Andreas Kramer

Zivilrechtlicher Auskunftsanspruch gegenüber Access Providern

Verpflichtung zur Herausgabe der Nutzerdaten von Urheberrechtsverletzern unter Berücksichtigung der Enforcement-Richtlinie (RL 2004/48/EG)

Verlag Dr. Kovač

Schriftenreihe

Recht der Neuen Medien

Band 39

ISSN 1616-9603

Verlag Dr. Kovač

Andreas Kramer

Zivilrechtlicher Auskunftsanspruch gegenüber Access Providern

Verpflichtung zur Herausgabe
der Nutzerdaten von Urheberrechtsverletzern
unter Berücksichtigung der Enforcement-Richtlinie
(RL 2004/48/EG)

Verlag Dr. Kovač

Hamburg
2007

VERLAG DR. KOVAČ
FACHVERLAG FÜR WISSENSCHAFTLICHE LITERATUR

Leverkusenstr. 13 · 22761 Hamburg · Tel. 040 - 39 88 80-0 · Fax 040 - 39 88 80-55

E-Mail info@verlagdrkovac.de · Internet www.verlagdrkovac.de

D 6

Die Rechtswissenschaftliche Fakultät der Westfälischen Wilhelms-Universität Münster hat diese Arbeit als Dissertation angenommen.

Erster Berichterstatter:	Prof. Dr. Thomas Hoeren
Zweiter Berichterstatter:	Prof. Dr. Bernd Holznagel, LL.M.
Dekan:	Prof. Dr. Reiner Schulze
Tag der mündlichen Prüfung:	31. Oktober 2006

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

ISSN: 1616-9603

ISBN: 978-3-8300-2867-3

Zugl.: Dissertation, Universität Münster, 2006

Meinen Eltern

Vorwort

Die vorliegende Arbeit wurde im Jahre 2006 von der Rechtswissenschaftlichen Fakultät der Westfälischen Wilhelms-Universität zu Münster als Dissertation angenommen. Die Arbeit berücksichtigt Rechtsprechung und Literatur sowie Gesetzgebungsverfahren bis Juli 2006.

Mein aufrichtiger Dank gilt meinem Betreuer Herrn Prof. Dr. Hoeren, auf dessen Anregung die Arbeit entstand. Herrn Prof. Dr. Holznagel möchte ich für die zügige Erstellung des Zweitgutachtens danken.

Meiner lieben Freundin Friederike danke ich für ihr Verständnis und ihre vielen aufmunternden Worte. Besonders herzlicher Dank gebührt schließlich meinen Eltern Heinrich und Maria Kramer, ohne deren großzügige Unterstützung sowohl mein Studium als auch diese Arbeit nicht möglich gewesen wäre. Ihnen ist diese Arbeit gewidmet.

Feedback zur Arbeit bitte per E-Mail an: andreaskramer@gmx.net.

Düsseldorf, im Januar 2007 *Andreas Kramer*

Inhaltsverzeichnis

Literaturverzeichnis

Ahrens, Hans-Jürgen	„Elektronische Dokumente und technische Aufzeichnungen als Beweismittel“, in: Schütze, Rolf A. (Hrsg.), Einheit und Vielfalt des Rechts, Festschrift für Reinhold Geimer zum 65. Geburtstag, S. 1 ff. München 2002 (zit.: Ahrens, in: FS Geimer, S.)
Asendorf, Claus Dietrich	„Auskunftsansprüche nach dem Produktpirateriegesetz und ihre analoge Anwendung auf Wettbewerbsverstöße“, in: Ulrich Löwenheim (Hrsg.), Festschrift für Fritz Traub zum 65. Geburtstag, S. 21 ff. Frankfurt 1994 (zit.: Asendorf, in: FS Traub, S.)
Bär, Wolfgang	„Auskunftsanspruch über Telekommunikationsdaten nach den neuen §§ 100g, 100h StPO“, in: MMR 2002, S. 358 ff.
Barton, Dirk M.	„(Mit-)Verantwortlichkeit des Arbeitgebers für die rechtsmissbräuchliche Online-Nutzung durch den Arbeitnehmer – Findet die Haftungsprivilegierung des § 9 Abs. 1 TDG auch auf den Arbeitgeber Anwendung?“, in: CR 2003, S. 592 ff.
Bauer, Fritz	„Der Beseitigungsanspruch nach § 1004 BGB - Zugleich ein Beitrag zum Problem der Rechtswidrigkeit auf dem Gebiet des Güterschutzes“, in: AcP 160 (1961), S. 456 ff.
Baumbach, Adolf (Begr.) Lauterbach, Wolfgang Albers, Jan Hartmann, Peter	Zivilprozessordnung 64. Auflage München 2006 (zit.: Bearbeiter, in: Baumbach /Lauterbach/Albers/ Hartmann, §, Rn.)

Beckmann, Kirsten	Verantwortlichkeit von Online-Dienste-anbietern in Europa und den Vereinigten Staaten von Amerika Münster 2001 (zit.: Beckmann, S.)
Berger, Christian	„Die Neuregelung der Privatkopie in § 53 Abs. 1 UrhG im Spannungsverhältnis von geistigem Eigentum, technischen Schutz-maßnahmen und Informationsfreiheit“, in: ZUM 2004, S. 257 ff.
Berger, Ernst Georg	„Verantwortung von TK-Unternehmen für wettbewerbswidrig genutzte Rufnum-mern“, in: MMR 2003, S. 642 ff.
Bohne, Michael	„Zur Auskunftserteilung durch Acces-Provider nach Schutzrechtsverletzungen im Internet“ – Anmerkung zum Urteil des OLG Frankfurt a.M. vom 25.1.2005 – 11 U 51/05, in: GRUR-RR 2005, S. 145 ff.
Breyer, Patrick	Die systematische Aufzeichnung und Vor-haltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland (Vorratsdatenspeicherung, traffic data retention) Frankfurt a. M. 2005, abrufbar unter: http://publikatio-nen.ub.uni-frankfurt.de/ volltexte/2005/ 500/pdf/BreyerPatrick.pdf (zit.: Breyer, Vorratsdatenspeicherung, S.)
Bröcker, Klaus T. Czychowski, Christian Schäfer, Detmar (Hrsg.)	Praxishandbuch Geistiges Eigentum im Internet München 2003 (zit.: Bearbeiter, in: Bröcker/Czychowski/ Schäfer, §, Rn.)

Büchner,Wolfgang (Hrsg.)	Beck`scher TKG-Kommentar 2. Auflage München 2000 (zit.: Bearbeiter, in: Beck-TKG, §, Rn.)
Czychowski, Christian	„Auskunftsansprüche gegenüber Internetzugangsprovidern „vor“ dem 2. Korb und „nach“ der Enforcement-Richtlinie der EU“, in: MMR 2004, S. 514 ff.
Decker, Ute	„Haftung für Urheberrechtsverletzungen im Internet“, in: MMR 1999, S. 7 ff.
Dietz, Ingo Richter, Michael	„Internetzugänge unter Internet Service Providern“, in: CR 1998, S. 528 ff.
Dix, Alexander	„Vorratsspeicherung von IP-Adressen?“, in: DuD, S. 234 ff.
Dorschel, Joachim	Anmerkung zum Urteil des OLG Hamburg v. 28.4.2005 – 5 U 156/04, in: CR 2005, S. 516 ff.
Dreier, Thomas	„Ausgleich, Abschreckung und andere Rechtsfolgen von Urheberrechtsverletzungen - Erste Gedanken zur EU-Richtlinie über die Maßnahmen und Verfahren zum Schutz der Rechte an geistigem Eigentum“, in: GRUR Int. 2004, S. 706 ff.
Dreier, Thomas Schulze, Gernot	Urheberrechtsgesetz 2. Auflage 2006 Kommentar (zit.: Dreier/Schulze,§ , Rn.)
Dustmann, Andreas	Die privilegierten Provider - Haftungseinschränkungen im Internet aus urheberrechtlicher Sicht Baden-Baden 2001 (zit.: Dustmann, Provider, S.)

Eckhard, Jens	„Datenschutz und Überwachung im Regierungsentwurf zum TKG“, in: CR 2003, S. 805 ff.
Ehret, Susanne	„Internet-Auktionshäuser auf dem haftungsrechtlichen Prüfstand – Ein Beitrag zur zivilrechtlichen Haftung von Internet-Auktionshäusern für rechtswidrige Auktionsangebote“, in: CR 2003, S. 754 ff.
Einziger, Kurt Schubert, Agnes Schwabl, Wolfgang Wessely, Karin Zykan, David	„Wer ist 217.204.27.214? – Access Provider im Spannungsfeld zwischen Auskunftsbegehr-(lichkeit)en der Rechteinhaber und Datenschutz“, in: MR 2005, S. 113 ff.
Engel-Flechsig, Stefan	„Das Informations- und Kommunikationsdienstegesetz des Bundes und der Mediendienstestaatsvertrag der Bundesländer“, in: ZUM 1997, S. 231 ff.
Engel-Flechsig, Stefan Maennel, Frithjof Tettenborn, Alexander	„Das neue Informations- und Kommunikationsdienste-Gesetz“, in: NJW 1997, S. 2981 ff.
Ensthaler, Jürgen Bosch, Wolfgang Völker, Stefan (Hrsg.)	Handbuch Urheberrecht und Internet Heidelberg 2002 (zit.: Bearbeiter, in: Entshaler/ Bosch/ Völker, S.)
Fechner, Frank	Geistiges Eigentum und Verfassung - schöpferische Leistungen unter dem Schutz des Grundgesetzes Tübingen 1999 (zit.: Fechner, S.)
Federrath, Hannes	„Technische Grundlagen von Auskunftsansprüchen“, in: ZUM 2006, S. 434 ff.

Federath, Hannes Hansen, Marit	„Anonym – total (l)egal?“, in: DuD 2003, S. 126 f.
Fezer, Karl-Heinz	Markenrecht Kommentar 3. Auflage München 2001 (zit.: Fezer, §, Rn.)
ders.	„Modernisierung des deutschen Rechts gegen den unlauteren Wettbewerb auf der Grundlage der Europäisierung des Wettbewerbsrechts“, in: WRP 2001, S. 989 ff.
Flechsig, Norbert P.	„Subdomain: Sicher versteckt und unerreichbar?“, in: MMR 2002, S. 347 ff.
Freytag, Stefan M.	Haftung im Netz - Verantwortlichkeit für Urheber-, Marken- und Wettbewerbsrechtsverletzungen nach § 5 TDG und § 5 MDStV München 1999 (zit.: Freytag, S.)
ders.	Anmerkung zum Urteil des BGH vom 17.5.2001 – I ZR 251/99 - Ambiente, in: CR 2001, S. 853 f.
ders.	„Providerhaftung im Binnenmarkt“, in: CR 2000, S. 600 ff.
Freiwald, Sven	Die private Vervielfältigung im digitalen Kontext am Beispiel des Filesharing Baden-Baden 2004 (zit.: Freiwald, Filesharing, S.)
Fritze, Ulrich Stauder, Dieter	„Die Beschaffung von Beweisen für die Verletzung von gewerblichen Schutzrechten“, in: GRUR Int. 1986, S. 342 ff.

Geis, Ivo	„Zivilprozeßrechtliche Aspekte des elektronischen Datenmanagements“, in: CR 1993, S. 653 ff.
Gerke, Marco	„Zugangsprovider im Fadenkreuz der Urheberrechtsinhaber – Eine Untersuchung der urheberrechtlichen Verantwortlichkeit von Downloadportalen und Zugangsprovidern für Musikdownloads“, in: CR 2006, S. 210 ff.
Gola, Peter Schomerus, Rudolf	Bundesdatenschutzgesetz 8. Auflage München 2005 (zit.: Gola/Schomerus, §, Rn.)
Golembiewski, Claudia	„Das Recht auf Anonymität im Internet“, in: DuD 2003, S. 129 ff.
Götting, Horst-Peter	„Die Entwicklung neuer Methoden der Beweisbeschaffung zur Bekämpfung von Schutzrechtsverletzungen - Die Anton-Piller-Order - Ein Modell für das deutsche Recht?“, in: GRUR Int. 1988, S. 729 ff.
Gounalakis, Georgios Rhode, Lars	„Das Informations- und Kommunikationsdienste-Gesetz. Ein Jahr im Rückblick: Rechtsrahmen des Bundes für die Informationsgesellschaft“, in: K&R 1998, S. 321 ff.
Gnirck, Karen Lichtenberg, Jan	„Internetprovider im Spannungsfeld staatlicher Auskunftsersuchen“, in: DuD, S. 598 ff.
Haeddicke, Maximilian	„Die Haftung für mittelbare Urheber- und Wettbewerbsrechtsverletzungen“, in: GRUR 1999, S. 397 ff.

Haidinger, Victoria	Gesetzliche Auskunfts- und Mitwirkungspflichten von Internet Service Providern gegenüber Behörden und Privaten, abrufbar unter: http://www.rechtsprobleme.at/doks/auskunftsmitwirkungspflichten-isp-haidinger.pdf (zit.: Haidinger, S.)
Harte-Bavendamm, Henning Henning-Bodewig, Frauke (Hrsg.)	Gesetz gegen den unlauteren Wettbewerb (UWG) Kommentar München 2004 (zit.: Harte/Henning/Bearbeiter, §, Rn.)
Hefermehl, Wolfgang Köhler, Helmut Bornkamm, Joachim	Wettbewerbsrecht 24. Auflage München 2006 (zit.: Hefermehl/ Köhler/ Bornkamm, §, Rn.)
Heghmanns, Michael	„Musiktauschbörsen im Internet aus strafrechtlicher Sicht“, in: MMR 2004, S. 14 ff.
Hess, Burkhard	Anmerkung zum Urteil des EuGH vom 14.7.1994, Rs. C-91/92 - Faccini Dori, in: JZ 1995, S. 150 f.
Hoeren, Thomas	Skriptum Internetrecht Münster, Stand Juni 2006, abrufbar unter: http://www.uni-muenster.de/jura/itm/hoeren (zit.: Hoeren, Internetrecht, S.)
ders.	Recht der Access Provider München 2004 (zit.: Hoeren, Access Provider, Rn.)
ders.	Anmerkung zum Urteil des BGH vom 11.3.2004 – I ZR 304/01 – Internetversteigerung, in: MMR 2004, S. 672 f.

Hoeren, Thomas Sieber, Ulrich (Hrsg.)	Handbuch Multimedia-Recht Loseblattsammlung; Stand: Dezember 2005 (zit.: Hoeren/Sieber/Bearbeiter, Kap., Rn.)
Ingerl, Reinhard Rohnke, Christian	Markengesetz Kommentar 2. Auflage München 2003 (zit.: Ingerl/Rohnke, §, Rn.)
Jacobs, Rainer	Anmerkung zum Urteil des BGH vom 24.3.1994 – I ZR 42/93 – Cartier-Armreif, in: GRUR 1994, 634 f.
Jani, Ole	„Was sind offensichtlich rechtswidrig hergestellte Vorlagen? Erste Überlegungen zur Neufassung von § 53 Abs. 1 Satz 1 UrhG“, in: ZUM 2003, S. 842 ff.
Jergolla, Maren	„Das Ende der wettbewerbsrechtlichen Störerhaftung?“, in: WRP 2004, S. 655 ff.
Kaufmann, Noogie C. Köcher, Jan	Anmerkung zum Urteil des LG Hamburg vom 7.7.2004 – 308 O 264/04, in: MMR 2005, S. 61 f.
Kitz, Volker	„Auskunftspflicht des Zugangsvermittlers bei Urheberrechtsverletzungen durch Nutzer“, in: GRUR 2003, S. 1014 ff.
ders.	„Die Zukunft der Auskunft oder: Die abenteuerliche Karriere des § 101a UrhG“, in: MMR 2005, S. 133 f.
ders.	„§ 101a UrhG: Für eine Rückkehr zur Dogmatik“, in: ZUM 2005, S. 298 ff.

ders.	„Urheberschutz im Internet und seine Einfügung in den Gesamtrechtsrahmen“, in: ZUM 2006, S. 444 ff.
Knaak, Roland	„Die EG-Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums und ihr Umsetzungsbedarf im deutschen Recht“, in: GRUR Int 2004, S.745 ff.
Köhler, Helmut	„Der ergänzende Leistungsschutz: Plädoyer für eine gesetzliche Regelung“, in: WRP 1999, S. 1075 ff.
Koenig, Christian Loetz, Sascha	„Sperrungsanordnung gegenüber Network- und Access-Providern“, in: CR 1999, S. 438 ff.
Köpsell, Stefan Federrath, Hannes Hansen, Marit	„Erfahrungen mit dem Betrieb eines Anonymisierungsdienstes“, in: DuD 2003, S. 139 ff.
Larenz, Karl Canaris, Claus-Wilhelm	Methodenlehre der Rechtswissenschaft 3. Auflage Berlin 1995 (zit.: Larenz/Canaris, Methodenlehre, S.)
Lehmann, Michael	„Unvereinbarkeit des § 5 Teledienstegesetz mit Völkerrecht und Europarecht“, in: CR 1998, S. 232 ff.
Leonard, Axel	Die Rechtsfolgen der Nichtumsetzung von EG-Richtlinien Frankfurt a.M. 1997 (zit.: Leonard, S.)
Linke, Thomas	Anmerkung zum Urteil des OLG Hamburg vom 28.4.2005 – 5 U 156/04, in: MMR 2005, S. 456 ff.

Loewenheim, Ulrich (Hrsg.)	Handbuch des Urheberrechts München 2003 (zit.: Loewenheim/Bearbeiter, §, Rn.)
Mangold, Hermann v. (Begr.) Starck, Christian (Hrsg.) Klein, Friedrich	Kommentar zum Grundgesetz Band 1: Präambel, Art. 1 bis 19 5. Auflage München 2005 (zit.: Bearbeiter, in: v. Mangold/ Klein/ Stark, Art., Rn.)
Manz, Friederike	Die Haftung für Urheberrechtsverletzungen im Internet nach deutschem und amerikanischen Recht München 1999 (zit.: Manz, S.)
Michael, Lothar	„Die drei Argumentationsstrukturen des Grundsatzes der Verhältnismäßigkeit“, in: JuS 2001, S. 148 ff.
Möring, Philipp (Begr.) Nicolini, Käte (Hrsg.)	Urheberrechtsgesetz Kommentar 2. Auflage München 2000 (zit.: Möhring/Nicolini/Bearbeiter, §, Rn.)
Müller-Terpitz, Ralf	„Regelungsreichweite des § 5 MDStV“, in: MMR 1998, S. 478 ff.
Musielak, Hans-Joachim (Hrsg.)	Kommentar zur Zivilprozessordnung 4. Auflage München 2005 (zit.: Musielak/Bearbeiter, §, Rn.)
Nirk, Rudolf Kurtze, Helmut	Geschmacksmustergesetz 2. Auflage Köln 1997 (zit.: Nirk/Kurtze, GeschmMG, §, Rn.)

Nordemann, Jan Bernd Dustmann, Andreas	„To Peer Or Not To Peer – Urheberrechtliche und datenschutzrechtliche Fragen der Bekämpfung der Internet-Piraterie“, in: CR 2004, S. 380 ff.
Nordemann, Wilhelm Vinck, Kai Hertin, Paul W.	Urheberrecht Kommentar 9. Auflage Stuttgart 1998 (zit.: Nordemann/Bearbeiter, § , Rn.)
Ohlenburg, Anna	„Der neue Telekommunikationsdatenschutz – Eine Darstellung von Teil 7 Abschnitt 2 TKG“, in: MMR 2004, S. 431 ff.
dies.	„Die neue EU-Datenschutzrichtlinie 2002/58/EG – Auswirkungen und Neuerungen für elektronische Kommunikation“, in: MMR 2003, S. 82 ff.
Olenhusen, Albrecht Götz v. Crone, Andreas	„Der Anspruch auf Auskunft gegenüber Internet-Providern bei Rechtsverletzungen nach Urheber- bzw. Wettbewerbsrecht“, in: WRP 2002, S. 164 ff.
Oppermann, Klaus	Der Auskunftsanspruch im gewerblichen Rechtsschutz und Urheberrecht Berlin 1997 (zit.: Oppermann, S.)
Palandt, Otto (Begr.)	Bürgerliches Gesetzbuch Kommentar 65. Auflage München 2006 (zit.: Palandt/Bearbeiter, §, Rn.)
Pichler, Rufus	„Haftung des Host-Providers für Persönlichkeitsrechtsverletzungen vor und nach dem TDG“, in: MMR 1998, S. 79 ff.

Pieroth, Bodo Schlink, Bernhard Kniesel, Michael	Polizei- und Ordnungsrecht 3. Auflage München 2005 (zit.: Pieroth/Schlink/Kniesel, §, Rn.)
Raabe, Franziska	„Der Auskunftsanspruch nach dem Referentenentwurf zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“, in: ZUM 2006, S. 439 ff.
Raabe, Oliver	„Die rechtliche Einordnung zweier Web-Anonymisierungsdienste“, in: DuD 2003, S. 134 ff.
Rebmann, Kurt (Hrsg.)	Münchener Kommentar zum Bürgerlichen Gesetzbuch Band 2, Schuldrecht Allgemeiner Teil (§§ 241-432) 4. Auflage München 2003 Band 5, Schuldrecht, Besonderer Teil III, (§§ 705-853) 4. Auflage München 2004 Band 6, Sachenrecht (§§ 853-1296) 4. Auflage München 2004 (zit.: MünchKommBGB/ Bearbeiter, § , Rn.)
Roßnagel, Alexander (Hrsg.)	Recht der Multimediadienste Kommentar zum IuKDG und zum MDStV Loseblattsammlung, Stand: April 2005 (zit.: Roßnagel/ Bearbeiter, Multimediadienste, Teil, Rn.)
ders. (Hrsg.)	Handbuch Datenschutzrecht München 2003 (zit.: Bearbeiter, in: Roßnagel, Handbuch Datenschutzrecht, Teil, Rn.)

Rücker, Daniel	„Notice and take down-Verfahren für die deutsche Providerhaftung? – Zur Begrenzung der Unterlassungshaftung durch das Verbot allgemeiner Überwachungspflichten“, in: CR 2005, S. 347 ff.
Säcker, Franz Jürgen (Hrsg.)	Berliner Kommentar zum Telekommunikationsgesetz Frankfurt a.M. 2006 (zit.: Bearbeiter, in: Säcker, TKG, §, Rn.)
Schaar, Peter	Datenschutz im Internet München 2002 (zit.: Schaar, Datenschutz im Internet, Rn.)
ders.	„Datenschutz bei Web-Services“, in: RDV 2003, S. 59 ff.
Schack, Heimo	„Urheberrechtliche Gestaltung von Webseiten unter Einsatz von Links und Frames“, in: MMR 2001, S. 9 ff.
Schäfer, Martin Rasch, Clemens Braun, Thorsten	„Zur Verantwortlichkeit von Online-Diensten und Zugangsvermittlern für fremde urheberrechtsverletzende Inhalte“, in: ZUM 1998, S. 451 ff.
Scheurle, Klaus Dieter Mayen, Thomas (Hrsg.)	Telekommunikationsgesetz: TKG Kommentar München 2002 (zit.: Bearbeiter, in Scheurle/Mayen, TKG, §, Rn.)
Schilken, Eberhard	„Ansprüche auf Auskunft und Vorlegung von Sachen im materiellen Recht und im Verfahrensrecht“, in: Jura 1988, S. 525 ff.
Schlegel, Oliver	Anmerkung zum Urteil des LG Hamburg vom 7.7.2004 – 308 O 264/04, in: CR 2005, S. 144 f.

Schmid, Matthias Wirth, Thomas	Urheberrechtsgesetz Handkommentar Baden-Baden 2004 (zit.: HK-UrhG, §, Rn.)
Schmidt-Bleibtreu, Bruno Klein, Franz (Begr.)	Kommentar zum Grundgesetz 10. Auflage München 2004 (zit.: Schmidt-Bleibtreu/ Klein/ Bearbeiter, Art., Rn.)
Schmitz, Peter	Anmerkung zur Entscheidung des RegPräs Darmstadt zur Speicherung von IP-Adressen durch Access Provider, in: MMR 2003, S. 214 ff.
Schmitz, Peter Dierking, Laura	„Inhalte- und Störerverantwortlichkeit bei Telekommunikations- und Telemediendiensten – Anregungen für das geplante neue Telemediengesetz“, in: CR 2005, S. 420 ff.
Schricker, Gerhart Henning-Bodewig, Frauke	„Elemente einer Harmonisierung des Rechts des unlauteren Wettbewerbs in der Europäischen Union“, in: WRP 2001, S. 1367 ff.
Sieber, Ulrich	Verantwortlichkeit im Internet München 1999 (zit.: Sieber, Verantwortlichkeit, Rn.)
Sieber, Ulrich Höfinger, Frank Michael	„Drittauskunftsansprüche nach § 101a UrhG gegen Internetprovider zur Verfolgung von Urheberrechtsverletzungen“, in: MMR 2004, S. 575 ff.
Simitis, Spiros (Hrsg.)	Kommentar zum Bundesdatenschutzgesetz 6. Auflage Baden-Baden 2006 (zit.: Bearbeiter, in: Simitis, §, Rn.)

Sobola, Sabine Kohl, Kathrin	„Haftung von Providern für fremde Inhalte“, in: CR 2005, S. 443 ff.
Spiekermann, Sarah	„Die Konsumenten der Anonymität – Wer nutzt Anonymisierungsdienste?“, in: DuD 2003, S. 150 ff.
Spindler, Gerald (Hrsg.)	Vertragsrecht der Internet-Provider 2. Auflage Köln 2004 (Bearbeiter, in: Spindler, Internet-Provider, Teil, Rn.)
ders.	Anmerkung zum Urteil des OLG Frankfurt a. M vom 25.1.2005 – 11 U 51/04, in: MMR 2005, S. 243 ff.
ders.	„Urheberrecht und Haftung der Provider – ein Drama ohne Ende? – Zugleich Anmerkung zum Urteil des OLG München vom 8.3.2001 – 29 U 3282/00“, in: CR 2001, S. 324 ff.
ders.	„Das Gesetz zum elektronischen Geschäftsverkehr – Verantwortlichkeit der Diensteanbieter und Herkunftslandprinzip“, in: NJW 2002, S. 921 ff.
Spindler, Gerald Dorschel, Joachim	„Auskunftsansprüche gegen Internet-Service-Provider – Zivilrechtliche Grundlagen und datenschutzrechtliche Grenzen“, in: CR 2005, S. 38 ff.
dies.	„Vereinbarkeit der geplanten Auskunftsansprüche gegen Internet-Provider mit EU-Recht“, in: CR 2006, S. 346 ff.

Spindler, Gerald Schmitz, Peter Geis, Ivo	TDG – Teledienstegesetz, Teledienstedatenschutzgesetz, Signaturgesetz Kommentar München 2004 (zit.: Bearbeiter, in: Spindler/ Schmitz/ Geis, §, Rn.)
Spindler, Gerald Volkmann, Christian	„Die zivilrechtliche Störerhaftung der Internet-Provider“, in: WRP 2003, S. 1 ff.
dies.	„Störerhaftung für wettbewerbswidrig genutzte Mehrwertdienst-Rufnummern und Domains“, in: NJW 2004, S. 808 ff.
Stadler, Thomas	Haftung für Informationen im Internet 2. Auflage Berlin 2005 (zit.: Stadler, Haftung, S.)
Staudinger, Julius v. (Begr.)	Kommentar zum Bürgerlichen Gesetzbuch Buch 2; Recht der Schuldverhältnisse (§§ 779-811) 14. Auflage Berlin 2002 (zit.: Staudinger/Bearbeiter, § , Rn.)
Stein, Friedrich (Begr.) Jonas, Martin	Kommentar zur Zivilprozessordnung Band 4/2 (§§ 348-510b ZPO) 21. Auflage Tübingen 1999 (zit.: Stein/Jonas/Berabeiter, §, Rn.)
Teplitzki, Otto	Wettbewerbsrechtliche Ansprüche und Verfahren 8. Auflage Köln 2002 (zit.: Teplitzky, Kap., Rn.)

Ulrich, Gustav-Adolf	Anmerkung zum Urteil des BGH vom 24.3.1994 – I ZR 42/93 – Cartier-Armreif, in: GRUR 1994, S. 979
Vassilaki, Irini	„Strafrechtliche Haftung nach § 8 ff. TDG“, in: MMR 2002, S. 659 ff.
Volkmann, Christian	Der Störer im Internet München 2005 (zit.: Volkmann, Störer im Internet, S.)
Wandtke, Artur-Axel Bullinger, Winfried (Hrsg.)	Praxiskommentar zum Urheberrecht 2. Auflage München 2006 (zit.:Wandtke/Bullinger/Bearbeiter, §, Rn.)
Wiebe, Andreas	„Auskunftsverpflichtung der Access Provider – Verpflichtung zur Drittauskunft bei Urheberrechtsverletzungen von Kunden, die an illegalem File-Sharing teilnehmen“, in: MR 2005, Beilage zu Heft 4 (zit.: Wiebe, MR 2005, Beilage zu Heft 4, S.)
Wuermeling, Ulrich Felixberger, Stefan	„Fernmeldegeheimnis und Datenschutz im Telekommunikationsgesetz“, in: CR 1997, S. 230 ff.
Wiume, Marc	Der Auskunftsanspruch im Markenrecht Frankfurt a.M. 2002 (zit.: Wiume, S.)
Ziegler, Cai	„Smarte Schwärme – Die Technik hinter modernen Peer-to-Peer-Netzen“, in: c`t 2005, Heft 16, S. 160 ff.
Zöller, Richard (Begr.)	Zivilprozessordnung 25. Auflage Köln 2005 (zit.: Zöller/Bearbeiter, §, Rn.)

Zombik, Peter	„Der Kampf gegen Musikdiebstahl im Internet – Rechtsdurchsetzung zwischen Bagatellschwelle und Datenschutz“, in: ZUM 2006, S. 450 ff.

Hinsichtlich der verwendeten Abkürzungen wird verwiesen auf:

Butz, Cornelie Kirchner, Hildebert	Abkürzungen der Rechtssprache 5. Auflage Berlin 2003

1. Teil: Einführung und Grundlagen

A. Einführung in die Problematik

Die Verbreitung der Digitaltechnik stellt immer wieder neue Anforderungen an das ursprünglich am analogen Umfeld ausgerichtete Urheberrechtsgesetz.[1] Nachdem mittlerweile sowohl die Anwendbarkeit des Urheberrechts auf digitale Werke als auch die urheberrechtliche Einordnung von Nutzungshandlungen im Onlinebereich weitestgehend geklärt ist,[2] hat die Urheberrechtsproblematik nunmehr die Ebene der Rechtsdurchsetzung erreicht.[3] Während es in wirtschaftlicher Hinsicht hierbei um Milliardenbeträge geht, gilt es in rechtspolitischer Hinsicht einen gerechten Interessenausgleich zwischen den Beteiligten herbeizuführen.

Den Inhabern von Urheber- und Leistungsschutzrechten bieten sich verschiedene Ansatzpunkte, um gegen die Verletzung ihrer Rechte im Onlinebereich vorzugehen. Da die meisten Urheberrechtsverletzungen in sog. „Tauschbörsen“[4] begangen werden, wurde zunächst versucht, direkt gegen die Betreiber dieser Portale sowie gegen die Hersteller der für deren Nutzung notwendigen Software vorzugehen. Dieser Weg hat sich in der Praxis aufgrund einer Vielzahl von rechtlichen und tatsächlichen Problemen jedoch zumeist als nicht gangbar erwiesen.[5]

Mittlerweile haben die Rechteinhaber erkannt, dass ein direktes Vorgehen gegen die Nutzer den erfolgsversprechensten Ansatz für eine Rechtsverfolgung darstellt. Es sind nämlich die Nutzer, die sich unlängst als einzige Konstante im Kampf gegen Urheberrechtsverletzungen herauskristallisiert haben.[6] Problematisch ist allerdings, dass die Nutzer im Internet nicht unter ihrem Namen und ihrer Adresse auftreten, sondern unter einer von ihrem Zugangsanbieter (Access Provider) zugewiesenen IP-Adresse. Anhand dieser Adresse, die in ihrer Funktion mit einer herkömmlichen Telefonnummer vergleichbar ist, kann der Rechteinhaber indes nur erkennen, von welchem Access Provider sie vergeben wurde. Die Rechtsverfolgung endet somit regelmäßig beim Access Provider. Nur dieser ist in der Lage, Auskunft darüber zu geben, welchem konkreten Nutzer die fraglich IP-Adresse

---

[1] Näher Hoeren, Access Provider, Rn. 415 ff.
[2] So auch Hoeren, Internetrecht, S. 22, der diese Fragen als *„first“* und *„second generation issues“* bezeichnet.
[3] Kitz, GRUR 2003, 1014, 1015.
[4] Zum Begriff und zur Funktionsweise sog. „Tauschbörsen“, siehe unten, 1.Teil C. III.
[5] Ausführlich dazu Dustmann, Provider, S. 202 ff.; Freiwald, Filesharing, S. 157 ff.
[6] Kitz, GRUR 2003, 1014, 1015.

zu dem Zeitpunkt der Verletzungshandlung zugeteilt war. Auf diese Auskunft ist der Rechteinhaber jedoch zwingend angewiesen, wenn er zivilrechtliche Unterlassungs- oder Schadensersatzansprüche gegen den Rechtsverletzer geltend machen will. Die Access Provider hingegen sind nur dann zur Auskunftserteilung bereit, wenn sie dazu auch gesetzlich verpflichtet sind. Diese wollen zum einen das Vertrauen ihrer Kunden in die Geheimhaltung deren persönlicher Daten nicht enttäuschen. Zum anderen sind sie zivil- und strafrechtlichen Risiken ausgesetzt, sofern die Auskunftserteilung von keiner gesetzlichen Ermächtigungsgrundlage getragen wird.

Unstreitig trifft den Access Provider eine gesetzliche Auskunftspflicht über Nutzerdaten nur gegenüber den Strafverfolgungsbehörden. Da auch vorsätzliche Urheberrechtsverletzungen unter den Voraussetzungen der § 106 ff. UrhG strafbewehrten Charakter haben, sind die Rechteinhaber teilweise dazu übergegangen, Strafanzeigen gegen die anonymen Rechtsverletzer unter Angabe deren IP-Adresse zu erstatten. Denn sofern die Staatsanwaltschaften die Ermittlungen aufnehmen und die gewünschten Auskünfte von den Access Providern einholen, können die Rechteinhaber im Wege der strafprozessualen Akteneinsicht die Identität der Rechtsverletzer in Erfahrung bringen. Somit können auch über diesen Umweg die notwendigen Auskünfte für eine zivilrechtliche Rechtsverfolgung eingeholt werden.

Allerdings führt auch dieses Vorgehen, vor allem aufgrund des Opportunitätsprinzips, vielfach nicht zum gewünschten Erfolg.[7] Sehen die Staatsanwaltschaften nämlich von der Rechtsverfolgung ab und holen die begehrte Auskunft auch nicht im Wege von Vorermittlungen ein, geht die strafprozessuale Akteneinsicht ins Leere. Diese Fälle dürften indes zunehmen. So haben die Staatsanwaltschaften, nachdem diese im Jahre 2005 mit tausenden von Strafanzeigen gegen unbekannte Urheberrechtsverletzer regelrecht überflutet wurden, eine Heraufsetzung der Bagatellgrenze angekündigt, unterhalb derer es zur Einstellung dieser Verfahren kommen soll.[8] Nicht zuletzt haben diese massenhaften Strafanzeigen jedoch auch einen Symbolcharakter. Sie halten dem Gesetzgeber die Notwendigkeit einer zivilrechtlichen Auskunftsverpflichtung der Access Provider vor Augen und verleihen damit zugleich der Forderung der Rechteinhaber nach der Statuierung einer gesetzlichen Auskunftspflicht Nachdruck. Denn obwohl die Rechteinhaber bereits mehrfach einen solchen Auskunftsanspruch ange-

[7] Vgl. unten, 2.Teil A. IV. 5. c) bb).

[8] Heise News, Meldung v. 3.1.2006: Massenstrafanzeigen gegen P2P-Nutzer: Bagatellregelung durch die Hintertür, http://www.heise.de/newsticker/meldung/67918.

mahnt haben,[9] ist dessen Umsetzung in den bisherigen Urheberrechtsreformen aufgrund von zahlreichen rechtlichen Problemen bei dessen Ausgestaltung unterblieben.[10]

Bedingt durch diese missliche Lage wurde seitens der Rechteinhaber versucht, eine Auskunftspflicht des Access Providers bereits auf der Grundlage des geltenden Rechts zu konstruieren.[11] Tatsächlich sind auch einige Gerichte der Argumentation der Rechteinhaber gefolgt. Danach soll der Access Provider für die Urheberrechtsverletzungen seiner Nutzer zumindest als mittelbarer Störer haften und als solcher gem. § 101a UrhG auf Auskunft über die Identität der Rechtsverletzer in Anspruch genommen werden können.[12] Diese – im einstweiligen Verfügungsverfahren ergangenen – Entscheidungen hatten jedoch im Berufungsverfahren keinen Bestand, [13] da die Berufungsgerichte zumindest die für den Erlass einer einstweiligen Verfügung gem. § 101a Abs. 3 UrhG erforderliche Offensichtlichkeit der Rechtsverletzung verneinten.

Diese Gerichtsentscheidungen könnten sich für die Access Provider mit der Umsetzung der Richtlinie 2004/48/EG[14] (sog. Enforcement-Richtlinie)[15] alsbald als Pyrrhussieg erweisen. Diese sieht in Art. 8 Abs. 1

---

[9] Vgl. Stellungnahme des „Forums der Rechteinhaber" zum Regierungsentwurf für ein Gesetz zum Urheberrecht in der Informationsgesellschaft v. Okt. 2002, S. 8, abrufbar unter: http://www.urheberrecht.org/topic/Info-RiLi/st/Forum-RegEntw.pdf , sowie zum Referentenentwurf eines Zweiten Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft v. 15.11.2004, S. 9, abrufbar unter: http://www.urheberrecht.org/topic/Korb-2/st/refentw/RefEntw-Korb2.pdf.

[10] So Kaufmann/Köcher, Anm. zu LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, MMR 2005, 61, 61 in Bezug auf die Ergebnisse der vom Bundesjustizministerium im Vorfeld des Referentenentwurfs v. 27.9.2004 eingesetzten Arbeitsgruppe „Internet", S.9, abrufbar unter: http://www.bmj.bund.de/media/archive/707.pdf.

[11] Vgl. die überarbeitete Fassung des im Auftrag der Motion Picture Association (MPAA) erstellten Gutachtens von Nordemann/Dustmann, CR 2004, 380, 380 ff.

[12] LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, CR 2005, 136 m. Anm. Schlegel = MMR 2005, 55 m. Anm. Kaufmann/Köcher; LG Frankfurt, Urt. v. 5.8.2004 – 2-3 O 297/04 n.v.; LG Köln, Urt. v. 28.7.2004 – 28 O 301/04, ZUM 2005, 236; LG München I, Urt. v. 28.7.2004 – 21 O 10372/04, n.v.

[13] OLG Hamburg, Urt. v. 28.4.2005 – 5 U 156/04, MMR 2005, 453 m. Anm. Linke = CR 2005, 512 m. Anm. Dorschel; OLG Frankfurt a.M., Urt. v. 25.1.2005 – 11 U 51/05, MMR 2005, 241 m. Anm. Spindler = CR 2005, 285; OLG München, Urt. v. 24.3.2005 – 6 U 4696/04 n.v.; im Berufungsverfahren vor dem OLG Köln wurde der Verfügungsantrages zurückgenommen, nachdem sich abzeichnete, dass der Senat das Urteil des Landgerichts aufheben wollte.

[14] Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates v. 29.4.2004 zur Durchsetzung der Rechte des geistigen Eigentums, ABl. L 195 v. 2.6.2004, S. 16.

[15] Auch Durchsetzungsrichtlinie genannt.

lit. c explizit vor, dass auch derjenige auf Auskunft über die Identität von Rechtsverletzern in Anspruch genommen werden kann, der zwar selbst keine Rechtsverletzung begeht, jedoch *„nachweislich für rechtsverletzende Tätigkeiten genutzte Dienstleistungen im gewerblichen Ausmaß erbrachte“*. Am 3.1.2006 ist daraufhin ein Referentenentwurf veröffentlicht worden, mit dem diese – auch Access Provider betreffende – Regelung in deutsches Recht umgesetzt werden soll.[16]

B. Gang der Untersuchung

Das Ziel dieser Untersuchung ist die Beantwortung der Frage, ob sich bereits nach dem geltenden Recht *(de lege lata)* oder aber zumindest nach der Umsetzung der Enforcement-RL *(de lege ferenda)* eine Verpflichtung des Access Providers gegenüber den Rechteinhabern auf Auskunft über die Identität jener Nutzer ergibt, die ihren Internetzugang für Urheberrechtsverletzungen missbrauchen.

Zu diesem Zweck werden im ersten Teil der Bearbeitung zunächst die für die Erfassung dieser Thematik unerlässlichen technischen, rechtlichen sowie gesellschaftspolitischen Grundlagen erläutert. Im zweiten und dritten Teil wird der für die Bearbeitung essentiellen Frage nachgegangen, ob den Rechteinhabern nach dem geltenden Recht eine materielle oder prozessuale Anspruchsgrundlage zur Seite steht, mittels derer die begehrten Auskünfte vom Access Provider erlangt werden könnten.

Der vierte und fünfte Teil der Bearbeitung widmet sich sodann der Frage, ob einer Inanspruchnahme des Access Providers nach den allgemeinen Regeln die spezialgesetzlichen Haftungsprivilegierungen des Teledienstegesetzes (TDG) und des Mediendienstestaatsvertrages (MDStV) oder aber datenschutzrechtliche Restriktionen sowie das Fernmeldegeheimnis entgegenstehen.

Im sechsten Teil soll unter der Prämisse, dass bereits nach geltendem Recht eine Auskunftspflicht des Access Providers besteht, hinsichtlich der Effektivität eines solchen Anspruchs der Frage nachgegangen werden, ob sich die potentiellen Rechtsverletzer durch die Benutzung eines sog. Anonymisierungsdienstes – in rechtlicher zulässiger Weise – dennoch einer Identifizierung entziehen können.

---

[16] Vgl. § 101 UrhG-E des Referentenentwurfs für ein Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums v. 3.1.2006, abrufbar unter: http://www.urheberrecht.org ; ausführlich dazu unten, 7.Teil C.

Im siebten Teil der Bearbeitung wird ein Ausblick auf die Auskunftspflicht des Access Providers gegeben werden, wie sie sich voraussichtlich *de lege ferenda* nach der Umsetzung der sog. Enforcement-RL (RL 2004/48/EG) darstellen wird. Hierzu bedarf es zunächst einer kritischen Würdigung des – im Referentenentwurf zur Umsetzung dieser Richtlinie vorgesehenen – Auskunftsanspruchs des § 101 UrhG-E. Weiterhin sind in dieser Hinsicht auch die geplanten Novellierungen des Datenschutzrechts, insbesondere die noch umzusetzende Richtlinie zur Vorratsdatenspeicherung (RL 2006/24/EG), dahingehend zu untersuchen, ob sich diese auf eine zivilrechtliche Auskunftspflicht des Access Providers auswirken. Im abschließenden achten Teil sollen die wesentlichen Ergebnisse dieser Arbeit zusammengefasst werden.

C. Technische Grundlagen

I. Die Leistungen des Access Providers

Der Access Provider stellt seinen Nutzern einerseits die infrastrukturellen Voraussetzungen für die Nutzung des Internets und andererseits die für die Versendung und das Empfangen von einzelnen Datenpaketen notwendigen Protokollfunktion zur Verfügung.[17]

1. Bereitstellung der Infrastruktur

Die primäre Dienstleistung des Access Providers besteht darin, dem Kunden eine Einwahlmöglichkeit[18] zur Verfügung zu stellen. Durch diese wird der Rechner oder das Netzwerk des Kunden mit einer Backbone verbunden, welche schließlich den Zugang zu einer Vielzahl von Netzen ermöglicht, deren Gesamtheit man als Internet bezeichnet.[19]

Um die Datenzugriffe möglichst effizient zu gestalten, betreiben Access Provider oftmals Proxy-Chache-Server. In technischer Hinsicht funktionieren diese so, dass Daten, die erstmalig von einem Nutzer angefordert werden, zunächst vom Ursprungsserver übermittelt werden. Während des Abrufs findet sodann eine automatische Zwischenspeicherung auf dem Proxy-Cache-Server des Providers statt. Wird daraufhin von einem weiteren Nutzer dieselbe Seite aufgerufen, müssen diese Daten nicht mehr vom Ur-

---

[17] Nach überwiegend vertretener Auffassung sind diese Leistungen dienstvertraglicher Natur, vgl. BGH, Beschl. v. 23.03.2005 – III ZR 338/04, JurPC Web-Dok. 72/2005, Abs. 7 m.w.N.; Spindler, in: Spindler, Internet-Provider, Teil IV, Rn. 93.

[18] *Point of Presence* (PoP).

[19] Hoeren/Sieber/Sieber, Teil 1, Rn. 16; Stadler, Haftung, S. 28.

sprungsserver angefordert werden, sondern können direkt vom Proxy-Cache-Server des Providers übermittelt werden. Die Aktualität dieser Daten wird zumeist dadurch gewährleistet, dass bei jeder Anforderung zunächst ein Abgleich mit der Originalquelle stattfindet. Sofern durch diesen Abgleich eine Aktualisierung der Daten des ursprünglichen Hosts festgestellt wird, werden diese Daten erneut von dieser Quelle angefordert und für weitere Nutzer auf dem Proxy-Cache-Server zwischengespeichert, anderenfalls erfolgt die Übermittlung direkt vom Proxy-Cache-Server des Providers. Der Vorteil dieser Zwischenspeicherungen besteht zum einen darin, dass die Nutzer auf die lokal vorhandenen Dateien wesentlich schneller zugreifen können, zum anderen werden dadurch die Netzlast sowie die Verbindungskosten verringert.[20]

Neben Proxy-Cache-Servern betreiben Access Provider zumeist auch sog. Router. Diese verbinden verschiedene Teilnetze miteinander und bestimmen den optimalen Weg der durchgeleiteten Datenpakete, indem sie diese im Hinblick auf das Ziel zum nächstgelegenen Router weiterleiten. Dies ist nicht zwangsläufig der geographisch nächste Router, sondern derjenige, der die schnellste Anbindung an das Ziel verspricht.[21]

2. Bereitstellung von Protokollfunktionen

Darüber hinaus stellt der Access Provider dem Nutzer die zur Datenübermittlung notwendigen Protokollfunktionen zur Verfügung.[22] Die Datenübertragung im Internet erfolgt auf Basis der TCP/IP-Protokolle. Diese bestehen aus dem Transportprotokoll TCP (*Transmission Control Protocol*), dem Netzwerkprotokoll IP (*Internet Protocol*) sowie aus den Anwendungsprotokollen, welche wiederum die Grundlage für die Dienste des Internets bilden (z.B. WWW-, FTP- und Filesharing-Dienste). Die Datenübermittlung erfolgt dergestalt, dass die zu übermittelnden Daten zunächst vom TCP-Protokoll in einzelne Datenpakete aufgeteilt werden. Diese Pakete erhalten eine fortlaufende Nummerierung und eine Port-Nummer. Durch die Nummerierung wird sichergestellt, dass die Datenpakete beim Empfänger in der richtigen Reihenfolge wieder zusammengesetzt und bei Verlust neu angefordert werden. Bei den Port-Nummern handelt es sich zumeist um standardisierte Kennungen, die sicherstellen, dass die Daten den entsprechenden weiterverarbeitenden Anwendungsprogrammen zugeführt werden, z.B. dass die Datenpakete einer Website auch vom Browser

[20] Hoeren/Sieber/Sieber, Teil 1, Rn. 27; Stadler, Haftung, S. 122 (Fn. 285).
[21] Vgl. Hoeren/Sieber/Sieber, Teil 1, Rn. 25.
[22] Näher dazu Hoeren/Sieber/Sieber, Teil 1, Rn. 42 ff.

und nicht vom E-Mail-Programm bearbeitet werden. Das *Internet Protocol* ist hingegen für die Adressierung und das Routing zuständig, also für das Versenden und die Wegfindung der einzelnen Pakete im Internet.[23] Diese Vorgänge können am besten mit der konventionellen Beförderung durch die Post verglichen werden. Dabei fungiert das IP Protokoll als Briefumschlag, in dem die einzelnen TCP-Pakete verpackt werden. Die im IP-Protokoll implementierte Routingtabelle wird sodann vom den bereits angesprochenen Routern ausgelesen, die daraufhin – wie ein Postverteilungszentrum – den optimalen Weg der Datenpakete bestimmen. Der Access Provider kann hinsichtlich der Übermittlung dieser Daten allenfalls als Briefträger eingestuft werden, da sich seine Tätigkeit darauf beschränkt, die Datenpakete vom Nutzer zum nächstgelegenen Router und in die umgekehrte Richtung zu transportieren.

3. Vergabe von IP-Adressen

Zusätzlich muss der Access Provider dafür Sorge tragen, dass die Datenpakete auch an den Nutzer adressiert werden können, mithin bedarf dieser einer eindeutigen Kennung. Als solche fungiert die IP-Adresse. Diese besteht aus vier durch Punkte getrennte Byte-Werte, deren Höhe zwischen 0 und 255 variiert (z.B. 84.62.160.63). Access Provider verfügen regelmäßig über einen Pool von IP-Adressen, die ihnen nach Maßgabe eines hierarchischen Systems, an dessen Anfang die ICANN[24] steht, zugeteilt werden.[25] Aus diesem Pool wird dem Rechner oder Netzwerk des Nutzers bei jeder Einwahl eine IP-Adresse zugewiesen.

Je nach Vertragsgestaltung kann es sich hierbei um eine feste (statische) oder aber um eine wechselnde (dynamische) IP-Adresse handeln. Ist vertraglich vereinbart worden, dass dem Kunden bei jeder Einwahl dieselbe IP-Adresse zugeteilt wird, liegt eine statische IP-Adresse vor.[26] Bedingt durch das schnelle Wachstum des Internets sind die IP-Adressen jedoch zu einem begehrten und knappen Gut geworden.[27] Daher wurden Verfahren entwickelt, um die IP-Adressen effizienter nutzen zu können. Ein solches Verfahren stellt die dynamische Vergabe von IP-Adressen dar. Bei dieser wird dem Nutzer bei jeder Einwahl ins Internet und nur für die Dauer der

---

[23] Hoeren/Sieber/Sieber, Teil 1, Rn. 68.
[24] Internet Corporation for Assigned Numbers und Names, http://www.icann.org
[25] Vgl. Hoeren/Sieber/Sieber, Teil 1, Rn. 54.
[26] Einzinger/Schubert/Schwabl/Wessely/Zykan, MR 2005, 113, 114.
[27] Das Problem der Knappheit von IP-Adressen wird sich mit dem bevorstehenden Übergang zum IPv6-Verfahren erledigen, vgl. http://www.ipv6.org.

Verbindung eine beliebige IP-Adresse aus dem Pool des Providers zugewiesen wird. Der Vorteil dieser dynamischen Vergabe besteht darin, dass eine IP-Adresse nicht dauerhaft für einen Nutzer reserviert wird, sondern mehreren Nutzern zur Verfügung steht. Aufgrund dieses Synergieeffektes stellt die dynamische Vergabe von IP-Adressen mittlerweile den Regelfall dar.

Die den Nutzern zugewiesenen IP-Adressen werden bei den Access Providern regelmäßig in den Protokolldateien (sog. Log-Dateien) gespeichert. Diese Dateien werden von den Providern in erster Linie für Abrechnungszwecke unterhalten, dienen darüber hinaus jedoch auch Beweiszwecken sowie zur Missbrauchsaufklärung, da anhand dieser Daten die IP-Adresse auch nachträglich einem bestimmten Nutzer zugeordnet werden kann.

II. Rechtsverfolgung anhand von IP-Adressen

Die Protokollierung der IP-Adressen in den Log-Dateien der Access Provider ist für die Auskunftsbegehren der Rechteinhaber von essentieller Bedeutung, da eine Identifizierung des Nutzers anhand seiner IP-Adresse nur dann erfolgreich sein kann, wenn diese Nutzerdaten beim Access Provider noch gespeichert sind.

Haben die Rechteinhaber eine verdächtige IP-Adresse generiert, so lässt sich diese zunächst bis zu dem Access Provider zurückverfolgen, der diese IP-Adresse vergeben hat. Für solche Identifizierungszwecke haben sich im Internet einige Informationsportale etabliert, die z.B. neben dem geographischen Standort des Nutzers einer fraglichen IP-Adresse auch Auskunft über den jeweiligen Access Provider des Nutzers geben.[28] Dadurch können die Rechteinhaber in Erfahrung bringen, an welchen Access Provider sie sich zu wenden haben, um die begehrte Auskunft über die Identität eines Rechtsverletzers zu erhalten.

Unterstützung im Kampf gegen die Produktpiraterie erhalten die Rechteinhaber inzwischen von mehreren Seiten. Neben der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU), die im Auftrag der Film- und Softwareindustrie nach Urheberrechtsverletzungen im Internet fahndet und aufgrund ihrer Ermittlungsmethoden unlängst selbst in die Kritik geriet,[29] sind mittlerweile eine Vielzahl von Anbietern auf dem Markt, die im Auf-

[28] Z.B. http://www.dnsstuff.com.

[29] Heise News, Meldung v. 4.2.2006: GVU-Fahnder als Raubkopierer-Komplizen, http://www.heise.de/newsticker/meldung/69206.

trag der Rechteinhaber mittels sog. Crawler-Programme das Internet nach Urheberrechtsverletzungen durchforsten, um die IP-Adressen vermeintlicher Rechtsverletzer zu generieren.

Für Aufsehen haben in dieser Hinsicht vor allem die Aktivitäten des Schweizer Unternehmens Logistep gesorgt, das im Auftrag eines Softwareherstellers massenhaft IP-Adressen von Rechtsverletzern in Filesharing-Netzwerken generierte und sodann die Access Provider mittels automatisierter E-Mails an deren Abuse-Adresse[30] aufforderte, diese IP-Adressen entgegen den datenschutzrechtlichen Bestimmungen nicht zu löschen, sondern für weitere Rechtsverfolgszwecke der Rechteinhaber vorzuhalten. Auf die Zulässigkeit solcher anlassbezogenen Speicherpflichten wird im Rahmen der Bearbeitung noch ausführlich eingegangen.[31]

III. Technische Voraussetzungen für Urheberrechtsverletzungen

Urheberrechtsverletzer bedienen sich zur Ausführung ihrer Verletzungshandlungen der Dienste des Internets, die wiederum auf den Anwendungsprotokollen des TCP/IP-Protokolls basieren. Zu den bekanntesten dieser Dienste gehören das World Wide Web (WWW), der nach dem File Transfer Protocol benannte Dienst FTP, Newsdienste, E-Mail-Dienste, Voice over IP (VoIP), Internet Relay Chat (IRC) sowie Streaming- und Filesharing-Dienste.[32] Da den meisten Auskunftsersuchen zu IP-Adressen Verletzungshandlungen mittels FTP-Servern oder Filesharing-Diensten zugrunde liegen, stehen vor allem darauf basierende Verletzungshandlungen im Fokus der nachfolgenden Bearbeitung. Diese Handlungen sollen im Folgenden näher betrachtet werden. Auf eine Darstellung von vorbereitenden Maßnahmen, wie die Digitalisierung und Komprimierung von Daten, soll an dieser Stelle verzichtet werden.[33]

1. Betrieb eines FTP-Servers

Sofern in den bisherigen Gerichtsverfahren auf dem Zivilrechtswege Auskunft über den Inhaber einer IP-Adresse verlangt wurde, lag diesen zumeist der Sachverhalt zugrunde, dass unter einer IP-Adresse ein sog. FTP-Server betrieben wurde, auf dem eine Vielzahl von urheberrechtlich geschützten Musikdateien im mp3-Format zum Download bereitgehalten

[30] E-Mail-Adresse, unter der bei einem Access Provider Rechtsverstöße gemeldet werden können, z.B. abuse@t-online.de.
[31] Siehe unten, 5. Teil, A, IV, 1, b, cc.
[32] Ausführlich dazu Hoeren/Sieber/Sieber, Teil 1, Rn. 77 ff.
[33] Ausführlich dazu Freiwald, Filesharing, S. 15 ff.

wurden.[34] In technischer Hinsicht ermöglicht dabei das *File Transfer Protocol* die Einwahl in bestimmte Server, auf denen dann mittels einer speziellen Software Daten beliebiger Formate oder Größe vom Server heruntergeladen (Download) oder auf diesem hinterlegt werden können (Upload). Die Zugangsberechtigung zum Server kann unterschiedlich ausgestaltet sein. Dieser kann entweder gegen Fremdzugriffe mit einem Passwortschutz versehen sein, oder aber es handelt sich um einen anonymen FTP-Server, bei dem ohne Benutzerkennung auf alle Daten zugegriffen werden kann.[35] Links zu FTP-Servern mit urheberrechtlich geschütztem Material kann man über entsprechende Channels im IRC oder auf speziellen Suchmaschinen finden.[36] Die FTP-Server, die Gegenstand der einschlägigen Gerichtsverfahren waren, verfügten noch über eine weitere technische Besonderheit. Denn obwohl den Servern von den Access Providern bei jeder Einwahl eine wechselnde dymamische IP-Adresse zugewiesen wurde, waren sie dennoch über eine gleich bleibende Domain erreichbar. Die Betreiber der Server bedienten sich nämlich eines dynamischen DNS-Dienstes. Diese Dienste sorgen dafür, dass die aktuell zugewiesene IP-Adresse an einen Domain-Name-Server übermittelt wird, der diese wiederum mit einer Domain verknüpft. Dadurch wird sichergestellt, dass ein Rechner trotz dynamischer IP-Adresse stets unter derselben Domain erreichbar ist.[37]

2. Filesharing-Netzwerke

Neben dem Betrieb von FTP-Servern stehen vor allem die – vorrangig für Urheberrechtsverletzungen genutzten – Filesharing-Netzwerke im Fadenkreuz der Rechteinhaber. In Deutschland werden diese Netzwerke[38] jährlich von ca. 7, 3 Mio. Personen genutzt. Sie beruhen auf Anwendungsprotokollen, die es den einzelnen Teilnehmern ermöglichen, direkt miteinander in Kontakt zu treten.[39] Die besondere Attraktivität dieser Netzwerke rührt daher, dass infolge der direkten Kontaktaufnahme zwischen den einzelnen Teilnehmern der aufwendige und teure Betrieb von gesonderten Servern entfällt.[40] Da zugleich auch die Grenzen zwischen der sonst übli-

---

[34] Vgl. OLG Hamburg, Urt. v. 28.4.2005 – 5 U 156/04, MMR 2005, 453, 453 = CR 2005, 512; LG Köln, Urt. v. 28.7.2004 – 28 O 301/04, ZUM 2005, 236, 236f.

[35] Schaar, Datenschutz im Internet, Rn. 15.

[36] Z.B. http://ftpsearch.com.

[37] Vgl. OLG Hamburg, Urt. v. 28.4.2005 – 5 U 156/04, MMR 2005, 453, 453 = CR 2005, 512.

[38] Zu den bekanntesten zählen die Napster-Nachfolger Kazaa, edonkey und BitTorrent.

[39] Näher zur Technik von Peer-to-Peer-Netzwerken Ziegler, c`t 2005, Heft 16, 160 ff.; Freiwald, Filesharing, S. 22 ff.

[40] Freiwald, Filesharing, S. 24.

chen Unterscheidung zwischen Server und Client verschwimmen, spricht man bei den Teilnehmern diese Netzwerke auch von Servants.[41] Aufgrund der Gleichberechtigung der Teilnehmer werden diese Netzwerke auch Peer-to-Peer[42](P2P)-Netzwerke genannt. Irreführend ist hingegen die gängige Bezeichnung „Tauschbörsen", da anders als bei einem Tausch i.S.d. BGB kein bestimmtes Exemplar den Besitzer wechselt, sondern durch das Herunterladen ein weiteres Vervielfältigungsstück entsteht.

Zur Teilnahme an Filesharing-Netzwerken benötigt man eine Zugangssoftware, die im Internet zumeist kostenlos heruntergeladen werden kann.[43] Je nach Programm kann es sein, dass der Teilnehmer nach der Installation der Software aufgefordert wird, Dateien auf seiner Festplatte zum Download für andere freizugeben. Teilweise besteht auch eine sog. Upload-Pflicht, so dass die Berechtigung zur Nutzung des Netzwerks von der Freigabe von Daten abhängig gemacht wird.[44] Sodann kann sich der einzelne Teilnehmer im Netzwerk selbst auf die Suche nach – zumeist illegal angebotenen – Dateien begeben.[45] Während es bei Napster lediglich möglich war, Musikdateien im mp3-Format zu tauschen, erlauben die neueren Netzwerke den Austausch von beliebigen Dateien, z.B. auch von wesentlich größeren Filmdateien.[46] Wie die Suche nach den Werken im Netzwerk vonstatten geht, hängt von dessen technischem Aufbau ab. Unterschieden wird in dieser Hinsicht zwischen zentralen und dezentralen Netzwerken.

a) Zentralisierte Netzwerke

Bei zentralisierten Netzwerken meldet sich der Teilnehmer über das Internet bei einem zentralen Server (Indexserver) an. Dieser speichert die IP-Adresse und den Bestand der freigegebenen Dateien des Teilnehmers. Die Dateien verbleiben jedoch auf der Festplatte des jeweiligen Nutzers und werden nicht auf den Indexserver geladen. Die Suche erfolgt nun anhand einer – von herkömmlichen Suchmaschinen bekannten – Suchmaske. Wird eine Suchanfrage durch einen Teilnehmer, z.B. nach bestimmten mp3-Dateien, gestartet, überprüft der Indexserver in dem vom ihm gespeicherten Datenbestand, ob sich die gewünschte Datei auf der Festplatte eines

[41] Ziegler, c`t 2005, Heft 16, 160, 160.
[42] „Peer" (engl.) = Gleichberechtigter.
[43] Sehr beliebt ist z.B. Kazaa Light.
[44] Freiwald, Filesharing, S. 24 (Fn. 66).
[45] Im Falle des Verfahrens gegen Napster wurde festgestellt, dass 87% der angebotenen Werke rechtswidrig bereitgestellt wurden; vgl. A&M Records, Inc et al. v. Napster, Inc., in: GRUR Int. 2000, 1066, 1067.
[46] Ziegler, c`t 2005, Heft 16, 160, 161.

anderes Teilnehmers befindet. Verläuft diese Prüfung positiv, wird dem Suchenden eine Liste mit den IP-Adressen und Port-Nummern der Anbieter angezeigt, von denen die gesuchten Dateien herunterladen werden können. Der Vorteil eines zentralen Indexservers besteht darin, dass die Nutzer stets den Gesamtdatenbestand aller Nutzer abfragen können. Dadurch kann bei jeder Suchabfrage eine hohe Trefferquote erzielt werden.[47] Zentrale Server bieten allerdings sowohl in technischer Hinsicht, etwa bei einem Ausfall des Servers, als auch in rechtlicher Hinsicht, wie die Verfahren gegen Napster gezeigt haben, erhebliche Angriffspunkte.[48] Aus diesem Grund sind die meisten Filesharingnetze mittlerweile dezentral, d.h. ohne zentralen Server, aufgebaut.

b) Dezentrale Netzwerke

Bei dezentralen Netzwerken werden die einzelnen Teilnehmer durch die Protokolldateien der Zugangssoftware wie bei einem Schneeballsystem miteinander verbunden.[49] Die Suchanfragen eines Nutzers werden wiederum nach dem Schneeballprinzip an alle Rechner des Netzwerkes weitergeleitet. Regelmäßig werden diese Anfragen mit einem sog. „Time To Live"-Befehl (TLL) versehen, der ein unendliches Kreisen der Suchanfrage verhindern soll.[50] Befindet sich eine gesuchte Datei auf dem Rechner eines Teilnehmers, erhält der Suchende eine Treffermeldung, die u.a. die IP-Adresse der Anbieter der gesuchten Datei beinhaltet, zu denen sodann eine Verbindung zum Zwecke des Downloads hergestellt werden kann. Weil dezentrale Netzwerke für die Rechteinhaber eine geringere juristische Angriffsfläche bieten, da man nicht gegen zentrale Serverbetreiber, sondern allenfalls gegen die Vertreiber der – urheberrechtlich zumeist unbedenklichen – Zugangssoftware vorgehen kann,[51] haben sich die Rechteinhaber auch technischer Mittel zur Bekämpfung der Urheberrechtspiraterie in Filesharing-Netzwerken bedient. So wurden anscheinend Unternehmen wie Overpeer Inc. und Mediasentry damit beauftragt, diese Netzwerke mit sog. Dummy-Dateien zu überfluteten. Diese Dateien suggerieren urheberrechtlich geschützte Werke als Inhalt, enthalten tatsächlich jedoch lediglich belanglose Daten.[52]

---

[47] Freiwald, Filesharing, S. 27.
[48] Ausführlich zum Verfahren gegen Napster, Dustmann, Provider, S. 203 ff.
[49] Nordemann/Dustmann, MMR 2004, 380, 382.
[50] Ziegler, c`t 2005, Heft 16,160, 161.
[51] Näher dazu Nordemann/Dustmann, MMR 2004, 380, 381; Freiwald, Filesharing, S. 157 ff.
[52] Heise News, Meldung v. 22.6.2005: Filmindustrie lässt angeblich gefälschte Pakete in BitTorrent einspeisen, http://www.heise.de/newsticker/meldung/60918; Heise News, Meldung

Die Netzwerkbetreiber reagierten umgehend und implementierten Filterprogramme, die anhand einer mathematischen Prüfsumme, dem sog. Hash-Wert, in der Lage sind, diese Dummy-Dateien herauszufiltern.[53] Dies hat nicht zuletzt auch zur Geschäftsaufgabe des Unternehmens Overpeer geführt.[54] Zudem haben sich im Internet einige Informationsportale gebildet, die Dateien auf Herkunft, Qualität und Echtzeit überprüfen und über kodierte Links eine direkte Verbindung über die Filesharing-Programme zu den geprüften Audio- oder Filmdateien herstellen.[55] Dies nahm die GEMA im Juni 2005 zum Anlass, 42 Access Provider zur Sperrung bekannter Linkportale aufzufordern.[56] Begründet wurde dies damit, dass die Provider durch die Zugangsgewährung aufgrund einer mittelbaren Störerhaftung zur Sperrung dieser Seiten verpflichtet seien.[57] Da eine solche Störerhaftung jedoch entgegen der Auffassung der GEMA kaum begründbar erscheint,[58] verwundert es nicht, dass die Rechteinhaber mit der Forderung nach einem Auskunftsanspruch gegen Access Provider die Front im Kampf gegen Urheberrechtsverletzungen nunmehr in die Richtung der Rechtsverletzer verschoben haben.

D. Gesellschaftspolitische Betrachtung der Urheberrechtspiraterie

Die massenhaften Urheberrechtsverletzungen im Internet führen einerseits zu immensen wirtschaftlichen Einbußen auf der Seite der Urheber und Leistungsschutzberechtigten und lassen andererseits auf eine anarchische Einstellung der Nutzer in Bezug auf geistige Eigentumsrechte schließen. Im Folgenden soll daher ein kurzer Überblick über diese wirtschaftlichen und sozialen Faktoren der Urheberrechtspiraterie im Internet gegeben werden.

---

v. 6.7.2002: Musiktauschbörsen: Das Imperium schlägt zurück, http://www.heise.de/newsticker/meldung/28863.

[53] Freiwald, Filesharing, S. 33.

[54] Heise News, Meldung v. 11.12.2005: Mutmaßlicher Tauschbörsen-Spoofer aus dem Rennen, http://www.heise.de/newsticker/meldung/67239.

[55] Nordemann/Dustmann, CR 2004, 380, 382 f.

[56] Heise News, Meldung v. 1.7.2005: GEMA fordert Provider zur Sperrung von Websites auf, http://www.heise.de/newsticker/meldung/61331.

[57] Presseerklärung der GEMA, http://www.gema.de/presse/briefe/brief55/sperrung.shtml; ausführlich zur Störerhaftung des Access Providers, siehe unten, 2. Teil, A. IV. 2.

[58] Vgl. Gercke, CR 2006, 210, 213 ff.; Stellungnahme des eco-Verbandes zur Sperraufforderung der GEMA, http://www.eco.de/servlet/PB/menu/1625892_pcontent_ll/content.html.

I. Ökonomischer Schaden durch Urheberrechtsverletzungen

Der seit Ende der neunziger Jahre konstante Anstieg von Urheberrechtsverletzungen hat dazu geführt, dass die durch die Urheberrechtspiraterie vorrangig betroffenen Wirtschaftszweige, namentlich die Software- und Unterhaltungsindustrie, jährlich neue Umsatzeinbrüche verkünden. Laut einer vom Software-Industrie-Verband BSA in Auftrag gegebenen Studie, ist allein der Softwareindustrie im Jahre 2004 aufgrund illegaler Softwarekopien ein Schaden von 1, 84 Mrd. € entstanden.[59] Da sich die Rechteinhaber angesichts der breiten Akzeptanz von Raubkopien längst von der Vorstellung verabschiedet haben, die Urheberrechtspiraterie umfassend eindämmen zu können, werden mittlerweile bescheidenere, jedoch durchaus erstrebenswerte Ziele gesteckt. Nach neuesten Berechnungen der BSA könnten durch eine zehnprozentige Absenkung des Anteils illegal genutzter Software, von derzeit 29 % auf 19 %, allein in der deutschen IT-Wirtschaft bis 2009 mehr als 115.000 neue Arbeitsplätze entstehen. Dies würde zugleich zu einem Anstieg des Beitrags der IT-Branche zum Bruttoinlandsprodukt von derzeit 80 Mrd. € auf 105 Mrd. € führen[60]

Ähnlich alarmierende Zahlen wie die BSA melden auch die deutschen Phonoverbände. Nach deren Berechnungen sind die Umätze von Tonträgern im Zeitraum von 1999 bis 2005 von 2,5 Mrd. auf 1,5 Mrd. € gefallen. Dies entspricht einer Verringerung der jährlichen pro Kopf Ausgaben von 30 auf 18 €.[61] Dieses Ergebnis korrespondiert auch mit den aktuellen Ergebnissen der sog. Brennerstudien, die jährlich von den deutschen Phonoverbänden[62] und der Filmförderungsanstalt (FFA)[63] bei der Gesellschaft für Konsumforschung (GFK) in Auftrag gegeben werden. Mittels dieser Studien wird das Nutzerverhalten in Bezug auf das Herunterladen aus dem Internet und das Brennen von Musik- und Filmtiteln analysiert. So geht aus der Brennerstudie 2005 der Musikindustrie hervor, dass 80,5% der im Jahre 2004 heruntergeladenen 475 Millionen Musikwerke aus illegalen Quellen stammen. Der Anteil legaler, jedoch kostenpflichtiger Downloadportale, wie z.B. Musicload und itunes, liegt hingegen lediglich bei 1,8%.[64] So-

[59] Studie der BSA abrufbar unter: http://www.bsa.org/germany/piraterie/piraterie.cfm .
[60] Vgl. http://www.bsa.org/germany/piraterie/idc-studie.cfm.
[61] Vgl. Jahresbericht 2005 des Bundesverbandes der phonographischen Wirtschaft e.V., abrufbar unter: http://www.ifpi.de/jb/2006/umsatz.pdf.
[62] Brennerstudie 2005 (Phonoverbände), abrufbar unter: http://www.ifpi.de/wirtschaft/brennerstudie2005.pdf.
[63] Brennerstudie 2005 (FFA), abrufbar, unter: http://www.filmfoerderungsanstalt.de/downloads/publikationen/brenner_studie4.pdf.
[64] Brennertudie 2005 (Phonoverbände), a.a.O., S. 16.

mit fristen legale Downloadangebote immer noch ein Tankstellendasein inmitten lauter illegaler Ölquellen.[65] Ähnlich ist die Situation der Filmindustrie. So haben im ersten Halbjahr 2005 rund 1,7 Mio. Menschen – nahezu ausschließlich illegal – 11,9 Mio. Filme aus dem Internet heruntergeladen, was allein im Vergleich zum Vorjahreszeitraum einem Plus von 16 % entspricht.[66]

In technischer Hinsicht lässt sich der stetige Anstieg von Urheberrechtsverletzungen mit der rasanten Verbreitung von Breitband-Zugängen erklären, die hohe Übertragungsraten gewährleisten. Allein von Anfang 2004 bis Sommer 2005 hat sich der Prozentsatz der Nutzer dieser High-Speed-Internetzugänge von 22 % auf 41% nahezu verdoppelt.[67] Von diesen Internetzugängen wird knapp die Hälfte in Zusammenhang mit einer Flatrate genutzt.[68]

II. Digitale Mentalität der Nutzer

Neben den verbesserten technischen Voraussetzungen für Urheberrechtsverletzungen lässt deren fortlaufender Anstieg aber auch auf eine mangelnde Sensibilisierung der Nutzer für geistige Eigentumsrechte schließen. Daran hat anscheinend auch die offensive „Raubkopierer sind Verbrecher“[69] – Kampagne der Unterhaltungsindustrie nichts geändert, in der mit drastischen Maßnahmen auf den strafbewehrten Charakter von Urheberrechtsverletzungen hingewiesen wurde. Denn obwohl die Bekanntheit dieser Kampagne im Vergleich von 2004 zu 2005 innerhalb der Zielgruppe der 20-29-jährigen von 41 % auf 64 % gesteigert werden konnte,[70] nahm die Anzahl vor Kinostart heruntergeladener Kinofilme im Vergleich zum Vorjahr sogar um einen Prozentpunkt zu.[71]

Die mangelnde Effektivität dieser Kampagne lässt sich vor allem daran festmachen, dass 36 % der Nutzer, die angaben, die „Raubkopierer sind Verbrecher“ –Kampagne zu kennen, auch weiterhin davon ausgehen, dass das Herunterladen aktueller Spiel- und Kinofilme aus dem Internet legal sei.[72] Dieses fehlende Unrechtsbewusstsein ist – laut einer von Microsoft

[65] Vgl. Meldung der IFPI, abrufbar unter: http://ifpi.de/news/news-102.htm.
[66] Brennerstudie 2005 (FFA), a.a.O., S. 23.
[67] Brennerstudie 2005 (FFA), a.a.O., S. 5.
[68] Brennerstudie 2005 (FFA), a.a.O., S. 5.
[69] Vgl. http://www.hartabergerecht.de.
[70] Brennerstudie 2005 (FFA), a.a.o., S. 18.
[71] Brennerstudie 2005 (FFA), a.a.o., S. 7.
[72] Brennerstudie 2005 (FFA), a.a.o., S. 22.

bei der Universität Witten/Herdecke in Auftrag gegebenen Studie[73] – vor allem darauf zurückzuführen, dass es bei Verletzungshandlungen im Internet am Merkmal der körperlichen Wegnahme fehlt, dieses jedoch den historisch gewachsenen Vorstellungen von Diebstahl zugrunde liege.[74] Das Ziel der Rechteinhaber, so die Studie, müsse daher sein, den Nutzern die Bedeutung von Nutzungsrechten nahe zu bringen, da nur so deren Unrechtsbewusstsein geschärft werden könne. Solange sich die Regelungen des Urheberrechts jedoch nicht mit dem intuitiven Rechtsverständnis der Nutzer decken, müsse man sich mit der glaubwürdigen Androhung von Sanktionen begnügen.[75] Glaubwürdig werden diese Sanktionen jedoch erst dann sein, wenn sich die Rechtsverletzer nicht mehr hinter ihrer anonymen IP-Adresse „verstecken" und sich so vor der Rechtsverfolgung in Sicherheit wiegen können.

E. Urheberrechtliche Grundlagen

Die Auskunftsbegehren der Rechteinhaber sind in letzter Konsequenz darauf gerichtet, gegen den namhaft gemachten Rechtsverletzer zivilrechtliche Unterlassungs- und Schadensersatzansprüche geltend zu machen. Vor diesem Hintergrund bedarf es zunächst einer Erläuterung, wer als Rechteinhaber in diesem Sinne anzusehen ist. Anschließend soll der Frage nachgegangen werden, ob den Rechteinhabern derartige Ansprüche gegen die Nutzer überhaupt zustehen. Hierzu bedarf es einer urheberrechtlichen Würdigung der oben genannten Nutzungshandlungen.

I. Rechteinhaber und deren Rechtsposition

Im Zentrum der nachfolgenden Bearbeitung stehen vor allem Rechtsverletzungen an Musik-, Film- und Softwarewerken. Nach § 2 Abs. 1 UrhG unterstehen diese Werke dem Schutz des Urheberrechtsgesetzes. In den vorliegend bedeutsamen Konstellationen werden Rechtsverletzungen an diesen Werken jedoch regelmäßig nicht von den Urhebern, also den Schöpfern i.S.d. § 7 UrhG, sondern von den Produzenten geltend gemacht. Diesen gewährt das Urheberrecht aufgrund ihrer organisatorischen, technischen und unternehmerischen Leistungen eigenständige Rechte, die man als Leistungsschutzrechte bezeichnet.[76] Entsprechende Regelungen finden

[73] Studie zur Digitalen Mentalität, abrufbar unter: http://download.microsoft.com/download/D/2/B/D2B7FE98-CA92-4E18-ACD6-94A915B4CAFF/Digitale_Mentalitaet.pdf.
[74] Studie zur Digitalen Mentalität, a.a.O., S. 4.
[75] Studie zur Digitalen Mentalität, a.a.O., S. 5.; Zombik, ZUM 2006, 450, 452.
[76] Wandtke/Bullinger/Wantdke, Einl. UrhG, Rn. 11.

sich in § 85 UrhG für die Musik- bzw. Tonträgerhersteller sowie in § 94 UrhG für die Filmhersteller. Für den Softwarehersteller gelten die Sonderregeln der §§ 69a ff. UrhG, insbesondere die in § 69c UrhG geschützten Rechte. Diese Leistungsschutzberechtigten sind vorrangig gemeint, wenn im Folgenden der Begriff der Rechteinhaber verwendet wird.

Urheberrechtsdogmatisch handelt es sich bei diesen Leistungsschutzrechten um Verwertungsrechte, wie sie auch den Urhebern nach den §§ 15 ff. UrhG zustehen. Im Gegensatz zu den Verwertungsrechten der Urheber ist der Katalog der Verwertungsrechte der Leistungsschutzberechtigten jedoch abschließend und erstreckt sich somit nicht zugleich auch auf neue Verwertungsformen.[77] Allerdings stehen auch den Leistungsschutzberechtigten die Verwertungsrechte zu, die vorliegend von Bedeutung sind. Dabei handelt es sich namentlich um das Vervielfältigungsrecht i.S.d. § 16 UrhG, das Verbreitungsrecht i.S.d. § 17 UrhG sowie das Recht der öffentlichen Zugänglichmachung nach § 19a UrhG.[78]

Jeder Eingriff in diese Verwertungsrechte ist rechtswidrig, sofern der Verwertung nicht ausdrücklich zugestimmt wurde oder der Eingriff nicht ausnahmsweise von einer der gesetzlichen Schrankenregelungen der §§ 44a ff. UrhG gedeckt ist.[79] Diese Schrankenregelungen gelten zwar in erster Linie nur im Verhältnis zum Urheber, allerdings wird deren Anwendungsbereich durch die Verweise in § 85 Abs. 3 UrhG und § 94 Abs. 4 UrhG zugleich auch auf die Tonträger- und Filmhersteller erstreckt. Keine Anwendung finden diese gesetzlichen Erlaubnissätze regelmäßig jedoch gegenüber den Softwareherstellern.[80] Jeder widerrechtliche Eingriff in die Verwertungsrechte der Rechteinhaber löst Unterlassungs- und Schadensersatzersatzansprüche nach dem zentralen urheberrechtlichen Verletzungstatbestand des § 97 UrhG aus. Während der in § 97 Abs. 1 UrhG verankerte Beseitigungs- und Unterlassungsanspruch verschuldensunabhängig gewährt wird, setzt der dortige Schadensersatzanspruch zusätzlich zumindest ein fahrlässiges Handeln des Verletzers voraus. Sollte dem Verletzer darüber hinaus Vorsatz zur Last fallen, ist diese Verletzungshandlung nach den § 106 ff. UrhG zudem strafbewehrt. Die Anwendbarkeit deutschen Urheberrechts hinsichtlich der zivilrechtlichen Verfolgung dieser Rechtsverletzungen folgt aus dem Schutzlandprinzip. Danach ist bei deliktischen Handlungen das Recht

[77] Wandtke/Bullinger/Heerma, § 15, Rn. 11, 19; Möhring/Nicolini/Kroitsch, § 15, Rn. 13.
[78] Vgl. § 69c Nr. 1-4 UrhG, § 85 Abs. 1 S. 1 UrhG, § 94 Abs. 1 S. 1 UrhG.
[79] Ausführlich dazu Hoeren, Access Provider, Rn. 488 ff.
[80] Vgl. Wandtke/Bullinger/Grützmacher, § 69a UrhG, Rn. 74 f.

des Landes anzuwenden, für das Schutz begehrt wird.[81] Sofern die Nutzer eines deutschen Access Providers Urheberrechtsverletzungen im Internet begehen, können diese Verletzungshandlungen somit immer auch vor einem deutschen Gericht geltend gemacht werden.[82]

II. Urheberrechtsverletzungen auf der Nutzerseite

Nachfolgend ist zu untersuchen, in welche Verwertungsrechte die Nutzer eingreifen, wenn sie urheberrechtlich geschützte Werke in Filesharing-Netzwerken oder auf FTP-Servern zum Download bereitstellen oder herunterladen. Anschließend wird der Frage nachgegangen, ob dadurch bedingte Eingriffe ausnahmsweise von einer gesetzlichen Schrankenregelung, insbesondere der Privatkopierschranke des § 53 UrhG, gedeckt werden und damit zulässig sind.[83]

1. Eröffnung einer Downloadmöglichkeit

Das Anbieten von urheberrechtlich geschütztem Material auf einem FTP-Server oder in einem Filesharing-Netzwerk setzt zunächst eine Speicherung des Werkes auf einem Datenträger voraus. Sofern die Werke dazu, wie beim Filesharing üblich, in einen zum Download freigegebenen Ordner oder aber auf einen (FTP-)Server übertragen werden müssen (Upload), stellt die dortige Speicherung – wie jede dauerhafte oder vorübergehende Festlegung auf einem Datenträger – eine Vervielfältigung im Sinne des § 16 UrhG dar.[84] Diese Eingriffe in das Vervielfältigungsrecht der Rechteinhaber sind auch durch keine gesetzliche Schrankenregelung gedeckt. Es handelt sich bei diesen weder um eine nach § 44a UrhG zulässige kurzfristige, technisch bedingte Zwischenspeicherung, noch ist diese Vervielfältigung eine nach § 53 Abs. 1 S. 1 UrhG zulässige Privatkopie. Denn § 53 UrhG nimmt nur zu privaten Zwecken vorgenommene Vervielfältigungen von dem Zustimmungserfordernis aus. Nicht davon erfasst werden jedoch Vervielfältigungen, die zum Zwecke der Eröffnung einer an die Öffentlichkeit gerichteten Downloadmöglichkeit vorgenommen werden.[85] Somit

---

[81] Hoeren, Access Provider, Rn. 420.

[82] Vgl. BGH, Urt. v. 3.3.2004 – 2 StR 109/03, GRUR 2004, 421, 422 – CD-Export; BGH, Urt. v. 26.6.2003 – I ZR 176/01, GRUR, 2003, 876, 877 – Sendeformat; Schricker/Katzenberger, vor § 120 UrhG, Rn. 145.

[83] Zur urheberrechtlichen Zulässigkeit vorbereitender Maßnahmen wie Digitalisierung und Komprimierung von Werken, vgl. Völker, in: Ensthaler/Bosch/Völker, S. 171; Freiwald, Filesharing, S. 126 ff.

[84] Loewenheim/Loewenheim, § 20, Rn. 14 m.w.N.

[85] Jani, ZUM 2003, 842, 848; Berger, ZUM 2004, 257, 258.

ist bereits der ohne Zustimmung der Rechteinhaber vorgenommene Upload urheberrechtlich geschützter Werke rechtswidrig.

Werden diese Daten sodann zum Download freigegeben, wird zudem in das neu geschaffene Verwertungsrecht der öffentlichen Zugänglichmachung aus § 19a UrhG eingegriffen.[86] Dies gilt zumindest dann, wenn die Dateien auf einem für jedermann zugänglichen Server oder aber in einem für jedermann offenen Filesharing-Netzwerk bereitgestellt werden.[87] Nicht von § 19a UrhG erfasst ist hingegen das Bereitstellen von Dateien auf nicht öffentlichen Servern, was z.B. dann der Fall ist, wenn ein FTP-Server mit einem Passwortschutz versehen ist, durch den sichergestellt wird, das nur persönlich verbundene Nutzer auf die Daten zugreifen können.[88] Eine gesetzliche Schrankenregelung für einen Eingriff in § 19a UrhG ist lediglich in § 52a UrhG für den – in den vorliegend zu begutachtenden Konstellationen nicht einschlägigen – Fall vorgesehen, dass urheberrechtlich geschützte Werke zu Forschungs- und Unterrichtszwecken öffentlich zugänglich gemacht werden. Demzufolge ist auch das Bereitstellen einer öffentlichen Downloadmöglichkeit von urheberrechtlich geschützten Werken wegen Verstoßes gegen § 19a UrhG rechtswidrig.

2. Download bereitgestellter Werke

Läd der Nutzer die im Internet angebotenen Werke auf seinen Rechner herunter, begeht er durch die Speicherung auf seinen Datenträgern eine erneute Vervielfältigung i.S.d. § 16 UrhG.[89] Fraglich ist insofern, ob nicht zumindest diese Vervielfältigung von der Privatkopierschranke des § 53 Abs. 1 UrhG gedeckt ist. Voraussetzung dafür ist nach § 53 Abs. 1 S. 1 Hs. 2 UrhG jedoch, dass es sich bei der Quelle des Downloads nicht um eine *„offensichtlich rechtswidrig hergestellte Vorlage“* handelt. Über die Auslegung dieses Tatbestandsmerkmals und dessen Auswirkungen auf die Zulässigkeit von Downloads wird kontrovers diskutiert. Nach einer Auffassung soll es sich bei den fraglichen Downloadangeboten bereits deshalb um rechtswidrige Vorlagen handeln, weil diese zwangsläufig mit einer

[86] OLG Hamburg, Urt. v. 28.4.2005 – 5 U 156/04, MMR 2005, 453, 454 = CR 2005, 512; Berger ZUM 2004, 257, 258; § 19a UrhG ist durch das „Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft“ v. 10. 9. 2003 (sog. Erster Korb), BGBl. I S. 1774, in das UrhG integriert worden; zur Rechtslage vor Inkrafttreten des § 19a UrhG, vgl. Loewenheim/Hoeren, § 21, Rn. 54 ff.

[87] Heghmanns, MMR 2004, 14, 15.

[88] Vgl. Wandtke/Bullinger/Ehrhardt, § 19a UrhG, Rn. 32.

[89] Wandtke/Bullinger/Heerma, § 16 UrhG, Rn. 14; Berger, ZUM 2004, 257, 259.

Rechtsverletzung des § 19a UrhG einhergehen.[90] Dieser Auffassung steht jedoch der Wortlaut des § 53 Abs. 1 S. 1 UrhG entgegen. Dieser stellt hinsichtlich der Rechtswidrigkeit der Vorlage lediglich auf deren Herstellung, nicht aber auf die Zulässigkeit deren Verbreitung ab.[91] Entscheidend ist daher lediglich, ob die öffentlich zugänglich gemachte Vorlage rechtswidrig hergestellt wurde. In dieser Hinsicht drängt sich die Frage auf, ob sich das Kriterium der offensichtlichen Rechtswidrigkeit nach objektiven[92] oder subjektiven[93] Kriterien bemisst. Für eine subjektive Betrachtungsweise spricht der Umstand, dass auch im Gesetzgebungsverfahren hinsichtlich dieses Kriteriums auf die Sichtweise des einzelnen Nutzers abgestellt wurde.[94] Geht man somit – in genetischer Auslegung des § 53 Abs. 1 S. 1 UrhG – von der Maßgeblichkeit der Sichtweise des vervielfältigenden Nutzers aus, ist weiterhin zu klären, wann sich aus dessen Sicht eine Vorlage als offensichtlich rechtswidrig darstellt. Unstreitig ist dies dann der Fall, wenn Musik- oder Filmwerke vor deren Veröffentlichung i.S.d. § 6 Abs. 1 UrhG heruntergeladen werden. Denn in diesen Fällen konnte der Anbieter über kein rechtmäßig erlangtes Exemplar verfügen, von welchem eine rechtmäßige Privatkopie und damit eine rechtmäßige Vorlage hätte angefertigt werden können.[95] Bei bereits erschienenen und zu erwerbenden Werken wird dies hingegen unterschiedlich beurteilt. Teilweise wird vertreten, dass es für den Nutzer in diesen Fällen regelmäßig nicht erkennbar sei, ob es sich bei dem zum Download bereitgestellten Werk um eine rechtmäßige oder rechtswidrige Vorlage handele. Daher seien diese Downloads von der Schrankenregelung des § 53 UrhG gedeckt, sofern sich nicht ausnahmsweise aus den Begleitumständen etwas anderes ergebe.[96]

Nach anderer Auffassung soll zur Beurteilung dieser Frage auf die Kriterien der groben Fahrlässigkeit zurückzugreifen sein. Danach ergebe sich die offensichtliche Rechtswidrigkeit einer Vorlage zumindest bei Filesharing-Netzwerken bereits aus dem Kopierumfeld, da die dort angebotenen Werke nahezu ausnahmslos auf rechtswidrigen Vorlagen beruhen.[97]

Dieser Ansicht ist unter mehreren Gesichtspunkten zuzustimmen. So wird zunächst auch den Nutzern dieser Netzwerke der Umstand bekannt sein,

---

[90] So aber Jani, ZUM 2003, 842, 849.
[91] Berger, ZUM 2004, 257, 259.
[92] So Jani, ZUM 2003, 842, 850 ; Nordemann/Dustmann, CR 2004, 380, 381.
[93] So Wandtke/Bullinger/Lüft, § 53 UrhG, Rn. 15; Berger, ZUM 2004, 257, 260.
[94] Vgl. BT-Drs. 15/1066, S. 2
[95] Wandtke/Bullinger/Lüft, a.a.O.
[96] Wandtke/Bullinger/Lüft, a.a.O.
[97] Berger, ZUM 2004, 257, 258.

dass dort nahezu ausschließlich rechtswidrig erstellte Kopien zum Download angeboten werden. Weiterhin spricht für die offensichtliche Rechtswidrigkeit der dortigen Vorlagen, dass dem Bereitstellen von Werken in Filesharing-Netzwerken oder auf FTP-Servern regelmäßig Vervielfältigungshandlungen vorausgehen, die bereits aufgrund ihrer Zweckrichtung, nämlich dem öffentlichen Anbieten dieser Werke, nicht von der Schrankenregelung des § 53 UrhG gedeckt sind. Weiterhin steht einer extensiven Auslegung der Privatkopierschranke des § 53 UrhG entgegen, dass es sich bei dieser um eine Ausnahmebestimmung zu dem grundsätzlich den Rechteinhabern zustehenden Vervielfältigungsrecht handelt. Als solche ist sie bereits aus dogmatischen Gesichtspunkten restriktiv auszulegen.[98] Der von der erstgenannten Auffassung vertretene Ansatz ist daher dahingehend umzudrehen, dass beim Download von Musik- und Filmwerken aus einem Filesharing-Netzerk oder von FTP-Servern regelmäßig von einer offensichtlich rechtswidrig hergestellten Vorlage auszugehen ist, sofern nicht ausnahmsweise aus den Begleitumständen auf die Rechtmäßigkeit der Vorlage geschlossen werden kann. Generell unzulässig ist hingegen der ohne Zustimmung des Rechteinhabers vorgenommene Download von Computerprogrammen, da die Privatkopierregelung des § 53 UrhG auf diese Werke nicht anwendbar ist.[99]

Selbst wenn ausnahmsweise von einer rechtmäßig erstellten Vorlage ein Download in einem Filesharing-Netzwerk getätigt werden sollte, sind die technischen Besonderheiten einiger Netzwerke zu beachten. So werden z.B. im eDonkey-Netzwerk die Dateien, die jemand heruntergeladen hat, zugleich für andere Nutzer zum Download bereitgestellt, so dass der Nutzer, selbst wenn er einen rechtmäßigen Download tätigt, zugleich auch eine Verletzung des § 19a UrhG begeht.[100]

Der Gesetzgeber wird der Diskussion um das Eingreifen der Privatkopierschranke bei Downloads alsbald durch die Umsetzung des sog. Zweiten Korbes der Urheberrechtsreform ein Ende bereiten. So ist im Gesetzesentwurf[101] vorgesehen, den § 53 UrhG dahingehend zu erweitern, dass die

---

[98] BGH, Urt. v. 11.7.2002 – I ZR 255/00, JurPC, Web-Dok. 302/2002, Abs. 26 – Elektronischer Pressespiegel; BGH, Urt. v. 24.1.2002 – I ZR 102/99, GRUR 2002, 605, 606 – Verhüllter Reichstag.

[99] Schricker/Loewenheim, § 69a UrhG, Rn. 23; Wandtke/Bullinger/Grützmacher, § 69a UrhG, Rn. 75 m.w.N.

[100] Nordemann/Dustmann, CR 2004, 380, 381.

[101] Gesetzesentwurf der Bundesregierung zum Zweiten Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft v. 3.1.2006, abrufbar, unter: http://www.urheberrecht.org/topic/Korb-2/bmj/2006-01-03-Gesetzentwurf.pdf.

Privatkopie nicht nur dann unzulässig ist, wenn die Vorlage offensichtlich rechtswidrig ist, sondern auch dann, wenn die Vorlage offensichtlich rechtswidrig öffentlich zugänglich gemacht wurde, also auch bei Verstößen gegen § 19a UrhG.[102] Da für Eingriffe in § 19a UrhG – mit Ausnahme der Schranke für Forschungs- und Unterrichtszwecke gem. § 52a UrhG – keine gesetzliche Schrankenregelung in Betracht kommt, wird mit dem Erlass dieser Regelung, neben dem Download eines Softwarewerkes, auch jeder ohne Zustimmung der Rechteinhaber vorgenommene Download von Musik- und Filmwerken als rechtswidrig einzustufen sein.

3. Ergebnis

Die ohne Zustimmung des Rechteinhabers vorgenommene Bereitstellung von urheberrechtlich geschützten Werken auf Servern oder in Filesharing-Netzwerken ist wegen Verstoßes gegen § 19a UrhG stets rechtswidrig. Zudem wird regelmäßig auch der Download dieser Werke rechtswidrig sein, da die diesen Vervielfältigungen zugrunde liegenden Vorlagen regelmäßig als offensichtlich rechtswidrig einzustufen sind. Spätestens mit der Umsetzung des Zweiten Korbes der Urheberrechtsreform werden auch Downloads von rechtswidrig bereitgestellten Werken keinesfalls mehr von der Privatkopierschranke des § 53 UrhG gedeckt sein. Damit stehen den Rechteinhabern in diesen Fällen gegen die Nutzer die zivilrechtlichen Unterlassungs- und Schadensersatzansprüche des § 97 UrhG zur Seite.

[102] Gesetzesentwurf, a.a.O., S. 7.

2. Teil: Auskunftsansprüche gegen den Access Provider als Rechtsverletzer

Im ersten Teil der Bearbeitung wurden die technischen, gesellschaftspolitischen und urheberrechtlichen Grundlagen der Urheberrechtspiraterie im Internet dargestellt. Nunmehr geht es um die zentrale Frage, ob die Rechteinhaber gegen die Access Provider einen Anspruch auf Namhaftmachung der für sie anonymen Rechtsverletzer haben, um die ihnen nach § 97 UrhG zustehenden Ansprüche auch geltend machen zu können. In dieser Hinsicht sollen zunächst Anspruchsgrundlagen untersucht werden, deren Passivlegitimation an eine eigenständige Rechtsverletzung des Anspruchsgegners geknüpft ist. Obwohl die Frage der Verletzereigenschaft des Access Providers eng mit den spezialgesetzlichen Haftungsprivilegierungen des Teledienstegesetzes (TDG) sowie des Mediendienstestaatsvertrages (MDStV) verknüpft ist, sollen diese Regelungen vorerst außer Betracht gelassen und das haftungsrelevante Verhalten der Access Provider zunächst nach allgemeinen Regeln beurteilt werden.[103]

A. Drittauskunft gem. § 101a UrhG

Der Auskunftsanspruch nach § 101a UrhG hat sich im Laufe der aktuellen Diskussion um eine Auskunftspflicht des Access Providers über Nutzerdaten sowohl in der Rechtsprechung als auch in der Literatur als aussichtsreichster Anknüpfungspunkt herauskristallisiert. Aufsehen haben in dieser Hinsicht vor allem die – im einstweiligen Verfügungsverfahren ergangenen – Entscheidungen der Landgerichte Köln und Hamburg erregt, in denen die Access Provider auf Grundlage des § 101a UrhG verpflichtet wurden, die Identität von Nutzern offen zu legen, die auf FTP-Servern rechtswidrig mp3-Dateien zum Download angeboten hatten.[104] Die Reaktionen auf diese Urteile waren kontrovers. Während man seitens des Bundesjustizministeriums – entgegen vorheriger Ankündigungen[105] – offenbar keinen Handlungsbedarf zur Umsetzung eines spezialgesetzlichen Auskunftsanspruchs gegen Access Provider mehr sah,[106] sind diese Urteile in der Literatur mit-

[103] Ausführlich zur Haftung des Access Providers im Regelungsbereich des TDG/MDStV, siehe unten, 4. Teil D. E.

[104] LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, CR 2005, 136 m. Anm. Schlegel = MMR 2005, 55 m. Anm. Kaufmann/Köcher; LG Köln, Urt. v. 28.7.2004 – 28 O 301/04, ZUM 2005, 236.

[105] Heise News, Meldung v. 30.6.2004: Justizministerium will Online-Kopierern weitere Steine in den Weg legen, http://www.heise.de/newsticker/meldung/48723.

[106] Dafür spricht die Nichtaufnahme dieses Punktes in die Eckpunkte zur Urheberrechtsreform v. 9.9.2004, abrufbar unter: http://www.bmj.bund.de/media/archive/749.pdf.

unter auf so heftige Kritik gestoßen, dass sogar *„für eine Rückkehr zur Dogmatik“* plädiert wurde.[107] Mittlerweile sind diese Entscheidungen im Berufungsverfahren allerdings entweder aufgehoben oder angesichts einer sich abzeichnenden Niederlage nicht mehr weiterverfolgt worden, mithin hatte keines dieser Urteile auch im Berufungsverfahren Bestand.[108] Im Folgenden sind die im Laufe der Diskussion hervorgebrachten Argumente kritisch zu begutachten. In methodischer Hinsicht empfiehlt es sich zunächst, sich die Entstehungsgeschichte und die Grundkonzeption des § 101a UrhG zu vergegenwärtigen, da diese für dessen Auslegung von entscheidender Bedeutung sind.

I. Entstehungsgeschichte und Grundkonzeption

Der Anspruch auf Drittauskunft[109] gem. § 101a UrhG gehört zu den spezialgesetzlichen Auskunftsansprüchen, die im Jahre 1990 durch das Produktpirateriegesetz (PrPG) vom 7. März 1990[110] in das Urheberrecht und die gewerblichen Schutzrechte integriert wurden.[111] Ziel dieses Gesetzes war es, das Sanktionssystem im gewerblichen Rechtsschutz und im Urheberrecht zu vereinheitlichen.[112] Aufgrund der Vergleichbarkeit der Schutzrechte entschied sich der Gesetzgeber für einen horizontalen Regelungsansatz.[113] So befinden sich neben dem Urheberrecht auch in den anderen Schutzrechten Auskunftsansprüche, die hinsichtlich ihrer Voraussetzungen weitestgehend mit der Auskunftspflicht aus § 101a UrhG korrespondieren.[114]

Hintergrund der Einführung dieser Auskunftsansprüche war die Tatsache, dass den Interessen der Rechteinhaber an der Eindämmung massenhafter und gezielter Schutzrechtsverletzungen mit dem gewohnheitsrechtlich anerkannten und aus den §§ 242, 259, 260 BGB hergeleiteten allgemeinen Auskunftsanspruch nur unzureichend Rechnung getragen wurde. Denn dieser fungiert in erster Linie als Hilfsanspruch zur Durchsetzung eines gegen den Auskunftspflichtigen selbst gerichteten Schadensersatz- oder Beseiti-

---

[107] Vgl. den Titel des Aufsatzes von Kitz, ZUM 2005, 298 ff. *(„§ 101a UrhG: Für eine Rückkehr zur Dogmatik“).*
[108] Vgl. oben, Fn. 12.
[109] Zum Begriff der Drittauskunft, Wiume, S. 56.
[110] BGBl. I S. 442.
[111] Zur Entstehungsgeschichte des PrPG, Oppermann, S. 101 ff.
[112] Amtl. Begründung, BT-Drs. 11/4792, S. 15.
[113] Zum horizontalen Regelungsansatz, Oppermann, S. 106 f.
[114] Vgl. §§ 140b PatG, 24b GebrMG, 19 MarkenG, 14a Abs. 3 GeschmMG, 37b SortenschutzG, 9 HalblSchG.

gungsanspruchs. Dafür sind jedoch zumeist keine Informationen über die Identität der Lieferanten und weiterer Schutzrechtsverletzer notwendig, die der Verletzte jedoch benötigt, um auch gegen diese Vorgehen zu können.[115] Ein solcher auf Drittauskunft gerichteter Anspruch wurde dem Verletzten damals nur unter besonderen Voraussetzungen zugesprochen, etwa als Teil des Schadensersatz- oder Beseitigungsanspruchs im Falle der Verletzung von Preis- und Vertriebsbindungssystemen.[116] Soweit ein solcher Anspruch gewährt wurde, war zudem unklar, ob dieser auch gegen den unvorsätzlich handelnden Rechtsverletzer gerichtet werden konnte. Dies hielt der Gesetzgeber jedoch für zwingend erforderlich, damit sich der unvorsätzliche Rechtsverletzer einer Auskunftspflicht nicht unter Berufung auf seinen guten Glauben entziehen kann. Weiterhin wollte der Gesetzgeber die Durchsetzbarkeit dieser Ansprüche im einstweiligen Verfügungsverfahren sicherstellen, die bis dahin daran scheiterte, dass dies auf eine unzulässige Vorwegnahme der Hauptsache hinauslief.[117]

Mit dem Erlass des PrPG wurde diesen Unzulänglichkeiten bisheriger Auskunftsansprüche Rechnung getragen. So wurden die durch das PrPG geschaffenen Auskunftsansprüche verschuldensunabhängig ausgestaltet. Somit können diese auch gegen den unvorsätzlich handelnden Rechtsverletzer gerichtet werden. Bei offensichtlichen Rechtsverletzungen wird dem Auskunftsgläubiger zudem kraft gesetzlicher Anordnung die Möglichkeit eingeräumt, diesen Anspruch im einstweiligen Verfügungsverfahren durchzusetzen. Darüber hinaus hat der Gesetzgeber darauf verzichtet, die Auskunftspflicht erst im Falle der originären Produktpiraterie, also bei massenhaften und gezielten Schutzrechtsverletzungen, eingreifen zu lassen. Dies ist auf die gesetzgeberische Erkenntnis zurückzuführen, dass die Erscheinungsformen der Produktpiraterie so vielfältig ausgeprägt sind und zudem einem ständigen Wandel unterworfen sind, dass sich der Begriff der Produktpiraterie einer gesetzgeberischen Definition entzieht.[118] Damit es durch eine solche Definition nicht zu Schutzlücken komme, sollten daher zunächst alle Schutzrechtsverletzungen von den Auskunftstatbeständen erfasst werden.[119] Als Korrektiv zu der weiten Auskunftsverpflichtung wurden § 101a UrhG und die weiteren Auskunftsansprüche mit einer Verhält-

[115] Amtl. Begründung, BT-Drs. 11/4792, S. 30.
[116] Näher dazu Wiume, S. 56 ff.; Oppermann, S. 48 ff.
[117] Amtl. Begründung, BT-Drs. 11/4792, S. 31.
[118] Amtl. Begründung, BT-Drs. 11/4792, S. 18; zum Begriff der Produktpiraterie Wiume, S. 104.
[119] Amtl. Begründung, BT-Drs. 11/4792, S. 31; Bohne, Anm. zu OLG Frankfurt a.M., Urt. v. 25.1.2005 – 11 U 51/05, GRUR-RR 2005, 145, 145.

nismäßigkeitsklausel versehen, mittels derer den Gerichten eine flexible Möglichkeit zur Bekämpfung der Produktpiraterie an die Hand gegeben werden sollte.[120]

II. Anwendbarkeit des § 101a UrhG im Onlinebereich

Betrachtet man die Tatbestandsvoraussetzungen der durch das PrPG geschaffenen Auskunftsansprüche, so fällt auf, dass die Tatbestände jeweils an die zentralen Verletzungstatbestände des entsprechenden Schutzgesetzes anknüpfen. Wer also nach den allgemeinen Regeln auf Unterlassung haftet, den trifft auch die spezialgesetzliche Auskunftspflicht über die Vertriebswege der schutzrechtsverletzenden Ware. So sieht der mit § 101a UrhG korrespondierende markenrechtliche Drittauskunftsanspruch nach § 19 MarkenG vor, dass auskunftspflichtig ist, wer eine Rechtsverletzung i.S.d. §§ 14, 15, 17 MarkenG begangen hat. Ebenso kann z.B. der Patentrechtsverletzer, also derjenige, der den §§ 9-13 PatG zuwider handelt, nicht nur auf Unterlassung und Schadensersatz gem. § 139 PatG, sondern gem. § 140b PatG auch auf Auskunft in Anspruch genommen werden. Auch in dieser Hinsicht kommt somit der horizontale Regelungsansatz des Gesetzgebers zum Tragen.

Nach dieser Regelungssystematik wäre zu fordern, dass auch § 101a UrhG auf den zentralen urheberrechtlichen Verletzungstatbestand des § 97 UrhG verweist, so dass auch nach § 101a UrhG jeden eine Auskunftspflicht trifft, der ein durch das Urheberrechtsgesetz geschütztes Recht verletzt hat. Demnach müssten auch alle internetspezifischen Verletzungen der §§ 16, 19a UrhG als auskunftsbegründende Verletzungshandlungen i.S.d. § 101a UrhG zu qualifizieren sein.

Der rechtsgebietsübergreifenden Gesetzesdogmatik zuwider, verweist der Wortlaut des § 101a Abs. 1 UrhG jedoch gerade nicht auf den zentralen Verletzungstatbestand des § 97 UrhG, sondern spricht vielmehr einschränkend von Verletzungshandlungen durch die *„Herstellung oder Verbreitung von Vervielfältigungsstücken“*. Vereinzelt wird diese Abweichung von der Regelungssystematik des PrPG offenbar gar nicht wahrgenommen und schlichtweg unterstellt, dass jede Rechtsverletzung i.S.d. § 97 UrhG eine Auskunftspflicht nach § 101a UrhG begründet.[121] Dies dürfte indes zu weit gehen. Zwar hat sich der Gesetzgeber nicht explizit dazu geäußert, dass er den Tatbestand des § 101a UrhG enger fassen wollte als die Ansprüche in

[120] Amtl. Begründung, BT-Drs. 11/4792, S. 18; Oppermann, S. 113.
[121] So offenbar Oppermann, S.120.

den anderen Schutzgesetzen. Allerdings sollte der Wortlaut des § 101a UrhG, so der Gesetzgeber, an die allgemeine Terminologie des Urheberrechts angepasst werden.[122] Dementsprechend dürften mit Rechtsverletzungen des Herstellungs- und Verbreitungsrechts in erster Linie Rechtsverletzungen der §§ 15 Abs. 2, 16, 17 UrhG gemeint sein, also solche, denen zumeist körperliche Vervielfältigungstücke zugrunde liegen.[123] Vor diesem Hintergrund ist fraglich, ob sich der Anwendungsbereich des § 101a UrhG überhaupt auf unkörperliche, digitale Vervielfältigungsstücke im Onlinebereich erstreckt. Zur Beantwortung dieser Frage ist – in Anlehnung an den Wortlaut des § 101a Abs. 1 UrhG – zunächst zwischen Urheberrechtsverletzungen durch die Herstellung und durch die Verbreitung von digitalen Vervielfältigungsstücken zu differenzieren.

1. Herstellung digitaler Vervielfältigungstücke

Ausweislich seines Wortlauts werden vom Anwendungsbereich des § 101a UrhG zunächst Verletzungshandlungen *„durch die Herstellung (…) von Vervielfältigungsstücken“* erfasst. Dies deutet eindeutig auf Rechtsverletzungen des Vervielfältigungsrechts aus § 16 UrhG hin. Da zudem im Rahmen des § 16 UrhG nicht zwischen körperlichen und digitalen Vervielfältigungsstücken differenziert wird,[124] müssten demnach auch Verletzungshandlungen durch die Herstellung digitaler Vervielfältigungsstücke, z.B. durch rechtswidrige Up- und Downloads, vom Anwendungsbereich des § 101a UrhG erfasst sein.

Dem wird von einer Auffassung entgegengehalten, dass § 101a UrhG bereits deshalb nicht unmittelbar auf digitale Vervielfältigungsstücke anzuwenden sei, weil der Gesetzgeber im Jahre 1990 bei Erlass des PrPG in erster Linie analoge Vervielfältigungsstücke vor Augen gehabt haben dürfte.[125] In dogmatischer Hinsicht läuft diese Argumentation auf eine teleologische Reduktion hinaus. Denn § 101a UrhG soll auf Vervielfältigungshandlungen im Onlinebereich nicht angewendet werden, obwohl sich der Wortlaut dieser Regelung auch auf diese Verletzungshandlungen erstreckt. An dem Vorliegen der Voraussetzungen einer solchen teleologischen Reduktion des § 101a UrhG kann jedoch gezweifelt werden. Das Institut der

---

[122] Amtl. Begründung, BT-Drs. 11/4792, S. 43.
[123] Dreier/Schulze, § 101a UrhG, Rn. 7; Wandtke/Bullinger/Bohne, § 101a UrhG, Rn. 5.
[124] So Loewenheim/Loewenheim, § 20, Rn. 10 f.; HK-UrhG, § 16, Rn. 6.
[125] Sieber/Höfinger, MMR 2004, 575, 577; Manz, S. 91; für eine analoge Anwendung bei Verletzungen des § 16 UrhG Wandtke/Bullinger/Bohne, § 101a UrhG, Rn. 6; v.Ohlenhusen/Crone, WRP 2002, 164, 166.

teleologischen Reduktion dient nämlich dazu, den zu weit gefassten Wortsinn einer Norm auf den ihr nach dem Regelungszweck oder Sinnzusammenhang des Gesetzes zukommenden Anwendungsbereich zu reduzieren.[126] Seine Rechtfertigung findet es in dem Gebot der Gerechtigkeit, das gebietet, Ungleiches auch ungleich zu behandeln.[127] Eine teleologische Reduktion des § 101a UrhG auf körperliche Vervielfältigungsstücke wäre somit nur dann gerechtfertigt, wenn tatsächlich eine Gleichbehandlung dieser Verletzungshandlungen im Rahmen des § 101a UrhG nicht gerechtfertigt wäre. Für das Bedürfnis einer solchen Ungleichbehandlung wird angeführt, dass sich die Situation des Auskunftspflichtigen im Onlinebereich erheblich von der im Offlinebereich unterscheide. So lasse sich die Auskunft im Offlinebereich zumeist anhand von schriftlichen Aufzeichnungen rekonstruieren, wohingegen sich die Auskunftserteilung im Onlinebereich schwieriger gestalte und oftmals datenschutzrechtliche Belange und das Fernmeldegeheimnis tangiere.[128]

Dieser Auffassung ist zunächst zuzugeben, dass einer Auskunftspflicht nach § 101a UrhG in der Tat sowohl rechtliche Vorschriften, wie etwa die Haftungsprivilegierungen nach dem TDG bzw. des MDStV, datenschutzrechtliche Vorschriften oder das Fernmeldegeheimnis entgegenstehen können. Zu weit würde es jedoch gehen, aufgrund dieser Tatsache bereits den Anwendungsbereich des § 101a UrhG für Rechtsverletzungen im Onlinebereich insgesamt entfallen zu lassen. Denn sofern für eine Auskunftserteilung aus tatsächlichen Gründen enorme Aufwendungen zu tätigen sind, ist dies eine Frage der Verhältnismäßigkeit, der eigens durch die Verhältnismäßigkeitsklausel des § 101a Abs. 1 UrhG Rechnung getragen wurde und die daher auch an dieser Stelle erörtert werden sollte. Ferner sind auch datenschutz- und telekommunikationsrechtliche Vorschriften, die einer Auskunftspflicht entgegenstehen könnten, nicht im Rahmen der Tatbestandsvoraussetzungen des § 101a UrhG zu erörtern. Dogmatisch handelt es sich dabei um Fragen einer rechtlichen Unmöglichkeit gem. § 275 BGB, die auf der Ebene der rechtshindernden Einwendungen zu berücksichtigen sind.[129] Zu Recht hat daher auch das Münchener Landgericht einen Rechtsverletzer auf der Grundlage des § 101a UrhG zur Auskunft über die Herkunft von Bildern verpflichtet, die dieser unter Verletzung des Vervielfältigungsrecht

[126] Larenz/Canaris, Methodenlehre, S. 210 f.
[127] Larenz/Canaris, Methodenlehre, S. 211.
[128] So Sieber/Höfinger, MMR 2004, 575, 577.
[129] Kitz, ZUM 2005, 298, 301.

des § 16 UrhG aus dem Internet heruntergeladen hatte.[130] Denn in diesem Fall war die Auskunftserteilung weder unverhältnismäßig i.S.d. § 101a Abs. 1 UrhG noch verstieß diese gegen ein gesetzliches Verbotsgesetz.

Zudem spricht auch der Regelungsgehalt des § 97 UrhG gegen eine teleologische Reduktion des § 101a UrhG auf analoge Vervielfältigungsstücke. Denn auch im Rahmen des § 97 UrhG wird nicht zwischen analogen und digitalen Vervielfältigungsstücken differenziert, sondern nur der Verstoß gegen das Vervielfältigungsrecht des § 16 UrhG als solches sanktioniert, obwohl auch der Gesetzgeber des § 97 UrhG in erster Linie analoge Vervielfältigungsstücke vor Augen gehabt haben durfte. Vor diesem Hintergrund ist somit auch eine teleologische Reduktion des § 101a UrhG auf körperliche Vervielfältigungshandlungen nicht gerechtfertigt. Mithin ist § 101a UrhG auch bei Rechtsverletzungen des § 16 UrhG durch die Herstellung digitaler Vervielfältigungsstücke unmittelbar anwendbar.[131]

2. Verbreitung digitaler Vervielfältigungsstücke

Weiterhin werden vom Wortlaut des § 101a Abs. 1 UrhG Rechtsverletzungen *„durch die (…) Verbreitung von Vervielfältigungsstücken“* erfasst.

a) Unmittelbare Anwendbarkeit des § 101a UrhG

In dieser Hinsicht könnte man zunächst daran denken, auch die unkörperliche Verbreitung von Vervielfältigungsstücken im Internet unmittelbar unter das Merkmal des Verbreitens zu subsumieren. Dies vertritt offenbar das Kölner Landgericht[132], nach dessen Ansicht § 101a UrhG auch dann unmittelbar anwendbar sein soll, wenn jemand Musikdateien im Internet auf einem FTP-Server zum Download bereithält. So führt das Gericht aus, dass derjenige, der die Downloadmöglichkeit anbiete und den Download zulasse, als Lieferant und somit als Verbreiter des Vervielfältigungstücks angesehen werden müsse.[133] Bedeckt hielt sich das Gericht jedoch hinsichtlich der Frage, ob es den Betrieb des FTP-Servers als eine – unstreitig von § 101a UrhG erfasste – Verletzung des Verbreitungsrechts des § 17 UrhG oder aber als Verletzung des Rechts der öffentlichen Zugänglichmachung gem. § 19a UrhG qualifiziert, mit der Folge, dass auch Rechtsverletzungen

[130] LG München, Urt. v. 7.5.2003 – 21 O 5250/03, MMR 2004, 192, 193 = JurPC Web-Dok. 286/2003 – Onlinefotos.
[131] So auch Kitz, ZUM 2005, 298, 299.
[132] LG Köln, Urt. v. 28.7.2004 – 28 O 301/04, ZUM 2005, 236.
[133] LG Köln, Urt. v. 28.7.2004 – 28 O 301/04, ZUM 2005, 236, 238.

des § 19a UrhG unmittelbar unter den Verbreitungsbegriff des § 101a UrhG zu fassen wären.

Beiden Ansätzen kann nicht gefolgt werden. Zunächst kann die Verbreitung von digitalen Vervielfältigungsstücken über das Internet nicht als Verbreitungshandlung i.S.d. § 17 UrhG angesehen werden. Denn § 17 UrhG setzt voraus, dass ein körperliches Vervielfältigungsstück seinen Besitzer wechselt. Dies ist beim Onlineabruf jedoch gerade nicht der Fall.[134] Zudem ist auch einer erweiternden Auslegung des § 17 UrhG auf Onlinesachverhalte seit der Integration des § 19a UrhG im Jahre 2003 die Grundlage entzogen worden. Dadurch ist nämlich die Verbreitung von digitalen Inhalten durch das Internet eindeutig dem Recht der öffentlichen Zugänglichmachung gem. § 19a UrhG zugeordnet worden. Somit können diese Rechtsverletzungen bereits unter dem Gesichtspunkt der Spezialität nicht mehr unter § 17 UrhG gefasst werden.[135]

Zudem können Rechtsverletzungen des § 19a UrhG auch nicht unmittelbar unter den Verbreitungsbegriff des § 101a UrhG gefasst werden. Dem steht entgegen, dass mit der ausdrücklichen Benennung des Rechts der öffentlichen Zugänglichmachung ein neuer Terminus in das Urheberrecht Einzug gehalten hat, ohne dass zugleich auch der Tatbestand des § 101a UrhG um den Begriff der öffentlichen Zugänglichmachung erweitert wurde. Daher kommt allenfalls eine analoge Anwendung des § 101a UrhG auf Rechtsverletzungen des § 19a UrhG in Betracht.

b) Analoge Anwendung auf Verletzungen des § 19a UrhG

Voraussetzung für eine analoge Anwendung des § 101a UrhG auf Verletzungen des § 19a UrhG ist zunächst, dass § 101a UrhG einer Analogie überhaupt zugänglich ist. Sollte dies der Fall sein, ist darüber hinaus zu fordern, dass sich die Nichtaufnahme des Terminus der öffentlichen Zugänglichmachung in den Anwendungsbereich des § 101a UrhG als planwidrige Regelungslücke darstellt. Weiterhin muss auch eine hinreichende Ähnlichkeit zwischen einer Auskunftspflicht bei Verletzungen des § 19a UrhG und Verletzungen der §§ 16, 17 UrhG bestehen.

---

[134] Loewenheim/Hoeren, § 21, Rn. 64; Freiwald, Filesharing, S. 132 m.w.N.

[135] LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, CR 2005, 135, 136 = MMR 2005, 55; Freiwald, Filesharing, S. 133.

aa) Analogiefähigkeit des § 101a UrhG

Teilweise wird dem § 101a UrhG bereits die Analogiefähigkeit abgesprochen. Dies soll daraus resultieren, dass § 101a UrhG nach seinem Wortlaut eben nur die Verletzung der körperlichen Verwertungsrechte der §§ 15 Abs. 1, 16, 17 UrhG erfasst. Dieser beziehe weder die unkörperlichen Verwertungsrechte i.S.d. § 15 Abs. 2 UrhG mit ein, noch das körperliche Ausstellungsrecht gem. § 18 UrhG. Damit handele es sich bei § 101a UrhG um einen Ausnahmetatbestand, der als solcher schon dogmatisch einer erweiternden Auslegung bzw. einer Analoge entzogen sei.[136]

Dem kann in dieser Pauschalität nicht gefolgt werden. Dieser Auffassung ist zwar zuzugeben, dass Ausnahmetatbestände regelmäßig eng auszulegen sind. Nicht zutreffend ist jedoch die Annahme, dass diese deshalb auch stets einer analogen Anwendung entzogen sind. Denn das Gebot der restriktiven Auslegung von Ausnahmetatbeständen ist lediglich darauf zurückzuführen, dass bei diesen die Gefahr besonders groß ist, dass die Regelungsabsicht des Gesetzgebers durch eine zu weite Auslegung in ihr Gegenteil verkehrt wird.[137] Im Wege eines *argumentum e contrario* lässt sich daraus jedoch zugleich ableiten, dass Ausnahmetatbestände zumindest in den Fällen analog angewendet werden können, in denen eine Analogie ausnahmsweise mit dem Willen des Gesetzgebers korrespondiert. In dieser Hinsicht sind also insbesondere die Gesetzesmaterialien heranzuziehen. In diesen führte der historische Gesetzgeber des PrPG aus, dass es vorrangiges Ziel dieses Gesetzes sei, gezielte und massenhafte Schutzrechtsverletzungen zu bekämpfen.[138]

Im Gegensatz zu Verletzungen des § 18 UrhG, die allenfalls Einzelfallcharakter haben, wird dieser Schutzzweck durch die massenhaften Schutzrechtsverletzungen des § 19a UrhG mittlerweile jedoch in erheblichem Maße tangiert. Somit kann auch nicht davon ausgegangen werden, dass eine analoge Anwendung des § 101a UrhG auf Rechtsverletzungen des § 19a UrhG den Willen des Gesetzgebers des PrPG konterkariert. Mithin ist § 101a UrhG in Bezug auf Rechtsverletzungen des § 19a UrhG einer Analogie durchaus zugänglich.

---

[136] Linke, Anm. zu OLG Hamburg, Urt. v. 28.4.2005 – 5 U 156/04, MMR 2005, 456, 457.
[137] Larenz/Canaris, Methodenlehre, S. 176.
[138] Amtl. Begründung zum PrPG, BT-Drs. 11/4792, S. 30.

bb) Planwidrige Regelungslücke

Voraussetzung für eine analoge Anwendung des § 101a UrhG auf Rechtsverletzungen des § 19a UrhG ist zunächst, dass sich die Nichterstreckung des Anwendungsbereichs auf diese Verletzungshandlungen als planwidrige Regelungslücke darstellt. Die Begründung einer planwidrigen Regelungslücke setzt jedoch nicht nur das Fehlen einer gesetzlichen Regelung voraus, sondern erfordert darüber hinaus, dass sich ihr Fehlen nach der Systematik des Gesetzes und nach den vom Gesetzgeber zu Grunde gelegten Wertungen als „planwidrige Unvollständigkeit" des Gesetzes darstellt.[139]

(1) Ursprüngliche Beschränkung auf körperliche Verwertungshandlungen

Vereinzelt wird behauptet, dass es an der Planwidrigkeit des § 101a UrhG bereits deshalb mangelt, weil der Gesetzgeber schon bei Erlass des § 101a UrhG die Möglichkeit der Verbreitung unkörperlicher Vervielfältigungsstücke durch digitale Datennetze vorhergesehen und die Anwendbarkeit des § 101a UrhG in dieser Kenntnis bewusst auf körperliche Vervielfältigungsstücke i.S.d. § 17 UrhG beschränkt hat.[140] Begründet wird dies damit, dass der Gesetzgeber bereits 1990 die Kommunikation über digitale Datennetze – wie z.B. durch BTX und Modemverbindungen – gekannt habe. Da die Informationsmittlung über solche Datennetze bereits damals von der herrschenden Meinung als Unterfall der unkörperlichen Verwertung angesehen wurde,[141] hätte es nach dieser Auffassung nahe gelegen, den Tatbestand auch auf unkörperliche Urheberrechtsverletzungen zu erstrecken.[142]

Dieser Ansicht ist jedoch entgegenzuhalten, dass unkörperliche Verwertungshandlungen über digitale Datennetze im Jahre 1990 allenfalls Einzelfallcharakter besaßen und bereits deshalb nicht in den Fokus des Gesetzgebers rückten. Dieser wollte vornehmlich die Verletzung solcher Verwertungsrechte mit einer Auskunftspflicht belegen, die besonders häufig verletzt werden.[143] Solche massenhaften Rechtsverletzungen haben sich damals jedoch vor allem in Gestalt der Verletzung des Herstellungs- und Verbreitungsrechts manifestiert, nicht aber in Gestalt unkörperlicher Verbreitungshandlungen i.S.d. § 15 Abs. 2 UrhG. Der Annahme, dass der

[139] Larenz/Canaris, Methodenlehre, S. 194.
[140] Sieber/Höfinger, MMR 2004, 575, 576.
[141] Vgl. Schricker/v. Ungern-Sternberg, § 19a UrhG, Rn. 34 ff. m.w.N.
[142] Sieber/Höfinger, MMR 2004, 575, 576.
[143] Amtl. Begründung zum PrPG, BT-Drucks. 11/4792, S. 30.

Gesetzgeber bereits bei Erlass des PrPG die Gefahr massenhafter Schutzrechtsverletzungen durch unkörperliche Verbreitungshandlungen vorausgesehen hat und diese bewusst nicht dem Anwendungsbereich des PrPG unterwerfen wollte, ist somit zu widersprechen.

(2) Begründung einer nachträglichen Planwidrigkeit

In Betracht kommt vielmehr, dass die Nichterstreckung des Tatbestandes auf Rechtsverletzungen des § 19a UrhG zumindest als nachträglich entstandene Planwidrigkeit des § 101a UrhG zu werten ist. Eine solche wird insbesondere dadurch begründet, dass infolge des technischen oder wirtschaftlichen Fortschritts neue Fragen aufgeworfen werden, die nunmehr einer Regelung bedürfen, die der Gesetzgeber bei Erlass der Norm noch nicht gesehen hat.[144] Auch der Gesetzgeber des § 101a UrhG konnte die seit Ende der neunziger Jahre stark ansteigende Zahl von Schutzrechtsverletzungen durch unkörperliche Verwertungshandlungen im Internet nicht voraussehen. Zudem wird in den Gesetzesmaterialien explizit darauf hingewiesen, dass Schutzrechtsverletzungen auch innerhalb des jeweiligen Schutzrechts – wie hier im Urheberrecht – einem ständigem Wandel unterworfen sind und daher die Gefahr besteht, dass die Tatbestände des PrPG bei einer zu engen Fassung der Tatbestandsvoraussetzungen bereits in kurzer Zeit überholt sein könnten und leer zu laufen drohen.[145] So liegt es auch in den vorliegenden Konstellationen. Denn mit der Verlagerung der urheberrechtlichen Produktpiraterie auf den Onlinebereich sind zugleich auch die körperlichen Verbreitungshandlungen i.S.d. § 17 UrhG durch unkörperliche Verwertungshandlungen gem. § 19a UrhG substituiert worden. Gemessen an der Regelungsabsicht des historischen Gesetzgebers, der eine umfassende Eindämmung von massenhaften Schutzrechtsverletzungen vor Augen hatte, kann die Nichterstreckung des § 101a UrhG daher nur als nachträglich entstandene planwidrige Regelungslücke gewertet werden.

(3) Nachträgliche bewusste Nichtregelung

Diese nachträgliche Planwidrigkeit könnte jedoch dadurch wieder entfallen sein, dass sich der Gesetzgeber in der Zwischenzeit bewusst gegen die Erstreckung des Tatbestandes auf unkörperliche Verwertungshandlungen ausgesprochen hat. Für diese Annahme lässt sich anführen, dass der Tatbestand des § 101a UrhG bei Einführung des § 19a UrhG, im Gegensatz zu

[144] Larenz/Canaris, Methodenlehre, S. 200.
[145] Amtl. Begründung zum PrPG, BT-Drs 11/4792, S. 18.

vielen anderen Vorschriften,[146] nicht um den Terminus der öffentlichen Zugänglichmachung erweitert wurde. Zumindest wird man dies nicht als offensichtliches Versäumnis des Gesetzebers ansehen können,[147] da das Urheberrechtsgesetz schon vor Einführung des § 19a UrhG Gegenstand diverser Gesetzgebungsverfahren war, durch die dieses Gesetz an die Bedürfnisse der Informationsgesellschaft angepasst wurde, ohne dass zugleich der Tatbestand des § 101a UrhG auf unkörperliche Verwertungshandlungen erstreckt wurde.[148] Zu weit geht es jedoch, daraus den Umkehrschluss zu ziehen, dass der Gesetzgeber die planwidrige Regelungslücke in eine – die Analogie ausschließende – planmäßige Lücke verwandelt hat. Denn es bleibt zu berücksichtigen, dass § 101a UrhG nie selbst Gegenstand dieser Gesetzgebungsverfahren war. Somit lassen sich in dieser Hinsicht auch keine Gesetzesmaterialien rekurrieren, aus denen hervorgeht, dass sich der Gesetzgeber bewusst gegen eine Erstreckung des Anwendungsbereichs des § 101a UrhG auf Rechtsverletzungen des § 19a UrhG ausgesprochen hat.[149]

Dies ergibt sich auch nicht daraus, dass bereits im Vorfeld der Umsetzung des Ersten Korbes der Urheberrechtsreform ein Auskunftsanspruch gegen Provider in Gestalt des § 101b UrhG gefordert,[150] jedoch nicht umgesetzt wurde.[151] Dieser Tatsache kann zwar entnommen werden, dass sich der Gesetzgeber bewusst mit der Thematik der Auskunftsansprüche auseinandergesetzt hat. Allerdings lassen sich daraus keine unmittelbaren Rückschlüsse auf die Anwendbarkeit des § 101a UrhG auf Verletzungen des § 19a UrhG ziehen. Denn der geforderte Auskunftsanspruch sollte verletzungsunabhängig ausgestaltet werden und bezog sich daher lediglich auf die – noch zu prüfende – Frage, ob der Access Provider auch unabhängig von einer eigenen Verletzungshandlung i.S.d. § 101a UrhG als Nichtverletzer auf Auskunft in Anspruch genommen werden kann.[152] Somit wird

---

[146] Z.B. §§ 85 Abs. 1 S. 1, 95 Abs. 1 S. 1 UrhG .

[147] So aber LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, CR 2005, 135, 136 = MMR 2005, 55.

[148] Ausführlich dazu Sieber/Höfinger, MMR 2004, 575, 577.

[149] So auch LG Köln, Urt. v. 26.7.2004 – 28 O 301/04, ZUM 2005, 236, 239.

[150] Vgl. Stellungnahme des Forums der Rechteinhaber v. Oktober 2002, S. 8, abrufbar unter: http://www.urheberrecht.org/topic/Info-RiLi/st/Forum-RegEntw.pdf , sowie Stellungnahme zum Referentenentwurf eines Zweiten Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft v. 15.11.2004, S. 9, abrufbar unter: http://www.urheberrecht.org/topic/Korb-2/st/refentw/RefEntw-Korb2.pdf.

[151] So Sieber/Höfinger, MMR 2004, 575, 577; Kaufmann/Köcher, Anm. zu LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, MMR 2005, 61, 61.

[152] Vgl. dazu unten, 3. Teil A. B.

die nachträgliche Planwidrigkeit des § 101a UrhG in Bezug auf Verletzungen des § 19a UrhG auch durch die Nichteinführung eines verletzungsunabhängigen Auskunftsanspruchs nicht erschüttert.

(4) Zwischenergebnis

Die Regelung des § 101a UrhG ist hinsichtlich der Nichterstreckung des Anwendungsbereichs auf Verletzungen des Rechts der öffentlichen Zugänglichmachung aus § 19a UrhG planwidrig unvollständig. Mithin liegt eine planwidrige Regelungslücke vor.

cc) Vergleichbarkeit der Interessenlage

Darüber hinaus muss auch eine hinreichende Vergleichbarkeit zwischen den gesetzlich geregelten Auskunftspflichten bei Rechtsverletzungen der §§ 16, 17 UrhG und einer Auskunftspflicht bei Rechtsverletzungen des § 19a UrhG bestehen, und zwar sowohl auf der Seite des Verletzten als auch auf der des Verletzers.[153]

(1) Vergleichbarkeit auf der Seite des Verletzten

Für eine Vergleichbarkeit der Interessenlage auf der Seite der verletzten Rechteinhaber spricht zunächst eine wirtschaftliche Betrachtung. Denn körperliche und unkörperliche Verbreitungshandlungen unterscheiden sich lediglich in der Form der Übermittlung, nicht jedoch in wirtschaftlicher Hinsicht. Da der Rechteinhaber in beiden Fällen dadurch einen Schaden erleidet, dass er durch Dritte an der ihm zustehenden wirtschaftlichen Verwertung seiner Werke gehindert wird, spricht zunächst vieles dafür, diese Sachverhalte auch gleich zu behandeln.[154]

Vereinzelt wird jedoch vertreten, dass eine Vergleichbarkeit in wirtschaftlicher Hinsicht nicht gegeben sei, weil auch im Rahmen des Erschöpfungsgrundsatzes stets zwischen körperlichen und unkörperlichen Verbreitungshandlungen unterschieden werde.[155] Warum dies allerdings gegen die Einbeziehung von Verletzungshandlungen des § 19a UrhG in den Anwendungsbereich des § 101a UrhG sprechen sollte, ist indes nicht ersichtlich. Bereits aus der Tatsache, dass die Einschränkung der wirtschaftlichen Verwertungsmöglichkeiten durch den Erschöpfungsgrundsatz nur für kör-

[153] Kitz, GRUR 2003, 1014, 1017, allerdings in Bezug auf eine analoge Anwendung des § 101a UrhG auf den Nichtverletzer; siehe unten, 3.Teil A.
[154] Loewenheim/Hoeren, § 21, Rn. 64 f. m.w.N.
[155] Spindler/Dorschel, CR 2005, 38, 40.

perliche Vervielfältigungen i.S.d. § 17 UrhG, nicht aber auch für die öffentliche Zugänglichmachung gilt,[156] lässt sich nämlich entnehmen, dass der Inhaber des Rechts der öffentlichen Zugänglichmachung gem. § 19a UrhG angesichts seines umfassenderen Schutzrechts noch schutzbedürftiger ist als der Inhaber eines Verbreitungsrechts nach § 17 UrhG. Dieser Umstand spricht somit eher für als gegen eine Planwidrigkeit des § 101a UrhG in Bezug auf Rechtsverletzungen des § 19a UrhG.

Neben den wirtschaftlichen Interessen des Verletzten muss zudem berücksichtigt werden, dass die Rechteinhaber auch bei Rechtsverletzungen im Onlinebereich auf die Auskunft über weitere Verletzer angewiesen sind, um den Umfang der Rechtsverletzung abschätzen zu können. Dieses Bedürfnis ist im Onlinebereich sogar noch höher, da sich bei Verwertungshandlungen im Internet die Herkunft und die Vertriebswege oftmals noch schwieriger rekonstruieren lassen als bei herkömmlichen Schutzrechtsverletzungen.[157] Somit ist zumindest auf der Seite der Rechteinhaber von einer vergleichbaren Interessenlage auszugehen ist.

(2) Vergleichbarkeit auf der Seite des Verletzers

In Bezug auf die Vergleichbarkeit der Interessenlage auf der Seite des Verletzers werden zumeist dieselben Einwände hervorgebracht, wie sie bereits im Rahmen der obigen Ausführungen zur teleologischen Reduktion des § 101a UrhG bei Rechtsverletzungen durch digitale Vervielfältigungshandlungen erörtert wurden. Wie oben bereits ausgeführt, sind jedoch tatsächliche Einwände gegen die Auskunftserteilung im Rahmen der Verhältnismäßigkeitsprüfung und rechtliche Verbotsvorschriften auf der Ebene der rechtshindernden Einwendungen zu berücksichtigen.

Weiterhin wird seitens des OLG Hamburg[158] gegen eine Vergleichbarkeit auf der Seite des Rechtsverletzers eingewendet, dass bei Rechtsverletzungen des § 19a UrhG, im Gegensatz zu denen des § 17 UrhG, zumeist keine Vertriebskette im herkömmlichen Sinne vorliege. So könne der Access Provider bereits aus tatsächlichen Gründen lediglich Auskunft über die Identität eines einzelnen Verletzers geben. Die Offenlegung einzelner

[156] Vgl. Art. 3 Abs. 3 Richtlinie 2001/29/EG (InfoSoc-RL); Dreier/Schulze, § 19a UrhG, Rn. 11.

[157] Wandtke/Bullinger/Bohne, § 101a UrhG, Rn. 1 geht daher davon aus, dass § 101a UrhG gerade im Onlinebereich wachsende Bedeutung zukommen wird.

[158] OLG Hamburg, Urt. v. 28.4.2005 – 5 U 156/04, MMR 2005, 453 = CR 2005, 512 ; OLG Frankfurt a.M., Urt. v. 25.1.2005 – 11 U 51/05, MMR 2005, 241, 243 = CR 2005, 285.

Rechtsverletzer sei jedoch mit dem Sinn und Zweck der Auskunftspflichten des § 101a UrhG nicht vereinbar.[159]

Dem ist in zweierlei Hinsicht zu widersprechen. Erstens wird auch im Offlinebereich, z.B. der Spediteur, in der Regel nur Auskunft über die Identität einzelner Auftraggeber geben können, nicht aber über die einzelnen Glieder einer mitunter langen Vertriebskette. Zweitens dient der § 101a UrhG der Ausschaltung jeglicher Quellen von Urheberrechtsverletzungen, mithin auch des einzelnen Rechtsverletzers.[160] Dies muss erst recht im Onlinebereich gelten. Denn die Loslösung der Produktpiraterie von den herkömmlichen aufwendigen Vertriebsstrukturen, verbunden mit der Möglichkeit des weltweiten Abrufs der bereitgestellten Werke, macht die einzelne Rechtsverletzung des § 19a UrhG noch gefährlicher als eine herkömmliche Schutzrechtsverletzung i.S.d. § 17 UrhG. Zudem haben die Fahndungserfolge der GVU[161] in Zusammenarbeit mit der Staatsanwalt in der Sache ftp-welt.de gezeigt, dass der Verletzer des § 19a UrhG oftmals sehr wohl in der Lage ist, mehr als nur einen Abnehmer offen zu legen, auch wenn die Auskunftserteilung in diesem Verfahren freilich strafrechtlich bedingt war und nicht auf § 101a UrhG beruhte.[162]

Bekräftigt wird die Vergleichbarkeit dieser Rechtsverletzungen auch dadurch, dass Verletzungen des § 16 UrhG und des § 19a UrhG im Onlinebereich eng miteinander einhergehen. Wer z.B. auf seiner Homepage rechtswidrig Bilder unter Verstoß des § 19a UrhG bereitstellt, der wird diese Werke zumeist auch rechtswidrig i.S.d. § 16 UrhG vervielfältigt haben. Daher könnte der Rechtsverletzer in diesen Fällen – auch unabhängig von einer Rechtsverletzung des § 19a UrhG – bereits aufgrund des Verstoßes gegen das Vervielfältigungsrecht des § 16 UrhG gem. § 101a UrhG auf Auskunft über die Herkunft dieser Werke in Anspruch genommen werden.

Auch vor diesem Hintergrund ist nicht ersichtlich, warum der Rechtsverletzer des § 19a UrhG hinsichtlich seiner Auskunftspflicht gegenüber denjenigen der §§ 16, 17 UrhG privilegiert werden sollte, sofern auch dieser in der Lage ist, eine entsprechende Auskunft unter zumutbarem Aufwand zu erteilen. Somit ist auch auf der Seite des Verletzers eine vergleichbare Inte-

---

[159] OLG Hamburg, Urt. v. 28.4.2005 – 5 U 156/04, MMR 2005, 453, 455 = CR 2005, 512.

[160] Amtl. Begründung, BT-Drs. 11/4792, S. 31; Bohne, Anm. zu OLG Frankfurt a.M., Urt. v. 25.1.2005 – 11 U 51/05, GRUR-RR 2005, 145, 145.

[161] Gesellschaft für die Verfolgung von Urhebererrechtsverletzungen e.V.

[162] Heise News, Meldung v. 17.9.2004: Warez-Razzia: FTPWelt-Nutzer müssen mit Strafverfahren rechnen, http://www.heise.de/newsticker/meldung/51196

ressenlage zu bejahen, so dass die Voraussetzungen für eine analoge Anwendung des § 101a UrhG auf Rechtsverletzungen des § 19a UrhG insgesamt gegeben sind.

3. Zwischenergebnis

Der Tatbestand des § 101a UrhG ist auch auf den Onlinebereich anwendbar. Während bei Rechtsverletzungen des § 16 UrhG durch die Herstellung digitaler Vervielfältigungsstücke eine direkte Anwendbarkeit gegeben ist, liegen bei Verletzungen des § 19a UrhG zumindest die Voraussetzungen für eine analoge Anwendung des § 101a UrhG vor.

III. Rechtsverletzung im geschäftlichen Verkehr

Weiterhin setzt § 101a UrhG voraus, dass die Rechtsverletzung im geschäftlichen Verkehr erfolgt ist. Der Terminus des geschäftlichen Verkehrs entstammt dem UWG, so dass insoweit auf die hierzu ergangene wettbewerbsrechtliche Rechtsprechung zurückgegriffen werden kann.[163] Danach sind geschäftliche Handlungen solche, die mit dem Erwerb oder der Berufsausübung eines Einzelnen zusammenhängen, mithin alles, was sich nicht im rein privaten oder amtlichen Bereich abspielt.[164] Sinn und Zweck dieser Beschränkung des Tatbestandes ist es, private Letztverbraucher von der Auskunftspflicht auszunehmen, da von diesen keine weiteren Schutzrechtsverletzungen mehr zu befürchten seien.[165] In diesem Zusammenhang ist auch § 101a Abs. 2 UrhG zu sehen, nach dem nur Auskunft über gewerbliche Abnehmer zu erteilen ist.

Diese Beschränkung des Tatbestandes erscheint bei Rechtsverletzungen im Onlinebereich allerdings nicht mehr sachgerecht. Denn gerade dort zeichnen sich Urheberrechtsverletzungen dadurch aus, dass sie erst durch das arbeitsteilige Verhalten privater Endnutzer ermöglicht werden. Daher sollte dem Vorschlag gefolgt werden, den Anwendungsbereich des § 101a UrhG bereits dann als eröffnet anzusehen, wenn die Nutzung von digitalen Inhalten über den urheberrechtsfreien Bereich der privaten Nutzung gem. § 53 UrhG bzw. über den bestimmungsgemäßen Bereich der Nutzung nach § 69d Abs. 1 UrhG hinausgeht.[166] In diesen Fällen sollte sowohl Auskunft

[163] Wandtke/Bullinger/Bohne, § 101a UrhG, Rn. 7.
[164] BGH, Urt. v. 14.7.1961 – I ZR 40/60, GRUR 1962, 45, 47 – Betonzusatzmittel; BGH, Urt. v. 3.4.1981 – I ZR 41/80, GRUR 1981, 665, 666 – Knochenbrecherin.
[165] Amtliche Begründung zum PrPG, BT-Drs. 11/4792, S. 32.
[166] Dreier/Schulze, § 101a UrhG, Rn. 10.

von als auch über den nicht gewerblich agierenden Rechtsverletzer verlangt werden können.

Im Rahmen des Access Providing ist das Merkmal der Handlung im geschäftlichen Verkehr hingegen unproblematisch zu bejahen, da der Geschäftszweck des Access Providers gerade in der Bereitstellung des Internetzugangs besteht. Da es ferner unerheblich ist, ob mit der Handlung im geschäftlichen Verkehr auch die Erzielung eines Gewinns beabsichtigt wird,[167] wird dieses Kriterium auch von nicht kommerziellen Anbietern – wie z.B. dem Betreiber des Deutschen Forschungsnetzes (DFN) – erfüllt.

IV. Passivlegitimation des Access Providers

Nachdem soeben erarbeitet wurde, dass sich der Anwendungsbereich des § 101a UrhG auch auf Rechtsverletzungen der §§ 16, 19a UrhG erstreckt, gilt es nunmehr die Frage zu beantworten, ob auch der Access Provider eine auskunftsbegründende Rechtsverletzung i.S.d. § 101a UrhG begeht, wenn er den Nutzern die Dienstleistungen zur Verfügung stellt, die von diesen für Urheberrechtsverletzungen genutzt werden.[168] In dieser Hinsicht soll zunächst das haftungsrelevante Verhalten der Access Provider nach den allgemeinen Regeln untersucht werden, wobei etwaige Haftungsprivilegierungen nach dem TDG/MDStV vorerst außer Betracht bleiben.[169] Sollte dem Access Provider nach den allgemeinen Regeln eine unmittelbare oder zumindest eine mittelbare Rechtsverletzung zur Last gelegt werden können, wird sodann die Frage zu beantworten sein, ob diese Rechtsverletzung ausreicht, um eine Passivlegitimation i.S.d. § 101a UrhG zu begründen.

1. Unmittelbare Störerhaftung durch Access Providing

Fraglich ist zunächst, ob der Access Provider bereits eine eigenständige Rechtsverletzung i.S.d. §§ 16, 19a UrhG begeht, wenn seine Dienstleistungen für Rechtsverletzungen genutzt werden.

---

[167] Dreier/Schulze, § 101a UrhG, Rn. 6; Fezer, § 14, Rn. 41.

[168] Davon zu trennen ist die Frage, ob § 101a UrhG auch einen verletzungsunabhängigen Anspruch gegen Access Provider auf Auskunft gewährt; dazu unten, 3.Teil A. B.

[169] Zur Frage, ob Auskunftsansprüche gegen Access Provider durch eine gesetzliche Haftungsprivilegierung ausgeschlossen werden, siehe unten, 4. Teil E.

a) Unmittelbare Verletzung des § 16 UrhG

In Betracht kommt zunächst eine Verletzung des Vervielfältigungsrechts aus § 16 UrhG durch Zwischenspeicherungen des übermittelten Dateninhalts im Rahmen des Routings sowie auf den Proxy-Cache-Servern. Sofern beim Routing technisch bedingte Zwischenspeicherungen stattfinden, sind die einzelnen Datenpakete in der Regel jedoch so klein, dass ihnen per se kein urheberrechtlicher Schutz zukommt.[170] Werden urheberrechtlich geschützte Werke hingegen zur beschleunigten Übermittlung auf Proxy-Cache-Servern zwischengespeichert, findet stets ein Eingriff in das Vervielfältigungsrecht des § 16 UrhG statt. Dieser ist allerdings durch die Schrankenregelung des § 44a Nr. 1 UrhG[171] gedeckt, da es sich in diesen Fällen um technisch ephemere Vervielfältigungen handelt, die ausschließlich der Übertragung in einem Netz zwischen Dritten durch einen Vermittler dienen und keine eigenständige wirtschaftliche Bedeutung haben.[172] Eine unmittelbare Rechtsverletzung des § 16 UrhG durch Access Providing scheidet somit aus.

b) Unmittelbare Verletzung des § 19a UrhG

Der Access Provider könnte jedoch dadurch, dass er bei Urheberrechtsverletzungen seiner Nutzer die Aufgabe des Datentransportes übernimmt, eine Verletzungshandlung i.S.d. § 19a UrhG zur Last gelegt werden. Denn dieses Verwertungsrecht umfasst nicht nur das Bereitstellen von Werken, sondern auch den anschließenden Übertragungsakt. Daher spricht man auch von einem zweiaktigen Tatbestand.[173] Gegen einen eigenständigen Eingriff des Access Providers in das Recht des § 19a UrhG spricht allerdings eine Parallele zum nahezu wortgleichen Senderecht des § 20 UrhG. Denn auch im Rahmen des § 20 UrhG wird der technische Dienstleister, der nur die Übertragungstechnik bereitstellt und die Sendung technisch durchführt, nicht zugleich zum Sendeunternehmer, der die Sendung öffentlich zugänglich macht. Sendunternehmer ist nämlich nur derjenige, der die Sendung kontrolliert und verantwortet.[174] Gleiches muss für den Access Provider gelten. Auch dieser stellt lediglich in passiver Weise die techni-

---

[170] Schricker/Loewenheim, § 16 UrhG, Rn. 22; HK-UrhG, § 16, Rn. 7; ausführlich zur urheberrechtlichen Einordnung der Datenübertragung,Völker, in: Entshaler/Bosch/Völker, S. 183 ff.

[171] § 44a UrhG setzt Art. 5 Abs. 1 Richtlinie 2001/29/EG (InfoSoc-RL) um.

[172] Sieber/Höfinger, MMR 2004, 575, 579; Wandtke/Bullinger/v.Welser, § 44a UrhG, Rn. 9.

[173] Dreier/Schulze, § 19a UrhG, Rn. 6; HK-UrhG, § 19a, Rn. 2.

[174] BGH, Urt. v. 8.7.1993 – I ZR 124/91, BGHZ 123, 149, 154 – Verteileranlagen; Dustmann, Provider, S. 70; Möhring/Nicolini/Hillig, § 87, Rn. 11 m.w.N.

schen Voraussetzungen für Rechtsverletzungen zur Verfügung und hat zudem keinen Einfluss auf die von ihm übermittelten Daten. Somit macht auch dieser kein Werk öffentlich zugänglich i.S.d. § 19a UrhG.[175] Bekräftigt wird eine dahingehende Auslegung des § 19a UrhG zudem durch Erwägungsgrund 27 der Richtlinie 2001/29/EG (InfoSoc-RL).[176] Darin wird klargestellt, dass durch die bloße Bereitstellung der Infrastruktur nicht in das Wiedergaberecht eingegriffen wird, dessen Unterfall auch das Recht der öffentlichen Zugänglichmachung darstellt.[177] Zudem lässt sich dieses Ergebnis auch im Wege eines *argumentum a maiore ad minus* aus dem Recht der Hyperlinks ableiten. Stellt nämlich bereits das bewusste Setzen eines Hyperlinks keine urheberrechtliche Nutzungshandlung dar,[178] so muss dies erst recht für die passive und unbewusste Datenübermittlung durch den Access Provider gelten, da dieser eine viel größere Distanz zu diesen Werken aufweist als der Linksetzende. Dem Access Provider kann somit auch keine unmittelbare Rechtsverletzung des § 19a UrhG zur Last gelegt werden.

c) Veranlasserhaftung

Der Access Provider könnte jedoch nach den Grundsätzen der Veranstalter- bzw. Veranlasserhaftung als unmittelbarer Verletzer anzusehen sein. Danach ist auch derjenige unmittelbarer Verletzer, der eine Rechtsverletzung zwar nicht selbst vornimmt, jedoch wertungsmäßig ein primäres Interesse an dieser Rechtsverletzung hat, weil er diese veranlasst hat und den wirtschaftlichen Nutzen daraus zieht.[179] Auf diesen Grundsätzen beruhte auch die Musikbox-Aufsteller-Entscheidung des Kammergerichts. Darin wurden nicht nur die Nutzer einer Musikbox, sondern auch deren Aufsteller als unmittelbarer Urheberrechtsverletzer angesehen, da dieser maßgeblichen Einfluss auf die Programmgestaltung sowie die rechtliche und tatsächliche Verfügungsgewalt über das Gerät habe.[180] Der Access Provider kann jedoch nicht als Veranlasser in diesem Sinne angesehen werden. Die-

---

[175] Sieber/Höfinger, MMR 2004, 575, 580; Kitz, GRUR 2003, 1014, 1015.

[176] Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22.5.2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, abrufbar unter: http://europa.eu.int/eur-lex/pri/de/oj/dat/2001/l_167/l_16720010622de00100019.pdf

[177] So auch Sieber/Höfinger, MMR 2004, 575, 579.

[178] BGH, Urt. v. 17.7.2004 – I ZR 259/00, MMR 2003, 719, 722 = GRUR 2003, 985 – Paperboy; Hoeren, Access Provider, Rn. 585.

[179] BGH, Urt. v. 19.6.1956 – I ZR 104/54, GRUR 1956, 515, 516 – Tanzkurse; BGH, Urt. v. 16.6.1971 – I ZR 120/69, GRUR 1972, 141, 142 – Konzertveranstalter.

[180] KG, Urt. v. 28.3.1958 – 5 U 2090/57, GRUR 1959, 150, 151 – Musikbox-Aufsteller.

ser hat weder Einfluss auf das Onlineverhalten seiner Nutzer noch kann und darf er diese Inhalte kontrollieren. Der Access Provider kann daher nicht mit Aufsteller einer Musikbox verglichen werden, sondern allenfalls mit dem Lieferanten des in der Musikbox befindlichen Plattenspielers. Festzuhalten bleibt somit, dass auch durch die Bereitstellung der infrastrukturellen Voraussetzungen für Urheberrechtsverletzungen im Internet keine unmittelbare Verletzungshandlung in Gestalt der Veranstalter- bzw. Veranlasserhaftung begründet wird.

d) Zwischenergebnis

Der Access Provider kann unter keinem rechtlichen Gesichtspunkt als unmittelbarer Störer der §§ 16, 19 UrhG qualifiziert werden.

2. Mittelbare Störerhaftung

Da dem Access Provider im Rahmen seiner Tätigkeit keine eigenständige Rechtsverletzung zur Last gelegt werden kann, stellt sich die Frage, ob dieser nicht zumindest akzessorisch für die Rechtsverletzungen seiner Nutzer haftet. In dieser Hinsicht lässt sich zunächst an eine deliktische Teilnehmerhaftung gem. § 830 Abs. 2 BGB denken. Diese wird jedoch regelmäßig daran scheitern, dass § 830 Abs. 2 BGB eine vorsätzliche Teilnahmehandlung voraussetzt.[181] Denn der Access Provider leistet weder vorsätzlich Beihilfe zu den Rechtsverletzungen seiner Nutzer noch stiftet er vorsätzlich zu einer solchen an. In Betracht kommt daher allenfalls eine verschuldensunabhängige mittelbare Störerhaftung.

Mittelbarer Störer ist nach allgemeiner Ansicht jeder, der willentlich und adäquat-kausal zu einer Urheberrechtsverletzung beigetragen hat, wobei als Mitwirkung auch die Unterstützung oder Ausnutzung der Handlung eines eigenverantwortlich handelnden Dritten genügt, sofern der in Anspruch Genommene die rechtliche Möglichkeit zur Verhinderung dieser Handlung hatte.[182] Damit die Störerhaftung jedoch nicht über Gebühr auf Dritte erstreckt wird, die nicht selbst die rechtswidrige Beeinträchtigung vorgenommen haben, setzt die Haftung des mittelbaren Störers nach der neueren Rechtsprechung des BGH die Verletzung von Prüfpflichten voraus.[183] Da-

---

[181] Palandt/Sprau, § 830, Rn. 4.

[182] St. Rspr., vgl. BGH, Urt. 6.7.1954 – I ZR 38/54, GRUR 1955, 97, 99 f. – Constanze II; BGH, Urt. v. 3.2.1994 – I ZR 321/91,GRUR 1994, 441, 443 – Kosmetikstudio.

[183] Vgl. BGH, Urt. v. 10.10.1996 – I ZR 129/94, GRUR 1997, 313, 315 f. = WRP 1997, 325 – Architektenwettbewerb; BGH, Urt. v. 15.10.1998 – I ZR 120/96, GRUR 1999, 418, 419 f.

nach haftet der Inanspruchgenommene auch dann nicht als mittelbarer Störer, wenn er geltend machen kann, dass ihm eine solche Prüfung nach den Umständen überhaupt nicht oder nur eingeschränkt zumutbar war.[184] Bevor jedoch auf die Frage eingegangen werden kann, ob den Access Provider eine zumutbare Prüfpflicht hinsichtlich des Onlineverhaltens seiner Nutzer trifft, müssen zunächst die allgemeinen Voraussetzungen der Störerhaftung auch in der Person des Access Providers erfüllt sein.

a) Willentlicher und adäquat-kausaler Beitrag

Die erste Voraussetzung für das Eingreifen der Störerhaftung des Access Providers ist, dass dieser einen willentlichen und adäquat-kausalen Beitrag zu den Urheberrechtsverletzungen seiner Nutzer leistet. Nach Stadler[185] soll ein solcher Beitrag jedoch gerade nicht in der bloßen Bereitstellung des Internetzugangs sowie dem Transport von Daten gesehen werden können. Zudem sei diese Leistung des Access Providers nicht willentlich, da es gerade nicht auf die willentliche Bereitstellung der Infrastruktur ankomme, sondern auf die willentliche Mitwirkung an der Urheberrechtsverletzung selbst.[186] Dies setze jedoch zwingend die Kenntnis der übermittelten Inhalte voraus, die der Access Provider nicht habe. [187]

Stadlers Auffassung steht im Widerspruch zur allgemeinen negativen Formel der Adäquanz. Nach dieser ist von einem adäquat-kausalen Verhalten bereits dann auszugehen, wenn aus der Sicht des optimalen Beobachters die Möglichkeit des Schadenseintritts nicht so weit entfernt war, dass sie nach der Lebenserfahrung vernünftigerweise nicht in Betracht gezogen werden konnte.[188] Dementsprechend hat der BGH bereits in früheren Entscheidungen ausgeführt, dass als Störer auch derjenige in Anspruch genommen werden kann, *„der im Rahmen seiner gewerblichen Tätigkeit dem privaten Vervielfältiger das Rüstzeug und die Möglichkeit zur mühelosen Vervielfältigung verschafft.“*[189] Der Verursachungszusammenhang entfalle auch nicht dadurch, dass die Geräte auch in einer rechtmäßigen Weise ge-

---

= WRP 1999, 211 – Möbelklassiker; BGH, Urt. v. 17.5.2001 – I ZR 251/99, GRUR 2001, 1038, 1039 = WRP 2001, 1305 – Ambiente.

[184] BGH, Urt. v. 15.10.1998 – I ZR 120/96, GRUR 1999, 418, 419 = WRP 1999, 211 – Möbelklassiker.

[185] Stadler, Haftung, S. 203 f.

[186] So Stadler, Haftung, S. 204 unter Berufung auf BGH, Urt. v. 17.5.2001 – I ZR 251/99 – Ambiente.

[187] Stadler, Haftung, S. 204.

[188] Vgl. Palandt/Heinrichs, Vorb. v. § 249, Rn. 59.

[189] BGH, Urt. v. 29.5.1964 – Ib ZR 4/63, GRUR 1965, 104, 106 – Personalausweise.

nutzt werden können. Ausreichend sei vielmehr, dass bei objektiver Betrachtung das rechtsverletzende Verhalten dieses Dritten nicht außerhalb der Wahrscheinlichkeit liege.[190]

Diese Voraussetzungen sind auch in den vorliegenden Konstellationen erfüllt. Denn mit der Bereitstellung der technischen Infrastruktur, mittels derer problemlos Urheberrechtsverletzungen im Internet getätigt werden können, liegt es auch keinesfalls außerhalb der Wahrscheinlichkeit, dass diese in rechtsmissbräuchlicher Weise benutzt wird. Somit leistet auch der Access Provider einen adäquat-kausalen Beitrag zu den Urheberrechtsverletzungen seiner Nutzer.[191] Zudem ist der Annahme zu widersprechen, dass ein willentlicher Beitrag zu einer Urheberrechtsverletzung stets eine willentliche Mitwirkung an einer konkreten Urheberrechtsverletzung voraussetzt. Dies liefe im Ergebnis auf ein dem Störerhaftungsrecht fremdes Vorsatzerfordernis hinaus. Ein solches lässt sich jedoch – entgegen Stadler – auch nicht aus der Ambiente-Entscheidung des BGH ableiten, da auch in dieser explizit auf den verschuldensunabhängigen Charakter der Störerhaftung abgestellt wird.[192] Zwar gibt es durchaus Strömungen in der Rechtsprechung und der Literatur, die eine Aufgabe der Störerhaftung zugunsten der deliktsrechtlichen Kategorien der Täterschaft und Teilnahme gem. § 830 Abs. 2 BGB erwägen.[193] Allerdings hat der BGH gerade im Hinblick auf diese Stimmen ausdrücklich klargestellt, dass zumindest im Immaterialgüterrecht auch weiterhin am Institut der verschuldensunabhängigen Störerhaftung festgehalten werden soll.[194] Das von der Rechtsprechung postulierte Willentlichkeitserfordernis ist daher vielmehr in dem Sinne zu verstehen, dass es lediglich den Handlungsbegriff dahingehend präzisiert, dass nicht willentlich gesteuertes Verhalten aus dem Haftungstatbestand der Störerhaftung ausscheidet.[195] Da der Access Provider jedoch willentlich sowohl den Internetzugang bereitstellt als auch den Datentransport vornimmt, ist auch dieses Merkmal in seiner Person erfüllt. Mithin leistet der

---

[190] BGH, Urt. v. 9.6.1983 – I ZR 70/81, GRUR 1984, 54, 55 – Kopierläden.

[191] So auch LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, CR 2005, 136, 139 = MMR 2005, 55; Hoeren/Sieber/Spindler, Teil 29, Rn. 355.

[192] BGH, Urt. v. 17.5.2001 – I ZR 251/99, GRUR 2001, 1038, 1039 = WRP 2001, 1305 – Ambiente.

[193] Vgl. BGH, Urt. v. 24.6.2003 – KZR 32/02, BGHZ 155, 189, 194 f. – Buchpreisbindung; BGH, Urt. v. 15.5.2003 – I ZR 292/00, GRUR 2003, 969, 970 m.w.N. = WRP 2003, 1350 – Ausschreibung von Vermessungsleistungen; Jergolla, WRP 2004, 655, 659.

[194] So ausdrücklich BGH, Urt. v. 11.3.2004 – I ZR 304/01, MMR 2004, 668,671 = GRUR 2004, 860 – Internet-Versteigerung.

[195] Volkmann, Störer im Internet, S. 62.

Access Provider sowohl einen adäquat-kausalen als auch einen willentlichen Beitrag zu den Urheberrechtsverletzungen seiner Nutzer.[196]

b) Verhinderungsmöglichkeit

Weiterhin setzt die Begründung einer mittelbaren Störerhaftung voraus, dass der Inanspruchgenommene auch die rechtliche Möglichkeit zur Verhinderung dieser Rechtsverletzungen hat. In dieser Hinsicht lässt sich eine Parallele zur Unterlassungshaftung des Telekommunikationsbetreibers bei der missbräuchlichen Verwendung von überlassenen Mehrwertdienstenummern ziehen, wie sie sich vor der Einführung des § 13a TKV darstellte.[197] Danach wurde die Störerhaftung der Telekommunikationsanbieter damit begründet, dass sie den Missbrauch der Rufnummern nach Kenntniserlangung durch Kündigung unterbinden könnten.[198] Eine solche Kündigungsmöglichkeit steht in der Regel auch dem Access Provider offen. Zumeist lässt sich dieser in den Allgemeinen Geschäftsbedingungen bei rechtsmissbräuchlichen Verhalten ein Recht zur Sperrung des Nutzers oder ein vertragliches Kündigungsrecht einräumen.[199] Darüber hinaus dürfte dem Provider bei Urheberrechtsverletzungen seiner Nutzer auch ein gesetzliches außerordentliches Kündigungsrecht aus § 314 BGB zustehen. Denn rechtswidrige Handlungen der Nutzer stellen stets eine schwerwiegende Vertragsverletzung dar, die geeignet ist, eine Fortsetzung des Vertrages für den Provider als unzumutbar erscheinen zu lassen.[200] Der Provider hat somit zumindest nach Kenntnisnahme von Rechtsverletzungen seiner Kunden auch die rechtliche Möglichkeit, (weitere) Schutzrechtsverletzungen zu verhindern.[201] Somit sind die allgemeinen Voraussetzungen der Störerhaftung in der Person des Access Providers erfüllt.

---

[196] So auch LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, CR 2005, 136, 139 = MMR 2005, 55.

[197] Ausführlich zur Störerhaftung nach § 13a TKV und deren Übertragbarkeit auf Access Provider, siehe unten, 2.Teil IV. 2. c) bb) (b).

[198] Vgl. Hoeren, Access Provider, Rn. 634 m.w.N.

[199] Spindler, in: Spindler, Internet Provider, Teil IV, Rn. 236.

[200] LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, CR 2005, 136, 139 = MMR 2005, 55; Spindler, in: Spindler, Internet-Provider, Teil IV, Rn. 317.

[201] Diese Verhinderungsmöglichkeit entfällt jedoch, wenn es dem Access Provider aus rechtlichen Gründen verwehrt ist, die Identität des Verletzer zu ermitteln; dazu unten, 5. Teil A. IV, B.

c) Verletzung von Prüfpflichten

Da sich in der neueren Rechtsprechung zur wettbewerbs- und urheberrechtlichen Störerhaftung – wie soeben ausgeführt – die Erkenntnis durchgesetzt hat, dass die Störerhaftung nicht über Gebühr auf Dritte erstreckt werden darf, die nicht selbst die rechtswidrige Beeinträchtigung vorgenommen haben, muss der Access Provider weiterhin eine ihm obliegende Prüfpflicht verletzt haben, um als mittelbarer Störer qualifiziert werden zu können.

aa) Dogmatische Einordnung der Prüfpflichten

Die vom BGH im Wettbewerbs- und Urheberrecht vorgenommene Einschränkung der Störerhaftung ist in der Literatur überwiegend begrüßt worden.[202] Bemängelt wurde allerdings, dass der BGH mit dem Begriff der Prüfpflichten einerseits einen wenig greifbaren und lediglich auf Billigkeits- und Zumutbarkeitserwägungen basierenden Terminus eingeführt hat, es andererseits jedoch offen gelassen hat, woraus sich diese Prüfpflichten ergeben sollen, welchen Inhalt diese haben und wie diese dogmatisch einzuordnen sind.[203] Bedingt durch die Unschärfe dieser Begrifflichkeit wurde im Schrifttum der Versuch unternommen, die Prüfpflichten auf eine dogmatisch tragfähige Grundlage zu stellen.

Überzeugen können in dieser Hinsicht die Ausführungen einiger Literaten, nach denen die vom BGH postulierten Prüfpflichten in das Gewand der deliktsrechtlichen Verkehrssicherungspflichten zu kleiden sind und die Haftungsbeschränkung des mittelbaren Störers damit im Rahmen der Zurechnung vorzunehmen ist.[204] Für diese dogmatische Einordnung spricht, dass der Grundsatz der Haftungsbeschränkung auf der Zurechnungsebene auch rechtsgebietsübergreifende Geltung für sich beanspruchen kann, wie die Lehre von der objektiven Zurechnung im Strafrecht oder das Erfordernis des Unmittelbarkeitszusammenhangs im öffentlichen Gefahrenabwehrrecht zeigen.[205] Zudem zeigen gerade die Erfahrungen aus dem Deliktsrecht, dass die Lehre von den Verkehrssicherungspflichten eine flexible

---

[202] Haedicke, GRUR 1999, 397, 399 m.w.N.; Volkmann, Störer im Internet, S. 129.
[203] Vgl. Haedicke, GRUR 1999, 397, 399.
[204] So Dustmann, Provider, S. 58; Freytag, S. 73 ff.; Spindler, in Spindler/Schmitz/Geis, § 8 TDG, Rn. 23 m.w.N.; Volkmann, Störer im Internet, S. 138; für eine Einordnung im Rahmen der Rechtswidrigkeit, Haedicke, GRUR 1999, 397, 401 f.
[205] Volkmann, Störer im Internet, S. 138.

Handhabe von mittelbaren Rechtsverletzungen ermöglicht und durchweg zu sachgemäßen Ergebnissen führt.[206]

Nun könnte man auch gegen diese Haftungskonstruktion den dogmatischen Einwand erheben, dass mit der Einführung von Verkehrssicherungspflichten letztlich doch ein fahrlässigkeitsähnlicher Sorgfaltsverstoß – und somit ein Verschuldenselement – in das verschuldensunabhängige Störerhaftungsrecht eingeführt wird.[207] Dies wird jedoch hinzunehmen sein, zumal sich die Lehre von den Verkehrssicherungspflichten nicht auf das gesamte Störungshaftungsrecht erstrecken soll, sondern lediglich zur Beschränkung der zu Recht als zu weit empfundenen mittelbaren Störerhaftung dient. Festzuhalten bleibt insofern, dass sich das vom BGH postulierte Prüfpflichtenerfordernis in dogmatischer Hinsicht an die deliktsrechtlichen Verkehrssicherungspflichten anlehnt.

bb) Verkehrssicherungspflichten des Access Providers

Stellt man im Rahmen der Prüfpflichten somit auf Verkehrssicherungspflichten ab, so gilt auch für die mittelbare Störerhaftung des Access Providers der Grundsatz, dass dieser, weil er unstreitig eine Gefahrenquelle für Urheberrechte Dritter schafft, geeignete und zumutbare Maßnahmen treffen muss, um die Verwirklichung dieser Gefahr möglichst zu verhindern.[208] Fraglich ist insofern, welche Maßnahmen den Access Providern zur Verhinderung von Urheberrechten durch deren Nutzer abverlangt werden können.

(1) Hinweispflicht zur Beachtung fremder Urheberrechte

So könnte man zunächst daran denken, die Verkehrssicherungspflichten des Access Providers bereits dann als erfüllt anzusehen, wenn dieser seine Nutzer zu Beachtung fremder Urheberrechte ermahnt. Stützen ließe sich diese Annahme insbesondere auf die Wertungen der sog. Kopierläden-Entscheidung[209] des BGH aus dem Jahre 1983. Darin wurde ausgeführt, dass auch der Betreiber eines Kopierladens nicht als mittelbarer Störer für die Urheberrechtsverletzungen seiner Kunden haftet, wenn dieser seine Kunden deutlich darauf hinweist, dass diese fremde Urheberrechte zu be-

---

[206] Vgl. Palandt/Sprau, § 823, Rn. 51.
[207] So Stadler, Haftung, S. 54.
[208] Vgl.: BGH, Urt. v. 28.4.1952 – III ZR 118/51, BGHZ 5, 378, 380f.; BGH, Urt. v. 23.10.1975 – III ZR 108/73, BGHZ 65, 221, 224.
[209] BGH, Urt. v. 9.6.1983 – I ZR 70/81, GRUR 1984, 54 – Kopierläden.

achten haben.[210] Da sich solche Hinweise in nahezu allen Allgemeinen Geschäftsbedingungen von Access Providern befinden,[211] lässt sich argumentieren, dass auch der Access Provider mit einem solchen Hinweis seinen Verkehrssicherungspflichten bereits nachgekommen ist und somit nicht mehr als mittelbarer Störer in Anspruch genommen werden kann.[212] Allerdings ist fraglich, ob sich eine solch weitgehende Haftungsprivilegierung auch mit der neueren Rechtsprechung des BGH zur Haftung von Internet-Providern in Einklang bringen lässt.

(2) Auferlegung von Überwachungspflichten

Grund für die Annahme, dass dem Access Provider durchaus strengere Prüfpflichten aufgebürdet werden können, bietet vor allem die Internet-Versteigerung-Entscheidung des BGH aus dem Jahre 2004.[213] Darin führte der erste Zivilsenat aus, dass ein Onlineauktionshaus, wenn es auf Markenrechtsverletzungen auf deren Portal hingewiesen werde, durchaus auch Vorsorge dafür treffen muss, dass es nicht zu weiteren, gleich gelagerten Markenrechtsverletzungen kommt.[214] Erwogen wurde dabei insbesondere der Einsatz einer Filtersoftware zu Verhinderung von Rechtsverletzungen.[215]

Insofern könnte man auf den ersten Blick erwägen, auch dem Access Provider dahingehende Kontrollpflichten aufzuerlegen. So erscheint nämlich auch für den Access Provider eine Verpflichtung zum Einsatz einer Filtersoftware, mittels der Urheberrechtsverletzungen unterbunden werden können, nicht von vornherein ausgeschlossen. In dieser Hinsicht bietet sich vor allem der Einsatz des – im Auftrag des Bundesverbandes der Phonographischen Wirtschaft (IFPI) entwickelten – Right Protection System (RPS) an. Dieses System setzt den Betrieb eines Proxy-Servers voraus, auf dem eine Filtersoftware installiert wird, die in der Lage ist, jede Dateianforderung

---

[210] BGH, Urt. v. 9.6.1983 – I ZR 70/81, GRUR 1984, 54, 55 – Kopierläden.

[211] Vgl. Allgemeine Geschäftsbedingen von T-Online, Punkt 4.2.2., abrufbar unter: ftp://software.t-online.de/pub/service/pdf/agbdiens.pdf.

[212] So auch ECO-Verband, Backgrounder v. 21.7.2005 zu den Sperraufforderungen der GEMA an Zugangsprovider, n.v., S. 6, mit Verweis auf BGH, Urt. v. 9.6.1983 – I ZR 70/81 – Kopierläden.

[213] BGH, Urt. v. 11.3.2004 – I ZR 304/01, MMR 2004, 668 m. Anm. Hoeren = BGH GRUR 2004, 860 – Internet-Versteigerung.

[214] BGH, Urt. v. 11.3.2004 – I ZR 304/01, MMR 2004, 668, 671 f.= BGH GRUR 2004, 860 – Internet-Versteigerung.

[215] Vgl. Hoeren, Anm. zu BGH, Urt. v. 11.3.2004 – I ZR 304/01 – Internet-Versteigerung, MMR 2004, 672, 672 f.

der Nutzer auf ihre urheberrechtliche Zulässigkeit zu überprüfen und ggf. zu unterbinden.[216]

Eine solche präventive Filterpflicht wird dem Access Provider, zumindest als Verkehrssicherungspflicht, jedoch nicht zuzumuten sein. Denn zunächst würde der Provider durch den Betrieb solcher Proxy-Server mit erheblichen Kosten belastet. Diese Kosten erscheinen bereits deshalb unverhältnismäßig, weil diese nicht etwa für ein hochwertiges Schutzgut der Allgemeinheit aufzubringen wären, sondern allein zur Wahrung privatwirtschaftlicher Interessen Dritter.[217] Darüber hinaus würde eine solche Filterung zu einer erheblichen Verlangsamung des Datenstromes führen, der sich negativ auf die gesamte Netzkommunikation auswirken würde.[218] Eine präventive Verpflichtung zur Filterung von Inhalten ist dem Access Provider somit bereits nach den allgemeinen Haftungsregeln nicht zuzumuten.[219] Nicht zuletzt stehen einer solchen Filterpflicht auch rechtliche Bedenken entgegen. So werden Prüfpflichten des Access Providers zusätzlich durch das Fernmeldegeheimnis aus § 88 TKG beschränkt, dass dem Access Provider bereits die Kenntnisnahme von übermittelten Inhalten verbietet.[220] Zudem stünde einer präventiven Prüfpflicht auch das in § 8 Abs. 2 S. 1 TDG normierte Verbot allgemeiner Überwachungspflichten entgegen, nach dem den Access Providern weder eine allgemeine Überwachungs- noch eine Nachforschungspflicht hinsichtlich der Rechtswidrigkeit der von ihnen übermittelten Inhalte auferlegt werden darf.[221] Vor diesem Hintergrund ist letztlich auch die Internet-Versteigerung-Entscheidung des BGH selbst nicht frei von Widersprüchen. Wenn man Internetauktionshäuser – mit dem BGH – nämlich als Host-Provider qualifiziert, für die auch die Haftungsprivilegierungen des TDG eingreifen, so lässt sich auch die dort postulierte Prüfpflicht der Provider nur schwerlich mit dem aus § 8 Abs. 2 S. 1 TDG resultierenden Verbot von allgemeinen Überwachungspflichten vereinbaren.[222] Festzuhalten bleibt somit zunächst, dass Access Provider im Rahmen von Verkehrssicherungspflichten nicht zur proaktiven Überwachung der von ihnen durchgeleiteten Daten angehalten werden können.

---

[216] Dazu Dustmann, Provider, S. 181 ff.
[217] Volkmann, Störer im Internet, S. 160.
[218] Volkmann, Störer im Internet, S. 160.
[219] So auch LG Köln, Urt. v. 28.7.2004 – 28 O 301/04, ZUM 2005, 236, 239.
[220] Gerke, CR 2006, 210, 215; Spindler, in: Spindler/Geis/Schmitz, in: Spindler/Schmitz/Geis, § 9 TDG, Rn. 32 ff.; ausführlich zum Eingriff in das Fernmeldegeheimnis durch Auskunftsverlangen, siehe unten, 5.Teil B.
[221] Vgl. Spindler, in: Spindler/Schmitz/Geis, § 8 TDG, Rn. 11.
[222] Näher dazu, Rücker, CR 2005, 347 ff.

(3) Pflichten nach Kenntnisnahme von Rechtsverletzungen

Andererseits könnten sich jedoch zumindest dann Kontrollpflichten für den Access Provider ergeben, wenn dieser zuvor auf konkrete Urheberrechtsverletzungen seiner Nutzer aufmerksam gemacht wurde. Zumindest würden solche nachträglichen Handlungspflichten nicht gegen das aus § 8 Abs. 2 S. 1 TDG resultierende Verbot von proaktiven Überwachungspflichten verstoßen.[223] Nach einer weit verbreiteten Auffassung ist der Access Provider daher bereits dann als mittelbarer Störer anzusehen, wenn dieser von Dritten über konkrete Urheberrechtsverletzungen seiner Nutzer in Kenntnis gesetzt wurde.[224] Diese Auffassung geht allerdings zu weit. Wenn dem Access Provider nämlich eine präventive Überwachung des durchgeleiteten Dateninhalts verwehrt ist, so kann dieser mit der erstmaligen Inkenntnissetzung nicht zugleich auch eine ihm obliegende Prüfpflicht verletzt haben. Allenfalls wird eine solche durch die Inkenntnissetzung begründet. Insofern stellt sich vielmehr die Frage, ob der Access Provider nach einer solchen Inkenntnissetzung Maßnahmen treffen muss, um einer Inanspruchnahme als mittelbarer Störer zu entgehen.

(a) Übertragung der Grundsätze der Ambiente-Entscheidung

Hinsichtlich des Entstehens einer solchen nachträglichen Prüfpflicht liegt es zunächst nahe, die Wertungen der Ambiente-Entscheidung[225] des BGH auch auf Access Provider zu übertragen. In dieser Entscheidung hat der BGH das Erfordernis einer Verletzung zumutbarer Prüfpflichten erstmalig auf den Onlinebereich übertragen. Der Entscheidung lag die Frage zugrunde, unter welchen Voraussetzungen die deutsche Vergabestelle für Domainnamen (DENIC) als mittelbare Störerin für markenrechtsverletzende Domains in Anspruch genommen werden kann. Im Hinblick auf den Umfang bestehender Prüfpflichten betonte der BGH, dass auch die Funktion und Aufgabenstellung des als Störer in Anspruch Genommenen berücksichtigt werden müsse. Da es sich bei der DENIC um eine private Organisation handele, die keine eigenen erwerbswirtschaftlichen Zwecke verfolgt und im Sinne des Allgemeinwohls handelt, sei dieser im Rahmen des automatisierten Anmeldeverfahrens eine Überprüfung der Registrierungen auf deren Rechtswidrigkeit überhaupt nicht zuzumuten. Selbst wenn die DENIC auf eine Rechtsverletzung hingewiesen werde, bestehe nur eine

[223] Spindler/Volkmann, WRP 2003, 1, 3.
[224] So OLG Frankfurt a.M., Urt. v. 25.1.2005 – 11 U 51/05, MMR 2005, 241, 243 = CR 2005, 285; Spindler, in: Spindler/Schmitz/Geis, § 9 TDG, Rn. 34 m.w.N.
[225] BGH, Urt. v. 17.5.2001 – I ZR 251/99, GRUR 2001, 1038 = WRP 2001, 1305 – Ambiente.

eingeschränkte Prüfpflicht. Eine Registrierung sei erst dann zu löschen, wenn deren Rechtswidrigkeit offenkundig ist und dies auch von einem juristischen Laien ohne weiteres festgestellt werden kann.[226]

Teilweise wird vertreten, dass sich die Wertungen der Ambiente-Entscheidung auch auf die anderen Akteure des Internets übertragen lassen, mithin diese Entscheidung Leitcharakter für die gesamte mittelbare Störerhaftung im Bereich geistiger Schutzrechte für die Fälle mit Internetbezug habe.[227] Vor diesem Hintergrund könnte man in Erwägung ziehen, dass spezifische Verkehrssicherungspflichten des Access Providers, wie z.B. eine Sperrung des Nutzers, ebenfalls erst mit der Inkenntnissetzung von offenkundigen Rechtsverletzungen begründet werden können.

Gegen eine Übertragung dieser Grundsätze und damit für eine strengere Haftung des Access Providers könnte allerdings sprechen, dass die Rechtsprechung in den Folgeentscheidungen darauf hingewiesen hat, dass sich die Haftungsprivilegierung der DENIC nicht auf kommerzielle Provider übertragen lasse, da diese im Gegensatz zur DENIC nicht im Allgemeininteresse tätig werden, sondern eigene erwerbswirtschaftliche Zwecke verfolgen.[228] Diese von der Rechtsprechung postulierte Haftungsverschärfung für kommerzielle Anbieter dürfte jedoch in erster Linie auf die – mit der DENIC vergleichbaren – Host-Provider bezogen sein und sich nicht auf Access Provider übertragen lassen. Auch diese verfolgen zwar regelmäßig ökonomische Interessen, jedoch ist insofern haftungsprivilegierend zu berücksichtigen, dass Access Provider, ebenso wie die DENIC, eine unerlässliche und sozialadäquate Aufgabe im Rahmen der Netzkommunikation wahrnehmen.[229]

Darüber hinaus spricht einiges dafür, dass der Access Provider in Bezug auf Prüfpflichten einer noch weitergehenden Privilegierung als die DENIC bedarf. Denn im Gegensatz zur DENIC haben Access Provider keine Herrschaftsgewalt über die durchgeleiteten Inhalte, mithin können sie diese nicht auf ihre Rechtswidrigkeit überprüfen. Sie wären somit gezwungen, sich vollends auf die Angaben der Rechteinhaber zu verlassen, ohne die behaupteten Rechtsverletzungen eigenhändig verifizieren zu können. Eine

---

[226] BGH, a.a.O., 1039 f.

[227] Freytag, Anm. zu BGH, Urt. v. 17.5.2001 – I ZR 251/99 – Ambiente, CR 2001, 853, 854; Stadler, Haftung, S. 55.

[228] Vgl. BGH, Urt. v. 11.3.2004 – I ZR 304/01, MMR 2004, 668, 671 = BGH GRUR 2004, 860 – Internet-Versteigerung.

[229] Volkmann, Störer im Internet, S. 160.

dahingehende Prüfpflicht wäre aber selbst dann als unzumutbar anzusehen, wenn die Rechteinhaber den Access Providern so aussagekräftige Beweise für die behaupteten Rechtsverletzungen vorlegen würden, dass eine eingehende Rechtsprüfung entbehrlich erscheint. Denn während die Prüfpflicht der DENIC und anderer Host-Provider auf deren Content und damit auf Einzelfälle begrenzt sein dürfte, sähen sich Access Provider angesichts der Tatsache, dass Rechteinhaber mitunter tausende verdächtige IP-Adressen generieren, mit einer erheblichen Anzahl von Prüfungsersuchen konfrontiert, denen nachzukommen wäre, um einer mittelbaren Störerhaftung zu entgehen. Die Prüfung dieser Sachverhalte würde jedoch sowohl die wirtschaftlichen als auch personellen Kapazitäten des Providers bei weitem überschreiten.[230] Da sich die Wertungen der DENIC-Rechtsprechung somit nicht auf Access Provider übertragen lassen, greift die Störerhaftung des Access Providers nicht bereits dann ein, wenn dieser bei Hinweisen auf (einzelne) offenkundige Rechtsverletzung untätig bleibt.

(b) Übertragung der Grundsätze des § 13a TKV

Da Access Provider in haftungsrechtlicher Sicht noch umfassender zu privilegieren sind als andere Internet-Akteure, ist es naheliegend, die gesetzgeberischen Wertungen des § 13a TKV zu rekurrieren. Durch diese Norm sind die Verkehrssicherungspflichten von Rufnummer-Providern einer positivrechtlichen Regelung zugeführt worden. § 13a TKV ist lex specialis zu der allgemeinen Störerhaftung und führt im Ergebnis zu einer umfassenderen Haftungsprivilegierung des Rufnummer-Providers als dies nach den allgemeinen Haftungsgrundsätzen der Fall wäre.[231]

Nach § 13a TKV muss derjenige, der anderen eine Mehrwertdienstenummer überlässt, diese zunächst darauf hinweisen, dass die Rufnummer nicht für rechtswidrige Tätigkeiten genutzt werden darf. Dies korrespondiert insoweit mit den oben angesprochenen Hinweisen der Access Provider zur Beachtung fremder Urheberrechte in deren Allgemeinen Geschäftsbedingungen. Darüber hinaus werden jedoch hohe Anforderungen an eine weitergehende Handlungspflicht des Rufnummer-Providers gestellt. Voraussetzung ist zunächst, dass dieser *„gesicherte Kenntnis“* von einem Rechtsverstoß des Kunden erhält. Das Merkmal der *„gesicherten Kenntnis“* geht über das Kenntniserfordernis des § 11 TDG hinaus. Es liegt erst dann vor, wenn der Verpflichtete über alle die Rechtswidrigkeit begründenden Umstände informiert wurde, diese auf ihre Rechtswidrigkeit prüfen kann und

[230] So auch Volkmann, Störer im Internet, S. 160.
[231] Berger, MMR 2003, 642, 645; Spindler/Volkmann, NJW 2004, 808, 809.

diese Prüfung nach gesicherter Rechtslage zwingend zu einer Rechtswidrigkeit führt.[232] Ist dies der Fall, muss der Rufnummer-Provider unverzüglich *„Maßnahmen“* zur zukünftigen Unterbindung von Verstößen dieses Nutzers treffen. Zu diesen Maßnahmen zählt zunächst, den jeweiligen Nutzer abzumahnen. Durch diese Abmahnung soll dem Nutzer die Rechtswidrigkeit seiner Tätigkeit vor Augen gehalten und er dazu bewegt werden, seine Tätigkeit auf den rechtlich zulässigen Rahmen zu beschränken. Nur wenn eine solche Abmahnung keine Wirkung zeigt und der Provider auf erneute Rechtsverstöße hingewiesen wird, soll als *ultima ratio* eine Sperrung des jeweiligen Nutzers in Betracht kommen.[233]

Auch wenn für die Regelung des § 13a TKV ausweislich der Gesetzesbegründung vor allem die Haftungsprivilegierung für Host-Provider gem. § 11 TDG zum Vorbild genommen wurde,[234] spricht nichts dagegen, diese Wertungen in modifizierter Weise auch für Access Provider fruchtbar zu machen.[235] Denn Rufnummer-Betreiber stehen in der Regel den Access Providern näher als den Host-Providern, da auch diese Verbindungen zu einem Dienst bzw. Kommunikationsnetz herstellen.[236] Modifiziert werden müssen diese Haftungsgrundsätze jedoch bereits deshalb, weil es dem Access Provider, wie soeben festgestellt wurde, nicht zuzumuten ist, auf jeden angezeigten Rechtsverstoß zu reagieren. Andererseits ist jedoch nicht ersichtlich, warum dem Access Provider nicht zumindest dann ein Beitrag zur Verhinderung weiterer Rechtsverletzungen abverlangt werden sollte, wenn durch dessen Nutzer Schutzrechtsverletzungen im erheblichen Maße getätigt werden. Dies sollte z.B. dann gelten, wenn der Access Provider durch eindeutige Hinweise der Rechteinhaber (z.B. mittels dokumentierter Testdownloads und Screenshots vom Angebot eines FTP-Servers) darauf hingewiesen wird, dass ein Nutzer unter Verstoß des § 19a UrhG eine Vielzahl von Werken zum Download bereitstellt. [237]

Bei solch schwerwiegenden Rechtsverletzungen wird es auch dem Access Provider zumutbar sein, den Nutzer zunächst abzumahnen sowie bei wiederholten Verstößen von seinem vertraglichen oder gesetzlichen Kündi-

---

[232] So Berger, MMR 2003, 642, 645.
[233] Hoeren, Access Provider, Rn. 634.
[234] Amtl. Begründung zu § 13a TKV, BR-Drs. 505/02, S. 4.
[235] Ähnlich Spindler/Volkmann, NJW 2004, 808, 810 für die Vergabe von Sub-Domains.
[236] OLG Stuttgart, Urt. v. 1.8.2002 – 2 U 47/01, NJW-RR 2003, 1273, 1274; Spindler/Volkmann, NJW 2004, 808, 809.
[237] A.A. Spindler/Dorschel, CR 2005, 38, 42, die davon ausgehen, dass Prüfpflichten immer nur dann begründet werden können, wenn der Access Provider eigenhändig auf den fraglichen Inhalt zugreifen und diesen auf seine Rechtswidrigkeit überprüfen kann.

gungsrecht aus § 314 BGB Gebrauch zu machen bzw. den Zugang des Kunden zu sperren. Dadurch könnte ein gerechter Interessenausgleich erzielt werden. Für den Kunden böte eine Abmahnpflicht des Access Providers den Vorteil, dass sich dieser nicht sogleich mit einer sofortigen Sperrung seines Anschlusses konfrontiert sähe, die mitunter, z.B. bei der Sperrung eines Unternehmenszugangs, zu erheblichen finanziellen Verlusten führen könnte. Zugleich könnte der Nutzer zu den behaupteten Rechtsverstößen Stellung nehmen und hätte es zudem selbst in der Hand, seinen Vertragsstatus durch Rückkehr in die Legalität aufrecht zu erhalten. Ebenso würde hierdurch das vertragliche Haftungsrisiko des Access Providers hinsichtlich einer unberechtigten Sperrung verringert und zugleich auch dem Interesse der Rechteinhaber an der Abstellung dieser Rechtsverletzungen Rechnung getragen.

An dieser Stelle ist jedoch bereits darauf hinzuweisen, dass die soeben beschriebenen Verkehrssicherungspflichten nur dann durchdringen können, wenn der Access Provider auch datenschutzrechtlich berechtigt ist, sowohl die IP-Adresse der Nutzer zu speichern als auch diese einem bestimmten Nutzer zuzuordnen,[238] da er anderenfalls den Nutzer nicht identifizieren und ihm somit auch keine Abmahnung zustellen könnte. In diesen Fällen würde der Access Provider seinen Verkehrssicherungspflichten bereits mit den oben beschriebenen Hinweispflichten genügen.

(c) Auskunftserteilung als spezielle Verkehrssicherungspflicht

Selbst wenn man die datenschutzrechtliche Zulässigkeit dieser – an § 13a TKV angelehnten – Handlungspflichten unterstellt, wäre den Rechteinhabern freilich nicht viel geholfen, wenn der Access Provider lediglich seinen Kunden abmahnt bzw. dessen Zugang sperrt, der Nutzer jedoch sein rechtsverletzendes Verhalten über einen anderen Zugangsprovider fortsetzt. Zielführender wäre es für die Rechteinhaber daher, wenn sich die Verkehrssicherungspflicht des Access Providers unmittelbar in einer Auskunftspflicht über die Identität des Nutzers konkretisieren würde. In dieser Hinsicht wurde bereits bezüglich des Subdomain Providers die Auffassung vertreten, dieser müsse im Rahmen seiner Verkehrssicherungspflichten die Identität seiner anonym agierenden Kunden preisgeben, sofern diese rechtsverletzende Handlungen begehen.[239]

[238] Ausführlich dazu unten, 5. Teil A. IV.
[239] Flechsig, MMR 2002, 347, 351.

Eine solche Forderung ist mit dem Störerhaftungsrecht jedoch nicht in Einklang zu bringen. Könnte sich nämlich der potentielle mittelbare Störer durch eine Preisgabe von Identitäten von seiner Haftung lösen, würde dies gegen den Grundsatz des Störerhaftungsrechts verstoßen, dass der mittelbare Störer neben dem Hauptverantwortlichen uneingeschränkt als Störer haftet.[240] Dies liefe auf ein gestuftes Haftungssystem – vergleichbar mit dem amerikanischen notice-and-take-down Verfahren – hinaus, auf dessen Einführung der Gesetzgeber bisher bewusst verzichtet hat.[241] Vor allem lässt sich gegen eine auf Auskunft gerichtete Verkehrssicherungspflicht einwenden, dass zivilrechtliche Drittauskunftsansprüche nur sehr zurückhalten gewährt werden und zumeist, wie der Anspruch aus § 101a UrhG, spezialgesetzlich geregelt sind. Daher würde es dogmatisch schon befremdlich anmuten, wenn man derartige Auskunftspflichten über den Umweg von Verkehrssicherungspflichten konstruieren könnte, würden dadurch doch die Voraussetzungen der spezialgesetzlichen Auskunftstatbestände obsolet. Aus diesem Grund lassen sich also auch durch Verkehrssicherungspflichten keine unmittelbaren Drittauskunftspflichten begründen.

3. Ergebnis der Störerhaftung

Werden im Internet durch die Nutzer des Access Providers Urheberrechte Dritter verletzt, so kann der Access Provider hierfür nicht als unmittelbarer Verletzer i.S.d. § 97 UrhG zu Verantwortung gezogen werden, weil er weder unmittelbarer Verletzer des § 16 UrhG noch des § 19a UrhG ist. Da der Access Provider mit der Zugangsgewährung jedoch einen adäquatkausalen und willentlichen Beitrag zu den Urheberrechtsverletzungen seiner Nutzer setzt, kommt zumindest eine mittelbare Störerhaftung in Betracht. Für dessen Begründung ist jedoch erforderlich, dass dem Access Provider eine Verletzung von Prüf- bzw. Verkehrssicherungspflichten vorgeworfen werden kann. In präventiver Hinsicht obliegt diesem zumindest eine dahingehende Verpflichtung, seine Nutzer zur Beachtung fremder Urheberrechte anzuhalten. Da jedoch nahezu alle Access Provider solche Hinweise in ihren Allgemeinen Geschäftsbedingungen vorsehen, scheidet eine mittelbare Störerhaftung der Access Provider zumindest bei sog. einfachen Schutzrechtrechtsverletzungen in der Regel aus. Allenfalls bei schwerwiegenden Schutzrechtsverletzungen erscheint es gerechtfertigt, den Access Provider – in Anlehnung an § 13a TKV – zu verpflichten, konkrete Nutzer abzumahnen oder im Falle wiederholter Verstöße zu sperren, sofern

[240] BGH, Urt. v. 27.5.1986 – VI ZR 169/85, NJW 1986, 2503, 2504; Spindler, in: Spindler/Schmitz/Geis, § 8 TDG, Rn. 31.
[241] Volkmann, Störer im Internet, S. 157.

die dafür erforderlichen Handlungen datenschutzrechtlich zulässig sind. Keinesfalls konkretisieren sich Verkehrssicherungspflichten der Access Provider jedoch bereits in einer Verpflichtung zur Auskunftserteilung, da dadurch die Tatbestandsvoraussetzungen spezieller Auskunftsverpflichtungen – wie die des § 101a UrhG – ausgehebelt würden.

4. Verletzereigenschaft des Access Providers als mittelbarer Störer

Sofern ausnahmsweise eine mittelbare Störerhaftung des Access Providers begründet werden kann oder man mit der – hier abgelehnten Auffassung – davon ausgeht, dass der Access Provider bereits nach Kenntniserhalt von einfachen Rechtsverletzungen seiner Nutzer als mittelbarer Störer haftet,[242] stellt sich die Frage, ob die mittelbare Störereigenschaft überhaupt eine Verletzungshandlung i.S.d. § 101a UrhG begründen kann. Gegen die Erstreckung des Anwendungsbereichs des § 101a UrhG auf mittelbare Verletzungshandlungen werden eine Reihe von Argumenten vorgebracht, die im Folgenden näher betrachtet werden sollen.

a) Erfordernis einer eigenhändigen (vorsätzlichen) Verletzungshandlung

Namentlich Kitz vertritt die Auffassung, dass sich der Anwendungsbereich des § 101a UrhG nur auf eigenhändige Verletzungshandlungen erstreckt. Hierzu beruft er sich auf den Wortlaut des § 101a UrhG, nach dem die Rechtsverletzung gerade *„durch“* die Herstellung oder Verbreitung von Vervielfältigungsstücken verursacht worden sein muss. Nach Kitz soll dieser Zusatz im Sinne einer tätigkeitsbezogenen, eigenhändigen Komponente zu verstehen sein, die sowohl die Passivlegitimation des Teilnehmers als auch des mittelbaren Störers ausschließt.[243]

Kitz ist zunächst zuzugeben, dass der Wortlaut des § 101a UrhG in der Tat den Schluss zulässt, dass nur eine eigenhändige Verletzungshandlung des Anspruchsgegners auskunftsbegründend wirkt. Allerdings lässt sich diese Beschränkung des Kreises der Passivlegitimierten nur schwerlich mit dem horizontalen Regelungsansatz des Gesetzgebers vereinbaren. Gegen eine solche Beschränkung des Anwendungsbereichs lässt sich zunächst der – auf § 101a UrhG verweisende – geschmacksmusterrechtliche Auskunftsan-

[242] So OLG Frankfurt a.M., Urt. v. 25.1.2005 – 11 U 51/05, MMR 2005, 241, 243 = CR 2005, 285; Spindler, in: Spindler/Schmitz/Geis, § 9 TDG, Rn. 34 m.w.N.

[243] Kitz, ZUM 2005, 298, 301; zustimmend Dorschel, Anm. zu OLG Hamburg, Urt. v. 28.4.2005 – 5 U 156/04, CR 2005, 516, 517.

spruch des § 14a GeschMG a.F.[244] rekurrieren. Auch nach dessen Wortlaut ist nur derjenige auskunftspflichtig, der ein Muster oder Model *„dadurch"* verletzt, dass er widerrechtlich eine Nachbildung hergestellt oder verbreitet hat. Trotz dieses terminologischen Gleichklangs mit § 101a UrhG, haftet dennoch nicht nur der eigenhändige unmittelbare Verletzer auf Auskunft gem. § 14a Abs. 3 GeschmMG a.F. i.V.m. § 101a UrhG, sondern jeder, dessen Verhalten für die Rechtsverletzung ursächlich ist.[245] Weiterhin haftet auch nach dem mit § 101a UrhG korrespondierenden markenrechtlichen Auskunftsanspruch des § 19 MarkenG jeder, der eine Verletzungshandlung i.S.d. §§ 14, 15, 17 MarkenG begangen hat. Auch diese Ansprüche richten sich neben den unmittelbaren Täter zumindest auch gegen den Teilnehmer einer Markenrechtsverletzung.[246] In Anbetracht des horizontalen Regelungsansatzes des Gesetzgebers ist der Auffassung von Kitz, dass nur der eigenhändige unmittelbare Verletzer auch Verletzer i.S.d. § 101a UrhG sein kann, somit zu widersprechen.

Abzulehnen ist daher auch die noch restriktivere Ansicht Schlegels[247], nach der eine Auskunftspflicht nach § 101a UrhG nur durch eine vorsätzliche Mittäterschaft an einer Vertriebskette begründet werden soll. Dies soll daraus folgen, dass nur derjenige etwas offen legen könne, der sich mit Wissen und Wollen an der Vertriebskette beteilige.[248] Dieser Ansicht ist sowohl in tatsächlicher als auch in rechtlicher Hinsicht zu widersprechen. So hängt z.B. die Frage, ob der Access Provider die Identität seines Nutzers offen legen kann, lediglich davon ab, ob dieser – in rechtlich zulässiger Weise – eine Verknüpfung zwischen der IP-Adresse und der Identität des Verletzers herstellen kann, nicht aber davon, ob er vorsätzlich oder unvorsätzlich an dessen Rechtsverletzung partizipiert hat. In rechtlicher Hinsicht würde das von Schlegel vertretene Vorsatzerfordernis den Willen des Gesetzgebers des PrPG geradezu konterkarieren. Denn dieser hat explizit ausgeführt, dass der Auskunftsanspruch verschuldensunabhängig ausgestaltet werden muss, um der Gefahr zu begegnen, dass sich der konkret belangte Verletzer erfolgreich auf seinen guten Glauben berufen kann.[249] Demzufolge kann die Begründung einer Verletzereigenschaft i.S.d. § 101a UrhG

---

[244] Außerkraftgetretenen durch das Geschmacksmusterreformgesetz vom 12. März 2004, BGBl. I/2004, S. 390 ff; der Auskunftsanspruch ist dabei mit verändertem Wortlaut in § 46 GeschMG überführt worden.
[245] Nirk/Kurtze, GeschmMG, § 14a, Rn. 10, 12.
[246] Fezer, § 14, Rn. 508; Ingerl/Rohnke, vor §§ 14-19, Rn. 20.
[247] Schlegel, Anm. zu LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, CR 2005, 144, 144.
[248] Schlegel, a.a.O.
[249] Amtl. Begründung zum PrPG, BT-Drs. 11/4792, S. 31.

nicht vom Vorliegen einer vorsätzlichen und unmittelbaren Verletzungshandlung abhängig gemacht werden. Festzuhalten bleibt daher zunächst, dass zumindest eine Beschränkung des Kreises der Passivlegitimierten auf eigenhändige täterschaftliche Verletzungshandlungen abzulehnen ist. Damit ist allerdings noch keine Aussage darüber getroffen, ob auch der mittelbare Rechtsverletzer auskunftspflichtig i.S.d. § 101a UrhG sein kann.

b) Beschränkung auf den deliktischen Verletzer

Nach überwiegend vertretener Auffassung wird eine Passivlegitimation des mittelbaren Störers mit der Begründung abgelehnt, dass unter das im Tatbestand erhobene Merkmal des Verletzens nur der deliktische Verletzer subsumiert werden kann, also der Täter und der vorsätzliche handelnde Teilnehmer i.S.d. §§ 830 Abs. 1 S. 1, 830 Abs. 2 BGB.[250] Untermauert wird diese Annahme vor allem mit dogmatischen Argumenten. So wird behauptet, der Begriff des Verletzens in § 101a UrhG könne nicht generell mit dem Merkmal des mittelbaren Störens gleichgesetzt werden, da der mittelbare Störer auch kein Verletzer i.S.d. § 97 UrhG sei. Dessen Unterlassungspflicht folge nämlich nicht aus § 97 UrhG, sondern aus §§ 862, 1004 BGB.[251] Diese Ansprüche seien jedoch lediglich Abwehransprüche, die keine Auskunftspflichten begründen könnten.[252]

Auch dieser Argumentation kann in dieser Pauschalität nicht gefolgt werden. Zunächst ist der Annahme zu widersprechen, dass die Haftung des mittelbaren urheberrechtlichen Störers nicht auf § 97 UrhG beruhen soll. Zwar wurde der mittelbare Störer in der früheren Rechtsprechung tatsächlich in analoger Anwendung unter § 1004 BGB gefasst,[253] allerdings betraf dies Entscheidungen, die vor In-Kraft-Treten des spezialgesetzlichen urheberrechtlichen Unterlassungstatbestandes im Jahre 1965 ergangen sind. In den Gesetzesmaterialien zum Urheberrechtsgesetz wurde jedoch ausgeführt, dass die Fallgruppen der mittelbaren Störerhaftung fortan nicht mehr von § 1004 BGB, sondern vom zentralen urheberrechtlichen Verletzungstatbestand erfasst werden sollen,[254] also von § 97 UrhG. Da auch der Wort-

[250] OLG Hamburg, Urt. v. 28.4.2005 – 5 U 156/04, MMR 2005, 453, 456 mit zust. Anm. Linke = CR 2005, 512; OLG Frankfurt a.M., Urt. v. 25.1.2005 – 11 U 51/05, MMR 2005, 241, 243 mit abl. Anm. Spindler = CR 2005, 285; Kitz, ZUM 2005, 298, 299.
[251] Kitz, ZUM 2005, 298, 299.
[252] OLG Hamburg, a.a.O.; OLG Frankfurt, a.a.O.
[253] Vgl. BGH, Urt. v. 29.5.1964 – Ib ZR 4/63, GRUR 1965, 104, 108 – Personalausweise; BGH GRUR 1964, 94, 96 – Tonbandgeräte-Händler I; BGH GRUR 1955, 492 – Tonbandgerätehersteller.
[254] Amtl. Begründung zum UrhG, BT-Drs. IV/270, S. 103; Freytag, S. 66.

laut des § 97 UrhG jedoch nicht explizit von mittelbarem Stören, sondern allgemein von Verletzen spricht, kommt als dogmatischer Anknüpfungspunkt für die mittelbare Störerhaftung nur das in § 97 UrhG erhobene Merkmal des Verletzens in Betracht. Daher ist davon auszugehen, dass auch der mittelbare Störer als Verletzer i.S.d. § 97 UrhG zu qualifizieren ist.[255] Vor diesem Hintergrund ist somit nicht ersichtlich, warum für den – offensichtlich an § 97 UrhG angelehnten – Verletzerbegriff des § 101a UrhG etwas anderes gelten sollte. Gestützt wird diese Annahme ferner durch den horizontalen Regelungsansatz des Gesetzgebers. So werden nämlich auch im Rahmen des markenrechtlichen Auskunftsanspruchs nach § 19 MarkenG nicht nur Täter und Teilnehmer unter den Verletzerbegriff des § 19 Abs. 1 MarkenG subsumiert, sondern jeder, der eine Verletzungshandlung begangen oder daran mitgewirkt hat. [256] Schließlich korrespondiert die Erstreckung des Verletzerbegriffes auf den mittelbaren Störer auch mit dem verletzungsunabhängigen Charakter, den der Gesetzgeber diesen Ansprüchen zugeschrieben hat.[257]

c) Zwischenergebnis

Die gegen eine Passivlegitimation des mittelbaren Störers hervorgebrachten Bedenken können nicht überzeugen. Eine einschränkende Auslegung des Anwendungsbereichs des § 101a UrhG auf eigenhändige oder vorsätzliche Verletzungshandlungen ergibt sich weder aus dem Wortlaut noch aus der Gesetzessystematik und widerspricht zudem dem historischen Willen des Gesetzgebers. Demnach ist also auch der Access Provider passivlegitimiert i.S.d. § 101a UrhG, sofern dieser ausnahmsweise als mittelbarer Störer qualifiziert werden kann.

V. Verhältnismäßigkeit einer Auskunftspflicht des Access Providers

Da eine Auskunftserteilung nach § 101a Abs. 1 UrhG zudem unter dem Vorbehalt der Verhältnismäßigkeit steht, ist weiterhin zu untersuchen, ob sich die Inanspruchnahme des Access Providers auf Herausgabe von Nutzerdaten als verhältnismäßig darstellt.

---

[255] So auch BGH, Urt. v. 15.10.1998 – I ZR 120/96, GRUR 1999, 418, 419 f. m.w.N. = WRP 1999, 211 – Möbelklassiker.

[256] BGH, Urt. v. 23.2.2006 – I ZR 27/03 – Parfümtestkäufe, Rn. 32, abrufbar unter: http://juris.bundesgerichtshof.de/cgibin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=2006-2&nr=35913&pos=12&anz=219&Blank=1.pdf ; Ingerl/Rohnke, § 19 Rn. 10, vor §§ 14-19, Rn. 29 ff.

[257] Amtl. Begründung zum PrPG, BT-Drs. 11/4792, S. 31.

1. Regelungsgehalt der Verhältnismäßigkeitsklausel

Mit der Verhältnismäßigkeitsklausel hat der Gesetzgeber zum Ausdruck gebracht, dass dem Auskunftsanspruch nach § 101a UrhG eine Abwägung widerstreitender Interessen zugrunde liegt.[258] Vereinzelt wird die Auffassung vertreten, dass es sich bei dem Passus *„es sei denn, dass dies im Einzelfall unverhältnismäßig ist“* lediglich um einen deklaratorischen Hinweis auf den aus dem Rechtsstaatsprinzip abgeleiteten Grundsatz der Verhältnismäßigkeit[259] handelt. Da dieser Grundsatz ohnehin die gesamte deutsche Rechtsordnung beherrscht, könne auch der Verhältnismäßigkeitsklausel des § 101a UrhG kein eigenständiger Regelungscharakter zukommen.[260] Dem ist jedoch zu widersprechen. Die Verhältnismäßigkeitsklausel ist bereits deshalb nicht ausschließlich deklaratorischer Natur, weil der Wortlaut nicht nur das Bestehen einer Verhältnismäßigkeitsprüfung anordnet, sondern zugleich auch eine Aussage über die Verteilung der Darlegungs- und Beweislast hinsichtlich der Unverhältnismäßigkeit einer Auskunftpflicht trifft. Diese Umstände sind nach dem eindeutigen Wortlaut nämlich vom Verletzer vorzutragen.[261] Dadurch kann man der Verhältnismäßigkeitsklausel des § 101a UrhG zugleich die gesetzgeberische Wertung entnehmen, dass im Regelfall das Interesse der Rechteinhaber an einer Aufdeckung und Verfolgung von Schutzrechtsverletzungen das Interesse der Verletzer an der Geheimhaltung ihrer Vertriebswege überwiegt.[262]

2. Umfang der Verhältnismäßigkeitsprüfung

Hinsichtlich des Umfangs der Verhältnismäßigkeitsprüfung lässt sich den Gesetzesmaterialien lediglich entnehmen, dass die Verhältnismäßigkeitsklausel in erster Linie den Verletzer vor einer Ausforschung durch einen Konkurrenten schützen soll. Der Verletzer soll einem Konkurrenten nicht unnötig Betriebsinterna wie Kunden- oder Lieferantenlisten offenbaren müssen, wenn weitere Schutzrechtsverletzungen ausgeschlossen und eingetretene Schäden ausgeglichen sind.[263] Dieser Schutzzweck ist im Rahmen der Auskunftspflicht des Providers bereits deshalb nicht tangiert, da

---

[258] Dreier, § 101a UrhG, Rn. 8.

[259] Dazu BVerfGE, Beschl. v. 26.2.1969 – 2 BvL 15, 23/68, BVerfGE 25, 269, 292 – Verfolgungsverjährung; Schmidt-Bleibtreu/Klein/Hofmann, Art. 20, Rn. 73 ff.

[260] Nordemann/Nordemann, § 101a UrhG, Rn. 5.; Schricker/Wild, § 101a UrhG, Rn. 4.

[261] Wandtke/Bullinger/Bohne, § 101a UrhG, Rn. 9.

[262] BGH, Urt. v. 24.3.1994 – I ZR 42/93, GRUR 1994, 630, 633 – Cartier-Armreif; Wandtke/Bullinger/Bohne, § 101a UrhG, Rn. 9; ebenso Fezer, § 19 MarkenG, Rn. 14 zum markenrechtlichen Auskunftsanspruch.

[263] Amtl. Begründung zum PrPG, BT-Drs. 11/4792, S. 32.

die Anspruchssteller in den hier einschlägigen Konstellationen keine Konkurrenten des Providers, sondern Inhaber von Urheber- und Leistungsschutzrechten sind, die zudem kein wettbewerbliches Interesse an den Nutzerdaten der Provider haben. Andererseits ist jedoch nicht davon auszugehen, dass der Gesetzgeber den Schutzzweck der Verhältnismäßigkeitsklausel auf unzulässige Ausforschungsfälle beschränken wollte.[264] Zweckmäßigerweise ist auch im Rahmen der Verhältnismäßigkeitsprüfung des § 101a UrhG, ebenso wie bei der Interessenabwägung im Rahmen des allgemeinen Auskunftsanspruchs aus § 242 BGB, das aus dem öffentlichen Recht bekannte Verhältnismäßigkeitsprinzip uneingeschränkt für anwendbar zu erklären, da nur so eine umfassende Abwägung aller Umstände des Einzelfalles vorgenommen werden kann.[265]

3. Voraussetzungen des Verhältnismäßigkeitsgrundsatzes

In Anlehnung an den öffentlich-rechtlichen Verhältnismäßigkeitsgrundsatz ist somit zu fordern, dass die Auskunftserteilung durch den Access Provider für die Rechtsverfolgung der Rechteinhaber geeignet, erforderlich und angemessen ist.

a) Geeignetheit der Auskunftserteilung

Geeignet ist die Auskunftserteilung des Access Providers dann, wenn mit der Preisgabe der Identität des Nutzers der vom Gesetzgeber angestrebte Gesetzeszweck, also die Bekämpfung von Schutzrechtsverletzungen,[266] zumindest gefördert werden könnte.[267] Dies ist der Fall, da die Preisgabe der Identität der Rechtsverletzer es den Rechteinhabern ermöglicht, diese zivilrechtlich zu verfolgen und dadurch künftige Rechtsverletzungen zu unterbinden.[268]

b) Erforderlichkeit angesichts strafprozessualer Auskunftsmöglichkeiten

Schwieriger gestaltet sich die Frage, ob der Auskunftsanspruch nach § 101a UrhG für die Rechteinhaber auch erforderlich ist. Das wäre abzulehnen, wenn den Rechteinhabern ein vergleichbar geeignetes, jedoch milderes Mittel zur Verfügung stehen würde, um zivilrechtliche Ansprüche

---

[264] Wiume, S. 173 f.
[265] So auch Oppermann, S. 127; vgl. auch Fezer, § 19 MarkenG, Rn. 14.
[266] Amtl. Begründung zum PrPG, BT-Drs. 14/4792, S. 30.
[267] Vgl. Michael, JuS 2001, 148, 149.
[268] LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, CR 2005, 136, 139 = MMR 2005, 55.

gegen die Nutzer des Access Providers durchzusetzen.[269] Dies wäre z.B. dann der Fall, wenn sich die Rechteinhaber die Identität der Rechtsverletzer in zumutbarer Weise selbst beschaffen könnten.[270] Dass der Rechteinhaber eine generierte IP-Adresse nicht eigenhändig einem bestimmten Nutzer zuordnen kann, ergibt sich bereits daraus, dass dieser ansonsten auf Auskunft des Access Providers gar nicht angewiesen wäre. Unbenommen bleibt es dem Rechteinhaber jedoch, sich die Ermittlungsbefugnisse der Staatsanwaltschaft zunutze zu machen, indem er unter Angabe der IP-Adresse eine Strafanzeige gegen den unbekannten Rechtsverletzer erstattet, um sodann im Wege der Akteneinsicht nach § 406e StPO Kenntnis von der Identität des Rechtsverletzers zu erlangen.[271] Ob diese Möglichkeit jedoch ein gleich geeignetes Mittel darstellt, kann bezweifelt werden. So werden sich die Rechteinhaber gerade bei geringfügigen Urheberrechtsverletzungen häufig damit konfrontiert sehen, dass die Staatsanwaltschaften das Strafverfolgungsinteresse verneinen und die Rechteinhaber auf den Privatklageweg nach §§ 374 Abs. 1 Nr. 8, 376 StPO verweisen.[272] Sofern die Staatsanwaltschaft die Auskunft über die IP-Adresse nicht im Wege von Vorermittlungen nach Nr. 87 RiStBV einholt, geht daher auch das Akteneinsichtsrecht nach § 406e StPO ins Leere. Die Fälle, in denen es nach dem Opportunitätsprinzip zu einer Einstellung des Verfahrens kommt, dürften indes zunehmen, nachdem die Staatsanwaltschaften infolge der Überlastung durch die massenhafte Erstattung von Strafanzeigen unter Angabe von IP-Adressen bereits haben anklingen lassen, Verfahren künftig einzustellen, wenn nicht nachweislich eine erhebliche Anzahl von urheberrechtlich geschützten Werken heruntergeladen oder zum Download bereitgestellt wurde.[273] Somit bestehen Zweifel daran, dass die Möglichkeit der strafprozessualen Akteneinsicht ein gleich geeignetes Mittel zur Erlangung der gewünschten Auskunft darstellt.

Gestützt wird diese Annahme zudem dadurch, dass es gerade vor dem Hintergrund des ultima-ratio-Gedankens des Strafrechts nicht gerechtfertigt wäre, die Gewährung eines effektiven zivilrechtlichen Rechtsschutzes von der Bejahung eines öffentlichen Strafverfolgungsinteresses abhängig zu

---

[269] Vgl. Michael, JuS 2001, 148, 149.
[270] Oppermann, S. 130 f. m.w.N.
[271] Vgl. Kitz, GRUR 2003, 1014, 1018; ausführlich zum Akteneinsichtsrecht des § 406e StPO, Oppermann, S. 198 ff.
[272] Kitz, GRUR 2003, 1014, 1018.
[273] Vgl. Heise News, Meldung v. 26.1.2006: Generalstaatsanwaltschaft klagt über ungebremste P2P-Strafanzeigen-Maschinerie, http://www.heise.de/newsticker/meldung/68882.

machen.[274] Des Weiteren spricht für die Möglichkeit einer separaten Geltendmachung zivilrechtlicher Auskunftsansprüche die Tatsache, dass die Auskunftsansprüche des PrPG größtenteils leer liefen, wenn man in allen Fällen, in denen die Möglichkeit einer strafprozessualen Akteneinsicht bestünde, diese Ansprüche insgesamt für nicht erforderlich halten und damit als unverhältnismäßig einstufen würde. So sind nicht nur Urheberrechtsverletzungen, sondern auch die Verletzung der anderen geistigen Schutzrechte ebenfalls strafbewehrt.[275] Die Möglichkeit einer parallelen Geltendmachung von zivil- und strafrechtlichen Ansprüchen findet zudem eine Stütze in den Gesetzesmaterialien des PrPG. Darin wird explizit darauf hingewiesen, dass es dem verletzten Schutzrechtsinhaber auch weiterhin frei stehe, einen Strafantrag zu stellen, um auf den Informationsgewinn der Staatsanwaltschaft zugreifen zu können.[276] Dieser Passus kann nur in dem Sinne verstanden werden, dass beide Anspruchskategorien nebeneinander anwendbar sind. Resümierend lässt sich also festhalten, dass die Möglichkeit der strafprozessualen Akteneinsicht der Erforderlichkeit einer zivilrechtlichen Auskunftspflicht nach § 101a UrhG nicht entgegensteht.

c) Angemessenheit

Im Rahmen der Angemessenheit einer Auskunftspflicht sind im Allgemeinen sowohl das Verschulden des Verletzers[277], die Schwere der Verletzungshandlung[278] als auch der Aufwand[279] der Auskunftserteilung zu berücksichtigen. Wird der Access Provider als mittelbarer Störer in Anspruch genommen, mangelt es jedoch bereits an dessen Verschulden. Dies allein vermag zwar angesichts des verschuldensunabhängigen Charakters des § 101a UrhG noch keine Unangemessenheit der Auskunftspflicht insgesamt begründen. Allerdings ist auch die Schwere einer bloß mittelbaren Verletzungshandlung als gering einzustufen. Weiterhin ist zu berücksichtigen, dass sich die Situation des Access Providers von den originären Rechtsverletzern des § 101a UrhG erheblich unterscheidet. Denn im Gegensatz zu diesen, weist der Access Provider keine unmittelbare Beziehung zum Verletzungsgegenstand auf, mithin kann er nicht als Teil einer klassi-

[274] LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, CR 2005, 136, 139 = MMR 2005, 55; LG Köln, Urt. v. 28.7.2004 – 28 O 301/04, ZUM 2005, 236, 240.
[275] Z.B. §§ 143 ff. MarkenG.
[276] Amtl. Begründung zum PrPG, BT-Drs. 14/4792, S. 33.
[277] Vgl. Fezer, § 19 MarkenG, Rn. 14; Wiume, S. 185.
[278] Wiume, S. 187 m.w.N.
[279] LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, CR 2005, 136, 139 = MMR 2005, 55; ablehnend Wiume, S. 183.

schen Vertriebskette angesehen werden.[280] Zudem dürften sich die Access Provider, anders als herkömmliche Rechtsverletzer, nicht nur mit einzelnen, sondern mit einer Vielzahl von Auskunftsersuchen konfrontiert sehen. Geht man zudem mit dem OLG Hamburg davon aus, dass allein für das Auslesen einer IP-Adresse Kosten in Höhe von 35 € aufgewendet werden müssen,[281] dann trifft den Access Provider nicht nur ein erheblicher Arbeitsaufwand, sondern auch eine enorme Kostenlast. Denn anders als im Falle der strafprozessualen Auskunftspflicht, bei der dem Access Provider ein Entschädigungsanspruch nach § 23 JVEG zusteht,[282] sieht § 101a UrhG gerade keine Entschädigungsregelung vor, nach der diese Kosten vom Anspruchsgegner zu erstatten wären. Sofern in dieser Hinsicht darauf verwiesen wird, dass sich der Provider hinsichtlich dieser Kosten an seinem rechtsverletzenden Nutzer schadlos halten könne,[283] darf nicht verkannt werden, dass auch eine Verweisung auf die Geltendmachung von Ansprüchen gegenüber Dritten, nicht zuletzt aufgrund des Ausfallrisikos, zu einer erheblichen Belastung der Access Provider führen kann.

Bereits die Abwägung der gegenteiligen Interessen aus Art. 14 GG, namentlich des Rechts am eingerichteten und ausgeübten Gewerbetrieb des Access Providers sowie der vermögenswerten Verwertungsrechte der Rechteinhaber, führt daher zu der Annahme, dass eine Inanspruchnahme des Access Providers nach § 101a UrhG zumindest in den Fällen einer bloß mittelbaren Störerhaftung regelmäßig als unverhältnismäßig einzustufen ist. Dies gilt zumindest dann, wenn es sich bei den Rechtsverletzungen der Nutzer um sog. „einfache Schutzrechtsverletzungen" handelt, also solche, bei denen z.B. nur einzelne Werke aus einem Filesharing-Netzwerk heruntergeladen werden. Andererseits dürfte eine Auskunftspflicht aufgrund mittelbarer Störerhaftung zumindest dann verhältnismäßig sein, wenn unter einer IP-Adresse, die ggf. noch mit einer dynamischen Domain verbunden ist, eine erhebliche Anzahl von Werken zum Download bereitgestellt wird oder Werke in großem Umfang heruntergeladen werden.[284]

---

[280] OLG Frankfurt a.M., Urt. v. 25.1.2005 – 11 U 51/05, MMR 2005, 241, 243= CR 2005, 285.

[281] OLG Hamburg, Urt. v. 28.4.2005 – 5 U 156/04, JurPC Web-Dok. 62/2005, Abs. 23 = MMR 2005, 453 = CR 2005, 512.

[282] OLG Zweibrücken, Beschl. v. 24.6.1997 – 1 Ws 313/97 NJW 1997, 2692, 2692 zur Vorgängervorschrift des § 17a ZSEG.

[283] LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, CR 2005, 136, 139 = MMR 2005, 55.

[284] Ein vergleichbarer Sachverhalt lag auch den einschlägigen Entscheidungen der Landgerichte Hamburg und Köln zugrunde.

VI. Durchsetzbarkeit der Auskunftspflicht im einstweiligen Verfügungsverfahren

Auch wenn sich die Inanspruchnahme des Access Providers ausnahmsweise als verhältnismäßig erweist, kommt hinsichtlich der Geltendmachung des Anspruchs erschwerend hinzu, dass sie dieser regelmäßig nicht im Wege des einstweiligen Verfügungsverfahrens durchsetzen ließe. Denn notwendige Voraussetzung für den Erlass einer einstweiligen Verfügung ist nach § 101a Abs. 3 UrhG, dass sich die Rechtsverletzung als offensichtlich darstellt. Von einer offensichtlichen Rechtsverletzung ist jedoch nur dann auszugehen, wenn die Rechtslage unzweifelhaft ist und keine Umstände erkennbar sind, die im Hautpsacheverfahren einer Klärung bedürfen, mithin eine Fehlentscheidung und damit eine ungerechtfertigte Belastung des Anspruchsgegners ausgeschlossen werden kann.[285] Maßgeblich ist insofern jedoch nicht die Rechtsverletzung des Nutzers,[286] sondern die des Access Providers.[287] Angesichts der umstrittenen Voraussetzungen für die Begründung einer mittelbaren Störerhaftung von Access Providern, kann von einer klaren Rechtslage jedoch keine Rede sein. Dementsprechend würde sich eine Auskunftspflicht des Access Providers aufgrund einer mittelbaren Störerhaftung zumindest nicht im einstweiligen Verfügungsverfahren durchsetzen lassen.[288]

VII. Zusammenfassung

Ein Auskunftsanspruch gegen Access Provider nach § 101a UrhG ist lediglich unter sehr restriktiven Voraussetzungen gegeben. Zunächst ist festzuhalten, dass sich der Anwendungsbereich des § 101a UrhG nicht nur auf Rechtsverletzungen des § 16 UrhG, sondern in analoger Anwendung auch auf Rechtsverletzungen des § 19a UrhG erstreckt. Allerdings verlangt der Tatbestand des § 101a UrhG eine Rechtsverletzung des Auskunftspflichtigen, mithin des Access Providers. Dieser begeht durch die bloße Bereitstellung der infrastrukturellen Voraussetzungen für Urheberrechtsverletzungen jedoch zumindest keine unmittelbare Urheberrechtsverletzung. Aufgrund seines adäquat-kausalen Beitrags zu solchen Rechtsverletzungen kommt

---

[285] OLG Hamburg, Urt. v. 28.4.2005 – 5 U 156/04, MMR 2005, 453, 456 =CR 2005, 512; Wandtke/Bullinger/Bohne, § 101a URhG, Rn. 12.

[286] So offenbar LG Köln, Urt. v. 28.7.2004 – 28 O 301/04, ZUM 2005, 236, 239.

[287] OLG Frankfurt a.M., Urt. v. 25.1.2005 – 11 U 51/05, MMR 2005, 241, 243= CR 2005, 285.

[288] So auch OLG München, Urt. v. 24.3.2005 – 6 U 4696/04 n.v; vgl. auch Heise News, Meldung v. 21.12.2004: Juristischer Rückschlag für Musikindustrie im Kampf gegen Raubkopierer, http://www.heise.de/newsticker/meldung/54486.

allerdings eine Haftung als mittelbarer Störer in Betracht. Diese setzt voraus, dass der Access Provider eine ihm obliegende Prüfpflicht verletzt hat. Unter solchen Prüfpflichten sind – in Anlehnung an die deliktische Zurechnung von mittelbaren Rechtsgutsverletzungen – spezifische Verkehrssicherungspflichten zu verstehen. Diesen genügt der Access Provider bereits dann, wenn er seine Nutzer, z.B. in seinen Allgemeinen Geschäftsbedingungen, zur Beachtung fremder Urheberrechte ermahnt. Allenfalls bei schwerwiegenden Schutzrechtsverletzungen erscheint es gerechtfertigt, den Access Providern – in Anlehnung an § 13a TKV – zu verpflichten, konkrete Nutzer abzumahnen oder im Falle wiederholter Verstöße zu sperren. Kommt der Access Provider auch diesen Pflichten nach, ist eine mittelbare Störerhaftung ausgeschlossen.

Sofern ausnahmsweise eine mittelbare Störereigenschaft des Access Providers bejaht werden kann, ist diese auch geeignet eine Passivlegitimation im Rahmen des § 101a UrhG zu begründen, da der Kreis der Passivlegitimierten – entgegen einer weit verbreiteten Auffassung – nicht auf den unmittelbaren Urheberrechtsverletzer beschränkt ist. Ferner muss die Auskunftserteilung auch der Verhältnismäßigkeitsklausel des § 101a Abs. 1 UrhG genügen, nach der eine umfassende Interessenabwägung nach dem Vorbild des öffentlich-rechtlichen Verhältnismäßigkeitsgrundsatzes stattfindet. Der Erforderlichkeit der Auskunftserteilung des Access Providers steht nicht entgegen, dass der Rechteinhaber die gewünschte Auskunft unter Umständen auch über den Umweg der strafprozessualen Akteneinsicht bekommen könnte. Allerdings erweist sich die Inanspruchnahme des Access Providers nur dann als verhältnismäßig, wenn dieser aufgrund „schwerwiegender Rechtsverletzungen“ seiner Nutzer in Anspruch genommen wird, nicht jedoch bereits bei einzelnen Schutzrechtsverletzungen. Darüber hinaus wird sich dieser Anspruch regelmäßig nicht im einstweiligen Verfügungsverfahren durchsetzen lassen, da sich eine mittelbare Störerhaftung des Access Providers zumindest nicht als offensichtliche Rechtsverletzung i.S.d. § 101a Abs. 3 UrhG darstellen wird. Zudem soll an dieser Stelle bereits darauf hingewiesen werden, dass ein Auskunftsanspruch nach § 101a UrhG ausgeschlossen ist, wenn sich der Access Provider auf ein gesetzliches Haftungsprivileg nach dem TDG/MdStV berufen kann, oder einer Auskunftserteilung datenschutzrechtliche Bestimmungen oder das Fernmeldegeheimnis entgegenstehen. Auf diese Fragen wird im Laufe der Bearbeitung jedoch noch ausführlich eingegangen.[289]

[289] Dazu ausführlich im vierten und fünften Teil der Bearbeitung.

B. Allgemeiner urheberrechtlicher Auskunftsanspruch

Teilweise wird in der Literatur die Auffassung vertreten, dass sich auch aus dem allgemeinen urheberrechtlichen Auskunftsanspruch aus § 97 UrhG i.V.m. § 242 BGB eine Auskunftspflicht von Providern über die Identität deren Nutzer ableiten lasse.[290] Bedeutung erlangt diese Ansicht vor allem dann, wenn man – entgegen der hier vertretenen Auffassung – entweder die Eröffnung des Anwendungsbereichs des § 101a UrhG auf unkörperliche Vervielfältigungsstücke im Onlinebereich ablehnt, oder aber den mittelbaren Störer nicht als Verletzer i.S.d. § 101a UrhG ansieht und dem Access Provider somit die Passivlegitimation abspricht.

Ein Rückgriff auf § 242 BGB soll nach dieser Auffassung trotz der spezialgesetzlichen Regelung des § 101a UrhG auch dogmatisch unbedenklich sein, weil § 101a Abs. 5 UrhG ausdrücklich klarstelle, dass weitergehende Ansprüche auf Auskunft durch § 101a UrhG unberührt bleiben.[291] Keine Bedenken sieht diese Auffassung ferner in dem Umstand, dass nach § 242 BGB regelmäßig nur Auskünfte zur Vorbereitung eines gegen den Auskunftspflichtigen selbst gerichteten Hauptanspruchs gewährt werden,[292] hier jedoch Auskunft über Dritte begehrt wird, nämlich über der Identität der Kunden des Access Providers. Dies sei deshalb unschädlich, weil auch in der Rechtsprechung zum ergänzenden wettbewerbsrechtlichen Leistungsschutz mittlerweile anerkannt sei, dass sich aus § 242 BGB ein Anspruch auf Drittauskunft ergeben könne. Diese Rechtsprechung soll sich angesichts der Vergleichbarkeit wettbewerbsrechtlicher und immaterialgüterrechtlicher Ansprüche auch auf das Urheberrecht übertragen lassen. Daher soll sich auch aus dem allgemeinen urheberrechtlichen Auskunftsanspruch aus § 97 UrhG i.V.m. § 242 BGB eine Drittauskunftspflicht des Access Providers ergeben können.[293]

Diese Auffassung soll im Folgenden einer kritischen Würdigung unterzogen werden. Dabei ist zunächst zu klären, ob für den Fall, dass der Access Provider als mittelbarer Störer qualifiziert werden kann, auch die Voraus-

---

[290] v.Olenhusen/Crone, WRP 2002, 164, 167; Spindler/Dorschel, CR 2005, 38, 40 f. stellen zwar auf § 242 BGB i.V.m. der verletzten Norm ab, lassen allerdings offen, ob es sich bei dieser Norm um § 1 UWG a.F. bzw. § 3 UWG n.F. oder aber um § 97 UrhG handelt; zur Anwendbarkeit des allg. wettbewerbsrechtlichen Auskunftsanspruch auf Urheberrechtsverletzungen, siehe unten, 2.Teil C.

[291] v.Olenhusen/Crone, WRP 2002, 164, 167; Spindler/Dorschel, CR 2005, 38, 40 f.

[292] BGH, Urt. v. 19.3.1987 – I ZR 98/85, GRUR 1987, 647, 648 – Briefentwürfe; Teplitzky, Kap. 38, Rn. 5.

[293] Vgl. Spindler/Dorschel, CR 2005, 38, 40.

setzungen des allgemeinen urheberrechtlichen Auskunftsanspruchs gegeben sind. Sollte dies zu bejahen sein, stellt sich die Frage, ob sich die wettbewerbsrechtliche Rechtsprechung zur Drittauskunft tatsächlich auf das Urheberrecht übertragen lässt und sich also auch auf der Rechtsfolgenseite des allgemeinen urheberrechtlichen Auskunftsanspruchs eine Verpflichtung zur Auskunftserteilung über Dritte ergeben kann.

I. Voraussetzungen des allgemeinen Auskunftsanspruchs

Der allgemeine urheberrechtliche Auskunftsanspruch wird in erweiternder Auslegung der §§ 259, 260 BGB auf § 242 BGB i.V.m. § 97 UrhG gestützt und ist mittlerweile gewohnheitsrechtlich anerkannt.[294] Auf der Tatbestandsebene setzt dieser zunächst das Bestehen einer rechtlichen Beziehung zwischen Anspruchssteller und Anspruchsgegner voraus.[295] Da die Rechtsprechung das früher postulierte Vorsatzerfordernis auf der Seite des Verletzers mittlerweile aufgegeben hat, kann ein Rechtsverhältnis in diesem Sinne nunmehr auch durch eine mittelbare Störerhaftung begründet werden.[296] Somit besteht ein solches gesetzliches Schuldverhältnis auch dann, wenn der Access Provider lediglich als mittelbarer Störer für die Urheberrechtsverletzungen seiner Nutzer haftet.

Seine Rechtfertigung findet der allgemeine Auskunftsanspruch darin, dass es dem Verletzten nach Treu und Glauben möglich sein muss, Auskunft über Tatsachen zu erlangen, über deren Bestehen dieser in entschuldbarer Weise im Ungewissen ist und sich die notwendigen Auskünfte auch nicht auf zumutbare Weise selbst beschaffen kann, wohingegen der Verletzer unschwer und in zumutbarer Weise diese Auskünfte geben könnte.[297] Dies soll dann der Fall sein, wenn eine umfassende einzelfallbezogene Interessenabwägung ergibt, dass das Auskunftsinteresse des Anspruchsstellers das Geheimhaltungsinteresse des Anspruchsgegners überwiegt.[298] Da sich die Kriterien dieser Interessenabwägung in der Rechtsprechung weitestgehend der Verhältnismäßigkeitsprüfung im Rahmen der spezialgesetzlichen Aus-

[294] BGH, Urt. v. 7.12.1979 – I ZR 157/77, GRUR 1980, 227, 232 – Monumenta Germaniae Historica; BGH, Urt. v. 24.3.1994 – I ZR 42/93, GRUR 1994, 630, 632 – Cartier-Armreif.
[295] Teplitzky, Kap. 38, Rn. 6.
[296] BGH, Urt. v. 17.5.2001 – I ZR 291/98, GRUR 2001, 841, 843 – Entfernung der Herstellernummer II; anders noch BGH, Urt. v. 24.3.1994 – I ZR 42/93, GRUR 1994, 630, 632 – Cartier-Armreif m. abl. Anm. Jakobs, GRUR 1994, 634, 635; Teplitzky, Kap. 38, Rn. 6.
[297] BGH, Urt. v. 7.12.1979 – I ZR 157/77, GRUR 1980, 227, 233 – Monumenta Germaniae Historica; ausführlich hierzu, Wiume, S. 40 ff.
[298] BGH, Urt. v. 24.3.1994 – I ZR 42/93, GRUR 1994, 630, 632 – Cartier-Armreif; BGH, Urt. v. 17.5.2001 – I ZR 291/98, GRUR 2001, 841, 843 – Entfernung der Herstellernummer II.

kunftsansprüche des PrPG angeglichen haben,[299] kann in dieser Hinsicht also auf die Ausführungen zur Verhältnismäßigkeitsprüfung im Rahmen des § 101a Abs. 1 UrhG verwiesen werden.[300] Demnach liegen also zumindest dann die Tatbestandsvoraussetzungen des allgemeinen Auskunftsanspruchs aus § 97 UrhG i.V.m. § 242 BGB vor, wenn der Access Provider als mittelbarer Störer für schwerwiegende Urheberrechtsverletzungen seiner Nutzer auf Auskunft in Anspruch genommen wird.

II. Drittauskunft als Rechtsfolge des § 242 BGB

Zu klären ist daher, ob der allgemeine urheberrechtliche Auskunftsanspruch auf der Rechtsfolgenseite einen Anspruch auf Auskunft über Dritte gewährt. Für den allgemeinen wettbewerbsrechtlichen Auskunftsanspruch infolge der Verletzung ergänzender Leistungsschutzrechte wird dies allgemein angenommen, wenn weitere Verletzungshandlungen durch einen Dritten drohen und der Verletzte ohne die Auskunft des Verletzers keine rechtliche Möglichkeit hat, gegen diesen vorzugehen.[301] Da dies durchaus auch der Interessenlage des in seinen Verwertungsrechten verletzten Rechteinhabers entspricht, liegt auf den ersten Blick tatsächlich eine Übertragung der wettbewerbsrechtlichen Rechtsprechungsgrundsätze auf das Urheberrecht nahe.

1. Übertragbarkeit der wettbewerbsrechtlichen Drittauskunftspflicht auf das Urheberrecht

Bei genauerer Betrachtung stößt jedoch nicht nur die Adaption wettbewerbsrechtlicher Rechtsprechungsgrundsätze auf das Urheberrecht, sondern bereits die Ableitung von Drittauskunftsansprüchen aus dem wettbewerbsrechtlichen Auskunftsanspruch selbst auf dogmatische Bedenken. So könnte die Übertragung des wettbewerbsrechtlichen Drittauskunftsanspruch aus § 242 BGB auf das Urheberrecht bereits daran scheitern, dass es auch in den Fällen der Verletzung wettbewerbsrechtlicher Leistungsschutzrechte angezeigt gewesen wäre, die Drittauskunftspflicht des Verletzers nicht aus § 242 BGB, sondern aus einer analogen Anwendung der spezialgesetzlichen Drittauskunftsansprüche des PrPG abzuleiten. Zur Beurteilung dieser Frage bedarf es zunächst einer näheren Betrachtung der dogmatischen Grundlage ergänzender Leistungsschutzrechte.

---

[299] Teplitzky, Kap. 38, Rn. 9 m.w.N.
[300] Siehe oben, 2. Teil A. V.
[301] BGH, Urt. v. 24.3.1994 – I ZR 42/93, GRUR 1994, 630, 633 – Cartier-Armreif.

a) Dogmatische Einordnung ergänzender Leistungsschutzrechte

Im Gegensatz zu den Immaterialgüterrechten begründen wettbewerbsrechtliche Leistungen in der Regel keine Sonderausschließlichkeitsrechte. Außerhalb des Immaterialgüterrechts ist daher grundsätzlich jeder dazu berechtigt, die Leistungen eines anderen nachzuahmen. Dies beruht auf der Erkenntnis, dass jede Leistung der Gegenwart auf dem Erbe der Vergangenheit aufbaut. Aus diesem Grund kann auch von einem Mitbewerber nicht verlangt werden, den bereits erreichten Entwicklungsstand sowie eine günstige Marktnachfrage unberücksichtigt zu lassen.[302] Dieser Grundsatz gilt allerdings nicht uneingeschränkt. Er findet dort eine Grenze, wo besondere – über die bloße Nachahmung hinausgehende – Umstände die Nachahmung unlauter erscheinen lassen.[303] Hierzu haben sich in der Rechtsprechung im Laufe der Zeit einige Fallgruppen herausgebildet, die unter dem Begriff des „ergänzenden wettbewerbsrechtlichen Leistungsschutzes“ zusammengefasst und unter die Generalklausel des § 1 UWG a.F. subsumiert wurden. Nachdem jedoch vor allem in der Literatur die Forderung nach einer gesetzlichen Regelung dieser Fallgruppen erhoben wurde,[304] hat der Gesetzgeber im Rahmen der Novelle des Wettbewerbsrechts im Jahre 2004 die Grundlinien dieser Rechtsprechung in § 4 Nr. 9 UWG kodifiziert.

b) Rechtsprechung zur wettbewerbsrechtlichen Drittauskunftspflicht

Dass ergänzende Leistungsschutzrechte vielfach auch als *„Quasi-Immaterialgüterrechte“* bezeichnet werden,[305] rührt nicht zuletzt daher, dass in der Rechtsprechung bei Verletzungen ergänzender Leistungsschutzrechte weitestgehend auf die immaterialgüterrechtliche Judikatur zurückgegriffen wird.[306] So verwunderte es auch nicht, dass der BGH in seiner Cartier-Armreif-Entscheidung[307] aus dem Jahre 1994 die Grundsätze der Regelungen des PrPG rekurriert hat, um einen in seinem ergänzenden

---

[302] BGH, Urt. v. 4.11.1966 – Ib ZR 77/65, GRUR 1967, 315, 317 – skai-cubana; Hefermehl/Köhler/Bornkamm, § 4, Rn. 9.4; Harte/Henning/Sambuc, Einl. F, Rn. 207.

[303] BGH, Urt. v.16.1.1997 – I ZR 9/95, BGHZ 134, 250, 267 = GRUR 1997, 459 – CB-Infobank; BGH, Urt. v. 10.12.1998 – I ZR 100/96, BGHZ 140, 183, 189 = GRUR 1999, 325 – Elektronische Pressearchive; BGH, Urt. v. 21.2.2002 – I ZR 265/99, GRUR 2002, 629, 631 = WRP 2002, 1058 – Blendsegel.

[304] Köhler, WRP 1999, 1075, 1080 ff.; Fezer, WRP 2001, 989, 1004 ff.; Schricker/Henning-Bodewig WRP 2001, 1367, 1381.

[305] So Jacobs, Anm. zu BGH, Urt. v. 24.3.1994 – I ZR 42/93 – Cartier-Armreif, GRUR 1994, 634, 635.

[306] Vgl. Ulrich, Anm. zu BGH, a.a.O., Cartier-Armreif, ZIP 1994, 979, 979.

[307] BGH, Urt. v. 24.3.1994 – I ZR 42/93, GRUR 1994, 630 – Cartier-Armreif.

Leistungsschutzrecht Verletzten einen Anspruch auf Drittauskunft einzuräumen. Dieser Entscheidung lag der Sachverhalt zugrunde, dass auf einer Schmuckmesse von einem Aussteller ein aufwendig verarbeiteter goldener Armreif ausgestellt wurde. Dieser Armreif verletzte den Anspruchssteller in seinem „ergänzenden wettbewerbsrechtlichen Leistungsschutzrecht", da das ausgestellte Exemplar eine wettbewerbliche Eigenart besaß und eine sog. sklavische Nachahmung der vom Anspruchssteller vertriebenen Armreife darstellte. Der Verletzte begehrte daraufhin vom Verletzer Auskunft über den Namen und die Anschrift seines Lieferanten.

Im Rahmen dieser Entscheidung musste der BGH zunächst klären, ob einer Drittauskunftspflicht im Wettbewerbsrecht nicht die spezialgesetzlichen Auskunftsansprüche des PrPG entgegenstehen, da diese Drittauskunftspflichten eben nur für Verletzungen von Immaterialgüterrechten vorsehen, nicht aber für Verletzungen wettbewerbsrechtlich geschützter Leistungsrechte. Zutreffend verneinte der Senat einen solchen abschließenden Charakter des PrPG unter Verweis auf die Gesetzesbegründung. Aus dieser geht hervor, dass die Aufnahme eines Drittauskunftsanspruchs in das Wettbewerbsrecht nicht etwa deshalb unterblieben ist, weil der Gesetzgeber einen solchen Anspruch bei Verletzungen wettbewerbsrechtlicher Leistungsschutzrechte nicht gewähren wollte, sondern weil die Statuierung eines Auskunftsanspruchs bei Produktpiraterie in ein Gesetz, das – mit Ausnahme der ergänzenden Leistungsschutzrechte – grundsätzlich vom Prinzip der Nachahmungsfreiheit ausgeht, als systemwidrig betrachtet wurde.[308]

Nachdem der BGH festgestellt hatte, dass die Auskunftsansprüche des PrPG keinen abschließenden Regelungscharakter haben, mithin einer Drittauskunftspflicht bei der Verletzung wettbewerbsrechtlicher Rechtspositionen nicht entgegenstehen, galt es zu klären, auf welche dogmatische Grundlage ein solcher Auskunftsanspruch gestützt werden könnte. Der BGH zog zunächst eine analoge Anwendung des § 101a UrhG in Betracht, verneinte jedoch das Vorliegen einer planwidrigen Regelungslücke des PrPG, da man die fragliche Auskunftspflicht auch über eine Fortentwicklung des Rechtsgedankens von Treu und Glauben gem. § 242 BGB i.V.m. § 1 UWG a.F. konstruieren könne, also über den allgemeinen wettbewerbsrechtlichen Auskunftsanspruch.[309]

[308] BGH, a.a.O., 633; Amtl. Begründung zum PrPG, BT-Drs 11/4792, S. 19 f.
[309] BGH, a.a.O., 632.

c) Kritik an der Ableitung von Drittauskunftspflichten aus § 242 BGB

Diese dogmatische Bindung der wettbewerbsrechtlichen Drittauskunft an § 242 BGB ist vor allem im Schrifttum zu Recht auf Kritik gestoßen.[310] Denn bereits der Umstand, dass der BGH in dieser Entscheidung erstmals überhaupt einen Drittauskunftsanspruch im Wettbewerbsrecht konstruiert hat, spricht dafür, dass zumindest bis zu diesem Zeitpunkt sehr wohl von einer Regelungslücke auszugehen war. Aufgrund der Vergleichbarkeit zwischen Verletzungen von Immaterialgüterrechten und ergänzenden wettbewerbsrechtlichen Leistungsschutzrechten, die zudem bereits der Gesetzgeber des PrPG betont hat,[311] hätte es daher näher gelegen, diese Regelungslücke durch eine analoge Anwendung des § 101a UrhG zu schließen.[312] Dafür spricht zudem, dass der auf § 242 BGB gestützte Auskunftsanspruch bereits deshalb in seinem Regelungsbereich hinter dem des § 101a UrhG zurücksteht, da sich dieser selbst bei offensichtlichen Rechtsverletzungen regelmäßig nicht im einstweiligen Verfügungsverfahren durchsetzen lässt.[313] Sofern man also von der Vergleichbarkeit von Urheberrechten und ergänzenden Leistungsschutzrechten ausgeht, wäre bereits im Rahmen der Cartier-Armreif-Entscheidung eine Analogie zu § 101a UrhG der bessere Weg gewesen.

Ein wesentlicher Punkt, der gegen die Fortführung des von der Rechtsprechung eingeschlagen Weges spricht, ist in der aktuellen Diskussion bisher unberücksichtigt geblieben. Dies betrifft die Tatsache, dass der Gesetzgeber die Fallgruppen des ergänzenden Leistungsschutzes im Zuge der Novellierung des Wettbewerbsrechts im Jahre 2004 in § 4 Nr. 9 UWG positivrechtlich geregelt hat. Hat der historische Gesetzgeber des PrPG noch argumentiert, dass die Statuierung einer Drittauskunft bei Verletzung wettbewerbsrechtlicher Leistungsschutzrechte systemwidrig sei, weil auch das Wettbewerbsrecht einen solchen Verletzungstatbestand nicht vorsehe,[314] kann dies vor dem Hintergrund des neu geschaffen § 4 Nr. 9 UWG nicht mehr aufrecht erhalten werden. Vielmehr ist davon auszugehen, dass der historische Gesetzgeber die Drittauskunftsansprüche des PrPG sicherlich auch auf das Wettbewerbsrecht ausgedehnt hätte, wenn bereits damals ein positivrechtlicher Verletzungstatbestand für ergänzende Leistungsschutzrechte im UWG existiert hätte. Somit liegt zumindest seit der Einführung

[310] Asendorf, in: FS Traub, S. 21 ff.; Wiume, S. 62 ff.
[311] Vgl. amtl. Begründung zum PrPG, BT-Drs. 11/4792, S. 19.
[312] Asendorf, in: FS Traub, S. 31; Wiume, S. 63 f.
[313] Schricker/Wild, § 101a UrhG, RN. 5; Wiume, S. 64 f.
[314] Amtl. Begründung zum PrPG, BT-Drs. 11/4792, S. 20.

des § 4 Nr. 9 UWG eine nachträgliche Planwidrigkeit des PrPG in Bezug auf eine wettbewerbsrechtliche Drittauskunft vor, die zudem aufgrund der Vergleichbarkeit der Verletzungshandlungen eine analoge Anwendung der Auskunftsansprüche des PrPG auf das Wettbewerbsrecht gebietet.

d) Zwischenergebnis

Die wettbewerbsrechtliche Rechtsprechung zur Drittauskunft lässt sich schon aus dem Grund nicht auf den allgemeinen urheberrechtlichen Auskunftsanspruch aus § 97 UrhG i.V.m. § 242 BGB übertragen, weil bereits die dogmatische Grundlage des von der Rechtsprechung gewährten wettbewerbsrechtlichen Drittauskunftsanspruchs fragwürdig ist. Spätestens seit der gesetzlichen Normierung der ergänzenden wettbewerbsrechtlichen Leistungsschutzrechte in § 4 Nr. 9 UWG ist auch in diesen Fällen vielmehr eine analoge Anwendung des § 101a UrhG angezeigt.

2. Spezialität des § 101a UrhG

Sofern man mit der Rechtsprechung dennoch von der Möglichkeit einer auf § 242 BGB gestützten Drittauskunft im Wettbewerbsrecht ausgeht, stellt sich die Frage, ob § 101a UrhG nicht insoweit eine Sperrwirkung entfaltet, dass zumindest innerhalb des Urheberrechts ein Rückgriff auf Treu und Glauben zur Begründung von Drittauskunftspflichten ausgeschlossen ist. Von den Befürworten einer urheberrechtlichen Drittauskunftspflicht aus § 97 UrhG i.V.m § 242 BGB wird in dieser Hinsicht vorgetragen, dass ein Rückgriff auf § 242 BGB in dogmatischer Hinsicht unbedenklich sei, da eine Drittauskunftspflicht aus § 242 BGB als weitergehender Anspruch i.S.d. § 101a Abs. 5 UrhG anzusehen sei, der von den tatbestandlichen Einschränkungen des § 101a UrhG unberührt bleibe.[315]

Dem kann nicht gefolgt werden. Die Bestimmung des § 101a Abs. 5 UrhG dürfte vielmehr als deklaratorischer Hinweis auf bestehende Auskunftspflichten im Zweipersonenverhältnis zu verstehen sein. Dafür spricht ein Blick in die Gesetzesmaterialien zu § 101a Abs. 5 UrhG. Darin findet sich die Ausführung, dass *„sonstige Ansprüche auf Auskunft, etwa zur Vorbereitung von Schadensersatz- und Beseitigungsansprüchen, wie sie durch die Rechtsprechung entwickelt wurden und zum Teil schon gewohnheitsrechtlich anerkannt sind“*, von den Sondervorschriften des PrPG nicht berührt werden sollen.[316] Misst man diesem Passus die Bedeutung bei, dass

[315] v.Olenhusen/Crone, WRP 2002, 164, 167; Spindler/Dorschel, CR 2005, 38, 40 f.
[316] Amtl. Begründung zum PrPG, BT-Drs. 11/4792, S. 32.

§ 101a Abs. 5 UrhG lediglich die Auskunftsansprüche unberührt lässt, die bereits zum Zeitpunkt des Erlasses des PrPG existierten, kann sich diese Regelung schon aus diesem Grund nicht auf urheberrechtliche Drittauskunftsansprüche erstrecken. Interpretiert man die Gesetzesmaterialien hingegen in dem Sinne, dass von § 101a Abs. 5 UrhG auch die zukünftige Entwicklung der Drittauskunft durch richterrechtliche Rechtsfortbildung erfasst werden soll, kann auch dies im Ergebnis nicht zu einer urheberrechtlichen Drittauskunft auf Grundlage des § 242 BGB führen. Denn auch die richterrechtliche Rechtsfortbildung durch § 242 BGB findet ihre Grenze in den allgemeinen Grundsätzen der Dogmatik und der Gewaltenteilung.[317] Der zivilrechtlichen Dogmatik würde es jedoch diametral entgegenstehen, wenn man in Fällen, in denen die spezialgesetzlichen Voraussetzungen des § 101a UrhG nicht erfüllt sind, dieselbe Rechtsfolge durch einen Rückgriff auf Treu und Glauben gem. § 242 BGB herbeiführen könnte. Deshalb ist davon auszugehen, dass § 101a UrhG zumindest insoweit eine Sperrwirkung entfaltet, dass ein urheberrechtlicher Drittauskunftsanspruch nur unter den Voraussetzungen des § 101a UrhG gewährt wird.

III. Ergebnis

Aus dem allgemeinen urheberrechtlichen Auskunftsanspruch aus § 97 UrhG i.V.m. § 242 BGB lässt sich kein Anspruch auf Drittauskunft ableiten. Eine Parallele zum wettbewerbsrechtlichen Anspruch auf Drittauskunft geht bereits deshalb fehl, weil auch in diesen Fällen vielmehr eine analoge Anwendung des § 101a UrhG als ein Rückgriff auf Treu und Glauben angezeigt ist. Im Urheberrecht ist ein Rückgriff auf § 242 BGB bei Drittauskunftsansprüchen zudem bereits durch die spezialgesetzliche Regelung des § 101a UrhG die Grundlage entzogen.

C. Allgemeiner wettbewerbsrechtlicher Auskunftsanspruch

Geht man hingegen – entgegen der hier vertretenen Auffassung – davon aus, dass sich zumindest aus dem allgemeinen wettbewerbsrechtlichen Auskunftsanspruch aus § 1 UWG a.F. bzw. § 3 UWG n.F. i.V.m. § 242 BGB eine Drittauskunftspflicht ableiten lässt, ist fraglich, ob der Access Provider in den Fällen, in denen er ausnahmsweise als mittelbarer Störer i.S.d. § 97 UrhG qualifiziert werden kann, nicht zugleich auch eine wett-

[317] MünchKommBGB/Roth, § 242, Rn. 27.

bewerbsrechtliche Verletzungshandlung begeht, aufgrund derer er sodann auf Drittauskunft in Anspruch genommen werden kann.[318]

Der Konstruktion einer solchen Auskunftspflicht über den Umweg des Wettbewerbsrechts steht allerdings entgegen, dass die Geltendmachung wettbewerbsrechtlicher Ansprüche ausgeschlossen ist, sofern die fragliche Nutzerhandlung bereits als Verletzung eines Sonderschutzrechts qualifiziert werden kann.[319] Demzufolge scheidet ein wettbewerbsrechtlicher Anspruch gegen Access Provider aus, wenn dieser bereits als mittelbarer Störer im Sinne des Urheberrechts für die Rechtsverletzungen seiner Nutzer haftet. Ist eine Handlung hingegen urheberrechtlich unbedenklich, was beim Access Providing der Regelfall sein dürfte, kommen wettbewerbsrechtliche Ansprüche aus ergänzendem Leistungsschutz nur bei Hinzutreten *„besonderer Umstände"* in Betracht, die das Verhalten als unlauter erscheinen lassen.[320] Solche Umstände werden in der Person des Access Providers jedoch bereits deshalb nicht erfüllt sein, weil sich Access Providing als sozialadäquates Verhalten darstellt.[321] Darüber hinaus ist es auch in dogmatischer Hinsicht sehr fraglich, einen wettbewerbsrechtlichen Auskunftsanspruch zur Vorbereitung der Verfolgung von Urheberrechtsverletzungen heranzuziehen.[322]

D. Drittauskunft als Störungsbeseitigung i.S.d. § 97 UrhG

Weiterhin könnte man im Falle der mittelbaren Störerhaftung des Access Providers in Erwägung ziehen, den Rechteinhabern einen Auskunftsanspruch als besondere Form des Beseitigungsanspruchs aus § 97 UrhG zuzusprechen.[323] Auch dies wird vor allem dann virulent, wenn man – entgegen der hier vertretenen Auffassung – dem mittelbaren Störer die Passivlegitimation im Rahmen des § 101a UrhG abspricht. Für eine solche Auskunftspflicht lässt sich wiederum eine Parallele zum Wettbewerbsrecht ziehen. Denn auch in der wettbewerbsrechtlichen Rechtsprechung zur Ver-

---

[318] In diesem Sinne interpretiert Stadler, Haftung, S. 200 die Ausführungen von Spindler/Dorschel, CR 2005, 38, 40.

[319] BGH, Urt. v. 17.6.1992 – I ZR 182/90, GRUR 1992, 697, 699 – Alf m.w.N.; BGH, Urt. v. 10.10.1993 – I ZR 147/89, GRUR 1993, 34, 37 – Bedienungsanweisung; Baumbach/Hefermehl/Köhler, § 4, Rn. 9.6 f.;

[320] BGH, Urt. v. 17.7.2004 – I ZR 259/00, MMR 2003, 719, 722 m.w.N. = GRUR 2003, 985 – Paperboy; Harte/Henning/Sambuc, Einl F., Rn. 213; Baumbach/Hefermehl/Köhler, § 4, Rn. 9.7.

[321] Vgl. Volkmann, Störer im Internet, S. 160.

[322] Stadler, Haftung, S. 201.

[323] Ausführlich zur Auskunftspflicht als besondere Form des Beseitigungsanspruchs, Oppermann, S. 63 ff.

letzung von Vertriebsbindungssystemen wurde dem Verletzten in analoger Anwendung des § 1004 BGB ein Drittauskunftsanspruch als besondere Form des Störungsbeseitigungsanspruchs zugestanden.[324]

Wiederum sprechen jedoch dogmatische Bedenken gegen eine über den Beseitigungsanspruch konstruierte Auskunftspflicht. Denn nach zutreffender Auffassung ergibt sich aus der notwendigen Abgrenzung zwischen dem auf Wiederherstellung eines Zustandes gerichteten deliktischen Schadensersatzanspruch und dem verschuldensunabhängigen Beseitigungsanspruch, dass der Störer im Rahmen des Beseitigungsanspruchs nur den *actus contrarius* seiner störenden Handlung schuldet.[325] Dies ist deshalb notwendig, damit die Voraussetzungen der auf Naturalrestitution gerichteten verschuldensabhängigen Schadensersatzhaftung nicht durch das verschuldensunabhängige Störerhaftungsrecht unterlaufen werden.[326] Mit dem Beseitigungsanspruch kann der Access Provider somit allenfalls verpflichtet werden seine störende Tätigkeit, also die Zugangsgewährung, zu unterlassen, nicht jedoch auch Auskunft über den unmittelbaren Störer zu erteilen. Des weiteren würde durch die Auskunftserteilung auch nicht unmittelbar die Störung beseitigt, sondern lediglich in das Belieben des Verletzten gestellt. Der Access Provider würde daher allenfalls Beihilfe zur Beseitigung der unmittelbaren Störquelle leisten.[327] Zudem spricht auch die Gesetzessystematik des UrhG gegen die Konstruktion einer Drittauskunftspflicht aus § 97 UrhG. Ein solcher Rückgriff auf § 97 UrhG dürfte vor dem Hintergrund des § 101a UrhG bereits unter Spezialitätsgesichtspunkten ausgeschlossen sein. Festzuhalten bleibt somit, dass der Access Provider nach § 97 UrhG lediglich auf Unterlassen seiner störenden Tätigkeit, nicht aber auch auf Auskunft über Dritte in Anspruch genommen werden kann.

E. Ergebnis

Als Anspruchsgrundlage der Rechteinhaber für eine verletzungsabhängige Auskunftspflicht des Access Providers kommt allein § 101a UrhG in Betracht. Dieser setzt jedoch voraus, dass der Access Provider zumindest als mittelbarer Störer für die Rechtsverletzungen seiner Nutzer haftet. Da eine solche mittelbare Störerhaftung des Access Providers jedoch kaum be-

[324] OLG Köln, Urt. v. 7.11.1969 – 6 U 26/69, GRUR 1970, 525, 526 – Offenbarungseid; OLG Köln, Urt. v. 21.11.1969 – 6 U 33/69, GRUR 1970, 526, 527 – finesse.
[325] Bauer, AcP 160 (1961), 465, 489; MünchKommBGB/Medicus, § 1004, Rn. 73 ; Oppermann, S. 68 f.
[326] MünchKommBGB/Medicus, § 1004, Rn. 71.
[327] Oppermann, S. 70; Wiume, S. 78.

gründbar erscheint, stellt auch dieser Anspruch kein geeignetes Mittel zur Bekämpfung der Urheberrechtspiraterie im Internet dar.

3. Teil: Verletzungsunabhängige Auskunfts- und Vorlageansprüche

Gerade vor dem Hintergrund, dass sich verletzungsabhängige Auskunftsansprüche gegen Access Provider nur schwerlich begründen lassen, stellt sich die Frage, ob eine materiell-rechtliche Anspruchsgrundlage existiert, nach der ein Access Provider auch verletzungsunabhängig auf Auskunft über die Identität seiner Nutzer in Anspruch genommen werden kann. Sollte dies nicht der Fall sein, ist zu klären, ob den Rechteinhabern zumindest ein Einsichts- oder Vorlageanspruch hinsichtlich der Datenträger zur Seite steht, auf denen die Log-Dateien gespeichert sind. Weiterhin ist zu untersuchen, ob zivilprozessuale Möglichkeiten bestehen, mittels derer die begehrten Auskünfte eingeholt werden könnten.

A. Anwendbarkeit des § 101a UrhG auf den Nichtverletzer

Der historische Gesetzgeber des PrPG schrieb dem Auskunftsanspruch aus § 101a UrhG auf die Fahne, dass dieser der Aufdeckung gezielter und massenhafter Schutzrechtsverletzungen dienen möge.[328] Vor diesem Hintergrund wurde im vorherigen Kapitel ausgeführt, dass diesem Schutzzweck im digitalen Zeitalter nur dadurch Rechnung getragen werden kann, wenn sich der Anwendungsbereich des § 101a UrhG auch auf Verletzungshandlungen der §§ 16, 19a UrhG durch digitale Vervielfältigungsstücke erstreckt. Weiterhin wurde aufgrund der Tatsache, dass der Gesetzgeber den § 101a UrhG verschuldensunabhängig ausgestalten wollte, die Erstreckung der Passivlegitimation auf den mittelbaren Störer für erforderlich gehalten. Da eine mittelbare Störerhaftung jedoch nur unter sehr restriktiven Voraussetzungen gegeben ist, kann der Access Provider zumeist nicht gem. § 101a UrhG auf Auskunft über die Identität seiner Nutzer in Anspruch genommen werden.

Hinsichtlich dieses Rechtsverfolgungsdefizits stellt sich nun die Frage, ob es der Schutzzweck des § 101a UrhG gebietet, auch denjenigen mit einer Auskunftspflicht zu belegen, der selbst zwar keine Verletzungshandlung begeht, aber – wie der Access Provider – in rein tatsächlicher Hinsicht in der Lage ist, über Verletzungshandlungen Dritter Auskunft zu geben.

[328] Amtl. Begründung zum PrPG, BT-Drs. 11/4792, S. 32.

I. Analoge Anwendung des § 101a UrhG

Angesichts des klaren Wortlauts des § 101a UrhG, der explizit eine Verletzungshandlung des Anspruchsgegners voraussetzt, kommt auch in dieser Hinsicht allenfalls eine analoge Anwendung in Betracht. Erforderlich sind daher eine planwidrige Regelungslücke sowie eine vergleichbare Interessenlage zwischen der Auskunftspflicht des Verletzers und des Nichtverletzers.

1. Planwidrige Regelungslücke

Zunächst lässt sich eine Regelungslücke des UrhG hinsichtlich einer Drittauskunftspflicht von Nichtverletzern durchaus bejahen. Denn Auskunftspflichten nach dem UrhG werden nicht verletzungsunabhängig gewährt, sondern setzen zumindest ein durch die Störerhaftung des Anspruchsgegners begründetes Schuldverhältnis voraus. An der Planwidrigkeit dieser Regelungslücke kann jedoch gezweifelt werden. Denn Auskunftsansprüche, die unabhängig von einer Verletzungshandlung eine Auskunftspflicht vorsehen, sind dem deutschen Zivilrecht sowohl in materieller als auch in prozessualer Hinsicht grundsätzlich fremd.[329] Sofern dennoch verletzungsunabhängig ein Auskunftsanspruch gewährt wird, wie z.B. in §§ 13, 13a UKlaG[330], handelt es sich um Ausnahmetatbestände, denen kein allgemeiner Programmsatz entnommen werden kann. Dies bedeutet auch für das Urheberrecht, dass dieses nicht bereits deshalb planwidrig unvollständig ist, weil es keine verletzungsunabhängige Auskunftspflicht vorsieht.

Weiterhin spricht auch die Gesetzgebungsgeschichte der bisherigen Urheberrechtsnovellierungen gegen eine solche Analogie. So wurde seitens des Forums der Rechteinhaber bereits im Rahmen des Ersten Korbes der Urheberrechtsreform die Integration eines selbständigen Unterlassungs- sowie Auskunftsanspruchs gegen Provider gefordert, der unabhängig von einer Rechtsverletzung bestehen sollte.[331] Der vorgeschlagene Auskunftsanspruch lautete:

> ***„§ 101b Anspruch auf Auskunft gegen Vermittler***
>
> *„Vermittler(…) können vom Verletzten auf unverzügliche Auskunft über den Dritten in Anspruch genommen werden, der den*

[329] Spindler/Dorschel, CR 2005, 38, 44 m.w.N.
[330] Dazu sogleich, 3. Teil C.
[331] Stellungnahme des „Forums der Rechteinhaber“ vom Oktober 2002, S. 8, abrufbar unter: http://www.urheberrecht.org/topic/Info-RiLi/st/Forum-RegEntw.pdf.

Dienst für die Verletzung eines nach diesem Gesetz geschützten Rechts genutzt hat. § 101a Absätze 2 bis 5 gelten entsprechend."

Der Gesetzgeber hat von der Umsetzung dieser Forderung jedoch abgesehen, da er angesichts der knappen Umsetzungsfrist der sog. InfoSoc-RL[332] zunächst nur die zwingenden Vorgaben dieser Richtlinie umsetzen wollte, zu denen Auskunftsansprüche jedoch nicht zählten.[333] Diese und weitere streitige Fragen sollten erst abschließend erörtert und sodann zum Gegenstand eines weiteren Gesetzgebungsverfahrens gemacht werden.[334] Der Erörterungsprozess zur Umsetzung dieses Zweiten Korbes wurde seitens des Bundesjustizministeriums (BMJ) im Herbst 2003 durch einen Fragenkatalog angestoßen. In diesem wurde explizit die Frage aufgeworfen, ob es der Einführung eines Auskunftsanspruchs gegen Provider bedarf.[335] Trotz der daraufhin von den Rechteinhabern erneut erhobenen Forderungen nach der Statuierung eines verletzungsunabhängigen Auskunftstatbestandes,[336] ist ein solcher wiederum nicht in den Referentenentwurf aufgenommen worden. Wie aus der Zusammenfassung der vom BMJ im Vorfeld des Referentenentwurfs eingesetzten Arbeitsgruppe "Internet" hervorgeht, dürfte dies darauf zurückzuführen sein, dass einer Auskunftspflicht des Providers beachtliche rechtliche Probleme – insbesondere aus dem Datenschutz- und dem TK-Recht – entgegenstehen.[337] Auch wenn die Einführung eines solchen Anspruchs mittlerweile in den Referentenentwurf zur Umsetzung der Enforcement-RL[338] Einzug gehalten hat,[339] ändert dies nichts an der Tatsache, dass sich der Gesetzgeber bereits intensiv mit der Statuierung eines

---

[332] Richtlinie 2001/29/EG.

[333] Begr. zum Regierungsentwurf v. 16.8.2002, BR-Drs. 684/02, S. 33; Sieber/Höfinger, MMR 2004, 575, 577.

[334] Begr. zum Regierungsentwurf v. 16.8.2002, BR-Drs. 684/02, S. 31.

[335] Vgl. Frage D des Fragenkataloges des BMJ „Fragen zur weiteren Reform des Urheberrechts in der Informationsgesellschaft", abrufbar, unter: http://www.urheberrecht.org/topic/Korb-2/bmj/Fragebogen.pdf.

[336] Vgl. Stellungnahme des „Forums der Rechteinhaber" zum Referentenentwurf eines Zweiten Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft vom 15. November 2004, S. 9, abrufbar unter: http://www.urheberrecht.org/topic/Korb-2/st/refentw/RefEntw-Korb2.pdf.

[337] So Kaufmann/Köcher, Anm. zu LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, MMR 2005, 61, 61 in Bezug auf die Ergebnisse der vom Bundesjustizministerium im Vorfeld des Referentenentwurfs v. 27.9.2004 eingesetzten Arbeitsgruppe „Internet", S.9, abrufbar unter: http://www.bmj.bund.de/media/archive/707.pdf.

[338] Richtlinie 2004/48/EG.

[339] Vgl. § 101 UrhG des Referentenentwurfs für ein Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums v. 3.1.2006, abrufbar unter: http://www.urheberrecht.org.; ausführlich dazu, unten 7. Teil C.

verletzungsunabhängigen Auskunftsanspruchs auseinandergesetzt und diesen bisher bewusst nicht in das Urheberrecht integriert hat. Somit ist auch eine Planwidrigkeit des § 101a UrhG hinsichtlich der Nichterstreckung des Kreises der Passivlegitimierten auf den Nichtverletzer zu verneinen.[340]

2. Vergleichbare Interessenlage

Darüber hinaus würde es auch an einer vergleichbaren Interessenlage zwischen der gesetzlichen Auskunftspflicht des Verletzers und dem nicht geregelten Fall der Auskunftspflicht des Nichtverletzers fehlen. So ist zwar zumindest auf der Seite der Rechteinhaber von einer vergleichbaren Interessenlage auszugehen, da diese – wie im normalen Anwendungsfall des § 101a UrhG – zur Durchsetzung ihrer Rechte auf die Auskunft des Dritten angewiesen sind. Auf der Seite der Auskunftspflichtigen stellt sich die Situation indes anders dar. Denn während dem auskunftspflichtigen Verletzer deshalb eine Auskunftspflicht auferlegt wird, weil er durch seine Verletzungshandlung ein Schuldverhältnis mit dem Verletzten begründet hat, steht der Nichtverletzer mit dem Rechteinhaber in keinerlei rechtlicher Beziehung, aus der eine solche Auskunftspflicht erwachsen könnte.[341] Auch der Access Provider ist regelmäßig lediglich ein unbeteiligter Dritter, der die begehrte Auskunft faktisch zwar geben könnte, nicht jedoch weil er Teil einer Verletzerkette ist, sondern weil er die Identität des Verletzers im Rahmen seiner erlaubten Geschäftstätigkeit erlangt hat. Dies unterscheidet ihn erheblich vom originären Auskunftspflichtigen des § 101a UrhG.[342]

Weiterhin lassen sich gegen eine Gleichbehandlung von Verletzer und Nichtverletzer in Bezug auf Auskunftspflichten nach § 101a UrhG auch verfassungsrechtliche Bedenken in Bezug auf Art. 12 GG erheben. So wird zwar im Regelfall des § 101a UrhG die für einen Eingriff in das Grundrecht der Berufsfreiheit notwendige berufsregelnde Tendenz zu verneinen sein, weil es sich in diesen Fällen um einen zivilrechtlichen Interessenausgleich zwischen dem Verletzer und dem Verletzten handelt.[343] Dies soll sich nach einer Auffassung jedoch anders darstellen, wenn der Access Provider zur Auskunft über Tatsachen herangezogen wird, die dieser lediglich Rahmen seiner Tätigkeit als Telekommunikationsdienstleister erlangt hat.[344] Hinsichtlich der Rechtfertigung eines solchen Eingriffs sei zu be-

[340] So auch Kitz, ZUM 2005, 298, 300.
[341] Kitz, GRUR 2003, 1014, 1017.
[342] Kitz, GRUR 2003, 1014, 1017.
[343] Vgl. Manssen, in: v. Mangoldt/Klein/Starck, Art. 12. Rn. 73.
[344] Spindler/Dorschel, CR 2005, 38, 44.

zweifeln, dass dieser durch vernünftige Gründe des Allgemeinwohls getragen werde,[345] da eine Auskunftspflicht des Providers nach § 101a UrhG weniger auf das Allgemeinwohl als vielmehr auf die Kompensation wirtschaftlicher Einbußen Dritter gerichtet sei.[346] Zudem kann an der Verhältnismäßigkeit einer verletzungsunabhängigen Auskunftspflicht auf Grundlage des § 101a UrhG auch deshalb gezweifelt werden, weil § 101a UrhG – im Gegensatz zu §§ 13, 13a UKlagG – keine Entschädigungsregelung vorsieht. Da es jedoch nicht angemessen erscheint, dem Nichtverletzer die Kosten der Auskunftserteilung aufzubürden, spricht auch dieser Umstand gegen eine vergleichbare Interessenlage zwischen der Auskunftspflicht des Verletzers und des Nichtverletzers.

3. Zwischenergebnis

Hinsichtlich einer analogen Anwendung des § 101a UrhG auf den Nichtverletzer mangelt es sowohl an einer planwidrigen Regelungslücke als auch an einer vergleichbaren Interessenlage.

II. Richtlinienkonforme Auslegung des § 101a UrhG

Weiterhin wird vertreten, dass sich der Anwendungsbereich des § 101a UrhG zumindest in richtlinienkonformer Auslegung auf den Nichtverletzer erstrecken müsse.[347] Dies soll sich aus Art. 8 Abs. 3 InfoSoc-RL ergeben. Danach haben die Mitgliedstaaten dafür Sorge zu tragen, dass „*die Rechteinhaber gerichtliche Anordnung gegen Vermittler beantragen können, deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandter Schutzrechte genutzt werden*."

Die Voraussetzungen für eine richtlinienkonforme Auslegung dürften indes nicht vorliegen. Diese ist nämlich kein unbeschränkt nutzbares Instrument, mit dem im Konfliktfall die Richtlinienbestimmungen an die Stelle innerstaatlicher Regelungen gesetzt werden können. Vielmehr ist diese ihrerseits durch die nationalen Auslegungsregeln beschränkt.[348] Daraus folgt, dass einer nach Wortlaut und Sinn eindeutigen nationalen Vorschrift auch

---

[345] Vgl. BVerfG, Urt. 11.6.1958 – 1 BvR 596/56, BVerfGE 7, 377, 405 – Apotheken-Urteil; Manssen, in: v. Mangoldt/Klein/Starck, Art. 12. Rn. 139.

[346] Spindler/Dorschel, CR 2005, 38, 44.

[347] So Czychowski, MMR 2004, 514, 518; ähnlich Nordemann/Dustmann, CR 2004, 380, 386, die aus Art. 8 Abs. 3 InfoSoc-RL offenbar eine Passivlegitimation des Providers als Verletzer konstruieren wollen.

[348] EuGH, Urt. v. 10.04.1984 – Rs. 79/83 , EuGHE 1984, 1921, 1942 f. = NJW 1984, 2021; ausführlich hierzu, Leonard, S. 118 m.w.N.

im Wege einer richtlinienkonformen Auslegung kein entgegengesetzter Sinn verliehen werden darf. Auch diese kann sich daher lediglich in den vom Wortlaut der nationalen Norm gezogenen Grenzen bewegen.[349] Der Wortsinn des § 101a UrhG ist jedoch bereits überschritten, wenn man § 101a UrhG auf den Nichtverletzer anwendet, obwohl dieser explizit eine Verletzungshandlung des Anspruchsgegners voraussetzt.

Lässt man hingegen eine richtlinienkonforme Auslegung nicht bereits am Wortlaut des § 101a UrhG scheitern, ist weiterhin zu fordern, dass Art. 8 Abs. 3 InfoSoc-RL auch tatsächlich eine Verpflichtung zur Einführung eines verletzungsunabhängigen Auskunftsanspruchs entnommen werden kann. Dieser spricht jedoch lediglich von *„gerichtlichen Anordnungen“*, nicht aber auch von Auskunftsansprüchen. Angesichts des Terminus der gerichtlichen Anordnung ist bereits fraglich, ob es sich bei Art. 8 Abs. 3 InfoSoc-RL überhaupt um eine materiell-rechtliche Regelung handelt. Vielmehr könnte diese auch in dem Sinne interpretiert werden, dass dadurch bereits bestehende materielle Ansprüche einschränkend an das Erfordernis einer gerichtlichen Anordnung geknüpft werden.[350]

Selbst wenn man vom materiell-rechtlichen Charakter dieser Norm ausginge, ließe sich aus dieser Regelung lediglich ableiten, dass rechtliche Maßnahmen gegen Access Provider möglich sein müssen, nicht jedoch auch, wie diese auszugestalten sind. Nicht zu beanstanden ist daher auch die Auffassung des deutschen Gesetzgebers. Dieser sah in Art. 8 Abs. 3 InfoSoc-RL lediglich die verbindliche Vorgabe, dass sich Sperrungs- und Beseitigungsansprüche auch gegen Provider durchsetzen lassen müssen.[351] Vor dem Hintergrund, dass diese – aus § 97 UrhG resultierenden – Ansprüche nach § 8 Abs. 2 S. 2 TDG explizit von den Haftungsfreistellungen der Provider nach den §§ 9-11 TDG ausgenommen sind, wurde hinsichtlich des Art. 8 Abs. 3 InfoSoc-RL kein Umsetzungsbedarf gesehen.[352] Daran mag man bemängeln, dass Sperrungs- und Beseitigungsansprüche nach § 97 UrhG eine Verletzungshandlung des Anspruchsgegners voraussetzen, wohingegen Art. 8 Abs. 3 InfoSoc-RL verletzungsunabhängig ausgestaltet

[349] EuGH, Urt. v. 14.7.1994 – Rs. C-91, JZ 1995, 149, 150 – Faccini Dori; Heß, Anmerkung zu EuGH, Urt. v. 14.7.1994 – Rs. C-91 – Faccini Dori, JZ 1995, 150, 151.

[350] Ausführlich unten 4. Teil E. IV. 5.

[351] BT-Drs 15/38, S. 39; anders der österreichische Gesetzgeber, der auf Grundlage des Art. 8 Abs. 3 InfoSoc-RL mit dem § 87b Abs. 3 UrhG einen Auskunftsanspruch schuf, der sich auch gegen Access Provider richtet, vgl. Haidinger, S. 44; Wiebe, MR 2005, Beilage zu Heft 4, S. 6 ff.

[352] BT-Drs. 15/38, S. 39.

ist.[353] Keinesfalls ist der Gesetzgeber jedoch hinsichtlich der Nichteinführung eines verletzungsunabhängigen Auskunftsanspruchs hinter dem zwingenden Unsetzungserfordernis des Art. 8 Abs. 3 InfoSoc-RL zurückgeblieben. Für diese Auffassung spricht auch ein Umkehrschluss *(arg. e contrario)* zur Enforcement-RL. Denn der Einführung des in Art. 8 Enforcement-RL vorgesehenen Auskunftsanspruchs[354] hätte es freilich nicht bedurft, wenn sich dieser bereits zwingend aus Art. 8 Abs. 3 InfoSoc-RL ergäbe.

Schließlich wäre eine dahingehende richtlinienkonforme Auslegung selbst dann zu versagen, wenn Art. 8 Abs. 3 InfoSoc-RL tatsächlich zwingend die Einführung eines solchen Auskunftsanspruchs vorsähe. Dies liefe nämlich auf eine – im Wege der richtlinienkonformen Auslegung vorgenommene – horizontale Anwendung einer Richtlinie hinaus. Eine solche wird vom EuGH jedoch in ständiger Rechtsprechung abgelehnt.[355] Aus diesem Grund ergibt sich auch nach dem Ablauf der Umsetzungsfrist zur Enforcement-RL[356] keine Verpflichtung, den Anwendungsbereich des § 101a UrhG in richtlinienkonformer Auslegung auf den Nichtverletzer zu erstrecken.[357] Der Tatbestand des § 101a UrhG lässt sich also weder durch eine Analogie noch im Wege einer richtlinienkonformen Auslegung auf den Nichtverletzer erstrecken. Der Access Provider kann somit nicht auf Auskunft nach § 101a UrhG in Anspruch genommen werden, wenn ihm keine Urheberrechtsverletzung zur Last gelegt werden kann.

B. Drittauskunft aus §§ 13, 13a UKlaG

Aufgrund der Tatsache, dass den Rechteinhabern gegen die Nutzer des Access Providers, die widerrechtlich in deren Verwertungsrechte eingreifen, Unterlassungsansprüche nach § 97 UrhG zustehen, könnte man daran denken, den Rechteinhabern einen Auskunftsanspruch nach §§ 13, 13a des Unterlassungsklagengesetzes (UKlaG) zuzugestehen. Diese Regelungen gewähren dem Inhaber eines Unterlassungsanspruchs einen verschuldens- und verletzungsunabhängigen Anspruch auf Drittauskunft. Dieser Anspruch richtet sich auch gegen Betreiber von Post-, Telekommunikations-, Tele- oder Mediendiensten, mithin auch gegen Access Provider.[358] Diese

[353] Vgl. die Gegenäußerung des Bundesrates, BT-Drs. 15/38, S. 35, Nr. 1 d), der sich explizit für einen selbständigen Unterlassungsanspruch gegen Provider ausspricht.
[354] Ausführlich dazu, siehe unten 7. Teil B.
[355] EuGH, Urt. v. 26.2.1986 – Rs. 152/84, EuGHE 1986, 723, 733 = NJW 1986, 2178 – Marshall; Spindler/Dorschel, CR 2005, 38, 47 m.w.N.
[356] Die Umsetzungsfrist ist am 29.04.2006 abgelaufen.
[357] A.A. Schricker/Wild, § 101a UrhG, Rn. 8.
[358] Näher zur rechtlichen Einordnung des Access Providers, siehe unten 4. Teil D.

müssen unter den Voraussetzungen der §§ 13, 13a UKlaG Auskunft über die Identität ihrer Nutzer erteilen. Dadurch soll der Gefahr vorgebeugt werden, dass der Unterlassungspflichtige deshalb nicht in Anspruch genommen werden kann, weil er sich hinter einer Anschrift oder Internetkennung verbirgt.[359] Eben diese Problematik liegt auch der Geltendmachung von urheberrechtlichen Ansprüchen gegen die Nutzer der Access Provider zugrunde. Zudem billigt § 13 Abs. 4 UKlaG dem als Nichtverletzer in Anspruch genommenen einen Ausgleichsanspruch gegen den Anspruchsgegner zu, so dass dieser Anspruch, anders als im Falle einer analogen Anwendung des § 101a UrhG auf den Nichtverletzer,[360] auch im Hinblick auf die Kostenlast nicht als unverhältnismäßig angesehen werden kann.

Allerdings unterliegen Auskunftspflichten nach §§ 13, 13a UKlaG einigen Einschränkungen. So wird ein Auskunftsanspruch nach § 13 Abs. 1 UKlaG nur zur Durchsetzung von Ansprüchen nach §§ 1, 2 UKlaG gewährt, mithin bei Verstößen gegen Verbraucherschutzvorschriften. Die Durchsetzung von urheberrechtlichen Unterlassungsansprüchen gem. § 97 UrhG steht jedoch nicht im Interesse der Verbraucher, sondern im geschäftlichen Interesse der Rechteinhaber. Daher sind diese Ansprüche eindeutig nicht verbraucherschützender Natur. Zudem wären die Rechteinhaber auch nicht aktivlegitimiert i.S.d. § 13 Abs. 1 UKlaG, da sie weder Wettbewerbsverbände noch anspruchberechtigte Stellen i.S.d. § 3 Abs. 1 Nr. 1 u. 3 UKlaG sind.

Auch auf § 13a UKlaG kann das Begehren der Rechteinhaber nicht gestützt werden. Zwar unterliegt dieser Anspruch bezüglich des Kreises der Aktivlegimitierten nicht den Einschränkungen des § 13 Abs. 1 UKlaG, jedoch ist auch § 13a UKlaG nur bei Verstößen gegen verbraucherschützende Vorschriften anwendbar, nämlich nur dann, wenn es um die Durchsetzung von Unterlassungsansprüchen bezüglich der Lieferung unbestellter Sachen, der Erbringung unbestellter sonstiger Leistungen sowie der Zusendung oder sonstiger Übermittlung unverlangter Werbung geht. Aufgrund des auf den Verbraucherschutz abstellenden Schutzzwecks der §§ 13, 13a UKlaG würde es daher auch hinsichtlich einer analogen Anwendung dieser Vorschriften auf Rechtsverletzungen des § 97 UrhG zumindest an einer planwidrigen Regelungslücke fehlen. Darüber hinaus würde ein solcher Anspruch auch daran scheitern, dass die §§ 13a S. 1 i.V.m. 13 Abs. 2 S. 1 UKlaG nur eine Verpflichtung zur Herausgabe von

[359] Palandt/Bassenge, § 13 UKLaG, Rn. 1.
[360] Siehe oben 3. Teil A.

Bestandsdaten i.S.v. §§ 5 TDDSG, 95 TKG vorsehen,[361] bei der Auskunftserteilung über (dynamische) IP-Adressen jedoch auch Verbindungsdaten i.S.d. §§ 6 TDDSG, 96 TKG betroffen sind.[362]

C. Besichtigungs- und Einsichtsanspruch gem. §§ 809, 810 BGB

Steht den Rechteinhabern somit auch kein verletzungsunabhängiger Auskunftsanspruch gegenüber den Access Providern zur Seite, so stellt sich die Frage, ob deren Begehren auf Auskunft über die Identität der Nutzer nicht durch die materiellrechtlichen Beseitigungs- und Einsichtsansprüche des allgemeinen Zivilrechts gem. §§ 809, 810 BGB Rechnung getragen werden könnte. Diese Vorschriften gewähren unter bestimmten Voraussetzungen einen eigenen schuldrechtlichen Anspruch auf Besichtigung einer Sache sowie Einsicht in eine Urkunde. Sinn und Zweck dieser Vorschriften ist es, den vermeintlich Geschädigten in die Lage zu versetzen, dass dieser beurteilen kann, ob er einen durchsetzbaren Anspruch hat.[363] Vor diesem Hintergrund ist zu klären, ob sich danach nicht auch ein Anspruch auf Begutachtung der Datenträger des Access Providers ergeben kann, auf denen die Log-Dateien gespeichert sind, so dass zumindest über diesen Umweg die Identität von Rechtsverletzern zur weiteren Rechtsverfolgung offen gelegt werden könnte.

I. Besichtigungsanspruch nach § 809 BGB

Der Anwendungsbereich des Besichtigungsanspruchs des § 809 BGB ist nicht auf die Geltendmachung von Ansprüchen nach dem BGB beschränkt. Dieser erstreckt sich auch auf das Urheberrecht, sofern mit einer gewissen Wahrscheinlichkeit von einer Urheberrechtsverletzung ausgegangen werden kann.[364] Voraussetzung für einen Besichtigungsanspruch nach § 809 BGB ist zunächst, dass der Anspruchssteller gegen den Besitzer der Sache einen Anspruch in Ansehung der Sache hat oder sich Gewissheit verschaffen will, ob ihm ein solcher Anspruch zusteht. Maßgeblich ist insoweit der Sachbegriff des § 90 BGB.[365] Da von diesem auch Speichermedien erfasst

[361] Vgl. Palandt/Bassenge, § 13 UKlaG, Rn. 6.
[362] Kitz, GRUR 2003, 1014, 1016; ausführlich zur datenschutzrechtlichen Einordnung der Auskunftserteilung, siehe unten 5. Teil A. IV.
[363] Palandt/Sprau, § 809 Rn. 1.
[364] BGH, Urt. v. 22.5.2002 – I ZR 45/01, JurPC Web-Dok. 282/2002, 2. Leistsatz = GRUR 2001, 1046 – Faxkarte; MünchKommBGB/Hüffer, § 809, Rn. 13.
[365] Palandt/Sprau, § 809 Rn. 3.; Staudinger/Marburger, § 809, Rn. 1.

werden,[366] sind auch die Datenträger, auf denen die Log-Dateien der Access Provider gespeichert sind, Sachen i.S.d. § 809 BGB.[367] In Ansehung der Sache besteht der Anspruch dann, wenn dieser in einer rechtlichen Beziehung zur Sache steht. Dazu muss er entweder selbst Gegenstand des Anspruchs sein, oder aber zumindest von dem Bestand der Sache oder ihrer Beschaffenheit abhängen.[368] Dies ist hinsichtlich der fraglichen Speichermedien jedoch nicht der Fall. Die Speichermedien der Access Provider sind weder selbst Gegenstand der aus der Urheberrechtsverletzung der Nutzer resultierenden Ansprüche, noch hängen die Ansprüche der Rechteinhaber vom Bestand der gespeicherten Daten ab.[369] Deutlich wird dies durch eine Gegenprobe. Denn der Anspruch gegen die Nutzer aus § 97 UrhG entfällt nicht dadurch, dass die Daten auf dem Speichermedium des Access Providers gelöscht werden. Darüber hinaus scheitert der Anspruch aus § 809 BGB auch deshalb, weil dieser lediglich ein materiell-rechtlicher Hilfsanspruch ist, der zur Durchsetzung eines Hauptanspruchs gegen den Besitzer der Sache dient.[370] Vorliegend geht es jedoch nicht um die Durchsetzung eines gegen den Access Provider gerichteten Anspruchs, sondern um einen Anspruch gegen dessen Nutzer. Somit ergibt sich aus § 809 BGB kein Anspruch der Rechteinhaber auf Einsicht in die Log-Dateien der Access Provider.

II. Urkundeneinsicht nach § 810 BGB

Im Gegensatz zum Besichtigungsanspruch aus § 809 BGB setzt der Anspruch auf Urkundeneinsicht nach § 810 BGB keinen Hauptanspruch gegen den Anspruchsgegner voraus.[371] So reicht es aus, wenn der Anspruchsteller darlegen kann, dass er ein rechtliches Interesse an der Einsicht einer Urkunde hat und einer der Vorlagetatbestände des § 810 BGB erfüllt ist. Voraussetzung für eine solche Verpflichtung des Access Providers ist jedoch zunächst, dass es sich bei den auf den Datenträgern gespeicherten Log-Dateien um Urkunden i.S.d. § 810 BGB handelt.

---

[366] BGH, Urt. v. 4.11.1987 – VIII ZR 314/86, BGHZ 102, 135, 144; Palandt/Heinrichs, § 90, Rn. 2.
[367] Vgl. Staudinger/Marburger, § 809, Rn. 3, 9.
[368] MünchKommBGB/Hüffer, § 809, Rn. 4.; Staudinger/Marburger, § 809, Rn. 5.
[369] Kitz, GRUR 2003, 1014, 1016.
[370] Oppermann, S. 91; Wiume, S. 94.
[371] Staudinger/Marburger, § 810, Rn. 1; Kitz, GRUR 2003, 1014, 1016.

1. Urkundenqualität der Log-Dateien

Der Urkundenbegriff des § 810 BGB bestimmt sich – aufgrund des Zusammenspiels dieser Vorschriften mit den §§ 422, 429 ZPO – nach den Grundsätzen des Zivilprozessrechts.[372] Danach sind Urkunden durch Niederschrift verkörperte Gedankenerklärungen.[373] In Bezug auf die Log-Dateien mangelt es jedoch bereits am Merkmal der Schriftlichkeit, wenn die Daten lediglich in elektronischer Form auf dem jeweiligen Datenträger vorliegen.[374] Aber auch wenn diese Daten ausnahmsweise in ausgedruckter Form vorlägen, würden diese den Urkundenbegriff nicht erfüllen. So werden zwar teilweise auch Ausdrucke von elektronischen Dokumenten auf Papier als Urkunde angesehen. Dies gilt allerdings nur unter der Voraussetzung, dass auch diesen Ausdrucken ein menschlicher Gedanke entnommen werden kann.[375] Das ist jedoch nicht der Fall, wenn die Ausdrucke, wie im Falle der Log-Dateien, lediglich die Tatsache der Eingabe und Programmierung von Daten belegen.[376] Somit handelt es sich bei den Log-Dateien, gleichgültig in welcher Form diese vorliegen, nicht um unmittelbar vom Tatbestand des § 810 BGB erfasste Urkunden.

2. Analoge Anwendung des § 810 BGB auf elektronische Dokumente

Teilweise wird in Bezug auf elektronisch verkörperte Dokumente wie den Log-Dateien für eine analoge Anwendung des § 810 BGB plädiert. Begründet wird dies damit, dass der technische Fortschritt dazu führe, dass schriftliche Gedankenerklärungen immer häufiger durch technische Aufzeichnungen ersetzt werden und diese auch in ihrem Beweiswert in der Regel den herkömmlichen Niederschriften ebenbürtig sind.[377]

Bedeutung erlangt diese Auffassung vor allem dann, wenn man auch die mit § 810 BGB korrespondierte zivilprozessuale Verpflichtung zur Urkundenvorlage gem. § 422 ZPO in analoger Anwendung auf elektronische Dokumente erstreckt. Eine solche Auslegung des § 422 ZPO läge vor allem im Interesse des vermeintlich Vorlageberechtigten, da in diesem Fall nicht die Regeln über den Augenscheinsbeweis, sondern auch die für den Vorlageberechtigten günstigeren Regeln über den Urkundenbeweis an-

[372] MünchKommBGB/Hüffer, § 810, Rn. 3.
[373] Hartmann, in: Baumbach/Lauterbach/Albers/Hartmann, Übers. § 415 ZPO, Rn. 5.
[374] Vgl. Stein/Jonas/Berger, ZPO, vor § 371, Rn. 6; Geis, CR 1993, 653, 654.
[375] Hartmann, in: Baumbach/Lauterbach/Albers/Hartmann, vor § 415 ZPO, Rn. 7; Stein/Jonas/Berger, vor § 371 ZPO, Rn. 7; differenzierend Geis, CR 1993, 653, 654.
[376] Vgl. Zöller/Geimer, vor § 415, Rn. 2.
[377] Staudinger/Marburger, § 810, Rn. 8.

wendbar wären.[378] Allerdings hat sich der Gesetzgeber mittlerweile explizit gegen eine analoge Anwendung der §§ 810 BGB, 422 ZPO auf sämtliche elektronische Dokumente ausgesprochen. So wurde mit dem Erlass des § 371 Abs. 1 S. 2 ZPO[379] zunächst klargestellt, dass elektronische Dokumente nicht den Regeln über den Urkundenbeweis, sondern ausschließlich denen über den Augenscheinsbeweis unterworfen sind.[380] Zwar wurde diese Vorschrift durch die später eingefügte Regelung des § 371a ZPO[381] teilweise relativiert, da nach dieser Regelung zumindest auch elektronische Dokumente, die mit einer elektronischen Signatur versehen sind, dem Urkundenbeweis zugänglich sind. Auch daraus lässt im Wege eines Umkehrschlusses jedoch ableiten, dass die Regelungen über Urkunden bzw. den Urkundenbeweis auf andere elektronische Dokumente – wie den Log-Dateien der Access Provider – gerade keine Anwendung finden sollen. Eine analoge Anwendung des § 810 BGB scheitert daher zumindest deshalb, weil sich die Nichterstreckung des § 810 BGB auf elektronische Dokumente nicht als planwidrig erweist.

3. Anforderungen an ein Einsichtsrecht nach § 810 BGB

Folgt man hingegen der Auffassung, nach der sich der Anwendungsbereich des § 810 BGB in analoger Anwendung auch auf elektronische Dokumente erstreckt, so müssen zur Begründung eines Einsichtsrechts in die Datenträger des Access Providers auch die übrigen Voraussetzungen des § 810 BGB gegeben sein. So verlangt der Tatbestand weiterhin, dass der verletzte Rechteinhaber ein rechtliches Interesse an der Vorlage hat. Ein solches Interesse liegt vor, wenn der Anspruchssteller die Kenntnis der Urkunde für die Erhaltung, Förderung oder Verteidigung seiner rechtlich geschützten Sphäre benötigt.[382] Dies ist auch in Bezug auf die Log-Dateien zu bejahen, da diese von den Rechteinhabern für die Rechtsverfolgung von Urheberrechtsverletzern und damit zur Verteidigung ihrer rechtlich geschützten Sphäre benötigt werden. Weiterhin setzt eine Vorlagepflicht nach § 810 BGB voraus, dass die Voraussetzungen einer der drei Vorlagetatbestände erfüllt sind. So muss die Urkunde entweder im Interesse des Anspruchsstellers errichtet worden sein (1.Fall), ein zwischen ihm und einem anderen

[378] Ahrens, in: FS Geimer, S. 3.
[379] Eingefügt durch das Formvorschriftenanpassungsgesetz v. 13.7.2001, BGBl. 2001 I, S. 1542.
[380] BT-Drs. 14/4987, S. 23.
[381] Eingefügt durch das Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz – JKomG) v. 22.3.2005 mit Wirkung zum 1.4.2005, BGBl. I, S. 837.
[382] MünchKommBGB/Hüffer, § 810, Rn. 10; Staudinger/Marburger, § 809, Rn. 10.

bestehendes Rechtsverhältnis beurkunden (2.Fall) oder Verhandlungen über ein Rechtsgeschäft enthalten (3.Fall).

In Betracht kommen allenfalls die ersten beiden Fälle. Eine Errichtung im Interesse des Anspruchsstellers setzt voraus, dass die Urkunde zumindest auch dazu errichtet wurde, dem Anspruchssteller als Beweismittel zu dienen, seine rechtlichen Beziehungen zu fördern, zu sichern, zu klären oder auf ihren Bestand einzuwirken.[383] Die Log-Dateien sind jedoch allenfalls dazu bestimmt, das Rechtsverhältnis zwischen Access Provider und Nutzer zu dokumentieren, nicht aber um den Rechteinhabern die Rechtsverfolgung zu erleichtern.[384] Auch die Voraussetzungen des zweiten Falles des § 810 BGB sind nicht erfüllt. Zwar ist insofern nicht der Zweck der Errichtung maßgeblich, sondern nur, ob in der Urkunde ein Rechtsverhältnis zwischen dem Anspruchssteller und einem Dritten niedergelegt ist.[385] Allerdings ist auch dies in Bezug auf die Log-Dateien zu verneinen. Diese lassen allenfalls Rückschlüsse darauf zu, dass ein Nutzer mit einer bestimmten IP-Adresse zu einem bestimmten Zeitpunkt online war. Da sie jedoch nicht den Inhalt der Kommunikationsinhalte enthalten, wird auch nicht die Verletzungshandlung als solche dokumentiert, durch die das deliktische Rechtsverhältnis zwischen dem Rechteinhaber und dem Nutzer begründet wird. Somit ist auch keiner der Vorlagetatbestände des § 810 BGB erfüllt.

III. Ergebnis

Die Rechteinhaber haben weder einen Anspruch auf Vorlage der Datenträger gem. § 809 BGB noch können sie gem. § 810 BGB Einsicht in die auf diesen Datenträgern gespeicherten Log-Dateien verlangen.

D. Zivilprozessuale Auskunfts- und Vorlagepflichten

Neben den materiell-rechtlichen Auskunfts- und Vorlageansprüchen sieht auch das Prozessrecht Anspruchsgrundlagen vor, mit denen Rechteinhaber die für die Geltendmachung ihrer Ansprüche notwendigen Auskünfte von Dritten erlangen können.

I. Prozessuale Vorlegungsansprüche

Nach §§ 428, 429 ZPO kann ein Dritter im Klagewege zur Vorlegung von Urkunden genötigt werden. Eine solche Klage ist jedoch nach §§ 429, 422

[383] MünchKommBGB/Hüffer, § 810, Rn. 5; Wiume, S. 99.
[384] Kitz, GRUR 2003, 1014, 1016.
[385] MünchKommBGB/Hüffer, § 810, Rn. 7; Schilken, Jura 1988, 525, 529.

ZPO nur dann erfolgreich, wenn auch eine Vorlagepflicht hinsichtlich der Urkunde nach bürgerlich-rechtlichen Vorschriften besteht, also insbesondere nach § 810 BGB.[386] Da dessen Voraussetzungen jedoch – wie soeben ausgeführt – nicht vorliegen, scheidet auch eine Vorlagepflicht nach §§ 428, 429 ZPO aus.

In Betracht kommt jedoch eine Vorlagepflicht nach § 142 ZPO. Diese ist nicht auf Urkunden beschränkt, sondern erstreckt sich auch auf sonstige Unterlagen. Von letzteren werden insbesondere auch Datenträger erfasst.[387] Der Dritte kann die Vorlage gem. § 142 Abs. 2 ZPO nur dann verweigern, wenn ihm dies nicht zumutbar ist oder er zur Zeugnisverweigerung gem. §§ 383 ff. ZPO berechtigt ist. Letztlich wird jedoch auch diese Vorschrift dem Begehren der Rechteinhaber nicht gerecht. Denn § 142 ZPO setzt einen bereits anhängigen Prozess gegen den Dritten voraus, vorliegend also gegen den Nutzer des Providers.[388] Dazu muss der Rechteinhaber jedoch zunächst einen den Anforderungen des § 253 ZPO genügenden Klagantrag stellen. Ein solcher erfordert nach § 253 Abs. 2 Nr. 1 ZPO zwar nicht zwingend eine namentliche Bezeichnung der zu verklagenden Person. Jedoch muss sich die Identität der Partei zumindest durch Auslegung ermitteln lassen.[389] Dies ist jedoch nicht möglich, wenn dem Rechteinhaber lediglich die IP-Adresse des (anonymen) Nutzers bekannt ist. Eine Vorlagepflicht des Access Providers aus § 142 ZPO wird daher regelmäßig daran scheitern, dass der Rechteinhaber keinen – den Anforderungen des § 253 ZPO genügenden – Klageantrag stellen kann.[390] Eine Anordnung nach § 142 ZPO ist daher immer nur dann möglich, wenn dem Rechteinhaber eine Klageerhebung möglich ist, weil er die Identität des Rechtsverletzers auf einem anderen Wege erlangt hat. In diesen Fällen könnte der vermeintliche Anspruch sodann im Wege einer Anordnung nach § 142 ZPO mittels der Log-Dateien verifiziert werden. Diese Fälle dürften jedoch eine zu vernachlässigende Randerscheinung darstellen.[391]

II. Zeugenvernehmung des Access Providers

Aufgrund der fehlenden Kenntnis von der Identität des Rechtsverletzers wird zumeist auch die Möglichkeit einer Zeugenvernehmung des Access

[386] Musielak/Huber, § 422, Rn. 1.
[387] Hartmann, in: Baumbach/Lauterbach/Albers/Hartmann, ZPO, § 142, Rn. 10.
[388] Kitz, GRUR 2003, 1014, 1017.
[389] Musielak/Foerste, § 253, Rn. 18.
[390] Kitz, GRUR 2003, 1014, 1017.
[391] Kitz, GRUR 2003, 1014, 1017.

Providers ausscheiden, da auch diese einen bereits anhängigen Prozess gegen den Rechtsverletzer voraussetzt. Selbst wenn jedoch – nach dem Vorbild des US-amerikanischen John-Doe-Verfahrens – die Möglichkeit der Klageerhebung gegen einen noch unbekannten Rechtsverletzer bestünde, könnte die gewünschte Auskunft nicht im Wege der Zeugenvernehmung ermittelt werden. Denn die Vernehmung von Zeugen zur Ermittlung von Tatsachen, die zur Konkretisierung eines Prozessvortrags benötigt werden, wie hier die Identität des Klagegegners, ist auf einen unzulässigen Ausforschungsbeweis gerichtet.[392] Daher scheidet auch eine Zeugenvernehmung des Access Providers aus.

III. Selbstständiges Beweisverfahren gem. §§ 485 ff. ZPO

Andererseits besteht unter den Voraussetzungen der §§ 485 ff. ZPO die Möglichkeit, bereits vor einer Klageerhebung ein selbständiges Beweisverfahren durchzuführen. Dies gilt insbesondere dann, wenn Beweismittel drohen verloren zu gehen, vorliegend z.B. durch Löschung der Log-Dateien. Allerdings kann auch ein solcher Antrag gegen den Access Provider im Ergebnis nicht durchdringen. Das Beweissicherungsverfahren dient nämlich nur der Sicherung von konkreten Beweisen, nicht jedoch auch zur Erlangung von Beweisen, die benötigt werden, um Ansprüche gegen Dritte geltend zu machen.[393] Würde man dies zulassen, so könnte der Antragssteller die spezifischen Voraussetzungen der materiellrechtlichen Vorlage- und Auskunftsansprüche umgehen. Eine solche Zweckentfremdung des selbständigen Beweisverfahrens zur Klärung von Rechtsfragen ist daher abzulehnen.[394]

E. Ergebnis

Den Rechteinhabern steht weder in materieller noch in prozessualer Hinsicht ein verletzungsunabhängiger Auskunft- oder Vorlageanspruch gegen den Access Provider zu. Somit verbleibt es dabei, dass sich eine Auskunftspflicht des Access Providers allenfalls unter den Voraussetzungen des § 101a UrhG ergibt, der allerdings zwingend eine mittelbare Störereigenschaft des Access Providers voraussetzt.

---

[392] Musielak/Huber, § 373 ZPO, Rn. 12.
[393] Götting, GRUR Int. 1988, 729, 737; Fritze/Stauder, GRUR Int. 1986, 342, 342.
[394] Hartmann, in: Baumbach/Lauterbach/Albers/Hartmann, § 487, Rn. 5.

4. Teil: Gesetzliche Haftungsprivilegierung des Access Providers

Eine Auskunftspflicht des Access Providers nach den allgemeinen Regeln steht weiterhin unter dem Vorbehalt, dass der Inanspruchnahme des Access Providers kein gesetzliches Haftungsprivileg entgegensteht. In dieser Hinsicht sind insbesondere die gesetzlichen Haftungsbeschränkungen des Teledienstegesetzes (TDG) sowie des Mediendienstestaatsvertrag (MDStV) von Bedeutung. Im Folgenden sollen zunächst die Grundlagen und die Konzeption dieser Haftungsregeln dargestellt werden. Danach wird die Frage zu beantworten sein, ob diese Regelungen auch die urheberrechtliche (Mit-)Haftung modifizieren können und, sofern dies der Fall ist, ob sich auch der Access Provider auf ein solches Haftungsprivileg berufen kann, wenn er als mittelbarer Störer für die Urheberrechtsverletzungen seiner Nutzer auf Auskunft in Anspruch genommen wird.

A. Grundlagen der gesetzlichen Haftungsprivilegierungen

I. Entstehungsgeschichte

Im Jahre 1997 wurden mit dem Informations- und Kommunikationsdienstegesetz (IuKDG) auf Bundesebene, dessen Art. 1 das Teledienstegesetz (TDG) darstellt, sowie mit dem Mediendienste-Staatsvertrag (MDStV) auf Länderebene, Rahmenbedingungen für die Dienste in der Informationsgesellschaft in Gesetzesform gegossen. Dass diese Rahmenbedingungen nicht in einem einheitlichen Gesetz geregelt wurden, ist auf einen Streit zwischen dem Bund und den Ländern um die Gesetzgebungszuständigkeit zurückzuführen. Während sich der Bund auf seine Kompetenz für die Telekommunikation (Art. 73 Nr. 7 GG), das Recht der Wirtschaft (Art. 74 Abs. 1 Nr. 11 GG), den gewerblichen Rechtsschutz und das Urheberrecht (Art. 73 Nr. 9), das Strafrecht (Art. 74 Abs. 1 Nr. 1 GG) sowie den Jugendschutz (Art. 74 Abs. 1 Nr. 7) berief, schlossen die Länder ihre Zuständigkeit aus ihrer Kompetenz zur Rundfunkgesetzgebung.[395] Trotz der kontroversen Auffassungen zur Gesetzgebungszuständigkeit haben sich Bund und Länder jedoch darauf verständigt, einen einheitlichen Rechtsrahmen zu schaffen, um die als notwendig erachteten Regelungen nicht an unterschiedlichen Auffassungen in Kompetenzfragen scheitern zu lassen.[396]

---

[395] Näher zum Kompetenzkonflikt, Gounalakis/Rhode, K&R 1998, 321, 322; Roßnagel/Roßnagel, Multimediadienste, Teil 1, Einf, Rn. 28.

[396] Vgl. Engel-Flechsig, ZUM 1997, 231, 231.

Gesetzgebungsbedarf wurde vor allem hinsichtlich der Haftungsproblematik gesehen. Es galt insbesondere die erheblichen Rechtsunsicherheiten zu beseitigen, die durch die seit Mitte der neunziger Jahre gegen Internet-Provider angestrengten Verfahren virulent wurden. In diesen Verfahren wurden auch Access Provider für fremde Rechtsverletzungen zur Verantwortung gezogen.[397] Da der Gesetzgeber in dieser extensiven Rechtsprechung eine Gefährdung für die Investitionsbereitschaft in die neuen Medien sah, wurde eine gesetzliche Beschränkung der Verantwortlichkeit von Providern für zwingend erforderlich gehalten.[398] Mit den Regelungen der §§ 5 TDG/MDStV a.F. ist diesen Bedürfnissen Rechnung getragen worden. Diese Haftungsregeln stellen das Kernstück dieser Gesetzeswerke dar.[399]

Infolge der Umsetzung der zwingenden Vorgaben der Art. 12-15 der E-Commerce-Richtlinie (ECRL)[400] durch das Gesetz über rechtliche Bedingungen für den elektronischen Geschäftsverkehr (EGG), sind die Verantwortlichkeitsregeln des TDG zum 14.12.2001 neu gefasst und in die §§ 8-11 TDG überführt worden. Die Länder haben daraufhin mit Wirkung zum 01.07.2002 den MDStV angepasst und die Haftungsregeln mit identischem Wortlaut in §§ 6-9 MDStV normiert. Da somit zumindest aus haftungsrechtlicher Sicht eine exakte Abgrenzung der Gesetzeswerke dahinstehen kann, beschränkt sich die folgende Darstellung der Haftungsregeln im Wesentlichen auf die Rechtslage nach dem TDG.[401]

II. Neuregelung durch das Telemediengesetz (TMG)

Die mitunter schwierige Abgrenzung zwischen Tele- und Mediendiensten könnte sich indes bald erledigen. Denn das Bundesministerium für Wirtschaft und Arbeit (BMWA) hat im November 2005 einen Referentenentwurf für ein Telemediengesetz (TMG) veröffentlicht. Dieser wurde in leicht modifizierter Form am 14.6.2006 vom Bundeskabinett bestätigt.[402]

---

[397] Vgl. die Aufzählung bei Spindler, in: Spindler/Geis/Schmitz, vor § 8 TDG, Rn. 2.

[398] Amtl. Begründung zum IuKD, BT-Drs. 13/7385, S. 16 f.

[399] Spindler, in: Spindler/Geis/Schmitz, vor § 8 TDG, Rn. 1.

[400] Richtlinie 2000/31/EG.

[401] Zur Abgrenzung der Anwendungsbereiche, unten 4. Teil D. 4.; zu den inhaltlichen Unterschieden zwischen TDG und MDStV, Hoeren, Access Provider, Rn. 608.

[402] Vgl. Heise-News, Meldung v. 14.6.2006, Bundeskabinett beschließt Neuordnung des Medienrechts, http://www.heise.de/newsticker/meldung/74271; Entwurf des Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetzes (ElGVG), dessen Art. 1 das Telemediengesetz (TMG) darstellt (im Folgenden: Gesetzesentwurf zum TMG genannt), abrufbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/M-O/elgvg-elektronischer-

Der Entwurf sieht vor, dass die Regelungen des TDG, des MDStV und des Teledienstedatenschutzgesetzes (TDDSG) einem einheitlichen Regelungswerk zugeführt werden. Zugleich soll durch dieses Gesetz die Differenzierung zwischen Tele- und Mediendiensten entfallen, da beide Dienste künftig unter dem einheitlichen Begriff der „Telemedien" zusammengefasst werden.[403] Weiterhin sollen die Haftungsregeln der §§ 8-11 TDG und der §§ 6-9 MDStV in unveränderter Weise in die Vorschriften der §§ 7-10 TMG überführt werden. Insoweit wird es also in haftungsrechtlicher Hinsicht zu keiner Änderung der bestehenden Gesetzeslage kommen.[404] Das TMG wird voraussichtlich im Frühjahr 2007 in Kraft treten.[405]

B. Grundkonzeption der Verantwortlichkeitsregeln

I. Regelungssystematik

Den Regelungen des TDG/MDStV liegt – ebenso wie dem Produktpirateriegesetz – ein horizontaler Regelungsansatz zugrunde. Die Haftungsregeln gelten querschnittsmäßig für alle Rechtsgebiete, sofern diese nicht gem. §§ 2 Abs. 4 TDG, 2 Abs. 1 MDStV explizit vom Anwendungsbereich ausgenommen sind.[406] Dogmatisch handelt es sich bei den Haftungsregeln um keine eigenständigen Haftungstatbestände, die eine Verantwortlichkeit von Providern begründen oder erweitern, sondern um solche, die eine sich aus den allgemeinen Regeln ergebende Verantwortlichkeit beschränken.[407] Im Gegensatz zum allgemeinen Haftungsrecht knüpfen die Haftungsregeln nicht an die übermittelten Inhalte und die daran angeknüpften Rechte an, sondern an der jeweiligen Tätigkeit des Diensteanbieters.[408] Dabei gilt der Grundsatz, dass sich die Haftung für Informationen in dem Maße abschwächt, in dem die inhaltliche und technische Beziehung zu diesen abnimmt.[409] Dadurch sollen insbesondere die Einflussnahme- und Kontrollmöglichkeiten der Diensteanbieter hinsichtlich der Verbreitung von Inhalten berücksichtigt werden.[410] Die Verantwortlichkeitsregeln differenzieren

---

gesch_C3_A4ftsverkehr-vereinheitlichungsgesetz,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf.

[403] Begr. des Gesetzesentwurfs zum TMG, a.a.O., S. 14.

[404] Begr. des Gesetzesentwurfs zum TMG, a.a.O., S. 22.

[405] Vgl. Heise News, Meldung v. 22.11.2005: Grundzüge des neuen Telemediengesetzes vorgestellt, http://www.heise.de/newsticker/meldung/66523.

[406] OLG Stuttgart, Urt. v. 1.8.2002 – 2 U 47/01, MMR 2002, 746, 748 m. Anm. Spindler; Spindler, in: Spindler/Geis/Schmitz, vor § 8 TDG, Rn. 20.

[407] Hoeren, Access Provider, Rn. 610.

[408] Spindler, in: Spindler/Geis/Schmitz, vor § 8 TDG, Rn. 1.

[409] Dustmann, Provider, S. 93.

[410] Pichler, MMR 1998, 79, 79.

in dieser Hinsicht zwischen dem Bereithalten eigener und fremder Informationen sowie der Übermittlung und der Vermittlung des Zugangs zu fremden Informationen.

Der Anbieter eigener Informationen (Content-Provider) hat gem. § 8 Abs. 1 TDG uneingeschränkt nach den allgemeinen Gesetzen für die von ihm bereitgehaltenen Informationen einzustehen, da er die engste Beziehung zu diesen Informationen aufweist. Im Gegensatz dazu sind die Anbieter fremder Inhalte (Host- und Access-Provider) unter den Voraussetzungen der §§ 9-11 TDG für diese Informationen überhaupt nicht verantwortlich.[411] Flankiert werden diese Vorschriften von § 8 Abs. 2 TDG, der unabhängig vom Eingreifen einer Haftungsprivilegierung anwendbar ist. Dieser statuiert in § 8 Abs. 2 S. 1 TDG das sog. Verbot proaktiver Überwachungspflichten, welches verbietet, den Anbietern fremder Inhalte eine Überwachungs- oder Nachforschungspflicht hinsichtlich der Rechtswidrigkeit der fremden Inhalte aufzuerlegen. Die Regelung des § 8 Abs. 2 S. 2 TDG sieht dagegen eine Rückausnahme von den Haftungsprivilegierungen vor. Danach werden Verpflichtungen zur Entfernung und Sperrung nach den allgemeinen Gesetzen von den Haftungsprivilegierungen ausgenommen.[412]

II. Dogmatische Einordnung

Die dogmatische Einbettung der Haftungsregeln des TDG/MDStV in die Anspruchsprüfung wird seit jeher kontrovers beurteilt. Angesichts des rechtsgebietsübergreifenden Charakters dieser Regelungen erscheint es zunächst angebracht, diese auch auf einer einheitlichen Prüfungsstufe zu berücksichtigen. In dieser Hinsicht werden sowohl innerhalb der Rechtsprechung als auch in der Literatur verschiedene Ansätze vertreten. Diese lassen sich in zwei Strömungen einteilen. Während einige versuchen die Haftungsregeln in den Prüfungsaufbau der allgemeinen Normen einzubinden (Tatbestandslösung),[413] sprechen sich andere für eine eigenständige Prüfungsstufe neben den haftungsbegründenden Normen des allgemeinen Rechts aus (Filterlösung).[414]

---

[411] Zur Eröffnung des Anwendungsbereichs des TDG/MDStV für Access Provider, unten 4. Teil D.; zum Begriff der Verantwortlichkeit, unten. 4. Teil E IV. 1.

[412] Zur Frage, ob § 8 Abs. 2 S. 2 TDG auch Auskunftsansprüche von den Haftungsfreistellungen ausnimmt, siehe unten, 4. Teil E. IV.

[413] Freytag, ZUM 1999, 185, 189f; Dustmann, Provider, S. 130 f.; Spindler, in: Spindler/Geis/Schmitz, vor § 8 TDG, Rn. 28 m.w.N.

[414] BGH, Urt. v. 23.9.2003 – VI ZR 335/02, NJW 2003, 3764, 3765 = JurPC Web- Dok. 323/2003; OLG Düsseldorf, Urt. v. 26.4.2004 – I-20 U 204/02, MMR 2004, 315, 316; En-

1. Tatbestandslösung

Betrachtet man die Verantwortlichkeitsregeln als Tatbestandsmerkmale, so bieten sich verschiedene Anknüpfungspunkte für deren dogmatische Einordnung. Zunächst könnte man erwägen, diese Regeln als Modifikation des allgemeinen Verschuldensmaßstabs anzusehen.[415] Dies findet durchaus auch eine Stütze in den Gesetzesmaterialien, da in diesen ausgeführt wird, dass sich der – den §§ 8-11 TDG übergeordnete – Begriff der Verantwortlichkeit *„auf das Einstehenmüssen für eigenes Verschulden“* bezieht.[416]

Der Einordnung als Verschuldensmaßstab kann jedoch keine rechtsgebietsübergreifende Geltung beigemessen werden. So wäre es z.B. im Bereich des Strafrechts dogmatisch nicht haltbar, die Voraussetzungen des in § 11 TDG erhobenen Merkmals der *„Kenntnis von der rechtswidrigen Handlung“* im Rahmen der Schuld zu erörtern, da die Kenntnis eines Sachverhalts im Strafrecht keine Voraussetzung der Schuld, sondern des subjektiven Tatbestandes ist.[417] Auch mit dem öffentlichen Gefahrenabwehrrecht wäre diese Einordnung nicht vereinbar, da sich Gefahrabwehrmaßnahmen auch gegen den nicht schuldhaft handelnden Störer richten können.[418] Letztlich kann die Einordnung als Verschuldensmaßstab auch im Zivilrecht nicht überzeugen, da somit auch sämtliche verschuldensunabhängige Ansprüche von den Haftungsprivilegierungen ausgenommen wären. Dies ließe sich jedoch nicht mit dem Sinn und Zweck der Verantwortlichkeitsregeln vereinbaren, da die Diensteanbieter bei verschuldensunabhängigen Ansprüchen nicht weniger schutzbedürftig sind als bei verschuldensabhängigen Ansprüchen.[419]

Als aussichtsreicherer Anknüpfungspunkt für eine rechtsgebietsübergreifende Einordnung der Haftungsregeln bietet sich daher an, diese als positiv-rechtliche Regelungen des Zurechnungszusammenhangs zu begreifen.[420] Dafür spricht zunächst, dass das Merkmal des Zurechnungszusammenhangs Grundvoraussetzung aller Haftungsgrundlagen des Zivil-, Straf-

---

gel-Flechsig/Maennel/Tettenborn, NJW 1997, 2981, 2984; Hoeren, Internetrecht, S. 368; Sieber, Verantwortlichkeit, Rn. 246; Stadler, Haftung, S. 45.

[415] So Pichler, MMR 1998, 79, 87 (Fn. 137).

[416] Amtl. Begründung zum IuKD, BT-Drs. 13/7385, S. 20.

[417] Dustmann, Provider, S. 130.

[418] Vgl. Pieroth,/Schlink/Kniesel, § 9, Rn. 10 m.w.N., Rn. 15.

[419] Dustmann, Provider, S. 130; Stadler, Haftung, S. 46; näher zur Anwendbarkeit der §§ 8-11 TDG auf verschuldensunabhängie Ansprüche, siehe unten, 4. Teil E. IV. 1.

[420] So Freytag, ZUM 1999, 185, 189f.; zustimmend Dustmann, Provider, S. 130f.; Spindler, in Spindler/Schmitz/Geis, vor § 8, Rn. 28.

und des öffentlichen Rechts ist.[421] Insofern würde diese Einordnung am ehesten dem querschnittsartigen Charakter der Verantwortlichkeitsregeln gerecht.[422] Jedoch ist auch diese Auffassung mit einem Makel behaftet. Sie setzt nämlich zwingend voraus, dass die Verantwortlichkeitsregeln des TDG/MDStV entweder günstiger als die allgemeinen Haftungsregeln sind oder aber diesen zumindest entsprechen. Sind die Haftungsregeln im Einzelfall für den Diensteanbieter jedoch ungünstiger als die allgemeinen Regeln, würden diese letztlich haftungsschärfend wirken.[423] Dies widerspräche jedoch der Intention des Gesetzgebers, der die Haftung der Diensteanbieter lediglich einschränken, nicht aber erweitern wollte.[424] Daher kann auch eine Einordnung der Haftungsregeln als Modifikation des Zurechnungszusammenhangs in letzter Konsequenz nicht überzeugen. Die Haftungsregeln lassen sich somit nicht rechtsgebietsübergreifend als Tatbestandsmerkmale der allgemeinen Haftungsnormen in den Prüfungsaufbau integrieren.

2. Filterlösung

Vorzugswürdig erscheint daher die Filterlösung, nach der die Verantwortlichkeitsregeln im Rahmen einer eigenständigen Prüfungsstufe neben den allgemeinen Haftungsnormen zu prüfen sind. Diese Auffassung kann sich sowohl auf die Gesetzesmaterialien zum IuKDG als auch auf die zum EGG berufen. Denn in den Begründungen zu beiden Gesetzen wird explizit hervorgehoben, dass sich die Wirkungsweise der Verantwortlichkeitsregeln untechnisch mit der eines Filters vergleichen lässt.[425]

Kontrovers wird allerdings diskutiert, ob es sich bei diesen Regeln um einen „Vor-Filter“ handelt, der erst passiert werden muss, bevor eine Prüfung der allgemeinen Haftungsregeln erfolgt,[426] oder aber um einen „Nach-Filter“, der eine nach den allgemeinen Haftungsregeln begründete Haftung nachträglich ausschließt.[427] Selbst der Gesetzgeber scheint in dieser Frage keinen einheitlichen Standpunkt zu vertreten. Ist noch in der Begründung

[421] So auch Dustmann, in: Bröcker/Czychowski/Schäfer, § 4, Rn. 63.
[422] Sobola/Kohl, CR 2005, 443, 445.
[423] Vgl. das Beispiel bei Stadler, Haftung, S. 46.
[424] Amtl. Begründung zum EGG, BT-Drs. 14/6098, S. 22 f.
[425] Amtl. Begründung zum IuKDG, BT-Drs. 13/7385, S. 51; Amtl. Begründung zum EGG, BT-Drs. 14/6098, S. 23.
[426] So OLG Düsseldorf, Urt. v. 26.4.2004 – I-20 U 204/02, MMR 2004, 315, 316; Hoeren, Internetrecht, S. 368; Sieber, Verantwortlichkeit, Rn. 246; Engel-Flechsig/Maennel/Tettenborn, NJW 1997, 2981, 2984.
[427] Stadler, Haftung, S. 45.

zum IuKDG explizit davon die Rede, dass die Haftungsregeln der Prüfung der allgemeinen Haftungsnormen vorgelagert seien,[428] spricht die spätere Begründung zum EGG dafür, dass sich auch der Gesetzgeber inzwischen der „Nach-Filter"-Theorie angeschlossen hat.[429] Darin wird nämlich ausgeführt, dass *„ein Diensteanbieter für die Rechtsgutverletzung gleichwohl nicht verantwortlich [ist], wenn er sich auf das Eingreifen der §§ 9, 10 oder 11 berufen kann"*. Dies lässt darauf schließen, dass zunächst eine Haftung nach den allgemeinen Regeln begründet werden muss, bevor das Eingreifen einer Haftungsprivilegierung zu diskutieren ist. Für diese Auffassung spricht ferner, dass es auch der gängigen Rechtsdogmatik entspricht, ein Verhalten zunächst rechtlich zu qualifizieren und erst anschließend die Frage zu erörtern, ob der Betroffene für dieses Verhalten auch persönlich zur Verantwortung gezogen werden kann.[430] Die Haftungsregeln sollen daher im Folgenden als „Nachfilter" betrachtet werden, auch wenn dies aus haftungsrechtlicher Sicht letztlich dahinstehen kann.[431]

C. Anwendbarkeit der Haftungsprivilegierungen auf das Urheberrecht

Bevor auf die Frage eingegangen wird, inwieweit sich der Access Provider auf die Haftungsprivilegierungen berufen kann, wenn er für die Urheberrechtsverletzungen seiner Nutzer auf Auskunft in Anspruch genommen wird, ist zunächst zu klären, ob die Haftungsregeln überhaupt geeignet sind, den urheberrechtlichen Haftungsmaßstab zu modifizieren. Sofern zu §§ 5 TDG/MDStV a.F. noch behauptet wurde, dass sich die Haftungsprivilegierungen wegen ihres Wortlauts und ihrer Entstehungsgeschichte nicht auf das Urheberrecht erstrecken, [432] ist dieser Auffassung spätestens seit der Neufassung des TDG und des MDStV durch die Umsetzung der E-Commerce-Richtlinie (ECRL) die Grundlage entzogen worden. So ist nunmehr – wie von der ECRL gefordert[433] – das gesamte Urheberrecht gem. § 4 Abs. 4 Nr. 6 TDG vom Herkunftslandprinzip ausgenommen. Dieser Regelung hätte es freilich nicht bedurft, wenn das Urheberrecht von vornherein nicht dem Anwendungsbereich des TDG unterfiele.[434] Zumin-

[428] Amtl. Begründung zum EGG, BT-Drs. 13/7385, S. 51.
[429] So auch Sobola/Kohl, CR 2005, 443, 445.
[430] Vgl. Dustmann, Provider, S. 129 m.w.N.,
[431] LG Düsseldorf, Urt. v. 29.10.2002 – 4a O 464/01, MMR 2003, 120, 122.
[432] OLG München, Urt. v. 8.3.2001 – 29 U 3282/00, ZUM 2001, 420 – MIDI-Files; zu Recht ablehnend, Spindler, CR 2001, 324, 325 ff.
[433] Vgl. Anhang zu Art. 3 ECRL.
[434] Spindler, in: Spindler/Schmitz/Geis, § 2 TDG, Rn. 6; Schmitz/Dierking, MMR 2005, 420, 421 m.w.N.

dest nach dem Willen des Gesetzgebers sind die Haftungsprivilegierungen somit auch auf urheberrechtliche Sachverhalte anwendbar. Allerdings werden gegen die Anwendbarkeit der Haftungsregeln auf das Urheberrecht sowohl völkerrechtliche als auch verfassungsrechtliche Bedenken hervorgebracht, die einer näheren Betrachtung bedürfen.

I. Völkerrechtliche Bedenken; Vereinbarkeit mit Art. 41, 45 TRIPS

Nach einer vereinzelt vertretenen Auffassung sollen die Haftungsregeln des TDG und des MDStV nicht mit Art. 41, 45 des TRIPS-Übereinkommens vereinbar sein, sofern sie eine Haftungsprivilegierung hinsichtlich der Verletzung von geistigen Schutzrechten, insbesondere des Urheberrechts, vorsehen.[435] Nach den Art. 41, 45 TRIPS müssen die Vertragsstaaten dem Verletzten einen Schadensersatzanspruch gegen den Verletzer gewähren, wenn dieser *„wusste oder vernünftigerweise hätte wissen müssen, dass er eine Verletzungshandlung vornahm"*. Aus dieser Regelung soll sich ergeben, dass TRIPS nicht nur die Einführung eines Ersatzanspruches gegen unmittelbare Verletzer, sondern auch gegen mittelbare Verletzer fordert. Da die Inanspruchnahme von mittelbaren Verletzern jedoch gerade durch die Haftungsprivilegierungen ausgeschlossen werde, seien diese Regelungen völkerrechtswidrig.[436]

Der dieser Auffassung zugrunde liegenden extensiven Auslegung der Art. 41, 45 TRIPS ist zu widersprechen. Deutlich wird dies daran, dass die Erstreckung von TRIPS auf mittelbare Rechtsgutverletzungen zu dem sinnwidrigen Ergebnis führen würde, dass sämtliche Rechtsnormen der Mitgliedstaaten, die eine Haftungsprivilegierung für technische Dienstleister vorsehen, völkerrechtswidrig wären. Dies beträfe neben den Haftungsregeln des TDG/MDStV auch die diesen zugrunde liegenden Art. 12-14 der ECRL sowie den amerikanischen Digital Millennium Copyright Act.[437] Da dies jedoch offensichtlich dem Normverständnis der Vertragsstaaten widerspricht, ist vielmehr davon auszugehen, dass sich diese mit Art. 41, 45 TRIPS lediglich gegenseitig zur Einführung eines gegen den – vorsätzlich oder fahrlässig handelnden – unmittelbaren Verletzer gerichteten Schadensersatzanspruchs verpflichten wollten, nicht jedoch zugleich auch die Einführung einer Haftung für bloß mittelbare Verursachungsbei-

[435] Lehmann, CR 1998, 232 ff.
[436] Lehmann, CR 1998, 232, 233 f.; ähnlich Schack, MMR 2001, 9, 16.
[437] Dustmann, Provider, S. 115.

träge vor Augen hatten.[438] Die Haftungsregeln des TDG/MDStV verstoßen somit nicht gegen Art. 41, 45 TRIPS und sind daher auch nicht völkerrechtswidrig.

II. Verfassungsrechtliche Bedenken

Weiterhin werden gegen die Haftungsprivilegierungen verfassungsrechtlichen Bedenken erhoben, soweit diese Geltung für das Urheberrecht beanspruchen. Dies betrifft zum einen die formelle Verfassungsmäßigkeit der §§ 6-9 MDStV und zum anderen die materielle Vereinbarkeit der Haftungsbeschränkungen mit dem grundgesetzlichen Schutz der Urheber und Leistungsschutzberechtigten aus Art. 14 GG.

1. Verfassungsmäßigkeit der Haftungsregeln des MDStV

Nach Auffassung einiger Literaten sollen die Haftungsprivilegierungen der §§ 6-9 MDStV verfassungswidrig sein, weil das Urheberrecht gem. Art. 73 Nr. 9 GG der ausschließlichen Gesetzgebungskompetenz des Bundes unterliegt und somit den Ländern eine Regelung dieser Materie verwehrt sei.[439] Um die daraus resultierenden Schutzlücken zu schließen, wird entweder eine analoge Anwendung der Haftungsregeln des TDG,[440] oder aber, sofern man die Analogievoraussetzungen verneint, eine unmittelbare Anwendung der Art. 12-15 der ECRL für erforderlich gehalten.[441]

Diesen Ansichten lässt sich jedoch entgegenhalten, dass selbst für den Fall, dass die §§ 6-9 MDStV verfassungswidrig wären, diese Normen zumindest solange von den Gerichten anzuwenden wären, bis das BVerfG von seiner alleinigen Verwerfungskompetenz für formelle Gesetze Gebrauch gemacht und diese Regelungen für nichtig erklärt hat.[442] Dieser Fall dürfte indes nicht eintreten, da bereits erhebliche Zweifel an einem Eingriff in die Gesetzgebungskompetenz des Bundes bestehen. So treffen die Haftungsregeln des MDStV aufgrund ihres horizontalen Regelungsansatzes zwar auch die Materie des Urheberrechts, das nach Art. 73 Nr. 9 GG der ausschließlichen Gesetzgebungskompetenz des Bundes unterliegt. Ein Eingriff in einen spe-

---

[438] Dustmann, Provider, S. 114 f.; Freytag, S. 21; Sieber, Verantwortlichkeit, Rn. 226; Decker, MMR 1999, 7, 10.

[439] Pichler, MMR 1998, 79, 80 f.;. Schaefer/Rasch/Braun, ZUM 1998, 451, 455; Müller-Terpitz, MMR 1998, 478, 480, alle zu § 5 MDStV a.F.; Spindler, in: Spindler/Schmitz/Geis, Einf. zum TDG, Rn. 10 zu §§ 6-9 MDStV n.F.

[440] Müller-Terpitz, MMR 1998, 478, 480.

[441] Spindler, in: Spindler/Schmitz/Geis, TDG Einf, Rn. 10; Dustmann, in: Brö-cker/Czychowski/Schäfer, § 4 Rn. 59.

[442] Stadler, Haftung, S. 89; ähnlich Decker, MMR 1999, 7, 8.

ziellen Kompetenzbereich erfordert allerdings, dass das fragliche Gesetz die kompetenzrechtliche Materie unmittelbar und nicht nur mittelbar regelt oder aber der Schwerpunkt des Gesetzes diese Spezialmaterie zum Gegenstand hat. [443] Beides ist jedoch zu verneinen. Weder liegt der Schwerpunkt der §§ 6-9 MDStV im Bereich des Urheberrechts, da diese querschnittsartig für alle Rechtsgebiete gelten, noch treffen diese Normen unmittelbar urheberrechtsspezifische Regelungen, indem sie rechtsgebietsübergreifend die Haftung für mittelbare Rechtsgutverletzungen modifizieren. Somit ist davon auszugehen, dass der Bund hinsichtlich der Regelungen des TDG lediglich von seiner konkurrierenden Gesetzgebungskompetenz gem. Art. 74 GG Gebrauch gemacht hat und die Kompetenz für den Erlass von Regelungen für Mediendienste, wie die Regelung des § 2 Abs. 4 Nr. 3 TDG klarstellt, den Ländern zugebilligt hat.[444] Aus diesem Grund sind die Regelungen der §§ 6-9 MDStV zumindest nicht formell verfassungswidrig.

Ob sich der Streit hinsichtlich der formellen Verfassungsmäßigkeit dieser Regeln durch die Vereinheitlichung von Tele- und Mediendiensten im Rahmen des TMG erledigen wird, bleibt abzuwarten, da sich der Bund insofern auch die Gesetzgebungskompetenz für Mediendienste anmaßt.

2. Vereinbarkeit mit Art. 14 GG

In materieller Hinsicht stellt sich die Frage, ob den Haftungsprivilegierungen des TDG/MDStV nicht im Wege einer verfassungskonformen Auslegung die Anwendbarkeit auf das Urheberrecht abgesprochen werden muss. So werden die vermögenswerten Elemente des Urheberrechts, also auch die Verwertungsrechte der Rechteinhaber, dem Eigentumsbegriff des Art. 14 Abs. 1 S. 1 GG zugeordnet.[445] Nach dem Inhalt der Eigentumsgarantie hat der Rechteinhaber einen Anspruch darauf, dass ihm der wirtschaftliche Nutzen seiner Arbeit zugeordnet wird, soweit dessen Belange nicht ausnahmsweise, wie in den Fällen der Schrankenregelungen der §§ 44a ff. UrhG, hinter den Belangen des Allgemeinwohls zurückzutreten haben.[446] Allerdings ist der Gesetzgeber hinsichtlich der Ausgestaltung der Verwertungsrechte nicht gehalten, dem Urheber jede nur erdenkliche Verwer-

[443] Dustmann, Provider, S. 118 m.w.N.; Stadler, Haftung, S. 90.
[444] Stadler, Haftung, S. 89 m.w.N.
[445] BVerfG, Beschl. v. 7.7.1971 – I BvR 765/66, BVerfGE 31, 229 – Schulbücher; BVerfG, Beschl. v. 3.10.1989 – I BvR 775/86, BVerfGE 81, 12 – Vermietungsvorbehalt; näher Fechner, S. 152 ff.; Urheberpersönlichkeitsrechte sind hingegen durch Art. 1 Abs. 2 GG geschützt.
[446] BVerfG, Beschl. v. 7.7.1971 – I BvR 765/66, BVerfGE 31, 229, 243– Schulbücher.

tungsmöglichkeit einzuräumen. Dementsprechend ist der Prüfungsmaßstab des BVerfG auf die Frage begrenzt, ob dem Urheber noch ein angemessenes Entgelt für seine Leistung verbleibt.[447]

Die Haftungsregeln des TDG/MDStV lassen die materiellen Verwertungsbefugnisse der Rechteinhaber unberührt. Aus der Fortsetzungsfunktion des Haftungsrechts ergibt sich jedoch, dass sich der Schutzbereich des Art. 14 Abs. 1 GG auch auf die Gewährung effektiver Rechtsverfolgungsansprüche erstrecken muss.[448] Diesem Erfordernis hat der Gesetzgeber mit den §§ 97 ff. UrhG Rechnung getragen. Deren Durchsetzbarkeit könnte allerdings durch die Haftungsfreistellungen der Diensteanbieter gehemmt sein, so dass im Einzelfall eine Reduzierung des Anwendungsbereichs dieser Vorschriften angezeigt sein könnte.

Im Ergebnis kann dies jedoch nicht überzeugen. Zunächst bleibt es dem Verletzten unbenommen gegen den unmittelbaren Verletzer vorzugehen. Dass er daran aufgrund der Verhältnisse des Internets oftmals gehindert sein wird, darf jedoch nicht dazu führen, dass es bei faktischen Rechtsverfolgungsproblemen zu einer pauschalen Belastung Dritter kommt.[449] Zudem muss beachtet werden, dass dem Eigentumsrecht der Rechteinhaber sowohl die Berufsfreiheit der Diensteanbierter aus Art. 12 GG als auch das deren Nutzer schützende Fernmeldegeheimnis aus Art. 10 GG gegenüber zu stellen ist, dessen Schutz auch in das Verhältnis Rechteinhaber und Access Provider ausstrahlen dürfte.[450]

Schließlich verbietet sich eine verfassungskonforme Reduzierung des Anwendungsbereichs der Haftungsprivilegierungen in Bezug auf Urheberrechtsverletzungen auch deshalb, weil jede verfassungskonforme Auslegung ihre Grenze dort findet, wo sie mit dem Wortlaut oder klar erkennbaren Willen des Gesetzgebers in Widerspruch tritt.[451] Mit den Regelungen der §§ 4 Abs. 4 Nr. 6 TDG, 5 Abs. 4 Nr. 6 MDStV, nach denen das Urheberrecht vom Herkunftslandsprinzip ausgenommen ist, hat der Gesetzgeber jedoch eindeutig zum Ausdruck gebracht hat, dass sich der Anwendungsbereich der Haftungsprivilegierungen auch auf das Urheberrecht erstrecken soll. Somit ist auch aus diesem Grund kein Raum für eine verfassungskon-

[447] BVerfG, Beschl. v. 11.10.1988 – I BvR 743/86, BVerfGE 79, 29, 41 f. – Vollzugsanstalten.; ausführlich Fechner, S. 163 ff.
[448] Dustmann, Provider, S. 125.
[449] Dustmann, Provider, S. 126.
[450] Dustmann, Provider, S. 126.
[451] BVerfG, Beschl. v. 30.7.1964, 1 BvL 16-25/62, BVerfGE 18, 97, 111 – Zusammenveranlagung.

forme Reduzierung des Anwendungsbereichs. Erschwerend kommt hinzu, dass die Haftungsregeln auf Art. 12-15 ECRL zurückgehen, so dass die verfassungsrechtliche Beurteilung der Haftungsfragen noch von der Problematik des Vorrangs des Gemeinschaftsrechts überlagert wird.[452] Festzuhalten bleibt insofern, dass die Anwendbarkeit des TDG/MDStV auf das Urheberrecht auch nicht durch eine verfassungskonforme Auslegung im Lichte des Art. 14 GG ausgeschlossen wird.

3. Zwischenergebnis

Der Anwendbarkeit der Haftungsregeln des TDG/MDStV auf das Urheberrecht stehen weder völkerrechtliche noch verfassungsrechtliche Bedenken entgegen. Diese Regeln sind daher auch geeignet, den urheberrechtlichen Haftungsmaßstab zu modifizieren.

D. Anwendbarkeit der Haftungsprivilegierungen auf Access Provider

Voraussetzung für das Eingreifen einer Haftungsprivilegierung auf der Seite des Access Providers ist zunächst, dass Access Providing in den Anwendungsbereich des TDG/MDStV fällt. Problematisch erscheint in dieser Hinsicht, dass die Leistungen des Access Providers im Wesentlichen telekommunikationsbezogen sind, Telekommunikationsdienstleistungen i.S.d. Telekommunikationsgesetzes (TKG) aber gem. §§ 2 Abs. 4 Nr. 1 TDG, 2 Abs. 1 S. 3 MDStV explizit vom Anwendungsbereich dieser Regelungswerke ausgenommen sind. Bevor auf die Reichweite dieser Ausschlussklauseln einzugehen ist, muss jedoch zunächst feststehen, dass Access Providing sowohl in den Anwendungsbereich des TKG als auch in den des TDG/MDStV fällt.

I. Eröffnung des Anwendungsbereichs des TKG

Der Access Provider stellt seinen Nutzern einerseits die für den Internetzugang notwendige technische Infrastruktur zur Verfügung und erbringt andererseits die für die Nutzung des Internets erforderlichen Protokollfunktionen (IP-Adresse, Routing). Bereits die für die Erbringung dieser Dienstleistungen notwendigen technischen Einrichtungen, wie Router und Proxy-Cache-Server, stellen Telekommunikationsanlagen i.S.d. § 3 Nr. 23 TKG dar, da sie es gestatten, elektromagnetische oder optische Signale zu senden, zu übertragen oder zu empfangen.[453] Zudem erfüllt auch die vom Ac-

[452] Vgl. Spindler, in: Spindler/Schmitz/Geis, vor § 8 TDG, Rn. 9 m.w.N. zum Vorrang des Gemeinschaftsrechts.

[453] Dietz/Richter, CR 1998, 528, 530; Wuermeling/Felixberger, CR 1997, 230, 233.

cess Provider vorgenommene Datenübermittlung die Voraussetzungen des Telekommunikationsbegriffes des § 3 Nr. 22 TKG. Daher ist Access Providing insgesamt als Telekommunikationsdienst i.S.d. § 3 Nr. 24 TKG zu qualifizieren.[454] Dem steht auch nicht entgegen, dass sich die Provider zur Erbringung ihrer Dienstleistungen oftmals der Dienste Dritter bedienen.[455] Nach funktionalen Kriterien ist somit zunächst der Anwendungsbereich des TKG eröffnet.

II. Eröffnung des Anwendungsbereichs des TDG/MDStV

Die Abgrenzungsproblematik zwischen TKG und TDG/MDStV wird erst dann virulent, wenn Access Providing nicht nur in den Anwendungsbereich des TKG, sondern auch in den des TDG/MDStV fällt. Der Anwendungsbereich dieser Regelungswerke ist zumindest dann eröffnet, wenn Access Providing als Tele- oder Mediendienst qualifiziert werden kann. Das ist der Fall, wenn sich dieses entweder unter die Generalklauseln der §§ 2 Abs. 1 TDG, 2 Abs. 1 MDStV oder unter eines der Regelbeispiele der §§ 2 Abs. 2 TDG, 2 Abs. 2 MDStV fassen lässt.

Hinsichtlich der Regelbeispiele des TDG kommt allenfalls eine Subsumtion unter § 2 Abs. 2 Nr. 3 TDG in Betracht. Danach werden Angebote zur Nutzung des Internets oder weiterer Netze den Telediensten zugeschrieben. Ein Blick in die Gesetzesmaterialien lässt jedoch erkennen, dass der Gesetzgeber bei Erlass dieser Regelung nicht die Zugangsvermittlung zum Internet, sondern vor allem nachgeschaltete Angebote zur Nutzung der Inhalte und Dienste des Internets, wie z.B. Suchmaschinen, vor Augen hatte.[456] Ferner lässt sich Access Providing auch unter keines der Regelbeispiele für Mediendienste gem. § 2 Abs. 2 MDStV fassen, da diese noch enger auf Inhalte zugeschnitten sind.[457] Es verbleibt somit lediglich ein Rückriff auf die Generalklauseln der §§ 2 Abs. 1 TDG, 2 Abs. 1 MDStV. Allerdings betreibt der Access Provider auch weder einen *„an die Allgemeinheit gerichteten Informations- und Kommunikationsdienst in Text, Ton oder Bild“* i.S.d. § 2 Abs. 2 MDStV noch ist dessen Tätigkeit für eine indi-

[454] Vgl. OVG Münster, Beschl. v. 19.3.2003 – 8 B 2567/02, MMR 2003, 348, 351; Dietz/Richter, CR 1998, 528, 530 f.
[455] Koenig/Loetz, CR 1999, 438, 439; Volkmann, Störer im Internet, S. 16.
[456] Amtl. Begründung zum IuKDG, BT-Drs. 13/7385, S. 19; Volkmann, Störer im Internet, S. 17.
[457] Volkmann, a.a.O.

viduelle Nutzung von kombinierbaren Daten wie Zeichen, Bildern und Tönen i.S.d. § 2 Abs. 1 TDG bestimmt.[458]

Der Access Provider sorgt durch seine Zugangsgewährung vielmehr dafür, dass der Nutzer solche – von Dritten bereitgestellten – Dienste auch tatsächlich in Anspruch nehmen kann.[459] Access Providing stellt demzufolge eine Telekommunikationsdienstleistung dar, die mit den Tele- oder Mediendiensten nicht auf einer Ebene steht, sondern diesen vorgeschaltet ist.[460] Ansonsten würde auch der Zusatz in § 2 Abs. 1 TDG, dass Telediensten eine *„Übermittlung mittels Telekommunikation zugrunde liegt“*, keinen Sinn ergeben.[461] Da der Access Provider somit selbst keinen Tele- oder Mediendienst betreibt, wäre der Anwendungsbereich des TDG/MDStV nach rein funktionalen Kriterien zu versagen, so dass es auf die Ausschlussregelung des § 2 Abs. 4 Nr. 1 TDG, § 2 Abs. 1 S. 3 MDStV gar nicht mehr ankäme.

Dass dieses Ergebnis jedoch offensichtlich nicht mit den Vorstellungen des Gesetzgebers übereinstimmt, lässt sich bereits aus der Definition des Dienstanbieters nach §§ 3 Nr. 1 TDG/MDStV ableiten. Danach ist ein Diensteanbieter, wer *„eigene oder fremde Teledienste zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt“*. Wäre die Zugangsvermittlung jedoch nicht vom Anwendungsbereich des TDG/MDStV erfasst, würde die zweite Alternative der §§ 3 Nr. 1 TDG/MDStV leer laufen.[462] Zudem sind auch die für Diensteanbieter geltenden Verantwortlichkeitsregelungen der §§ 9-11 TDG, 7-9 MDStV eindeutig auf Access Provider zugeschnitten.[463] Zwar darf nicht verkannt werden, dass sich der Anwendungsbereich des TDG/MDStV weder durch die Verantwortlichkeitsregeln noch durch die Definition des Diensteanbieters, sondern ausschließlich nach §§ 2 TDG/MDStV bestimmt.[464] Daraus muss man allerdings nicht den offensichtlich mit der gesetzgeberischen Intention kollidierenden Schluss ziehen, dass auch die Verantwortlichkeitsregelungen insgesamt nicht auf Access Provider anwendbar sind.[465] Der scheinbare Widerspruch zwischen diesen Bestimmungen löst sich nämlich auf, wenn man hinsichtlich der Er-

[458] Volkmann, Störer im Internet, S. 18.
[459] Koenig/Loetz, CR 1999, 438, 440.
[460] Volkmann, a.a.O.
[461] Volkmann, a.a.O.
[462] Koenig/Loetz, CR 1999, 438, 439; Volkmann, Störer im Internet, S. 20.
[463] OVG Münster, Beschl. v. 19.3.2003 – 8 B 2567/02, MMR 2003, 348, 350f.; Freytag, CR 2000, 600, 606.
[464] Stadler, Haftung, S. 74.
[465] So aber Stadler, Haftung, S. 74.

öffnung des Anwendungsbereichs dieser Regelungswerke nicht auf funktionale, sondern auf inhaltliche Kriterien abstellt.[466] Danach muss der Anwendungsbereich nach §§ 2 TDG/MDStV nicht in der Person des Access Providers, sondern lediglich in der Person des Tele- oder Mediendienstebetreibers eröffnet sein, zu dessen Angebot eine Zugangsmöglichkeit geschaffen wird. Sollte der Access Provider sodann für die Übermittlung dieser fremden Inhalte zur Verantwortung gezogen werden, kann sich dieser zumindest als Diensteanbieter i.S.d. § 3 Nr. 1 TDG/MDStV auf die Haftungsprivilegierungen der §§ 9-11 TDG, 7-9 MDStV berufen.[467]

Gestützt wird dieses Ergebnis durch eine richtlinienkonforme Auslegung der auf Art. 12 der ECRL zurückgehenden §§ 9 TDG, 7 MDStV.[468] So wird in Erwägungsgrund 18 der ECRL explizit festgestellt, dass auch Access Provider in den Genuss der Haftungsprivilegierung kommen sollen. Dies ist auch nur sachgerecht, da nicht einzusehen wäre, warum lediglich Host-Provider von diesen Regelungen profitieren sollten, obwohl diese im Gegensatz zu den Access Providern einen viel engeren Bezug zu den angebotenen Inhalten aufweisen.[469]

III. Parallele Anwendbarkeit von TDG/MDStV und TKG

Da sowohl der europäische als auch der deutsche Gesetzgeber gerade auch die Access Provider privilegieren wollte, ist es daher auch verfehlt, die Ausschlussklauseln der §§ 2 Abs. 4 Nr. 1 TDG, 2 Abs. 1 S. 3 MDStV lediglich an ihrem Wortlaut zu messen und dem Access Provider eine Haftungsprivilegierung zu versagen, nur weil dieser Telekommunikationsdienstleistungen i.S.d. § 3 TKG erbringt.[470] Zielführender ist in dieser Hinsicht eine systematisch-teleologische Auslegung unter Berücksichtigung der unterschiedlichen Gesetzeszwecke. Danach regelt das TKG lediglich die technisch-organisatorischen Fragen der Telekommunikationserbringung, während TDG/MDStV die Haftung für die mittels Telekommunikation übermittelten Informationen regeln.[471] Also kann sich der Access Provider trotz der Ausschlussnorm des § 2 Abs. 4 Nr. 1 TDG bzw. § 2 Abs. 1

---

[466] Volkmann, Störer im Internet, S. 21 ff.
[467] Volkmann, Störer im Internet, S. 23.
[468] Vgl. OVG Münster, Beschl. v. 19.3.2003 – 8 B 2567/02, MMR 2003, 348, 350; Freytag, CR 2000, 600, 603.
[469] So auch Volkmann, Störer im Internet, S. 20; Spindler, in: Roßnagel, Multimediadienste, Teil 2, § 2 TDG, Rn. 86.
[470] So aber Stadler, Haftung, S. 74.
[471] BGH, Urt. v. 22.11.2001 – III ZR 5/01, NJW 2002, 361, 362; Spindler, in Spindler/Schmitz/Geis, § 2 TDG, Rn. 26.

S. 3 MDStV auf eine Haftungsprivilegierung nach dem TDG/MDStV berufen, sofern dieser für die von ihm übermittelten Informationen in Anspruch genommen wird.

Dieses Ergebnis steht zudem im Einklang mit dem Entwurf des Telemediengesetzes. So wird in § 1 Abs. 1 TMG-E klargestellt, dass lediglich die ausschließliche Telekommunikation nicht in den Anwendungsbereich des TMG fallen soll. In der Begründung hierzu wird – unter besonderer Bezugnahme auf Access Provider – ausgeführt, dass andere Telekommunikationsanbieter, deren Leistungen überwiegend in der Übertragung von Signalen bestehen, hinsichtlich der Haftung für fremde Inhalte sehr wohl auch von den Haftungsprivilegierungen des TMG erfasst werden.[472]

IV. Bestimmung der einschlägigen Haftungsregeln

Steht somit fest, dass die Haftungsregeln des TDG/MDStV auch auf Access Provider anwendbar sind, stellt sich die – angesichts des haftungsrechtlichen Gleichklangs zwischen TDG und MDStV eher untergeordnete – Frage, welches Regelungswerk im konkreten Fall einschlägig ist. Dies richtet sich danach, ob es sich bei dem Angebot, zu dem der Zugang vermittelt wird, um einen Tele- oder Mediendienst handelt.[473] In dieser Hinsicht ist jeder abgeschlossene Teil des Internetangebots gesondert zu bestimmen. Jeder Internetauftritt kann daher sowohl Tele- als auch Mediendienst sein kann.[474] Als Abgrenzungskriterium fungiert dabei die redaktionelle Gestaltung des Angebots. Steht bei dem übermittelten Inhalt eine *„redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund“*, liegt ein Mediendienst i.S.d. § 2 MDStV vor, der die Anwendbarkeit des MDStV begründet. Sind diese Anforderungen nicht erfüllt, ist hingegen von einem Teledienst auszugehen.[475] Bei einem besonderen Maß an Meinungsrelevanz des Angebots kommt darüber hinaus eine Einstufung als Rundfunkdienst i.S.d. § 2 RStV in Betracht.[476] Da der RStV jedoch keine gesonderte Haftungsprivilegierung für Provider vorsieht, wird in diesen Fällen für eine analoge Anwendung des § 7 MDStV plädiert.

---

[472] Begr. des Gesetzesentwurfs zum TMG, a.a.O. (Fn. 402), S. 17.
[473] Hoeren, Access Provider, Rn. 601.
[474] Hoeren, Access Provider, Rn. 601; ausführlich zur Abgrenzung zwischen TDG und MDStV, Stadler, Haftung, S. 79 ff.; Volkmann, Störer im Internet, S. 13 f.
[475] Volkmann, Störer im Internet, S. 13 m.w.N.
[476] Zur Abgrenzung zwischen TDG/ MDStV und RStV, Volkmann, Störer im Internet, S. 12 f.

Dies ist auch sachgerecht, da der Gesetzgeber des TDG/MDStV von einer vollumfänglichen Privilegierung des Access Providers ausgegangen ist.[477]

Im Rahmen der rechtswidrigen Bereitstellung von urheberrechtlich geschützten Werken, wie z.B. dem Anbieten von Audio- und Videodateien in Peer-to-Peer-Netzwerken oder auf FTP-Servern, wird eine redaktionelle Gestaltung in der Regel zu verneinen sein, so dass diese Angebote regelmäßig als Teledienste i.S.d. § 2 TDG einzustufen sind. Dies dürfte selbst dann gelten, wenn in Downloadportalen die dort bereitgehaltenen Filme mit Kritiken und politischen Stellungnahmen versehen sind. Denn auch in diesen Fällen stellt die Downloadmöglichkeit als solche wiederum eine eigenständige Informations- bzw. Kommunikationseinheit dar, die als Teledienst zu qualifizieren ist.[478]

V. Zwischenergebnis

Die Tätigkeit des Access Providers fällt sowohl in den Anwendungsbereich des TKG als auch in den des TDG und MDStV. Diese Regelungskomplexe sind – trotz der Ausschlußklausel des § 2 Abs. 4 Nr. 1 TDG, § 2 Abs. 1 S. 3 MDStV – nebeneinander anwendbar. Die Anwendbarkeit des TKG beschränkt sich auf technisch-organisatorische Fragen. Bezüglich des Inhalts der übermittelten Daten sind hingegen die Vorschriften des TDG/MDStV einschlägig. Der Access Provider kann sich somit hinsichtlich der von ihm übermittelten Inhalte zumindest als Diensteanbieter i.S.d. § 3 Nr. 1 TDG/MDStV auf die Haftungsprivilegierungen des TDG/MDStV berufen. Das bloße Bereitstellen von urheberrechtlich geschützten Daten im Internet ist als Teledienst zu qualifizieren. Insoweit greifen also die Haftungsregeln des TDG ein, wenn der Access Provider für diese Urheberrechtsverletzungen seiner Nutzer zur Verantwortung gezogen wird.

E. Umfang der Haftungsprivilegierung des Access Providers

Maßgeblich für den Umfang der Haftungsfreistellung des Access Providers sind die Regelungen der §§ 9, 10 TDG. Diese sehen einerseits eine Haftungsprivilegierung für das Durchleiten von Informationen (§ 9 Abs. 1 TDG) und andererseits eine Privilegierung hinsichtlich der kurzzeitigen Zwischenspeicherung von Informationen (§§ 9 Abs. 2, 10 TDG) vor.

---

[477] Volkmann, Störer im Internet, S. 23 f.

[478] Beckmann, S. 72; a.A. offenbar Schmitz/Dierking, CR 2005, 420, 421, die nicht zwischen der Downloadmöglichkeit und der inhaltlichen Beschreibung des Angebots differenzieren.

I. Durchleitung von Informationen (§ 9 Abs. 1 TDG)

Die auf Art. 12 Abs. 1 ECRL zurückgehende Regelung des § 9 Abs. 1 TDG sieht eine Befreiung des Diensteanbieters von Verantwortlichkeitsrisiken vor, die aus einer rein technischen, automatisierten Durchleitung von Informationen resultieren.[479] Diensteanbieter i.S.d. § 9 Abs. 1 TDG sind neben dem Access Provider auch Network-Provider sowie die Betreiber von Router-Rechnern und Anonymisierungsdiensten.[480]

Nach § 9 Abs. 1 S. 1 TDG ist der Access Provider für das reine Durchleiten von Informationen (Routing) sowie das Vermitteln des Zugangs[481] zu einem Kommunikationsnetz nicht verantwortlich, sofern er die Übermittlung nicht veranlasst, den Adressaten der übermittelten Information nicht ausgewählt und die übermittelten Informationen nicht ausgewählt oder verändert hat. Privilegiert ist also die rein passive, automatisierte Tätigkeit, innerhalb derer der Provider weder Kenntnis noch Kontrolle über die weitergeleiteten oder gespeicherten Informationen hat.[482] Ebenfalls von der Privilegierung umfasst sind technisch bedingte Änderungen des übermittelten Inhalts.[483] Dies zielt im Wesentlichen auf das Routing ab, bei dem die Informationen für Übermittlungszwecke in kleinere Datenpakete aufgeteilt werden.[484]

Die Voraussetzungen des § 9 Abs. 1 S. 1 TDG sind somit auch dann erfüllt, wenn der Access Provider einem Nutzer den Zugang zum Internet gewährt und dieser den Zugang zur rechtswidrigen Verbreitung urheberrechtlich geschützten Materials verwendet. Denn auch der Access Provider hat in diesen Fällen weder Kontrolle noch Kenntnis über die übermittelten Informationen. Allerdings steht diese Haftungsfreistellung unter dem Vorbehalt des § 9 Abs. 1 S. 2 TDG. Danach entfällt die Privilegierung, wenn der Provider mit einem Nutzer zusammenarbeitet, um rechtswidrige Handlungen zu begehen (kollusives Zusammenwirken).

Fraglich ist in dieser Hinsicht, ob nicht zumindest dann von einem kollusiven Zusammenwirken zwischen Access Provider und Nutzer auszugehen ist, wenn der Access Provider seitens der Rechteinhaber auf die Rechtsver-

---

[479] Amtl. Begründung zum EGG, BT-Drs. 14/6098, S. 24.
[480] Spindler, in: Spindler/Schmitz/Geis, § 9 TDG, Rn. 16 ff.; zur Anwendbarkeit des § 9 TDG auf sog. Anonymisierungsdienste, siehe unten 6. Teil B. I.
[481] Damit ist die Bereitstellung von Einwahlknoten (sog. PoP's) gemeint.
[482] Erwägungsgrund 42 der ECRL.
[483] Erwägungsgrund 43 der ECRL.
[484] Spindler, in: Spindler/Schmitz/Geis, § 9 TDG, Rn . 5.

letzungen des Nutzers hingewiesen wurde und in Kenntnis dieser Rechtsverletzungen den Nutzer nicht abmahnt oder dessen Zugang sperrt. So ließe sich argumentieren, dass in diesen Fällen weitere Rechtsverletzungen des Nutzers seitens des Access Providers zumindest billigend in Kauf genommen werden, dieser also zumindest mit Eventualvorsatz (dolus eventualis) handelt. Dies dürfte indes jedoch nicht ausreichen, um ein kollusives Zusammenwirken i.S.d. § 9 Abs. 1 S. 2 TDG zu bejahen. Denn sowohl dessen Wortlaut *(„um rechtswidrige Handlungen zu begehen")* als auch Erwägungsgrund 44 der ECRL lassen darauf schließen, dass nur ziel- und zweckgerichtetes Handeln die Haftungsprivilegierung entfallen lässt. Ein solches Verhalten ist jedoch nicht bereits bei bedingtem, sondern erst bei direktem Vorsatz erfüllt.[485] Somit entfällt das Haftungsprivileg des Access Providers auch dann nicht, wenn dieser seitens der Rechteinhaber auf Rechtsverletzungen seiner Nutzer hingewiesen wird und Maßnahmen zur Verhinderung weiterer Schutzrechtsverletzungen unterlässt.

II. Zwischenspeicherung von Informationen (§§ 9 Abs. 2, 10 TDG)

Hinsichtlich der Privilegierung für Zwischenspeicherungen ist zwischen der automatischen, kurzfristigen Zwischenspeicherung i.S.d. § 9 Abs. 2 TDG und der kurzzeitigen Zwischenspeicherung zur beschleunigten Übermittlung gem. § 10 TDG zu unterscheiden. Die Regelung des § 9 Abs. 2 TDG dient der Umsetzung von Art. 12 Abs. 2 ECRL und stellt klar, dass kurzzeitige Zwischenspeicherungen der reinen Durchleitung gleichgestellt sind, soweit diese zur Durchführung der Übermittlung vorgenommen werden und sich auf die technisch unbedingt notwendige Zeit beschränken. Erforderlich ist jedoch stets ein Bezug zu einer konkreten Abfrage des Nutzers.[486] Die Regelung des § 9 Abs. 2 TDG zielt daher in erster Linie auf eine Privilegierung für technisch bedingte Zwischenspeicherungen im Rahmen des Routings ab.[487]

Darüber hinaus sieht § 10 TDG – in Umsetzung von Art. 13 ECRL – eine Privilegierung für das sog. Caching oder Proxy-Caching vor, also die Fälle, bei denen von den Nutzern abgerufene Inhalte zur beschleunigten Datenübermittlung auf einem Proxy-Cache-Server des Access Providers zwischengespeichert werden.[488] Voraussetzung für das Eingreifen einer Privi-

[485] Spindler, in: Spindler/Schmitz/Geis, § 9 TDG, Rn. 9; Vassilaki, MMR 2002, 659, 660; Barton, CR 2003, 592, 596.
[486] Begr. des RegE zum EGG, BT-Drs. 14/6098, S. 24.
[487] Stadler, Haftung, S. 122.
[488] Vgl. oben 1. Teil C. I. 1.

legierung nach § 10 TDG ist zunächst, dass der Nutzer keinen direkten Zugriff auf die zwischengespeicherten Daten hat. Dies dient der Abgrenzung zu dem in § 11 TDG geregelten Hosting, bei dem die Nutzer direkt auf die beim Provider zwischengespeicherten Daten zugreifen können.[489] Weiterhin steht eine Privilegierung für das Caching unter dem Vorbehalt, dass auch die Voraussetzungen des § 10 S. 1 Nr. 1 bis 5 TDG kumulativ erfüllt sind. In Betracht kommt ein Verstoß gegen § 10 S. 1 Nr. 5 TDG für den Fall, dass der Access Provider darauf hingewiesen wird, dass auf seinem Proxy-Cache-Server rechtswidrig bereitgehaltene Werke zwischengespeichert werden. Nach dieser Regelung entfällt das Haftungsprivileg, wenn die Access Provider die derart gespeicherten Inhalte nicht unverzüglich entfernen oder den Zugang zu diesen sperren, *„sobald sie Kenntnis davon erhalten haben, dass die Informationen am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt worden oder der Zugang zu ihnen gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Sperrung oder Entfernung angeordnet hat.“*

Der Wortlaut des § 10 Abs. 1 Nr. 5 TDG legt indes nahe, dass die bloße Inkenntnissetzung von der Rechtswidrigkeit der Information allein gerade nicht ausreicht, um das Haftungsprivileg entfallen zu lassen. Bestätigt wird diese Annahme durch den Verweis des § 10 S. 2 TDG auf § 9 Abs. 1 S. 2 TDG. Denn auch nach § 9 Abs. 1 S. 2 TDG geht das Haftungsprivileg nicht schon mit der Kenntnis von der Rechtswidrigkeit eines Inhalts verlustig, sondern erst bei kollusiven Zusammenwirken mit dem Rechtsverletzer. Der Access Provider ist somit auch dann haftungsprivilegiert, wenn dessen Nutzer urheberrechtswidrig Werke aus dem Internet herunterladen und diese Werke automatisch auf dem Proxy-Cache-Server des Access Providers zum Abruf für weitere Nutzer zwischengespeichert werden.

III. Zwischenergebnis

Der Umfang der Haftungsprivilegierung des Access Providers nach §§ 9, 10 TDG umfasst die Bereitstellung des Internetzugangs, die Durchleitung von Informationen sowie deren kurzzeitige Zwischenspeicherung zum Zwecke einer effektiven Datenübertragung. Insofern ist die Tätigkeit des Access Providers insgesamt als haftungsprivilegiert anzusehen. Dies gilt selbst dann, wenn die Dienstleistungen für Urheberrechtsverletzungen genutzt werden und der Access Provider von diesen Rechtsverletzungen in Kenntnis gesetzt wurde.

---

[489] Spindler, NJW 2002, 921, 923.

IV. Rückausnahme für Auskunftsansprüche gem. § 8 Abs. 2 S. 2 TDG

Ob sich der Access Provider auch im Falle gegen ihn gerichteter Auskunftsbegehren auf eine Haftungsprivilegierung nach §§ 9, 10 TDG berufen kann, hängt davon ab, ob auch Auskunftsansprüche von dieser Haftungsprivilegierung erfasst sind. Dem könnte die Rückausnahmeregelung des § 8 Abs. 2 S. 2 TDG[490] entgegenstehen. Nach dieser werden *„Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen"* von den Haftungsprivilegierungen ausgenommen. Während Einigkeit darüber herrscht, dass nach dieser Regelung auch im persönlichen Anwendungsbereich des TDG eine Störerhaftung des Access Providers nach den allgemeinen Regeln möglich sein muss,[491] ist die Reichweite dieser Ausnahme umstritten. Dies gilt insbesondere hinsichtlich der Frage, ob durch § 8 Abs. 2 S. 2 TDG auch verschuldensunabhängige (Auskunfts-)Ansprüche von den Haftungsprivilegierungen ausgenommen werden.

1. Ausnahme verschuldensunabhängiger (Auskunfts-)Ansprüche

Sowohl in der Rechtsprechung als auch in der Literatur wird vertreten, dass § 8 Abs. 2 S. 2 TDG die gesamte verschuldensunabhängige Störerhaftung von den Haftungsprivilegierungen der §§ 9-11 TDG ausnimmt. Dies gelte daher auch für verschuldensunabhängige Auskunftsansprüche, insbesondere den § 101a UrhG. Es sei nämlich unverständlich, wenn einerseits auch im Anwendungsbereich der Haftungsprivilegierungen eine Störerhaftung eingreift, andererseits jedoch Auskunftsansprüche, die ebenfalls auf der Störerhaftung beruhen, nicht durchsetzbar sein sollten.[492]

Für eine solch extensive Auslegung des § 8 Abs. 2 S. 2 TDG lässt sich zunächst auch ein Passus in den Gesetzesmaterialien rekurrieren. So wird hinsichtlich des – den Haftungsregeln übergeordneten – Terminus der „*Verantwortlichkeit*" ausgeführt, dass damit lediglich das *„Einstehenmüssen für eigenes Verschulden"* gemeint sei.[493] Dies erinnert an die – ebenfalls mit dem Begriff der Verantwortlichkeit überschriebene – Regelung

---

[490] § 8 Abs. 2 S. 2 TDG entspricht § 6 Abs. 2 S. 2 MDStV; die nachfolgenden Ausführungen sind somit für die Haftung nach dem MDStV entsprechend heranzuziehen.

[491] BGH, Urt. v. 11.3.2004 – I ZR 304/01, MMR 2004, 668, 670 = BGH GRUR 2004, 860 – Internet-Versteigerung; Spindler, in: Spindler/Schmitz/Geis, § 8 TDG, Rn. 15.

[492] LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, CR 2005, 136, 138 = MMR 2005, 55; ausdrücklich in diesem Sinne Spindler/Dorschel, CR 2005, 38, 41.

[493] Begr. des RegE zum IuKDG, BT-Drs. 13/7385, S. 19.

des § 276 BGB.[494] Auch nach dieser haftet der Schuldner nur für vorsätzliches und fahrlässiges Verhalten, nicht aber auch verschuldensunabhängig. Daher ließe sich im Wege eines Umkehrschlusses *(arg. e contrario)* aus dem Terminus der Verantwortlichkeit tatsächlich ableiten, dass die Haftungsregeln des TDG nur verschuldensabhängige Ansprüche erfassen, nicht aber auch die gesamte verschuldensunabhängige Störerhaftung. Aus diesem Blickwinkel wären auch verschuldensunabhängige Auskunftsansprüche – wie der § 101a UrhG – von den Haftungsprivilegierungen des TDG ausgenommen. Demnach stünde dem Access Provider kein Haftungsprivileg zur Seite, wenn er – gem. § 101a UrhG – auf Auskunft in Anspruch genommen wird.

a) Dogmatische Einwände in Bezug auf § 101a UrhG

Nach Stadler[495] soll § 101a UrhG jedoch bereits deshalb nicht unter die Rückausnahme des § 8 Abs. 2 S. 2 TDG fallen, weil sich dieser Anspruch keinesfalls ausschließlich der von den Haftungsfreistellungen ausgenommenen Störerhaftung zuordnen lasse. Vielmehr sei § 101a UrhG, wie auch andere Auskunftsansprüche, stets nur ein Annexanspruch, der in dogmatischer Hinsicht wie der Hauptanspruch zu behandeln sei. Sofern also im Hauptsacheverfahren ein Schadensersatzanspruch geltend gemacht werde, könne auch der diesen vorbereitende Auskunftsanspruch nicht gem. § 8 Abs. 2 S. 2 TDG vom Anwendungsbereich der §§ 9-11 TDG ausgenommen sein, da Schadensersatzansprüche unstreitig von den Haftungsprivilegierungen der §§ 9-11 TDG erfasst seien.[496]

In dieser Hinsicht ist Stadler allerdings entgegenzuhalten, dass es sich bei § 101a UrhG gerade nicht um einen Annexanspruch handelt, der auf die Durchsetzung von Ansprüchen gegen den auf Auskunft in Anspruch genommen selbst, also den Access Provider, gerichtet ist. Es handelt sich vielmehr um einen selbstständigen, nicht akzessorischen Anspruch, der ein Vorgehen gegen einen Dritten ermöglichen soll,[497] in diesem Fall also gegen den Nutzer. Zudem würde auch ein gegen den Nutzer des Access Providers gerichteter Schadensersatzanspruch keineswegs an den Haftungsprivilegierungen der §§ 9-11 TDG scheitern, da der Nutzer zumindest nicht als Anbieter fremder Informationen qualifiziert werden kann. Allenfalls

[494] Dies übersieht Stadler, Haftung, S. 44, der den Begriff der Verantwortlichkeit als Novum im deutschen Recht ansieht.
[495] Stadler, Haftung, S. 202.
[496] Stadler, Haftung, S. 202.
[497] Dreier/Schulze, § 101a UrhG, Rn. 1.

kann dieser – z.B. beim Betrieb eines FTP-Servers – als Content-Provider angesehen werden. Einem solchen ist jedoch bereits gem. § 8 Abs. 2 S. 1 TDG eine Reklamation auf die Haftungsprivilegierungen verwehrt.

Vor dem Hintergrund, dass sich der § 101a UrhG nicht nur gegen den mittelbaren Störer, sondern auch gegen den vorsätzlichen Verletzer richtet, könnte man Stadler jedoch darin beipflichten, dass es in der Tat seltsam anmutet, den § 101a UrhG dem Bereich der Störerhaftung zuzuschlagen, sofern der Anspruchsgegner aufgrund einer vorsätzlichen Verletzungshandlung in Anspruch genommen wird. Auch dies spricht indes nicht dagegen, den § 101a UrhG zumindest dann auch im Bereich der Störerhaftung anzusiedeln, wenn der Access Provider – wie in den hier einschlägigen Konstellationen – als mittelbarer Störer auf Auskunft in Anspruch genommen werden soll.

b) Widerspruch zur Gesetzessystematik und Zielsetzung der Haftungsregeln

Auch wenn Stadlers Argumentation gegen eine Erstreckung des § 8 Abs. 2 S. 2 TDG auf Auskunftsansprüche nicht vollends überzeugen kann, sprechen doch andere gewichtige Argumente gegen die Annahme, dass man aus den Ausführungen des Gesetzgebers zum Begriff der Verantwortlichkeit im Wege eines Umkehrschlusses den Anwendungsbereich des § 8 Abs. 2 S. 2 TDG auf die gesamte verschuldensunabhängige Störerhaftung erstrecken kann. Denn eine dahingehende Auslegung stößt einerseits auf gesetzessystematische Bedenken und lässt sich andererseits nur schwerlich mit der – den Haftungsregeln übergeordneten – Zielsetzung des Gesetzgebers vereinen.

Der Widerspruch zur Gesetzessystematik lässt sich im Wege eines *argumentum ad absurdum* verdeutlichen. Interpretiert man den Terminus der Verantwortlichkeit, unter dessen Stern die Haftungsprivilegierungen des TDG stehen, in dem Sinne, dass Ansprüche, die auf der verschuldensunabhängigen Störerhaftung beruhen, von vornherein nicht von den §§ 9-11 TDG erfasst werden, so hätte es der Ausnahmeregelung des § 8 Abs. 2 S. 2 TDG gar nicht bedurft. Anderenfalls käme man zu dem widersinnigen Ergebnis, dass nach § 8 Abs. 2 S. 2 TDG Ansprüche von den Haftungsprivilegierungen der §§ 9-11 TDG ausgenommen werden, die diesen von vornherein nicht unterliegen. Demzufolge hätte die Vorschrift des § 8 Abs. 2 S. 2 TDG in Bezug auf verschuldensunabhängige Ansprüche überhaupt keinen eigenständigen Regelungsbereich, mithin wäre sie überflüssig.

Nun ließe sich zwar argumentieren, dass es sich bei § 8 Abs. 2 S. 2 TDG, wie auch bei § 8 Abs. 1 TDG, lediglich um einen deklaratorischen Hinweis auf die bestehende Haftungslage handelt.[498] Dem steht jedoch der Wortlaut des § 8 Abs. 2 S. 2 TDG entgegen. Danach wird eben nicht die gesamte verschuldensunabhängige Störerhaftung von den Haftungsprivilegierungen ausgenommen, sondern nur Ansprüche zur *„Entfernung und Sperrung der Nutzung von Informationen"*. Dies spricht vielmehr dafür, dass § 8 Abs. 2 S. 2 TDG sehr wohl einen eigenständigen Regelungsgehalt aufweist. Dieser besteht nämlich darin, die gem. §§ 9-11 TDG grundsätzlich bestehenden Haftungsfreistellungen der Diensteanbieter dahingehend zu durchbrechen, dass diese nicht für Entfernungs- und Sperrungsansprüche gelten. Es handelt sich bei § 8 Abs. 2 S. 2 TDG somit um eine echte Ausnahmebestimmung, die als solche bereits einer restriktiven Auslegung bedarf.[499] Gegenteiliges folgt auch nicht aus der Internet-Versteigerung-Entscheidung des BGH. Auch darin hat der BGH nicht etwa im Wege eines *obiter dictum* alle verschuldensunabhängigen Ansprüche gem. § 8 Abs. 2 S. 2 TDG von den Haftungsprivilegierungen ausgenommen, sondern nur klargestellt, dass Unterlassungsansprüche gem. § 8 Abs. 2 S. 2 TDG nicht vom Haftungsprivileg des § 11 TDG erfasst werden.[500]

Letztlich stünde eine derartig extensive Interpretation des § 8 Abs. 2 S. 2 TDG auch in eklatantem Widerspruch zur gesetzgeberischen Zielsetzung. Denn primäres Regelungsziel der Haftungsregeln des TDG ist die Reduzierung der zivil- und strafrechtlichen Risiken der Provider hinsichtlich einer Inanspruchnahme aus mittelbaren Rechtsgutverletzungen.[501] Dieses Risiko ist bei verschuldensunabhängigen Ansprüchen aufgrund der sehr viel weiteren Haftung jedoch ungleich höher als bei verschuldensabhängigen Schadensersatzansprüchen.[502] Um den Willen des Gesetzgebers nicht vollständig zu konterkarieren, ist daher davon auszugehen, dass die §§ 8-11 TDG eine gesetzliche Einschränkung der Störerhaftung darstellen, die

---

[498] Zum deklaratorischen Charakter des § 8 Abs. 1 TDG, Amtl. Begr. zum EGG, BT-Drs. 14/6098, S. 23; Stadler, Haftung, S. 91.

[499] Näher zur Auslegung von Ausnahmebestimmungen, Larenz/Canaris, Methodenlehre, S. 176; vgl. auch oben, 2. Teil A. II. 2. b) aa).

[500] Vgl, BGH, Urt. v. 11.3.2004 – I ZR 304/01, MMR 2004, 668, 670 = BGH GRUR 2004, 860 – Internet-Versteigerung; so auch Stadler, Haftung, S. 201 f.

[501] Begr. des RegE zum IuKDG, BT-Drs. 13/7385, S. 16.

[502] LG Düsseldorf, Urt. v. 29.10.2002 – 4a O 464/01, MMR 2003, 120, 123; LG Berlin, Urt. v. 25.2.2003 – 16 O 476/01, MMR 2004, 195 , 197; Ehret, CR 2003, 754, 760.

gem. § 8 Abs. 2 S. 2 TDG nur bezüglich Verpflichtungen zur Entfernung oder Sperrung durchbrochen werden kann.[503]

c) Zwischenergebnis

Verschuldensunabhängige Auskunftsansprüche – wie der § 101a UrhG – sind nicht bereits deshalb von den Haftungsprivilegierungen der §§ 9-11 TDG ausgenommen, weil davon nur verschuldensabhängige Ansprüche erfasst werden. Die Regelung des § 8 Abs. 2 S. 2 TDG nimmt gerade nicht die gesamte verschuldensunabhängige Störerhaftung von den Haftungsprivilegierungen der §§ 9-11 TDG aus, sondern nur Entfernungs- und Sperrungsansprüche. Auskunftsansprüche wären somit allenfalls dann von den Haftungsprivilegierungen ausgenommen, wenn sich auch diese unter die in § 8 Abs. 2 S. 2 TDG erhobenen Merkmale der *„Verpflichtungen zur Entfernung oder Sperrung“* subsumieren ließen.

2. Subsumtion von Auskunftspflichten unter § 8 Abs. 2 S. 2 TDG

Nach der oberinstanzlichen Rechtsprechung sollen einer Subsumtion von Auskunftspflichten unter § 8 Abs. 2 S. 2 TDG vor allem dogmatische Bedenken entgegenstehen.[504] So wird zunächst darauf hingewiesen, dass die vom Anwendungsbereich des TDG ausgenommenen Entfernungs- und Sperrungsansprüche ihre dogmatische Grundlage in den gesetzlichen Regelungen über die Besitz- und Eigentumsstörung der §§ 862, 1004 BGB finden. Diese Regelungen erfassen jedoch nur Abwehransprüche in Form des Unterlassens eines adäquat-kausalen Handelns. Auskunftspflichten seien jedoch nicht auf ein Unterlassen, sondern auf ein aktives Handeln gerichtet. Zudem fänden diese ihre dogmatische Grundlage auch nicht in den §§ 862, 1004 BGB, sondern in § 242 BGB. Aus diesem Grund seien Auskunftsansprüche keine unter § 8 Abs. 2 S. 2 TDG fallenden Abwehransprüche.[505]

---

[503] OLG Düsseldorf, Urt. v. 26.2.2004 – I 10 U 204/02, MMR 2004, 315, 316; Hoeren, Anm. zu BGH, Urt. v. 11.3.2004 – I ZR 304/01 – Internet-Versteigerung, MMR 2004, 672, 673; Kaufmann/Köcher, Anm. zu LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, MMR 2005, 61, 61.

[504] OLG Hamburg, Urt. v. 28.4.2005 – 5 U 156/04, MMR 2005, 453, 456 = CR 2005, 512; OLG Frankfurt a.M., Urt. v. 25.1.2005 – 11 U 51/05, MMR 2005, 241, 243 = CR 2005, 285, jeweils mit Verweis auf BGH, Urt. v. 18.10.2001 – I ZR 22/99, WRP 2002, 532, 533 – Meißner Dekor.

[505] OLG Hamburg, a.a.O.; OLG Frankfurt a.M.,a.a.O.

Dem entgegnet Dorschel[506], zunächst zu Recht, dass sich auch eine Pflicht zur Sperrung oder Beseitigung nicht immer nur in einem schlichten Unterlassen, sondern oftmals auch in einer auf aktives Tun gerichteten Handlungspflicht konkretisiert.[507] Darüber hinaus will Dorschel jedoch auch Auskunftspflichten unter das in § 8 Abs. 2 S. 2 TDG erhobene Merkmal der Beseitigung subsumieren. In dieser Hinsicht verweist er darauf, dass auch in der wettbewerbsrechtlichen Rechtsprechung anerkannt sei, dass sich die Drittauskunftspflicht aus dem Beseitigungsanspruch ableite.[508] Hilfsweise soll sich dieses Ergebnis nach Auffassung von Spindler/Dorschel[509] aus einer richtlinienkonformen Auslegung des § 8 Abs. 2 S. 2 TDG ergeben. Diese Regelung gehe nämlich auf Art. 15 ECRL zurück und statuiere daher lediglich das dort niedergelegte Verbot proaktiver Überwachungspflichten. Derartige Überwachungspflichten seien jedoch nicht betroffen, wenn der Access Provider zur Herausgabe von Daten verpflichtet werde, die diesem bereits bekannt seien.[510]

Dies überzeugt nicht. Einer Parallele zum Wettbewerbsrecht steht – wie oben bereits ausgeführt – entgegen, dass sich der Drittauskunftsanspruch auch im Wettbewerbsrecht nicht aus dem allgemeinen Beseitigungsanspruch ableitet, sondern auch in diesen Fällen eine analoge Anwendung des § 101a UrhG angezeigt ist.[511] Darüber hinaus verbietet sich eine Subsumtion von Drittauskunftspflichten unter den urheberrechtlichen Beseitigungsanspruch aus § 97 UrhG bereits deshalb, weil die spezialgesetzlichen Tatbestandsvoraussetzungen des § 101a UrhG nicht durch einen Rückgriff auf § 97 UrhG ausgehebelt werden dürfen.[512] Zudem lässt sich dieses Ergebnis auch nicht durch eine richtlinienkonforme Auslegung des § 8 Abs. 2 S. 2 TDG im Lichte des Art. 15 Abs. 1 ECRL revidieren. Denn insoweit verkennen Spindler/Dorschel, dass § 8 Abs. 2 S. 2 TDG nicht auf das aus Art. 15 Abs. 1 ECRL resultierende Verbot von proaktiven Überwachungspflichten, sondern auf die Regelungen der Art. 12 Abs. 3, 13 Abs. 2, 14 Abs. 3 ECRL zurückgeht.[513] Dass sich unter den – aus diesen Regelungen übernommenen – Terminus der Beseitigung und Sperrung jedoch keine Auskunftspflichten fassen lassen, ergibt sich bereits aus der gesonderten

[506] Dorschel, Anm. zu OLG Hamburg, a.a.O., CR 2005, 516, 517.
[507] Dorschel, a.a.O.
[508] Dorschel, a.a.O.
[509] CR 2005, 38.
[510] Spindler/Dorschel, CR 2005, 38, 41.
[511] Siehe oben, 2. Teil B. II.
[512] Siehe oben, 2. Teil D.
[513] Amtl. Begründung zum EGG, BT-Drs. 14/6098, S. 23.

Erwähnung dieser Ansprüche in Art. 15 Abs. 2 ECRL. Festzuhalten bleibt insofern, dass sich Auskunftsansprüche nicht unmittelbar unter die in § 8 Abs. 2 S. 2 TDG erhobenen Merkmale der Entfernung und Sperrung subsumieren lassen.

3. Erst-Recht-Schluss und Analogie

Als weiteres Hilfsargument wird vertreten, dass sich der Anwendungsbereich des § 8 Abs. 2 S. 2 TDG zumindest im Wege eines Erst-Recht-Schlusses *(arg. a maiore ad minus)* auf Auskunftsansprüche erstrecken müsse, da den Access Provider eine Auskunftserteilung weit weniger belaste als eine Sperrung des jeweiligen Nutzers.[514]

Bereits an der behaupteten Minderbelastung kann gezweifelt werden. Denn im Gegensatz zur Sperrung ist der Provider bei der Herausgabe von Nutzerdaten erheblichen datenschutzrechtlichen sowie vertraglichen Haftungsrisiken ausgesetzt.[515] Selbst wenn es hingegen zuträfe, dass sich eine Auskunftserteilung im konkreten Fall als weniger belastend darstellen würde, dürften die Voraussetzungen für ein *argumentum a maiori ad minus* indes nicht erfüllt sein. Ein solches ist nämlich nur dann gerechtfertigt, wenn die *ratio legis* einer gesetzlichen Bestimmung auf einen anderen, ähnlichen Tatbestand, in ungleich höherem Maße zutrifft.[516] Dies wäre z.B. anzunehmen, wenn eine Regelung existierte, die es einem Rechteinhaber erlauben würde, die Preisgabe der Identität eines Nutzers zu verlangen, der rechtmäßig urheberrechtlich geschützte Inhalte im Internet verbreitet. In diesem Fall wäre anzunehmen, dass die Auskunftspflicht somit „erst recht" auch bei einem unrechtmäßigen Anbieten von Inhalten gilt. Eine Auskunftspflicht kann jedoch nicht als ein solches „Minus" zur Sperrpflicht betrachtet werden, da die Auskunftserteilung nicht in der Sperrung aufgeht, sondern dessen Wirkungskreis bei weitem übersteigt. So wird bei einer Auskunftserteilung über den Nutzer, im Gegensatz zu einer Sperrung desselben, der Rechtskreis zwischen Provider und Nutzer um den Rechteinhaber erweitert. Mithin wird der Nutzer zugleich auch Rechtsverfolgungsmaßnahmen Dritter ausgesetzt.[517] Hinzu kommt, dass ein Beseitigungsanspruch, ebenso wie eine Sperrverpflichtung, stets auf ein zukünftiges Ver-

[514] LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, CR 2005, 136, 138 = MMR 2005, 55; LG Köln, Urt. v. 28.7.2004 – 28 O 301/04, ZUM 2005, 236, 240; Czychowski, MMR 2004, 514, 516.

[515] Ähnlich Kaufmann/Köcher, Anm. zu LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, MMR 2005, 61, 61.

[516] Larenz/Canaris, Methodenlehre, S. 208.

[517] Vgl. Sieber/Höfinger, MMR 2004, 574, 580.

halten gerichtet ist, sich die Auskunftspflicht jedoch auf die Sanktion eines vergangenen Verhaltens bezieht.[518] Da es sich bei der Auskunftspflicht somit nicht um ein „Minus", sondern um ein Aliud zur Sperrpflicht handelt, kann auch ein *argumentum a maiore ad minus* nicht überzeugen.[519] Der Vollständigkeit halber sei an dieser Stelle erwähnt, dass auch eine analoge Anwendung des § 8 Abs. 2 S. 2 TDG ausscheidet, da es aufgrund der soeben angeführten Gründe zumindest auch an der Vergleichbarkeit zwischen Auskunfts- und Sperrpflichten mangelt.[520]

4. Zwischenergebnis

Die Rückausnahme des § 8 Abs. 2 S. 2 TDG findet keine Anwendung auf Auskunftsansprüche. Somit können sich Access Provider auch in Bezug auf Auskunftspflichten auf die Haftungsfreistellungen des TDG berufen. Der Access Provider kann daher selbst in den Fällen, in denen er nach den allgemeinen Vorschriften als unmittelbarer Störer zu qualifizieren wäre, nicht auf Auskunft (gem. § 101a UrhG) in Anspruch genommen werden.

5. Erforderlichkeit einer gerichtlichen oder behördlichen Anordnung

Geht man – entgegen der hier vertretenen Auffassung – davon aus, dass Auskunftsansprüche vom Anwendungsbereich des § 8 Abs. 2 S. 2 TDG erfasst werden und der Access Provider somit hinsichtlich dieser Ansprüche nicht privilegiert wäre, könnte man weiterhin die Frage aufwerfen, ob die Rechteinhaber überhaupt befugt wären, zivilrechtliche Ansprüche unmittelbar gegen die Provider durchzusetzen. Zweifel an einer solchen Befugnis bestehen angesichts des Wortlauts der – dem § 8 Abs. 2 S. 2 TDG zugrunde liegenden – Bestimmungen der Art. 12 Abs. 3, 13 Abs. 2, 14 Abs. 3 ECRL. Danach besteht eine Verpflichtung zur Abstellung bzw. Verhinderung von Rechtsgutverletzungen nämlich nur aufgrund einer gerichtlichen oder behördlichen Anordnung.

Gegen ein solches Anordnungserfordernis wird hervorgebracht, dass der Wortlaut des § 8 Abs. 2 S. 2 TDG eine solche Beschränkung gerade nicht vorsehe.[521] Zudem sei das in der ECRL verankerte Erfordernis einer gerichtlichen oder behördlichen Kontrolle lediglich als Voraussetzung für eine strafrechtliche Sanktion zu interpretieren. Für die Geltendmachung

---

[518] Sieber/Höfinger, a.a.O.

[519] So auch OLG Hamburg, Urt. v. 28.4.2005 – 5 U 156/04, MMR 2005, 453, 456 = CR 2005, 512; Sieber/Höfinger, a.a.O.

[520] Sieber/Höfinger, a.a.O.

[521] Stadler, Haftung, S. 99; Spindler, in: Spindler/Schmitz/Geis, § 8 TDG, Rn. 16.

zivilrechtlicher Ansprüche könne dies bereits deshalb nicht durchdringen, weil dem materiellen Zivilrecht ein solcher richterlicher oder behördlicher Vorbehalt grundsätzlich fremd sei.[522]

Diese Auffassung kann sich neben dem Wortlaut des § 8 Abs. 2 S. 2 TDG zunächst auch auf Erwägungsgrund 45 der ECRL berufen. Darin wird ausgeführt, dass solche Anordnungen *„insbesondere"* von Gerichten oder nationalen Behörden erlassen werden können. Insofern ließe sich argumentieren, dass es des Zusatzes *„insbesondere"* nicht bedurft hätte, wenn die von den Haftungsprivilegierungen ausgenommenen Ansprüche stets nur mittels einer gerichtlichen oder behördlichen Anordnung geltend gemacht werden könnten. Erwägungsgrund 45 der ECRL spricht somit eher dafür, dass diese Ansprüche auch unmittelbar geltend gemacht werden können.

Andererseits ist jedoch zu berücksichtigen, dass die Formulierung des Erwägungsgrundes 45 keinen Einzug in den Wortlaut der Bestimmungen der ECRL gehalten hat. Diese sehen explizit eine behördliche oder gerichtliche Anordnung als zwingende Voraussetzung für die Geltendmachung von Ansprüchen vor, die nicht von den Haftungsprivilegierungen erfasst werden. Angesichts dessen ist zu bezweifeln, dass der Wortlaut dieser Bestimmungen allein durch Erwägungsgrund 45 relativiert wird. Ferner ist zu beachten, dass die Verantwortlichkeitsregeln der ECRL eine Vollharmonisierung des Haftungsrechts vorsehen. Daher ist es den Mitgliedstaaten untersagt, den Diensteanbieter einer strengeren als in der Richtlinie vorgesehenen Haftung zu unterwerfen.[523] Dementsprechend darf auch das durch die Richtlinie vorgegebene Mindestmaß an Privilegierung der Access Provider nicht durch § 8 Abs. 2 S. 2 TDG herabgesetzt werden. Für die Annahme, dass der deutsche Gesetzgeber durch den Verzicht auf das Erfordernis einer behördlichen oder gerichtlichen Anordnung zulasten der Access Provider von den Vorgaben der ECRL abgewichen ist, sprechen jedoch die dadurch bedingten Haftungsrisiken. Denn gerade im Bereich des Urheberrechts ist es mitunter notwendig, eine umfassende Recherche zu betreiben, um die Urheberrechtswidrigkeit einer Nutzungshandlung und damit die Berechtigung des Anspruchs eines Rechteinhabers beurteilen zu können. Da der Access Provider eine solche Recherche nicht leisten kann, andererseits jedoch zum Handeln gezwungen ist, wenn derartige Ansprüche an ihn herangetragen werden, sieht er sich erheblichen Haftungsrisiken ausgesetzt. Da dieses Haftungsrisiko entfallen würde, wenn diese Ansprü-

[522] Wiebe, MR 2005, Beilage zu Heft 4, S. 8.

[523] Vgl. Amtl. Begründung zum EGG, BT-Drs. 14/6098, S. 22; Spindler, in: Spindler/Schmitz/Geis, vor § 8 TDG, Rn. 10.

che nur aufgrund einer gerichtlichen oder behördlichen Anordnung geltend gemacht werden könnten, ist insofern von einer unzulässigen Haftungsverschärfung zulasten der Access Provider auszugehen.

Vor diesem Hintergrund wird auch im Rahmen der bevorstehenden Umsetzung des Telemediengesetzes, in das die Haftungsregeln der §§ 9-11 TDG unverändert übernommen werden sollen, gefordert, in den Wortlaut dieser Bestimmungen aufzunehmen, dass sich die nicht von den Privilegierungen erfassten Ansprüche entweder nur mittels gerichtlicher oder behördlicher Anordnung oder allenfalls bei offensichtlichen Rechtsverletzungen unmittelbar durchsetzen lassen sollen.[524] Selbst eine Abkehr vom Anordnungserfordernis bei offensichtlichen Rechtsverletzungen kann jedoch in Bezug auf Access Provider nicht überzeugen. Dagegen lässt sich ein Argument anführen, das aus der Haftungsprivilegierung des § 10 TDG für das Caching folgt. So ergibt sich aus § 10 S. 1 Nr. 5 TDG, dass der Access Provider die auf seinem Proxy-Cache-Server bereitgehaltene Informationen nicht bereits dann entfernen oder sperren muss, wenn diese offensichtlich rechtswidrig sind, sondern nur dann, wenn dies durch ein Gericht oder eine Verwaltungsbehörde angeordnet wurde. Würde man hingegen im Rahmen des § 8 Abs. 2 S. 2 TDG eine solche Anordnung für nicht erforderlich halten, so käme man zu dem widersprüchlichen Ergebnis, dass gegen den Access Provider einerseits Ansprüche auf Entfernung und Sperrung von Informationen geltend gemacht werden könnten, dieser jedoch andererseits dieselben Informationen gem. § 10 TDG bis zu einer gerichtlichen oder behördlichen Anordnung weiterhin auf seinem Proxy-Cache-Server zum Abruf bereithalten dürfte.

Die Regelung des § 8 Abs. 2 S. 2 TDG ist daher richtlinienkonform dahingehend auszulegen, dass Ansprüche, die den Filter des § 8 Abs. 2 S. 2 TDG durchlaufen, nur mittels einer gerichtlichen oder behördlichen Anordnung geltend gemacht werden können.[525] Dass der Gesetzgeber ein solches Verfahren zur Durchsetzung dieser Ansprüche bisher nicht geregelt hat, spricht darüber hinaus nicht gegen diese Annahme, sondern für ein Versäumnis seitens des nationalen Gesetzgebers.

---

[524] Stellungnahme des BITKOM zum Entwurf eines Telemediengesezes v. 12.5.2005, S. 6, abrufbar unter: http://www.bitkom.org/files/documents/050512_BITKOM-Stellungnahme_TMG_und_9_RAeStV.pdf.

[525] So offenbar auch Hoeren, Access Provider, Rn. 628, der ohne nähere Begründung von einem Anordnungserfordernis ausgeht.

F. Ergebnis

Die gesetzlichen Haftungsprivilegierungen des TDG/MDStV sind als (nachträglicher) Filter zu verstehen, der eine nach den allgemeinen Regeln begründete Haftung von Diensteanbietern ausschließt. Diese Regeln sind auch in der Lage, den urheberrechtlichen Haftungsmaßstab zu modifizieren. Der Access Provider kann sich als Diensteanbieter i.S.d. § 3 Nr. 1 TDG auf die Haftungsprivilegierungen der §§ 9, 10 TDG berufen. Diese sehen eine vollumfängliche Haftungsprivilegierung des Access Providers vor, die auch durch eine Inkenntnissetzung von Rechtsverletzungen nicht erschüttert werden kann. Auch Auskunftsansprüche werden von dieser Haftungsprivilegierung erfasst. Insbesondere lassen sich diese nicht unter die Rückausnahmebestimmung des § 8 Abs. 2 S. 2 TDG fassen. Zudem ließen sich nicht privilegierte Ansprüche auch nur mittels einer gerichtlichen oder behördlichen Anordnung durchsetzen. Festzuhalten bleibt, dass die Durchsetzung einer nach den allgemeinen Regeln – wie z.B. nach § 101a UrhG – begründeten Auskunftspflicht des Access Providers zumindest an den Haftungsprivilegierungen des TDG scheitert.

5. Teil: Entgegenstehende Geheimschutzvorschriften

Sofern man – entgegen der hier vertretenen Auffassung – davon ausgeht, dass den Rechteinhabern ein Auskunftsanspruch zusteht und dieser auch den Filter des TDG passiert,[526] ist weiterhin zu klären, ob einer Auskunftserteilung Geheimschutzvorschriften in Gestalt von datenschutzrechtlichen Bestimmungen oder dem Fernmeldegeheimnis entgegenstehen. Sollte dies der Fall sein, wäre der Anspruch auch wegen Verstoßes gegen ein Verbotsgesetz gem. § 275 BGB ausgeschlossen (rechtliche Unmöglichkeit).[527]

A. Vereinbarkeit einer Auskunftserteilung mit dem Datenschutzrecht

I. Grundzüge des Datenschutzrechts

Datenschutzrechtliche Regelungen sind nicht einheitlich in einem Gesetzeswerk normiert, sondern in einer Vielzahl von Gesetzen verstreut. Neben dem Bundesdatenschutzgesetz (BDSG) und den spezifischen Landesdatenschutzgesetzten (LDSG) gibt es eine Reihe von bereichsspezifischen Vorschriften. Von diesen sind vorliegend insbesondere das TK-Datenschutzrecht nach den §§ 91 ff. TKG[528] sowie die datenschutzrechtlichen Regelungen für Tele- und Mediendienste nach dem TDDSG/MDStV von Bedeutung sind. Letztere sollen, wie oben bereits ausgeführt, alsbald in das geplante Telemediengesetz überführt werden.

Zur Systematik zwischen den verschiedenen Gesetzeswerken ist anzumerken, dass die bereichsspezifischen Vorschriften in ihrem Regelungsbereich jeweils Vorrang vor den Regelungen des BGSG und der LDSGe genießen (§§ 1 Abs. 2 TDDSG, 91 TKG, 16 Abs. 2 MDStV). Dies bedeutet im Umkehrschluss zugleich, dass die allgemeinen Vorschriften anwendbar bleiben, sofern die bereichsspezifischen Vorschriften für eine bestimmte Frage keine abschließende Regelung vorsehen.[529]

---

[526] So LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, CR 2005, 136, 137 f. = MMR 2005, 55; LG Köln, Urt. v. 28.7.2004 – 28 O 301/04, ZUM 2005, 236, 238 ff.; Czychowski, MMR 2004 514, 516 f.; Nordemann/Dustmann, CR 2004 380, 384 f.

[527] Kitz ZUM 2005, 298, 301; Sieber/Höfinger, MMR 2004, 575, 583 sprechen sich hingegen für einen Vorrang des Datenschutzrecht nach den Grundsätzen der Normenkollision aus, Spindler/Dorschel, CR 2006, 341, 342 wollen dieses Ergebnis bereits aus dem Gemeinschaftsrecht ableiten.

[528] Durch das Gesetz v. 22.6.2004, BGBl. I 2004, S. 1190, wurden die Regelungen des TKG neu gefasst und der bisher im TDDSV geregelte Datenschutz in das TKG übernommen.

[529] Hoeren, Access Provider, Rn. 29; Roßnagel, in: Roßnagel, Datenschutzrecht, Teil 7.9., Rn. 36.

Datenschutzrechtliche Vorschriften greifen immer dann ein, wenn personenbezogene Daten betroffen sind. Darunter sind nach § 3 Abs. 1 BDSG *„Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“* zu verstehen. Im Gegensatz zu natürlichen Personen unterfallen juristische Personen jedoch nur bezüglich Telekommunikationsdaten und dem Fernmeldegeheimnis dem Schutzbereich des Datenschutzrechts.[530] Alle datenschutzrechtlichen Regelungen sind durch gemeinsame, rechtsgebietsübergreifende Prinzipien geprägt.[531] Nach dem Prinzip des Verbots mit Erlaubnisvorbehalt ist die Erhebung, Verarbeitung oder Nutzung dieser Daten grundsätzlich verboten, sofern nicht ausnahmsweise eine Einwilligung des Betroffenen vorliegt oder eine gesetzliche Vorschrift diese Nutzung erlaubt oder anordnet.[532] Weiterhin unterliegen personenbezogene Daten dem Prinzip der Datensparsamkeit und Datenvermeidung sowie einer strengen Zweckbindung.[533]

II. Anwendbarkeit des Datenschutzrechts im Rahmen von Auskunftsersuchen

Voraussetzung für das Eingreifen datenschutzrechtlicher Bestimmungen im Rahmen von Auskunftsersuchen ist also zunächst, dass durch diese personenbezogene Daten tangiert werden, also Daten, nach denen die Identität eines Betroffenen zumindest bestimmt werden kann. In dieser Hinsicht ist zunächst zwischen den beteiligten Parteien, also den Access Providern und den Rechteinhabern, zu differenzieren.

1. Anwendbarkeit des Datenschutzrechts auf Access Provider

Betrachtet man den Personenbezug der betroffenen Daten zunächst aus der Sicht des Access Providers, so ist dieser bei Auskunftsersuchen eindeutig zu bejahen. Dies trifft zunächst auf die beim Access Provider gespeicherten persönlichen Angaben wie Name und Anschrift der Nutzer zu,[534] auf dessen Preisgabe die Auskunftsbegehren gerichtet sind. Zudem weisen für den Access Provider auch die von ihm vergebenen (dynamischen oder statischen) IP-Adressen einen Personenbezug auf, da der Provider diese Adressen bestimmten Nutzern zuordnen kann.[535]

---

[530] Hoeren, Access Provider, Rn. 9.
[531] Ausführlich dazu Hoeren, Access Provider, Rn. 9 ff.
[532] Klesczewski, in: Säcker, TKG, § 91, Rn. 14.
[533] Klesczewski, in: Säcker, TKG, § 91, Rn. 23.
[534] Vgl. Klesczewski, in: Säcker, TKG, § 91, Rn. 21.
[535] Hoeren, Access Provider, Rn. 13.; Schaar, Datenschutz im Internet, Rn. 171.

2. Anwendbarkeit des Datenschutzrechts auf Rechteinhaber

Fraglich ist hingegen, ob auch die Rechteinhaber datenschutzrechtliche Vorschriften zu beachten haben, wenn sie die IP-Adressen potentieller Rechtsverletzer generieren und diese, verbunden mit dem Auskunftsbegehren, an die Access Provider weiterleiten. Für die Rechteinhaber ist der Personenbezug von IP-Adressen jedoch regelmäßig zu verneinen, da diese, anders als die Access Provider, nicht in der Lage sind, diese Adresse einem bestimmten oder bestimmbaren Nutzer zuzuordnen. Eine solche Zuordnung könnte allenfalls dann gelingen, wenn die IP-Adresse mit einer Domain verbunden ist, durch die Rückschlüsse auf deren Betreiber gezogen werden können.[536] Dass solche unmittelbaren Rückschlüsse bei den hier fraglichen Auskünften auszuschließen sind, liegt auf der Hand, da die Auskunftsbegehren ansonsten entbehrlich wären. Für die Rechteinhaber ist der Personenbezug von IP-Adressen in den vorliegenden Konstellationen daher zu verneinen.

Teilweise wird jedoch vertreten, dass es sich bei IP-Adressen, unabhängig vom Blickwinkel der Daten verarbeitenden Stelle, stets um personenbezogene Daten handelt.[537] Begründet wird das damit, dass es verhindert werden müsse, dass Daten von Stellen, für die diese Daten keinen Personenbezug aufweisen, gesammelt und an Dritte übermittelt werden können, die wiederum problemlos einen Personenbezug herstellen können. Dies soll zu einer unverhältnismäßigen Einschränkung des Datenschutzrechts führen.[538] Nach dieser Auffassung dürften also auch die Rechteinhaber nur aufgrund einer gesetzlichen Ermächtigung IP-Adressen generieren und weiterleiten.

Diese Ansicht lässt jedoch den Umstand unberücksichtigt, dass für den Dritten, in diesem Fall für den Access Provider, sehr wohl die Datenschutzgesetze eingreifen, sofern diesem Daten übermittelt werden, die für ihn einen Personenbezug aufweisen. So darf der Access Provider diese Daten seinerseits nur dann verarbeiten oder übermitteln, wenn eine gesetzliche Regelung dies erlaubt. Eine Verkürzung des Datenschutzrechts wäre somit nur dann zu befürchten, wenn man dem Access Provider einen Rechtsbruch in der Hinsicht unterstellen würde, dass sich dieser nicht an zwingende datenschutzrechtliche Regelungen hält.[539] Weiterhin lässt sich gegen diese Auffassung anführen, dass nicht ersichtlich ist, warum diejeni-

[536] Hoeren, Access Provider, Rn. 12.
[537] So Schaar, Datenschutz im Internet, Rn. 174; Dix, DuD 2003, 234, 235.
[538] Schaar, Datenschutz im Internet, Rn. 174.
[539] Vgl. Schmitz, in: Spindler/Schmitz/Geis, § 1 TDDSG, Rn. 28.

gen datenschutzrechtlichen Restriktionen unterliegen sollten, von denen keine Gefahr für eine Beeinträchtigung datenschutzrechtlicher Belange ausgeht, weil sie diese Daten keiner bestimmten oder bestimmbaren Person zuordnen können. In diesen Fällen dürfte bereits der Schutzzweck des Datenschutzrechts nicht tangiert sein.[540] Vorzugswürdigung ist daher die oben ausgeführte Auffassung, nach der hinsichtlich der Frage des Eingreifens datenschutzrechtlicher Regelungen allein auf den Blickwinkel der datenverarbeitenden Stelle abzustellen ist. Nur wenn diese ohne unverhältnismäßig großen Aufwand einen Personenbezug herstellen kann, liegt ein personenbezogenes Datum vor, das die Anwendbarkeit der Datenschutzgesetze begründet.[541] Sofern die Rechteinhaber dazu nicht in der Lage sind, unterliegen sie hinsichtlich des Umgangs mit IP-Adressen auch keinen datenschutzrechtlichen Beschränkungen.

III. Datenschutzrechtliche Einordnung des Access Providers

Da zumindest Access Provider bei Auskunftsverlangen der Rechteinhaber datenschutzrechtliche Vorschriften zu beachten haben, stellt sich die Frage, nach welchem konkreten Gesetzeswerk sich die Zulässigkeit der Auskunftserteilung beurteilt. In Betracht kommen die datenschutzrechtlichen Regelungen für Teledienste nach dem TDDSG sowie das TK-Datenschutzrecht nach den §§ 91 ff. TKG.

Nach dem Evaluationsbericht der Bundesregierung zum IuKDG soll Access Providing in den Anwendungsbereich des TDDSG fallen, weil zumindest die vom Access Provider bereitgestellten Protokollfunktion, insbesondere die Vergabe von IP-Adressen, als Teledienste zu qualifizieren seien.[542] Nach Kitz folgt die Anwendbarkeit des TDDSG auf Access Provider hingegen bereits daraus, dass auch der Zugangsvermittler von der Begriffsdefinition des Diensteanbieters in § 2 Nr. 1 Alt. 2 TDDSG erfasst wird.[543]

Der Auffassung der Bundesregierung steht – nach der hier vertretenen Ansicht – entgegen, dass der Access Provider keinen Tele-, sondern – einen diesen Diensten vorgeschalteten – Telekommunikationsdienst betreibt.[544] Kitz kann man indes entgegenhalten, dass allein die Definition des Diensteanbieters gem. § 2 Nr. 1 Alt. 2 TDDSG keine Anwendbarkeit des

[540] Vgl. Dammann, in: Simitis, § 3, Rn. 31; Hoeren/Sieber/Sieber, Teil 19. Rn. 555.
[541] So auch Gola/Schomerus, § 3, Rn. 9; Hoeren, Access Provider, Rn. 11.
[542] Vgl. BT-Drs. 14/1191, S. 7.
[543] Kitz, ZUM 2005, 298, 301.
[544] Siehe oben, 4. Teil D. II.

TDDSG begründen kann. Dessen Anwendungsbereich bestimmt sich nämlich nicht nach § 2 TDDSG, sondern nach § 1 TDDSG und setzt insofern zwingend die Erbringung eines Teledienstes voraus.

Vorzuziehen ist eine funktionsbezogene Betrachtungsweise. Danach ist beim rein technischen Transportvorgang von Daten die Anwendbarkeit des TKG gegeben, während das TDDSG einschlägig ist, sobald Daten auf der Anwendungsebene erhoben werden.[545] Demnach ergibt sich z.B. dann die Anwendbarkeit des TDDSG, wenn es um die Frage geht, ob der Inhalt einer Suchmaschinenabfrage gespeichert werden darf.[546] Beim Access Providing steht hingegen in erster Linie die Unterhaltung einer funktionsfähigen Schnittstelle zum Internet im Vordergrund, um Daten für den Kunden zu senden oder zu empfangen. Diese Tätigkeit beschränkt sich auf den Transportvorgang und ist daher nicht auf der Anwendungs-, sondern auf der Transportebene anzusiedeln. Somit sind hinsichtlich des Access Providing die Regelungen des TK-Datenschutzrechts einschlägig.[547]

Diese Zuordnung des Access Providers zum TK-Datenschutzrecht wird zudem durch den Entwurf des Telemediengesetzes (TMG) bestätigt. So wird in § 11 Abs. 3 TMG-E ausgeführt, dass für Telemedien, die überwiegend aus der Übertragung von Signalen über Telekommunikationsnetze bestehen, hinsichtlich der Erhebung und Verwendung von personenbezogenen Daten vorrangig die Regelungen des TK-Datenschutzrechts eingreifen. Ausweislich der Entwurfsbegründung soll dies insbesondere für Access Provider gelten.[548]

IV. Datenschutzrechtliche Zulässigkeit auskunftsrelevanter Handlungen

Nach dem Prinzip des Verbots mit Erlaubnisvorbehalt ist für eine zulässige Auskunftserteilung seitens des Access Providers erforderlich, dass alle auskunftsrelevanten Nutzungen der IP-Adressen entweder durch eine Einwilligung des betroffenen Nutzers oder aber durch eine gesetzliche Ermächtigungsgrundlage gedeckt sind. Dies betrifft die Speicherung von IP-Adressen in den Log-Dateien, die Zuordnung der IP-Adresse zu einem bestimmten Nutzer sowie die anschließende Übermittlung dessen persönlicher Daten an die Rechteinhaber. Zumindest an einer Einwilligung des

[545] Beck-TKG/Büchner, § 89 TKG, Rn. 13; Hoeren/Sieber/Schmitz, Teil 16.4, Rn. 17 ff.; Schaar, RDV, 2003, 59, 60.
[546] Schaar, RDV, 2003, 59, 61.
[547] So auch AG Darmstadt, Urt. v. 30.6.2005 – 300 C 397/04, MMR 2005, 634, 635.
[548] Begr. des Gesetzesentwurfs zum TMG, a.a.O. (Fn. 402), S. 18.

Nutzers wird es regelmäßig fehlen. Für eine solche wäre weiterhin erforderlich, dass der Betroffene der entsprechenden Datenverarbeitung ausdrücklich und ohne jeglichen Zwang zugestimmt hat.[549] Aus diesem Grund wären auch standardisierte Einwilligungserklärungen in die Speicherung und Auskunftserteilung in den Allgemeinen Geschäftsbedingungen der Access Provider als unwirksam zu betrachten.[550]

Maßgeblich wird es daher auf die gesetzliche Erlaubnissätze der §§ 91 ff. TKG ankommen. Das TKG differenziert zwischen der Erhebung und Verwendung von Bestands- und Verbindungs- bzw. Verkehrsdaten[551]. Als Bestandsdaten werden Daten bezeichnet, die für die Begründung und inhaltliche Ausgestaltung des Vertragsverhältnisses erforderlich sind (§ 3 Nr. 3 TKG). Dies betrifft insbesondere Angaben zur Person des Nutzers sowie zu den Vertragsmerkmalen.[552] Verkehrsdaten sind dagegen Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden (§ 3 Nr. 30 TKG). Die Zulässigkeit der Nutzung von Bestandsdaten beurteilt sich nach § 95 TKG, die von Verkehrsdaten nach § 96 TKG.

1. Zulässigkeit der Speicherung von IP-Adressen

Für die Rechteinhaber ist es im Rahmen von Auskunftsersuchen von essentieller Bedeutung, dass die den Nutzern zugewiesenen IP-Adressen beim Access Provider noch über das jeweilige Verbindungsende hinaus gespeichert werden, da ansonsten zumindest eine nachträgliche Identifizierung des potentiellen Rechtsverletzers bereits aus tatsächlichen Gründen unmöglich ist. Sofern diese Daten beim Access Provider über das Verbindungsende hinaus gespeichert werden, ist weiterhin zu beachten, dass diese Daten nur dann auch für Auskunftsersuche zur Verfügung stehen, wenn sich deren Speicherung als rechtmäßig darstellt. Mithin muss eine derartige Speicherung von einer gesetzlichen Ermächtigungsgrundlage gedeckt sein. In dieser Hinsicht ist zunächst zu klären, ob es sich bei den IP-Adressen um Bestandsdaten i.S.d. § 95 TKG oder aber um Verbindungsdaten i.S.d. § 96 TKG handelt, da für diese beiden Kategorien unterschiedliche Anforderungen an eine zulässige Speicherung gestellt werden. So sind Verkehrsdaten nach § 96 Abs. 2 TKG unverzüglich nach dem Ende der Verbindung

[549] Schaar, Datenschutz im Internet, Rn. 555 f.
[550] Vgl. Schaar, Datenschutz im Internet, Rn. 593.
[551] Der Begriff der Verkehrsdaten wurde im Rahmen der TKG-Novelle 2004 durch den Begriff der Verkehrsdaten ersetzt, vgl. Begr. des RegE, BT-Drs. 15/2316, S. 89.
[552] Klesczewski, in: Säcker, TKG, § 95, Rn. 3.

zu löschen, sofern sie nicht zum Aufbau einer weiteren Verbindung oder für die in §§ 97, 99, 100 und 101 TKG genannten Zwecke erforderlich sind. Die Speicherung von Bestandsdaten ist gem. § 95 Abs. 1 TKG hingegen zumindest während der gesamten Vertragsdauer zulässig, sofern die Speicherung dieser Daten für die weitere Erfüllung des Vertragsverhältnisses erforderlich ist. Zu klären ist daher zunächst, wie statische und dynamische IP-Adressen in dieser Hinsicht zu kategorisieren sind.

a) Statische IP-Adressen

Statische IP-Adressen haben – wie dynamische IP-Adressen – zunächst eine technische Funktion, da sie dem Nutzer eine Kennung verleihen. Darüber hinaus weisen statische IP-Adressen jedoch auch eine vertragliche Komponente auf. Einer solchen Adresse ist nämlich immanent, dass sich der Access Provider verpflichtet hat, dem Nutzer bei jeder Einwahl ins Internet dieselbe IP-Adresse zuzuweisen.[553] Statische IP-Adressen sind somit auch Vertragsmerkmale und als solche den Bestandsdaten i.S.d. § 3 Nr. 3 TKG zuzuschlagen.[554] Da dem Access Provider diese IP-Adresse vorliegen muss, damit er diese dem Nutzer bei jeder erneuten Einwahl zuweisen kann, ist deren Speicherung für die weitere Vertragserfüllung auch erforderlich i.S.d. § 95 TKG. Somit ist eine über das jeweilige Verbindungsende hinausgehende Speicherung von statischen IP-Adressen zulässig.[555]

b) Dynamische IP-Adressen

Hat der Nutzer mit dem Access Provider hingegen keine vertragliche Vereinbarung über die Vergabe einer bestimmten (statischen) IP-Adresse getroffen, wird diesem bei jeder Einwahl ins Internet eine (wechselnde) dynamische IP-Adresse aus dem Adressenpool des Access Providers zugewiesen. Die Funktion von dynamischen IP-Adressen beschränkt sich auf die technische Seite. Diese werden lediglich zur Begründung des Zugangs zum Internet sowie zur Datenübertragung im Rahmen der jeweiligen Sitzung benötigt.[556] Sie sind daher ausschließlich als Kennungen i.S.d. § 96 Abs. 1 Nr. 1 TKG zu qualifizieren und somit den Verkehrsdaten zuzu-

[553] Vgl. Einzinger/Schubert/Schwabl/Wessely/Zykan, MR 2005, 113, 114; Wiebe, MR 2005, Beilage zu Heft 4, S. 10.
[554] Vgl. Schaar, RDV 2003, 59, 62; Bär, MMR 2002, 358, 359.
[555] Vgl. Schmitz, in: Spindler/Schmitz/Geis, § 6 TDDSG, Rn. 88 für die mit § 95 TKG korrespondierende Vorschrift des § 6 TDDSG.
[556] Wiebe, MR 2005, Beilage zu Heft 4, S. 14.

schlagen.[557] Als solche sind sie gem. § 96 Abs. 2 TKG unverzüglich nach dem Ende der Verbindung zu löschen, sofern eine längere Speicherung nicht ausnahmsweise durch eine gesetzliche Ermächtigungsgrundlage gedeckt ist. Im Folgenden ist daher zunächst zu untersuchen, ob eine Ermächtigungsgrundlage für eine solche vorsorgliche Speicherung von dynamischen IP-Adressen besteht. Sollte dies nicht der Fall sein, wird die Frage zu beantworten sein, ob der Access Provider nicht zumindest dann, wenn er während der Internetsitzung eines Nutzers seitens der Rechteinhaber auf Rechtsverletzungen hingewiesen wird, berechtigt oder verpflichtet ist, die dem Nutzer zugewiesene IP-Adresse zu speichern, damit diese den Rechteinhabern für weitere Rechtsverfolgungsmaßnahmen zur Verfügung steht (sog. anlassbezogene Speicherpflicht).

aa) Vorsorgliche Speicherung für Abrechnungs- und Rechtsverfolgungszwecke

Als Ermächtigung für eine vorsorgliche Speicherung von IP-Adresen kommt zunächst § 97 Abs. 3 TKG in Betracht. Danach ist die Speicherung von Verkehrsdaten zulässig, sofern diese zur Entgeltermittlung und Entgeltabrechnung benötigt werden. Ob auch die Speicherung von IP-Adressen für diese Zwecke notwendig ist, wird kontrovers beurteilt und ist insbesondere in Bezug auf (zeit- und volumenunabhängige) Flatrates umstritten.

So hat das Regierungspräsidium Darmstadt als Aufsichtsbehörde von T-Online entschieden, dass eine über das Verbindungsende hinausgehende Speicherung von IP-Adressen zulässig sei, weil der Zugangsanbieter nur mittels der IP-Adresse die kostenpflichtige Erbringung seiner Leistung korrekt und durchsetzbar nachweisen könne.[558] Darüber hinaus könne durch die Protokollierung von IP-Adressen einerseits der Umfang der Leistungserbringung dargelegt und andererseits eine vom Kunden behauptete Leistungsstörung widerlegt werden.[559] Dies gelte auch für Flatrate-Kunden, da diese z.B. auch eine Verbindung über Modem, ISDN oder GSM herstellen

---

[557] Begr. des RegE zum TKG, BT-Drs. 15/2316, S. 89; Klesczewski, in: Säcker, TKG, § 96, Rn. 5; zur Frage, ob auch statische IP-Adressen Verbindungsdaten i.S.d. § 96 TKG sein können, unten 5. Teil B. I. 2.

[558] RegPräs. Darmstadt, MMR 2003, 213, 213 =DuD, 2003, 177; zuständige Aufsichtsbehörde wäre in diesem Fall indes nicht das Reg.Präs. sondern der Bundesdatenschutzbeauftrage gewesen, vgl. Schmitz, Anm. zur Entscheidung des RegPräs Darmstadt, MMR 2003, 214, 215.

[559] RegPräs. Darmstadt, a.a.O.

könnten, welche nicht vom Pauschaltarif abgedeckt wäre.[560] Der von der Speicherpraxis von T-Online betroffene Nutzer reichte daraufhin Klage beim Amtsgericht Darmstadt ein. Dieses folgte in weiten Teilen der Argumentation des Nutzers. So hielt das Gericht der Auffassung des RegPräs. entgegen, dass eine Speicherung zu Rechtsverfolgungszwecken bereits nicht mit dem Wortlaut des § 97 Abs. 3 TKG vereinbar sei. Danach seien eben nur Speicherungen von Daten zur Ermittlung des Entgelts zulässig, nicht jedoch Speicherungen zum Nachweis der Richtigkeit solcher Abrechnungen.[561] Die Argumentation des RegPräs. könne bereits deshalb nicht überzeugen, weil damit in letzter Konsequenz selbst die Speicherung von Inhaltsdaten gerechtfertigt werden könnte.[562] Weiterhin wies das Amtsgericht darauf hin, dass das gesetzliche Verbot der Datenspeicherung zu Beweiszwecken den Providern auch hinsichtlich der Durchsetzbarkeit von Forderungen nicht zum Nachteil gereiche. Denn nach § 16 Abs. 2 TKV treffe den Anbieter keine Nachweispflicht für Einzelverbindungen, die aufgrund rechtlicher Verpflichtungen gelöscht wurden. Sofern die Berechtigung einer Forderung bestritten werde, müsse der Anbieter lediglich nachweisen, dass ein Vertrag besteht und sein Abrechnungssystem ordnungsgemäß funktioniert, um den Beweis des ersten Anscheins für sich in Anspruch nehmen zu können.[563] Somit bedürfe es auch zur Geltendmachung einer Entgeltforderung keiner Speicherung von IP-Adressen.[564]

Während diesen Ausführungen des Amtsgerichts uneingeschränkt beizupflichten ist, muss dem Gericht jedoch widersprochen werden, soweit es zumindest eine Speicherung von IP-Adressen bis zum Abschluss der Entgeltermittlung für zulässig hält.[565] Denn dies würde voraussetzen, dass die Speicherung von IP-Adressen zur Entgeltermittlung auch erforderlich ist. Das ist jedoch weder bei Flatrates noch bei sonstigen Vertragsbindungen oder Internet-by-Call-Verbindungen der Fall.[566] Liegt eine Vertragsbindung vor, so erhält der Nutzer in der Regel eine Nutzerkennung und ein Passwort, mittels derer er sich bei der Einwahl gegenüber dem Provider

[560] RegPräs. Darmstadt, a.a.O.
[561] AG Darmstadt, Urt. v. 30.6.2005 – 300 C 397/04, MMR 2005, 634, 635.
[562] AG Darmstadt, a.a.O.
[563] AG Darmstadt, a.a.O, 636; kritisch in Bezug auf volumenabhängige Abrechnungsmodelle bei Web-Hosting-Verträgen, OLG Düsseldorf, Urt. v. 26.2.2003 – 18 U 192/02, JurPC Web-Dok. 156/2003, Abs. 13 ff. = CR 2003, 581.
[564] AG Darmstadt, a.a.O., 636; so auch Schmitz, in: Spindler/Schmitz/Geis, § 6 TDDSG, Rn. 86.
[565] AG Darmstadt, a.a.O., 635.
[566] Roßnagel, in: Roßnagel, Handbuch Datenschutzrecht, Teil 7.9, Rn. 79; Schaar, Datenschutz im Internet, Rn. 446.

autorisiert. Der Nutzungsvorgang wird sodann in den Log-Dateien des Providers der Kundenummer oder Buchungskontonummer des Nutzers zugeordnet. Wird das Entgelt im Rahmen dieser Vertragsbindung nach der Dauer der Internetsitzung berechnet, bedarf es zu dessen Ermittlung lediglich der Speicherung der Nutzerkennung und der Dauer der Verbindung bzw. bei volumenabhängigen Tarifen der Speicherung des übertragenen Datenvolumens, nicht jedoch auch der Speicherung der IP-Adresse.[567] Bei volumen- und zeitunabhängigen Flatrate-Verträgen ist – entgegen der Ansicht des Amtsgerichts – überhaupt keine über das Ende der Verbindung hinausgehende Speicherung von Nutzerdaten zur Entgeltermittlung notwendig.[568] Ähnlich verhält es sich bei Internet-by-Call-Verbindungen, deren Entgelt über die herkömmliche Telefonrechnung abgegolten wird. Hier reicht es zur Entgeltermittlung aus, wenn bei der Einwahl des Nutzers dessen Telefonnummer und die Dauer der Sitzung gespeichert werden.[569] Festzuhalten bleibt somit, dass die Speicherung von IP-Adressen für die Entgeltermittlung nicht erforderlich ist und diese Daten somit gem. § 97 Abs. 3 S. 2 TKG unverzüglich nach dem Verbindungsende zu löschen sind. Demzufolge kann eine vorsorgliche Speicherung von IP-Adressen zumindest nicht auf § 97 TKG gestützt werden.

Dieser Sichtweise hat sich mittlerweile auch das Landgericht Darmstadt[570] angeschlossen, das sich im Rahmen der Berufungsverhandlung mit der Entscheidung des Amtsgerichts auseinanderzusetzen hatte. Das Gericht hob darin das Urteil des Amtsgerichts auf, weil es ebenfalls zu dem Schluss kam, dass die Speicherung der IP-Adressen von Flatrate-Nutzern für die Entgeltermittlung nicht erforderlich ist und diese Daten somit sofort nach der Beendigung der Verbindung zu löschen sind.[571] Dies gilt darüber hinaus auch dann, wenn der Nutzer einen Einzelverbindungsnachweis nach § 99 TKG beantragt hat. Denn gem. § 99 Abs. 1 S. 1 TKG werden auch im Rahmen eines Einzelverbindungsnachweises nur Daten vorgelegt, die nach § 97 TKG erhoben werden durften.

---

[567] Vgl. Hoeren/Sieber/Schmitz, Teil 16.4, Rn. 128; Roßnagel, in: Roßnagel, Handbuch Datenschutzrecht, Teil 7.9, Rn. 79.

[568] Hoeren/Sieber/Schmitz, Teil 16.4, Rn. 128; Schmitz, Anm. zur Entscheidung des RegPräs Darmstadt, MMR 2003, 214, 216.

[569] Dix, DuD, 2003, 234, 235.

[570] LG Darmstadt, Urt. v. 25.01.2006, Az. 25 S 118/2005, abrufbar unter: http://www.datenschutzkontor.com/docs/LG_Darmstadt_Speicherung_IP-Adressen.pdf. = CR 2006, 249 = GRUR-RR 2006, 173.

[571] LG Darmstadt, a.a.O., S. 9.

bb) Vorsorgliche Speicherung zur Missbrauchsbekämpfung

Eine gesetzliche Ermächtigung zur vorsorglichen Speicherung von IP-Adressen könnte sich jedoch aus den Vorschriften zur Datenerhebung in Missbrauchsfällen ergeben. So darf der Diensteanbieter nach § 100 Abs. 3 TKG bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte auch Verkehrsdaten erheben und verwenden, soweit dies zur Aufdeckung oder Unterbindung von Leistungserschleichungen und sonstiger rechtswidriger Inanspruchnahmen von TK-Netzen erforderlich ist. Bereits aus der Tatsache, dass solche Maßnahmen gem. § 100 Abs. 3 TKG zu dokumentieren und dem Bundesbeauftragten für Datenschutz unverzüglich anzuzeigen sind, lässt sich jedoch der Einzelfallcharakter dieser Regelung ableiten, der es verbietet, § 100 Abs. 3 TKG als Ermächtigungsgrundlage für eine allgemeine Vorratsdatenspeicherung anzusehen.[572] Ferner ergibt sich dieses Ergebnis auch daraus, dass ansonsten die differenzierten Löschungspflichten des § 97 TKG schlichtweg überflüssig wären.

Nach Auffassung des RegPräs. Darmstadt soll sich die Zulässigkeit einer vorsorglichen Speicherung von IP-Adressen jedoch zumindest aus § 9 BDSG ergeben, da die Speicherung dieser Daten zur Gewährleistung der Datensicherheit notwendig sei.[573] Dies gelte insbesondere für die Erreichung einer wirksamen Zugriffskontrolle nach Nr. 3 der Anlage zu § 9 BDSG.[574] In dieser Hinsicht bestehen jedoch bereits Zweifel daran, dass § 9 BDSG – als Regelung des allgemeinen Datenschutzrechts – neben den bereichsspezifischen Vorschriften des TDDSG und der §§ 91 ff. TKG überhaupt ein eigener Anwendungsbereich verbleibt.[575] Selbst wenn dies der Fall wäre, dürften dessen Voraussetzungen regelmäßig nicht erfüllt sein. Sinn und Zweck des § 9 BDSG ist nämlich der Schutz der beim Telekommunikationsanbieter gespeicherten Daten vor einem unberechtigten Zugriff durch dessen Nutzer.[576] Diesem Gesetzeszweck würde es jedoch nicht gerecht, wenn man daraus zugleich eine Ermächtigung zur vorsorglichen Speicherung weiterer personenbezogener Daten ableiten würde, hätte dies doch zur Folge, dass auch diese Daten zugleich wieder der Gefahr eines missbräuchlichen Zugriffs ausgesetzt werden.[577] Ferner würde es gera-

---

[572] Vgl. Hoeren/Sieber/Büttgen, Teil 16.3, Rn. 117; zur Frage, ob sich aus aus § 100 Abs. 3 TKG eine anlassbezogene Speicherpflicht ableiten lässt, unten 5.Teil A. IV. 1. b) cc) (2).
[573] RegPräs. Darmstadt, MMR 2003, 213, 214 = DuD, 2003, 177.
[574] RegPräs. Darmstadt, a.a.O.
[575] Näher dazu Dix, DuD 2003, 234, 236.
[576] Dix, DUD 2003, 234, 236.
[577] AG Darmstadt, Urt. v. 30.6.2005 – 300 C 397/04, MMR 2005, 634, 636.

dezu einer Aufhebung der bereichsspezifischen Regelungen des TDDSG und der §§ 91 ff. TKG gleichkommen, wenn man mit dem Reg.Präs. Darmstadt aus § 9 BDSG eine Art Generalerlaubnis zur Datenverarbeitung ableiten würde.[578] Schließlich ist die vorsorgliche Speicherung von Verkehrsdaten auf der Grundlage des § 9 BDSG auch deshalb abzulehnen, weil diese in erheblichem Widerspruch zum Gebot der Datenvermeidung und Datensparsamkeit stünde.[579] Die Regelung des § 9 BDSG ermächtigt damit – wie auch § 100 Abs. 3 TKG – zumindest nicht zur vorsorglichen, sondern allenfalls zu einer einzelfall- und anlassbezogenen Speicherung von Verkehrsdaten.

cc) Anlassbezogene Speicherpflicht nach Aufforderung

Ist eine vorsorgliche Speicherung von dynamischen IP-Adressen somit unzulässig, stellt sich die Frage, ob der Access Provider nicht zumindest zu einer anlassbezogenen Speicherung verpflichtet ist, wenn dieser während einer bestehenden Verbindung des Nutzers seitens der Rechteinhaber auf eine konkrete Rechtsverletzung hingewiesen und angehalten wird, die Nutzerdaten für etwaige Rechtsverfolgungszwecke vorzuhalten. Solche Aufforderungen zur Speicherung von Verkehrsdaten, die auch Quick-Freeze-Order genannt werden, entsprechen – ungeachtet ihrer rechtlichen Zulässigkeit – bereits der gängigen Praxis. So werden Access Provider infolge gesteigerter Rechtsverfolgungsmaßnahmen mittlerweile massenhaft zur Speicherung von Verbindungsdaten angehalten, damit diese den Rechteinhabern für ein weiteres strafrechtliches oder zivilrechtliches Verfahren nicht verlustig gehen. Dieses Prozedere lag auch den Speicheraufforderungen zugrunde, die im Auftrag eines Rechteinhabers von dem Schweizer Dienstleister Logistep an die Abuse-Adressen einiger Access Provider versendet wurden.

(1) Anlassbezogene Speicherpflicht aufgrund Störerhaftung

Logistep begründete die Speicherpflicht des Access Providers damit, dass dieser mit der Speicheraufforderung von konkreten Rechtsverletzungen in Kenntnis gesetzt werde und mit dieser Kenntniserlangung die verschuldensunabhängige Störerhaftung eingreife, die den Provider zur Speicherung der gewünschten Verbindungsdaten verpflichte.[580] Ein Provider, dem innerhalb von zwei Wochen über 500 solcher E-Mails zugingen, darunter

[578] Schmitz, in: Spindler/Schmitz/Geis, § 6 TDDSG, Rn. 86.
[579] Dix, DuD, 2003, 234, 236.
[580] Vgl. LG Flensburg, Urt. v. 25.11.2005 – 6 O 108/05, MMR 2006, 181, 181 f.

167 an einem Tag, was nach eigenen Angaben zu einer Blockierung des E-Mail-Servers führte, erwirkte daraufhin wegen eines Eingriffs in den eingerichteten und ausgeübten Gewerbebetrieb eine einstweilige Verfügung, mit der Logistep weitere Speicheranmahnungen untersagt wurden. Der seitens Logistep beim Landgericht Flensburg dagegen eingelegte Widerspruch hatte keinen Erfolg. Zwar bejahte das Gericht das Eingreifen der Störerhaftung des Access Providers bereits mit der Kenntniserlangung von einer Rechtsverletzung[581] und nicht erst – wie nach der hier vertretenen Auffassung – mit der Verletzung einer Prüf- bzw. Verkehrssicherungspflicht.[582] Zutreffend verneinte es aber eine aus der Störerhaftung resultierende Speicherpflicht, da die Störerhaftung allenfalls einen Unterlassungsanspruch begründe, nicht aber zur Mitwirkung hinsichtlich der Durchsetzung von strafrechtlichen oder zivilrechtlichen Sanktionen verpflichte.[583] Da dieser Auffassung zumindest im Ergebnis zu folgen ist, bleibt festzuhalten, dass sich auch durch eine etwaige Störerhaftung des Access Providers keine anlassbezogene Speicherpflicht von IP-Adressen begründen lässt.

(2) Anlassbezogene Speicherpflicht aus § 100 Abs. 3 TKG

Eine solche anlassbezogene Speicherpflicht könnte sich jedoch über § 100 Abs. 3 TKG konstruieren lassen. Zwar wurde soeben festgestellt, dass § 100 Abs. 3 TKG keine Ermächtigungsgrundlage für eine vorsorgliche Speicherung von IP-Adressen darstellt. Dies könnte sich jedoch hinsichtlich einer anlassbezogenen Speicherung einzelner IP-Adressen anders darstellen. So dürfen nach § 100 Abs. 3 TKG zumindest dann Verkehrsdaten – wie IP-Adressen – gespeichert werden, wenn dies *„zum Aufdecken sowie Unterbinden von Leistungserschleichungen und sonstigen rechtswidrigen Inanspruchnahmen der Telekommunikationsnetze und –dienste erforderlich“* ist. Der Wortlaut des § 100 Abs. 3 TKG lässt zunächst lediglich darauf schließen, dass die Speicherung solcher Daten zulässig ist, wenn diese zur Aufklärung von Verletzungshandlungen benötigt werden, die sich gegen den Telekommunikationsanbieter selbst richten, nicht jedoch auch Speicherungen zum Zwecke der Rechtsverfolgung Dritter erfasst. Allerdings ließe sich vor dem Hintergrund, dass Access Provider ihre Nutzer regelmäßig zur Beachtung fremder Urheberrechte verpflichten, auch argumentieren, dass die Verletzung fremder Urheberrechte zugleich auch eine Überschreitung des vertraglichen Nutzungsrechts darstellt, so dass auch in

[581] LG Flensburg, a.a.O., 181 mit Verweis auf OLG Frankfurt a.M., Urt. v. 25.1.2005 – 11 U 51/05, MMR 2005, 241.
[582] Siehe oben, 2. Teil A. IV. 2. c).
[583] LG Flensburg, a.a.O., 181.

diesen Fällen eine rechtswidrige Inanspruchnahme der Leistungen des Providers vorliegt, die gem. § 100 Abs. 3 TKG zur Speicherung von Verkehrsdaten berechtigt. Selbst wenn man hiervon ausginge, würde sich daraus jedoch noch keine Speicherpflicht des Access Providers ergeben. Denn ausweislich seines klaren Wortlauts (*„darf“*), ist der Telekommunikationsanbieter in diesen Fällen nicht zur Speicherung verpflichtet, sondern lediglich ermächtigt. Mithin stellt § 100 Abs. 3 TKG die Speicherung solcher Daten allein ins Ermessen des Telekommunikationsanbieters. Eine Reduzierung dieses gesetzlich eingeräumten Ermessens auf eine Speicherpflicht für den Fall, dass der Access Provider während einer Verbindung auf die Rechtsverletzung eines Nutzers aufmerksam gemacht und zur Speicherung der fraglichen IP-Adresse aufgefordert wird, kann dieser Regelung – angesichts des auf die Interessen des Telekommunikationsanbieters abstellenden Schutzzwecks – nicht entnommen werden. Mithin lässt sich auch aus § 100 Abs. 3 TKG keine anlassbezogene Speicherpflicht des Access Providers ableiten.

c) Zwischenergebnis

Der Access Provider ist lediglich zur vorsorglichen Speicherung von statischen IP-Adressen berechtigt, da es sich bei diesen um Bestandsdaten handelt, deren Speicherung gem. § 95 Abs. 1 TKG zur Erfüllung des Vertragsverhältnisses erforderlich ist. Nicht zulässig ist hingegen die vorsorgliche Speicherung der regelmäßig vergebenen dynamischen IP-Adressen. Diese stellen Verkehrsdaten i.S.d. § 96 TKG dar. Als solche sind sie gem. § 96 Abs. 2 TKG unverzüglich nach dem Ende der Verbindung zu löschen, da sie weder zur Entgeltermittlung noch zur Missbrauchsbekämpfung erforderlich sind. Weiterhin steht den Rechteinhabern keine Rechtsgrundlage zur Seite, mittels derer sie Access Provider anlassbezogen zur Speicherung einzelner dynamischer IP-Adressen zum Zwecke der Rechtsverfolgung verpflichten können. Es ist also zu konstatieren, dass zumindest Auskunftsersuchen zu dynamischen IP-Adressen regelmäßig bereits deshalb ins Leere gehen, weil die IP-Adressen der Rechtsverletzer für Rechtsverfolgungszwecke nicht – in rechtlich zulässiger Weise – zur Verfügung stehen.

2. Zulässigkeit der Ermittlung des Rechtsverletzers

Weiterhin wäre für eine zulässige Auskunftserteilung erforderlich, dass die Access Provider auch die notwendigen Verknüpfungen dieser IP-Adressen mit den jeweiligen Nutzern herstellen dürfen. Wie eine solche Identifizie-

rung der Nutzer von statten geht, hängt davon ab, ob es sich bei den fraglichen IP-Adressen um dynamische oder statische handelt. Wurde eine dynamische IP-Adresse vergeben, so müssen zur Verknüpfung zwingend die Log-Dateien des Access Providers ausgelesen werden. Bei statischen IP-Adressen kann mitunter bereits ein Blick in die Vertragsunterlagen genügen. In beiden Fällen stellt die Nutzung der IP-Adressen zum Zwecke der Identifizierung des Nutzers jedoch eine Verwendung i.S.d. §§ 95, 96 TKG dar und unterliegt damit hinsichtlich der Zulässigkeit auch den dortigen Beschränkungen. Da die Ermittlung der Identität des Nutzers anhand seiner IP-Adresse jedoch für die Erfüllung des Vertrags zwischen Access Provider und Nutzer nicht erforderlich ist und auch keine andere gesetzliche Ermächtigungsgrundlage für diesen Nutzungsvorgang in Betracht kommt, ist auch die Ermittlung des Nutzers anhand seiner IP-Adresse rechtswidrig.[584]

Allenfalls könnte man in dieser Hinsicht in Erwägung ziehen, dass sich das Auslesen der IP-Adressen der Nutzer als notwendige Vorbereitungshandlung zur Auskunftserteilung darstellt und damit vom Regelungsgehalt einer gesetzlichen Norm miterfasst ist, die eine Übermittlung der Nutzerdaten für zulässig erklärt. Fraglich ist daher, ob sich der Access Provider hinsichtlich der Übermittlung von Nutzerdaten auf eine gesetzliche Ermächtigung berufen kann.

3. Zulässigkeit der Auskunftserteilung

Ebenso wie das TDDSG sieht auch das TKG nur eine Übermittlung von Bestands- und Verbindungsdaten für Strafverfolgungszwecke und zudem nur an Gerichte und Behörden vor, nicht jedoch auch an private Rechteinhaber zum Zwecke der zivilrechtlichen Rechtsverfolgung.[585] Eine solche Ermächtigung könnte sich jedoch aus den Vorschriften des allgemeinen Datenschutzrechts ergeben, sofern dessen Anwendbarkeit nicht bereits aufgrund der Spezialität des TK-Datenschutzrechts ausgeschlossen ist.

---

[584] Kitz, GRUR 2003, 1014, 1018; Sieber/Höfinger, MMR 2004, 575, 582.

[585] Kitz, a.a.O.; ähnlich Czychowski, MMR 2004, 514, 517; Nordemann/Dustmann, CR 2004 380, 386, jeweils mit Verweis auf den Fragenkatalog des BMJ zum „Zweiten Korb“, in dem unter Frage D ausgeführt wird, dass Provider „derzeit aufgrund datenschutzrechtlicher Bestimmungen nur gegenüber Strafverfolgungsbehörden Auskunftspflichten“ haben, abrufbar unter: http://www.urheberrecht.org/topic/Korb-2/bmj/Fragebogen.pdf.

a) Rückgriff auf § 28 Abs. 3 Nr. 1 BDSG

Nach einer Auffassung soll auch im Anwendungsbereich des spezialgesetzlichen Datenschutzrechts ein Rückgriff auf den allgemeinen Übermittlungstatbestand des § 28 Abs. 3 Nr. 1 BDSG zulässig sein.[586] Dieser erklärt eine Übermittlung personenbezogener Daten für zulässig, soweit dies zur Wahrung berechtigter Interessen eines Dritten erforderlich ist und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Diese Voraussetzungen sollen nach dieser Auffassung auch in den vorliegenden Konstellationen erfüllt sein. Zunächst sei nämlich auch der Rechteinhaber im Verhältnis zum Access Provider und dessen Nutzer ein Dritter i.S.d. § 28 Abs. 3 Nr. 1 BDSG.[587] Zudem sei die Geltendmachung zivilrechtlicher (Auskunfts-) Ansprüche ein berechtigtes Interesse in diesem Sinne.[588] Ferner habe der Nutzer kein schutzwürdiges Interesse an der Geheimhaltung seiner Identität. Sofern dieser nämlich ein auf Dauer angelegtes urheberrechtswidriges Download-Portal (Teledienst) betreibt, ergebe sich die mangelnde Schutzbedürftigkeit bereits daraus, dass dieser durch die Unterdrückung seiner Identität gegen die Informationspflicht aus § 6 Abs. 1 Nr. 1 TDG verstößt, die ihrerseits eine gesetzliche Einschränkung des Rechts auf informationelle Selbstbestimmung darstellt.[589] Aber auch der „einfache Rechtsverletzer“ habe aufgrund seines rechtswidrigen Verhaltens kein schutzwürdiges Geheimhaltungsinteresse, zumal es sich bei den fraglichen Verstößen um strafbewehrte Urheberrechtsverletzungen handele.[590] Da die Interessenabwägung somit zugunsten der Rechteinhaber ausfallen müsse, sei auch die Übermittlung der Identität des Verletzers von der Ermächtigungsgrundlage des § 28 Abs. 3 Nr. 1 BDSG gedeckt.[591]

aa) Spezialität der §§ 91 ff. TKG

Einem solchem Rückgriff auf § 28 Abs. 3 Nr. 1 BDSG könnte jedoch der in § 1 Abs. 3 BDSG verankerte Grundsatz der Spezialität entgegenstehen. Aus diesem ergibt sich, dass die bereichsspezifischen Datenschutzbestimmungen – wie die des TDDSG und die §§ 91ff. TKG – in ihrem Anwendungsbereich den allgemeinen Bestimmungen des BDSG als speziellere Normen vorgehen. Vor der TKG-Novelle im Jahre 2004, in der die TDSV

[586] LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, CR 2005, 136, 140 ff. = MMR 2005, 55; Czychowski, MMR 2004 514, 517; Nordemann/Dustmann, CR 2004 380, 387.
[587] LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, CR 2005, 136, 140 = MMR 2005, 55.
[588] Nordemann/Dustmann, CR 2004, 380, 387; Czychowski, MMR 2004 514, 517.
[589] LG Hamburg, a.a.O.
[590] Czychowski, a.a.O.
[591] LG Hamburg, a.a.O.; Nordemann/Dustmann, a.a.O.; Czychowski, a.a.O.

in das TKG integriert wurde, ergab sich dies explizit aus § 1 Abs. 2 TDSV. Auch wenn diese Regelung nicht in das neue TKG aufgenommen wurde, so zeigt die Gesetzgebungsgeschichte, dass auch der Gesetzgeber des TKG weiterhin an dem Grundsatz der Spezialität des TK-Datenschutzrechts festhalten wollte.[592] Zudem wird auch in den Gesetzesmaterialien zum TDDSG auf den abschließenden Charakter der spezialgesetzlichen Erlaubnissätze verwiesen und explizit hervorgehoben, dass ein Rückgriff auf die allgemeinen Erlaubnistatbestände des BDSG, insbesondere auf den § 28 BDSG, unzulässig sei, soweit die Voraussetzungen für eine gesetzliche Erlaubnis hinsichtlich des Umgangs mit personenbezogenen Daten der Nutzer nach dem TDDSG nicht vorliegen.[593]

Dieser genetischen Auslegung wird mitunter entgegengehalten, dass der Gesetzgeber in den Gesetzesmaterialien nicht hinreichend zwischen den verschiedenen Tatbestandsvarianten des § 28 BDSG differenziert habe. Die dortigen Ausführungen beträfen nämlich nur das Konkurrenzverhältnis zwischen § 28 Abs. 1 BDSG und den bereichspezifischen Regelungen zur Datenerhebung und Datenverarbeitung für eigene Geschäftszwecke, nicht hingegen die Regelungen zur Datenübermittlung im berechtigten Drittinteresse.[594] Dieses Konkurrenzverhältnis richte sich nach dem allgemeinen Subsidiaritätsgrundsatz des Datenschutzrechts. Dieser besage, dass eine Subsidiarität des BDSG nur dann eintritt, wenn die allgemeinen Regeln des BDSG und die bereichsspezifischen Datenschutzregeln des TKG/TDDSG tatbestandlich miteinander konkurrieren.[595] Eine solche Tatbestandskonkurrenz zwischen § 28 Abs. 3 Nr. 1 BDSG und den Regelungen des TDDSG sowie der §§ 91 ff. TKG sei jedoch zu verneinen. Denn weder das TDDSG noch die §§ 91 ff. TKG enthielten eine mit § 28 Abs. 3 Nr. 1 BDSG vergleichbare Regelung zur Auskunftserteilung an nicht öffentliche Stellen, die eine umfassende Interessenabwägung zwischen dem allgemeinen Persönlichkeitsrecht des Betroffenen (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und dem Eigentumsrecht der Rechteinhaber (Art. 14 GG) ermöglicht.[596] Daher sei solange ein Rückgriff auf § 28 Abs. 3 Nr. 1 BDSG gebo-

[592] Amtl. Begründung zum TKG, BT-Drs. 15/2316, S. 88.
[593] Amtl. Begründung zum EGG, BT-Drs. 14/6098, S. 14.
[594] LG Hamburg, a.a.O.,141.
[595] LG Hamburg, a.a.O., 141 f. m.w.N.
[596] LG Hamburg, a.a.O.,142; Czychowski, MMR 2004, 514, 517; Nordemann/Dustmann, CR 2004, 380, 387.

ten, bis der Gesetzgeber für diese Fälle einschlägige Spezialnormen in das TDDSG und TKG einfügt habe.[597]

Dieser Auffassung ist die Gefolgschaft zu versagen. Zunächst handelt es sich zwischen den TDDSG/TKG und dem BDSG hinsichtlich der Zulässigkeit einer Übermittlung von Daten sehr wohl um tatbestandlich konkurrierende Normen. Der Regelungsbereich der §§ 91 ff. TKG erstreckt sich nach § 91 Abs. 1 TKG auf die Erhebung und Verwendung personenbezogener Daten. Diese Begriffe sind synonym zu den bisher in der TDSV verwendeten Begriffen des Erhebens, Verarbeitens sowie Nutzens zu verstehen.[598] Da nach § 3 Abs. 4 Nr. 3a BDSG der Begriff des Verarbeitens auch die Übermittlung von Daten erfasst, ist somit auch in dieser Hinsicht von einer Normenkonkurrenz zwischen TDDSG/TKG und dem BDSG auszugehen, die einen Rückgriff auf die allgemeine Vorschrift des § 28 Abs. 3 Nr. 1 BDSG verbietet.[599] Zudem spricht gegen die Möglichkeit eines solches Rückgriffs, dass der Gesetzgeber die Erlaubnissätze der bereichsspezifischen Datenschutzbestimmungen gerade vor dem Hintergrund, dass die Privatsphäre der Nutzer durch die vielfältigen Möglichkeiten zur Datenverarbeitung einer großen Gefahr ausgesetzt ist, bewusst restriktiv gehalten hat.[600]

Für den abschließenden Charakter der §§ 91 ff. TKG hinsichtlich der Übermittlung von Verbindungsdaten spricht schließlich auch der Umstand, dass nicht ersichtlich ist, warum private Rechteinhaber eine solche Auskunft ohne weiteres bekommen sollten, während Strafverfolgungsbehörden für die gleiche Auskunft nach §§ 100g, 100h StPO einer richterlichen Anordnung bedürfen.[601] Zumindest die Gesetzessystematik spricht somit für einen abschließenden Charakter der §§ 91 ff. TKG und damit für die Unzulässigkeit eines Rückgriffs auf § 28 BDSG.

bb) Verfassungs- und richtlinienkonforme Auslegung

Als Hilfsargument für eine Anwendbarkeit des § 28 Abs. 3 Nr. 1 BDSG wird angeführt, dass sich dessen Anwendbarkeit zumindest im Wege einer

---

[597] LG Hamburg, a.a.O., 143.

[598] Amtl. Begründung zum TKG, BT-Drs. 15/2316, 88; Spindler/Dorschel, CR 2005, 38, 45; Ohlenburg, MMR 2004, 431, 432; kritisch: Eckhard, CR 2003, 805, 806.

[599] Vgl. Klesczewski, in: Säcker, TKG, § 91, Rn. 14; Beck-TKG/Büchner, § 89, Rn. 14.

[600] Roßnagel, in: Roßnagel, Handbuch Datenschutzrecht, Teil 7.9, Rn. 60; Spindler/Dorschel, CR 38, 45 m.w.N.

[601] Kaufmann/Köcher, Anm. zu LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, MMR 2005, 61, 62.

verfassungs-[602] oder aber einer richtlinienkonformen Auslegung[603] des einfachen Rechts ergeben müsse.

Hinsichtlich der verfassungskonformen Auslegung wird ausgeführt, dass eine praktische Konkordanz zwischen dem Eigentumsrecht der Rechteinhaber aus Art. 14 GG und dem Recht der Nutzer auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG bestehe. Da sich der Nutzer rechtswidrig verhalte, müsse die Abwägung zugunsten der Rechteinhaber ausfallen, mithin § 28 Abs. 3 Nr. 1 BDSG anwendbar sein.[604] Dem lässt sich entgegenhalten, dass der Gesetzgeber diese praktische Konkordanz mit den bereichsspezifischen Regelungen des TDDSG und TKG, nach denen bewusst nur restriktiv Erlaubnissätze zur Verarbeitung personenbezogener Daten zugelassen wurden, bereits einer einfachgesetzlichen Lösung zugeführt hat. Diese mag, sofern eine Auskunftserteilung auch in diesen Fällen für unzulässig erklärt wird, zwar rechtspolitisch zu beanstanden sein, allerdings ist der Normsetzungsprimat des Gesetzgebers zu respektieren. Zudem ist diese restriktive Fassung der Erlaubnissätze auch europarechtlich determiniert. Diese Regelungen gehen auf die TK-Datenschutzrichtlinie[605] zurück. Auch diese sieht jedoch keine dahingehende Auskunftspflicht vor.[606]

Es verbleibt somit die Auffassung, nach der sich die Anwendbarkeit des § 28 Abs. 3 Nr. 1 BDSG zumindest im Wege einer richtlinienkonformen Auslegung der Datenschutzbestimmungen ergeben soll. Zur Begründung werden – die nach der Datenschutzrichtlinie erlassenen – Art. 8 Abs. 1 und Abs. 3 der InfoSoc-RL herangezogen, nach denen die Mitgliedstaaten verpflichtet werden, einen effektiven Urheberrechtsschutz vorzusehen. Dieser soll jedoch nicht gewährleistet sein, wenn die Offenlegung der Identität von Urheberrechtsverletzern an datenschutzrechtlichen Bestimmungen scheitert.[607] Eine dahingehende richtlinienkonforme Auslegung kann jedoch deshalb nicht überzeugen, weil auch Art. 8 InfoSoc-RL nicht zwingend die Statuierung einer derartigen Auskunftspflicht vorschreibt. So wird in Erwägungsgrund 60 der InfoSoc-RL ausdrücklich darauf hingewiesen,

---

[602] LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, CR 2005, 136, 142.
[603] Czychowski, MMR 2004, 514, 518.
[604] LG Hamburg, a.a.O.
[605] Richtlinie 2002/58/EG des europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation v. 12.7.2002, ABl. EG L 201 v. 31.7.2002, S. 37, abrufbar unter: http://www.datenschutz-berlin.de/recht/eu/rv/tk_med/tkdsr_de.htm.
[606] Spindler/Dorschel, CR 2005, 38, 45 f.
[607] Czychowski, MMR 2004, 514, 518.

dass die nationalen und gemeinschaftsrechtlichen Vorschriften des Datenschutzes von dieser Richtlinie unberührt bleiben.[608] Demzufolge kann auch Art. 8 InfoSoc-RL das deutsche Datenschutzrecht nicht modifizieren. Somit kann die Anwendbarkeit des § 28 Abs. 3 Nr. 1 BDSG weder durch eine verfassungs- noch durch eine richtlinienkonforme Auslegung des einfachgesetzlichen Rechts herbeigeführt werden. Dies gilt im Übrigen auch für die Bestimmungen der Enforcement-RL, da auch in dieser ausdrücklich darauf hingewiesen wird, dass die nationalen datenschutzrechtlichen Bestimmungen unberührt bleiben.[609]

b) Zwischenergebnis

Für eine Übermittlung von Nutzerdaten an die Rechteinhaber besteht derzeit keine datenschutzrechtliche Ermächtigungsgrundlage.[610] Insbesondere steht einem Rückgriff auf den allgemeinen Erlaubnissatz des § 28 Abs. 3 Nr. 1 BDSG der abschließende Charakter des speziellen TK-Datenschutzrechts entgegen.

4. Ergebnis

Die für eine Auskunftserteilung notwendigen Nutzungsvorgänge sind datenschutzrechtlich unzulässig. Zunächst ist der Access Provider allenfalls zu einer vorsorglichen Speicherung von statischen IP-Adressen berechtigt. Die regelmäßig vergebenen dynamischen IP-Adressen sind hingegen unmittelbar nach dem Ende der jeweiligen Verbindung des Nutzers zu löschen. Da den Rechteinhabern auch keine Ermächtigungsgrundlage für eine anlassbezogene Speicherpflicht zur Seite steht, scheitern Auskunftsansprüche zu dynamischen IP-Adressen regelmäßig bereits daran, dass diese Daten für Rechtsverfolgungszwecke nicht zur Verfügung stehen. Selbst im Falle einer zulässigen Speicherung von IP-Adressen ist der Access Provider weder berechtigt den konkreten Nutzer anhand seiner IP-Adresse zu identifizieren, noch diese Daten an die Rechteinhaber zu übermitteln. Soweit die Access Provider dennoch unberechtigt eine Speicherung von dynamischen IP-Adressen vornehmen bzw. Nutzerdaten an private Dritte übermitteln, stellt dies eine Ordnungswidrigkeit i.S.d. § 149 Abs. 1 Nr. 16 u. 17 TKG dar. Diese kann gem. § 149 Abs. 2 TKG mit einer Geldbuße von bis zu dreihunderttausend Euro geahndet werden kann. Sollte es durch

---

[608] Vgl. auch Wiebe, MR 2005, Beilage zu Heft 4, S. 13.
[609] Vgl. Erwägungsgrund 15 und Art. 8 Abs. 3 lit. e der Enforcement-RL.
[610] Zur Zulässigkeit einer Übermittlung von Nutzerdaten nach dem Telemediengesetz (TMG), siehe unten 7. Teil D. II.

eine solche unberechtigte Auskunftserteilung zu einem gerichtlichen Verfahren gegen den Nutzer kommen, wird sich dieser wegen des damit einhergehenden Verstoßes gegen sein verfassungsrechtlich geschütztes Recht auf informationelle Selbstbestimmung auf ein Beweisverwertungsverbot berufen können.[611]

B. Vereinbarkeit der Auskunftserteilung mit dem Fernmeldegeheimnis

Neben datenschutzrechtlichen Bestimmungen könnte eine Auskunftserteilung auch gegen das Fernmeldegeheimnis aus Art. 10 GG, § 88 TKG verstoßen. Das wäre der Fall, wenn durch die Auskunftserteilung in das Fernmeldegeheimnis eingegriffen wird und dieser Eingriff nicht durch eine gesetzliche Ermächtigung i.S.d. § 88 Abs. 3 S. 3 TKG legitimiert ist.

I. Schutzbereich des Fernmeldegeheimnisses

Nach der einfachgesetzlichen Ausprägung des Fernmeldegeheimnisses in § 88 Abs. 1 TKG umfasst dieses den *„Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war“*. Dem Diensteanbieter ist es nach § 88 Abs. 3 TKG untersagt, sich oder anderen Kenntnis vom Inhalt oder den näheren Umständen der Kommunikation zu verschaffen. Zu den näheren Telekommunikationsumständen zählen alle Umstände, die den jeweiligen Telekommunikationsvorgang individualisierbar machen.[612] Im Kern umfasst der Schutzbereich des Fernmeldegeheimnisses somit die Frage, wer, wann, mit wem, wohin, und auf welche Art und Weise kommuniziert hat.[613] Geschützt sind damit insbesondere die gem. § 96 Abs. 1 Nr. 1 TKG zu den Verkehrsdaten zählenden dynamischen IP-Adressen, nicht aber auch – die als Bestandsdaten i.S.d. § 95 TKG zu qualifizierenden – statischen IP-Adressen.[614] Ebenfalls nicht vom Fernmeldegeheimnis erfasst sind Kommunikationsvorgänge, die von vornherein an die Öffentlichkeit gerichtet sind.[615] Hinsichtlich der Frage, ob auch die Erteilung von Auskünften zu IP-Adressen in das Fernmeldegeheimnis eingreift, ist wie-

[611] Kitz, ZUM 2005, 298, 303.
[612] BVerfG, Beschl. v. 20.6.1984 – 1 BvR 1494/78, BVerfGE 67, 157, 172 – G 10; BVerfG, Beschl. v. 25.3.1992 – 1 BvR 1430/88, BVerfGE 85, 386, 396 – Fangschaltungen; Zerres, in: Scheurle/Mayen, TKG, § 85, Rn. 17.
[613] Beck-TKG/Büchner, § 85, Rn. 3.
[614] Vgl. BVerfG, Urt. v. 12.03.2003 – 1 BvR 330/96, 1 BvR 248/99, JurPC Web-Dok. 101/2003, Abs. 46 ff.; Beck-TKG/Büchner, § 85, Rn. 3.
[615] Beck-TKG/Büchner, § 85, Rn. 2 m.w.N.

derum zwischen dynamischen und statischen IP-Adressen zu differenzieren.

1. Eingriff durch Auskünfte zu dynamischen IP-Adressen

Obwohl dynamische IP-Adressen – als Verbindungsdaten – unstreitig dem Fernmeldegeheimnis unterfallen, geht eine Auffassung davon aus, dass Auskunftsbegehren zu solchen Verbindungsdaten bereits den Schutzbereich des Fernmeldegeheimnisses nicht tangieren. Es werde eben nur Auskunft über die Identität des Nutzers, nicht jedoch über nähere Umstände der Kommunikation verlangt.[616] Diese Umstände seien dem Auskunftsersuchenden nämlich bereits bekannt, da er sowohl von der konkreten Kennung des Anschlussinhabers als auch vom genauen Zeitpunkt des Kommunikationsvorganges Kenntnis habe. Das Auskunftsverlangen sei daher nicht auf die Herausgabe von Verbindungsdaten, sondern auf die Preisgabe des Namens und der Anschrift des bereits individualisierten Nutzers gerichtet. Somit werde lediglich eine Herausgabe von Bestandsdaten verlangt, die als solche nicht unter das Fernmeldegeheimnis fallen.[617]

Diese Ansicht ist abzulehnen. Zwar ist das Auskunftsbegehren tatsächlich auf die Identität des Nutzers und damit auf ein Bestandsdatum gerichtet, allerdings müssen zur Erlangung dieser Daten wiederum Verbindungsdaten ausgelesen werden. Durch das Auslesen der Log-Dateien zum Abgleich der IP-Adresse mit der Identität des Nutzers verschafft sich der Provider jedoch Kenntnis darüber, welcher Nutzer an dem vom Rechteinhaber bezeichneten Kommunikationsvorgang beteiligt war, mithin erlangt dieser Kenntnis über – dem Fernmeldegeheimnis unterliegende – nähere Umstände der Kommunikation. Um den Schutzbereich des Fernmeldegeheimnisses in diesen Fällen nicht unangemessen zu verkürzen, muss jedoch auch diese Verknüpfung zwischen Bestands- und Verkehrsdaten vom Schutzbereich des Fernmeldegeheimnisses umfasst sein.[618]

Weiterhin wird vertreten, das Fernmeldegeheimnis sei in diesen Fällen nicht betroffen, weil der Schutzbereich des Fernmeldegeheimnisses dahingehend einzuschränken sei, dass dieses nur Individualkommunikation –

---

[616] LG Stuttgart, Beschl. v. 4.1.2005 – 13 Qs 89/04, CR 2005, 598, 598 = NJW 2005, 614.

[617] LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, CR 2005, 136, 143 = MMR 2005, 55; LG Stuttgart, a.a.O.

[618] LG Bonn, Beschl. v. 21.5.2004 – 31 Qs 65/04, DuD 2004, 628, 629; Gnirck/Lichtenberg, DuD 2004, 598, 600; Kaufmann/Köcher, Anm. zu LG Hamburg, Urt. v. 7.7.2004 – 308 O 264/04, MMR 2005, 60, 61; Wiebe, MR 2005, Beilage zu Heft 4, S. 16.

wie z.B. E-Mail oder Internet-Telefonie (VoIP) – erfasse.[619] Davon sei das öffentliche Anbieten von urheberrechtlich geschützten Werken im Internet zu unterscheiden. Diese Kommunikationsvorgänge seien von vornherein an die Öffentlichkeit gerichtet und bereits deshalb nicht vom Schutzbereich des Fernmeldegeheimnisses erfasst.[620] Der Access Provider könne zudem anhand der Übertragungsprotokolle erkennen, ob ein entsprechender Nutzungsvorgang individuell oder öffentlich sei.[621] Aus diesen Gründen werde auch durch Auskünfte zu diesen öffentlichen Kommunikationsvorgängen nicht in das Fernmeldegeheimnis eingegriffen.[622]

Auch dieser Auffassung kann nicht gefolgt werden. Ihr steht entgegen, dass die fraglichen Auskunftsbegehren gerade nicht auf die öffentlich gemachten Inhalte, sondern auf die näheren Umstände der diesen Nutzungshandlungen vorgelagerten Zugangsgewährung gerichtet sind, mithin auf Umstände, die gerade nicht zur Veröffentlichung bestimmt sind.[623] Sofern behauptet wird, der Provider könne anhand der verwendeten Übertragungsprotokolle erkennen, ob der jeweilige Kommunikationsvorgang des Nutzers individuell oder allgemeinbezogen ist, kann dies schon vor dem Hintergrund nicht überzeugen, dass z.B. E-Mails keineswegs ausschließlich über das SMTP-Protokoll abgerufen werden müssen, da die meisten E-Mail-Provider auch einen Abruf über das HTTP-Protokoll ermöglichen.[624] Festzuhalten bleibt somit, dass Auskunftsansprüche zu dynamischen IP-Adressen das Fernmeldegeheimnis tangieren. Denn sobald der Access Provider seine Log-Dateien hinsichtlich der Frage ausliest, welcher Nutzer mit einer bestimmten IP-Adresse zu einem bestimmten Zeitpunkt online war, verschafft er sich gem. § 88 Abs. 3 S. 1 Alt. 1 TKG Kenntnis über die näheren Kommunikationsumstände seines Nutzers. Somit wird bei Auskünften zu dynamischen IP-Adressen bereits durch das Auslesen der Log-Dateien in den Schutzbereich des Fernmeldegeheimnisses eingegriffen.

---

[619] So LG Köln, Urt. v. 28.7.2004 – 28 O 301/04, ZUM 2005, 236, 241.
[620] LG Hamburg, a.a.O., 144; Nordemann/Dustmann, CR 2004, 380, 387; Czychowski, MMR 2004, 514, 518 f.; Zombik, ZUM 2006, 450, 453.
[621] Czychowski, MMR 2004, 514, 518 f.
[622] LG Hamburg, a.a.O., 144; Nordemann/Dustmann, CR 2004, 380, 387; Czychowski, MMR 2004, 514, 518 f.;
[623] So auch Stadler, Haftung im Internet, S. 206; Spindler/Dorschel, CR 2005, 38, 46; Wiebe, MR 2005, Beilage zu Heft 4, S. 16.
[624] Z.B. über http://www.gmx.de; vgl. Stadler, S. 207 (Fn. 589).

2. Eingriff durch Auskünfte zu statischen IP-Adressen

Während dynamische IP-Adressen als Verbindungsdaten zu qualifizieren sind und somit unstreitig dem Fernmeldegeheimnis unterliegen, sind die vertraglich vereinbarten statischen IP-Adressen bei isolierter Betrachtungsweise zunächst lediglich als Vertragsmerkmale einzuordnende Bestandsdaten i.S.d. § 95 TKG. Als solche unterliegen sie nicht dem Fernmeldegeheimnis, da diese Daten unmittelbar durch Einsehen der Vertragsunterlagen gewonnen werden können und es somit keiner Auswertung eines Telekommunikationsvorganges bedarf.[625]

Daraus lässt sich aber nicht der zwingende Schluss ziehen, dass der Access Provider hinsichtlich der Erfüllung von Auskunftsbegehren zu statischen IP-Adressen ebenfalls nicht in das Fernmeldegeheimnis eingreift.[626] So ist nämlich zu beachten, dass auch vermeintliche Bestandsdaten dem Fernmeldegeheimnis unterliegen können. Dies ist dann der Fall, wenn diese Daten selbst zum Gegenstand eines konkreten Telekommunikationsvorgangs gemacht werden, da sie dadurch zugleich auch als Verbindungsdaten zu qualifizieren sind.[627] Verdeutlichen lässt sich dies durch einen Vergleich der statischen IP-Adresse mit einer herkömmlichen Telefonnummer. Bei beiden handelt es sich zunächst um vertragliche Merkmale, mithin um Bestandsdaten. Zugleich erfüllen statische IP-Adressen im Rahmen von Telekommunikationsvorgängen, wie auch Telefonnummern, eine technische Funktion, da sie eine Adressierungsfunktion im Hinblick auf die zu übermittelnden Daten übernehmen. In Bezug auf konkrete Telekommunikationsvorgänge sind sie damit zugleich auch Kennungen i.S.d. § 96 Abs. 1 Nr. 1 TKG und damit Verkehrsdaten.[628]

Sofern die Rechteinhaber somit Auskunft über die Beteiligten solcher konkreten Telekommunikationsvorgänge verlangen, ist in dieser Hinsicht also nicht die vertragliche Komponente als Bestandsdatum betroffen, sondern deren technische Ausprägung als Verkehrsdatum. Dafür spricht auch, dass die Rechteinhaber regelmäßig nicht erkennen können, ob es sich bei einer generierten IP-Adresse um eine dynamische oder eine statische IP-Adresse handelt. Aus diesem Grund sind auch die Auskunftsbegehren zu statischen

---

[625] LG Bonn, Beschl. v. 21.5.2004 – 31 Qs 65/04, DuD 2004, 628, 629, DuD 2004, 628, 628; Hoeren, Access Provider, Rn. 49.

[626] So jedoch LG Stuttgart, Beschl. v. 4.1.2005 – 13 Qs 89/04, CR 2005, 598, 599; LG Bonn, Beschl. v. 21.5.2004 – 31 Qs 65/04, DuD 2004, 628, 628 f.

[627] Klesczewski, in: Säcker, TKG, § 88, Rn. 14.

[628] Vgl. Klesczewski, in: Säcker, a.a.O.

IP-Adressen nicht auf den Inhaber einer bestimmten (statischen) IP-Adresse gerichtet sind, sondern darauf, wer mit einer bestimmten IP-Adresse zu einer bestimmten Zeit an einem Kommunikationsvorgang beteiligt war, mithin auf einen näheren Kommunikationsumstand. Der Access Provider erlangt somit regelmäßig auch dann gem. § 88 Abs. 3 S. 1 Alt. 1 TKG Kenntnis von dem Fernmeldegeheimnis unterliegenden Tatsachen, wenn er den Nutzer einer statischen IP-Adresse identifiziert. Man könnte einem dadurch bedingten Eingriff in das Fernmeldegeheimnis zwar entgegenhalten, dass der Access Provider zur Erlangung dieser Information nicht zwingend die Log-Dateien auslesen muss, sondern die Identität des Nutzers auch anhand der Vertragsunterlagen in Erfahrung bringen kann. Letztlich kann dieser Einwand jedoch dahinstehen, da der Access Provider durch die Auskunftserteilung zumindest dem Rechteinhaber und damit einem Dritten i.S.d. § 88 Abs. 3 S. 1 Alt. 2 TKG diese Kenntnis verschafft. Somit greift der Access Provider auch bei Auskunftsersuchen zu statischen IP-Adressen zumindest durch die Übermittlung der Identität des Nutzers in das Fernmeldegeheimnis ein.

3. Zwischenergebnis

Durch die Erfüllung von Auskunftsbegehren der Rechteinhaber greift der Access Provider in das Fernmeldegeheimnis ein. Liegt dem Begehren eine dynamische IP-Adresse zugrunde, wird bereits durch die Bestimmung der Identität des Nutzers gem. § 88 Abs. 3 S. 1 Alt. 1 TKG in das Fernmeldegeheimnis eingegriffen, da es dazu des Auslesens von Verkehrsdaten bedarf. Bei Auskunftsersuchen zu statischen IP-Adressen stellt zumindest die Übermittlung dieser Daten an die Rechteinaber einen Eingriff in das Fernmeldegeheimnis dar, da insofern einem Dritten i.S.d. § 88 Abs. 3 S. 1 Alt. 2 TKG Kenntnis über nähere Kommunikationsumstände verschafft wird.

Dieses Ergebnis lässt sich auch durch die neuere, restriktive Rechtsprechung des Bundesverfassungsgerichts (BVerfG) zum Schutzbereich des Fernmeldegeheimnisses nicht erschüttern.[629] So hat das BVerfG zwar festgestellt, dass nähere Umstände der Kommunikation nicht mehr vom Fernmeldegeheimnis aus Art. 10 GG, sondern lediglich vom Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG geschützt werden, sofern sich diese Daten nach Abschluss des Telekommunikationsvorganges im Herrschaftsbereich des Kommunikationsteil-

[629] BVerfG, Urt. v. 2.3.2006 – 2 BvR 2099/04, Absatz-Nr. (1 - 142), abrufbar unter: http://www.bverfg.de/entscheidungen/rs20060302_2bvr209904.html.

nehmers befinden und dieser über die Daten frei verfügen kann.[630] Vorliegend geht es jedoch um solche Daten, die beim Access Provider erhoben wurden und auf die der Nutzer keinen Einfluss hat. Diese vom Transportmittler erhobenen Daten fallen jedoch auch nach der neueren Rechtsprechung des BVerfG weiterhin in den Schutzbereich des Fernmeldegeheimnisses aus Art. 10 GG bzw. § 88 TKG.[631]

II. Gesetzliche Ermächtigung zur Auskunftserteilung

Da durch Auskunftserteilungen zu IP-Adressen in das Fernmeldegeheimnis eingegriffen wird, hängt die Zulässigkeit der Auskunftserteilung gem. § 88 Abs. 3 S. 3 TKG davon ab, ob diese von einer gesetzlichen Ermächtigungsgrundlage gedeckt ist. Eine solche muss zudem den Anforderungen des *„einfachgesetzlichem Zitiergebots"*[632] des § 88 Abs. 3 S. 3 GG genügen, sich also explizit auf Telekommunikationsvorgänge beziehen. Durch dieses Erfordernis soll sichergestellt werden, dass der Gesetzgeber eine bewusste Abwägung zwischen dem Fernmeldegeheimnis und den Interessen Dritter vorgenommen hat.[633] Hinsichtlich der Übermittlung von Telekommunikationsdaten an Dritte ist eine solche Ermächtigungsgrundlage jedoch nicht ersichtlich. Insbesondere kann diese nicht in § 101a UrhG i.V.m. § 28 Abs. 3 Nr. 1 BDSG gesehen werden,[634] da keine dieser beiden Normen Bezug auf Telekommunikationsvorgänge nimmt oder erkennen lässt, dass ihr eine bewusste Abwägung zwischen der Auskunftserteilung und der Wahrung des Fernmeldegeheimnisses zugrunde liegt.[635]

III. Ergebnis

Eine Auskunftserteilung des Access Providers über die Identität des sich hinter einer (dynamischen oder statischen) IP-Adresse verbergenden Nutzers verstößt gegen das Fernmeldegeheimnis aus § 88 TKG. Zugleich erfüllt ein solcher Verstoß den objektiven Tatbestand des § 206 StGB.

C. Ergebnis der geheimschutzrechtlichen Betrachtung

Der Durchsetzung von Auskunftsansprüchen gegen Access Provider steht sowohl das Datenschutzrecht als auch das Fernmeldegeheimnis entgegen.

---

[630] BVerfG, a.a.O., Absatz-Nr. 72.
[631] BVerfG, a.a.O., Absatz-Nr. 77.
[632] So Breyer, Vorratsdatenspeicherung, S. 103.
[633] Zerres, in: Scheurle/Mayen, TKG, § 85, Rn. 40.
[634] So aber ausdrücklich Czychowski, MMR 2004, 514, 519.
[635] So auch Sieber/Höfinger, MMR 2004, 575, 584.

Diese Ansprüche sind somit wegen rechtlicher Unmöglichkeit gem. § 275 BGB ausgeschlossen.

6. Teil: Vereitelung von Auskunftsansprüchen durch Anonymisierungsdienste

Selbst wenn Access Provider nach den geltenden gesetzlichen Regelungen sowohl zur Speicherung von IP-Adressen als auch zur Herausgabe von Nutzerdaten an die Rechteinhaber berechtigt wären, steht und fällt die Effektivität eines solchen Auskunftsanspruchs mit den technischen Möglichkeiten, die Nutzer ergreifen können, um einer Identifizierung zu entgehen. In dieser Hinsicht sind vor allem Anonymisierungsdienste von besonderem Interesse. Diese können als technische Ausprägung des verfassungsrechtlich geschützten Rechts auf Anonymität angesehen werden, welches sich aus dem informationellen Selbstbestimmungsrecht und dem allgemeinen Persönlichkeitsrecht ableiten lässt.[636] Einfachgesetzlich hat dieses Recht eine Ausprägung in § 4 Abs. 6 TDDSG und § 18 Abs. 6 MDStV gefunden. Danach ist den Nutzern dieser Dienste eine anonyme Inanspruchnahme zu ermöglichen, soweit dies technisch möglich und zumutbar ist.

Zur Realisierung dieses Rechts auf Anonymität wird seit Anfang 2001 in Kooperation der technischen Universität (TU) Dresden mit der Freien Universität Berlin und dem Unabhängigen Landeszentrum für Datenschutz Schleswig Holstein sowie mit Förderung des Bundesministeriums für Wirtschaft und Arbeit, das Forschungs- und Entwicklungsprojekt „AN.ON-Anonymität Online“[637] durchgeführt. Der AN.ON.-Dienst soll Internet-Nutzern ein anonymes Surfen ermöglichen. Neben AN.ON existieren mittlerweile mehrere vergleichbare Dienste, die ebenfalls für eine Anonymisierung des Nutzers sorgen sollen.[638] Im Folgenden soll zunächst die technische Funktionsweise eines Anonymisierungsdienstes am Beispiel des AN.ON. skizziert werden. Sodann soll dieser Dienst unter den rechtlichen Gesichtspunkten der Haftung für Rechtsverletzungen Dritter sowie des Datenschutzrechts untersucht werden.

---

[636] Vgl. Federrath/Hansen, DuD 2003, 126, 126.
[637] http://anon.inf.tu-dresden.de.
[638] Vgl. hierzu die Darstellungen bei Köpsell/Federrath/Hansen, DuD 2003, 139, 139 f.; Federrath, ZUM 2006, 434, 437.; www.safersurf.com.

A. Technische Funktionsweise am Beispiel des AN.ON.-Dienstes

Der AN.ON.-Dienst basiert im Wesentlichen auf zwei Komponenten, der Client-Software JAP und dem von David Chaum entwickelten Verfahren der unkodierten Mixe. In vereinfachter Form stellt sich die Funktionsweise wie folgt dar. In der Regel wird in jeder Anfrage, die ein Nutzer an einen Webserver richtet, sowohl die Ausgangs-IP-Adresse, also diejenige, die dem Nutzer vom Access Provider zugewiesen wurde, als auch die Ziel-IP-Adresse des Webservers sowie der angeforderte Inhalt gespeichert. Hat der Nutzer jedoch die JAP-Software aktiviert, werden seine Anfragen über den Access Provider an den ersten Mix-Server einer voreingestellten Mixkaskade gesendet. Dieser Mix-Server verschlüsselt die Anfrage des Nutzers in der Weise, dass dessen Ausgangs-IP-Adresse durch die IP-Adresse des Mix-Servers ersetzt wird. Sodann wird diese Anfrage über weitere Mix-Server, die ebenfalls eine Umwandlung der IP-Adresse vornehmen, an den eigentlichen Ziel-Server weitergeleitet. In umgekehrter Weise erfolgt der Datentransport zurück an den Nutzer.[639]

Wird dieser Datenverkehr seitens der Rechteinhaber zurückverfolgt, so ist als Ausgangspunkt nicht die IP-Adresse des Nutzers, sondern lediglich die des letzten Servers der Mixkaskade zu erkennen. Eine Zuordnung dieser IP-Adresse zu der ursprünglich vom Access Provider vergebenen ist jedoch nicht absolut unmöglich. Theoretisch wäre eine solche Identifizierung dann möglich, wenn auch die Mixkaskadenbetreiber die den Nutzern zugewiesenen IP-Adressen speichern und kollusiv hinsichtlich der Aufdeckung des Nutzers zusammenarbeiten würden.[640] Da die Mixkaskadenbetreiber des AN.ON.-Dienstes jedoch auf die Speicherung der den Nutzern zugewiesenen IP-Adressen verzichten, ist zumindest eine nachträgliche Zuordnung der IP-Adresse ausgeschlossen. Dies kommt einer anonymen Nutzung zumindest faktisch gleich.[641] Generiert ein Rechteinhaber also die IP-Adresse eines Rechtsverletzers, der sich eines Anonymisierungsdienstes bedient, ist dessen Identifizierung in der Regel nicht möglich. In diesen Fällen scheitert ein Auskunftsanspruch somit bereits in tatsächlicher Hinsicht.

---

[639] Vgl. Golembiewski, DuD 2003, 129, 131; Schmitz, in: Spindler/Schmitz/Geis, § 1 TDDSG, Rn. 15; näher zur technischen Funktionsweise: http://anon.inf.tu-dresden.de/desc/encr_jap.html.

[640] So auch Schmitz, in: Spindler/Schmitz/Geis, § 4 Rn. 47; Fedderrath, ZUM 2006, 434, 437; a.A. Golembiewski, DuD 2003, 129, 132.

[641] Golembiewski, DuD 2003, 129, 132.

B. Rechtliche Einordnung eines Anonymisierungsdienstes

In rechtlicher Hinsicht ist zunächst von Interesse, ob der Betreiber eines Anonymisierungsdienstes für die Rechtsverletzungen seiner Nutzer zur Verantwortung gezogen kann, oder ob auch für diesen die Haftungsprivilegierungen des TDG eingreifen.

I. Haftungsrechtliche Einordnung

Ob sich auch der Betreiber eines Anonymisierungsdienstes auf ein Haftungsprivileg nach dem TDG berufen kann, hängt zunächst davon ab, wie dessen Tätigkeit rechtlich zu qualifizieren ist. Hinsichtlich des reinen Datentransports und den bereitgestellten technischen Ressourcen kann der Anonymisierungsdienst durchaus mit einem Access Provider verglichen werden. Ebenso wie dieser ist der Anonymisierungsdienst ein geschäftsmäßiger Erbringer von Telekommunikationsleistungen nach dem TKG.[642] Die Umwertungsfunktion durch Manipulation der Ausgangs-IP-Adresse ist hingegen nach überwiegend vertretener Auffassung als Teledienst einzustufen, da sie nicht auf der Transport-, sondern der Anwendungsebene stattfindet.[643] Der Anonymisierungsdienst erfüllt somit in zweifacher Hinsicht den Begriff des Diensteanbieters i.S.d. § 3 Nr. 1 TDG, nämlich als Zugangsvermittler und als Anbieter eines eigenen Teledienstes. Nach der gebotenen technisch-funktionalen Abgrenzung der Anwendungsbereiche zwischen TDG und TKG,[644] kann sich der Betreiber eines Anonymisierungsdienstes somit, wie auch der Access Provider, unabhängig von der Ausschlussnorm des § 2 Abs. 4 Nr. 1 TDG auf die Haftungsprivilegierung des § 9 TDG berufen. Dessen Voraussetzungen dürften regelmäßig erfüllt sein. Insbesondere wird in der Verschleierung der Kommunikationsvorgänge keine – die Privilegierung ausschließende – Veränderung von Daten i.S.d. § 9 Abs. 1 Nr. 3 TDG gesehen werden können, da durch diese Maßnahmen der Informationsgehalt der übermittelten Daten nicht angetastet wird.[645] Greift somit eine Haftungsprivilegierung nach § 9 TDG ein, ist die Haftung der Betreiber von Anonymisierungsdiensten –wie die der Access Provider – nur unter den Voraussetzungen des § 8 Abs. 2 S. 2 TDG gegeben. Da diese Regelung keine Auskunftsansprüche von den Haftungsfreistellungen ausnimmt,[646] würden somit auch gegen Anonymisierungsdienste

[642] Raabe, DuD 2003, 134, 135.
[643] Raabe, DuD 2003, 134, 136; Schmitz, in: Spindler/Schmitz/Geis, § 1 TDDSG, Rn. 15.
[644] Siehe oben, 4. Teil D. III.
[645] Raabe, DUD 2003, 134, 136.
[646] Siehe oben, 4. Teil E. IV.

gerichtete Auskunftsansprüche nicht nur in tatsächlicher, sondern auch in rechtlicher Hinsicht scheitern.

II. Datenschutzrechtliche Einordnung

Da Anonymisierungsdienste sowohl einen Tele- als auch einen Telekommunikationsdienst betreiben, gelten für diese sowohl die datenschutzrechtlichen Regelungen für Teledienste nach dem TDDSG als auch das TK-Datenschutzrecht gem. §§ 91 ff. TKG. Das TDSG ist einschlägig, wenn es um die als Teledienst zu qualifizierende Anonymisierungsfunktion durch Umwertung der IP-Adresse geht. Sofern ein Anonymisierungsdienst kostenpflichtig zur Verfügung gestellt wird, bedarf es für Abrechnungszwecke zumindest der Erhebung von Bestandsdaten.[647] Die Zulässigkeit der Erhebung der dafür benötigten Daten richtet sich nach § 5 TDDSG, da in vertraglicher Hinsicht die als Teledienst zu qualifizierende Anonymisierungsfunktion im Vordergrund steht.[648] Bezüglich der Vergabe von IP-Adressen durch den Mixserver handelt es sich jedoch um eine telekommunikationsrechtliche Dienstleistung auf der Transportebene. Die IP-Adresse fungiert in dieser Hinsicht als Kennung i.S.d. § 96 Abs. 1 Nr. 1 TKG und ist daher den Verkehrsdaten zuzurechnen. Daher gelten für den Betreiber eines Anonymisierungsdienstes hinsichtlich der Speicherung von IP-Adressen dieselben Beschränkungen wie für Access Provider.[649] Sofern einige Dienste die IP-Adressen zumindest zum Zwecke der strafrechtlichen Verfolgung aufzeichnen, wie es der JANUS-Dienst tat,[650] ist somit auch dies mangels gesetzlicher Ermächtigung rechtswidrig. In der Regel zeichnen sich Anonymisierungsdienste jedoch gerade dadurch aus, dass sie sich strikt an die gesetzlichen Vorgaben halten und somit auf eine über das Verbindungsende hinausgehende Speicherung von IP-Adressen gänzlich verzichten.

III. Ergebnis

Mit Hilfe eines Anonymisierungsdienstes könnte sich ein Rechtsverletzer der Rechtsverfolgung regelmäßig selbst dann entziehen, wenn der Access Provider zur Speicherung und Weitergabe von Verkehrsdaten berechtigt wäre. Nicht unerwähnt bleiben soll an dieser Stelle, dass die missbräuchliche Verwendung dieser Dienste im Verhältnis zur Gesamtnutzung bisher

---

[647] Auch der AN.ON-Dienst wird wegen Ablaufs der Fördermittels bald kostenpflichtig, vgl. Heise News, Meldung v. 19.2.2006: Anonymisierungsdienst AN.ON wird kostenpflichtig, http://www.heise.de/newsticker/meldung/69761

[648] Raabe, DUD 2003, 134, 137.

[649] Vgl. oben, 5.Teil A. IV.

[650] Vgl. Raabe, DUD 2003, 134, 137.

nur einen verschwindend geringen Prozentsatz einnimmt.[651] Dies mag daran liegen, dass es durch den zwischengeschalteten Anonymisierungsdienst zu einer Verringerung der Datenübertragungsrate kommt.[652] Es ist jedoch davon auszugehen, dass sich die Bereitschaft zum Missbrauch dieser Dienste für Rechtsverletzungen proportional zum Anstieg der Rechtsverfolgungsmaßnahmen erhöhen wird. Dies birgt für Rechteinhaber die erhebliche Gefahr, dass sich die Statuierung eines gegen Access Provider gerichteten Auskunftsanspruchs als stumpfes Schwert erweisen könnte, wenn dieser Anspruch durch die Nutzung von Anonymisierungsdiensten faktisch ausgehebelt werden könnte.

[651] Golembiewski, DuD 2003, 129, 132.
[652] Vgl. Spiekermann, DuD 2003, 150, 151 *(„durchschnittlich um ca. 10%").*

7. Teil: Auskunftsansprüche gegen Access Provider *de lege ferenda*

Im Folgenden wird die Rechtslage zur Auskunftspflicht von Access Providern untersucht, wie sie sich nach dem Referentenentwurf vom 03.01.2006 zur Umsetzung der Richtlinie 2004/48/EG[653] (Enforcement-RL) abzeichnet.[654] Dazu wird zunächst der Gegenstand der Richtlinie dargestellt und sodann der Umsetzungsbedarf hinsichtlich der Einführung eines verletzungsunabhängigen Auskunftsanspruchs gegen Access Provider erörtert. Anschließend wird die im Referentenentwurf vorgesehene Drittauskunftspflicht nach § 101 UrhG-E einer kritischen Würdigung unterzogen.

A. Gegenstand der Richtlinie 2004/48/EG (Enforcement-RL)

Durch die Enforcement-RL[655] werden die Mitgliedstaaten verpflichtet, materiell-rechtliche Sanktionen und verfahrensrechtliche Instrumente vorzusehen, die erforderlich sind, um die Durchsetzung der Rechte des geistigen Eigentums sicherzustellen (Art. 1 RL). In dieser Hinsicht sieht die RL Regelungen zur Vereinheitlichung der Beweisvorlagepflichten des Verletzers (Art. 6 RL), des Beweissicherungsverfahrens (Art. 7 RL) sowie zum vorliegend bedeutsamen Auskunftsanspruch gegen Dritte (Art. 8 RL) vor. Daneben enthält die RL Regelungen zu einstweiligen Maßnahmen und Sicherungsmaßnahmen (Art. 9 RL), Abhilfemaßnahmen (Art. 10 RL), Unterlassungsanordnungen (Art. 11 RL) und Ersatzmaßnahmen (Art. 12 RL), Regeln zum Schadensersatz (Art. 13 RL), zu den Prozesskosten (Art. 14 RL) sowie zur Veröffentlichung von Gerichtsentscheidungen (Art. 15 RL). Die RL knüpft an die Regelungen des TRIPS-Übereinkommens an. Während sie einerseits in einigen Punkten über dessen Regelungsgehalt hinausgeht,[656] ist sie anderseits – im Gegensatz zu TRIPS – auf zivilrechtliche Regelungen zur Durchsetzung der Rechte des geistigen Eigentums beschränkt.[657] Aus Art. 2 Abs. 1 RL ergibt sich, dass die RL keine Voll-, sondern lediglich eine Mindestharmonisierung vorsieht. Danach bleiben für den Rechteinhaber günstigere – als die in der RL vorgesehenen – Regelungen unberührt. Da die RL vorrangig der prozessualen Durchsetzung

---

[653] Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates v. 29.4.2004 zur Durchsetzung der Rechte des geistigen Eigentums, ABl. EG NR. L 195 v. 2.6.2004, S. 16; zur Entstehungsgeschichte, Dreier, GRUR-Int. 2004, 706 ff.

[654] Referentenentwurf v. 3.1.2006 für ein Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums (im Folgenden: Referentenentwurf), abrufbar unter: http://www.urheberrecht.org/topic/enforce/bmj/2006-01-03-DurchsetzungsG-E.pdf.

[655] Im Folgenden RL genannt.

[656] Knaak, GRUR-Int. 2004, 745, 747; Referentenentwurf, a.a.O., S. 46.

[657] Vgl. Art. 2 Abs. 3 lit. b u. c RL.

geistiger Schutzrechte dient, sind auch die gemeinschaftsrechtlichen materiell-rechtlichen Bestimmungen zum Urheberrecht und den verwandten Schutzrechten ausgenommen.[658] Dies betrifft somit insbesondere auch die den Haftungsregeln des TDG/MDStV zugrunde liegenden Bestimmungen der E-Commerce-RL und der InfoSoc-RL.[659] Somit kann auch im Rahmen des Anwendungsbereichs der RL auf die obigen Ausführungen zu den Haftungsprivilegierungen der Access Provider zurückgegriffen werden. Gleiches gilt für die datenschutzrechtlichen Bestimmungen, da auch diese von der RL unberührt bleiben.[660]

B. Umsetzungsbedarf hinsichtlich des Auskunftsrechts (Art. 8 RL)

Vor allem im Hinblick auf den urheberrechtlichen Drittauskunftsanspruch aus § 101a UrhG stellt sich die Frage, ob überhaupt Umsetzungsbedarf hinsichtlich des Auskunftsrechts nach Art. 8 RL besteht. Zur Klärung dieser Frage bedarf es zunächst einer näheren Betrachtung dessen Regelungsgehalts. Art. 8 RL ist an Art. 47 TRIPS angelehnt, geht aber sowohl hinsichtlich des Umfangs der Auskunftsverpflichtung als auch bezüglich des Kreises der Passivlegitimierten über dessen Anwendungsbereich hinaus.[661] So erstreckt sich die Auskunftspflicht nach Art. 8 RL nicht nur – wie auch im Falle des § 101a UrhG – auf den Verletzer, sondern unter bestimmten Voraussetzungen auch auf den Nichtverletzer. Von besonderem Interesse hinsichtlich der Auskunftspflicht des Access Providers ist die Regelung des Art. 8 Abs. 1 lit. c RL. Diese lautet:

> ***„Artikel 8***
> ***Recht auf Auskunft***
> *(1) Die Mitgliedstaaten stellen sicher, dass die zuständigen Gerichte im Zusammenhang mit einem Verfahren wegen Verletzung eines Rechts des geistigen Eigentums auf einen begründeten und die Verhältnismäßigkeit wahrenden Antrag des Klägers hin anordnen können, dass Auskünfte über den Ursprung und die Vertriebswege von Waren oder Dienstleistungen, die ein Recht des geistigen Eigentums verletzen, von dem Verletzer und/oder jeder anderen Person erteilt werden, die […]*
> ***c) nachweislich für rechtsverletzende Tätigkeiten genutzte Dienstleistungen in gewerblichem Ausmaß erbrachte […]“***

[658] Erwägungsgrund 15, 16 der RL.
[659] Erwägungsgrund 15, 16 der RL.
[660] Vgl. Erwägungsgrund 15, Art. 8 Abs. 3 lit. e RL.
[661] Näher, Referentenentwurf, a.a.O., S. 56 f.

Zutreffend haben die Entwurfsverfasser hinsichtlich der Erstreckung der Drittauskunftspflicht auf den Nichtverletzer Umsetzungsbedarf gesehen, da § 101a UrhG – im Gegensatz zu Art. 8 Abs. 1 lit. c RL – weder in direkter noch in analoger Anwendung eine Auskunftspflicht des Nichtverletzers statuiert. Danach wird eine Auskunftspflicht nämlich zumindest an eine Verletzung von Prüfpflichten geknüpft.[662] Insofern galt es zu klären, wie eine solche Auskunftspflicht des Nichtverletzers in deutsches Recht umgesetzt werden könnte. Angesichts der Tatsache, dass eine Auskunftspflicht des Nichtverletzers nach Art. 8 Abs. 1 RL nur im Zusammenhang mit einem gerichtlichen Verfahren gewährt werden muss, haben die Entwurfsverfasser zunächst auch die Möglichkeit einer Zeugenvernehmung (des Access Providers) in Betracht gezogen.[663] Zutreffend wurde dies jedoch wieder verworfen, da eine Zeugenvernehmung, die auf die Ermittlung der Identität des Rechtsverletzers gerichtet ist, auf einen unzulässigen Ausforschungsbeweis hinausliefe.[664] Daher sieht die – Art. 8 RL umsetzende – Regelung des § 101 UrhG-E vor, dass die Auskunftspflicht des Dritten vorrangig an materiell-rechtliche Voraussetzungen geknüpft wird. Diese Voraussetzungen des § 101 UrhG-E sind im Folgenden – unter dem Aspekt der Auskunftspflicht des Access Providers – kritisch zu begutachten. Obwohl sich die folgenden Ausführungen primär auf den urheberrechtlichen Auskunftsanspruch nach § 101 UrhG-E des Referentenentwurfes beziehen, lassen sich diese Wertungen angesichts des horizontalen Ansatzes des Referentenentwurfs[665] auch auf die weiteren im Entwurf vorgesehenen Auskunftsansprüche hinsichtlich der anderen Schutzrechte übertragen.[666]

C. Auskunftspflicht des Access Providers nach § 101 UrhG-E

Die im Folgenden zu untersuchende Regelung des § 101 UrhG-E lautet:

„§ 101
Anspruch auf Auskunft
(1) Wer das Urheberrecht oder ein anderes nach diesem Gesetz geschütztes Recht widerrechtlich verletzt, kann von dem Verletzten auf unverzügliche

---

[662] Referentenentwurf, a.a.O., S. 57; zugleich bestätigen die Entwurfsverfasser dadurch die hier vertretene Auffassung, nach der auch der mittelbare Störer vom Anwendungsbereich des § 101a UrhG erfasst wird, vgl. oben, 2. Teil A. IV. 4.

[663] Referentenentwurf, a.a.O., S. 58.

[664] Referentenentwurf, a.a.O., S. 58; näher dazu oben, 3. Teil E. II.

[665] Vgl. Referentenentwurf, a.a.O., S. 73.

[666] Der Regelung des § 101 UrhG-E entsprechen die Regelungen des § 140b PatG-E, § 24b GebrMG-E, §§ 19, 128, 135 MarkenG-E, § 46 GeschmMG, § 37b SortenschutzG-E des Referentenentwurfs.

Auskunft über die Herkunft und den Vertriebsweg der rechtsverletzenden Vervielfältigungsstücke oder sonstigen Erzeugnisse in Anspruch genommen werden.
(2) In Fällen offensichtlicher Rechtsverletzung oder in Fällen, in denen der Verletzte gegen den Verletzer Klage erhoben hat, besteht der Anspruch unbeschadet von Absatz 1 auch gegen eine Person, die in gewerblichem Ausmaß
[…]
***3. für rechtsverletzende Tätigkeiten genutzte Dienstleistungen erbrachte** oder […] Im Fall der gerichtlichen Geltendmachung des Auskunftsanspruchs nach Satz 1 kann das Gericht den gegen den Verletzer anhängigen Rechtsstreit auf Antrag bis zur Erledigung des wegen des Auskunftsanspruchs geführten Rechtsstreits aussetzen. Der zur Auskunft Verpflichtete kann von dem Verletzten den Ersatz der für die Auskunftserteilung erforderlichen Aufwendungen verlangen […]*
(4) Die Ansprüche nach den Absätzen 1 und 2 sind ausgeschlossen, wenn die Inanspruchnahme im Einzelfall unverhältnismäßig ist.
(5) Erteilt der zur Auskunft Verpflichtete die Auskunft vorsätzlich oder grob fahrlässig falsch oder unvollständig, so ist er dem Verletzten zum Ersatz des daraus entstehenden Schadens verpflichtet.
(6) Wer eine wahre Auskunft erteilt hat, ohne dazu nach Absatz 1 oder 2 verpflichtet gewesen zu sein, haftet Dritten gegenüber nur, wenn er wusste, dass er zur Auskunftserteilung nicht verpflichtet war.
(7) In Fällen offensichtlicher Rechtsverletzung kann die Verpflichtung zur Erteilung der Auskunft im Wege der einstweiligen Verfügung nach den §§ 935 bis 945 der Zivilprozessordnung
angeordnet werden. […]
(9) Kann die Auskunft nur unter Verwendung von Verkehrsdaten (§ 3 Nr. 30 des Telekommunikationsgesetzes) erteilt werden, ist für ihre Erteilung eine vorherige richterliche Anordnung über die Zulässigkeit der Verwendung der Verkehrsdaten erforderlich, die von dem Verletzten zu beantragen ist. Für den Erlass dieser Anordnung ist das Landgericht, in dessen Bezirk der zur Auskunft Verpflichtete seinen Wohnsitz, seinen Sitz oder eine Niederlassung hat, ohne Rücksicht auf den Streitwert ausschließlich zuständig. Die Entscheidung trifft die Zivilkammer. Für das Verfahren gelten die Vorschriften des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit mit Ausnahme des § 28 Abs. 2 und 3 entsprechend. Die Kosten der richterlichen Anordnung trägt der Verletzte. Gegen die Entscheidung des Landgerichts ist die sofortige Beschwerde zum Oberlandesgericht statthaft. Sie kann nur darauf gestützt werden, dass die Entscheidung auf einer Verletzung des Rechts beruht. Die Entscheidung des Oberlandesgerichts ist unanfechtbar. Die Vorschriften zum Schutz personenbezogener Daten bleiben im Übrigen unberührt.
(10) Durch Absatz 2 in Verbindung mit Absatz 9 wird das Grundrecht des Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) eingeschränkt."

Bevor allerdings auf die Auskunftspflicht des Access Providers als Nichtverletzer nach § 101 Abs. 2 UrhG-E eingegangen wird, soll zunächst die Auskunftspflicht des Verletzers dargestellt werden, wie sie sich nach § 101 Abs. 1 UrhG-E abzeichnet.

I. Auskunftspflicht des Verletzers

Im Gegensatz zu § 101a Abs. 1 UrhG, der eine Auskunftspflicht nur bei Verletzungshandlungen *„durch die Herstellung oder Verbreitung von Vervielfältigungsstücken“* vorsah, was nach einer Auffassung dazu führen sollte, dass nur körperliche Verwertungshandlungen vom Anwendungsbereich des § 101a UrhG erfasst werden,[667] wird durch die Formulierung des § 101 Abs. 1 UrhG-E klargestellt, dass nunmehr jede Verletzungshandlung eine Auskunftspflicht begründet.[668] Zudem wird durch den Verzicht auf den Zusatz des § 101a UrhG, dass die Rechtsverletzung *„durch“* eine Handlung des Anspruchsgegners vorgenommen werden muss, auch der Auffassung die Grundlage entzogen, nach der sich der urheberrechtliche Drittauskunftsanspruch nur auf eigenhändige Verletzungshandlungen erstrecken soll.[669]

Dies ist zu begrüßen und entspricht im Wesentlichen der hier bereits zu § 101a Abs. 1 UrhG vertretenen Auslegung. Positiv zu werten ist weiterhin der Verzicht auf das Erfordernis, dass die Verletzungshandlung *„im geschäftlichen Verkehr“* vorgenommen werden muss, da dies bei § 101a UrhG zu Auslegungsproblemen hinsichtlich der erforderlichen Intensität einer Rechtsverletzung geführt hat.[670] Weiterhin kann nach § 101 Abs. 1 UrhG-E – im Gegensatz zu § 101a UrhG – nicht nur Auskunft über die Herkunft und den Vertriebsweg der rechtsverletzenden Vervielfältigungsstücke, sondern auch über sonstige Erzeugnisse verlangt werden. Dieser unpräzise Terminus der sonstigen Erzeugnisse dürfte als dahingehende Bekräftigung zu verstehen sein, dass sich die Auskunftspflicht des § 101 UrhG-E auch auf unkörperliche Vervielfältigungsstücke erstreckt.[671] Dennoch wird eine Auskunftspflicht des Access Providers nach § 101 Abs. 1 UrhG-E regelmäßig ausscheiden, da dieser nach der hier vertretenen Auf-

[667] Vgl. oben, 2. Teil A. II. 1.
[668] Referentenentwurf, a.a.O., S. 99.
[669] Vgl. oben, 2 Teil A. IV. 4. a).
[670] Siehe oben, 2.Teil, A. III.
[671] Vgl. Referentenentwurf, a.a.O., S. 99

fassung nur unter sehr restriktiven Voraussetzungen als Verletzer qualifiziert werden kann.[672]

II. Auskunftspflicht des Access Providers als Nichtverletzer

Als Anknüpfungspunkt für eine verletzungsunabhängige Auskunftspflicht des Access Providers kommt die Regelung des § 101 Abs. 2 S. 1 Nr. 3 UrhG-E in Betracht. Danach kann bei offensichtlichen Rechtsverletzungen sowie wenn der Verletzte gegen den Verletzer Klage erhoben hat, auch derjenige auf Auskunft in Anspruch genommen werden, der im gewerblichen Ausmaß für rechtsverletzende Tätigkeiten genutzte Dienstleistungen erbracht hat.

1. Auskunftspflicht nach Klageerhebung gegen den Nutzer

In dieser Hinsicht soll zunächst eine Auskunftspflicht des Access Providers nach § 101 Abs. 2 S. 1 Alt. 2 UrhG-E begutachtet werden. Danach wird die Auskunftspflicht des Nichtverletzers an die Bedingung geknüpft, dass bereits Klage gegen den Rechtsverletzer erhoben wurde. Mit dieser Regelung wird die Vorgabe aus Art. 8 Abs. 1 RL umgesetzt, dass zumindest im Zusammenhang mit einem gerichtlichen Verfahren wegen der Verletzung eines Rechts des geistigen Eigentums ein Auskunftsanspruch gegen Dritte zu gewähren ist.[673] Der Anwendungsbereich dieser Alternative dürfte jedoch gerade im Hinblick auf Auskunftsersuche gegen Access Provider sehr beschränkt sein, da eine Klageerhebung voraussetzt, dass dem Rechteinhaber der Rechtsverletzer (namentlich) bekannt ist. Denn anders als nach dem amerikanischen John-Doe-Verfahren, kann nach dem deutschen Zivilprozessrecht keine Klage gegen den anonymen Rechtsverletzer unter Angabe einer IP-Adresse erhoben werden. Dem steht § 253 ZPO entgegen, nach dem der Klagegegner in der Klageschrift zumindest durch Auslegung identifizierbar sein muss.[674] Von einer dahingehenden Änderung der Zivilprozessordnung, die solche Klageerhebungen ermöglichen würde, haben die Verfasser des Referentenentwurfs jedoch abgesehen, da die RL in dieser Hinsicht keine zwingenden Vorgaben enthält.[675]

---

[672] Vgl. oben, 2.Teil A. IV. 3.

[673] Referentenentwurf, a.a.O., S. 79 f.

[674] Vgl oben, 3. Teil E. I.

[675] Referentenentwurf, a.a.O., S. 80; zu Recht kritisch, Stellungnahme der Deutschen Landesgruppe der IFPI e.V. und des Bundesverbandes der Phonographischen Wirtschaft e.V. vom 16.2.2006 zum Referentenentwurf eines Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums (im Folgenden: Stellungnahme Phonoverbände), Ab-

Die Möglichkeit der Klageerhebung unter Angabe einer IP-Adresse böte hingegen einige Vorteile. Könnte der Rechteinhaber direkt Klage gegen den Rechtsverletzer erheben, würde sich ein gesondertes Verfahren gegen den Access Provider, wie dies in § 101 UrhG-E vorgesehen ist, erledigen. Zudem wäre der Access Provider im Verfahren des Rechteinhabers gegen den Nutzer nicht Partei, sondern Zeuge. Als solcher würde ihn kein Haftungs- und Kostenrisiko treffen. Zugleich wäre der Provider von jeglicher Prüfpflicht befreit, da die Anspruchsvoraussetzungen stets einer umfassenden richterlichen Kontrolle unterlägen.[676] Es ließe sich gegen diese Konstruktion durchaus einwenden, dass eine zwingende richterliche Kontrolle zu einer immensen Belastung der Gerichte führen könnte. Bedauerlich ist allerdings, dass der Referentenentwurf jegliche Auseinandersetzung mit dieser Thematik vermissen lässt.

Der Anwendungsbereich des § 101 Abs. 2 S. 1 Alt. 2 UrhG-E dürfte daher auf die Fälle der Offlinepiraterie beschränkt sein, bei denen bereits Klage gegen den bekannten Rechtsverletzer erhoben wurde und von einem Dritten, wie z.B. einem Spediteur, weitere Angaben i.S.d. § 101 Abs. 3 Nr. 1 u. 2 UrhG-E benötigt werden, um die Höhe der gegen den Verletzer gerichteten Schadensersatzforderung beziffern zu können. In diesen Fällen steht dem Antragssteller zudem gem. § 101 Abs. 2 S. 2 UrhG-E die Möglichkeit offen, einen Antrag auf Aussetzung des gerichtlichen Verfahrens zu stellen. Dadurch soll sichergestellt werden, dass die durch die Auskunftserteilung gewonnenen Erkenntnisse noch in den Rechtsstreit einfließen können.[677] Festzuhalten bleibt jedoch, dass eine Auskunftspflicht gem. § 101 Abs. 2 S. 1 Alt. 2 UrhG-E gegen Access Provider angesichts der nicht vorhandenen Möglichkeit einer Klageeinreichung unter Angabe einer IP-Adresse keine praktische Relevanz haben wird.

---

schnitt II, Nr. 11, abrufbar unter: http://www.ifpi.de/recht/pdf/20060216_ifpi_enforcement.pdf.

[676] Vgl. Stellungnahme des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) vom 26.4.2004 zum Thema Rechtsdurchsetzung im Internet im Rahmen des zweiten Korbs der Urheberrechtsreform (im Folgenden: Stellungnahme des BITKOM), S. 8 ff., abrufbar unter: http://www.bitkom.org/files/documents/Stellungnahme_Rechtsdurchsetzung_im_Internet_-_26-04-2004.pdf .

[677] Referentenentwurf, a.a.O., S. 80.

2. Auskunftspflicht bei offensichtlichen Rechtsverletzungen

Zur Begründung einer verletzungsunabhängigen Auskunftspflicht des Access Providers bietet sich daher allenfalls die Regelung des § 101 Abs. 2 S. 1 Alt. 1 UrhG-E an. Nach dieser kann ein Nichtverletzer auch unabhängig von einer vorherigen Klageerhebung auf Auskunft in Anspruch genommen werden, sofern sich die Rechtsverletzung des Dritten als offensichtlich darstellt. Teilweise wird behauptet, dass diese Regelung mit dem Abstellen auf eine offensichtliche Rechtsverletzung in ungerechtfertiger Weise zulasten der Rechteinhaber von Art. 8 RL abweicht. Danach werde die Auskunftspflicht des Dritten nämlich bereits durch einen *„die Verhältnismäßigkeit wahrenden Antrag"* begründet, nicht jedoch an das Vorliegen einer offensichtlichen Rechtsverletzung geknüpft.[678]

Diese Kritik ist unzutreffend. Art. 8 Abs. 1 RL schreibt lediglich vor, dass ein die Verhältnismäßigkeit wahrender Antrag zur Auskunftspflicht des Dritten führt, wenn bereits Klage gegen den Rechtsverletzer erhoben wurde. Dies betrifft die Fälle des § 101 Abs. 2 S. 1 Alt. 2 UrhG-E. Indem § 101 Abs. 2 S. 1 Alt. 1 UrhG-E allerdings auch eine Drittauskunftspflicht vorsieht, die unabhängig von einem gegen den Nutzer anhängigen Prozess gewährt wird, geht die Möglichkeit einer Drittauskunftspflicht bei offensichtlichen Rechtsverletzungen somit über den Regelungsgehalt des Art. 8 Abs. 1 RL sogar noch hinaus. Durch diese Regelung soll vielmehr dem in der RL nicht beachteten Umstand Rechnung getragen werden, dass die Rechteinhaber bereits vor Klageerhebung ein berechtigtes Interesse daran haben können, die Identität des Verletzers in Erfahrung zu bringen.[679]

Hinsichtlich der Anforderungen, die an eine offensichtliche Rechtsverletzung zu stellen sind, wird in der Entwurfsbegründung auf § 101a Abs. 3 UrhG verwiesen.[680] Somit ist die Offensichtlichkeit auch nach § 101 Abs. 2 UrhG-E erst dann zu bejahen, wenn die Rechtsverletzung so eindeutig ist, dass eine ungerechtfertigte Inanspruchnahme des Dritten ausgeschlossen werden kann.[681] In diesen Fällen soll sich der Auskunftsanspruch gem. § 101 Abs. 7 UrhG-E – wie im Falle des § 101a Abs. 3 UrhG – zugleich auch im einstweiligen Verfügungsverfahren durchsetzen lassen. Zugleich

---

[678] Stellungnahme der Filmwirtschaft vom 23.2.2006 zum Referentenentwurf eines Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums (im Folgenden: Stellungnahme der Filmwirtschaft), S. 4, abrufbar unter: http://www.spio.de/media_content/635.pdf

[679] Referentenentwurf, a.a.O., S. 80.

[680] Referentenentwurf, a.a.O., S. 80, 82.

[681] Vgl. Wandtke/Bullinger/Bohne, § 101 UrhG, Rn. 12 m.w.N.

soll der Auskunftspflichtige durch das Offensichtlichkeitserfordernis hinsichtlich der Prüfung entlastet werden, ob tatsächlich eine Rechtsverletzung des Dritten vorliegt.[682] An dieser von den Entwurfsverfassern intendierten Entlastungswirkung kann jedoch gezweifelt werden.

a) Entlastungswirkung durch das Offensichtlichkeitserfordernis

Zweifel an einer Entlastungswirkung auf der Seite der Auskunftspflichtigen bestehen bereits deshalb, weil nach dem Entwurf eben nicht jede Rechtsverletzung auskunftsbegründend wirken soll, sondern nur eine offensichtliche. Damit wird die Prüfpflicht letztlich nicht erleichtert, sondern lediglich auf das Merkmal der Offensichtlichkeit verlagert. Keine Hilfe verspricht da auch der Hinweis der Entwurfsverfasser, dass die Offensichtlichkeit der Rechtsverletzung sowohl bei Zweifeln in tatsächlicher als auch in rechtlicher Hinsicht entfallen soll.[683] Denn für die Rechteinhaber wird sich eine Verletzung ihrer Verwertungsrechte stets als offensichtlich darstellen und als solche an die Anspruchsgegner herangetragen werden.[684] Somit ist zunächst zu konstatieren, dass sich die von den Entwurfsverfassern intendierte Entlastungswirkung zumindest nicht bereits aus der Konzeption des § 101 Abs. 2 UrhG-E ergibt.

b) Entlastung der Beteiligten durch Einbeziehung von Verbänden

Interessant erscheint vor diesem Hintergrund der Vorschlag, eine solche Entlastungswirkung über einen Rückgriff auf die Grundsätze zur Grenzbeschlagnahme nach § 111b UrhG zu konstruieren.[685] So unterliegen auch nach § 111b Abs. 1 UrhG rechtsverletzende Gegenstände der Beschlagnahme nur, *„sofern die Rechtsverletzung offensichtlich ist“*. Hierzu hat sich in der Praxis ein Verfahren etabliert, nach dem die Kriterien der Offensichtlichkeit durch die Verbände der Schutzrechtsinhaber definiert werden. Die auf dieser Basis verfassten Anträge der Schutzrechtsinhaber werden sodann wiederum durch die Verbände gestellt. Dadurch soll der ord-

[682] Referentenentwurf, a.a.O., S. 80.
[683] Referentenentwurf, a.a.O., S. 80.
[684] Stellungnahme des Deutschen Forschungsnetzes (DFN) zu § 101 UrhG-E in Art. 6 des Referentenentwurf des Bundesministerium der Justiz v. 3.1.2006 für ein „Gesetz zur Verbesserung von Rechten des geistigen Eigentums“ (im Folgenden: Stellungnahme DFN), S. 4, abrufbar, unter: http://www.dfn.de/content/fileadmin/3Beratung/Recht/StellnFoReUrhG280206.pdf.
[685] Stellungnahme der Phonoverbände, a.a.O., Abschnitt II, Nr. 5.

nungsgemäße und missbrauchfreie Ablauf des Antrags- und Beschlagnahmeverfahrens gewährleistet werden.[686]

Für eine Übertragung dieser Grundsätze auf die Auskunftspflicht nach § 101 Abs. 2 UrhG-E spricht, dass dadurch sichergestellt werden könnte, dass die Auskunftsbegehren hinsichtlich des Inhalts und der Form bestimmten Mindestanforderungen genügen. Unter diesen Voraussetzungen könnte der Access Provider sodann die gewünschte Auskunft erteilen, ohne dass dieser in eine umfangreiche rechtliche Prüfung des Sachverhalts einsteigen müsste.[687] Sollte ein Auskunftsbegehren diesen Anforderungen nicht genügen, ist weiterhin zu fordern, dass der Access Provider diesem Begehren mangels Darlegung einer offensichtlichen Rechtsverletzung nicht nachzukommen braucht. Die Integration eines solchen Verfahrens in den Auskunftsanspruch des § 101 Abs. 2 UrhG-E erscheint daher sinnvoll. Damit dieses Verfahren jedoch auch durch die Verbände betrieben werden kann, sollte der Gesetzgeber von der Ermächtigung des Art. 4 lit. d RL Gebrauch machen und den Kreis der Passivlegitimierten auch auf Berufsorganisationen mit ordnungsgemäß anerkannter Befugnis zur Vertretung von Inhabern von Rechten des geistigen Eigentums erstrecken.[688] Die damit einhergehende Bündelung von Auskunftsbegehren dürfte darüber hinaus nicht nur im Interesse der Access Provider und der Rechteinhaber, sondern auch im Interesse der Verletzer und des Staates liegen. So wird durch eine Verletzungshandlung mitunter in die Verwertungsrechte mehrerer Rechteinhaber eingegriffen. Wenn deren Ansprüche gebündelt geltend gemacht werden könnten, würde dies einerseits die Prozesskosten für alle Beteiligten gering gehalten und andererseits einer übermäßigen Beanspruchung der Gerichte entgegenwirken.[689]

Bis zur Einführung eines solchen Verfahrens wird im Rahmen des § 101 Abs. 2 UrhG-E zumindest zu fordern sein, dass die Rechteinhaber die behauptete Rechtsverletzung z.B. durch Screenshots und dokumentierte

---

[686] Ausführlich dazu Wandtke/Bullinger, Kefferpütz, § 111b UrhG, Rn. 11 ff.

[687] Ähnlich Stellungnahme des BITKOM zum Referentenentwurf eines Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentum v. 14.2.2006, S. 2 *(„Meldung einer Rechtsverletzung unter Wahrung formaler Anforderungen“)*, abrufbar unter: http://www.bitkom.org/files/documents/Stellungnahme_RefE_zur_NachahmungsR_Endversion_14_02_06.pdf.

[688] So auch Stellungnahme der Filmwirtschaft vom 23.2.2006 zum Referentenentwurf eines Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums (im Folgenden: Stellungnahme der Filmwirtschaft), S. 9, abrufbar unter: http://www.spio.de/media_content/635.pdf; Zombik, ZUM 2006, 450, 455.

[689] Stellungnahme der Filmwirtschaft, a.a.O., S. 10.; Zombik, a.a.O.

Testdownloads nachweisen, den Access Providern darüber hinaus aussagekräftige Beweise für ihre Rechteinhaberschaft an den betreffenden Werken darlegen und zugleich versichern, dass dem potentiellen Rechtsverletzer an diesen Werken keinerlei Nutzungsrechte zustehen. Sofern ein Auskunftsbegehren diesen Anforderungen nicht genügt, sollte die Offensichtlichkeit einer Rechtsverletzung zu verneinen sein und damit auch die Auskunftspflicht insgesamt entfallen.

3. Gewerblichkeit des Access Providing

Weiterhin steht die Auskunftspflicht des Access Providers nach § 101 Abs. 2 UrhG-E unter dem Vorbehalt, dass dieser die für rechtsverletzende Tätigkeiten genutzten Dienstleistungen im gewerblichen Ausmaß erbracht hat. Hinsichtlich dieses Gewerblichkeitserfordernisses auf der Seite des Auskunftspflichtigen wird die berechtigte Kritik hervorgebracht, dass die Entwurfsverfasser diese Begrifflichkeit wörtlich aus Art. 8 Abs. 1 lit. c RL übernommen haben, ohne diesen Begriff jedoch näher zu konkretisieren.[690] Verstärkt wird diese Kritik dadurch, dass sich auch in der Richtlinie selbst hierzu keine direkten Ausführungen finden lassen. Darin wird in Erwägungsgrund 14 lediglich in Bezug auf gewerbliche Schutzrechtsverletzungen durch die Nutzer dieser Dienstleistungen darauf hingewiesen, dass von der Gewerblichkeit der Schutzrechtsverletzung auszugehen ist, wenn diese zur Erlangung eines unmittelbaren oder mittelbaren wirtschaftlichen oder kommerziellen Vorteils vorgenommen worden ist. Dies korrespondiert mit der Verwendung des Begriffs der Gewerblichkeit im aktuellen Regierungsentwurf zum Zweiten Korb der Urheberrechtsreform.[691] So wird auch in der Begründung zu § 53 Abs. 2 S. 1 Nr. 1 UrhG-E, nach dem eine zulässige Privatkopie voraussetzt, dass diese nicht zu gewerblichen Zwecke vorgenommen wurde, ausgeführt, dass ein gewerbliches Handeln auch bei der nur mittelbaren Vorfolgung von erwerbswirtschaftlichen Zwecken vorliegen soll.[692]

Seitens des Deutschen Forschungsnetzes (DFN) wird daher befürchtet, dass diese Begriffsbestimmung auch zur Konkretisierung gewerblich erbrachter Dienstleistungen i.S.d. § 101 Abs. 2 UrhG-E herangezogen wer-

---

[690] Stellungnahme des DFN, a.a.O., S. 2.

[691] Referentenentwurf für ein zweites Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft“ v. 3.1.2006 („Zweiter Korb“), S. 7, abrufbar unter: http://www.urheberrecht.org/topic/Korb-2/bmj/2006-01-03-Gesetzentwurf.pdf

[692] Referentenentwurf v. 3.1.2006 („Zweiter Korb), a.a.O., S. 59.

den könnte.[693] Dies würde laut DFN dazu führen, dass auch Hochschulen und Forschungseinrichtungen eine Auskunftspflicht nach § 101 UrhG-E treffen könnte, sofern deren Projekte mit Drittmitteln aus der Wirtschaft gefördert werden. Eine Gleichstellung mit der kommerziellen Providerwirtschaft sei jedoch nicht gerechtfertig, da der Schwerpunkt dieser Einrichtungen im Bereich der Wissenschaft und Forschung liege. Daher wird vorgeschlagen, den Anwendungsbereich des § 101 Abs. 2 UrhG-E auf *„unmittelbar zu Erwerbszwecken“* erbrachte Dienstleistungen zu beschränken.[694]

Dieser Auffassung ist hinsichtlich der Notwendigkeit einer Privilegierung für Einrichtungen der Forschung und Wissenschaft zuzustimmen. Um den Argumentationsspielraum hinsichtlich des Nichteingreifens der Auskunftspflicht für andere (kommerzielle) Provider nicht unnötig zu vergrößern, dürfte jedoch eine Beschränkung des Anwendungsbereichs auf „überwiegend zu Erwerbszwecken“ gerichtete Dienstleistungen als ausreichend zu erachten zu sein. Bei dieser Auslegung des § 101 Abs. 2 UrhG-E würden alle kommerziellen Access Provider, also solche, die den Internetzugang zum Zwecke der Gewinnerzielung anbieten, vom Anwendungsbereich dieser Regelung erfasst, zugleich jedoch Hochschulen und Forschungseinrichtungen ausgenommen.

4. Gewerbliche Verletzungshandlung auf der Nutzerseite

Obwohl der Wortlaut des § 101 Abs. 2 UrhG-E lediglich voraussetzt, dass der Anspruchsgegner im gewerblichen Maße tätig und die Rechtsverletzung des Nutzers offensichtlich ist, soll die Auskunftspflicht des Dritten nach der Entwurfsbegründung darüber hinaus unter dem Vorbehalt stehen, dass auch die Rechtsverletzung selbst ein gewerbliches Ausmaß erreicht.[695] Demzufolge muss also auch die Urheberrechtsverletzung des Nutzers des Access Providers das Merkmal der Gewerblichkeit erfüllen, um eine Auskunftspflicht des Access Providers nach § 101 UrhG-E auszulösen. Hinsichtlich der Voraussetzungen dieses Kriteriums wird auf Erwägungsgrund 14 der Richtlinie verwiesen.[696] Danach wird die Gewerblichkeit dahingehend definiert, dass die Handlung *„zwecks Erlangung eines unmittelbaren oder mittelbaren wirtschaftlichen oder kommerziellen Vorteils vorgenommen“* wird. Nicht darunter fallen sollen in gutem Glauben vorgenommene

[693] Stellungnahme des DFN, a.a.O., S. 3.
[694] Stellungnahme des DFN, a.a.O., S. 3.
[695] Referentenentwurf, a.a.O., S. 78.
[696] Referentenentwurf, a.a.O., S. 78.

Handlungen von Endverbrauchern sowie bösgläubige Handlungen, die eine Bagatellgrenze nicht überschreiten. Dies sollen Handlungen sein, denen keine *„gewisse Nachhaltigkeit“* innewohnt.[697]

a) Kritik am Gewerblichkeitserfordernis

Das im Referentenentwurf postulierte Gewerblichkeitserfordernis auf der Seite des Rechtsverletzers sieht sich gerade in Bezug auf den urheberrechtlichen Auskunftsanspruch nach § 101 UrhG-E mit einer erheblichen Kritik konfrontiert. Die wesentlichen Kritikpunkte sollen im Folgenden dargestellt und sodann ein Lösungsvorschlag unterbreitet werden.

aa) Nichtberücksichtigung struktureller Unterschiede zwischen den einzelnen Schutzrechten

Zunächst wird gegen das Erfordernis einer gewerblichen Verletzungshandlung eingewendet, dass dadurch die strukturellen Unterschiede zwischen den einzelnen Schutzrechten nicht genügend berücksichtigt würden.[698] Dass diese Kritik durchaus berechtigt ist, belegt ein Blick auf den mit § 101 UrhG-E korrespondierenden patentrechtlichen Auskunftsanspruch aus § 140b PatG-E. Denn während eine Patentrechtsverletzung, wie sich im Wege eines Umkehrschlusses (*arg. e contrario)* aus § 11 Nr. 1 PatG ergibt, stets eine Verletzungshandlung im gewerblichen Verkehr voraussetzt, wird eine Urheberrechtsverletzung bereits durch eine einfache, mithin nicht gewerbliche Verletzungshandlung begründet. Während somit also dem Inhaber eines Patentes bei jeder Verletzungshandlung ein Auskunftsanspruch nach § 140b PatG-E zur Seite steht, werden die Inhaber von Urheber- und Verwertungsrechten schlechter gestellt, wenn der Auskunftsanspruch nach § 101 UrhG-E ebenfalls nur bei gewerblichen Verletzungshandlungen eingreift. Bei strikter Einhaltung des Gewerblichkeitserfordernisses kommt es somit zu einer Verkürzung des urheberrechtlichen gegenüber dem patentrechtlichen Auskunftsanspruch. Vor diesem Hintergrund wird seitens der Rechteinhaber für einen Wegfall dieses Kriteriums im Rahmen des § 101 UrhG-E plädiert.[699]

---

[697] Referentenentwurf, a.a.O., S. 78.
[698] So Stellungnahme der Filmwirtschaft, a.a.O., S. 4 f.
[699] Stellungnahme der Filmwirtschaft, a.a.O., S. 4 f.; Stellungnahme der Phonoverbände, a.a.O., Abschnitt II, Punkt 6.

bb) Verstoß gegen Art. 41 TRIPS

Weiterhin soll das Erfordernis einer gewerblichen Verletzungshandlung gegen Art. 41 des TRIPS-Übereinkommens verstoßen, weil danach eine Beschränkung von zivilrechtlichen Rechtsbehelfen auf gewerbliche Verletzungshandlungen unzulässig sei.[700] Diese Kritik geht indes zu weit. Die Art. 41, 45 TRIPS sind lediglich als Institutsgarantie für Schadensersatzansprüche bei der Verletzung von geistigen Eigentumsrechten anzusehen.[701] Daher können diese auch keine verbindlichen Anforderungen an die Ausgestaltung von Drittauskunftsansprüchen stellen.

cc) Beweisprobleme im Onlinebereich

Die schwerwiegendste Kritik am Gewerblichkeitserfordernis entzündet sich an deren Beweisbarkeit. So wird befürchtet, dass durch das Gewerblichkeitserfordernis eine zivilrechtliche Verfolgung von Urheberrechtsverletzungen im Onlinebereich nahezu unmöglicht gemacht wird, da sich der Beweis einer gewerblichen Verletzungshandlung aufgrund der technischen Besonderheiten des Internets nur selten erbringen lassen wird.[702] Diese Kritik ist vor allem in Bezug auf dynamische IP-Adressen durchaus berechtigt. Stellt man hinsichtlich des – für das Vorliegen der Gewerblichkeit maßgeblichen – Kriteriums der Nachhaltigkeit[703] auf eine zeitliche Komponente ab, so wird ein dahingehender Nachweis regelmäßig daran scheitern, dass dem Nutzer bei jeder Einwahl ins Internet, spätestens jedoch nach 24 Stunden, vom Access Provider eine neue dynamische IP-Adresse zugewiesen wird.[704] Der Beweis der Nachhaltigkeit ließe sich somit allenfalls dann führen, wenn der Nutzer über eine statische IP-Adresse verfügt oder unter einer dynamischen IP-Adresse einen Server betreibt, dessen jeweils aktuelle IP-Adresse mittels eines sog. Dynamic-DNS-Dienstes mit einer permanenten Domain verknüpft wird.

Ferner ergeben sich unabhängig von der Verwendung dynamischer oder statischer IP-Adressen Beweisprobleme, wenn man hinsichtlich des Kriteriums der Nachhaltigkeit auf die Erheblichkeit bzw. den Umfang der Rechtsverletzung abstellt. Dies gilt vor allem in Bezug auf Rechtsverlet-

---

[700] Stellungnahme der Filmwirtschaft, a.a.O., S. 5; Stellungnahme der Phonoverbände, a.a.O., Abschnitt II, Punkt 6.
[701] Vgl. Spindler, vor § 8 TDG, Rn. 5 m.w.N.; siehe auch oben, 4. Teil C. I.
[702] Stellungnahme der Filmwirtschaft, a.a.O., S. 5 f.; Stellungnahme der Phonoverbände, a.a.O., Abschnitt II, Punkt 6.
[703] Vgl. Referentenentwurf, a.a.O., S. 78.
[704] Stellungnahme der Filmwirtschaft, a.a.O., S. 5 f.

zungen in Filesharing-Netzwerken. So ist es nämlich bei neuartigen Netzwerken, wie z.B. BitTorrent, nicht möglich, sich das gesamte Downloadangebot eines Nutzers anzeigen zu lassen, sondern nur die Anbieter eines zuvor explizit gesuchten Werkes.[705] Da für Außenstehende dadurch nicht erkennbar ist, wie viele Werke der einzelne Nutzer insgesamt bereithält, erweckt zunächst jeder Nutzer den Anschein des nicht gewerblichen Handelns.[706]

Festzuhalten bleibt, dass der Beweis hinsichtlich des gewerblichen Handelns auf der Nutzerseite aufgrund der technischen Besonderheiten des Internets, vor allem bei der Verwendung dynamischer IP-Adressen und bei Rechtsverletzungen in Filesharing-Netzwerken, nur schwer zu führen sein wird. Daher drohen Auskunftsansprüche nach § 101 UrhG-E insgesamt am Merkmal der gewerblichen Verletzungshandlung zu scheitern. Dieses Ergebnis stünde zudem im Widerspruch zu den Zielsetzungen der Entwurfsverfasser. Dem § 101 UrhG-E liegt nämlich gerade auch die Intention zugrunde, die (massenhaften) Schutzrechtsverletzungen in Filesharing-Netzwerken einzudämmen.[707]

dd) Widerspruch zu strafrechtlichen Sanktionen

Im Zusammenhang mit den drohenden Rechtsverfolgungsproblemen wurde insbesondere vor dem Hintergrund, dass auch im Referentenentwurf zum Zweiten Korb der Urheberrechtsreform die Einführung einer strafrechtlichen Bagatellklausel gem. § 106 Abs. 3 UrhG vorgesehen war,[708] bemängelt, dass den Rechteinhabern auch bei klar beweisbaren (einzelnen) Urheberrechtsverletzungen die Rechtsverfolgungsmöglichkeiten insgesamt genommen werden und geringfügige Urheberrechtsverletzungen somit faktisch legalisiert würden.[709] Dies soll nicht nur verfassungsrechtlich im Hinblick auf Art. 14 GG bedenklich sein, sondern auch deshalb, weil im Referentenentwurf zum Zweiten Korb hinsichtlich der strafrechtlichen Bagatellgrenze explizit ausgeführt wurde, dass es zwar nicht Aufgabe des Staates sei, die Schulhöfe zu kriminalisieren, es den Rechteinhaber jedoch frei stehe, zivilrechtliche Schadensersatzklagen gegen diese Nutzer zu erheben.[710] Auch diese Möglichkeit werde den Rechteinhabern jedoch genom-

[705] Vgl. Zombik, ZUM 2006, 450, 455.
[706] Stellungnahme der Phonoverbände, Abschnitt II, Punkt 6.
[707] Vgl. Referentenentwurf, a.a.O., S. 82.
[708] Referentenentwurf v. 3.1.3006 („Zweiter .Korb“), a.a.O. S. 14.
[709] Stellungnahme der Filmwirtschaft, a.a.O., S. 5.
[710] Referentenentwurf v. 3.1.3006 („Zweiter Korb“), a.a.O., S. 75.

men, wenn sich der Nachweis der Gewerblichkeit der Verletzungshandlung nicht erbringen lasse.[711]

Diese Kritik lässt sich zwar vor dem Hintergrund, dass sich die Bundesregierung mittlerweile – auf Druck der Rechteinhaber – für eine Streichung der strafrechtlichen Bagatellklausel ausgesprochen hat,[712] nicht mehr in dieser Weise aufrechterhalten. Denn somit ist auch bei Bagatelldelikten eine Strafverfolgung zumindest dem Grunde nach möglich. Allerdings lässt sich die Kritik auch unter diesen Vorzeichen führen. So erscheint es unverständlich, warum über den sog. „einfachen" Urheberrechtsverletzer das Damoklesschwert des Strafrechts hängen sollte, sich dessen Identität jedoch noch nicht einmal auf dem Zivilrechtswege feststellen lassen soll. Hält man neben den strafrechtlichen Sanktionen nämlich sowohl die Einführung einer zivilrechtlichen Auskunftspflicht als auch die einer Bagatellgrenze für erforderlich, so hätte es sicherlich näher gelegen, diese Bagatellgrenze im Strafrecht und nicht im Zivilrecht eingreifen zu lassen. Zudem wird dieser Umstand dazu führen, dass in den Fällen einzelner Schutzrechtsverletzungen die Staatsanwaltschaften wiederum massenhaft mit Strafanzeigen überzogen werden, da den Rechteinhabern einzig der Umweg über die strafprozessuale Akteneinsicht bliebe, um die Identität der Rechtsverletzer in Erfahrung zu bringen. Daher würde letztlich auch diese Problematik mit der Einführung des § 101 UrhG-E nicht beseitigt.

ee) Zwischenergebnis

Gegen die ungeschriebene Tatbestandsvoraussetzung, dass eine Auskunftspflicht des Nichtverletzers nach § 101 Abs. 2 UrhG-E nur dann besteht, wenn auch die Rechtsverletzung des Dritten ein gewerbliches Ausmaß erreicht, werden eine Reihe von Bedenken erhoben, die allesamt nicht ganz unberechtigt erscheinen. So wird darauf hingewiesen, dass eine derartige Beschränkung der urheberrechtlichen Drittauskunftspflicht unzulässig sein soll, weil diese die strukturellen Unterschiede zwischen den einzelnen Schutzrechten unberücksichtigt lässt. Weiterhin wird darauf aufmerksam gemacht, dass der Auskunftsanspruch im Onlinebereich, vor allem bei der Verwendung dynamischer IP-Adressen und bei Rechtsverletzungen in Fi-

[711] Stellungnahme der Filmwirtschaft, a.a.O., S. 5.

[712] Regierungsentwurf zum „Zweiten Korb" vom 22.3.2006, S. 37, abrufbar unter: http://www.bmj.de/media/archive/1174.pdf ; vgl. auch Heise News, Meldung v. 22.3.2006: Bundesregierung will bis zu drei Jahre Haftung für illegale Filesharer, http://www.heise.de/newsticker/meldung/71125.

lesharing-Netzwerken, weitestgehend leer läuft, da sich die Gewerblichkeit einer Rechtsverletzung in diesen Fällen nur schwerlich nachweisen lässt. Dies widerspricht der Intention der Entwurfsverfasser, da diese gerade auch die Bekämpfung von Rechtsverletzungen in Filesharing-Netzwerken vor Augen hatten. Zudem ist die Einführung einer solchen zivilrechtlichen Bagatellgrenze auch vor dem Hintergrund widersprüchlich, dass selbst das materielle Strafrecht keine derartige Bagatellgrenze vorsieht.

b) Lösungsvorschlag: Berücksichtigung des Gewerblichkeitserfordernisses im Rahmen der Verhältnismäßigkeitsprüfung

Sämtliche Kritik, die an dem im Referentenentwurf postulierten Gewerblichkeitserfordernis auf der Nutzerseite geäußert wurde, fußt auf einem gemeinsamen Standpunkt. Die Kritiker gehen davon aus, dass dieses Kriterium als (ungeschriebene) Tatbestandsvoraussetzung in den § 101 Abs. 2 UrhG-E hineinzulesen ist und daher alle Auskunftsansprüche an diesem Merkmal scheitern, sofern sich die Gewerblichkeit nicht zweifelsfrei beweisen lässt.

Die wesentlichen Kritikpunkte könnten jedoch dadurch abgemildert werden, dass man das Gewerblichkeitserfordernis lediglich als eines von mehreren Faktoren im Rahmen der Verhältnismäßigkeitsprüfung des § 101 Abs. 4 UrhG-E berücksichtigt. Dadurch würde zugleich den Gerichten die Möglichkeit eingeräumt, den Access Provider auch dann zur Auskunftserteilung zu verpflichten, wenn die Gewerblichkeit der Rechtsverletzung zwar nicht bewiesen werden kann, eine Abwägung mit anderen Faktoren jedoch ergibt, dass sich eine Auskunftserteilung ausnahmsweise dennoch als verhältnismäßig darstellt.[713]

Diese dogmatische Einordnung des Gewerblichkeitserfordernisses lässt sich auch durchaus mit dem Referentenentwurf in Einklang bringen. Denn auch die Entwurfsverfasser sind sich anscheinend unschlüssig, wie das Gewerblichkeitserfordernis in den Prüfungsaufbau zu integrieren ist. So wird zunächst in den Erläuterungen zu den Tatbestandsvoraussetzungen des § 101 Abs. 2 UrhG-E auf dieses Erfordernis hingewiesen. Dies spricht für eine Einordnung als ungeschriebene Tatbestandsvoraussetzung im Rahmen des § 101 Abs. 2 UrhG-E.[714] Weiterhin wird jedoch ausgeführt, dass das Gewerblichkeitserfordernis im Rahmen der Verhältnismäßigkeits-

[713] Dazu sogleich, 7 Teil C II. 2.

[714] Referentenentwurf, a.a.O., S. 78; daher eine Aufnahme des Gewerblichkeitserfordernisses in den Wortlaut des § 101 Abs. 2 UrhG-E fordernd, Stellungnahme des DFN, a.a.O., S. 3.

prüfung nach § 101 Abs. 4 UrhG-E zu berücksichtigen sein soll, nämlich hinsichtlich der Frage, ob die für eine Auskunftspflicht notwendige Bagatellgrenze überschritten ist.[715] Dies ist widersprüchlich, weil eine Berücksichtigung im Rahmen der Verhältnismäßigkeitsprüfung obsolet ist, wenn bereits eine gewerbliche Rechtsverletzung vorliegen muss, um die Tatbestandsvoraussetzungen des § 101 Abs. 2 UrhG-E zu erfüllen. Auch dieser Widerspruch löst sich jedoch auf, wenn man das Gewerblichkeitserfordernis auf der Ebene der Verhältnismäßigkeitsprüfung berücksichtigt. Eine dahingehende Auslegung des § 101 Abs. 2 UrhG-E steht zudem im Einklang mit der Enforcement-RL. Diese ist nämlich lediglich hinsichtlich der Einführung eines Auskunftsanspruchs bei gewerblichen Rechtsverletzungen verbindlich, stellt es andererseits jedoch ins Belieben der Mitgliedstaaten, diesen Anspruch auch bei nicht gewerblichen Rechtsverletzungen zu gewähren.[716] Die besseren Argumente sprechen somit dafür, die Gewerblichkeit der Rechtsverletzung nicht als starre Tatbestandsvoraussetzung im Rahmen des § 101 Abs. 2 UrhG-E, sondern als dynamisches Kriterium im Rahmen der Verhältnismäßigkeitsprüfung des § 101 Abs. 4 UrhG-E anzusehen. Zugleich würde dadurch den Gerichten eine flexible Möglichkeit an die Hand gegeben, um angemessen auf die unterschiedlichen Erscheinungsformen von Rechtsverletzungen im Onlinebereich reagieren zu können.

5. Verhältnismäßigkeit der Auskunftsverpflichtung

Ebenso wie der Auskunftsanspruch nach § 101a Abs. 1 UrhG, steht auch die Auskunftspflicht des § 101 UrhG-E gem. § 101 Abs. 4 UrhG-E unter dem Vorbehalt der Verhältnismäßigkeit. Erfreulich ist der Hinweis in den Entwurfsmaterialien, dass die Auskunft geeignet, erforderlich und angemessen sein muss, um den Grundrechtseingriff zu rechtfertigen.[717] Wurde nämlich hinsichtlich des Vorliegens einer unverhältnismäßigen Auskunftserteilung in den Gesetzesmaterialien zum PrPG lediglich auf den unzulässigen Ausforschungsbeweis hingewiesen,[718] wird durch diesen Passus nunmehr klargestellt, dass sich die Prüfung am öffentlich-rechtlichen Verhältnismäßigkeitsgrundsatz orientieren soll.[719]

---

[715] Referentenentwurf, a.a.O., S. 81.
[716] Erwägungsgrund 14 RL.
[717] Referentenentwurf, a.a.O., S. 81.
[718] Amtl. Begründung zum PrPG, BT-Drs. 11/4792, S. 32.
[719] Referentenentwurf, a.a.O., S. 81

Auch dies deckt sich mit der hier bereits zu § 101a UrhG vertretenen Auslegung der Verhältnismäßigkeitsklausel.[720] Daher kann an dieser Stelle, insbesondere hinsichtlich der Erforderlichkeit einer zivilrechtlichen Auskunftsverpflichtung angesichts der Möglichkeit der strafprozessualen Akteneinsicht, auf die obigen Ausführungen verwiesen werden.[721] Im Gegensatz zu § 101a UrhG steht der Inanspruchnahme des Access Providers zumindest in den Fällen, in denen dieser nach § 101 Abs. 2 UrhG-E als Nichtverletzer in Anspruch genommen wird, nicht die Problematik der Kostentragung entgegen. So sieht § 101 Abs. 2 S. 3 UrhG-E eine entsprechende Entschädigungsregelung vor, auf die im Folgenden noch eingegangen wird.

Da nach der hier vertretenen Auffassung das Erfordernis einer gewerblichen Verletzungshandlung im Rahmen des § 101 Abs. 4 UrhG-E zu berücksichtigen ist, ist weiterhin zu klären, unter welchen Voraussetzungen eine Auskunftspflicht des Nichtverletzers auch dann angemessen erscheint, wenn sich die Nachhaltigkeit einer Rechtsverletzung nicht zweifelsfrei belegen lässt. Sinnvoll erscheint in dieser Hinsicht, eine Differenzierung zwischen Verletzungshandlungen des § 19a UrhG und des § 16 UrhG vorzunehmen. Denn vor dem Hintergrund der Bekämpfung der Produktpiraterie fällt eine Rechtsverletzung des § 19a UrhG aufgrund ihres distributiven Charakters deutlich schwerer ins Gewicht als der einzelne unter Verstoß des § 16 UrhG vorgenommene Download. Daher erscheint es angebracht, bei Beweisschwierigkeiten hinsichtlich der Gewerblichkeit von Rechtsverletzungen zumindest bei Verletzungen des § 19a UrhG geringere Anforderungen an die Begründung einer Auskunftspflicht des Access Providers zu stellen.

6. Kosten der Auskunftserteilung

Der wesentliche Unterschied zur Auskunftspflicht aus § 101a UrhG besteht darin, dass der Provider nach § 101 Abs. 2 UrhG-E nicht als Verletzer, sondern als Dritter in Anspruch genommen wird. Im Gegensatz zum Verletzer kann dem Dritten jedoch nicht ohne weiteres eine Kostenlast hinsichtlich der Auskunftserteilung aufgebürdet werden. Diese Werteentscheidung ergibt sich für den Access Provider schon aus den Haftungsfreistellungen des TDG/MDStV (TMG), nach denen dieser für die von ihm übermittelten Inhalte nicht verantwortlich ist. Rechnung getragen wird diesem Umstand durch die Regelung des § 101 Abs. 2 S. 3 UrhG-E. Danach

[720] Siehe oben, 2 Teil A. V. 2.
[721] Siehe oben, 2.Teil A. V. 3. b).

kann der Auskunftspflichtige vom Verletzten Ersatz der für die Auskunftserteilung erforderlichen Kosten verlangen. Hinsichtlich der Höhe dieser Kosten wurde im Verfahren vor dem Oberlandesgericht Hamburg entschieden, dass für die Überprüfung einer einzelnen IP-Adresse Kosten i.H.v. 35 € anfallen.[722] Sollte zu diesem Zweck jedoch ein automatisiertes Abrufverfahren etabliert werden, dürften sich diese Kosten erheblich verringern.[723]

7. Schadensersatzhaftung des Access Providers

In haftungsrechtlicher Hinsicht sind Auskunftsbegehren für den Access Provider ein heikles Unterfangen. Kommt dieser einem Auskunftsbegehren nach, sieht er sich mit Schadensersatzansprüchen der Nutzer, anderenfalls mit Ansprüchen der Rechteinhaber konfrontiert. Der Auskunftsanspruch nach § 101 UrhG-E sieht mit den §§ 101 Abs. 6, Abs. 5 UrhG-E daher zwei Regelungen vor, mittels derer die Schadensersatzpflicht des Auskunftspflichtigen positivrechtlich konkretisiert wird.

a) Ausschluss von Schadensersatzansprüchen nach § 101 Abs. 6 UrhG-E

Nach § 101 Abs. 6 UrhG-E haftet derjenige, der einem unberechtigtem Auskunftsbegehren nach § 101 Abs. 1, Abs. 2 UrhG-E nachkommt, für eine wahre Auskunftserteilung nur dann, wenn er wusste, dass er zur Auskunftserteilung nicht verpflichtet war. Dogmatisch handelt es sich bei dieser Regelung um keine eigene Anspruchsgrundlage für Forderungen Dritter, sondern – wie bei den Haftungsregeln des TDG – um einen Filter zum Ausschluss solcher Forderungen.[724] Mit dem § 101 Abs. 6 UrhG-E soll laut der Entwurfsbegründung dem Umstand Rechnung getragen werden, dass der Verpflichtete in den Fällen des § 101 Abs. 2 UrhG-E zumeist nicht beurteilen kann, ob überhaupt eine Rechtsverletzung vorliegt.[725] Diesen Passus kann man daher durchaus als dahingehendes Eingeständnis werten, dass die von den Entwurfsverfassern intendierte Entlastungswirkung auf der Seite des Auskunftspflichtigen hinsichtlich des Vorliegens einer Rechtsverletzung allein durch die nach § 101 Abs. 2 UrhG erforderliche

[722] OLG Hamburg, Urt. v. 28.4.2005 – 5 U 156/04, JurPC Web-Dok. 62/2005, Abs. 23 = MMR 2005, 453 = CR 2005, 512.
[723] Dazu sogleich, 7. Teil C. III. 8. e).
[724] Referentenentwurf, a.a.O., S. 82.
[725] Referentenentwurf, a.a.O., S. 82.

Darlegung einer offensichtlichen Rechtsverletzung gerade nicht erreicht wird.[726]

Kritisch ist diese Regelung auch deshalb zu betrachten, weil der Access Provider aufgrund dieses gesetzlichen Haftungsprivilegs dazu geneigt sein dürfte, auch ohne ausreichende Prüfung des Begehrens Auskünfte über seine Nutzer zu erteilen, wenn deren Schadensersatzforderungen selbst im Falle einer unberechtigten Auskunftserteilung durch § 101 Abs. 6 UrhG-E ausgeschlossen werden. Dem Ziel der Entwurfsverfasser, durch einschränkende Voraussetzungen des Auskunftsanspruchs nach § 101 Abs. 2 UrhG, der *„Gefahr der Uferlosigkeit“* von Auskunftsbegehren entgegenzuwirken,[727] wird diese Regelung somit gerade nicht gerecht.[728]

b) Schadensersatzhaftung nach § 101 Abs. 5 UrhG-E

Erteilt der Auskunftspflichtige hingegen vorsätzlich oder grob fahrlässig eine falsche oder unvollständige Auskunft, ist er gem. § 101 Abs. 5 UrhG-E verpflichtet, dem Verletzten den daraus entstandenen Schaden zu ersetzen. Durch diese – nicht zwingend durch die Richtlinie vorgegebene – Regelung soll das Defizit beseitigt werden, dass fehlerhafte Auskünfte nach der bisherigen Gesetzeslage weitgehend folgenlos bleiben, da es hinsichtlich der Erfüllung dieser Ansprüche zumeist nicht auf deren Richtigkeit und Vollständigkeit ankommt.[729] Insofern stellt § 101 Abs. 5 UrhG-E – im Gegensatz zu § 101 Abs. 6 UrhG-E – keinen Filter, sondern eine eigenständige Anspruchsgrundlage für gegen den Access Provider gerichtete Schadensersatzforderungen der Rechteinhaber dar.

Kritisiert wird an dieser Regelung, dass sie im Zusammenspiel mit der Haftungsfreistellung des § 101 Abs. 6 UrhG-E dazu führe, dass Access Provider auch bei Zweifeln an der Begründetheit eines Auskunftsverlangens die begehrte Auskunft erteilen werden, um sich im Falle der Nichterteilung der Auskunft nicht nach § 101 Abs. 5 UrhG-E schadensersatzpflichtig zu machen.[730] Diese Auffassung impliziert damit sogleich, dass Schadensersatz nach § 101 Abs. 5 UrhG-E auch dann gewährt wird, wenn überhaupt keine Auskunft erteilt wird. Der Wortlaut dieser Regelung legt indes eher nahe, dass Ersatzansprüche nach § 101 Abs. 5 UrhG-E erst dann

[726] Dazu schon oben, 7.Teil C. II. 2.; ähnlich Kitz, ZUM 2006, 444, 446.
[727] So aber Referentenentwurf, a.a.O., S. 79.
[728] Stellungnahme des DFN, a.a.O., S. 4.
[729] Referentenentwurf, a.a.O., S. 81.
[730] Stellungnahme des DFN, a.a.O., S. 4.

zum Tragen kommen, wenn tatsächlich eine Auskunft erteilt wurde, diese jedoch falsch oder unvollständig ist.

Im Kern trifft diese Kritik allerdings zu. Kommt der Access Provider dem Auskunftsbegehren nämlich nicht nach, droht zumindest eine gerichtliche Geltendmachung dieses Anspruchs, so dass der Access Provider im Falle des Unterliegens mit den Gerichtskosten belastet wäre. Die Belastung des Access Providers mit solchen Kosten erweist sich jedoch als unverhältnismäßig, weil dem Access Provider einerseits die Haftungsprivilegierungen des TDG zur Seite stehen und dieser andererseits im Rahmen des § 101 Abs. 2 UrhG-E als Nichtverletzer in Anspruch genommen wird.[731] Da für den Access Provider aufgrund der Haftungsfreistellung des § 101 Abs. 6 UrhG-E jedoch kein Grund ersichtlich ist, diese Auskunft nicht zu erteilen, kann der Entwurfsbegründung zumindest in der Hinsicht zugestimmt werden, dass es für den Auskunftspflichtigen wirtschaftlich nicht sinnvoll ist, den Sachverhalt zu bestreiten und einen umfangreichen Prozess zu führen.[732] Dass dadurch zugleich die Gefahr potenziert wird, dass die Nutzer des Access Providers einer unberechtigten Rechtsverfolgung Dritter ausgesetzt werden, wird im Referentenentwurf hingegen nicht erwähnt.

c) Zwischenergebnis

Der Haftungsausschluss des § 101 Abs. 6 UrhG-E, nach dem die Haftung des Access Providers gegenüber Dritten auf vorsätzlich unberechtigte Auskunftserteilungen begrenzt ist, führt einerseits zu einer begrüßenswerten Privilegierung des Access Providers, wirkt sich andererseits jedoch zulasten der Nutzer aus, da diesen selbst im Falle unberechtigter Auskunftserteilungen kein Schadensersatzanspruch zur Seite steht. Aus diesem Grund dürften die Access Provider dazu geneigt sein, selbst bei Zweifeln über die Berechtigung des Auskunftsverlangens, die gewünschte Auskunft zu erteilen. Dieser negative Effekt für die Nutzer wird durch die drohende Ersatzhaftung der Provider aus § 101 Abs. 5 UrhG-E bzw. durch die im Falle eines gerichtlichen Unterliegens anfallenden Gerichtskosten noch zusätzlich verstärkt. Vor diesem Hintergrund stellt sich die Frage, ob dem berechtigten Interesse der Nutzer, nicht ins Fadenkreuz einer unberechtigten Rechtsverfolgung Dritter zu geraten, zumindest durch den Richtervorbehalt des § 101 Abs. 9 UrhG-E Rechnung getragen wird.

---

[731] Ähnlich Kitz, ZUM 2006, 444, 446.

[732] Vgl. Referentenentwurf, a.a.O., S. 79; so auch Stellungnahme des DFN, a.a.O., S. 4.

8. Richtervorbehalt nach § 101 Abs. 9 UrhG-E

Der Sinn und Zweck eines Richtervorbehalts besteht darin, erhebliche Grundrechtseingriffe einer vorherigen unabhängigen Kontrolle zuzuführen.[733] In diesem Sinne bestimmt § 109 Abs. 9 UrhG-E, dass es einer vorherigen richterlichen Anordnung bedarf, wenn die Auskunft nur unter Verwendung von – dem Fernmeldegeheimnis unterfallenden – Verkehrsdaten i.S.d. § 3 Nr. 30 TKG erteilt werden kann.

Die Entwurfsverfasser wollten nur diesen *„Sonderfall"*[734] mit einem Richtervorbehalt versehen, da sie davon ausgingen, dass ein Richtervorbehalt für sämtliche Auskunftsbegehren angesichts der Vielzahl von zu erwartenden Verfahren zu einer nicht hinnehmbaren Belastung der Gerichte führen würde. Zugleich wollte man die Kostenlast der Rechteinhaber gering halten.[735] Aus diesen Gründen entschied man sich, mit Ausnahme der Auskunft über Verkehrsdaten, die Auskunftspflicht nicht durch einen allgemeinen Richtervorbehalt, sondern durch materiell-rechtliche Tatbestandsvoraussetzungen zu konkretisieren.[736]

Im Folgenden ist zu untersuchen, ob auch Auskünfte zu IP-Adressen in den Anwendungsbereich des § 101 Abs. 9 UrhG-E fallen und somit einer richterlichen Anordnung bedürfen. Sollte dies zutreffen, stellt sich die Frage, ob es tatsächlich zwingend erforderlich ist, diese Auskünfte unter einen Richtervorbehalt zu stellen. Anschließend soll der Ablauf des Anordnungsverfahrens nach § 101 Abs. 9 UrhG-E dargestellt sowie ein Alternativvorschlag zu diesem Verfahren erörtert werden.

a) Anordnungserfordernis bei Auskünften zu IP-Adressen

Wird von einem Access Provider Auskunft über den Inhaber einer IP-Adresse begehrt, sind nach der hier vertretenen Auffassung stets dem Fernmeldegeheimnis unterliegende Verkehrsdaten i.S.d. § 3 Nr. 30 TKG betroffen. Dies gilt nicht nur für die – ausschließlich als Kennungen i.S.d. § 96 Abs. 1 Nr. 1 TKG zu qualifizierenden – dynamischen IP-Adressen, sondern auch für statische IP-Adressen, da bei Auskünften zu konkreten Kommunikationsvorgängen nicht deren Ausprägung als Bestandsdatum

[733] BVerfG, Urt. v. 20.2.2001 – 2 BvR 1444/00, BVerfGE 103, 142, 151.
[734] Referentenentwurf, a.a.O., S. 79.
[735] Referentenentwurf, a.a.O., S. 79.
[736] Referentenentwurf, a.a.O., S. 79.

i.S.d. § 95 TKG, sondern ebenfalls deren technische Ausprägung als Verkehrsdatum i.S.d. § 96 Abs. 1 Nr. 1 TKG betroffen ist.[737]

Von den Rechteinhabern wird in dieser Hinsicht wiederum ins Feld geführt, dass das Fernmeldegeheimnis bei Auskünften zu IP-Adressen gar nicht tangiert werde. Dies resultiere entweder daraus, dass das Auskunftsbegehren auf den Namen und die Anschrift des Nutzers und somit auf ein Bestandsdatum gerichtet ist,[738] oder aber, weil der fragliche Kommunikationsvorgang von vornherein an die Öffentlichkeit gerichtet sei und damit nicht der vom Schutzbereich erfassten Individualkommunikation unterfalle.[739] Wie oben bereits ausgeführt,[740] verkennen diese Auffassungen jedoch, dass bei Auskünften zu IP-Adressen stets in das Fernmeldegeheimnis eingegriffen wird. Bezieht sich das Begehren auf dynamische IP-Adressen ist dies bereits durch das Auslesen der Daten zum Zwecke der Identifizierung des Nutzers der Fall. Bei Auskünften zu statischen IP-Adressen wird zumindest durch die Auskunftserteilung in das Fernmeldegeheimnis eingegriffen. Zudem wird auch gerade keine Auskunft zu dem öffentlich gemachten Teil des Kommunikationsvorgangs begehrt, sondern über den diesen vorgelagerten Akt der (individuellen) Zugangsgewährung. Auskunftsersuche zu IP-Adressen bedürfen daher stets einer richterlichen Anordnung nach § 101 Abs. 9 UrhG-E. Insofern kann zu Recht davon gesprochen werden, dass der von den Entwurfsverfassern deklarierte *„Sonderfall“* zumindest in Bezug auf Auskunftsersuche zu IP-Adressen zum Regelfall wird. [741]

b) Erforderlichkeit eines Richtervorbehalts

Kritisch ist weiterhin anzumerken, dass der Referentenentwurf jegliche Diskussion hinsichtlich der Notwendigkeit eines Richtervorbehalts vermissen lässt.[742] Wenn nämlich, wie die Entwurfsverfasser betonen, die Belastung der Gerichte möglichst gering gehalten werden sollte,[743] so hätte es

---

[737] Siehe oben, 5. Teil B. I. 2.

[738] Stellungnahme des Börsenvereins des Deutschen Buchhandels e.V. v. 16.2.2006 zum Referentenentwurf für ein Gesetz zur Verbesserung der Durchsetzung von Rechten des Geistigen Eigentums (im Folgenden: Stellungnahme des Buchhandels), Punkt 3a, abrufbar unter: http://www.boersenverein.de/de/69181?rubrik=82993&dl_id=108190 , unter Verweis auf LG Stuttgart, Beschl. v. 4.1.2005 – 13 Qs 89/04, CR 2005, 598 = NJW 2005, 614.

[739] Stellungnahme der Filmwirtschaft, a.a.O., S. 3.

[740] 5. Teil B. I.

[741] Stellungnahme des DFN, a.a.O., S. 4.; Zombik, ZUM 2006, 450, 453.

[742] So auch Stellungnahme der Filmwirtschaft, a.a.O., S. 4.

[743] Referentenentwurf, a.a.O., S. 79.

zumindest einer Auseinandersetzung mit der Möglichkeit einer gesetzlichen Ermächtigung zur Herausgabe dieser Daten bedurft. Denn als zwingend kann der Richtervorbehalt nach § 101 Abs. 9 UrhG-E bereits deshalb nicht betrachtet werden, weil nach § 88 Abs. 3 S. 3 TKG Eingriffe in das Fernmeldegeheimnis auch durch eine einfachgesetzliche Regelung gerechtfertig werden können, sofern diese erkennen lässt, dass der Gesetzgeber eine bewusste Abwägung zwischen dem Fernmeldegeheimnis und den Interessen Dritter vorgenommen hat.[744] Von einer solchen Ermächtigung hat der Gesetzgeber auch in dem bereits angesprochenen Grenzbeschlagnahmeverfahren nach § 111b UrhG Gebrauch gemacht. So wird auch nach § 111b Abs. 2 S. 2 UrhG in den Fällen, in denen das Fernmeldegeheimnis betroffen ist, keine richterliche Anordnung hinsichtlich der Auskunftserteilung über den Namen und die Anschrift des vermeintlichen Verletzers verlangt. In dieser Hinsicht ist allerdings anzumerken, dass der in § 101 Abs. 9 UrhG-E vorgesehene Richtervorbehalt zumindest solange nicht durch eine gesetzliche Ermächtigungsgrundlage ersetzt werden sollte, wie es bei der durch die Haftungskonzeption des § 101 UrhG-E bedingten Gefahr verbleibt, dass datenschutzrechtliche Belange der Nutzer nur unzureichend berücksichtigt werden.

c) Ablauf des Anordnungsverfahrens

Hinsichtlich des Ablaufs des Anordnungsverfahrens sind gem. § 101 Abs. 9 S. 4 UrhG-E die Vorschriften des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit (FGG) entsprechend heranzuziehen. Da diese Regelungen für die vorliegenden Konstellationen jedoch keinen Gerichtsstand vorsehen, setzt § 101 Abs. 9 S. 2 in UrhG – in Anlehnung an § 143 Abs. 1 PatG – eine ausschließliche Zuständigkeit der landgerichtlichen Zivilkammern fest.[745] Gegen die Entscheidungen des Landgerichts ist gem. § 101 Abs. 9 S. 6 UrhG-E die sofortige Beschwerde zum Oberlandesgericht statthaft. Diese ist jedoch auf eine rechtliche Überprüfung beschränkt und zudem unanfechtbar (vgl. § 101 Abs. 9 S. 8 UrhG-E).

Kritik an dem Ablauf des Anordnungsverfahrens wird zunächst an der Regelung des § 101 Abs. 9 S. 2 UrhG-E geübt, nach der sich die örtliche Zuständigkeit der Landgerichte nach dem Wohnsitz, dem Sitz oder der Niederlassung des zur Auskunft Verpflichteten richtet. Kritisiert wird daran,

[744] Zerres, in: Scheurle/Mayen, TKG, § 85, Rn. 40; a.A. Breyer, Vorratsdatenspeicherung, S. 119, der in Bezug auf staatliche Zugriffe auf nähere Telekommunikationsumstände einen Richtervorbehalt für zwingend erforderlich hält.

[745] Referentenentwurf, a.a.O., S. 83.

dass eine solche Aufspaltung der örtlichen Zuständigkeit zu einer unterschiedlichen Spruchpraxis führen könne, die einerseits der Rechtssicherheit abträglich wäre und andererseits die Gefahr berge, dass die Rechtsverletzer ihre Aktivitäten in die Sphäre desjenigen Anbieters verlagern, in der sich eine für die Rechtsverletzer günstige Rechtsprechung herausgebildet hat.[746]

Berechtigt ist diese Kritik nur insofern, als dass man – in Anlehnung an § 16 Abs. 4 UrhWahrnG – die Vorteile einer ausschließlichen Zuständigkeitsregelung zumindest hätte erörtern können. Die Befürchtung, dass die Rechtsverletzer zu einem Provider wechseln, in dessen Gerichtsbezirk sich eine für sie freundliche Spruchpraxis herausgebildet hat, ist jedoch unbegründet. Sofern seitens der Rechtsverletzer tatsächlich Überlegungen angestellt werden, wie man sich der Rechtsverfolgung entziehen kann, dürfte die Wahl wohl eher auf die Nutzung eines (ausländischen) Anonymisierungsdienstes fallen oder aber eine Einwahl über einen ausländischen Provider in Betracht gezogen werden, der keiner Auskunftspflicht unterliegt.

d) Kosten des Anordnungsverfahrens

Bezüglich der Kosten des Anordnungsverfahrens sieht der Entwurf in Art. 1 eine Ergänzung der Kostenordnung (KostO) durch die Regelung des § 128c KostO-E vor. Danach beläuft sich die Gebühr für die richterliche Anordnung über die Verwendung von Verkehrsdaten auf 200 €. Wird der Antrag vorher zurückgenommen, ist eine Gebühr von 50 € zu entrichten. Nach § 101 Abs. 9 S. 5 UrhG-E sind diese Kosten vom Verletzten zu tragen, also von den Rechteinhabern. Die dadurch bedingte Entlastung des – als Nichtstörer zu qualifizierenden – Dritten ist zu begrüßen und vor dem Hintergrund der Verhältnismäßigkeit nicht zuletzt auch verfassungsrechtlich geboten. Die Rechteinhaber können sowohl die für die richterliche Anordnung nach § 101 Abs. 9 UrhG-E zu entrichtenden Kosten als auch die nach § 101 Abs. 2 S. 3 UrhG-E an den Access Provider zu zahlende Aufwandsentschädigung im Rahmen des gegen den Urheberrechtsverletzer gerichteten Schadensersatzanspruchs geltend machen und sich somit an diesem schadlos halten.[747]

Dennoch wird seitens der Rechteinhaber gegen die Kostentragungsregeln des Entwurfs eingewendet, dass diese einen ruinösen Charakter hätten, der eine flächendeckende Bekämpfung der Onlinepiraterie, vor allem in Filesharing-Netzwerken, unmöglich mache. Ruinös seien sie deshalb, weil die

[746] Stellungnahme der Phonoverbände, a.a.O., Abschnitt II, Nr. 9.
[747] Vgl. Referentenentwurf, a.a.O., S. 83.

Eindämmung der Onlinepiraterie im Gegensatz zur Offlinepiraterie ein Vorgehen gegen eine Vielzahl von Rechtsverletzern erforderlich mache, was zu einem erheblichen Ausfallrisiko hinsichtlich des Kostenersatzes führe. Da viele Rechteinhaber aus diesem Grund von einer Rechtsverfolgung absehen werden, würden diese Kosten letztlich sogar prohibitiv wirken.[748]

e) Alternativvorschlag: Vorgeschaltetes Abrufverfahren nach dem Vorbild der Grenzbeschlagnahme

Vor allem im Hinblick auf die von den Rechteinhabern zu tragenden Kosten eines Anordnungsverfahrens nach § 101 Abs. 9 UrhG-E, erheben die Rechteinhaber Bedenken an der Vereinbarkeit dieses Verfahrens mit Art. 3 Abs. 1 RL. Danach dürfen *„Maßnahmen, Verfahren und Rechtsbehelfe nicht unnötig kompliziert und kostspielig sein“*.[749] Aus diesem Grund unterbreiten die Rechteinhaber den Vorschlag, dem Anordnungsverfahren nach § 101 Abs. 9 UrhG-E ein automatisiertes Abrufverfahren vorzuschalten, dass sich wiederum an dem Verfahren der Grenzbeschlagnahme nach § 111b UrhG orientieren soll.[750] Demnach soll zunächst eine staatliche Stelle bestimmt werden, die – wie die Zollbehörden im Rahmen der Grenzbeschlagnahme – als Puffer zwischen den (widerstreitenden) Interessen der Beteiligten fungiert. Vorgeschlagen wird, diese Stelle z.B. bei der Regulierungsbehörde anzusiedeln. Dort könne sodann ein vollständig automatisiertes EDV-Verfahren betrieben werden. Der Ablauf dieses vorgeschlagenen Verfahrens soll im Folgenden kurz dargestellt werden.[751]

aa) Ablauf des vorgeschalteten Abrufverfahrens

1. Nachdem der Rechteinhaber auf einen Rechtsverstoß aufmerksam wurde, kann er diesen auf der automatisierten Erfassungsmaske des Systems zur Meldung bringen. Dabei hat er Angaben über den Gegenstand und den exakten Zeitpunkt der Rechtsverletzung sowie über die IP-Adresse des vermeintlichen Rechtsverletzers zu machen.

2. Diese Daten werden daraufhin automatisch an den entsprechenden Access Provider weitergeleitet. Von diesem werden die auf die Verbindungs-

---

[748] Stellungnahme der Phonoverbände, a.a.O., Abschnitt II, Nr. 8; Stellungnahme des Buchhandels, a.a.O., Punkt 3b.
[749] Stellungnahme der Filmwirtschaft, a.a.O., S. 7.
[750] Stellungnahme der Phonoverbände, a.a.O., Abschnitt II, Nr. 3.
[751] Ausführlich dazu, Stellungnahme der Phonoverbände, a.a.O., Abschnitt II, Nr. 3.

daten gestützten Bestandsdaten – ohne Prüfung – wiederum automatisch an die Behörde übermittelt.

3. Seitens der Behörde wird sodann der potentielle Rechtsverletzer davon in Kenntnis gesetzt, dass ihm ein Rechtsverstoß zur Last gelegt und die Ermittlung seiner Identität begehrt wird. Diesem soll nunmehr die Möglichkeit eingeräumt werden, z.B. durch Schweigen, der Weitergabe seiner Daten zuzustimmen oder aber zu widersprechen. Für den Fall des Widerspruchs ist der potentielle Verletzer zudem darauf aufmerksam zu machen, dass er im Falle des Unterliegens die für die Auskunft angefallen Kosten zu ersetzen hat. In beiden Fällen würde dem Rechteinhaber daraufhin die Entscheidung des vermeintlichen Verletzers mitgeteilt. Sollte der Verletzer der Weitergabe seiner Daten zugestimmt haben, werden diese sodann an den Rechteinhaber übermittelt. Somit muss der Rechteinhaber nur im Falle eines Widerspruchs des Nutzers das Anordnungsverfahren nach § 101 Abs. 9 UrhG-E einleiten.

bb) Vorteile eines vorgeschalteten Abrufverfahrens

Die Einführung eines solchen Abrufverfahrens kann einige Vorteile auf sich vereinen. Zunächst hätten die Rechteinhaber lediglich dann die Kosten für die richterliche Anordnung gem. § 128c KostO-E i.H.v. 200 € zu entrichten, wenn der vermeintliche Verletzer der Weitergabe seiner Daten nicht zugestimmt hat. Für den Rechtsverletzer, der seinen Rechtsverstoß anerkennt und deshalb in die Weitergabe seiner Daten einwilligt, wäre dies mit dem Vorteil verbunden, dass sich auch die gegen ihn gerichtete Schadensersatzerforderung erheblich verringern würde. Dem Verletzer wären allenfalls die für das automatisierte Abrufverfahren anfallenden Kosten aufzuerlegen. Diese dürften sich allerdings auf einen Bruchteil der sonst zu veranschlagenden 200 € belaufen. Gleiches gilt für die letztlich auch vom Verletzer zu tragenden Kosten für die Auskunftserteilung durch den Access Provider. Auch diese dürften durch das automatisierte Verfahren geringer ausfallen. Gleichzeitig verbliebe dem Nutzer die Möglichkeit, durch Widerspruch gegen die Weitergabe seiner Daten eine gerichtliche Überprüfung gem. § 101 Abs. 9 UrhG-E herbeizuführen. Weiterhin würde die Etablierung eines solches Verfahrens zu der von den Entwurfsverfassern gewünschten Entlastung der Gerichte führen, da diese nicht mehr bei jedem Auskunftsbegehren zu IP-Adressen tätig werden müssten.[752] Hinsichtlich der Errichtung und Unterhaltung eines solchen automatisierten Abruf-

[752] Vgl. Zombik, ZUM 2006, 450, 454.

verfahrens könnte zudem an eine privatwirtschaftliche Finanzierung gedacht werden, vor allem durch die Rechteinhaber. Nicht zuletzt vor dem Hintergrund des Art. 3 Abs. 1 RL, erscheint die Einführung eines solchen Verfahrens aufgrund der daraus resultierenden Vorteile für alle Beteiligten durchaus sinnvoll.

f) Zwischenergebnis

Auskunftsersuche zu IP-Adressen bedürfen stets einer richterlichen Anordnung nach § 101 Abs. 9 UrhG-E. Die Statuierung eines solchen Richtervorbehalts kann jedoch nicht als zwingend betrachtet werden, da dieser auch durch eine gesetzliche Ermächtigungsgrundlage ersetzt werden könnte. Die Einführung einer solchen Ermächtigungsgrundlage ist jedoch abzulehnen, da das Interesse der Nutzer an der Geheimhaltung ihrer Daten durch die Haftungskonzeption des § 101 UrhG-E nicht ausreichend berücksichtigt wird. Um einer unnötigen Belastung aller Beteiligten vorzubeugen, sollte jedoch die Einführung eines – der richterlichen Anordnung vorgeschalteten – automatisierten Abrufverfahrens nach dem Vorbild der Grenzbeschlagnahme des § 111b UrhG erwogen werden.

III. Zusammenfassung

Mit der Regelung des § 101 UrhG-E soll der Auskunftsanspruch des Art. 8 RL in deutsches Recht umgesetzt werden. Dieser Anspruch richtet sich gem. § 101 Abs. 1 UrhG-E – wie auch § 101a UrhG – zunächst gegen den Rechtsverletzer. Von besonderem Interesse für die Auskunftspflicht des Access Providers ist allerdings die Bestimmung des § 101 Abs. 2 Nr. 3 UrhG-E, die auch eine Auskunftspflicht des Nichtverletzers statuiert, sofern dieser *„für rechtsverletzende Tätigkeiten genutzte Dienstleistungen erbrachte“*. Diese Auskunftspflicht steht zunächst unter dem Vorbehalt, dass entweder bereits Klage gegen den Nutzer erhoben wurde oder aber dessen Rechtsverletzung als offensichtlich zu qualifizieren ist. Die erste Alternative dürfte keine praktische Relevanz haben, da die Rechteinhaber ohne Kenntnis der Identität des Rechtsverletzers keinen – den Anforderungen des § 253 ZPO genügenden – Klageantrag stellen können.

Somit wird es in der Regel darauf ankommen, ob sich die Rechtsverletzung des Nutzers als offensichtlich darstellt. Diesem Erfordernis liegt die gesetzgeberische Intention zugrunde, dass der Anspruchsgegner hinsichtlich der Prüfung entlastet werden soll, ob tatsächlich eine Rechtsverletzung vorliegt. Da sich eine solche Entlastungswirkung jedoch nicht bereits aus der Gesetzeskonzeption des § 101 Abs. 2 UrhG-E ableiten lässt, sollte zur

Konkretisierung des Merkmals der Offensichtlichkeit eine Parallele zur Grenzbeschlagnahme nach § 111b UrhG-E gezogen werden und die Offensichtlichkeit einer Rechtsverletzung daher erst dann zu bejahen sein, wenn die Rechteinhaber einen Antrag stellen, der bestimmte inhaltliche Mindestanforderungen erfüllt.

Weiterhin setzt die Begründung einer Auskunftspflicht des Nichtverletzers nach § 101 Abs. 2 UrhG-E voraus, dass dieser die für Rechtsverletzungen genutzten Dienstleistungen in gewerblichem Ausmaß erbracht hat. Vor dem Hintergrund drittmittelfinanzierter Forschungsprojekte erscheint es sinnvoll, dieses Kriterium nicht bereits bei „mittelbar zu Erwerbszwecken", sondern erst bei „überwiegend zu Erwerbszwecken" erbrachten Dienstleistungen als erfüllt anzusehen, da es nicht gerechtfertigt wäre, auch Einrichtungen der Forschung und Bildung mit derartigen Auskunftspflichten zu belegen.

Heftig umstritten ist das von Entwurfsverfassern postulierte – jedoch nicht in den Wortlaut des § 101 UrhG-E aufgenommene – Erfordernis, dass auch die Rechtsverletzung des Nutzers selbst ein gewerbliches Ausmaß erreicht haben muss. Berechtigt erscheint insbesondere die Kritik, dass sich die Gewerblichkeit von Rechtsverletzungen aufgrund der technischen Besonderheiten im Onlinebereich gerade bei der Verwendung dynamischer IP-Adressen und bei Rechtsverletzungen in Filesharing-Netzwerken nur schwerlich beweisen lässt. Daher sollte das von den Entwurfsverfassern postulierte Gewerblichkeitserfordernis nicht als starre Tatbestandsvoraussetzungen im Rahmen des § 101 Abs. 2 UrhG-E angesehen werden, sondern als dynamisches Kriterium im Rahmen der Verhältnismäßigkeitsprüfung des § 101 Abs. 4 UrhG-E, so dass in Ausnahmefällen davon abgesehen werden kann.

Kritisch zu betrachten ist weiterhin die Haftungsprivilegierung des § 101 Abs. 6 UrhG-E, die eine Schadensersatzhaftung des Access Providers bei unberechtigten Auskunftserteilungen auf die positive Kenntnis hinsichtlich der Nichtberechtigung des Auskunftsbegehrens begrenzt. Dies birgt die Gefahr, dass Access Provider den Auskunftsbegehren selbst bei Zweifeln über deren Berechtigung nachkommen und die Nutzer dadurch einer unberechtigten Rechtsverfolgung Dritter ausgesetzt werden.

Den schützenswerten Interessen der Nutzer wird jedoch durch den Richtervorbehalt des § 101 Abs. 9 UrhG-E Rechnung getragen, da nach diesem Auskünfte zu (statischen und dynamischen) IP-Adressen stets einer richter-

lichen Anordnung bedürfen. Allerdings sollte vor allem im Hinblick auf eine zu erwartende Kostenreduzierung für alle Beteiligten erwogen werden, der richterlichen Anordnung ein automatisiertes Abrufverfahren nach dem Vorbild der Grenzbeschlagnahme des § 111b UrhG vorausgehen zu lassen.

D. Datenschutzrecht *de lege ferenda*

Auch wenn den Rechteinhabern mit der Regelung des § 101 UrhG-E ein Auskunftsanspruch zur Durchsetzung ihrer zivilrechtlichen Ansprüche zur Seite steht, so ist jedoch zu beachten, dass ein danach begründeter Anspruch nur dann erfolgreich sein wird, wenn der Access Provider auch berechtigt ist, die für die Auskunftserteilung erforderlichen Daten zu speichern, auszulesen und zu übermitteln. Da nach § 101 Abs. 9 S. 9 UrhG-E die Vorschriften zum Schutz personenbezogener Daten unberührt bleiben, richtet sich die Zulässigkeit dieser Nutzungsvorgänge nach dem geltenden Datenschutzrecht. Somit wird es auch nach dem In-Kraft-Treten des § 101 UrhG-E dabei verbleiben, dass das Datenschutzrecht den archimedischen Punkt darstellt, an dem sich das Schicksal des Auskunftsanspruchs entscheidet.[753]

Der Access Provider ist *de lege lata* jedoch allenfalls zu einer über das Verbindungsende hinausgehenden Speicherung von statischen, nicht aber auch von dynamischen IP-Adressen berechtigt.[754] Ferner besteht auch keine Ermächtigungsgrundlage für die Übermittlung der durch das Auslesen dieser Daten gewonnen Bestandsdaten an die Rechteinhaber.[755] Daher würden auch auf § 101 UrhG-E gestützte Auskunftsersuche an datenschutzrechtlichen Vorgaben scheitern.

Aus diesem Grund sollen im Folgenden die anstehenden Novellierungen des Datenschutzrechts dahingehend untersucht werden, ob zumindest *de lege ferenda* eine entsprechende datenschutzrechtliche Ermächtigung der Access Provider zur Speicherung und Herausgabe dieser Daten an die Rechteinhaber zur Verfügung stehen wird. In dieser Hinsicht sind insbesondere die geplante Novellierung des TKG, die Verabschiedung des Te-

[753] So bereits Spindler, Anm. zu OLG Frankfurt a.M, Urt. v. 25.1.2005 – 11 U 51/04, MMR 2005, 243, 245 in Bezug auf eine Auskunftspflicht des Access Providers nach § 101a UrhG.
[754] Siehe oben, 5. Teil IV. 1.
[755] Siehe oben, 5. Teil IV. 3.

lemediengesetzes (TMG) sowie die absehbare Umsetzung der europäischen Richtlinie zur Vorratsdatenspeicherung[756] von Bedeutung.

I. Ermächtigung zur Vorratsdatenspeicherung nach § 96 Abs. 2 S. 1 TKG-E

Eine Änderung zur bestehenden Gesetzeslage könnte sich zunächst durch die geplante Novellierung des TKG abzeichnen. So ist im Referentenentwurf vom 31.1.2006[757] eine dahingehende Ergänzung des § 96 Abs. 2 S. 1 TKG vorgesehen, dass eine Speicherung von Verkehrsdaten auch dann zulässig sein soll, sofern dies *„für die durch andere gesetzliche Vorschriften begründeten"* Zwecke erforderlich ist (vgl. § 96 Abs. 2 S. 1 TKG-E).[758] Angesichts dieser unbestimmten Regelung, die viele Interpretationsmöglichkeiten eröffnet, wird teilweise die Befürchtung geäußert, dass damit versucht werden könnte, in verfassungswidriger Weise eine Vorratsdatenspeicherung von Verkehrsdaten durch die Hintertür zu legitimieren.[759]

Tatsächlich ist diese Regelung missverständlich, da sie nicht widerspiegelt, welche gesetzgeberische Intention ihr zugrunde liegt. Allerdings wird in der Entwurfsbegründung ausgeführt, dass dieser Passus lediglich deklaratorischer Natur sei und klarstellen solle, dass eine über das Verbindungsende hinausgehende Speicherung von Verbindungsdaten neben den in § 96 Abs. 2 S. 1 TKG genannten Zwecken auch dann zulässig ist, wenn die Strafverfolgungs- und Sicherheitsbehörden von ihren spezialgesetzlichen Auskunfts- und Übermittlungsbefugnissen hinsichtlich dieser Daten Gebrauch gemacht haben.[760] Somit kann dieser Regelung keine Ermächtigung oder gar Verpflichtung zu einer vorsorglichen Speicherung von Verkehrsdaten entnommen werden. Um einer derartigen Zweckentfremdung

---

[756] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung 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 (im Folgenden: Richtlinie 2006/24/EG), ABl. 105/54, abrufbar unter: http://eur-lex.europa.eu/LexUriServ/site/de/oj/2006/l_105/ l_10520060413de00540063.pdf.

[757] Referentenentwurf des Bundeswirtschaftsministerium vom 31.01.2006 für ein Gesetz zur Änderung telekommunikationsrechtlicher Vorschriften (im Folgenden: Referentenentwurf zum TKG), abrufbar unter: http://www.bmwi.de/Redaktion/Inhalte/ Pdf/Gesetz/TKG-Aend-2006,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf.

[758] Referentenentwurf zum TKG, a.a.O., S. 26; diese Fassung wurde mittlerweile auch im Regierungsentwurf v. 17.05.2006 bestätigt.

[759] So Stellungnahme des DFN, a.a.O., S. 6.

[760] So bereits die Begründung des Bundesrates zum Entwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Vorschriften vom 4.2.2005, BR-Drs. 92/05, S. 36.

dieser Generalklausel vorzubeugen, sollte diese gesetzgeberische Intention jedoch in den Wortlaut des § 96 Abs. 2 S. 1 TKG-E aufgenommen werden.[761] Da die bestehenden Speicherpflichten somit auch durch § 96 Abs. 2 S. 1 TKG-E nicht modifiziert werden, verbleibt es auch nach dieser Regelung bei der Rechtswidrigkeit der vorsorglichen Speicherung von Verkehrsdaten.

II. Übermittlungsbefugnisse *de lege ferenda*

Selbst wenn man davon ausgeht, dass – z.B. nach § 96 Abs. 2 S. 2 TKG-E – eine über das Verbindungsende hinausgehende Speicherung von Verkehrsdaten zulässig ist, besteht weiterhin das Problem, dass *de lege lata* keine Ermächtigungsgrundlage für die Übermittlung dieser Daten an die Rechteinhaber besteht.[762] Dies könnte sich jedoch mit der Umsetzung des geplanten Telemediengesetzes (TMG) ändern. So befinden sich im Gesetzesentwurf zum TMG auch datenschutzrechtliche Erlaubnissätze zur Übermittlung von Bestands- und Verbindungsdaten an die Inhaber von geistigen Schutzrechten. Die Regelung des § 14 Abs. 2 TMG-E sieht vor, dass Diensteanbieter *„auf Anordnung der zuständigen Stellen*" im Einzelfall Auskunft über Bestandsdaten erteilen dürfen, sofern dies für staatliche Zwecke oder *„zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist"*. Mit dem Verweis auf diese Regelung in § 15 Abs. 5 S. 4 TMG-E wird weiterhin klargestellt, dass die Herausgabebefugnisse auch für Verbindungs- bzw. Verkehrsdaten gelten sollen.[763] Zur Begründung dieser Verschlechterung des Datenschutzniveaus führten die Entwurfsverfasser aus, dass diese Regelungen als Vorgriff auf die notwendige Umsetzung der Enforcement-RL anzusehen seien, dessen Art. 8 die Einführung eines Auskunftsanspruchs zugunsten der Inhaber von geistigen Schutzrechten vorschreibe.[764]

Dass diese Erlaubnissätze zur Datenübermittlung teilweise als *„vollends undurchdacht"* bezeichnet werden,[765] rührt nicht von ungefähr. Denn zunächst mutet es seltsam an, die Rechteinhaber, wie dies § 14 Abs. 2 TMG-E vorsieht, als zuständige Stellen für die Anordnung der Erteilung

[761] So auch Stellungnahme des DFN, a.a.O., S. 3.
[762] Siehe oben, 5. Teil A. IV. 3.
[763] Die Regelungen der §§ 14, 15 TMG-E des Gesetzesentwurfs v. 14.6.2006 entsprechen den §§ 13,14 TMG des Referentenentwurfs vom November 2005.
[764] Begr. des Gesetzesentwurf zum TMG, a.a.O., (Fn. 402), S. 15.
[765] So Stellungnahme der Gruppen der Zivilgesellschaft vom 15.01.2006 zum TMG-E, S. 43, abrufbar unter: http://www.telemediengesetz.de.vu/Telemedienrecht-Forderungen_19-01-2006.pdf.

von Auskünften anzusehen. Zudem statuiert Art. 8 der Enforcement-RL auch keinen direkten Auskunftsanspruch von Rechteinhabern gegen die Diensteanbieter. In der Richtlinie ist lediglich vorgesehen, dass solche Auskunftsansprüche im Rahmen eines gerichtlichen Verfahrens auf richterliche Anordnung möglich sein müssen.[766] Darüber hinaus stellt sich vor dem Hintergrund des verfassungsrechtlichen Gleichheitsgrundsatzes die Frage, wie die Entwurfsverfasser die einseitige Privilegierung der Rechtsverfolgungsinteressen der Inhaber geistiger Eigentumsrechte rechtfertigen wollen, wird dadurch doch zugleich eine Schlechterstellung von Inhabern anderer zivilrechtlicher Ansprüche bewirkt.[767] Zudem sind diese Regelungen auf Access Provider bereits deshalb nicht anwendbar, weil diese nicht den datenschutzrechtlichen Vorschriften des TMG, sondern denen des TKG unterliegen.[768] Allerdings ist vor diesem Hintergrund davon auszugehen, dass entsprechende Übermittlungsbefugnisse auch in das TKG integriert werden.

Unabhängig vom Standort derartiger Übermittlungsbefugnisse stellt sich allerdings das Problem, dass das nationale Datenschutzschutzrecht vom EU-Datenschutzrecht überlagert wird. Daher müssen sich etwaige Übermittlungsbefugnisse auch mit den europarechtlichen Vorgaben vereinbaren lassen. Hinsichtlich der Statuierung einer Ermächtigung zur Übermittlung von Nutzerdaten an die Rechteinhaber dürfte sich der deutsche Gesetzgeber jedoch mit einem Problem konfrontiert sehen, dass sich aus der Regelung des Art. 6 TK-Datenschutzrechtsrichtlinie[769] ergibt. Diese enthält einen abschließenden Katalog von Erlaubnissätzen, der jedoch keine Ermächtigung hinsichtlich der Erteilung von – Verkehrsdaten betreffenden – Auskünften an private Rechteinhaber vorsieht.[770] Die Zulässigkeit einer solchen Auskunftspflicht könnte sich allenfalls aus Art. 15 Abs. 1 TK-Datenschutzrichtlinie ergeben. Durch diese Regelung wird Art. 6 TK-Datenschutzrichtlinie dahingehend eingeschränkt, dass die Mitgliedstaaten davon abweichende Rechtsvorschriften erlassen dürfen, sofern dies *„für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Fest-*

[766] Siehe oben, 7. Teil C. II. 2.
[767] So Stellungnahme des DFN, a.a.O., S. 7.
[768] Siehe oben, 5. Teil A. III.
[769] Richtlinie 2002/58/EG des europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation v. 12.7.2002, ABl. EG L 201 v. 31.7.2002, S. 37, abrufbar unter: http://www.datenschutz-berlin.de/recht/eu/rv/tk_med/tkdsr_de.htm
[770] Spindler/Dorschel, CR 2005, 38, 45.; siehe auch oben, 5.Teil A. IV. 3. a) bb).

stellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist." Als Rechtfertigung kommt in dieser Hinsicht allein der unzulässige Gebrauch von elektronischen Kommunikationssystemen in Betracht.[771] Da die anderen Varianten des Art. 15 Abs. 1 TK-Datenschutzrichtlinie jedoch allesamt von sicherheitsrelevanten Aspekten geprägt sind,[772] kann in der Tat bezweifelt werden, ob sich darunter auch Auskunftspflichten im privaten Drittinteresse subsumieren lassen.[773] Sofern der deutsche Gesetzgeber einen Erlaubnissatz in das TKG implementiert, der einer Übermittlung von Nutzerdaten an private Rechteinhaber für zulässig erklärt, ist dessen Vereinbarkeit mit der Datenschutzrechtsrichtlinie somit durchaus fraglich.

III. Einführung einer Vorratsdatenspeicherung durch die Richtlinie 2006/24/EG

Das letzte Wort über die Zulässigkeit der Speicherung und Übermittlung von Verkehrsdaten dürfte allerdings weder mit dem Erlass des Telemediengesetzes noch mit der Novellierung des TKG gesprochen sein. Denn nach einer langen und kontroversen Diskussion[774] ist Anfang 2006 die inzwischen in Kraft getretene Richtlinie 2006/24/EG zur Vorratsspeicherung von Daten auf den Weg gebracht worden.[775] Diese sieht vor, dass Telekommunikationsanbieter zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten zu einer 6- bis 24-monatigen Speicherung von Verkehrs- und Standortdaten verpflichtet werden. Dies betrifft auch die Speicherung von (statischen und dynamischen) IP-Adressen sowie die dazugehörigen Bestandsdaten wie z.B. Name und Anschrift des Nutzers,[776] mithin Daten, die im Rahmen zivilrechtlicher Auskunftsersuche von essentieller Bedeutung sind.

1. Beschlussfassung des deutschen Bundestages

Bereits am 16.2.2006 wurde die Umsetzung dieser Richtlinie mittels mehrerer Anträge[777] zum Gegenstand der parlamentarischen Debatte im Bun-

---

[771] So auch Kitz, ZUM 2006, 444, 449.
[772] Vgl. Ohlenburg, MMR 2003, 82, 84 f.
[773] Ebenfalls ablehnend, Spindler/Dorschel, CR 2006, 341, 346.
[774] Zusammenfassung unter: Heise News: Vorratsspeicherung von Verbindungsdaten in der Telekommunikation, http://www.heise.de/ct/aktuell/meldung/66857.
[775] Die Richtlinie ist am 3. Mai 2006 in Kraft getreten, vgl. Art. 16 RL 2006/24/EG.
[776] Vgl. Art. 5 Abs. 1 a) Nr. 2 RL 2006/24/EG.
[777] BT-Drs. 16/545, 16/128, 16/237, 16/690.

destag gemacht.[778] Im Rahmen dieser sehr intensiven Debatte wurden von den Gegnern einer derartigen Speicherpflicht eine Reihe von Argumenten hervorbracht. Während nach einer Auffassung bereits die Regelungskompetenz der EU in Frage gestellt und daher die Einreichung einer Nichtigkeitsklage vor dem EUGH gefordert wurde,[779] entzündete sich die Kritik hauptsächlich an der Verhältnismäßigkeit einer Vorratsdatenspeicherung im Hinblick auf die unstreitigen Eingriffe in das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung.[780]

Diese Kritik ist angesichts der vielfältigen Möglichkeiten, die sich bieten, um sich einer Identifizierung durch solche Speichermaßnahmen zu entziehen,[781] auch berechtigt. So können potentielle Straftäter einer Identifizierung durch die Vorratsspeicherung dadurch entgehen, dass sie sich in ein Internetcafe begeben, einen (ausländischen) Anonymisierungsdienst in Anspruch nehmen oder sich über einen ausländischen Provider einwählen, der keiner Speicherpflicht unterliegt. Noch deutlicher wird dies im Bereich der klassischen Telefonie. Bei dieser geht eine vorsorgliche Speicherung von Telekommunikationsdaten bereits dann ins Leere, wenn sich der potentielle Straftäter einer öffentlichen Telefonzelle bedient. Da jedoch nicht davon auszugehen ist, dass Terroranschläge oder andere schwere Straftaten vom heimischen PC über eine Einwahl bei einem deutschen Provider oder aber über den eigenen Telefonanschluss organisiert und verabredet werden, nimmt die Vorstellung, man könne mittels einer Vorratsdatenspeicherung auch diese Straftaten verhindern, geradezu utopische Züge an.

Dennoch wurde im Rahmen dieser Debatte letztlich mit großer Mehrheit der Antrag der Großen Koalition gebilligt, nach dem die Regelungen der Richtlinie *„mit Augenmaß“* und lediglich in ihren *„Mindestanforderungen“* umgesetzt werden sollen.[782] Die Befürworter dieses Antrags versuchten diesen damit zu rechtfertigen, dass die Grundrechte, in die durch die Vorratsdatenspeicherung eingegriffen werde, nicht schrankenlos gewährt würden. Zum Zwecke der Aufklärung schwerer Straftaten sei deren Ein-

[778] Plenarprotokoll 16/19, S. 1417 ff., abrufbar unter: http://dip.bundestag.de/btp/16/16019.pdf.

[779] So Jerzy Montag, Grüne, Plenarprotokoll 16/19, S. 1425; vgl. auch Heise News, Meldung vom 18.5.2006, Bundesregierung soll gegen EU-Richtlinie zur Vorratsdatenspeicherung klagen, http://www.heise.de/newsticker/meldung/73289.

[780] Vgl. Antrag der FDP-Fraktion, BT-Drs. 16/128; zur Eingriffqualität dieser Maßnahmen in das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung, siehe Breyer, Vorratsdatenspeicherung, S. 70 ff.

[781] Näher hierzu, Breyer, Vorratsdatenspeicherung, S. 190 ff.

[782] BT-Drs. 16/545.

schränkung verfassungsrechtlich geboten.[783] Bekräftigt wurde zudem, dass sich die Bürger und Unternehmen darauf verlassen können, dass die Vorgaben aus Brüssel nicht überschritten werden.[784] Insofern sei auszuschließen, dass die Strafverfolgungsbehörden auch bei Bagatelldelikten an die Daten herankämen.[785]

2. Kritik an der Beschlussfassung

Kritisch ist der im Bundestag angenommene Antrag vor allem deshalb zu betrachten, weil dieser – entgegen den Ausführungen dessen Befürworter – weit über die Mindestanforderungen der Richtlinie hinausgeht. Während Art. 1 Abs. 1 Vorratsdatenspeicherungsrichtlinie lediglich auf Speicherungen zum Zwecke der Verfolgung schwerer Straftaten abzielt, sieht der angenommene Antrag vor, dass die gespeicherten Daten gerade nicht ausschließlich der Aufklärung schwerer Straftaten dienen müssen, sondern auch zur Aufklärung von *„allen mittels Telekommunikation begangenen Straftaten“* herangezogen werden können.[786] Somit könnte auf diese Daten – entgegen den Versicherungen der Abgeordneten – auch dann zurückgegriffen werden, wenn es um die Aufklärung einzelner Urheberrechtsverletzungen in Filesharing-Netzwerken geht. Dies legt den Schluss nahe, dass die Speicherung zu Strafverfolgungszwecken lediglich als Vorstufe dafür anzusehen ist, dass diese Daten zukünftig nicht nur für staatliche Stellen, sondern auch für Rechtsverfolgungsinteressen privater Rechteinhaber zu Verfügung stehen sollen.[787] Vor diesem Hintergrund hat bereits die Art. 29-Arbeitsgruppe der EU-Datenschutzbeauftragten deutlich ihre ablehnende Haltung gegenüber einer derartigen Zweckentfremdung dieser Daten zum Ausdruck gebracht und gefordert, dass die Daten nur den staatlichen Strafverfolgungsbehörden, keinesfalls jedoch auch privaten Rechteinhabern zu Verfügung stehen dürfen.[788] Zudem stellt sich die Frage, ob sich ein dahingehender Zweckwechsel hinsichtlich der Nutzung dieser Daten überhaupt mit dem datenschutzrechtlichen Zweckbindungsgrundsatz vereinbaren ließe.

---

[783] BT-Drs. 16/545, S. 3, Nr. 11.
[784] Dr. Günter Krings, CDU, Plenarprotokoll 16/19, S. 1421.
[785] Daniela Raab, CSU, Plenarprotokoll 16/19, S. 1427.
[786] BT-Drs. 16/545, S. 4.
[787] Dies fordernd Zombik, ZUM 2006, 450, 456; in diese Richtung tendierend Raabe, Regierungsreferentin im Bundesjustizministerium, ZUM 2006, 439, 443.
[788] Heise News, Meldung v. 6.4.2006: EU-Datenschützer fordern klare Begrenzung der TK-Vorratsdatenspeicherung, http://www.heise.de/newsticker/meldung/71776.

3. Zweckbindung der Daten für Strafverfolgungszwecke

Nach dem Gebot der Zweckbindung dürfen personenbezogene Daten nur für diejenigen Zwecke verwendet werden, zu denen sie auch erhoben werden durften.[789] Dies bedeutet zugleich, dass Daten, die zum Zwecke der Bekämpfung schwerer Straftaten gewonnen wurden, nicht ohne weiteres für die Geltendmachung zivilrechtlicher Ansprüche genutzt werden dürfen.[790] Ein dahingehender Zweckwechsel der Nutzung der im Rahmen der Vorratsspeicherung generierten Daten ist jedoch nicht per se unzulässig. Erforderlich ist allerdings, dass auch dieser von einer gesetzlichen Ermächtigungsgrundlage gedeckt ist.[791] Einer solchen Ermächtigung würde insbesondere auch die TK-Datenschutzrichtlinie nicht entgegenstehen,[792] da gem. Art. 11 Vorratsdatenspeicherungsrichtlinie die restriktiven Erlaubnissätze des Art. 15 Abs. 1 TK-Datenschutzrechtsrichtlinie keine Anwendung auf Daten finden, die der Vorratsdatenspeicherung unterliegen. Allerdings sieht die Vorratsdatenspeicherungsrichtlinie in Art. 4 selbst eine dahingehende Einschränkung vor, dass diese Daten nur an nationale Behörden weitergegeben werden dürfen. Da diese nationalen Behörden von den Mitgliedstaaten zu benennen sind,[793] könnte man in Erwägung ziehen, auch diejenigen Gerichte als Behörden anzusehen, die nach § 101 Abs. 9 UrhG-E über das Auskunftsersuch der Rechteinhaber zu entscheiden haben. Ob dies auch die – sich an die richterliche Anordnung anschließende – Übermittlung der Nutzerdaten an die privaten Rechteinhaber legitimieren würde, erscheint angesichts des – ausschließlich auf die strafrechtliche Rechtsverfolgung abstellenden – Schutzzwecks der Richtlinie jedoch äußerst fraglich.[794]

4. Alternativvorschlag: Quick-Freeze-Verfahren

Gerade im Hinblick auf die drohende Verfassungswidrigkeit einer Vorratsdatenspeicherung, sollte als mildere Alternative über die Einführung einer anlassbezogenen Speicherpflicht nach dem Vorbild des sog. Quick-Freeze-Verfahrens nachgedacht werden.[795] Nach diesem Verfahren werden Kom-

---

[789] BVerfGE 65, 1, 46 – Volkszählung; BVerfGE 100, 313, 385 f. – Telekommunikationsüberwachung I; Breyer, Vorratsdatenspeicherung, S. 106.
[790] So auch Stellungnahme des DFN, a.a.O., S. 8.
[791] Breyer, Vorratsdatenspeicherung, S. 107.
[792] Vgl. oben, 7. Teil D. II.
[793] Vgl. Erwägungsgrund 25 der Vorratsdatenspeicherungsrichtlinie.
[794] Ähnlich Kitz, ZUM 2006, 444. 449.
[795] So auch Unabhängiges Zentrum für Datenschutz Schleswig-Holstein, 27 Tätigkeitsbericht (2005), Punkt 4.2.3, abrufbar unter:

munikationsdaten nur im Einzelfall und auf vorheriges Verlangen einer berechtigten Stelle „eingefroren“ und somit von den gesetzlichen Löschungspflichten ausgenommen, damit diese für spätere Rechtsverfolgungszwecke zur Verfügung stehen. Dieses Verfahren ist bereits Bestandteil der Cybercrime-Konvention des Europarates[796] und wird zudem mit Erfolg in den USA praktiziert, weshalb selbst dort eine vorsorgliche Speicherung von Kommunikationsdaten als entbehrlich angesehen wird.[797]

Zwar wurde die Einführung eines solchen Systems auch im Rahmen der parlamentarischen Debatte über die Umsetzung der Richtlinie zur Vorratsdatenspeicherung gefordert,[798] allerdings konnte sich ein dahingehender Antrag nicht durchsetzen. Dieser wurde mit der Argumentation verworfen, dass sich dieses Verfahren nicht zur Aufklärung von Straftaten eigne, bei denen auf in der Vergangenheit gespeicherte Telekommunikationsdaten zurückgegriffen werden müsse, die zwischenzeitlich aufgrund bestehender Löschpflichten nicht mehr zur Verfügung stünden.[799] Ob allein dieser Umstand geeignet ist, die durch die Vorratsdatenspeicherung bedingten erheblichen Grundrechtseingriffe zu rechtfertigen, kann vor allem vor dem Hintergrund der zahlreichen Umgehungsmöglichkeiten durchaus angezweifelt werden.

Hinzu kommt ein rechtsverfolgungstaktisches Argument. Wissen die potentiellen Straftäter nämlich von vornherein, dass eine vorsorgliche Speicherung von Verkehrsdaten stattfindet, werden diese stets Umgehungsmöglichkeiten in Betracht ziehen. Würde man hingegen lediglich eine anlassbezogene Speicherpflicht statuieren, so würden sich viele potentielle Straftäter auch weiterhin in Sicherheit wiegen und auf Umgehungsmaßnahmen verzichten. Insofern ist nicht auszuschließen, dass eine anlassbezogene Speicherpflicht mitunter zu einer wesentlich größeren Erhellung

---

http://www.datenschutzzentrum.de/material/tb/tb27/kap04_2.htm ; Achter Jahresbericht (2004) der Art. 29 Gruppe über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Europäischen Union und in Drittländern, abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/8th_annual_report_de.pdf.

796 Vgl. Breyer, Vorratsdatenspeicherung, S. 137 f.

797 Vgl. Breyer, Vorratsdatenspeicherung, S. 346 f.; angestoßen durch die Aktivitäten des europäischen Gesetzgebers ist jedoch auch in den USA die Debatte über die Einführung einer Vorratsdatenspeicherung zur Kriminalitätsbekämpfung neu entbrannt, vgl. Heise-News, Meldung v. 2.6.2006, Bericht: US-Regierung plant jahrelange Vorratsspeicherung von Internet-Daten, http://www.heise.de/newsticker/meldung/73833.

798 Antrag der FDP-Fraktion, BT-Drs. 16/128.

799 So Alfred Hartenbach, Parlamentarischer Staatssekretär der Bundesjustizministerin, Plenarprotokoll 16/19, S. 1426.

des Dunkelfeldes der polizeilichen Kriminalstatistik führt als eine Vorratsdatenspeicherung.

Als Kompromiss könnte man in dieser Hinsicht noch in Erwägung ziehen, die Strafverfolgungs- bzw. Sicherheitsbehörden zumindest bei tatsächlichem Vorliegen eines terroristischen Anschlags die Befugnis einzuräumen, eine kurzzeitige Speicherung des gesamten Datenverkehrs anzuordnen. Dies wurde auch in England und in den USA nach den Anschlägen des 11. September 2001 praktiziert und soll für die Ermittlungen in Bezug auf diese Anschläge von erheblichem Nutzen gewesen sein.[800]

Für die im Fokus dieser Bearbeitung stehende zivilrechtliche Verfolgung von Rechtsverletzungen könnte dieses Verfahren dergestalt nutzbar gemacht werden, dass die Rechteinhaber im Falle des Entdeckens einer Urheberrechtsverletzung die gleichzeitig generierte IP-Adresse unverzüglich an die von den Access Providern regelmäßig geführte Abuse-Adresse senden und den Provider zugleich auffordern, die benötigten Daten für eine nachfolgende Rechtsverfolgung zu speichern. Dies entspricht im Wesentlichen der bereits gängigen Praxis, für die allerdings, wie das Logistep-Verfahren vor dem LG Flensburg gezeigt hat, derzeit noch keine gesetzliche Grundlage besteht.[801] Eine solche anlassbezogene Speicherpflicht der Access Provider ließe sich auch ohne weiteres in das TKG integrieren. Damit es jedoch nicht, wie im Logistep-Verfahren, zu Blockierungen der E-Mail-Server der Provider kommt, sollten die Provider zudem (gesetzlich) angehalten werden, ein automatisiertes Verfahren zur Durchsetzung dieser Quick-Freeze-Order bereitzuhalten. Zudem ließe sich ein solches Quick-Freeze-Verfahren auch problemlos in das oben bereits angesprochene Abrufverfahren integrieren, welches sinnvollerweise einer richterlichen Anordnung nach § 101 Abs. 9 UrhG-E vorgeschaltet werden sollte. So könnte man in Erwägung ziehen, dass die Rechteinhaber die Quick-Freeze-Order nicht direkt an die Abuse-Adresse der Access Provider richten, sondern dies von dem automatisierten EDV-System vorgenommen wird, auf dessen Erfassungsmaske der Rechteinhaber die Rechtsverletzung zur Anzeige bringt.

Weiterhin ist jedoch zu beachten, dass die von Access Providern regelmäßig vergebenen dynamischen IP-Adressen nach der geltenden Rechtslage unmittelbar nach dem Verbindungsende zu löschen sind und daher auch ein Quick-Freeze-Verfahren nur erfolgreich wäre, wenn die Access Provi-

[800] Vgl. Breyer, Vorratsdatenspeicherung, S. 348.
[801] Vgl. oben, 5. Teil A. IV. 1. b) cc) (1).

der die Quick-Freeze-Order noch während einer bestehenden Internetsitzung des Nutzers oder unmittelbar danach erreicht. Vor diesem Hintergrund sollte daher zudem in Erwägung gezogen werden, die Access Provider zu verpflichten, auch die dynamischen IP-Adressen zumindest für einige Stunden bzw. wenige Tage über das Nutzungsende hinaus zu speichern. Auch diese – in begrenztem Maße vorsorgliche – Speicherpflicht dürfte sich noch im Rahmen der durch die Verhältnismäßigkeit gesetzten Grenzen bewegen. Zumindest wäre eine solche Speicherpflicht für die Provider weitaus weniger belastend als die vom Bundestag favorisierte halbjährliche Speicherung aller Kommunikationsdaten.

Nun liegt auf den ersten Blick die Vermutung nahe, dass dieser Alternativvorschlag angesichts des In-Kraft-Tretens der Richtlinie zur Vorratsdatenspeicherung verspätet kommt. Dies ist jedoch nicht ganz zutreffend. Denn die Umsetzung der Richtlinie 2006/24/EG in deutsches Recht ist keinesfalls bereits determiniert. Zunächst ist gegen diese Richtlinie aufgrund des Streits um die richtige Rechtsgrundlage von einigen Mitgliedsstaaten bereits Nichtigkeitsklage vor dem EuGH erhoben.[802] Selbst wenn diese Klagen nicht erfolgreich sein sollten und die Vorgaben dieser Richtlinie tatsächlich in nationales Recht umgesetzt werden, dürfte auch die Prüfungskompetenz des BVerfG hinsichtlich der die Richtlinie umsetzenden Gesetze nicht von vornherein zu versagen sein, sofern man davon ausgeht, dass durch die Richtlinie der unabdingbare Grundrechtsschutz nicht mehr gewährleistet ist.[803] Für diese Annahme lässt sich der Beschluss des BVerfG vom 6.4.2006 rekurrieren, in dem die bundesweite Rasterfahndung in der Zeit nach dem 11. September 2001 wegen Verstoßes gegen das *„strikte Verbot der Sammlung personenbezogener Daten auf Vorrat“* für verfassungswidrig erklärt wurde.[804] Sollte das BVerfG daher auch hinsichtlich der die Richtlinie umsetzenden Gesetze seine Prüfungskompetenz bejahen und in der Sache entscheiden, wird dieses zu beachten haben, dass mit der anlassbezogenen Speicherung von Daten nach dem Vorbild des Quick-Freeze-Verfahrens ein milderes Mittel zur Bekämpfung von Straftaten und weiteren Rechtsverletzungen im Internet zur Verfügung steht.

---

[802] Heise-News, Meldung v. 1.6.2006, Irland und Slowakei legen Klage gegen Vorratsdatenspeicherung ein, http://www.heise.de/newsticker/meldung/73751 ; vgl. auch Meldung v. 18.5.2006, Bundesregierung soll gegen EU-Richtlinie zur Vorratsdatenspeicherung klagen, http://www.heise.de/newsticker/meldung/73289.

[803] Vgl. BVerfG, Beschl. v. 7.6.2000 – 2 BvL 1/97 – Bananenmarktordnung, Absatz-Nr. (1 - 69), http://www.bverfg.de/entscheidungen/ls20000607_2bvl000197.html.

[804] BVerfG, 1 BvR 518/02 v. 4.4.2006, Absatz-Nr. (1 - 184), http://www.bverfg.de/entscheidungen/rs20060404_1bvr051802.html.

E. Zwischenergebnis

Da die Enforcement-RL die nationalen datenschutzrechtlichen Bestimmungen unberührt lässt, scheitert eine Auskunftspflicht des Access Providers nach § 101 UrhG-E – zumindest *de lege lata* – wiederum an datenschutzrechtlichen Bestimmungen.[805] Abhilfe verspricht in dieser Hinsicht auch nicht die geplante Neufassung des § 96 Abs. 2 S. 1 TKG, da diese Regelung bestehende Speicherpflichten nicht modifiziert. Darüber hinaus stehen einer Statuierung von Übermittlungsbefugnissen hinsichtlich dieser Daten europarechtliche Bedenken in Gestalt der TK-Datenschutzrichtlinie entgegen.

Eine Änderung dieser Rechtslage könnte sich allenfalls durch die Umsetzung der Richtlinie zur Vorratsdatenspeicherung abzeichnen. Bereits aufgrund der Zweckbindung diese Daten für Strafverfolgungszwecke, dürften die so gewonnenen Daten jedoch für zivilrechtliche Auskunftsansprüche nicht zur Verfügung stehen. Zudem bestehen angesichts der vielfältigen Umgehungsmöglichkeiten hinsichtlich einer Identifizierung durch eine Vorratsdatenspeicherung gerade vor dem Hintergrund der Geeignetheit dieser Maßnahme verfassungsrechtliche Bedenken. Zumindest dürfte sich eine Speicherpflicht nach dem Vorbild des Quick-Freeze-Verfahrens als ein gleich geeignetes, jedoch milderes Mittel zur Vorratsdatenspeicherung darstellen.

[805] Sofern man davon ausgeht, dass auch verletzungsunabhängige Auskunftsansprüche von den Haftungsprivilegierungen des TDG erfasst werden, würde ein Anspruch aus § 101 UrhG-E auch an § 8 Abs. 2 S. 2 TDG scheitern.

8. Teil: Zusammenfassung und Ausblick

Die Frage, ob Access Provider bei Urheberrechtsverletzungen zur Herausgabe von Nutzerdaten an private Rechteinhaber verpflichtet sind, ist ein hervorragendes Beispiel dafür, dass sich Onlinesachverhalte keinem bestimmten Rechtsgebiet zuweisen lassen, sondern rechtsgebietsübergreifend eine Vielzahl rechtlicher Fragen tangieren. Verdeutlichen lässt sich dies daran, dass den Rechteinhabern allein mit der Statuierung eines urheberrechtlichen Auskunftsanspruchs nicht viel geholfen ist. Denn ein solcher Anspruch muss bis zu dessen Erfüllung einige rechtliche Hürden nehmen. Als solche erweisen sich insbesondere die Haftungsprivilegierungen für Diensteanbieter nach dem TDG/MDStV, das Datenschutzrecht sowie das Fernmeldegeheimnis. Selbst wenn diese rechtlichen Hindernisse genommen werden, hängt die Effektivität eines solchen Anspruchs darüber hinaus entscheidend von der Frage ab, ob den Nutzern technische Möglichkeiten zur Verfügung stehen, mittels derer sie sich einer Identifizierung entziehen können.

Vor diesem Hintergrund wurde im Rahmen der Bearbeitung untersucht, ob den Rechteinhabern bereits *de lege lata* oder aber zumindest nach der Umsetzung der Enforcement-Richtlinie ein durchsetzbarer Auskunftsanspruch zur Seite steht, um auf dem Zivilrechtswege gegen Urheberrechtsverletzungen im Onlinebereich vorgehen zu können. Hinsichtlich der geltenden Rechtslage wurde festgestellt, dass einzig der urheberrechtliche Anspruch auf Drittauskunft gem. § 101a UrhG als taugliche materiell-rechtliche Anspruchsgrundlage für ein Auskunftsverlangen in Betracht kommt. Problematisch ist allerdings, dass eine Passivlegitimation des Access Providers i.S.d. § 101a UrhG zumindest voraussetzt, dass dieser nach den allgemeinen Regeln als mittelbarer Störer für die Urheberrechtsverletzungen seiner Nutzer haftet. Der Access Provider kann jedoch nur dann als mittelbarer Störer qualifiziert werden, wenn dieser eine ihm obliegende Prüf- bzw. Verkehrssicherungspflicht verletzt hat. Der Begründung einer solchen Pflicht des Access Providers sind jedoch durch die gesetzlichen Haftungsprivilegierungen sowie durch die geheimschutzrechtlichen Beschränkungen enge Grenzen gesetzt. So kann dem Access Provider insbesondere keine präventive Überwachung des von ihm übermittelten Inhalts auf dessen urheberrechtliche Unbedenklichkeit zugemutet werden. Zudem ist ihm aus datenschutzrechtlichen Gründen verwehrt, den entsprechenden Nutzer anhand seiner (dynamischen oder statischen) IP-Adresse zu ermitteln und diesen – in Anlehnung an § 13a TKV – abzumahnen oder zu sperren. Aus

diesem Grund genügt der Access Provider seinen Verkehrssicherungspflichten bereits dann, wenn dieser seine Nutzer in den Allgemeinen Geschäftsbedingungen zur Beachtung fremder Urheberrechte ermahnt. Da dies weitestgehend der Fall ist, kann ein Access Provider in der Regel nicht als mittelbarer Störer qualifiziert und damit auch nicht auf Auskunft i.S.d. § 101a UrhG in Anspruch genommen werden. Sofern der Access Provider ausnahmsweise dennoch als mittelbarer Störer haftet, wird sich dessen Inanspruchnahme zudem nur bei schwerwiegenden Rechtsverletzungen als verhältnismäßig i.S.d. § 101a UrhG darstellen.

Darüber hinaus würden verletzungsabhängige Auskunftsansprüche an den gesetzlichen Haftungsprivilegierungen des TDG scheitern. Diese sehen eine vollumfängliche Privilegierung des Access Providers vor, die eine nach den allgemeinen Regeln begründete Haftung ausschließt. Zwar finden diese Haftungsbeschränkungen nach § 8 Abs. 2 S. 2 TDG keine Anwendung auf Entfernungs- und Sperrungsansprüche, allerdings lassen sich Auskunftspflichten nicht unter diese Rückausnahmebestimmung subsumieren.

Selbst wenn man davon ausginge, dass Auskunftsansprüche den Filter der gesetzlichen Haftungsprivilegierungen passieren, würde die Geltendmachung eines Auskunftsanspruchs auch am Datenschutzrecht scheitern, da dem Access Provider die für die Auskunftserteilung notwendigen Nutzungshandlungen aus datenschutzrechtlichen Gründen verwehrt sind. So stehen die regelmäßig vergebenen dynamischen IP-Adressen für Auskunftsbegehren bereits deshalb nicht zur Verfügung, weil eine – über das Verbindungsende hinausgehende – Speicherung dieser Daten rechtswidrig ist. Da die Rechteinhaber die Access Provider auch nicht anlassbezogen zur Speicherung dieser IP-Adressen verpflichten können, scheitert die Geltendmachung von Auskunftsbegehren zu dynamischen IP-Adressen regelmäßig daran, dass diese Daten für Rechtsverfolgungszwecke nicht zur Verfügung stehen. Der Access Provider ist allenfalls zur vorsorglichen Speicherung von statischen IP-Adressen berechtigt. Allerdings scheitern Auskunftsansprüche selbst im Falle einer zulässigen Erhebung von IP-Adressen daran, dass der Access Provider weder berechtigt ist, den konkreten Nutzer anhand seiner IP-Adresse zu ermitteln noch die so gewonnenen Nutzerdaten an die Rechteinhaber zu übermitteln.

Weiterhin ist dem Access Provider die Auskunftserteilung auch vor dem Hintergrund der einfachgesetzlichen Ausprägung des Fernmeldegeheimnisses aus § 88 TKG verwehrt. Liegt einem Auskunftsbegehren eine dy-

namische IP-Adresse zugrunde, wird bereits durch die Bestimmung der Identität des Nutzers in das Fernmeldegeheimnis eingegriffen, da es dazu des Auslesens von Verkehrsdaten bedarf. Bei Auskunftsersuchen zu statischen IP-Adressen stellt zwar nicht zwingend die Ermittlung des Nutzers, wohl aber die anschließende Übermittlung dieser Daten an die Rechteinaber einen Eingriff in das Fernmeldegeheimnis dar. Da diese Eingriffe von keiner gesetzlichen Ermächtigungsgrundlage gedeckt sind, verstößt die Erfüllung von Auskunftsbegehren somit auch gegen das Fernmeldegeheimnis.

Würde ein solcher Anspruch hingegen alle rechtlichen Hürden nehmen, so ist weiterhin zu beachten, dass sich die potentiellen Rechtsverletzer einer Identifizierung – in rechtlich zulässiger Weise – durch die Nutzung von Anonymisierungsdiensten entziehen können, da durch diese die (nachträgliche) Zuordnung einer IP-Adresse zu einem bestimmten Nutzer vereitelt wird.

Mit der Umsetzung der Enforcement-RL wird voraussichtlich ein verletzungsunabhängiger Auskunftsanspruch in das Urheberrecht Einzug halten. So sieht § 101 Abs. 2 S. 1 Nr. 3 UrhG-E – in Umsetzung des Art. 8 Abs. 1 lit.c Enforcement-RL – eine verletzungsunabhängige Auskunftspflicht gewerblicher Dienstleister vor, deren Dienstleistungen von Dritten für Urheberrechtsverletzungen missbraucht werden. Diese Auskunftspflicht ist insbesondere auch auf Access Provider gemünzt. Abgesehen von den im Detail streitigen Tatbestandsvoraussetzungen des § 101 Abs. 2 UrhG-E, besteht die Hauptproblematik hinsichtlich der Auskunftspflicht des Access Providers darin, dass die Enforcement-RL in erster Linie am analogen Umfeld ausgerichtet ist und daher die nationalen datenschutzrechtlichen Bestimmungen unberührt lässt. Dementsprechend würde eine Auskunftspflicht des Access Providers selbst nach der Umsetzung der Enforcement-RL an datenschutzrechtlichen Bestimmungen scheitern.

Dieser *Status quo* wird auch weder durch die bevorstehende Novellierung des Telekommunikationsrechts noch durch die Richtlinie zur Vorratsdatenspeicherung zugunsten der Rechteinhaber modifiziert. Letztere sieht zwar eine mindestens halbjährliche vorsorgliche Speicherung von IP-Adressen und weiterer personenbezogener Daten vor, allerdings dürften diese Daten aufgrund ihrer strafrechtlichen Zweckbindung für die zivilrechtliche Rechtsverfolgung nicht zur Verfügung stehen. Zudem bestehen insbesondere im Hinblick auf ein Quick-Freeze-Verfahren ernsthafte Zweifel an der Verfassungsmäßigkeit einer solchen Vorratsdatenspeicherung.

Das Quick-Freeze-Verfahren stellt darüber hinaus auch hinsichtlich der zivilrechtlichen Auskunftsverpflichtung von Access Providern einen interessanten Ansatz dar. Diesen Ansatz sollte auch der Gesetzgeber aufgreifen, sofern dieser beabsichtigt, einem gegen Access Provider gerichteten Auskunftsanspruch nach § 101 UrhG-E über die Hürde des Datenschutzrechts zu verhelfen.

Aus unserem Verlagsprogramm:

Recht der Neuen Medien

Gundula Ernst
Vertragsschluß im Internet unter besonderer Berücksichtigung der E-Commerce-Richtlinie
Hamburg 2007 / 340 Seiten / ISBN 978-3-8300-2787-4

Torsten Spiegelhalder
Rechtsscheinhaftung im Stellvertretungsrecht bei der Verwendung elektronischer Signaturen
Hamburg 2007 / 186 Seiten / ISBN 978-3-8300-2802-4

Martin Bergfelder
Der Beweis im elektronischen Rechtsverkehr
Hamburg 2006 / 414 Seiten / ISBN 978-3-8300-2451-4

Karen Altermann
Die Zulässigkeit unverlangter E-Mail-Werbung nach der UWG-Novelle
Eine Darstellung der Ansprüche nach dem Wettbewerbsrecht, Zivilrecht einschließlich Unterlassungsklagengesetz, Datenschutzrecht und Markenrecht sowie der Folgen im Strafrecht
Hamburg 2006 / 310 Seiten / ISBN 978-3-8300-2348-7

Lilian Klewitz
Verbraucherschutz bei Rechtsgeschäften per Internet
Hamburg 2006 / 438 Seiten / ISBN 978-3-8300-2334-0

Marc Christian Bauer
Elektronische Agenten in der virtuellen Welt
Ein Beitrag zu Rechtsfragen des Vertragsschlusses, einschließlich der Einbeziehung allgemeiner Geschäftsbedingungen, des Verbraucherschutzes sowie der Haftung
Hamburg 2006 / 352 Seiten / ISBN 978-3-8300-2258-9

VERLAG DR. KOVAČ
FACHVERLAG FÜR WISSENSCHAFTLICHE LITERATUR
Postfach 570142 · 22770 Hamburg · www.verlagdrkovac.de · info@verlagdrkovac.de

Einfach Wohlfahrtsmarken helfen!