März 2010.
- TNS Infratest, im Auftrag von D21, (N)ONLINER Atlas 2011,** Eine Topographie des digitalen Grabens durch Deutschland, Juli 2011.

Verband unabhängiger Musikunternehmen e.V. (VUT), Stellungnahme des VUT zu den Fragen zur öffentlichen Anhörung Urheberrecht der Enquete-Kommission Internet und digitale Gesellschaft am 29.11.2010, Januar 2011.

Waldfogel, Joel / Rob, Rafael, Piracy on the High C's: Music Downloading, Sales Displacement, and Social Welfare in a Sample of College Students, Oktober 2004.

Wiggin & Entertainment Media Research, 2008, Digital Entertainment Survey, 2008.

3. Dokumente aus Internetquellen

Amendements déposée par Richard Miller/François Bellot, Document législatif n° 5-741/2, abrufbar unter: <http://www.senate.be/www/?Mlval=/publications/viewPub.html&COLL=S&LEG=5&NR=741&VOLGNR=2&LANG=fr> (Stand: 19.12.2011).

Anderson, Nate, Major ISPs agree to „six strikes“ copyright enforcement plan vom 7.7.2011, abrufbar unter: <http://arstechnica.com/tech-policy/news/2011/07/major-isps-agree-to-six-strikes-copyright-enforcement-plan.ars> (Stand: 19.12.2011).

ARD/ZDF-Onlinestudie 2011, abrufbar unter: <http://www.ard-zdf-onlinestudie.de/index.php?id=onlinenutzung00> (Stand: 19.12.2011).

Association of American Publishers, February 2011 sales report, abrufbar unter: www.publishers.org/press/30 (Stand: 19.12.2011).

Auftrag der Ministerin für Kultur und Kommunikation an Denis Olivennes, abrufbar unter: <http://www.culture.gouv.fr/culture/actualites/index-olivennes231107.htm> (Stand: 19.12.2011).

Begründung zum Entwurf eines Gesetzes über die Verbreitung und den Schutz schöpferischer Inhalte im Internet, S. 3, abrufbar unter: <http://www.culture.gouv.fr/culture/actualites/dossiers/internet-creation08/6%20-%20Projet%20de%20loi.pdf> (Stand: 19.12.2011).

Bericht über die Durchsetzung von Rechten des geistigen Eigentums im Binnenmarkt (2009/2178 (INI)) v. 3.6.2010, Berichterstatlerin: Marielle Gallo, abrufbar unter: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/juri/pr/801/801322/801322de.pdf (Stand: 19.12.2011).

Bericht zum Breitbandatlas 2010 des Bundesministeriums für Wirtschaft und Technologie, Teil 1, S. 5. Abrufbar unter: <http://www.zukunft-breitband.de/Dateien/BBA/PDF/breitbandatlas-bericht-2010-teil-1,property=pdf,bereich=bba,sprache=de,rwb=true.pdf> (Stand: 19.12.2011).

BIU, Marktzahlen, abrufbar unter: <http://www.biu-online.de/de/fakten/marktzahlen.html> (Stand: 19.12.2011).

Blog: File- Sharers To Recieve Warning Letters, But No 3 Strikes (enigmax), veröffentlicht am 2.11.2010 abrufbar unter: <http://torrentfreak.com/file-sharers-to-receive-warning-letters-but-no-3-strikes-101102/> (Stand: 19.12.2011).

Blog: Ireland Set To Force ISPs To Disconnect Pirates (enigmax), veröffentlicht am 21.6.2011, abrufbar unter: <http://torrentfreak.com/ireland-set-to-force-isps-to-disconnect-pirates-110621/> (Stand: 19.12.2011).

Blog: Irish Government Wants File- Sharing Compromise, Or Legislation Will Follow (enigmax), veröffentlicht am 15.11.2010, abrufbar unter: <http://torrentfreak.com/irish-government-wants-file-sharing-compromise-or-legislation-will-follow-101115/> (Stand: 19.12.2011).

Blog: IRMA to pursue and prosecute 23 people for illegally sharing music online (UnaRocks), veröffentlicht am 07.06.2007, abrufbar unter: <http://unarocks.blogspot.com/2007/06/irma-to-pursue-and-prosecute-23-people.html> (Stand: 19.12.2011).

Blog: ISP 3 Strikes Anti- Piracy Strategy Rewarded By Big Four Music Service (enigmax), veröffentlicht am 08.12.2010, abrufbar unter: <http://torrentfreak.com/isp-3-strikes-anti-piracy-strategy-rewarded-by-big-four-music-service-101208/> (Stand: 19.12.2011).

- Blog: ISP CEO Slams Copyright Law and Outdated Business Models (enigmax), veröffentlicht am 15.8.2011**, abrufbar unter: <http://torrentfreak.com/isp-ceo-slams-copyright-law-and-outdated-business-models-110815/> (Stand: 19.12.2011).
- Blog: ISP Wrongfully Sent 300 'First Strike' Letters To Innocents (enigmax), veröffentlicht am 17.6.2011**, abrufbar unter: <http://torrentfreak.com/isp-wrongfully-sent-300-first-strike-letters-to-innocents-110617/> (Stand: 19.12.2011).
- Blog: Müller, Klaus: Eircom Musikservice soll Three- Strikes relativieren, veröffentlicht am 12.12.2010**, abrufbar unter: <http://www.gulli.com/news/14875-eircom-musikservice-soll-three-strikes-relativieren-2010-12-12> (Stand: 19.12.2011).
- Blog: Urheberrecht: Kanadische Regierung plant enge Kooperation von Providern und Rechteinhabern (sac), veröffentlicht am 06.10.2011**, abrufbar unter: <http://unurl.org/eEV> (Stand: 19.12.2011).
- Bundesministerium für Justiz: Berliner Rede zum Urheberrecht**, abrufbar unter: www.bmj.de/SharedDocs/Reden/DE/2010/20100614_Berliner_Rede_zum_Urheberrecht.html (Stand: 19.12.2011).
- BMW, Schlaglichter der Wirtschaftspolitik, Monatsbericht Oktober 2009, 01.10.2009**, abrufbar unter: <http://www.bmw.de/BMWi/Navigation/Wirtschaft/Branchenfokus/kultur-kreativwirtschaft,did=315898.html?view=renderPrint> (Stand: 19.12.2011).
- Bornkamm, Den Aderlass stoppen; Interview mit dem Kölner Stadt-Anzeiger v. 3.11.2011**, abrufbar unter: <http://www.ksta.de/html/artikel/1320057515791.shtml> (Stand: 19.12.2011).
- Briefing Note on arrangement between Eircom and the Irish Record Music Association (IRMA) with regard to Copyright Infringement, March 2009**, abrufbar unter: <http://www.scribd.com/doc/13630351/Eircom-Irma-Briefing-Note-March-2009> (Stand: 19.12.2011).
- Cadman, Richard / Dineen, Chris, Price and Income Elasticity of Demand for Broadband Subscriptions: A Cross-Sectional Model of OECD Countries, 07.02.2008**, abrufbar unter: www.spcnetwork.co.uk/uploads/Broadband_Elasticity_Paper_2008.pdf (Stand: 19.12.2011).
- Consultation on the Review of the Copyright and Related Rights Act 2000**, abrufbar unter: http://www.djei.ie/science/ipr/copyright_review_2011.htm (Stand: 19.12.2011).
- Consumer Focus, Consumer Focus and the Citizens Advice response to notification of Digital Economy Act cost sharing order, October 2011**, abrufbar unter: <http://www.consumerfocus.org.uk/files/2010/10/Consumer-Focus-and-Citizens-Advice-response-to-notification-of-Digital-Economy-Act-cost-sharing-order.pdf> (Stand: 19.12.2011).
- Consumer Focus, Outdated copyright law confuses consumers, 24.2.2010**, abrufbar unter: <http://www.consumerfocus.org.uk/news/outdated-copyright-law-confuses-consumers> (Stand: 19.12.2011).
- Copyright Information AND Anti-Piracy Centre In Finland**, abrufbar unter: <http://antipiracy.fi/inenglish/> (Stand: 19.12.2011).
- Court Orders ISPs To Disconnect File- Sharers (enigmax), veröffentlicht am 29.06.2011**, abrufbar unter: <http://torrentfreak.com/court-orders-isps-to-disconnect-file-sharers-110629/> (Stand: 19.12.2011).
- Danaher, Brett / Michael D. Smith / Telang, Rahul / Chen, Siwen, The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France, Januar 2010**, abrufbar unter: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989240 (Stand: 24.01.2012).
- Dejean/Pénard/Suire, M@rsouin/CREM/Université de Rennes 1, Une première évaluation des effets de la loi Hadopi sur les pratiques des Internauteurs français, März 2010**, abrufbar unter: <http://www.marsouin.org/IMG/pdf/NoteHadopix.pdf> (Stand: 19.12.2011).
- Délibération de la CNIL n° 2011-022 du 20 janvier 2011**, abrufbar unter: http://electronlibre.info/IMG/pdf/AVIS_CNIL-HADOPI.pdf (Stand: 19.12.2011).
- Department for culture, media and sports, News: Ofcom to review aspects of Digital Economy Act, 1.02.2011**, abrufbar unter: http://www.culture.gov.uk/news/media_releases/7756.aspx (Stand: 19.12.2011).
- Digital and Physical Piracy in GB, Wave 5: November 2007**, abrufbar unter: http://www.ukfilmcouncil.org.uk/media/pdf/g/m/Ipsos_Piracy_UK_2007.pdf (Stand: 19.12.2011).

- Drücke, Florian / Süme, Oliver, Pro und Contra Warnhinweismodell, Ein Streit über den Umgang mit Filesharern**, abrufbar unter: <http://www.lto.de/de/html/nachrichten/5062/pro-und-contra-warnhinweismodell-ein-streit-ueber-den-umgang-mit-filesharern/> (Stand: 19.12.2011).
- Enquete-Kommission Internet und digitale Gesellschaft – Stellungnahme zu den rechtlichen Aspekten der Fragen der Fraktionen zur öffentlichen Anhörung Urheberrecht der Enquete-Kommission Internet und digitale Gesellschaft am 29. November 2010, S, 7**, abrufbar unter http://www.bundestag.de/internetenquete/dokumentation/Sitzungen/20101129/A-Drs__17_24_009_H-_Stellungnahme_Prof__Schwartmann.pdf (Stand: 19.12.2011).
- Europa Press releases RAPID, Europäische Kommission schlägt Verhandlungsrichtlinien für den Beitritt der Union zur Europäischen Menschenrechtskonvention (EMRK) vor, vom 17.3.2010**, abrufbar unter: <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/84&format=HTML&aged=0&language=DE&guiLanguage=en> (Stand: 19.12.2011).
- Hadopi, biens culturels et usages d'internet: pratiques et perceptions des internautes français (Erste Untersuchung der Hadopi, vorgelegt am 23.1.2011)**, abrufbar unter: <http://www.hadopi.fr/download/hadopiT0.pdf> (Stand: 19.12.2011).
- Hadopi, biens culturels et usages d'internet: pratiques et perceptions des internautes français, 2ème vague barométrique (Zweite Untersuchung der Hadopi, vorgelegt am 18.5.2011)**, abrufbar unter: http://www.hadopi.fr/sites/default/files/page/pdf/t1_etude_longue.pdf (Stand: 19.12.2011).
- Haupt, Johannes: Hollywood lanciert verschärftes Anti-Piraterie-Gesetz, vom 27.10.2011**, abrufbar unter: <http://heise.de/-1367627> (Stand: 19.12.2011).
- Heise online „T-Com speichert IP-Adressen nur noch sieben Tage“ veröffentlicht am 20.2.2007**, abrufbar unter: <http://www.heise.de/newsticker/meldung/T-Com-speichert-IP-Adressen-nur-noch-sieben-Tage-148387.html> (Stand: 19.12.2011).
- Huber, Peter M., Geistiges Eigentum und unionales Wettbewerbsrecht**, abrufbar unter: http://www.jura.uni-muenchen.de/personen/huber_peter/publikationen/geistigeseigentum.pdf (Stand: 19.12.2011).
- Institut für Urheberrecht und Medienrecht München, EuGH-Generalanwalt: Vorratsdaten-Richtlinie steht der Auskunftspflicht von Internetdienstleistern bei Urheberrechtsverletzung nicht entgegen, 25.11.2011**, abrufbar unter: <http://www.urheberrecht.org/news/4431/> (Stand: 19.12.2011).
- International Federation of the Phonographic Industry**, abrufbar unter: <http://www.ifpi.se/> (Stand: 19.12.2011).
- Interview in Promedia Heft 11, 2011, S. 5.**, abrufbar unter: <http://www.promedia-berlin.de/fileadmin/Archiv/2011/11/promedia201111-online01.pdf> (Stand: 19.12.2011).
- IPSOS**, abrufbar unter: <http://knowledgecenter.ipsos.de/docdetail.aspx?c=1043&did=2df20c44-f4c4-4e37-a746-e785070a02da> (Stand: 19.12.2011).
- IPSOS, Digital and Physical Piracy in GB, Wave 5: 5.11.2007**, abrufbar unter: http://www.ukfilmcouncil.org.uk/media/pdf/g/m/Ipsos_Piracy_UK_2007.pdf (Stand: 19.12.2011).
- IPSOS, Les Français face au téléchargement illégal de musique sur Internet - Les chiffres et résultats complets du sondage, 26.5.2008**, abrufbar unter: <http://www.ipsos.fr/ipsos-public-affairs/sondages/francais-face-au-telechargement-illegal-musique-sur-internet> (Stand: 19.12.2011).
- Karaganis (Ed.), Media piracy in emerging economies 2011, p. 33 f**, abrufbar unter: <http://piracy.ssrc.org> (Stand: 19.12.2011).
- Kennedy, John: Data commissioner investigating Eircom 'three strikes' system, veröffentlicht am 21.6.2011**, abrufbar unter: <http://www.siliconrepublic.com/comms/item/22309-data-commissioner-investiga/> (Stand: 19.12.2011).
- Kennedy, John: Radical copyright law reform to boost Ireland's digital economy?, veröffentlicht am 9.5.2011**, abrufbar unter: <http://www.siliconrepublic.com/new-media/item/21695-radical-copyright-law-refor/> (Stand: 19.12.2011).
- Kennedy, John: Telcos, ISPs anxious as digital copyright law changes loom, 22.6.2011**, abrufbar unter: <http://www.siliconrepublic.com/comms/item/22323-telcos-isps-anxious-as-dig/> (Stand: 19.12.2011).

- Krempf, Stefan: Kanada plant Warnhinweise an Copyright-Sünder, veröffentlicht am 5.10.2011**, abrufbar unter: <http://www.heise.de/newsticker/meldung/Kanada-plant-Warnhinweise-an-Copyright-Suender-1355412.html> (Stand: 19.12.2011).
- Leadbeater, Charles, The Digital Revolution: the Coming Crisis of the Creative Class**, abrufbar unter: <http://www.charlesleadbeater.net/cms/xstandard/Digital%20Britain%20Response.pdf> (Stand: 19.12.2011).
- Lee, New Zealand traffic down as „three strikes“ copyright law takes effect, vom 7.9.2011**, abrufbar unter: <http://arstechnica.com/tech-policy/news/2011/09/nz-traffic-down-as-three-strikes-copyright-law-takes-effect.ars> (Stand: 19.12.2011).
- McCallig, IRIS 2011-7:1/27** abrufbar unter: <http://merlin.obs.coe.int/iris/2011/7/article27.de.html> (Stand: 19.12.2011).
- McGonagle, IRIS 2006-4:15/26**, abrufbar unter: <http://merlin.obs.coe.int/iris/2006/4/article26.de.html> (Stand: 19.12.2011).
- McGonagle, IRIS 2010-6:1/34**, abrufbar unter: <http://merlin.obs.coe.int/iris/2010/6/article34.de.html> (Stand: 19.12.2011).
- McIntyre, Irish „Three Strikes“ System Investigated By Data Protection Commissioner, veröffentlicht am 15.6.2011**, abrufbar unter: <http://unurl.org/15> (Stand: 19.12.2011).
- Memorandum of Understanding vom 6.7.2011**, abrufbar unter: <http://www.copyrightinformation.org/sites/default/files/Memorandum%20of%20Understanding.pdf> (Stand: 19.12.2011).
- Müller, Klaus, Eircom Musikservice soll Three- Strikes relativieren, veröffentlicht am 12.12.2010**, abrufbar unter: <http://www.gulli.com/news/14875-eircom-musikservice-soll-three-strikes-relativieren-2010-12-12> (Stand: 19.12.2011).
- Müller, Klaus, Eircom: 300 falsche Three- Strikes- Warnungen versandt, veröffentlicht am 18.06.2011**, abrufbar unter: <http://www.gulli.com/news/16373-eircom-300-falsche-three-strikes-warnungen-versandt-2011-06-18> (Stand: 19.12.2011).
- Müller, Klaus: Finnland: Warnmails für Urheberrechtsverletzer, veröffentlicht am 3.11.2010**, abrufbar unter: <http://www.gulli.com/news/14632-finnland-warnmails-fuer-urheberrechtsverletzer-2010-11-03> (Stand: 19.12.2011).
- Parliament UK, Culture, Media and Sport Committee, News: Committee launches an inquiry into the Protection of Intellectual Property Rights Online, 10.11.2010**, abrufbar unter: <http://www.parliament.uk/business/committees/committees-a-z/commons-select/culture-media-and-sport-committee/news/committee-announces-new-inquiry/> (Stand: 19.12.2011).
- Pratiques et attentes des internautes: la consommation de contenus culturels sur Internet, September 2009**, abrufbar unter: http://lesrapports.ladocumentationfrancaise.fr/cgi-bin/brp/telestats.cgi?brp_ref=104000006&brp_file=0000.pdf.
- Pressemitteilung der CNIL vom 6.7.2011**, abrufbar unter: <http://www.cnil.fr/la-cnil/actu-cnil/article/article/dispositif-de-reponse-graduee-la-cnil-met-en-demeure-les-societes-de-perception-et-de-repa/> (Stand: 19.12.2011).
- Pressemitteilung der Recording Industry Association of America (RIAA) vom 6.7.2011**, abrufbar unter: http://www.riaa.com/newsitem.php?content_selector=newsandviews&news_month_filter=7&news_year_filter=2011&id=2DDC3887-A4D5-8D41-649D-6E4F7C5225A5 (Stand: 19.12.2011, nicht mehr!).
- Pressemitteilung von BVMI, Börsenverein und GfV zur Vorstellung der DCN-Studie 2011**, abrufbar unter: http://www.boersenverein.de/sixcms/media.php/976/110830_DCN_PM_FINAL.pdf (Stand: 19.12.2011).
- Projet de Loi favorisant la diffusion et la protection de la création sur internet, Exposé des motifs, a.a.O., S. 4 ; deutsche Fassung** abrufbar unter: <http://www.culture.gouv.fr/culture/actualites/communiq/albanel/creaallemand.htm> (Stand: 19.12.2011).
- Rapport d'activité 2010, Tätigkeitsbericht der Hadopi über ihre Aktivitäten in den ersten eineinhalb Jahren ihres Bestehens, September 2011**, abrufbar unter: <http://www.hadopi.fr/sites/default/files/page/pdf/rapport-d-activite-hadopi.pdf>, S. 8 (Stand: 19.12.2011).

SACEM, Les Français et la musique, Studie durchgeführt durch das Institut Opinionway, Januar 2011, abrufbar unter: http://www.sacem.fr/files/content/sites/fr/files/mediatheque/sacem/presse/etudes/etude%20sacem/sondage_francais_musique/sondage_les_francais_et_la_musique_2011.pdf (Stand: 19.12.2011).

Schwartzmann, Rolf, Provider müssen nicht auf ihre Kosten filtern und sperren, Legal Tribune Online v. 24.11.2011, abrufbar unter: <http://www.lto.de/de/html/nachrichten/4892/eugh-zum-urheberrechtsschutz-provider-muss-nicht-auf-ihre-kosten-filtern-und-sperren/> (Stand: 19.12.2011).

Sobiraj, Lars: Eircom kickt seit heute filesharer aus dem Internet, veröffentlicht am 24.5.2010, abrufbar unter: <http://www.gulli.com/news/13360-eircom-kickt-seit-heute-filesharer-aus-dem-internet-2010-05-24> (Stand: 19.12.2011).

Stellungnahme des Europäischen Datenschutzbeauftragten zu den laufenden Verhandlungen der Europäischen Union über ein Abkommen zur Bekämpfung von Produkt- und Markenpiraterie (Anti-Counterfeiting Trade Agreement, ACTA), (2010/C 147/01), Rz.: 6, v. 5.6.2010, abrufbar unter: <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:147:0001:0013:DE:PDF> (Stand: 19.12.2011).

Three Strikes, finnische Version (cen), veröffentlicht am 26.11.2010, abrufbar unter: <http://www.ip-notiz.de/three-strikes-finnische-version/2010/11/26/> (Stand: 19.12.2011).

Vorschläge der Rechteinhaber im Rahmen des Wirtschaftsdialogs für mehr Kooperation bei der Bekämpfung der Internetpiraterie im BMWi, Kurzfassung v. 3.5.2011, abrufbar unter: https://www.gema.de/fileadmin/user_upload/Presse/Publikationen/Kurzfassung_Dialogpapier.pdf (letzter Zugriff: 15.8.2011) (Stand: 19.12.2011).