Prof. Dr.Gerald Spindler
Lehrstuhl für Bürgerliches Recht, Handels- und Wirtschaftsrecht,
Multimedia- und Telekommunikationsrecht
Rechtsvergleichung
Institut für Wirtschaftsrecht

Georg-August-Universität Göttingen

Prof. Dr. Spindler, Platz der Göttinger Sieben 6, 37073 Göttingen

Platz der Göttinger Sieben 6
D-37073 Göttingen

Tel.: (0551) 39 - 7374
Fax: (0551) 39 - 4633
E-Mail: info@gerald-spindler.de

13. Dezember 2015

Stellungnahme

zum

Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes

(BT-Drs. 18/6745)

Das Gesetz zielt im Wesentlichen auf zwei Komplexe ab:

- der Reduktion von (Störer-) Haftungsrisiken bei WLANs und der Schaffung von Rechtssicherheit, um deren Verbreitung in Deutschland zu ermöglichen

- der „Klarstellung“, dass Hostprovider, deren Geschäftsmodelle im Wesentlichen auf der Verletzung von Urheberrechten beruhen, nicht in den Genuss der Haftungsprivilegierung nach § 10 TMG kommen können.[1]

Das Gesetz ist der EU-Kommission notifiziert worden – eine offizielle publizierte Stellungnahme der Kommission ist bislang nicht bekannt geworden.[2]

[1] Begr RegE BT-Drs. 18/6745 S. 1
[2] S. aber https://netzpolitik.org/2015/eu-kommission-kritisiert-gesetz-entwurf-zur-verschlimmbesserung-der-stoererhaftung/ Demnach soll angeblich die EU-Kommission den geplanten § 8 TMG-RegE als Verstoß gegen Art. 12 E-Commerce-RL bewertet haben, ebenso soll sie Bedenken im Hinblick auf Art. 16 EU-Grundrechte-Charta (Recht auf unternehmerische Freiheit) sowie der Meinungsfreiheit haben. Ferner soll sie im Hinblick auf § 10 TMG-RegE einen Verstoß gegen Art. 14 der E-Commerce-RL moniert haben.

Festzuhalten ist, dass

- § 8 TMG-RegE zwar auf erhebliche Vorbehalte zum einen hinsichtlich des rechtspolitischen Gehalts stößt, da die Verbreitung von WLANs kaum gefördert werden dürfe, zum anderen ein offener Tatbestand im Hinblick auf die Vereinbarkeit mit Art. 8 Abs. 3 Info-Soc-RL erforderlich ist

- § 10 TMG-RegE in europarechtlich unzulässiger Weise versucht, die Kenntnis nach Art. 14 E-Commerce-Richtlinie zu „präzisieren“

Dementsprechend geht die folgende Stellungnahme, die aufgrund der Kürze der Zeit nur kursorisch ausfallen kann, auf beide Komplexe gesondert ein:

I. Zu § 8 TMG-ReGE/§ 2 S. 1 Nr. 2a TMG-RegE - WLAN:

Die Vorschläge zu WLANs enthalten zwei Elemente:

- die Gleichstellung mit Access Providern

- die Begrenzung der Störerhaftung

A. Gleichstellung von WLANs mit Access Providern und Definition von WLANs

§ 8 Abs. 3 TMG-RegE sieht eine Gleichstellung der WLAN-Anbieter mit Zugangsvermittlern (Access-Providern) nach § 8 Abs. 1, 2 TMG (bzw. Art. 12 E-Commerce-Richtlinie).

> „(3) Die Absätze 1 und 2 gelten auch für Diensteanbieter nach Absatz 1, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen.

Die Gleichstellung mit Access Providern ist ausdrücklich zu begrüßen. Leider hatte die Rechtsprechung[3] im „leading case“ nicht erkannt, dass jedes WLAN, egal ob privat oder kommerziell oder öffentlich, den Charakter des Access Providing aufweist, da die Verbindung von Nutzern zu einem anderen Kommunikationsnetz hergestellt wird.[4] WLANs erfüllen die gleiche Funktion wie andere Access Provider, indem sie lediglich Inhalte transportieren; die rechtspolitischen

[3] BGH Urt. v. 12.5.2010 – I ZR 121/08 BGHZ 185, 330 - Sommer unseres Lebens.
[4] s. dazu bereits *Spindler* CR 2010, 592 ff.

Grundlagen der Haftungsprivilegierung in § 8 Abs. 1, 2 TMG gelten daher genauso auch für WLANs.

Europarechtliche Bedenken ergeben sich hier nicht: Zum einen sind WLANs als Access Provider im Sinne von Art. 12 der E-Commerce-RL zu qualifizieren, da sie den Zugang zu anderen Kommunikationsnetzen vermitteln und Inhalte transportieren.[5] Zum anderen wäre selbst wenn Art. 12 E-Commerce-RL nicht WLANs erfassen würde der deutsche Gesetzgeber nicht gehindert, die Haftungsprivilegierungen auf WLANs dann im Wege der Gleichstellung zu erstrecken. Zwar entfaltet Art. 12 E-Commerce-RL vollharmonisierende Wirkung – doch würde dies (wenn man der hiesigen Auffassung nicht folgen mag) nur im Anwendungsbereich gelten.

Zu begrüßen ist schließlich, dass der RegE nunmehr die unselige Unterscheidung zwischen privaten und kommerziellen Diensteanbietern bei WLANs aufgegeben hat.[6] Alles andere wäre ein Bruch mit der Systematik des TMG gewesen: Zwar verlangt die E-Commerce-RL nur bei kommerziellen Diensteanbietern die Implementierung der Haftungsprivilegierungen; doch sperrt sie keineswegs deren Erstreckung auf private Anbieter oder solche ohne kommerzielle Ausrichtung, etwa Universitäten oder andere öffentlich-rechtliche Einrichtungen. Davon hat der deutsche Gesetzgeber im TMG zu Recht Gebrauch gemacht, da nicht recht verständlich wäre, warum die Gründe für eine Haftungsprivilegierung (Vollautomatisierung, rein neutrale technische Unterstützung) nur für kommerzielle Anbieter gelten sollten.

B. Keine Technologieneutralität

Allerdings ist nicht recht einsichtig, warum der Gesetzgeber sein Ziel nur auf WLANs beschränken will. So definiert § 2 S. 1 Nr. 2a TMG-RegE ein WLAN als ein

> „Drahtloszugangsystem mit geringer Leistung und geringer Reichweite sowie mit geringem Störungsrisiko für weitere, von anderen Nutzern in unmittelbarer Nähe installierte Systeme dieser Art, welches nicht-exklusive Grundfrequenzen nutzt“.

Damit werden sämtliche andere Zugangsformen ausgeschlossen, etwa Funknetzwerke mit größerer Reichweite. Obwohl Einigkeit darüber herrscht, dass möglichst technologieneutrale Ansätze gewählt werden sollten, verengt der Gesetzgeber hier seine Maßnahmen auf einen bestimmten Typus von Zugangsformen – der zugegebenermaßen in der Praxis derzeit weit verbreitet ist, aber der keineswegs die letzte Entwicklung darstellen muss.

---

[5] Eingehend *Spindler* CR 2010, 592 ff. zu BGH Sommer unseres Lebens.
[6] Vgl. Begr RegE BT-Drs. 18/6745 S. 9.

Generell ist nicht verständlich, warum die Regelungen in § 8 Abs. 3, 4 TMG-RegE nur solche WLANs gelten sollen und nicht für alle Access Provider.[7] Da WLANs genauso wie andere Systeme nur den Zugang zu anderen Kommunikationsnetzen vermitteln und den Transport von Inhalten etc. übernehmen, sind sie nichts anderes als eine Unterkategorie der Access Provider bzw. der Zugangsvermittler im Sinne von § 8 TMG bzw. Art. 12 der E-Commerce-Richtlinie. Warum aber ausgerechnet nur WLANs in den Genuss einer (Störer-) Haftungsprivilegierung kommen sollen und nicht jegliche anderen Access Provider auch, ist nicht recht nachvollziehbar (sofern denn solche Privilegierungen zulässig sind, dazu sogleich). Die Bundesregierung gibt letztlich keine Begründung für die Beschränkung auf „lokale“ Netzwerke, sondern zieht sich lediglich auf den Koalitionsvertrag zurück.[8]

C. Die Begrenzung der Störerhaftung: Vereinbarkeit mit europäischem Recht

Neben der Privilegierung gegenüber Schadensersatzansprüchen oder einer strafrechtlichen Verantwortlichkeit will der Gesetzgeber vor allem die befürchteten Haftungsrisiken aus der Störerhaftung, wie sie die Rechtsprechung des BGH entwickelt hat, reduzieren und Rechtssicherheit schaffen. So sehr das Vorhaben grundsätzlich zu begrüßen ist, da generell die Kasuistik zur Störerhaftung von Internetintermediären kaum noch zu überblicken ist und grundsätzlich geregelt werden müsste,[9] wirft es doch im Einzelnen und insbesondere im Hinblick auf das derzeitige Europarecht Fragen auf:

> (4) Diensteanbieter nach Absatz 3 können wegen einer rechtswidrigen Handlung eines Nutzers nicht auf Beseiti-gung oder Unterlassung in Anspruch genommen werden, wenn sie zumutbare Maßnahmen ergriffen haben, um eine Rechtsverletzung durch Nutzer zu verhindern. Dies ist insbesondere der Fall, wenn der Diensteanbieter
>
> 1. angemessene Sicherungsmaßnahmen gegen den unberechtigten Zugriff auf das drahtlose lokale Netzwerk ergriffen hat und
>
> 2. Zugang zum Internet nur dem Nutzer gewährt, der erklärt hat, im Rahmen der Nutzung keine Rechtsverlet-zungen zu begehen.“

Der Gesetzgeber ist hier ersichtlich bemüht, die Rechtsprechung des BGH, wie sie vor allem in der bereits zitierten Entscheidung „Sommer unseres Lebens“ ihren Ausdruck gefunden hat, zu

---

[7] Im Ansatz auch die Stellungnahme des Stellungnahme BRat BT-Drs. 18/6745 S. 17f.
[8] Gegenäußerung BReG BT-Drs. 18/6745 S. 21.
[9] Hierzu schon die Vorschläge des Unterzeichners in dem Review-Report zur E-Commerce-Richtlinie im Auftrag der EU-Kommission *Verbiest/Riccio/Spindler* Study on the Liability of Internet Intermediaries, 2007, Markt/2006/E, abrufbar unter http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2575069 ; s. ferner *Spindler* FS 50 Jahre UrheberrechtsG, 2015, S. 399 ff. mwNachw zur Rspr. und einer Strukturierung.

kodifizieren.[10] In dieser Entscheidung hatte der BGH zwar zumutbare Sicherungsmaßnahmen gegen den unberechtigten Zugriff auf das WLAN gefordert, diese gleichzeitig aber für den durchschnittlichen privaten Betreiber eines WLAN erheblich reduziert (z.B. Veränderung der werksseitigen Voreinstellungen, Einschalten von Sicherungsmaßnahmen etc.). Allerdings führt § 8 Abs. 4 Nr. 1 TMG-RegE dies nur als besonderen Fall auf, so dass der Katalog der zumutbaren Maßnahmen, um Rechtsverletzungen durch Nutzer zu verhindern, keineswegs abschließend umschrieben ist. Ob damit tatsächlich das Ziel der Rechtssicherheit erreicht werden kann und ob gegenüber dem jetzigen Rechtszustand ein Mehrwert zu erwarten ist, erscheint eher zweifelhaft; wie noch darzulegen ist, dürfte aber ein solch offener Tatbestand europarechtlich sogar geboten sein.

Ferner erfasst § 8 Abs. 4 Nr. 1 TMG-RegE nur Sicherungsmaßnahmen gegen den unberechtigten Zugriff auf das Netzwerk. Was damit genau gemeint ist, bleibt offen: So führt die Begründung zum RegE letztlich wiederum die vom BGH ins Auge gefassten Maßnahmen an, insbesondere etwa Verschlüsselungen bzw. Sicherungen wie WPA2, hält aber auch die „freiwillige“ Registrierung der Nutzer für denkbar. Gemeint ist wohl auch damit die Vergabe eines Codes vor Ort oder die Identifizierung mittels Smartphone-Authentifizierung. Initiativen wie „Freifunk“, die ohne jeglichen Code etc. auskommen, dürften damit nicht unter die Privilegierung fallen.

Fraglich ist weiterhin, ob damit auch für die Zukunft (Unterlassungsansprüche) den Anforderungen der Rechtsprechung genüge getan wäre: Die Entscheidung des BGH bezog sich auf einen (typischen) Familienfall, in dem der Beklagte einwandte, dass ein unbekannter Dritter sich Zugang zu dem Netz verschafft und die Rechtsverletzungen begangen habe. Ohne eine Pflicht zur Sicherung des Netzes würde ein betroffener Rechteinhaber schutzlos stehen, da jederzeit irgendein nicht näher zu identifizierender Dritter die Rechtsverletzungen begangen haben könnte; umgekehrt reichen derartige Sicherungsmaßnahmen im Angehörigen und Familienkreis, da die in Betracht kommenden eigentlichen Rechtsverletzer eingrenzbar sind. Die Situation ist aber eine andere, wenn man sich auf öffentliche WLANs, etwa in Restaurants oder auf öffentlichen Plätzen etc. bezieht – auch die Absicherung eines WLANs gegenüber Dritten führt nicht dazu, dass angesichts eines stets wechselnden Personenkreis etwaige Rechtsverletzer ausfindig gemacht werden könnten. Auch wenn der Zugang zum WLAN von einem Code abhängig ist, ändert dies

[10] Deutlich Begr RegE BT-Drs. 18/6745 S. 12: „Die bisherigen, von der Rechtsprechung entwickelten Grundsätze werden dabei im Sinne von Regelbeispielen aufgegriffen und fortentwickelt, um möglichst weitgehend Rechtssicherheit zu schaffen. Dabei sollen die von der Rechtsprechung für private WLAN-Anschlussinhaber entwickelten Grundsätze gleichermaßen für alle anderen Betreiber von WLAN gelten.“

nichts daran, dass jeder mit Zugang zu dem öffentlichen Platz etc. (z.B. ein über einen Screen bei einer Stadtverwaltung im Wartesaal für jedermann bekanntgegebenen Code) sich den Zugang verschaffen kann.

Man mag mit dem Bundesrat einwenden, dass die Wahrscheinlichkeit von Rechtsverletzungen über solche WLANs extrem gering sei – ob und wie diese Annahme zutrifft, muss sich im Rahmen einer Evaluierung zeigen. Jedenfalls lässt sich kaum leugnen, dass allein mit einem jedermann gegebenen Code oder sonstigen Zugang die Rechtsverfolgung für Betroffene enorm erschwert werden könnte.

Aus europarechtlicher Sicht ist schließlich daran zu erinnern, dass der EuGH in der Telekabel-Entscheidung[11] grundsätzlich Sperrverfügungen gegenüber Access Providern zu dem Kanon an zu verlangenden Maßnahmen zählt – zwar zutreffend unter sehr eingeschränkten Bedingungen, aber aufgrund Art. 8 Abs. 3 der Richtlinie 2001/29/EG (InfoSoc-RL) sah sich das Gericht genötigt, solche Maßnahmen als von den Richtlinien unter Umständen gefordert anzusehen.

> „32 Der Anbieter von Internetzugangsdiensten ist an jeder Übertragung einer Rechtsverletzung im Internet zwischen einem seiner Kunden und einem Dritten zwingend beteiligt, da er durch die Gewährung des Zugangs zum Netz diese Übertragung möglich macht (vgl. in diesem Sinne Beschluss vom 19. Februar 2009, LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten, C-557/07, Slg. 2009, I-1227, Rn. 44). Infolgedessen ist davon auszugehen, dass ein Anbieter von Internetzugangsdiensten wie der im Ausgangsverfahren in Rede stehende, der seinen Kunden den Zugang zu Schutzgegenständen ermöglicht, die von einem Dritten im Internet öffentlich zugänglich gemacht werden, ein Vermittler ist, dessen Dienste zur Verletzung eines Urheberrechts oder eines verwandten Schutzrechts im Sinne von Art. 8 Abs. 3 der Richtlinie 2001/29 genutzt werden.
>
> 33 Bestätigt wird dieses Ergebnis durch das mit der Richtlinie 2001/29 verfolgte Ziel. Nähme man nämlich die Anbieter von Internetzugangsdiensten vom Anwendungsbereich des Art. 8 Abs. 3 der Richtlinie 2001/29 aus, würde der mit der Richtlinie angestrebte Schutz der Rechtsinhaber erheblich verringert (vgl. in diesem Sinne Beschluss LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten, Rn. 45).“

Dann aber ist fraglich, ob der deutsche Gesetzgeber in § 8 Abs. 4 TMG-RegE diese Maßnahmen ausschließen kann, wenn er allein auf zumutbare Sicherungsmaßnahmen gegen den unberechtigten Zugriff auf ein WLAN abstellt. Gleichzeitig betont der EuGH aber:

> „43 Wie insoweit aus dem 59. Erwägungsgrund der Richtlinie 2001/29 hervorgeht, sind die Modalitäten der von den Mitgliedstaaten nach Art. 8 Abs. 3 dieser Richtlinie vorzusehenden Anordnungen, wie z. B. Anordnungen in Bezug auf die zu erfüllenden Voraussetzungen und das einzuhaltende Verfahren, im nationalen Recht zu regeln.“

---

[11] EuGH Urt. v. 27.3.2014 - C 314/12 – UPC Telekabel

Damit ist es zur Erfüllung der Pflichten aus Art. 8 Abs. 3 InfoSoc-RL nicht zwingend erforderlich, dass Sperrverfügungen verhängt werden können. Allerdings bestehen hier durchaus Rest-Zweifel, da nicht ersichtlich ist, wie ein betroffener Rechteinhaber sonst Schutz erlangen könnte. Letztlich fängt § 8 TMG-RegE dies aber dadurch auf, dass der Katalog an Maßnahmen nicht abschließend umschrieben wird

Ferner will der RegE die Privilegierung gegenüber der Störerhaftung dadurch sicherstellen, dass der Nutzer zuvor erklärt haben muss, dass er keine Rechtsverletzungen begeht. In welcher Form dies geschieht, will der Gesetzgeber explizit den Betreibern überlassen, etwa durch eine Klick-Box, anscheinend aber auch allein durch die Verwendung eines Passwortes, mit dem der Zugang dann erreicht wird.[12] Ob dann damit eine konkludente Erklärung gemeint ist, erschließt sich nicht näher aus der Begründung. Ebenfalls soll die Aufnahme der Erklärung in AGB genügen.[13] Auch hier bleibt einiges unklar: Für die Einbeziehung von AGB genügt bekanntlich gem. § 305 Abs. 2 BGB, dass die andere Vertragspartei sie zur Kenntnis nehmen konnte (!), nicht aber musste.

> „(2) Allgemeine Geschäftsbedingungen werden nur dann Bestandteil eines Vertrags, wenn der Verwender bei Vertragsschluss
> 1. die andere Vertragspartei ausdrücklich oder, wenn ein ausdrücklicher Hinweis wegen der Art des Vertragsschlusses nur unter unverhältnismäßigen Schwierigkeiten möglich ist, durch deutlich sichtbaren Aushang am Ort des Vertragsschlusses auf sie hinweist und
> 2. der anderen Vertragspartei die Möglichkeit verschafft, in zumutbarer Weise, die auch eine für den Verwender erkennbare körperliche Behinderung der anderen Vertragspartei angemessen berücksichtigt, von ihrem Inhalt Kenntnis zu nehmen, und wenn die andere Vertragspartei mit ihrer Geltung einverstanden ist.“

Wie sich dies dann zu der vermeintlich erforderlichen Erklärung in § 8 Abs. 4 Nr. 2 TMG-RegE verhält, bleibt dunkel.

Allgemein dürfte dieser Erklärung auch kein großer Wert beizumessen sein: Diejenigen, die Rechtsverletzungen begehen wollen oder die sie billigend in Kauf nehmen, werden sich von einer solchen Erklärung kaum abhalten lassen – denn welche Sanktionen sollten sie zu vergegenwärtigen haben? Eine Schadensersatzhaftung gegenüber dem WLAN-Betreiber kommt von

[12] So explizit Begr RegE BT-Drs. 18/6745 S. 13.
[13] Begr RegE BT-Drs. 18/6745 S. 13.

vornherein nicht in Betracht, da dieser ja selbst nicht haftet, also auch keinen Regress nehmen könnte.

Klargestellt werden könnte allenfalls, wie vom Bundesrat vorgeschlagen, dass entsprechend Art. 12 E-Commerce-RL kollusives Zusammenwirken ausgenommen ist.[14]

Eine komplette Ausnahme von der Störerhaftung, wie sie vom Bundesrat vorgeschlagen wurde,[15] erscheint jedoch angesichts der oben zitierten Rechtsprechung des EuGH zu Art. 8 Abs. 3 der InfoSoc-RL nicht möglich.

Daher dürfte es auch nicht möglich sein, wie vom Bundesrat vorgeschlagen, keinerlei Differenzierungen zwischen berechtigten und unberechtigten Zugang zu treffen (im Hinblick auf öffentlich zugängliche Hotspots).[16]

Nach Auffassung des Bundesrats würden die Überwachungspflichten nach TKG (§§ 110, 113 TKG) genügen, zudem seien die privaten WLAN-Betreiber an kommerzielle Accessprovider angeschlossen, die den Rahmenbedingungen des TKG unterliegen.[17] Auch sei die Bedeutung von Filesharing gesunden, im Vordergrund stünde Streaming wie kinox.to, hier sei aber WLAN-Zugangspunkt gänzlich ungeeignet.

Es mag zutreffen, dass rechtstatsächlich keine massiven Urheberrechtsverletzungen zu befürchen sind, wie es offenbar ein Pilotprojekt der Medienanstalt Brandenburg mit Kabel Deutschland nahelegt, bei der es keine IP-Adressenabfragen wegen UrhR-Verletzungen gegeben habe.[18] Dennoch ändert dies nichts daran, dass von Rechts wegen dem Betroffenen nach der Auslegung des EuGH die Chance gegeben werden muss, entsprechende Maßnahmen vom Access Provider zu verlangen. Warum hier WLAN-Betreiber (gerade im Hinblick auf die richtige Gleichstellung mit Access Providern) anders zu behandeln sein sollten als sonstige Access Provider, ist nicht recht einsichtig.

Wenn man zudem die Störerhaftung gesetzlich ausformen wollte, fehlt es zudem nach wie vor an Regelungen zur Beteiligung Dritter, die der EuGH in der Entscheidung Telekabel deutlich angemahnt hat, und die zum Schutz der Grundrechte Dritter (Meinungsfreiheit etc.) dienen:

---

[14] Stellungnahme BRat BT-Drs. 18/6745 S. 16 f.
[15] Stellungnahme BRat BT-Drs. 18/6745 S. 17.
[16] Stellungnahme BRat BT-Drs. 18/6745 S. 18.
[17] Stellungnahme BRat BT-Drs. 18/6745 S. 18.
[18] Stellungnahme BRat BT-Drs. 18/6745 S. 19.

> 57 Die nationalen Gerichte müssen prüfen können, ob dies der Fall ist. Bei einer Anordnung wie der im Ausgangsverfahren in Rede stehenden haben sie aber, wenn der Anbieter von Internetzugangsdiensten Maßnahmen ergreift, die es ihm ermöglichen, das vorgeschriebene Verbot umzusetzen, nicht die Möglichkeit, eine solche Kontrolle im Stadium des Vollstreckungsverfahrens vorzunehmen, wenn keine dahin gehende Beanstandung erfolgt. Damit die im Unionsrecht anerkannten Grundrechte dem Erlass einer Anordnung wie der im Ausgangsverfahren fraglichen nicht entgegenstehen, ist es deshalb erforderlich, dass die nationalen Verfahrensvorschriften die Möglichkeit für die Internetnutzer vorsehen, ihre Rechte vor Gericht geltend zu machen, sobald die vom Anbieter von Internetzugangsdiensten getroffenen Durchführungsmaßnahmen bekannt sind.

II. Zu § 10 TMG-RegE – Host-Provider

§ 10 TMG-RegE versucht gegenüber § 8 TMG-RegE nicht nur die Störerhaftung zu regeln, sondern will auch Präzisierungen für die Haftung der Host-Provider generell herbeiführen.

> (2) Die Kenntnis von Tatsachen oder Umständen nach Absatz 1, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, wird vermutet, wenn es sich bei dem angebotenen Dienst um einen besonders gefahrgeneigten Dienst handelt. Ein besonders gefahrgeneigter Dienst liegt in der Regel dann vor, wenn
> 1. die Speicherung oder Verwendung der weit überwiegenden Zahl der gespeicherten Informationen rechtswidrig erfolgt,
> 2. der Diensteanbieter durch eigene Maßnahmen vorsätzlich die Gefahr einer rechtsverletzenden Nutzung fördert,
> 3. in vom Diensteanbieter veranlassten Werbeauftritten mit der Nichtverfolgbarkeit bei Rechtsverstößen geworben wird oder
> 4. keine Möglichkeit besteht, rechtswidrige Inhalte durch den Berechtigten entfernen

So sehr man das Anliegen nachvollziehen kann, evident rechtswidrige Geschäftsmodelle wie etwa früher kino.to zu unterbinden, stößt die vorgeschlagene Regelung doch auf erhebliche Bedenken, insbesondere aus europarechtlicher Hinsicht:

A. Art. 14 E-Commerce-RL als vollharmonisierende Regelung

§ 10 TMG setzt Art. 14 der E-Commerce-RL um. Alle Normen zur Haftungsprivilegierung der E-Commerce-RL sind vollharmonisierender Natur,[19] d.h. dass der nationale Gesetzgeber an sie gebunden ist und weder Ergänzungen noch Reduktionen, aber auch keine „Präzisierungen“ vornehmen kann, sofern diese nicht vom Wortlaut der Richtlinie gedeckt sind. Genau eine solche „Präzisierung“ wird aber mit § 10 Abs. 2 TMG-RegE erreicht – die von Art. 14 E-Commerce-RL nicht vorgesehen ist und die somit europarechtswidrig ist. Im Einzelnen:

---

[19] BGH, Urt. v. 4.7.2013 – I ZR 39/12– Terminhinweise auf Kartenausschnitten

B. Kenntnis und Vermutungsregelungen

§ 10 Abs. 2 TMG-RegE bezieht sich auf die Haftungsprivilegierung des § 10 TMG bzw. Art. 14 E-Commerce-RL generell und nicht etwa nur auf die Störerhaftung wie § 8 Abs. 4 TMG-RegE. Damit muss § 10 Abs. 2 TMG-RegE die Vorgaben des Art. 14 E-Commerce-RL einhalten. Dieser sieht aber für das Eingreifen einer Verantwortlichkeit (sowohl strafrechtlich als auch zivilrechtlich) Kenntnis vom rechtswidrigen Inhalt vor oder zumindest (zivilrechtlich) Kenntnis von Umständen, die solche rechtswidrigen Inhalte und Aktivitäten nahe legen. Art. 14 E-Commerce-RL kennt aber keinen Vermutungstatbestand, der auf bestimmte Umstände rekurrieren würde. Diese können im Rahmen des nationalen Zivilprozessrechts zwar entwickelt werden, etwa was Indizien angeht im Rahmen einer Beweiswürdigung; sie können aber nicht im Wege einer materiell- oder prozessrechtlichen Vermutung gesetzlich festgelegt werden.[20]

Dem widerspricht die Systematik des vorgesehen § 10 Abs. 2 TMG-RegE, der bei Vorliegen bestimmter Tatbestände eine Vermutungswirkung auslöst. Dies zeigt deutlich auch die Begründung:

> „Bei bestimmten Diensten, deren Geschäftsmodell auf der Verletzung des Rechts des geistigen Eigentums beruht, kann nach der allgemeinen Lebenserfahrung davon ausgegangen werden, dass dem Diensteanbieter ausreichend viele Tatsachen oder Informationen bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird. Diese Dienste bezeichnet die Rechtsprechung mittlerweile als „gefahrgeneigte Dienste“.[21]

Die einzelnen Tatbestände des § 10 Abs. 2 TMG-RegE sind ersichtlich von dem Bemühen geleitet, die in der Rechtsprechung des BGH zur Störerhaftung entwickelten Kriterien[22] auch für die Haftungsprivilegierung in § 10 TMG fruchtbar zu machen. Es ist zwar letztlich wünschenswert, dass wieder ein Gleichlauf der zivilrechtlichen Verantwortlichkeit bei Schadensersatzansprüchen und der Störerhaftung erreicht wird; doch kann dies nur auf europarechtlicher Ebene geschehen, was offenbar derzeit auf der Agenda der EU-Kommission steht.

Es ist in diesem Rahmen unrichtig, wenn die Begründung zum RegE behauptet,[23] dass die Kenntnis nach § 10 TMG gleichzusetzen sei mit den Kriterien, die in § 10 Abs. 2 TMG Reg-E aufgeführt sind; alle diese Kriterien entstammen der Rechtsprechung zur Störerhaftung und sind

---

[20] Ähnlich *Frey/Rudolph/Oster* CR 2015, Beil. Rz. 65 ff.
[21] Begr RegE BT-Drs. 18/6745 S. 14.
[22] Ausführlicher zur Systematik *Spindler* FS 50 Jahre UrheberrechtsG, 2015, S. 399 ff.
[23] So ausdrücklich Begr RegE BT-Drs. 18/6745 S. 9: „Von Kenntnis ist nach dem vorliegenden Gesetz insbesondere dann auszugehen, wenn das Geschäftsmodell weit überwiegend auf der Verletzung von z.B. Urheberrechten aufbaut, was bei Auslegung des geltenden Rechts auch heute schon der Fall sein dürfte. Dies unzweideutig festzulegen, bezweckt des Gesetzes.“

dort entwickelt worden, um die zumutbaren Prüf- und Kontrollpflichten zu konkretisieren.[24] In keinem einzigen dieser Fälle wurde über einen Schadensersatzanspruch entschieden – der eben Kenntnis oder zumindest Kennenmüssen der evidenten Umstände voraussetzt. Wäre die Annahme der Begr zum RegE richtig, fragt man sich unwillkürlich, warum die Gerichte keine Schadensersatzansprüche zuerkannt haben. Mit der Kenntnis haben die Kriterien nichts zu tun.[25]

Auch die Entscheidung des EuGH in der Sache L`Oreal vs. Ebay[26] kann hier nicht herangezogen werden: Der EuGH hatte hier die Anwendung von Art. 14 E-Commerce-RL davon abhängig gemacht, dass ein Hostprovider keine aktive Rolle im Hinblick auf den Inhalt des Dritten spielt, insbesondere nicht unterstützend bei Werbemaßnahmen eingreift etc.[27] Unabhängig davon, ob diese Kriterien überhaupt noch kodifiziert werden müssten (angesichts der Rechtsprechung), entspricht § 10 Abs. 2 TMG-RegE nicht diesen Kriterien. Von einer aktiv unterstützenden Rolle ist nirgendswo die Rede, stattdessen von überwiegend rechtswidrigen Inhalten.

C. Überwiegend auf Rechtswidrigkeit ausgerichtetes Geschäftsmodell

Ferner widerspricht auch en detail § 10 Abs. 2 Nr. 1 TMG-RegE der europarechtlichen Rechtslage: Das offensichtlich aus der Rechtsprechung des BGH zur Störerhaftung übernommene Kriterium des von der Rechtsordnung missbilligten Geschäftsmodells mag in der Störerhaftung berechtigt sein – die übrigens nur ab Kenntnis des Host-Providers eingreift, mithin nach der ersten Abmahnung, aber nicht vorher. Abgesehen davon, dass bislang – soweit ersichtlich – der BGH kein einziges Mal ein Geschäftsmodell als von der Rechtsordnung missbilligt angesehen hat, nicht einmal in den Rapidshare-Fällen,[28] würde dieses Kriterium bei der Schadensersatzhaftung auf jeden Fall Art. 15 der E-Commerce-RL widersprechen. Denn woher soll ein Provider ex ante (!) wissen, dass auf seinen Servern mehrheitlich Rechtsverletzungen begangen werden? Eine solche Kenntnis könnte er sich nur durch eine allgemeine Überwachung der Aktivitäten verschaffen – deren Einführung aber gerade von Art. 15 E-Commerce-RL den Mitgliedstaaten untersagt ist. Anders formuliert müsste der Provider vorausschauend seine Plattformen überprüfen, um zu wissen, ob bzw. wann überwiegende Rechtsverletzungen begangen werden – damit würde das Modell von Art. 14, 15 E-Commerce-RL in sein Gegenteil verkehrt. Egal wie man rechtspolitisch zu dem Modell der E-Commerce-RL stehen mag (für das es gute Gründe gibt, es zu modifizieren),

---

[24] Näher *Spindler* FS 50 Jahre UrheberrechtsG, 2015, S. 399 ff. mwNachw.
[25] Ebenso *Frey/Rudolph/Oster* CR 2015, Beil. Rz. 54 ff.
[26] EuGH Urt. v. 12. Juli 2011 – C-324/09
[27] Zur Maßgeblichlkeit dieses Kriteriums s. auch *Frey/Rudolph/Oster* CR 2015, Beil. Rz. 41 ff.
[28] BGH Urt. v. 12.7.2012 – I ZR 18/11 – Alone in the dark; BGH Urt. v. 15.8.2013 – I ZR 80/12 – File-Hosting Dienst.

es ist jedenfalls dem nationalen Gesetzgeber verwehrt, quasi durch die „Hintertür“ durch „Präzisierungen“ das Haftungsmodell der E-Commerce-RL zu unterlaufen.

Dies gilt umso mehr, wenn der Gesetzgeber offenbar bereits mehr als 50% von rechtswidrigen Inhalten als unzulässiges Geschäftsmodell ansehen will. Dabei soll es noch nicht einmal auf die absolute Zahl ankommen:

> Entscheidend ist hierbei nicht die absolute Zahl der rechtswidrigen Inhalte, sondern der relative Anteil der rechtswidrigen Inhalte. Liegt dieser bei weit über 50% der gespeicherten Informationen, kann davon ausgegangen werden, dass dem Diensteanbieter dies nicht verborgen geblieben ist.[29]

Als relativer Anteil ist dabei wohl das Verhältnis zu den rechtmäßigen Anteilen gemeint. Welche Probleme allerdings damit verbunden sind, zeigt sich schon, wenn man nicht nur das Urheberrecht, sondern etwa das Persönlichkeitsrecht in den Blick nimmt. Bekanntlich ist die Abwägung der Grundrechte der Meinungsäußerung, Art. 5 Abs. 1 GG, und des Persönlichkeitsschutzes (Art. 2 Abs. 1 GG) äußerst diffizil, erst recht, wenn Mediengrundrechte (Art. 5 Abs. 1 S. 2 GG) noch ins Spiel kommen. Aber selbst im Urheberrecht kann die Rechtswidrigkeit nicht sofort auf Anhieb geklärt werden, man nehme etwa Inhalte, die im Ausland aufgrund von bestimmten Schranken rechtmäßig auf ein Portal gespeichert wurden, das aber im Inland abrufbar ist.[30]

Ferner ist fraglich, was ein „relativer Anteil“ ist bzw. worauf dieser sich bezieht: Auf das gesamte Angebot eines Host-Providers? oder nur bestimmte Kategorien? Sollten etwa Gästeforen von Online-Zeitungen bzw. Medien zu einem provokanten Thema, indem die einschlägigen Beiträge nur so von Beleidigungen und Hetze wimmeln, sei es zu Flüchtlingen oder zu netzpolitischen Themen, eigenständig bewertet werden, da hier der „relative Anteil“ weit über 50% beträgt? Über welche Zeiträume sollte dieser Anteil bemessen werden? Gälte nur ein Zeitraum einer Woche, eines Tages, eines Monats oder eines Jahres, ab dem „nach der Lebenserfahrung“ Kenntnis anzunehmen ist?

Ferner will § 10 Abs. 2 Nr. 1 TMG-RegE nicht nur auf die Speicherung, sondern auch auf die „Verwendung der weit überwiegenden Zahl der gespeicherten Informationen“ in rechtswidriger Weise abstellen. Damit wird endgültig der Boden des Art. 14 E-Commerce-RL verlassen: Denn dieser stellt allein auf die Speicherung von fremden Inhalten ab – wie diese dann „verwandt“ werden (durch wen?) ist für Art. 14 E-Commerce-RL völlig belanglos. Art. 14 E-Commerce-RL

---

[29] So ausdrücklich Begr RegE BT-Drs. 18/6745 S. 14:

[30] Nach der wohl hM wäre der Host-Provider – bei unterstellter Annahme des § 10 Abs. 2 TMG-RegE – dann haftbar, da § 19a UrhG z.B. bei einem öffentlich Zugänglichmachen tangiert wäre und hierfür deutsches Recht Anwendung fände.

stellt allenfalls noch auf rechtswidrige Aktivitäten ab, die sich aber auch dann auf den Rechnern des Host-Providers abspielen müssen. Was in diesem Zusammenhang das Kriterium des Verwendens bedeuten soll, bleibt völlig unklar, zumal damit offenbar auch die weitere Verwendung der Daten bei den Nutzern in rechtswidriger Weise gemeint sein soll – wie aber ein Host-Provider Kenntnis davon erlangen soll, wie die Nutzer Daten weiter verwenden und in welchem Zusammenhängen, ist unklar.

Schließlich ist in diesem Zusammenhang darauf zu verweisen, dass § 10 Abs. 1 TMG-RegE nicht nur im Lichte des Zivilrechts, sondern auch des Strafrechts zu sehen ist. Hier gilt aber bekanntlich das Bestimmtheitsgebot, insbesondere dass ein betroffener Host-Provider klar erkennen können muss, ob er unter eine Strafbestimmung fällt oder nicht. Zwar handelt es sich bei § 10 TMG um eine Haftungsprivilegierung, so dass prima vista der Grundsatz „nulla poena sine lege“ nicht eingreift; doch würde die „Präzisierung“ des Gesetzgebers eine Rückausnahme darstellen und damit quasi wiederum zum Straftatbestand zählen. Wie aber der Hostprovider erkennen soll, dass eine „weit überwiegende“ Zahl der Inhalte, die er speichert, rechtswidrig sind, oder gar deren Verwendung, bleibt unklar.

D. Vorsätzliche Förderung der Gefahr einer rechtsverletzenden Nutzung

Ferner soll nach § 10 Abs. 2 Nr. 2 TMG RegE Kenntnis anzunehmen sein, wenn ein Diensteanbieter vorsätzlich die Gefahr einer rechtsverletzenden Nutzung fördert. Damit würde das TMG praktisch eine Art Vorfeldschutz einführen: Denn nicht die vorsätzliche Förderung der fremden Tat wäre schädlich (hier wäre im Rahmen der Grundsätze zur Beihilfe bereits per se Kenntnis anzunehmen), sondern allein schon die Förderung „der Gefahr“ genügt. Dies soll nach der Begründung schon dann der Fall sein, wenn Speicherplatz unentgeltlich angeboten wird, sofern in einer bestimmten Zahl Inhalte herauf- und heruntergeladen werden.[31]

> „Fördert der Dienstanbieter gezielt die Gefahr einer rechtswidrigen Nutzung, kann ebenfalls Kenntnis vermutet werden. Im Sinne der Rechtsprechung des BGH ist dies beispielsweise anzunehmen, wenn der Diensteanbieter, anders als im Bereich des „Cloud Computing“, für die Bereitstellung von Speicherplatz kein Entgelt verlangt, sondern seine Einnahmen von der Downloadhäufigkeit der hochgeladenen (rechtswidrigen) Dateien abhängig sind (Urteil v. 15.8.2013, Az. I ZR 80/12, „File-Hosting-Dienst“ bzw. „Rapidshare“). Nicht ausreichend ist, wenn Maßnahmen lediglich auch die Gefahr einer rechtsverletzenden Handlung fördern. Bei einem Geschäftsmodell, das im bloßen Angebot einer Cloud besteht, wird die Gefahr einer rechtsverletzenden Nutzung ebenfalls nicht gefördert.“

[31] So Begr RegE BT-Drs. 18/6745 S. 14.

Die Begründung zeigt bereits die Probleme der Abgrenzung: Reine Cloud-Dienste sollen nicht die Gefahr einer rechtsverletzenden Nutzung fördern, wohl aber Geschäfsmodelle, die Einnahmen von der Downloadhäufigkeit von Dateien abhängig machen. Wiederum ist festzuhalten, dass die Rechtsprechung aus dieser Unterscheidung keine Kenntnis ableitet, sondern nur die Intensität von Prüfungs- und Kontrollpflichten. Unklar wäre damit aber auch für die Zukunft, wie mit Cloud-Anbietern zu verfahren ist, die kostenlosen Speicherplatz anbieten, dann aber ab einem bestimmten Volumen Entgelte verlangen – sollten diese anders behandelt werden als Modelle, die nach dem Datentraffic Entgelte berechnen, wenn ja warum?[32]

E. Werbung mit rechtswidrigen Inhalten

Einigkeit wird man eher bei § 10 Abs. 2 Nr. 3 TMG-RegE erzielen kann – in diesen Fällen wirbt der Diensteanbieter mehr oder minder deutlich mit der Verfügbarkeit rechtswidriger Inhalte. Diese Fälle können aber schon durch § 10 S. 1 TMG bzw. Art. 14 E-Commerce-RL erfasst werden, da hier der Diensteanbieter evident Kenntnis von den rechtswidrigen Inhalten hat – er fordert förmlich zum Rechtsbruch auf.[33] Demgemäß hat die Rechtsprechung auch wenig Federlesens mit solchen Fällen gemacht.[34]

F. Keine Entfernung der Inhalte möglich

Schließlich zielt § 10 Abs. 2 Nr. 4 TMG-RegE auf Sachverhalte ab, in denen der Diensteanbieter keine Löschung der Inhalte ermöglicht. Der RegE rekurriert hier prima vista zutreffend auf die Pflicht nach § 10 TMG bzw. Art. 14 E-Commerce-RL des Diensteanbieters, nach Kenntnisnahme die Inhalte zu entfernen. Indes ist dies nur die Hälfte von Art. 14 E-Commerce-RL: denn dieser verlangt keineswegs die Löschung der Inhalte, er lässt es vielmehr genügen, wenn der Zugang zu ihnen gesperrt wird.

> Artikel 14
>
> (1) Die Mitgliedstaaten stellen sicher, daß im Fall eines Dienstes der Informationsgesellschaft, der in der Speicherung von durch einen Nutzer eingegebenen Informationen besteht, der Diensteanbieter nicht für die im Auftrag eines Nutzers gespeicherten Informationen verantwortlich ist, sofern folgende Voraussetzungen erfüllt sind:
>
> ... b) der Anbieter wird, sobald er diese Kenntnis oder dieses Bewußtsein erlangt, unverzüglich tätig, um die Information zu entfernen oder den Zugang zu ihr zu sperren."

---

[32] Bedenken auch bei *Frey/Rudolph/Oster* CR 2015, Beil. Rz. 81.
[33] Anders offenbar *Frey/Rudolph/Oster* CR 2015, Beil. Rz. 83 ff., die hierin eine verdeckte lauterkeitsrechtliche Vorschrift sehen – dies blendet indes die Parallelen zur Aufforderung zum Rechtsbruch aus, wie sie etwa in § 826 BGB entwickelt wurden.
[34] BGH, Urt v. 15.01.2009 - I ZR 57/07 – Cybersky, wiederum im Rahmen der Störerhaftung.

Egal, wie man hierzu rechtspolitisch stehen mag, aber eine „Präzisierung“ kann hierin nicht mehr gesehen werden, da die von der Richtlinie vorgesehen Alternativen unzulässig auf eine reduziert werden. Warum zudem ein Diensteanbieter, wenn er die Alternative der Sperrung des Zugangs wählt, per se Kenntnis von den Inhalten haben soll, ist nicht recht verständlich.

III. Auskunftsrechte für Verletzungen der Persönlichkeitsrechte

Ausdrücklich zu begrüßen ist dagegen der Vorschlag des Bundesrates, dass in § 14 Abs. 2 TMG neben dem Eigentum auch die „Persönlichkeitsrechte“ aufgeführt werden.[35] Hiermit wird ein Hindernis auf dem Weg zu Auskunftsansprüchen bei Verletzungen von Persönlichkeitsrechten aus dem Weg geräumt. Es war und ist nicht einzusehen, warum Rechteinhaber besser geschützt werden als Opfer von Diffamierungen etc.[36] Allein eine Reform des § 14 Abs 2 TMG genügt indes hier nicht; da der BGH angesichts des expliziten Schweigens einen Auskunftsanspruch für Persönlichkeitsrechtverletzungen verworfen hat,[37] ist hier eine Reform, die sich an § 101 UrhG anlehnt unter Berücksichtigung des Datenschutzes dringend erforderlich – und verfassungsrechtlich auch geboten.

Prof.Dr.Gerald Spindler

[35] Stellungnahme BRat BT-Drs. 18/6745 S. 19.
[36] Hierzu bereits *Spindler* DJT 2012 Gutachten F, der Vorschlag wurde vom Deutschen Juristentag angenommen.
[37] BGH, 01.07.2014 - VI ZR 345/13