

Inhaltsverzeichnis

Vorwort	V
Teil 1: Einleitung.....	1
A. Gang der Bearbeitung	2
B. Das Problem des Rechtsrahmens	6
I. Urheberrecht	7
II. Datenschutzrecht.....	10
Teil 2: Was ist Anonymität?.....	14
A. Identifizierbarkeit als Kriterium der (fehlenden) Anonymität	14
I. Identität	15
II. Sachverhalt	17
III. Zuordnung	17
IV. Sonderfall: Pseudonymität	18
B. Datenschutzrechtliche Anonymität	19
C. Tatsächliche und rechtliche Anonymität	20
D. Zusammenfassende Definition	22
Teil 3: Grundlagen für ein Recht auf Anonymität.....	23
A. Europarecht.....	24
I. EMRK	25
1. Ansatzpunkte.....	25
a) Schutz des Privatlebens	25
b) Recht auf Datenschutz.....	28
c) Schutz der Korrespondenz.....	30
2. Schranken.....	31

3. Bedeutung	32
II. Grundrechte-Charta.....	32
1. Schutz des Privatlebens	33
2. Schutz personenbezogener Daten.....	33
III. Sekundärrecht	33
1. Die EG-Datenschutzrichtlinie	34
2. Die EG-Telekommunikationsdatenschutzrichtlinie	35
3. Die EG-ePrivacy-Richtlinie	36
4. Die neue Datenschutzverordnung	37
5. Zusammenfassung	37
B. Verfassungsrecht	38
I. Das allgemeine Persönlichkeitsrecht	38
1. Das Recht auf informationelle Selbstbestimmung	38
2. Das Recht auf Privatsphäre	40
3. Das neue „Online-Grundrecht“	41
4. Das Recht auf Anonymität als eigenes Teilrecht	42
5. Schranken.....	43
II. Das Fernmeldegeheimnis	45
III. Andere Gewährleistungen	47
1. Meinungsfreiheit	47
2. Schutz der Wohnung.....	48
IV. Wirkung unter Privaten.....	49
V. Schutzpflichten	50
C. Einfaches Recht.....	51
I. Recht auf Anonymität in der Kommunikation	51
II. Allgemeines Recht auf Anonymität.....	53
III. Dogmatische Einordnung der Vorschriften.....	53
IV. Auslegung der Vorschriften	55
D. Gesammelte Aspekte – Gibt es ein Recht auf Anonymität?	57
 Teil 4: Anonymität im Internet	 59
A. Technische Grundlagen	60
I. Notwendige Adressierung im Internet	61
II. Die Rechnerkommunikation.....	63
III. Abgreifen von Daten.....	64
IV. Die MAC-Adresse.....	65

V. Die Bedeutung von Cookies	65
VI. Besonderheiten im IPv6	66
<i>B. Möglichkeiten der Anonymisierung</i>	68
I. „Echte“ Anonymisierungsdienste	69
1. Funktionsweise von JAP/Jondonym	69
2. Besonderheiten von TOR	70
II. Proxys	71
1. Was sind Proxys?	71
2. Anonymität durch Proxys?	71
<i>C. Anwendung der Grundsätze zur Anonymität auf das Internet</i>	72
I. Feststellung eines Verhaltens	73
II. Feststellung der Identität	73
1. Statische IP-Adressen und Cookies	74
2. Dynamische IP-Adressen	76
3. Bedeutung der Zuordnung zu einem Anschluss	77
4. Fehler bei der Zuordnung	81
5. Befristung der Speicherung durch Access-Provider	83
6. MAC-Adressen	84
7. IP-Spoofing und MAC-Spoofing	85
8. Anonymität und das IPv6	86
a) Netzwerk-Präfix	86
b) Interface-Identifizier	86
c) Zusammenfassung	87
III. Ergebnis	88
<i>D. Auswirkungen des Rechts auf Anonymität auf die vernetzte Welt</i>	89
I. Die Gewährleistung des Rechts auf Anonymität im Internet	89
1. Privatsphäre im Internet	90
2. Datenschutz im Internet	92
a) Schutz vor Verarbeitung der IP-Adresse	92
aa) Subjektive Auffassung	94
bb) Objektive Auffassung	95
cc) Systematischer Ansatz nach dem Gefahrbezug	95
dd) Folgen	98
b) Schutz vor Cookies	99
c) Schutz vor der Vergabe statischer IP-Adressen	101
aa) Vergabe des Netzwerk-Präfixes	101
bb) Vergabe des Interface-Identifiziers	103
d) Einwilligung als Werkzeug der Identifizierung	104

aa) Spezielle Koppelungsverbote	105
bb) Allgemeines Koppelungsverbot?.....	106
cc) Pflicht zur anonymen Gestaltung	107
3. Schutz der Telekommunikation.....	111
4. Schutz der Wohnung.....	111
II. Folgen: Anforderungen beim Betrieb von Diensten.....	112
 Teil 5: Konfliktfall: Effektive Durchsetzung von	113
urheberrechtlichen Ansprüchen vs. Anonymität	
 A. Bedeutung der Identifizierung für die Anspruchsdurchsetzung	113
B. Anspruchsdurchsetzung als Teil des grundrechtlichen Schutzes	114
I. Direkt aus Art. 14 GG	115
II. Durch Art. 19 Abs. 4 GG	117
III. Durch das Rechtsstaatsprinzip.....	118
IV. Europäischer Grundrechtsschutz	119
V. Ergebnis.....	119
 C. Verletzungen von Urheberrechten im Internet	120
I. Anwendbares Recht	121
II. Formen von Urheberrechtsverletzungen im Internet	124
1. Upload.....	124
a) Vervielfältigungen nach § 16 UrhG.....	124
b) Öffentliche Zugänglichmachung nach § 19a UrhG	125
2. Download.....	127
a) Eingreifen der Schranke des § 53 Abs. 1 S. 1 UrhG.....	127
b) Umgehung des Schutzes technischer Maßnahmen	129
3. Folgen	130
III. Haftung der Intermediäre	130
1. Schadensersatzansprüche.....	131
2. Unterlassungsansprüche.....	132
a) Haftung in P2P-Netzen.....	132
b) Haftung der Betreiber von Sharehoster-Servern	135
aa) Kriterien der Zumutbarkeit	135
(1) Filtersoftware	137
(2) Manuelle Überprüfung.....	139
(3) Pflicht zur Identifizierung der User.....	140
(4) Zusammenfassung	142
bb) Erweiterung wegen „von der Rechtsordnung nicht.....	143
gebilligtem Geschäftsmodell“?	

(1) Ansicht des OLG Hamburg.....	144
(2) Abgrenzung nach Gefahrgeneignis	145
cc) Ergebnis.....	148
c) Ergebnis	150
3. Verschaffen des Internet-Zugangs.....	150
4. Ergebnis	152

D. Rückverfolgung von Usern 152

I. Wie gelangen Rechteinhaber an IP-Adressen?.....	153
1. Suchen nach urheberrechtswidrigen Angeboten	153
a) Suchen in Tauschbörsen	153
b) Suchen auf Sharehoster-Servern	154
c) Rechtliche Bewertung	155
aa) Anwendbares Recht	155
(1) Einschlägige Vorschriften	155
(2) Anwendbarkeit des BDSG	156
bb) Zulässigkeit der Speicherung.....	156
(1) Zulässigkeit nach § 28 Abs. 1 Nr. 2 BDSG	157
(2) Zulässigkeit nach § 28 Abs. 1 Nr. 3 BDSG	159
(3) Verstoß gegen § 4 Abs. 2 BDSG	160
(a) Mitwirkung bei Speicherung der IP-Adresse?	161
(b) Ausnahmen	161
(c) Extensive Auslegung der Ausnahmenvorschriften ..	162
(4) Speicherung und Übermittlung durch	163
Anti-Piracy-Firmen	
(a) § 4 Abs. 2 S. 2 BDSG	164
(b) Zulässigkeit nach § 29 BDSG.....	165
(5) Ergebnis	168
cc) Beweisrechtliche Probleme.....	168
(1) Beweiserbringung durch EDV-Beweismittel.....	168
(2) Identifizierung des Inhalts von Dateien	169
(3) Grundsätze der Beweiswürdigung und.....	170
des Beweismaßes	
(4) Anscheinsbeweis für den Dateieinhalt?	172
d) Zusammenfassung.....	174
2. Feststellen getätigter Downloads	175
a) „Honeypots“	175
aa) Was sind Honeypots?.....	175
bb) Wie werden Honeypots urheberrechtlich verwendet?.....	175
cc) Rechtliche Bewertung.....	176
(1) Zulässigkeit der Ermittlungsmethode.....	176
(2) Eignung zur Beweisführung.....	177

(a)	Einwilligung in den Download	177
(b)	Erschöpfung bei digitalen Nutzungsarten.....	179
(c)	Einwilligung in weitere Nutzungshandlungen	180
(d)	Ergebnis	182
b)	Ergebnis	183
3.	Auskunftsansprüche.....	183
a)	Gegen Dienstebetreiber	184
aa)	Anspruchsgrundlage	185
bb)	Anspruchsvoraussetzungen	185
(1)	Offensichtliche Rechtsverletzung oder Klageerhebung	185
(2)	Verhalten des Anspruchsgegners.....	186
(3)	Gewerbliches Ausmaß	187
(4)	Anwendbarkeit des § 101 Abs. 9 UrhG?.....	189
cc)	Anspruchsinhalt	190
b)	Ergebnis	191
c)	Rechtliche Bewertung	191
aa)	Vereinbarkeit mit Gemeinschaftsrecht.....	192
bb)	Unmöglichkeit	192
cc)	Datenschutzrechtliche Probleme	194
(1)	Zulässigkeit der Weitergabe.....	194
(2)	Zulässigkeit der Speicherung	195
(a)	Zulässigkeit nach § 14 TMG.....	196
(b)	Zulässigkeit nach § 15 TMG.....	196
(c)	Einwilligung trotz § 13 Abs. 6 TMG?.....	198
dd)	Beweisrechtliche Probleme.....	201
(1)	Rechtfertigung der Beweisbeschaffung?.....	201
(2)	Folgen der Unzulässigkeit – Beweisverwertungsverbot?	202
d)	Gegen andere User	208
aa)	Anspruchsgrundlage	208
bb)	Anspruchsvoraussetzungen	209
e)	Ergebnis	209
4.	Anspruch auf Vorlage und Besichtigung.....	210
5.	Beschlagnahme der Server.....	211
II.	Wie lassen sich IP-Adressen zurückverfolgen?	212
1.	Auskunftsansprüche gegen Access-Provider	212
a)	Voraussetzungen des Anspruchs	213
b)	Problem: Zulässige Speicherung der IP-Adressen	214
aa)	Anwendbares Recht	214
bb)	Erlaubnisnormen im TKG	215
(1)	Dynamische IP-Adressen als Verkehrsdaten	215
(2)	Speicherung während der Verbindung	216

(3) Weitergehende Speicherung zu.....	217
Abrechnungszwecken	
(4) Weitergehende Speicherung zur Störungsbeseitigung	218
(5) Weitergehende Speicherung zu anderen Zwecken	219
cc) Speicherungspflicht?.....	220
(1) Aus einstweiliger Anordnung	220
(2) Auf „Zuruf“ des Anspruchsinhabers	222
c) Änderungen durch die Vorratsdatenspeicherung	223
de lege ferenda?	
d) Problem: Zulässige Weitergabe der Daten	224
aa) Europarechtliche Vorgaben	225
bb) Nationales Recht.....	225
(1) § 96 TKG	226
(2) Problem: Auskunft über Name hinter IP-Adresse als	
Auskunft über Verkehrsdatum?	227
(3) Rückgriff auf BDSG?	229
e) Ergebnis	229
2. Akteneinsicht im Ermittlungsverfahren.....	229
a) Verweis auf Privatklage	231
b) Einstellung des Verfahrens.....	231
c) Voraussetzungen des § 406e StPO.....	231
3. Problem: Auskunft bei unzulässig erhobenen IP-Adressen.....	233
4. Ergebnis	234
III. Rückverfolgung bei der Nutzung von	234
Anonymisierungsdiensten?	
1. Rückverfolgung gespeicherter Daten	234
2. Anordnung zukünftiger Überwachung	235
3. Praktische Auswirkungen	237
<i>E. Fazit – Bewertung der Konfliktlage</i>	<i>237</i>
I. Ausreichender Schutz der Anonymität	237
II. Ausreichender Schutz des Urheberrechts.....	238
1. Sharehoster-Server	239
a) Grundrechtlicher Handlungsbedarf.....	240
b) Europarechtlicher Handlungsbedarf	241
c) Ergebnis	243
2. Peer-to-Peer-Netze	243
III. Zusammenfassung.....	244

Teil 6: Überlegungen zur Lösung des Konflikts.....	246
A. Weitergehende Deanonymisierung der User	247
I. Verdachtsunabhängige Erfassung der IP-Adressen durch Dienstebetreiber	248
II. Identifizierungspflicht bei bestimmten Diensten.....	251
III. Rückverfolgung bei der Nutzung von Anonymisierungsdiensten?	253
B. Einbindung der Intermediäre de lege ferenda	254
I. Access-Provider	254
II. Host-Provider.....	256
1. Vereinbarkeit mit der RL 2004/48/EG	256
2. Haftungsausschluss nach RL 2000/31/EG?	258
a) Keine Überwachungspflichten	258
b) Keine eigenen Inhalte.....	259
c) Anwendung auf Unterlassungsansprüche?	260
d) Vorgaben des Art. 14 RL 2000/31/EG (§ 10 TMG)	261
e) Ergebnis	262
3. Neubestimmung der Haftung	262
a) Notice and Take-Down.....	262
b) Verhinderung künftiger Rechtsverletzungen.....	264
c) Umsetzung	267
C. Zusammenfassung und Ergebnisfindung	269
Literaturverzeichnis	271
Register.	281