

Kommunikation & Recht



Betriebs-Berater für

● Medien ● Telekommunikation ● Multimedia

6
K&R

- Editorial: EU Datenschutz-Grundverordnung – Anpassungen in letzter Minute · *Dr. Carlo Piltz*
- 361 Aktuelle Entwicklungen in der Providerhaftung im Jahr 2017
Dr. Christian Volkmann
- 367 Streit zwischen der ICANN und der DENIC:
Einfache Whois-Abfragen vor dem Aus
Nikola Šarac und Tobias H. Strömer
- 371 Open Source Compliance bei Embedded Systems
Dr. Hendrik Schöttle
- 375 Der Einkauf des fürsorgenden Familienvaters im Supermarkt
als Zeitgeschehen · *Dr. Oliver Stegmann*
- 378 Update Informationsfreiheits- und Transparenzrecht 2017/2018
Prof. Dr. Jens M. Schmittmann
- 385 Länderreport USA · *Clemens Kochinke*
- 387 BVerfG: Straßenfotografie nur mit Einwilligung
abgebildeter Personen
mit Kommentar von *Robert Golz*
- 391 BGH: Prüfpflicht eines Suchmaschinenbetreibers
bei Persönlichkeitsrechtsverletzungen
- 398 BGH: Lösungsanspruch gegen Ärztebewertungsportal
- 404 BGH: Vertrag zur Platzierung einer Internet-Werbeanzeige
stellt Werkvertrag dar
- 406 Brandenburgisches OLG: Elektronische Übermittlung
mehrerer Dateien mittels Container-Signatur erlaubt
- 409 OLG München: Partnerbörse: Keine unzumutbare Belästigung
durch E-Mail an registrierte Nutzer
- 423 BVerwG: Rundfunkbeitragspflicht für Anwalts-GbR

21. Jahrgang

Juni 2018

Seiten 361 – 432

RA Dr. Christian Volkmann, Berlin*

Aktuelle Entwicklungen in der Providerhaftung im Jahr 2017

Der folgende Beitrag schafft einen Überblick über die zur Verantwortlichkeit der Internet-Provider im Jahr 2017 geschaffenen Neuregelungen sowie die in diesem Jahr veröffentlichte Rechtsprechung unter besonderer Berücksichtigung der Haftung für fremde Inhalte.

I. Übersicht

Die Haftung der Internet-Provider stand im Jahr 2017 ganz im Lichte des Dritten Änderungsgesetzes zum Telemediengesetz. Die Gesetzesänderungen einschließlich seiner Begründung sind kritikwürdig, da Vieles auslegungsbedürftig und unklar ist. Zudem stehen die EU-Rechtswidrigkeit und die Verfassungswidrigkeit der Gesetzesänderungen im Raum. Abgesehen von den Gesetzesänderungen sind die Rechtsprechung des EuGH zur urheberrechtlichen Haftung für Hyperlinks und die Antwort des BGH darauf hervorzuheben.

II. Das Dritte Änderungsgesetz zum Telemediengesetz

Im Dritten Änderungsgesetz zum Telemediengesetz hat der Gesetzgeber die Haftung der Internet-Provider neu geregelt. Ziel des Gesetzgebers war es, WLAN-Betreibern so weit wie möglich Rechtssicherheit zu verschaffen, damit dem gestiegenen Bedürfnis nach einem öffentlichen Zugang zum Internet auch unter Nutzung von WLAN entsprochen werden kann.¹ Herausgekommen ist etwas anderes: Der Gesetzgeber hat nicht nur die WLAN-Haftung beschränkt, sondern in § 8 Abs. 1 S. 2 TMG die Haftung aller Access-Provider „insbesondere“ auf Schadensersatz, Unterlassung und Beseitigung ausgeschlossen und als Kompensation in § 7 Abs. 4 TMG einen Sperranspruch gegen WLAN-Anbieter eingeführt. Angesichts der Zielsetzung des Gesetzgebers, aber auch angesichts zu beachtenden höherrangigen Rechts ist zweifelhaft, dass dies so gewollt gewesen ist.

Unter Zugrundelegung zweier EU-Richtlinien, die im Lichte der Rechtsprechung des EuGH die Haftung der Access-Provider als Vermittler von Inhalten im Rechtsgebiet des geistigen Eigentums vorsehen (Art. 8 Abs. 3 der InfoSoc-Richtlinie, Art. 11 S. 3 der Enforcement-Richtlinie),² und angesichts der Zielsetzung des Dritten Änderungsgesetzes zum Telemediengesetz, das Angebot von WLAN (und nicht das der Access-Provider) zu fördern, scheint der weitgehende Ausschluss der Haftung aller Access-Provider auch in harmonisierten Rechtsgebieten bei gleichzeitiger Schaffung eines Anspruchs auf die Sperrung von Informationen nur gegen WLAN-Anbieter zumindest einmal frag-

würdig. Da auch die Gesetzesbegründung nicht hilfreich ist, sondern – im Gegenteil – für noch mehr Verwirrung als der verunglückte Gesetzestext sorgt, stellt der Gesetzgeber den Rechtsanwender im Bereich der Internethaftung vor die bislang wohl härteste Probe.

Nach der Auffassung des Verfassers können die Gesetzesänderungen wie folgt eingeordnet und bewertet werden:

1. § 8 Abs. 1 S. 2 – Ausschluss der Störerhaftung für Access-Provider

a) Adressat des Ausschlusses

Die Ausweitung der Haftungsprivilegierung in § 8 Abs. 1 S. 2 TMG gilt für alle Diensteanbieter im Sinne von § 8 Abs. 1 S. 1 TMG und damit nicht nur für WLAN-Anbieter, die in § 8 Abs. 3 TMG den Access-Providern gleichgestellt sind, sondern für alle klassischen Access-Provider.³ Im Hinblick auf die WLAN-Anbieter findet die Privilegierung unabhängig davon Anwendung, ob der WLAN-Anschluss kommerziell oder privat betrieben wird.⁴ Der Haftungsausschluss gilt jedoch nicht für Anbieter nach den §§ 9, 10 TMG, d. h. insbesondere nicht für Host-Provider.⁵ Er gilt auf der Anspruchsebene ausdrücklich für Schadensersatzansprüche sowie auch für Beseitigungs- und für Unterlassungsansprüche, sodass damit auch die Störerhaftung der Access-Provider ausgeschlossen ist.

b) Reichweite des Ausschlusses

Unklar ist, warum der Gesetzgeber den von ihm explizit genannten Ansprüchen auf Schadensersatz, Beseitigung und Unterlassung ein „insbesondere“ voranstellte. Hier kann nur spekuliert werden, da sich auch in der Gesetzesbegründung dazu nichts findet. Ob damit ein über diese drei Ansprüche hinausgehender Ausschluss erreicht werden sollte, erscheint unwahrscheinlich. Zwar hat „insbesondere“ einen einschränkenden Charakter. Ohne eine dem „insbesondere“ voranstehende allgemeine oder abstrakte Formulierung verliert sich aber die Bedeutung dieses Wortes, sodass es sich um eine nicht verwertbare Formulierung handelt und damit richtigerweise zu ignorieren sein dürfte.

* Mehr über den Autor erfahren Sie auf S. VIII.

¹ Begr. RegE, BT-Drs. 18/12202, S. 1.

² EuGH, 27. 3. 2014 – C-314/12, K&R 2014, 329, Rn. 32 – UPC Telekabel/Constantin.

³ Mantz, GRUR 2017, 969, 970.

⁴ Begr. RegE BT-Drs. 18/12202, S. 9; Spindler, NJW 2016, 2449, 2450; Spindler, CR 2016, 48, 49; Müller/Kipker, MMR 2016, 87, 88; Mantz, GRUR 2017, 969, 970 f.

⁵ Mantz, GRUR 2017, 969, 971.

Jedenfalls nicht berührt sind öffentlich-rechtliche Maßnahmen, auch wenn diese eine Beseitigung oder eine Unterlassung beinhalten können.⁶ Hierfür spricht, dass „rechtswidrige Handlung eines Nutzers“ nicht deckungsgleich mit den Voraussetzungen der behördlichen Gefahrenabwehr ist, die nicht zwingend rechtswidriges Verhalten eines Dritten voraussetzt. Zudem gäbe es bei einer Ausdehnung des § 8 Abs. 1 S. 2 TMG auf öffentlich-rechtliche Maßnahmen keinen Anwendungsbereich für § 8 Abs. 4 TMG, der das behördliche Ermessen bei einem Vorgehen gegen Access-Provider einschränkt.

c) Kosten

Nach § 8 Abs. 1 S. 2 Hs. 2 TMG können die von § 8 TMG erfassten Diensteanbieter nicht auf die für die Geltendmachung und Durchsetzung von Schadensersatz-, Beseitigungs- und Unterlassungsansprüchen entstehenden Kosten in Anspruch genommen werden. Bedeutung dürfte diese Regelung allerdings nicht haben. Denn soweit nach § 8 Abs. 1 S. 2 Hs. 1 TMG die Hauptansprüche des Geschädigten bzw. des in seinen Rechten Verletzten auf Schadensersatz, Beseitigung und Unterlassung ausgeschlossen sind, können Nebenansprüche im Hinblick auf die Geltendmachung und Durchsetzung dieser (nicht bestehenden) Ansprüche nicht bestehen.⁷

2. § 7 Abs. 3 TMG – Richtervorbehalt?

Für wenig Klarheit hat die Ergänzung in § 7 Abs. 3 TMG gesorgt, wonach Verpflichtungen zur Entfernung von Informationen oder zur Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen „aufgrund von gerichtlichen oder behördlichen Anordnungen“ unberührt bleiben sollen. Nach der Gesetzesbegründung sollen die Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nur zulässig sein, wenn sie klar gesetzlich geregelt sind und „aufgrund einer gerichtlichen oder behördlichen Anordnung erfolgen“.⁸ Hierdurch soll sichergestellt werden, dass eine Interessenabwägung im Einzelfall durch eine staatliche Stelle erfolgt.⁹ Dies lässt durchaus den Schluss zu, dass eine Verpflichtung des Diensteanbieters erst mit der gerichtlichen Anordnung entsteht, d. h. dass diese konstitutiv für die Verpflichtung ist. Da andererseits der Gesetzgeber aber auch davon ausgeht, dass der Diensteanbieter mit der Sperrung in Verzug geraten kann (und das wohl vor der gerichtlichen Anordnung), und nicht davon auszugehen ist, dass er ohne jegliche nähere Erläuterung in der Gesetzesbegründung einen derart untypischen¹⁰ Weg der zivilrechtlichen Anspruchsdurchsetzung gehen wollte, erscheint es zweifelhaft, dass der Gesetzgeber den materiell-rechtlichen Anspruch unter den Vorbehalt der gerichtlichen Anordnung stellen wollte.¹¹ § 7 Abs. 3 TMG hat daher an den Voraussetzungen der Inanspruchnahme von Access-Providern nichts geändert; ein Richtervorbehalt ist in § 7 Abs. 3 TMG nicht zu sehen.¹² Auch im Hinblick auf die Folgen für die Haftung der Host-Provider dürfte ein anderes Ergebnis kaum vom Gesetzgeber gewollt gewesen sein. So hätte die strenge Anwendung der Einfügung in § 7 Abs. 3 TMG auch Auswirkungen auf die Haftung der Host-Provider, insbesondere auf die Abmahnkosten nach der Inkenntnissetzung vom Rechtsverstoß, die mangels gerichtlicher Anordnung ohne korrespondierende Unterlassungsverpflichtung nicht durchgesetzt werden könnten.¹³

3. § 7 Abs. 4 TMG – Anspruch auf Websperren

Entgegen der bisherigen Dogmatik der Haftungsprivilegierungen im TMG als Einschränkung der Haftung nach den allgemeinen Gesetzen ist § 7 Abs. 4 TMG als Anspruchsgrundlage ausgestaltet.¹⁴ § 7 Abs. 4 TMG soll nach dem Willen des Gesetzgebers den weitreichenden Haftungsausschluss in § 8 Abs. 1 S. 2 TMG kompensieren und Anordnungen gegen Zugangsanbieter erlauben.¹⁵ Der Anspruch ist auf die Sperrung der Vermittlung des Zugangs zu einer bestimmten Website gerichtet (Websperre). Die Art der Sperre, die der Verletzte beanspruchen kann, wird in § 7 Abs. 4 TMG nicht festgelegt. Es bleibt damit den Gerichten überlassen, welche Sperrungen sie anordnen. Als Sperrmaßnahmen kommen eine Sperrung durch die Access-Provider mit Hilfe der im Regelfall von ihnen selbst betriebenen sog. Domain-Name-System-Server (DNS-Server) in Betracht sowie eine Blockade von IP-Adressen im Router oder mit Hilfe einer Firewall, durch den Einsatz eines Proxy-Servers oder mit Hilfe hybrider Filtersysteme.

a) Anwendung auf Access-Provider

§ 7 Abs. 4 TMG, der als Spezialregelung für WLAN- bzw. Zugangsanbieter unglücklich¹⁶ in den für alle Diensteanbieter der §§ 8 bis 10 TMG geltenden § 7 TMG eingefügt wurde, ist zwar nicht auf alle Diensteanbieter der §§ 8 bis 10 TMG anzuwenden,¹⁷ aber – entgegen seinem Wortlaut – auch nicht nur auf die in § 8 Abs. 3 TMG definierten WLAN-Anbieter, sondern auf sämtliche Access-Provider im Sinne des § 8 Abs. 1 S. 1 TMG.¹⁸ Im Recht des geistigen Eigentums müssen die Mitgliedsstaaten gem. Art. 8 Abs. 3 der InfoSoc-Richtlinie und Art. 11 S. 3 der Enforcement-Richtlinie Anordnungen gegen Access-Provider zum Abstellen von und zum Vorbeugen vor Rechtsverstößen ermöglichen. Denn Access-Provider sind als Vermittler anzusehen, deren Dienste von einem Dritten zur Verletzung des Urheberrechts (bzw. eines Rechts des geistigen Eigentums) genutzt werden.¹⁹ Die Anwendbarkeit von § 7 Abs. 4 TMG bloß auf WLAN-Anbieter stünde in Bezug auf Access-Provider, die nicht gleichzeitig auch WLAN-Anbieter sind, im Widerspruch zu Art. 8 Abs. 3 der InfoSoc-Richtlinie sowie Art. 11 S. 3 der Enforcement-Richtlinie.²⁰

Darüber hinaus finden sich in der Gesetzesbegründung Anhaltspunkte, die für eine Einbeziehung der Access-Provider in den Anwendungsbereich von § 7 Abs. 4 TMG

⁶ Spindler, NJW 2017, 2305, 2308.

⁷ Mantz, GRUR 2017, 969, 972.

⁸ Begr. RegE, BT-Drs. 18/12202, S. 11.

⁹ Begr. RegE, BT-Drs. 18/12202, S. 11.

¹⁰ Grisse, GRUR 2017, 1073, 1075.

¹¹ Grisse, GRUR 2017, 1073, 1075; Hofmann, GPR 2017, 176, 181.

¹² Grisse, GRUR 2017, 1073, 1075; Hofmann, GPR 2017, 176, 181 f.; Mantz, GRUR 2017, 969, 975.

¹³ Spindler, in: Spindler/Schmitz, TMG, 2. Aufl. 2018, § 7 Rn. 45.

¹⁴ Mantz, GRUR 2017, 969, 972.

¹⁵ Begr. RegE BT-Drs. 18/12202, S. 12.

¹⁶ Mantz, GRUR 2017, 969, 972; Grisse, GRUR 2017, 1073, 1081.

¹⁷ Mantz, GRUR 2017, 969, 972.

¹⁸ Spindler, NJW 2017, 2305, 2305; Grisse, GRUR 2017, 1073, 1078 f.; a. A. Sesing/Baummann, MMR 2017, 583, 588.

¹⁹ EuGH, 27. 3. 2014 – C-314/12, K&R 2014, 329, Rn. 32 – UPC Telekabel/Constantin; ebenso BGH, 26. 11. 2015 – I ZR 174/14, K&R 2016, 171, Rn. 25 – Störerhaftung des Access-Providers.

²⁰ Spindler, CR 2017, 333, 334; Grisse, GRUR 2017, 1073, 1078; a. A. wohl Sesing/Baummann, MMR 2017, 583, 588, die aber in § 8 Abs. 1 S. 2 TMG keinen Ausschluss von Sperranordnungen gegen Access-Provider auf Basis der Störerhaftung sehen und damit zu einer unionsrechtskonformen Auslegung gelangen.

sprechen. Gerade die Zielrichtung des Gesetzes, welches in der Schaffung von Rechtssicherheit für die Betreiber von WLAN-Netzwerken liegt und nicht in der Aufgabe jeglicher Haftung für alle Zugangsanbieter, spricht dagegen, dass der Gesetzgeber quasi nebenbei die Störerhaftung der Access-Provider komplett und ersatzlos streichen wollte.²¹ Zudem spricht der Gesetzgeber in der Gesetzesbegründung in Bezug auf § 7 Abs. 4 TMG nicht von WLAN-Anbietern, sondern von „Zugangsanbietern“.²² Die Vermittlung des Zugangs zu Telemedien im Sinne des § 2 Nr. 1 TMG ist aber die klassische Tätigkeit der Access-Provider²³ und nicht nur der WLAN-Anbieter. Dadurch verdeutlicht der Gesetzgeber, dass er die Störerhaftung der Zugangsanbieter in § 8 Abs. 1 S. 2 TMG nicht ersatzlos streichen, sondern im Recht des geistigen Eigentums durch § 7 Abs. 4 TMG ablösen wollte.

b) Anspruchsvoraussetzungen

Voraussetzung für die Geltendmachung eines Anspruchs auf die Sperrung einer Information gem. § 7 Abs. 4 TMG ist die Verletzung des Rechts am geistigen Eigentum. Der Begriff des geistigen Eigentums ist im Sinne der Enforcement-Richtlinie zu verstehen und umfasst daher neben den Urheberrechten etwa auch Marken- und Designrechte. Damit sind insbesondere die Verletzung von Persönlichkeitsrechten oder des lautereren Wettbewerbs nach dem UWG nicht von § 7 Abs. 4 TMG erfasst und keiner Störerhaftung der Access-Provider mehr zugänglich.²⁴

Es muss ein Telemediendienst im Sinne des TMG in Anspruch genommen worden sein, um die Rechtsverletzung zu begehen. Vorbereitende Maßnahmen fallen nicht hierunter, d. h. etwa das Herunterladen von Software, die später vom Nutzer für Rechtsverletzungen verwendet werden kann, oder die Verbreitung von Informationen, wie Rechte des geistigen Eigentums verletzt werden können, ohne dass diese Informationen selbst Rechte des geistigen Eigentums verletzen.²⁵ Vorbeugende Maßnahmen gegen Diensteanbieter sind nach § 7 Abs. 4 TMG nicht möglich, da gleich eingangs der Norm mit „Wurde“ ein bestehender Verstoß vorausgesetzt wird²⁶ und zudem die Wiederholung der Rechtsverletzung Anspruchsvoraussetzung ist. Auch die bloße Ankündigung einer Rechtsverletzung über eine bestimmte URL kann damit keinen (vorbeugenden) Sperranspruch begründen.

Der Anspruch auf die Sperrung von Informationen ist nur gegeben, wenn für den Inhaber des Rechts keine andere Möglichkeit besteht, der Verletzung seines Rechts abzuwehren. Damit führt der Gesetzgeber in den Sperranspruch ein Kriterium ein, das der nahezu ausschließlich durch das Richterrecht geprägten Störerhaftung bis in das Jahr 2015 hinein fremd gewesen ist: Nämlich das der nachrangigen Haftung desjenigen, der von der Verletzung weiter entfernt ist als ein anderer (Subsidiarität).²⁷ Es steht zu erwarten, dass die Gerichte für die Subsidiarität im Sinne von § 7 Abs. 4 TMG die vom BGH in der Entscheidung „Störerhaftung des Access-Providers“ entwickelten Kriterien heranziehen werden. Dazu sollen vor der Inanspruchnahme des Access-Providers die staatlichen Ermittlungsbehörden im Wege der Strafanzeige eingeschaltet oder private Ermittlungen wie etwa die Einschaltung eines Detektivs oder von Unternehmen, die „Ermittlungen im Zusammenhang mit rechtswidrigen Angeboten im Internet durchführen“, vorgenommen werden, um die vorrangig haftenden Webseiten- oder Host-Provider zu ermitteln.²⁸ Nur wenn die Inanspruchnahme der vorrangig haftenden Beteiligten

scheitert oder ihr jede Erfolgsaussicht fehlt, ist die Inanspruchnahme des Zugangsvermittlers nach § 7 Abs. 4 TMG möglich.

Gem. § 7 Abs. 4 S. 2 TMG muss die Sperrung zumutbar und verhältnismäßig sein. Aufgrund dieses Vorbehalts besteht für die Gerichte die Möglichkeit – wie bislang im Rahmen der Störerhaftung auch – in jedem Einzelfall zu entscheiden, ob der Verletzte gegen den Access-Provider überhaupt einen Anspruch auf Sperrung hat.

Zu berücksichtigen sind dabei nicht nur die Zumutbarkeit für den Provider, der als Passivlegitimierter die Maßnahme durchführen muss, sondern auch die Interessen und Grundrechte des Anspruchstellers sowie die der Internet-Nutzer, die weder mit der Rechtsverletzung noch mit der Verbreitung/Vermittlung derselben zu tun haben. Auch hier steht zu erwarten, dass die Gerichte den Abwägungsprozess des BGH in der Entscheidung „Störerhaftung des Access-Providers“ durchführen werden, der im Rahmen des Kriteriums der „Zumutbarkeit“ eine geradezu klassische Verhältnismäßigkeitsprüfung und eine umfassende Interessenabwägung vorgenommen hat.²⁹

Neben der Geeignetheit einer Sperre, die nicht bereits deshalb entfällt, weil Sperrungen umgangen werden können,³⁰ spielen dabei insbesondere die Kommunikationsgrundrechte der Beteiligten eine gewichtige Rolle. Maßnahmen gegenüber Access-Providern betreffen im Bereich der Kommunikationsgrundrechte zwar weder den Schutzbereich der Meinungsfreiheit der Access-Provider gem. Art. 5 Abs. 1 S. 1 GG³¹ noch den Schutzbereich der Pressefreiheit der Access-Provider gem. Art. 5 Abs. 1 S. 2 GG.³² Zu berücksichtigen sind aber die Grundrechte der Internetnutzer, die aufgrund von Sperrmaßnahmen auch auf rechtlich unbedenkliche Inhalte nicht mehr zugreifen können („Overblocking“). Denn eine Sperrung von Inhalten im Netz stellt einen Hinderungstatbestand in der Unterrichtung der Internet-Nutzer und damit einen Eingriff in die Informationsfreiheit nach Art. 11 Abs. 1 S. 2 GRCh, Art. 5 Abs. 1 S. 1 2. Alt. GG dar.³³ Auch der EuGH sieht in Sperrmaßnahmen einen Eingriff in den Schutzbereich der Informationsfreiheit nach Art. 11 GRCh und berücksichtigt diesen Eingriff im Rahmen seiner Abwägung der Haftung von Access-Providern.³⁴ Sperrmaßnahmen haben daher streng zielorientiert zu sein und dürfen den Internetnutzern die Möglichkeit, in rechtmäßiger Weise Zugang zu

21 *Grisse*, GRUR 2017, 1073, 1079; *Spindler*, CR 2017, 332, 334.

22 Begr. RegE BT-Drs. 18/12202, Seite 8 f.

23 OLG Hamburg, MMR 2014, 625, 627; *Spindler*, in: *Spindler/Schmitz* (Fn. 13), § 2 Rn. 25; *Frey*, MMR 2014, 650, 651.

24 S. zu den verfassungsrechtlichen Zweifeln an dieser Beschränkung des Rechtsschutzes *Spindler*, NJW 2017, 2305, 2306.

25 *Spindler*, in: *Spindler/Schmitz* (Fn. 13), § 7 Rn. 92.

26 *Mantz*, GRUR 2017, 969, 972.

27 So bereits der BGH vor der Gesetzesänderung: BGH, 26. 11. 2015 – I ZR 174/14, K&R 2016, 171, Rn. 81 – Störerhaftung des Access-Providers.

28 BGH, 26. 11. 2015 – I ZR 174/14, K&R 2016, 171, Rn. 87 – Störerhaftung des Access-Providers.

29 BGH, 26. 11. 2015 – I ZR 174/14, K&R 2016, 171, Rn. 32 – Störerhaftung des Access-Providers.

30 OVG Münster, 19. 3. 2003 – 8 B 2567/02, NJW 2003, 2183, 2186; *Volkman*, *Der Störer im Internet*, 2005, S. 232 f.; *Stegmann*, *Die Haftung der Basisinfrastruktur bei rechtswidrigen Internetangeboten*, 2010, S. 146.

31 *Spindler*, in: *Spindler/Schmitz* (Fn. 13), § 7 Rn. 80.

32 *Determann*, *Kommunikationsfreiheiten im Internet*, 1999, S. 445 f.; *Volkman* (Fn. 30), S. 38 f.; *Spindler*, in: *Spindler/Schmitz* (Fn. 13), § 7 Rn. 79.

33 Dazu BGH, 26. 11. 2015 – I ZR 174/14, K&R 2016, 171, Rn. 53 ff. – Störerhaftung des Access-Providers.

34 EuGH, 27. 3. 2014 – C-314/12, K&R 2014, 329, Rn. 55 ff. – UPC Telekabel/Constantin; BGH, 26. 11. 2015 – I ZR 174/14, K&R 2016, 171, Rn. 53 – Störerhaftung des Access-Providers; *Nolte/Wimmers*, GRUR 2014, 16, 18 f.

den verfügbaren Informationen zu erhalten, nicht unnötig vorenthalten.³⁵ Zu berücksichtigen sind weiterhin die Grundrechte der Access-Provider und hier insbesondere das Recht auf unternehmerische Freiheit gem. Art. 16 GRCh und das Recht der Berufsfreiheit gem. Art. 12 Abs. 1 GG. Sperrungen von Websites betreffen diese Grundrechte.³⁶ Dem Fernmeldegeheimnis gem. Art. 10 Abs. 1 GG und dem Grundrecht aus Art. 7 GRCh auf Achtung der Kommunikation kommt im Rahmen der Abwägung hingegen keine maßgebliche Bedeutung zu.³⁷ Art. 10 GG schützt die Vertraulichkeit individueller, schriftlich oder fernmeldetechnisch übertragener Kommunikation³⁸ und gewährleistet die freie Entfaltung der Persönlichkeit durch einen privaten, vor den Augen der Öffentlichkeit verschlossenen Austausch von Nachrichten, Gedanken und Meinungen.³⁹ Kommunikationsprozesse fallen aber dann nicht in den Schutzbereich des Fernmeldegeheimnisses, wenn ihre Inhalte für die Öffentlichkeit bestimmt sind, d. h. wenn ihnen der vertrauliche, individuelle Charakter fehlt.⁴⁰ Kann daher der Grundrechtsverpflichtete – wie es beim bloßen Abruf öffentlich zugänglicher Webseiten der Fall ist – dieselbe Information mit den gleichen technischen Mitteln abrufen wie der Nutzer, handelt es sich um eine solche öffentliche Kommunikation, die nicht dem Schutzbereich des Fernmeldegeheimnisses unterfällt.⁴¹ Zugangssperren verhindern zudem lediglich die Kommunikation; die bloße Verhinderung von Kommunikation fällt aber nicht in den Schutzbereich des Art. 10 Abs. 1 GG.⁴²

c) Prozessuales und Abmahnkosten nach den Neueregungen im TMG

Der Anspruch auf die Sperrung von Informationen im Internet wird im Klageweg wie jeder andere zivilrechtliche Anspruch geltend gemacht.⁴³ Der Anspruch kann auch im einstweiligen Rechtsschutz durchgesetzt werden.⁴⁴ Nach § 7 Abs. 4 S. 3 TMG hat der in seinen Rechten Verletzte keinen Anspruch auf die Erstattung seiner vor- und außergerichtlichen Kosten. Nicht erfasst von der Regelung sind die Gerichtskosten, die weiterhin die unterliegende Partei zu tragen hat.

III. Die Haftung der Inhaber von Internetanschlüssen

Die Haftung der Internetanschlussinhaber hat sich zu einem Dauerbrenner beim BGH entwickelt. Nach den Tauschbörse-Entscheidungen vom 11. 6. 2015,⁴⁵ den vorhergehenden Entscheidungen BearShare und Morpheus⁴⁶ sowie der grundlegenden Entscheidung Sommer unseres Lebens⁴⁷ entwickelte der BGH seine Rechtsprechung zuletzt mit den Entscheidungen Loud⁴⁸ und Afterlife⁴⁹ weiter.

Mit der Loud-Entscheidung aus dem Jahr 2017 hat der BGH die sekundäre Darlegungs- und Beweislast des Anschlussinhabers weiter konkretisiert. Die in dem Verfahren beklagten Eheleute beriefen sich zunächst darauf, dass jedes ihrer im Tatzeitpunkt im Haushalt lebenden volljährigen Kinder Zugang zum passwortgeschützten Internetanschluss gehabt habe und damit die rechtsverletzende Handlung habe vornehmen können. Besonders lag der Fall, weil die Eltern im Prozess vortrugen, dass sie wüssten, welches der Kinder die Rechtsverletzung begangen habe, sie dies aber nicht mitteilen wollten.

Dieses wohl klassische elterliche Dilemma löste der BGH zu Lasten der Eltern und verurteilte diese zur Zahlung von Schadensersatz. Grundlage ist die in ständiger Rechtsprechung des BGH in diesen Fällen geltende sekundäre Darlegungslast des Anschlussinhabers, selbst wenn dieser Anschluss – etwa wie bei einem Familienanschluss – regelmäßig von mehreren Personen genutzt wird.⁵⁰ Will der Anschlussinhaber seiner sekundären Darlegungslast genügen, muss er zur Aufklärung des Sachverhalts beitragen. Der Anschlussinhaber ist danach gehalten vorzutragen, welche anderen Personen selbständigen Zugang zu seinem Internetanschluss hatten und als Täter in Betracht kommen.⁵¹ Es genügt nicht, wenn der Anschlussinhaber die bloß theoretische Möglichkeit des Zugriffs von in seinem Haushalt lebenden Dritten auf seinen Internetanschluss behauptet.⁵² Er muss – wenn ihm darüber Erkenntnisse vorliegen – dazu auch das Kind benennen, welches die Rechtsverletzung begangen hat.⁵³

Den Frieden innerhalb der Familie und den Grundrechtsschutz ungestörten ehelichen und familiären Zusammenlebens nach Art. 7 GRCh und Art. 6 Abs. 1 GG gibt der BGH damit weitgehend dem Eigentumsrecht des Urheberrechtsinhabers gemäß Art. 17 Abs. 2 GRCh und Art. 14 Abs. 1 GG preis – und das auf Basis einer sekundären Darlegungslast eines Anschlussinhabers, dem in Bezug auf seinen Anschluss gegenüber volljährigen Familienmitgliedern⁵⁴ nicht einmal Verkehrssicherungspflichten obliegen, d. h. dem kein Handeln oder Unterlassen vorgeworfen werden kann.⁵⁵ Ohne tatsächlichen Anknüpfungspunkt an eine Haftung und nur auf Basis der vom BGH hier vertretenen sekundären Darlegungslast führt dies zu folgendem aus Sicht des Senats ausgewogenen Ergebnis:

- 35 BGH, 26. 11. 2015 – I ZR 174/14, K&R 2016, 171, Rn. 55 – Störerhaftung des Access-Providers; EuGH, 27. 3. 2014 – C-314/12, K&R 2014, 329, Rn. 63 ff. – UPC Telekabel/Constantin; *Leistner/Grisse*, GRUR 2015, 105, 108.
- 36 BGH, 26. 11. 2015 – I ZR 174/14, K&R 2016, 171, Rn. 37 – Störerhaftung des Access-Providers; EuGH, 27. 3. 2014 – C-314/12, K&R 2014, 329, Rn. 48 ff. – UPC Telekabel/Constantin in Bezug auf Art. 16 der GRCh; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 405.
- 37 BGH, 26. 11. 2015 – I ZR 174/14, K&R 2016, 171, Rn. 60 – Störerhaftung des Access-Providers.
- 38 BVerfG, 24. 1. 2012 – 1 BvR 1299/05, NJW 2012, 1419, 1421.
- 39 BVerfG, 25. 3. 1992 – 1 BvR 1430/88, BVerfGE 85, 386, 395 f.
- 40 BGH, 26. 11. 2015 – I ZR 174/14, K&R 2016, 171, Rn. 68 – Störerhaftung des Access-Providers; *Durner*, ZUM 2010, 833, 838.
- 41 *Billmeier*, Die Düsseldorf Sperrungsverfügung, 2007, S. 184 f.; a. A. *Sieber/Nolde*, Sperrverfügungen im Internet, 2009, S. 79 ff.
- 42 BGH, 26. 11. 2015 – I ZR 174/14, K&R 2016, 171, Rn. 65 – Störerhaftung des Access-Providers; *Durner*, ZUM 2010, 833, 841; *Spindler*, GRUR 2016, 451, 456; *Leistner/Grisse*, GRUR 2015, 19, 22 ff.
- 43 *Spindler*, in: *Spindler/Schmitz* (Fn. 13), § 7 Rn. 102.
- 44 *Spindler*, in: *Spindler/Schmitz* (Fn. 13), § 7 Rn. 103.
- 45 BGH, 11. 6. 2015 – I ZR 19/14, K&R 2016, 114 – Tauschbörse I; BGH, 11. 6. 2015 – I ZR 7/14, K&R 2016, 117 – Tauschbörse II; BGH, 11. 6. 2015 – I ZR 75/14, K&R 2016, 120 – Tauschbörse III.
- 46 BGH, 8. 1. 2015 – I ZR 169/12, K&R 2014, 513 – BearShare; BGH, 15. 11. 2012 – I ZR 74/12, K&R 2013, 322 – Morpheus.
- 47 BGH, 12. 5. 2010 – I ZR 121/08, K&R 2010, 492 – Sommer unseres Lebens.
- 48 BGH, 30. 3. 2017 – I ZR 19/16, K&R 2017, 787 – Loud.
- 49 BGH, 6. 10. 2016 – I ZR 154/15, K&R 2017, 269 – Afterlife.
- 50 BGH, 30. 3. 2017 – I ZR 19/16, K&R 2017, 787, Rn. 14 – Loud; BGH, 11. 6. 2015 – I ZR 75/14, K&R 2016, 120, Rn. 39 – Tauschbörse III; BGH, 12. 5. 2016 – I ZR 48/15, K&R 2016, 835, Rn. 34 – Everytime we touch.
- 51 BGH, 11. 6. 2015 – I ZR 75/14, K&R 2016, 120, Rn. 42 – Tauschbörse III, dazu *Specht*, GRUR 2017, 42, 44 f.
- 52 BGH, 11. 6. 2015 – I ZR 75/14, K&R 2016, 120, Rn. 42 – Tauschbörse III.
- 53 BGH, 30. 3. 2017 – I ZR 19/16, K&R 2017, 787, Rn. 24 – Loud.
- 54 Anders bei minderjährigen Familienmitgliedern, bei denen die Eltern als Anschlussinhaber Pflichten treffen, deren Verletzung zur Haftung führen kann, BGH, 11. 6. 2015 – I ZR 7/14, K&R 2016, 117, Rn. 32 – Tauschbörse II.
- 55 Kritisch daher *Spindler*, GRUR 2018, 16, 17; *Köhler*, ZUM 2017, 507, 512.

Die Eltern, denen nur vorgeworfen werden kann, dass sie wissen, welches ihrer Kinder die Rechtsverletzung begangen hat, seien nicht gezwungen, den Namen ihres Kindes zu offenbaren und es damit der straf- und zivilrechtlichen Verfolgung preiszugeben; sie müssten dann aber mit den prozessualen Konsequenzen leben und können die Vermutung ihrer eigenen Täterschaft prozessual nicht widerlegen.⁵⁶ Das erinnert an die Haftung des Halters eines Fahrzeugs, nur dass diese gesetzlich geregelt und versichert ist.

Ratsam erscheint es damit, wenn Anschlussinhaber prinzipiell nicht wissen, wer die Rechtsverletzung über ihren Anschluss begangen hat. Die dem Anschlussinhaber abverlangten „Aufklärungsmaßnahmen“ dürften – wenn nicht das ehrliche, vertrauensvolle und erfolgreiche Gespräch innerhalb der Familie erfolgt, das der BGH aber nicht unter den Schutz von Art. 7 GRCh und Art. 6 Abs. 1 GG stellt – kaum geeignet sein, den Täter zu identifizieren, zumal der BGH hier zu Recht zurückhaltend agiert und etwa nicht verlangt, den Internetzugang des Ehegatten einer Dokumentation zu unterwerfen oder den Computer des als Täter in Betracht kommenden Ehegatten, zu untersuchen.⁵⁷ Ein bisschen (unnütze) Aufklärung innerhalb der Familie sollte danach sein – aber wehe dem, der mit seiner Aufklärung erfolgreich ist oder dem, der ehrliche Kinder hat.

Als bald dürfte sich der EuGH dazu äußern. Das LG München hat dem EuGH die Frage vorgelegt, ob die bloße Benennung eines Familienmitglieds, das neben dem Anschlussinhaber selbst Zugriff auf diesen Anschluss hatte, ohne weitere Nachforschungen anzustellen, im Anwendungsbereich von InfoSoc-Richtlinie und Enforcement-Richtlinie ausreicht, um der Verantwortlichkeit zu entgehen.⁵⁸

IV. Die Haftung der Linksetzer und der Suchmaschinenbetreiber

Die Haftung von Linksetzern und Suchmaschinenbetreibern wurde zuletzt maßgeblich von Entscheidungen des EuGH und des BGH im Bereich des Urheberrechts beeinflusst. Andere Rechtsgebiete, die bislang die Haftungsrechtsprechung prägten, insbesondere das Persönlichkeitsrecht, traten in den Hintergrund.

1. Linksetzer und Suchmaschinen im Urheberrecht

Die Haftung von Linksetzern und Suchmaschinenbetreibern im Urheberrecht hat in den vergangenen Jahren, insbesondere im letzten Jahr, aufgrund mehrerer Entscheidungen des EuGH an Kontur verloren. Da Linksetzer und Suchmaschinenbetreiber nicht von den Haftungsprivilegierungen in Abschnitt 3 des TMG profitieren, richtet sich ihre Haftung nach den allgemeinen Gesetzen. An diesen allgemeinen Gesetzen – und damit ist nicht die Störerhaftung gemeint – setzt nun der EuGH an, wenn er den Tatbestand der „öffentlichen Wiedergabe“ in Art. 3 Abs. 1 der InfoSoc-Richtlinie auf das Setzen von Hyperlinks ausdehnt und damit im Linksetzen eine eigene Verwertungshandlung sieht, die zu einer eigenen Urheberrechtsverletzung des Linksetzers führen und ihn damit auch zum Täter einer Urheberrechtsverletzung machen kann. Zwar schränkt der EuGH diese weitreichende Ausdehnung der Verletzungshandlung an anderer Stelle im Tatbestand der „öffentlichen Wiedergabe“ noch ein, dies allerdings dogmatisch unbefriedigend und unklar.

Die Öffentlichkeit der Wiedergabe ist nach Auffassung des EuGH bereits dann eröffnet, wenn durch die Handlung (des Linksetzers) ein „neues Publikum“ erreicht wird.⁵⁹ Ein „neues Publikum“ soll erreicht sein, wenn der Adressatenkreis auf Personen erweitert wird, die nach dem Willen des Urhebers bzw. Rechteinhabers bei der Erlaubnis der ursprünglichen Wiedergabe nicht erreicht werden sollten.⁶⁰ Unter Zugrundelegung dieses weitreichenden Wiedergabebegriffs sind einfache Hyperlinks,⁶¹ eingebettete Hyperlinks zu rechtswidrigen Angeboten,⁶² das Verreiben von Abspiegelgeräten mit Software zu illegalen Streamingangeboten⁶³ oder das Vorhalten von Indexseiten zum Tausch von urheberrechtlich geschützten Werken via Peer-to-Peer-Verbindung⁶⁴ als „öffentliche Wiedergabe“ eingestuft worden.

Eingeschränkt wird diese weitreichende Haftung durch den EuGH nicht etwa durch ein weiteres Handlungskriterium bzw. ein Kriterium, das den Akt der Wiedergabe betrifft, sondern durch eine individuelle Beurteilung, die auf wertende und subjektive Kriterien abstellt.⁶⁵ Das Setzen eines Hyperlinks auf eine Internetseite mit geschützten Werken, die auf einer anderen Internetseite ohne Erlaubnis des Urheberrechtsinhabers frei zugänglich sind, soll danach nur dann als „öffentliche Wiedergabe“ im Sinne von Art. 3 Abs. 1 der InfoSoc-Richtlinie zu verstehen sein, wenn der Verlinkende die Rechtswidrigkeit der Veröffentlichung der Werke auf der anderen Internetseite kannte oder vernünftigerweise kennen konnte.⁶⁶ Bei Links mit Gewinnerzielungsabsicht wird diese Kenntnis vermutet.⁶⁷ Umgekehrt scheidet eine „öffentliche Wiedergabe“ aus, wenn Kenntnis bzw. fahrlässige Unkenntnis des Linksetzers nicht gegeben sind bzw. – bei der Gewinnerzielung dienenden linksetzenden Diensten – widerlegt wurde.

Die Einbettung dieser Rechtsprechung des EuGH, die mit wertenden Kriterien bereits an den Tatbestand der Verwertungshandlung selbst anknüpft, in die Dogmatik der Störerhaftung erscheint kaum möglich. Der BGH hat es versucht und Kriterien, die bislang nur für die Reichweite von Prüfungspflichten und damit für die Störerhaftung relevant waren, an zwei Stellen in seine Entscheidung Vorschaubilder III eingebunden, nämlich einmal beim Tatbestand der Verwertungshandlung und einmal bei der

56 BGH, 30. 3. 2017 – I ZR 19/16, K&R 2017, 787, Rn. 26 f. – Loud.

57 BGH, 6. 10. 2016 – I ZR 154/15, K&R 2017, 269, Rn. 26 – Afterlife.

58 LG München, 17. 3. 2017 – 21 O 24454/14, K&R 2017, 347.

59 EuGH, 8. 9. 2016 – C-160/15, K&R 2016, 661, Rn. 38 – GS Media/Sanoma; EuGH, 26. 4. 2017 – C-527/15, K&R 2017, 396, Rn. 33 – Stichting Brein/Wullems.

60 EuGH, 8. 9. 2016 – C-160/15, K&R 2016, 661, Rn. 38 – GS Media/Sanoma; EuGH, 26. 4. 2017 – C-527/15, K&R 2017, 396, Rn. 33 – Stichting Brein/Wullems.

61 EuGH, 8. 9. 2016 – C-160/15, K&R 2016, 661, Rn. 42 f. – GS Media/Sanoma.

62 EuGH, 8. 9. 2016 – C-160/15, K&R 2016, 661, Rn. 41 ff. – GS Media/Sanoma.

63 EuGH, 26. 4. 2017 – C-527/15, K&R 2017, 396, Rn. 48 ff. – Stichting Brein/Wullems.

64 EuGH, 26. 4. 2017 – C-527/15, K&R 2017, 396, Rn. 45 ff. – Stichting Brein/Wullems.

65 EuGH, 8. 9. 2016 – C-160/15, K&R 2016, 661, Rn. 49 und 55 – GS Media/Sanoma; EuGH, 26. 4. 2017 – C-527/15, K&R 2017, 396, Rn. 49 – Stichting Brein/Wullems; vgl. dazu LG Hamburg, 13. 6. 2017 – 310 O 117/17, K&R 2017, 811, 813, das von der Wiedergabehandlung eines Nutzers im Sinne der Rechtsprechung des EuGH zu Art. 3 Abs. 1 der InfoSoc-Richtlinie in „subjektiver Hinsicht“ spricht; dazu auch *Kahl/Schönfelder*, K&R 2017, 683, 687.

66 EuGH, 8. 9. 2016 – C-160/15, K&R 2016, 661, Rn. 49 und 55 – GS Media/Sanoma; EuGH, 26. 4. 2017 – C-527/15, K&R 2017, 396, Rn. 49 – Stichting Brein/Wullems.

67 EuGH, 8. 9. 2016 – C-160/15, K&R 2016, 661, Rn. 51 – GS Media/Sanoma; EuGH, 26. 4. 2017 – C-527/15, K&R 2017, 396, Rn. 49 – Stichting Brein/Wullems.

Reichweite der Prüfungspflichten.⁶⁸ Dies zeigt, dass ein sauberer Prüfungsaufbau der Voraussetzungen der Störerhaftung kaum noch möglich ist und diese zudem immer weiter mit Täterschaft und Teilnahme verschwimmt, sodass sich eine Ablösung der Störerhaftung im Urheberrecht zugunsten einer Haftung für die Verletzung urheberrechtlicher Verkehrspflichten⁶⁹ bzw. generell eine Ablösung der Störerhaftung durch die Zurechnung mittels Verkehrssicherungspflichten abzeichnet.

Hervorzuheben an der Entscheidung Vorschaubilder III ist allerdings noch die besondere Relevanz für Suchmaschinenbetreiber. Denn der BGH hat die Rechtsprechung des EuGH im Hinblick auf den Tatbestand der „öffentlichen Wiedergabe“ gem. Art. 3 Abs. 1 der InfoSoc-Richtlinie einschränkend dahingehend ausgelegt, dass die bei mit Gewinnerzielungsabsicht gesetzten Hyperlinks vermutete (widerlegbare) Kenntnis von der Rechtswidrigkeit eines Inhaltes jedenfalls bei von Suchmaschinen gesetzten Hyperlinks nicht gelte.⁷⁰ Dies begründet der BGH zu Recht mit der besonderen Bedeutung von Suchmaschinen für die Informationsvermittlung im Internet; Aufgabe und Funktionsweise der Suchmaschinen stehen – Gewinnerzielungsabsicht hin oder her – einer Pflicht des Anbieters der Suchmaschine entgegen, Nachforschungen zur Rechtmäßigkeit der Veröffentlichung von urheberrechtlich geschützten Inhalten im Internet anzustellen.⁷¹

Noch nicht von der Entscheidung des BGH beeinflusst war eine Entscheidung des OLG Frankfurt a. M. aus dem Jahr 2017, das allerdings auch den Wiedergabebegriff des EuGH seiner Entscheidung nicht zugrunde legte. Auf Basis der Zurechnung mittels der Kriterien der Störerhaftung haftet ein Konzernunternehmen nach Auffassung des OLG Frankfurt a. M., wenn es auf den urheberrechtswidrigen Inhalt eines zum selben Konzern gehörenden Unternehmens mittels Hyperlink verweist, zumal wenn beim Durchschnittsnutzer der Eindruck hervorgerufen wird, dass es sich bei dieser Webseite auch um eigene Inhalte handele, was der Senat daraus folgerte, dass nicht einmal hinreichend erkennbar gewesen sei, dass es sich um zwei unterschiedliche juristische Personen handelte.⁷²

2. Suchmaschinenbetreiber und das Persönlichkeitsrecht

Nach Auffassung des OLG Köln kommt bei der Verletzung von Persönlichkeitsrechten eine Unterlassungsverpflichtung nur dann in Betracht, wenn die behauptete Rechtsverletzung offensichtlich erkennbar ist. Dies setzt voraus, dass das Inkennntnissetzungsschreiben des Betroffenen so detailliert über den Sachverhalt informiert, dass die behauptete Rechtsverletzung in tatsächlicher Hinsicht eindeutig ist und zudem die nicht hinzunehmende Beeinträchtigung des Betroffenen auf der Hand liegt.⁷³

V. WLAN-Anbieter vor der TMG-Änderung, soziale Netzwerke und Keyword-Advertiser

Auch wenn einige Bereiche in der Haftung der Internet-Provider im vergangenen Jahr in den Hintergrund traten, gab es dennoch erwähnenswerte Entscheidungen, auf die zum Abschluss noch eingegangen werden soll.

1. WLAN-Anbieter vor Inkrafttreten der Änderungen des TMG

In einer Entscheidung vom 13. 6. 2017, d. h. vier Monate vor Inkrafttreten des Dritten Änderungsgesetzes zum Teleme-

diengesetz, entschied das LG Berlin, dass der Betreiber eines TOR-Exit-Node, mit dem dritte, namentlich nicht bekannte Personen einen zensur- und überwachungsfreien Zugang zum Internet erhalten, als Störer für Rechtsverletzungen der Nutzer dieses Anschlusses hafte. Das LG folgte diese Haftung nicht aus der abstrakten Gefahr des Betriebs eines solchen Anschlusses, sondern vielmehr daraus, dass der Betreiber, nachdem er konkrete Anhaltspunkte vom Missbrauch seines Anschlusses erhielt, untätig geblieben war.⁷⁴ Erhält der Betreiber Kenntnis vom Missbrauch seines Anschlusses, müsse er – so das LG Berlin – Sicherungsmaßnahmen ergreifen, um weitere Rechtsverletzungen zu verhindern.⁷⁵ Das Urteil des LG Berlin ist mit der Einführung von §§ 8 Abs. 1 S. 2, 7 Abs. 4 TMG zunächst insoweit hinfällig, als Unterlassung nicht mehr verlangt werden kann, sondern gem. § 7 Abs. 4 TMG lediglich noch die Sperrung. Hinzu kommt, dass es jedenfalls nach dem Vortrag der Beklagten in dem Verfahren der Klägerin möglich gewesen sei, die Nutzer des Netzwerks und damit die Rechtsverletzer selbst zu ermitteln. Unterstellt, dieser Vortrag war unstreitig oder bewiesen, würde der Anspruch nach der neuen Gesetzeslage an dem Erfordernis der Subsidiarität in § 7 Abs. 4 TMG scheitern bzw. wäre eine Auseinandersetzung der Kammer mit dem BGH-Urteil „Störerhaftung des Access-Providers“ wünschenswert gewesen, nach dem jedenfalls der Access-Provider nur noch subsidiär haftet.⁷⁶

2. Betreiber sozialer Netzwerke

Nach Auffassung des OLG Dresden genügt das bloße Teilen eines Beitrags in einem sozialen Netzwerks nicht den Anforderungen an das Zueigenmachen der in dem Beitrag enthaltenen Inhalte; das Teilen selbst ist eine bloße Verbreitungshandlung. Erst wenn weitere Umstände hinzutreten, etwa eine eigene Bewertung oder eine Leseempfehlung, kann dies eine inhaltliche Identifikation und damit ein Zueigenmachen des Inhalts begründen.⁷⁷

3. Werbung durch AdWord-Kampagne

Wer eine AdWord-Kampagne schaltet, ist nach Auffassung des OLG Schleswig als Störer verantwortlich, sobald er Kenntnis davon erlangt, dass bei Eingabe eines fremden, geschützten Kennzeichens eine eigene Werbung erscheint und er gegen die Nutzung des fremden AdWords nicht einschreitet.⁷⁸ Es genügt in diesem Zusammenhang auch nicht, wenn der Werbende sich beim IT-Dienstleister lediglich erkundigt hat, ob ein identisches oder ähnliches Keyword benutzt werde und dies verneint wurde.⁷⁹ Eine

68 BGH, 21. 9. 2017 – I ZR 11/16, K&R 2018, 110, Rn. 60 ff. und Rn. 67 f. – Vorschaubilder III; kritisch *Ohly*, GRUR 2018, 187, 188; vgl. auch LG Hamburg, 13. 6. 2017 – 310 O 117/17, K&R 2017, 811 ff., das allerdings im konkreten Fall schon den Tatbestand der „öffentlichen Wiedergabe“ ablehnte und eine Störerhaftung des Linksetzers nicht mehr prüfte.

69 *Ohly*, GRUR 2018, 187, 188; *Ohly*, ZUM 2017, 793, 801; *Leistner*, ZUM 2016, 980, 982; *Jaworski/Nordemann*, GRUR 2017, 567, 571 f.

70 BGH, 21. 9. 2017 – I ZR 11/16, K&R 2018, 110, Rn. 60 – Vorschaubilder III; dem folgend LG Hamburg, 13. 6. 2017 – 310 O 117/17, K&R 2017, 811 ff.; anders noch LG Hamburg, 18. 11. 2016 – 310 O 402/16, K&R 2017, 66.

71 BGH, 21. 9. 2017 – I ZR 11/16, K&R 2018, 110, Rn. 60 f. – Vorschaubilder III; zustimmend *Ohly*, GRUR 2018, 187, 188.

72 OLG Frankfurt a. M., 4. 4. 2017 – 11 W 41/16, K&R 2017, 588, 589.

73 OLG Köln, 13. 10. 2016 – 15 U 173/15, K&R 2017, 55, 57.

74 LG Berlin, 13. 6. 2017 – 16 O 270/16, K&R 2017, 739, 740.

75 LG Berlin, 13. 6. 2017 – 16 O 270/16, K&R 2017, 739, 740.

76 BGH, 26. 11. 2015 – I ZR 174/14, K&R 2016, 171, Rn. 83 – Störerhaftung des Access-Providers.

77 OLG Dresden, 7. 2. 2017 – 4 U 1419/16, K&R 2017, 287, 288.

78 OLG Schleswig-Holstein, 22. 3. 2017 – 6 U 29/15, K&R 2017, 415, 417.

79 OLG Schleswig-Holstein, 22. 3. 2017 – 6 U 29/15, K&R 2017, 415, 417.

täterschaftliche Haftung des Werbenden lehnte der Senat ab, weil das LG keine Feststellungen dazu getroffen hatte und unklar war, ob das streitgegenständliche Keyword nicht ggf. durch einen automatischen Algorithmus von Google verwendet worden war.⁸⁰

80 OLG Schleswig-Holstein, 22.3.2017 – 6 U 29/15, K&R 2017, 415, 416 f.

RA Nikola Šarac und RA Tobias H. Strömer, Düsseldorf*

Streit zwischen der ICANN und der DENIC: Einfache Whois-Abfragen vor dem Aus

Ob Google, Facebook, oder Deutsche Post: Mit dem immer weiter steigenden Wert von (mehr oder weniger) freiwillig herausgegebenen Daten häufen sich Datenschutz-Skandale und das Thema Datenschutz rückt mehr in den Fokus der Öffentlichkeit. Datenschützer aus aller Welt raten zu deutlich mehr Datensparsamkeit und das schlägt sich auch auf gesetzgeberischer Ebene nieder. Davon betroffen sind derzeit auch grundlegende Aspekte der Internet-Nutzung, wie der nachfolgende Beitrag aufzeigen soll.

I. Einleitung

Die Internet Corporation for Assigned Names and Numbers (ICANN) ist dafür zuständig, das Verfahren und die Art und Weise der Registrierung von Internet-Domains zu regeln. Sie koordiniert das Domain Name System und die Zuteilung von IP-Adressen.¹ Mit der Vergabe deutscher Internet-Adressen unterhalb von „.de“ hat die ICANN die in Frankfurt a. M. ansässige DENIC beauftragt.

Derzeit ist es nach den Regeln der ICANN erforderlich, dass die Identität jedes Domain-Inhabers sowie der bzw. die Ansprechpartner für technische und administrative Belange der Domain über eine sogenannte Whois-Abfrage in Erfahrung gebracht werden können. Das führte für Rechtsanwälte, Rechteinhaber und sonstige Interessierte zu der komfortablen Situation, dass sie mit verschwindend geringem Aufwand den etwa für eine Markenrechtsverletzung durch die Registrierung und Nutzung einer Domain Verantwortlichen finden und kontaktieren konnten. Die DENIC stellte ein weitestgehend offenes Whois-Abfragesystem bereit.

Damit ist es nun wohl aus und vorbei. Die öffentliche Zugänglichmachung von personenbezogenen Daten, insbesondere von EU-Bürgern, könnte nämlich mit grundsätzlichen Bestimmungen der VO (EU) 2016/679, der Datenschutz-Grundverordnung (DSGVO), die am 25. 5. 2018 scharf geschaltet wird, unvereinbar sein.

Die ICANN besteht grundsätzlich auch weiter auf einer größtmöglichen Offenheit des Whois-Systems. Ein rechtlicher Konflikt zwischen der ICANN, die die Möglichkeit

VI. Ausblick

Die Neuregelungen im TMG werden die Rechtsprechung in den kommenden Jahren gehörig auf Trab halten. Allein diese genügen, um weitere interessante Entscheidungen zur Haftung der Internet-Provider auch in Zukunft erwarten zu können.

hat, Vertragsverletzungen durch Registrierungsstellen mit Vertragsstrafen zu sanktionieren, und der DENIC, der bei Nichtbeachtung der DSGVO empfindliche Bußgelder drohen, war somit vorprogrammiert. Aber verbietet die DSGVO tatsächlich öffentliche Whois-Register?

II. Whois-Abfrage im Konflikt mit Datenschutzrecht/Privacy Laws

Bereits seit vielen Jahren wird der Konflikt um die Einhaltung von ICANN-Regeln (Punkt 3.7.7 des 2013 Registrar Accreditation Agreement) einerseits und nationalem Recht andererseits diskutiert.² Problematisch sind die umfassenden Sammel-, Aufbewahrungs- und Veröffentlichungspflichten, die die ICANN den Vertragspartnern auferlegt. Zuletzt hat sie im April 2017 eine Procedure veröffentlicht, die den Registries und Registrars in sechs Schritten eine Handlungsanleitung³ zur Verfügung stellt, wie sie sich in diesem Spannungsfeld verhalten sollen:

1. Sobald die Registry oder der Registrar von einem Ermittlungs-, Klage- oder Verwaltungsverfahren oder einer sonstigen Maßnahme in Bezug auf den Whois-Prozess erfährt, die die Einhaltung seiner Pflichten gegenüber der ICANN betreffen kann, hat er sie umfassend darüber zu informieren.
2. Sodann hat eine Konsultation mit der ICANN zu erfolgen. Das Ziel der Konsultation ist die Auflösung des Konflikts mit dem nationalen Recht unter größtmöglicher Wahrung der vertraglichen Pflichten gegenüber der ICANN.
3. Für den Fall, dass Änderungen des Whois-Prozesses aus Sicht des General Counsel der ICANN für erforderlich erachtet werden, die den vertraglichen Pflichten der Registry bzw. des Registrars widersprechen, kann die ICANN vorläufig davon absehen, Vertragsverletzungsverfahren einzuleiten.

* Mehr über die Autoren erfahren Sie auf S. VIII. Alle zitierten Internetquellen wurden zuletzt abgerufen: 9. 5. 2018.

1 <https://whois.icann.org/en/domain-name-registration-process>.

2 Vgl. <https://whois.icann.org/en/privacy>.

3 <https://whois.icann.org/en/revise-icann-procedure-handling-whois-conflicts-privacy-law>.