Mindbase Strategic Consulting
Stefan Herwig
Horster Straße 31
45897 Gelsenkirchen
Tel: 0209 38 650 670
Fax: 0209 38 650 668

Bundesministerium für Wirtschaft und Energie
z.H. Dr. Dörte Nieland
Scharnhorststr. 34-37
10115 Berlin
tmg@bmwi.bund.de

Betr.: Referentenentwurf eines 2. Gesetzes zur Änderung des Telemediengesetzes (2.TMGÄndG)

Eingabe
A/B/C Algorithmus – Vorschläge zur Anpassung des TMG / Stefan Herwig / Mindbase

Sehr geehrte Frau Dr. Nieland, sehr geehrte Damen und Herren,

am 04.März.2015 veranstalteten wir bei Ihnen im Hause einen Workshop u.a. zu den Themen Datenschutz und Providerhaftung. Im Nachgang wurden wir von Teilen des BMWi gebeten, unsere dort diskutierten Thesen, insbesondere zum Thema Providerhaftung schriftlich niederzulegen, und als Eingabe für die o.g. Gesetzesänderung einzureichen.
Von dieser Möglichkeit machen wir hiermit gerne Gebrauch.

Vorbemerkung
Wer wir sind:

Mindbase ist ein netzpolitischer Thinktank und eine Beratungsagentur. Ihr Geschäftsführer Stefan Herwig befasste sich im Rahmen seines kommunikationswissenschaftlichen Studiums seit 2007 wissenschaftlich mit netzpolitischen Problemstellungen wie Datenschutz, Providerhaftung, Netzökonomie und Urheberrecht. Er publizierte Ende 2012 wissenschaftlich zu dem Anhörungsthema: *Zur Austarierung von Anonymität und Verantwortung im Netz* (Zeitung für Datenschutz (ZD) 12/2012, C.H. Beck Verlag). Die Erkenntnisse aus seiner wissenschaftlichen Arbeit sind Grundlage für das hier vorgestellte Haftungskonzept.

Bei der Ausarbeitung dieser Eingabe wurde Mindbase juristisch durch Dr. Christian Volkmann beraten. Dr. Volkmann ist Rechtsanwalt mit Sitz in Berlin. Er ist Fachanwalt für Gewerblichen Rechtschutz, E-Commerce, Recht der neuen Medien (Internetrecht) und Urheberrecht. Er veröffentlichte seit 2002 über 40 Fachaufsätze zum Thema Providerhaftung. Curriculum Vitae: http://www.advokat.de/anwaelte/dr-christian-volkmann/

Vorbemerkung:
Austarierung von Anonymität und Verantwortung

Im Rahmen der Anhörung zur TMG-Novelle geht es um die Austarierung von verschiedenen Interessen zur Ermöglichung eines rechtssicheren Handelns der Beteiligten im digitalen Raum. Hierzu gehören diverse Providerbetreiber (Access-, Host-, Content-, WLAN-, und Serverprovider), deren direkte Nutzer (sowohl kommerzielle als auch privat operierende), sowie auch von deren Kommunikationsinhalten betroffene Dritte. Hierzu, also zu den „Dritten", gehören insbesondere Rechteinhaber, Urheber und Kreativwirtschaftsbranchen, aber auch Privatpersonen, über die kommuniziert wird und über die persönlichkeitsrechtsrelevante Äußerungen getätigt werden, als auch besonders schutzbedürftige Dritte wie Kinder und Jugendliche. Es gehören zu den „Dritten" Endnutzer, deren Daten im öffentlichen Raum verletzt und offengelegt werden, aber auch Opfer einer stetig steigenden Zahl an Cybercrime-Verbrechen durch Abomodelle, sogennante Scam- und Scareware, Phishing-Opfer, deren Konto-, Login- und Kreditkarteninformationen durch spezielle Phishingseiten ausgespäht werden oder deren Rechner durch Schadsoftware infiziert werden und die in Folge Teil von sog. Botnetzen werden, mit denen wiederum Spamversendung und DDos Attacken begangen werden. Eine angemessene Justierung der Providerhaftung birgt unserer Meinung nach das Potential, *allen* obengenannten Rechtsverstößen spürbar entgegenzuwirken.

Im Rahmen der hier gegenständlichen TMG-Novelle soll jedoch lediglich die Providerverantwortung für Urheberrechtsverletzungen präzisiert werden, sowie die Verantwortlichkeiten für WLAN-Betreiber konkretisiert werden. Wir rügen, dass durch dieses zu eng gesteckte Ziel, also die Konzentration auf lediglich urheberrechtsverletzende Seiten, angrenzende, ähnlich dringende Probleme, wie Persönlichkeitsrechtsverletzungen, Unterlaufen des Jugendmedienschutzes oder Cybercrime-Aktvitäten wie Phishing, und Malware-Distribution aus dem Fokus fallen könnten. Insofern droht die TMG-Novelle aufgrund ihres zu eng gesteckten Ziels wiederum nur Stückwerk zu werden.

Die Verfasser haben uns im Rahmen dieser Eingabe darum bemüht, nicht nur die durch Urheberrechtsverletzung erzeugten Problemstellungen zu begegnen, sondern sich ebenfalls auch anderen, darüber hinaus gehenden Problemstellungen durch Justierung der Providerhaftung ebenfalls zu minimieren.

Darüber hinaus rügen wir, dass durch die Überarbeitung der WLAN Haftung im Rahmen der Novelle neue Räume zur Verantwortungsdiffusion entstehen können, die einer holistischen Justierung der der Providerhaftung wiederum entgegenwirken. Hiermit droht sich der Geburtsfehler des gesamten dysfunktionalen Haftungssystems im TMG zu wiederholen: um die Wettbewerbsfähigkeit von Plattformbetreibern (in diesem Falle öffentlichen WLANs) zu ermöglichen, wird sowohl die Möglichkeit einer effektiven Rechtsdurchsetzung geschwächt, als auch das Schadenspotential dieser Plattformen auf Dritte nicht hinreichend gewürdigt. Darüber hinaus wird nicht berücksichtigt, dass nicht nur rechtsverletzende Nutzer in freien WLANs Schadenspotential erzeugen, sondern auch, dass betrügerische WLAN-Betreiber umfangreiche Missbrauchsmöglichkeiten für Nutzer haben, die in ihrem WLAN registriert sind. Auch hier drohen neue Räume für Verantwortungsdiffusion zu entstehen.

Im Rahmen der Beabsichtigung einer liberalisierten Haftung von WLAN-Betreibern wird häufig auch auf das Ausland verwiesen, indem eine Verantwortlichkeit nicht notwendig erscheint. Es wird jedoch häufig ignoriert, dass gerade diese Länder häufig eine

Vorratsdatenspeicherung implementiert haben, die dem Haftungsvakuum auf WLAN-Ebene entgegensteht.

Im Rahmen unserer Eingabe versuchen wir ein stringentes Providerhaftungskonzept auszuformulieren, welches der Gesamtheit der Problemstellungen begegnet. Es ist den Verfassern bekannt, dass für eine sinnvolle Anpassung des Providerhaftungsregimes eine lediglich bundesdeutsche TMG-Novelle mittelfristig nicht ausreicht, sondern dass ein wirksames Haftungsregime auch eine Anpassung der E-Commerce-Richtlinie auf europäischer Ebene und langfristig idealerweise auch eine weitergehende Harmonisierung der Rechtsprechung erfordern wird.

Teil I
Problemstellung und Ziel

Seit den frühen 2000er Jahren versucht die Rechtsprechung in Deutschland und in der Europäischen Union die Providerhaftung zu konkretisieren und einen verlässlichen und austarierten Rechtsrahmen zu schaffen. Die Versuche dürfen als gescheitert angesehen werden. Folge sind Rechtsunsicherheiten und kaum beherrschbare Haftungsrisiken auf Seiten der Provider und eklatante Rechtsschutzlücken auf Seiten der Rechteinhaber. Das Ziel dieser Eingabe ist es, die strukturellen Probleme der Gesetzeslage darzustellen, und konstruktive Vorschläge zu formulieren, wie dieser Fehlentwicklung entgegengewirkt werden kann.

1. Die Providerhaftung nach der aktuellen Rechtslage

Grund für die unbefriedigende Entwicklung sind die widerstreitenden Abwägungskriterien im Koordinatensystem der auf die Providerhaftung anwendbaren Regelungen. Da sind einerseits die schützenswerten Interessen der Inhaber von Rechten, die in den allgemeinen nationalen Gesetzen (UrhG, MarkenG, BGB) aber auch in der Urheberrechtsrichtlinie sowie der Enforcementrichtlinie der EU geregelt sind. Andererseits sind da die ebenfalls schützenswerten Interessen der Provider, die nach der E-Commerce-Richtlinie und dem TMG zu berücksichtigen sind.

Die abzuwägenden Interessen stehen sich seit Jahren nahezu unverändert gegenüber und haben in der deutschen und internationalen Rechtsprechung eine Einzelfallkasuistik hervorgebracht, die weit von einem rechtssicheren Haftungsrahmen bzw. einer den rechtsstaatlichen Anforderungen genügenden Rechtsdurchsetzung entfernt ist. Dies gilt insbesondere für Provider, die Inhalte für Dritte speichern („Host-Provider"), für Provider, die ihren Kunden den Zugang zum Netz vermitteln („Access-Provider") sowie für die Rechteinhaber. Bei den Access-Providern zeigt sich exemplarisch die ganze Hilflosigkeit der Rechtsprechung, wenn der EuGH in der Entscheidung vom 27.03.2014 - C-314/12 - UPC Telekabel Wien / Constantin Film Verleih im Leitsatz folgendes formuliert:

> *„Die durch das Unionsrecht anerkannten Grundrechte sind dahin auszulegen, dass sie einer gerichtlichen Anordnung nicht entgegenstehen, mit der einem Anbieter von Internetzugangsdiensten verboten wird, seinen Kunden den Zugang zu einer Website zu ermöglichen, auf der ohne Zustimmung der Rechtsinhaber Schutzgegenstände online zugänglich gemacht werden, wenn die Anordnung keine Angaben dazu enthält, welche Maßnahmen dieser Anbieter ergreifen muss, und wenn er Beugestrafen wegen eines Verstoßes gegen die Anordnung durch den Nachweis abwenden kann, dass er alle zumutbaren Maßnahmen ergriffen hat; dies setzt allerdings voraus, dass die ergriffenen Maßnahmen zum einen den Internetnutzern nicht unnötig die Möglichkeit vorenthalten, in rechtmäßiger Weise*

Zugang zu den verfügbaren Informationen zu erlangen, und zum anderen bewirken, dass unerlaubte Zugriffe auf die Schutzgegenstände verhindert oder zumindest erschwert werden und dass die Internetnutzer, die die Dienste des Adressaten der Anordnung in Anspruch nehmen, zuverlässig davon abgehalten werden, auf die ihnen unter Verletzung des Rechts des geistigen Eigentums zugänglich gemachten Schutzgegenstände zuzugreifen, was die nationalen Behörden und Gerichte zu prüfen haben."

Der EuGH schreibt in diesem Leitsatz nur auf, was die Gesetzeslage ihm vorgibt, und versucht diese mit einer Austarierung der Interessen in Einklang zu bringen. Weniger präzise und rechtssicher geht es allerdings kaum mehr. Wer welche Pflichten bei welcher Art der Rechtsverletzung und welcher Art der konkreten Ausgestaltung eines Dienste, der alle möglichen entscheidungsrelevanten Facetten aufweisen kann, haben soll, entscheiden die Gerichte über mehrere Instanzen zumeist anhand von allgemeinen Gerechtigkeitserwägungen. Dies geht so weit, dass in Bezug auf ein und denselben Dienst in einer Entscheidung „gesteigerte Prüfungspflichten" angenommen wurden (BGH, Urteil v. 15.08.2013 - I ZR 80/12 (Rn. 36) – File-Hosting-Dienst) mit weitreichenden Pflichten zur Verhinderung von Rechtsverletzungen und in einer anderen Entscheidung nur „normale Prüfungspflichten, die das Geschäftsmodell nicht gefährden (BGH, Urteil v. 12.07.2012 – I ZR 18/11 (Rn. 28) – Alone in the Dark). Zum Teil wird die Haftung der Provider von der Erkennbarkeit von Rechtsverstößen abhängig gemacht (BGH, Urteil v. 22.07.2010 – I ZR 139/08 (R. 50) – Kinderhochstühle im Internet I; BGH, Urteil v. 17.08.2011 – I ZR 57/09 (Rn. 28) – Stiftparfüm) oder davon, ob es sich um einen groben Verstoß handelt (s. BGH, Urteil v. 27.10-2011 – I ZR 131/10 (Rn. 30) – regierung-oberfranken.de, in Bezug auf die Haftung der DENIC) oder davon, ob der Anbieter dem Rechteinhaber ein Filtersystem zur Verfügung stellt mit der Möglichkeit, Rechtsverletzungen selbst aufzuspüren (BGH, Urteil v. 22.07.2010 – I ZR 139/08 (Rn. 38) – Kinderhochstühle im Internet I) davon, ob rechtsverletzende Angebote automatisiert beworben werden wie im Beispiel von Google Adwords (BGH, Urteil v. 16.05.2013 – I ZR 216/11 (Rn. 52) – Kinderhochstühle im Internet II) oder davon, ob Anbieter ihren Nutzern ermöglichen, ihre Dienste anonym zu nutzen (BGH, Urteil v. 12.07.2007 – I ZR 18/04 (Rn. 25) – Jugendgefährdende Medien bei eBay; BGH Urteil v. 15.08.2013 - I ZR 80/12 (Rn. 40) – File-Hosting-Dienst).

Rechteinhaber und Provider streiten in jedem Einzelfall erbittert, wessen Interessen überwiegen. Überwiegen die Interessen des Rechteinhabers, ist die Folge in aller Regel eine ganz erhebliche Belastung der haftenden Provider. Denn diese müssen die Rechtsverletzung nicht nur abstellen, sondern sie auch in der Zukunft verhindern, d. h. sie müssen Inhalte zwangsläufig filtern (st. Rspr. des BGH, Urteil v. 11.03.2004 – I ZR 304/01 – Internet-Versteigerung I; BGH, Urteil v. 19.04.2007 – I ZR 35/04 (Rn. 45) – Internet-Versteigerung II; BGH, Urteil v. 30.04.2008 – I ZR 73/05 (Rn. 51) – Internet-Versteigerung III; BGH, Urteil v. 17.08.2011 – I ZR 57/09 (Rn. 21) – Stiftparfüm). Überwiegen demgegenüber die Interessen des Providers, bleibt der Inhalt online; die Rechtsverletzung wird zementiert. Dies bedeutet im Ergebnis, dass die gerichtliche Entscheidung für eine der beiden Parteien untragbar ist.

2. Wirtschaftliche Einbußen durch die aktuelle Gesetzeslage

Die wirtschaftlichen Schäden dieses Systems auf Seiten sowohl der Provider als auch der Rechteinhaber sind eklatant. Rechteinhaber sehen sich einer Rechtslage gegenüber, die es ihnen zum Teil unmöglich macht, illegale Angebote ihres geistigen Eigentums im Netz abzustellen, was mit erheblichen Einbußen im Vertrieb verbunden ist. Es hat sich darüber hinaus in den Haftungslücken der geltenden Rechtsprechung ein Graumarkt von illegalen Services gebildet, die seit Jahren nahezu unbehelligt von der Rechtsprechung existieren können und mittels eines

untauglichen „Notice und Takedown-Verfahrens“ von der Haftungsprivilegierung des TMG und der E-Commerce Richtlinie haftungsprivilegiert werden, während sie gleichzeitig erhebliche Einkünfte durch illegale Distribution, den Verkauf von Premiumaccounts und Online-Anzeigen erzielen.

Demgegenüber fürchten gerade kleinere, wenig finanzstarke Provider ausufernde Prüfungspflichten, die mit erheblichen Kosten einhergehen. Dazu kommt ein nicht verlässlicher Haftungsrahmen, der entweder teure Rechtsstreitigkeiten provoziert oder der zur Vermeidung solcher Rechtsstreitigkeiten zu Überreaktionen auf beiden Seiten führt, nämlich auf Seiten der Rechteinhaber dazu, dass sie von einer Durchsetzung ihrer Rechte von vornherein absehen und auf Seiten gerade der kleineren Provider dazu, dass sie jeden Inhalt ohne Prüfung löschen, wenn dieser von dritter Seite als rechtswidrig moniert wird.

Darüber hinaus wird die Umsetzung neuer Ideen auf diese Weise gehemmt: Ein neuartiger Dienst, eine neuartige Funktionalität auf einer Plattform können ungeahnte Haftungsrisiken auslösen, die Anbieter ggf. nicht einzugehen bereit sind. Dies zeigt die Praxis, in der gerade kleine Anbieter aus Furcht vor der unsicheren Haftungslage im Internet Investitionen scheuen. Umgekehrt kann eine Reduzierung der Haftung durch teure technische Entwicklungen erreicht werden (z. B. durch das VeRi-Programm von eBay, s. BGH, Urteil v. 22.07.2010 – I ZR 139/08 (Rn. 38) – Kinderhochstühle im Internet I), die sich kleinere Provider nicht leisten können, was sie im Wettbewerb zu den großen Anbietern ganz erheblich benachteiligt.

3. Erfordernis der Anpassung der Struktur des TMG

Die Rechteinhaber stehen zudem vor einem besonderen Problem, das strukturell in der E-Commerce-Richtlinie und im TMG angelegt ist. Ein rechtsverletzender Inhalt wird von einer Person (dem eigentlichen Rechtsverletzer) in das Netz eingestellt und über verschiedene Anbieter (Host- und Access-Providern, Rechenzentren, ggf. auch die Suchmaschinen, etc.) gespeichert und verbreitet. Der Rechtsverletzer selbst kann in den meisten Fällen nicht verfolgt werden, weil er gar nicht bekannt ist. Die Provider können sich unter Umständen mit Zumutbarkeitserwägungen von der Haftung befreien. Durch dieses Zusammenspiel der Anonymität bzw. der Nichtgreifbarkeit desjenigen, der eigentlich für den Inhalt verantwortlich ist, und der Nichtverantwortlichkeit der Provider entsteht eine Rechtsschutzlücke. Es entsteht Verantwortungsdiffusion, teils unbeabsichtigt, oder vom TMG selbst induziert (vgl. §13 Abs. 6 TMG), teils von Plattformbetreibern im Graubereich durchaus gewollt und bewusst herbeigeführt.

Privilegiert werden durch dieses System weniger die Provider, sondern vielmehr der eigentliche Rechtsverletzer, der eine Struktur vorfindet, in der er sich anonym bewegen kann und vor der Rechtsdurchsetzung durch verletzte Dritte bewahrt ist. Diese Privilegierung des Rechtsverletzers geht – bei Verantwortungsdiffusion – sogar so weit, dass die Rechtsverletzung nicht einmal abgestellt werden kann: Die Beleidigung, die Verleumdung oder das illegal angebotene Musikstück bleiben im Netz, oder werden immer wieder neu hochgeladen, gepostet oder ausgeführt. Privilegiert werden auch die Rechtsverletzer, die anonym eigene Inhalte auf ihre Plattformen hochladen und auf diese Weise nach außen hin als „zu privilegierende“ Provider erscheinen.

Die uneingeschränkte Zulassung von Anonymität im Netz bei *gleichzeitiger* Verantwortungsdiffusion ist vor dem Hintergrund der im Netz bestehenden Gefährdungslage für Rechtsgüter ein Tatbestand, der in der Offline-Welt unbekannt ist. In allen Bereichen, in denen Anonymität gewährleistet wird, gibt es bei entsprechender Gefahrenlage gleichwohl ein System der Verantwortlichkeit, das es dem Verletzten ermöglicht, sich gegen

Rechtsverletzungen zu wehren. Dies gilt etwa im Presserecht, wo es trotz anonymer Quellen sowohl einen verantwortlichen Redakteur, als auch einen V.i.S.d.P. gibt. Auch in anderen Bereichen, die im weitesten Sinn mit menschlicher Kommunikation und Interaktion zu tun haben, ist eine Verantwortungsdiffusion für Kommunikationsinhalte im öffentlichen Raum weitgehend ausgeschlossen; So ist bei Demonstrationen der – den Behörden bekannte – Versammlungsleiter für die Einhaltung der Rechte und Pflichten der von ihm organisierten Versammlung verantwortlich.

Auch im Rahmen des motorisierten Straßenverkehrs wurde ein austariertes System entwickelt, das Anonymität so weit gewährleistet, bis ein Grad an Gefährlichkeit erreicht ist, der Anonymität nicht mehr zulässt: Während die Fortbewegung zu Fuß oder mit dem Fahrrad so wenig gefährlich ist, dass Anonymität gewährleistet werden kann, gilt dies nicht beim Fahren mit dem Motorrad, dem PKW oder dem LKW: Hier ist über das Kennzeichen der Fahrer – oder eben der Halter - ermittelbar. Bestimmte Gefährdungssituationen in öffentlichen Räumen erfordern daher entweder eine Deanonymisierung (Autokennzeichen) oder aber die Schaffung einer besonderen Verantwortlichkeit (verantwortlicher Redakteur), um Rechtsgüter zu schützen. Die bisherigen Haftungsalgorithmen im Netz weichen jedoch strukturell erheblich von dieser bewährten Haftungslogik ab. Sie kennen keine Risikoabwägung, und repräsentieren die Rechte Dritter nur sehr lückenhaft, weswegen es unerlässlich ist, das Haftungsregime dauerhaft neu aufzusetzen.

4. Vorschlag einer neuen Struktur: Das A/B/C-Konzept

Analog zu den Regelungen in der Offline-Welt muss gerade die Anonymität im Netz bzw. die Zulassung von Anonymität im Netz durch die Provider Grundlage des Haftungssystems sein. Dabei soll die Anonymität im Netz sowie insbesondere auch die Zulassung von Anonymität im Netz nicht prinzipiell unterbunden sondern ermöglicht werden.
Die Anonymität der Nutzer muss dann aber mit einer parallel einhergehenden zu justierenden Verantwortlichkeit der Provider austariert werden. Hierzu erwägen wir einen simplen Algorithmus: Betreiber, die

(A) die Durchleitung oder Speicherung von Inhalten auf Hostproviderebene im Rahmen ihrer Plattform oder ihres Dienstes ermöglichen,
(B) ihre Nutzer anonymisieren, und dann
(C) die Verantwortung für die Inhalte dieser Nutzer ablehnen,

erzeugen Verantwortungsdiffusion in öffentlichen Räumen.

Es gilt also zunächst, die Kombination von (A), (B) & (C) zu verhindern. Die logische Schlussfolgerung ist es, auf dieser Ebene Dienste zuzulassen, die entweder nur die Kombination von (A) und (B) zulassen, oder die Kombination von (A) und (C). Auch die Kombination von (B) und (C) ist möglich, dies wäre aber dann kein Dienst mehr, der für Kommunikation in öffentlichen Räumen auf Hostproviderebene fungieren würde, und insofern für unsere Problemstellung kaum relevant.

Tendenzen, die de lege lata in die Richtung gehen, die Ermöglichung von Anonymität jedenfalls als Abwägungskriterium stärker mit zu berücksichtigen, kommen bereits aus der Rechtsprechung (BGH, Urteil v. 15.08.2013 - I ZR 80/12 (Rn. 40) – File-Hosting-Dienst) sowie auch aus der Kommentarliteratur (Spindler/Volkmann, in: Spindler/Schuster Recht der elektronischen Medien, 3. Auflage, 2015, § 1004 BGB, R. 25). Die bloße Berücksichtigung der Ermöglichung von Anonymität als Abwägungskriterium bei der Frage der Zumutbarkeit von Prüfungspflichten, geht nach dem hiesigen Ansatz aber nicht weit genug, da

Rechtsschutzlücken verbleiben und eine Rechtssicherheit der Provider ebenfalls nicht hergestellt werden kann.

Nutzer, die sich durch die Rechtswahl ihres Wohn- oder Geschäftssitzes der Verantwortlichkeit innerhalb der Europäischen Union entziehen, werden wie anonyme Nutzer gewertet. Sie sind daher entsprechend mit in die Haftungsarithmetik des A/B/C-Konzeptes einzubeziehen.

Teil II.
Gesetzesentwurf mit Änderungen und Erläuterungen

Die Haftung der Diensteanbieter im Internet ist Gegenstand des Koalitionsvertrages. Die Bundesregierung hat ausgemacht, dass die stärkere Verantwortlichkeit von Diensteanbietern einen wesentlichen Beitrag zum Schutz der Verbraucher und zur Eindämmung von massenhaften Rechtsverletzungen im Internet leisten kann. Dies gilt in besonderem Maße für die Host-Provider. Hier sieht der Koalitionsvertrag die Verbesserung der Rechtsdurchsetzung insbesondere gegenüber Plattformen vor, deren Geschäftsmodell im Wesentlichen auf der Verletzung von Urheberrechten aufbaut.

Wir sind davon überzeugt, dass eine punktuelle Verschärfung der Haftung die Probleme der in ihren Rechten Verletzten dauerhaft nicht löst. Entscheidend ist es, den Rechtsverletzer greifbar zu machen, und die Rechtsverletzung abzustellen. Erst wenn ein Rechtsverletzer nicht gefunden/ermittelt werden kann, sollte erwogen werden, ob andere Beteiligte in die Haftung mit einbezogen werden können. Wir schlagen daher folgende Änderungen des derzeit geltenden TMG vor:

Mit den nachstehenden Regelungen wird die Haftung der Host-Provider auf Beseitigung und Unterlassen nach den allgemeinen Regelungen, d. h. insbesondere auch die Störerhaftung, in die Haftungsprivilegierungen des TMG ausdrücklich mit eingebunden. Die Haftungsprivilegierung wird allerdings davon abhängig gemacht, dass der eigentliche Rechtsverletzer der Rechtsverletzung für den Verletzten greifbar ist. Ist der Rechtsverletzer greifbar, wird der Provider von der Haftung auf Unterlassen befreit. Er ist lediglich verpflichtet, den rechtsverletzenden Inhalt zu löschen. Ist der Rechtsverletzer demgegenüber nicht greifbar, soll es eine uneingeschränkte Haftung des Host-Providers auf Beseitigung und Unterlassen geben.

Ausdrücklich einbezogen wird zudem eine Haftung der Rechenzentren, die rechtswidrigen Diensten Speicherplatz zur Verfügung stellen. Diese sollen sich ebenfalls nur auf eine Haftungsprivilegierung berufen können, wenn sie durch Preisgabe der Betreiber der illegalen Dienste an der Verhinderung von Rechtsverletzungen mitwirken.

Wir schlagen folgende Änderungen im Gesetzestext (Änderungen in Fettdruck) vor:

> *§ 10 Speicherung von Informationen*
> ***(1)*** *Diensteanbieter sind für fremde Informationen, die sie für einen Nutzer speichern, nicht verantwortlich, sofern*
>
> *1.*
> *sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben und ihnen im Falle von Schadensersatzansprüchen auch keine*

Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, oder
2.
sie unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie diese Kenntnis erlangt haben.
Satz 1 findet keine Anwendung, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.
(2) Diensteanbieter sind, wenn nicht der Nutzer bereits wiederholt Rechtsverletzungen über den Dienst des Diensteanbieters begangen hat, nur dann verpflichtet, eine Rechtsverletzung durch eine fremde Information, die sie für einen Nutzer speichern, nach den allgemeinen Gesetze zu verhindern,

a) wenn sie den Namen und die Anschrift des Nutzers, für den die Information gespeichert wird, nicht gespeichert und nach dem aktuellen Stand der Technik verifiziert haben oder sie dem Verletzten diese Daten nicht unverzüglich auf dessen Anforderung übermitteln, oder
b) wenn der Nutzer, für den die Information gespeichert wird, seinen Wohn- oder Geschäftssitz außerhalb des räumlichen Geltungsbereichs der Richtlinie 2000/31/EG hat

Die Verpflichtung des Diensteanbieters, die Rechtsverletzung abzustellen bleibt hiervon unberührt.

(3) Speichert der Diensteanbieter fremde Informationen für einen anderen Diensteanbieter, gilt Absatz 2 entsprechend.

Teil III.
Begründung

1. Erläuterungen der Regelungen

Die Klarstellung der Verantwortlichkeit der Host-Provider nach § 10 Abs. 2 setzt Artikel 14 Abs. 3 der Richtlinie 2000/31 um, der Möglichkeiten vorsieht, auch Host-Provider für das Abstellen und die Verhinderung von Rechtsverletzungen haftbar zu machen. Die Regelung sieht die Host-Provider nach Satz 2 zunächst grundsätzlich in der Verpflichtung, Rechtsverstöße durch Löschung von Inhalten abzustellen („take down“). Art. 11 S. 3 der Richtlinie 2004/48 (Enforcement-Richtlinie) und Art. 8 Abs. 3 der Richtlinie 2001/29 (Info-Richtlinie) stehen den Änderungen nicht entgegen, da mit der Verpflichtung des Host-Providers, die Rechtsverletzung abzustellen, gerichtliche Anordnungen gegen Vermittler möglich bleiben.

Weitergehende Pflichten sieht § 10 Abs. 2 die Regelung dann vor, wenn der Diensteanbieter eine anonyme Nutzung seines Dienstes zulässt und dadurch die Rechtsverfolgung von Rechtsverstößen durch den Verletzten unmöglich macht. In diesem Fall ist der Diensteanbieter verpflichtet, Rechtsverletzungen durch diese anonym handelnden Nutzer abzustellen und zu verhindern („take down“ and „stay down“). Er haftet dann nach den allgemeinen Gesetzen auf Unterlassung. Zentrales Kriterium sind die „Identifizierung“ des Nutzers. Ist der Nutzer identifiziert und seine Identität verifiziert, kann der Verletzte gegen ihn vorgehen; er braucht nicht die uneingeschränkte Haftung des Host-Providers. Ist der Nutzer nicht identifiziert aber ist der Host-Provider in der Lage, dem Verletzten die erforderlichen Daten des Nutzers herauszugeben, und tut er dies auch, ist ebenfalls keine uneingeschränkte Haftung des Providers

erforderlich. Ist der Nutzer aber nicht identifiziert bzw. identifizierbar, d. h. anonym und kann oder will der Provider die Daten nicht herausgeben, muss er weitergehende Pflichten übernehmen, um die Rechtsgüter des Verletzten zu wahren. Da der Host-Provider Namen und Anschrift des Nutzers nur im Fall einer Rechtsverletzung und dann nur gegenüber dem Verletzten preisgeben muss, wenn er die Haftungsprivilegierung erlangen möchte, kann der Nutzer für die Öffentlichkeit pseudonym bleiben, d. h. er ist gegenüber der Öffentlichkeit nicht identifziert. Erfolgt eine Identifizierung des Nutzers, muss diese allerdings verifiziert sein, d.h. es muss gewährleistet sein, dass sich ein Nutzer nicht hinter einer falschen Angabe oder einem falschen Impressum versteckt.

Ein datenschutzrechtliches Problem ist nicht erkennbar. § 13 Abs. 6 TMG erfordert die anonyme oder pseudonyme Nutzung des Dienstes, jedoch bezieht sich die Pflicht ausschließlich auf die Nutzung des Dienstes selbst. Der Diensteanbieter ist nicht verpflichtet, den Vertragsschluss anonym oder pseudonym zu ermöglichen (Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage, 2015, § 13 Rn. 22; Härting, NJW 2013, 2065 (2067). Will der Diensteanbieter von der Haftungsprivilegierung profitieren, kann er im Einklang mit § 13 Abs. 6 TMG die pseudonyme Nutzung zulassen. Eine datenschutzrechtliche Evaluation ist gleichwohl erforderlich, gerade im Hinblick auf die Herausgabe der Daten des Rechtsverletzers an den Verletzten zum Zwecke der Rechtsverfolgung. Hier könnte im Hinblick auf § 12 Abs. 2 TMG Regelungsbedarf bestehen.

Gleiches gilt, wenn der Nutzer zwar nicht anonym handelt, aber der Diensteanbieter die zur Verfolgung des Rechtsverstoßes gegen den Nutzers erforderlichen Daten nicht herausgibt oder wenn der Nutzer aufgrund seines Wohn- oder Geschäftssitzes für den Verletzten nicht greifbar ist. Auch hier ist der Diensteanbieter nicht nur verpflichtet, die Rechtsverletzung abzustellen. Er muss darüber hinaus den Rechtsverletzung zukünftig verhindern.

§ 10 Abs. 3 regelt die Verantwortlichkeit der Anbieter, die Host-Providern Speicherplatz zur Verfügung stellen. Dies sind in aller Regel Rechenzentren. Deren Identität ist in vielen Fällen, in denen Ansprüche gegen illegale Dienste (z. B. „kino.to“) durchzusetzen sind, durch eine sogenannte “Trace-Route“-Abfrage bekannt. Unbekannt sind jedoch oft die einzelnen Diensteanbieter, die Speicherplatz bei den Rechenzentren gemietet haben, und diesen für die Bereithaltung von rechtswidrigen Informationen oder illegalen Diensten nutzen. Gibt sich der rechtswidrig handelnde Dienst nicht erkennbar oder nur unter einer Anschrift, die eine zivilrechtliche Verfolgung unmöglich macht oder erheblich erschwert, ist das Rechenzentrum verpflichtet, die Daten herauszugeben, wenn es von der Haftungsprivilegierung profitieren möchte. Anderenfalls muss es den Dienst sperren bzw. die Inhalte löschen, da er in diesem Fall – ohne Privilegierung – dem Unterlassungsanspruch nach den allgemeinen Gesetzen ausgesetzt ist. Hierbei gilt es anzufügen, dass Rechenzentren teils erheblich von Angeboten im Graubereich profitieren.

(Wir verweisen hier explizit auf das Dossier von Volker Rieck und Stefan Herwig erschienen am 27.02. in der Musikwoche, Entertainment Media Verlag, Ausgabe Nr. 10, http://www.mediabiz.de/musik/news/serverprovider-report-ich-hab-noch-einen-server-in-berlin/391398. (Ein .pdf des Textes hängt der Eingabe an)).

2. Zielsetzung und Notwendigkeit der Regelungen

Ziel des Vorschlags ist es, Rechtsverletzungen im Internet abzustellen, ohne gleichzeitig die Provider über Gebühr zu belasten. Es soll ein Haftungsrahmen entstehen, der allen Beteiligten von Online-Kommunikationsvorgängen zumutbare Prüfpflichten auferlegt. Hierbei ist

insbesondere der internationale Charakter von Online-Kommunikationsvorgängen zu berücksichtigen, indem sich auch weiterhin nicht alle Rechtsverletzer mit verhältnismäßigen Mitteln ausfindig machen lassen können. Es kann aber einer strukturell statischen Verantwortungsdiffusion wirksam entgegengewirkt werden Darüber hinaus sollte es Host-Providern weiterhin unbenommen bleiben, eine anonyme Nutzung ihrer Dienste zuzulassen. In diesem Fall sollen sie aber gesteigerte Pflichten übernehmen.

Eine Beibehaltung der derzeitigen Rechtssituation mit Haftungslücken bei Anonymität und Nichtgreifbarkeit des eigentlichen Verursachers der Rechtsverletzung ist für alle Beteiligten unserer Ansicht nach unzumutbar.

3. Folgen des Gesetzes

a) Erfüllungsaufwand
Nutzer müssen bei der Veröffentlichung von Inhalten im Internet auf Hostproviderplattformen ihre Identifizierbarkeit durch den Hostprovider in vielen Fällen ermöglichen. Für die Öffentlichkeit bleibt der Nutzer weiterhin pseudonym.

Die Wirtschaft muss den Nutzern entsprechende Identifikationsmechanismen anbieten. Sie kann aber auf vielfache bestehende Strukturen und Angebote (exemplarisch: Paypal-Account, KlarNa, Microsoft.net Passport, Post-Ident-Verfahren, etc. zurückgreifen). Zur Vermeidung von „Chilling Effects“ könnte der Schlüssel zur Identifikation, insbesondere bei zukünftigen Identifikationsdiensten auch getrennt bei einem Dritten hinterlegt werden. Die Daten könnten mit sog. Hashwerten indexiert und aufgetrennt werden, wie es zum Teil bei Cookies und in der Werbung der Fall ist.

b) Auswirkungen auf die Provider
Die Provider werden durch den hier verfolgten Ansatz ganz erheblich entlastet. Denn sie können – wenn sie die pseudonyme Nutzung ihrer Dienste zur Bedingung machen – die Pflicht vermeiden, Rechtsverletzungen in der Zukunft zu verhindern. Die Pflicht zur Verhinderung der Rechtsverletzung wird auf diese Weise dem Rechtsverletzer derselben übertragen. Die Pflicht, Rechtsverletzungen abzustellen, indem Inhalte gelöscht werden, erfordert eine Auseinandersetzung mit dem Inhalt, aber keine Filterung der Plattformen auf identische oder ähnliche Inhalte. Die Provider profitieren daher von einer erheblichen Haftungserleichterung, wenn sie zumindest gewährleisten, dass die Nutzer identifiziert werden können und die Daten auch an die Verletzten herausgeben werden. Nach außen sind die Nutzer wirksam pseudonymisiert.

Der Aufwand der Provider wird aus einem weiteren Grund sinken. Denn der Ansatz wirkt selbstregulierend. Provider, die Anonymität nicht mehr zulassen bzw. eine Identifikation der Nutzer gewährleisten, schaffen signifikant weniger Anreize für Nutzer, Rechtsverletzungen über ihre Plattformen zu begehen, und erhöhen damit in Folge das Risiko für Rechtsverletzungen ihrer Nutzer. Nutzer, die wissen, dass sie über den Hostprovider einer Dienstleistung pseudonymisiert sind, aber im Zweifelsfalle zur Verantwortung gezogen können, werden sich anders verhalten, als Nutzer, die anonymisiert sind.

c) Auswirkungen auf die Rechteinhaber
Die Rechteinhaber haben nicht mehr unter der derzeit vorherrschenden Verantwortungsdiffusion zu leiden. Sie können entweder dem Rechtsverletzer auferlegen, Verletzungen ihrer Rechte in Zukunft zu unterlassen, oder – wenn der Provider die Identität des

Rechtsverletzers nicht preisgeben kann oder möchte – den Provider. Rechteinhaber sind dadurch in der Lage, ihre Rechte im Netz durchzusetzen. Strukturellen Rechtsverletzungen kann in jedem Falle entgegengewirkt werden.

Teil IV
Ausblick

Die hier vorgeschlagenen Regelungen stellen einen ersten Schritt dar, der unseres Erachtens im Rahmen der beabsichtigten TMG-Novelle realisierbar ist. In einem weiteren Schritt sind Präzisierungen der Vermittlerhaftung nach unserem Ansatz auf der Ebene der EU wünschenswert, insbesondere im Hinblick auf Art. 11 S. 3 der Richtlinie 2004/48 (Enforcement-Richtlinie) und Art. 8 Abs. 3 der Richtlinie 2001/29 (Info-Richtlinie).

Das Konzept, die Rechtsdurchsetzungsdefizite über den Punkt Providerhaftung zu schließen, ist damit jedoch noch lange nicht ausgereizt. Nicht nur sollte ein stringentes Providerhaftungskonzept mittelfristig auch europaweit über eine Öffnung der E-Commerce Richtlinie harmonisiert werden, es sollten auch weiterhin andere Providerebenen im Netz mit in diese Haftungslogik einbezogen werden, um eine Anonymisierung insbesondere kommerzieller Plattformen auch auf Ebene der Domainregistrare auszuschließen. Auch muss die Rolle sogenannter Anonymisierungsdienste kritisch hinterfragt werden.

Hierzu zählen wir unter anderem eine erweiterte Registrationspflicht für Plattformbetreiber, erweiterte Sanktionen gegen Registrarbetreiber, bis hin zur ICANN. Es ist essentiell, dass die Haftungslogik der verschiedenen Providerebenen sinnvoll ineinandergreift, und des Weiteren international harmonisiert wurde. Eine gute Analogie zu diesem Haftungsregime ist die Verantwortlichkeit im Straßenverkehr, in der auch Haftungen verschiedenster Ebenen, vom Fahrer, über den Halter, über den Automobilhersteller, den Betreiber von Verkehrsinfrastrukturen bis hin zu den Betreibern von Autovermietungen abgedichtet wurden. Das System ist ebenfalls daraufhin optimiert, dass die Verantwortlichkeit für Verstöße bestmöglich loziert werden kann, ohne die Anonymität einzelner Verkehrsteilnehmer unnötig aufzulösen. Ähnliches sollte bei der Ausgestaltung des Providerhaftungsregimes geschehen. Eine stringente Zuweisung von Verantwortlichkeit für Rechtsverstöße sollte Priorität bei der Ausgestaltung haben, und strukturelle Verantwortungsdiffusion für Inhalte und Plattformen sollte so minimiert werden, um Schaden für Dritte auszuschließen. Zusätzlich steht die Zumutbarkeit der Haftungsregeln für die Beteiligten im Fokus. Die Wettbewerbsfähigkeit von deutschen oder europäischen Telemedienbetreibern darf einer stringenten Rechtsdurchsetzung nicht übergeordnet werden, wie es bei der vergangenen Ausgestaltung des TMG der Fall war. Wir sind der Meinung, dass mit dem hier vorgeschlagenen Konzept ein bestmöglicher Kompromiss zwischen einem hohen Rechtsdurchsetzungsstandard einerseits und einer hohen Zumutbarkeit für die Beteiligten Verkehrskreise andererseits erreicht zu haben.

Die letzten Entscheidungen des EuGH zur Haftung der Access-Provider zeigen, dass auch diese in die Haftungsarithmetik mit einzubeziehen sind. Dies gilt auch nach dem A/B/C Konzept
. Denn Verantwortungsdiffusion findet auch statt, wenn der eigentliche Rechtsverletzer und der Host-Provider gleichzeitig nicht greifbar sind. Netzsperren sollen allerdings auch erst dann eingesetzt werden dürfen, wenn der Verletzte keine zeitnahe Möglichkeit hat, die Verletzung anderweitig abzustellen, etwa indem er an den ihm bekannten und greifbaren Nutzer oder den ihm bekannten und greifbaren Host-Provider herantreten kann. Die Haftung der Access-Provider sollte daher subsidiär zur Haftung der Host-Provider und der eigentlichen Rechtsverletzer sein. Access-Provider sollten nur dann herangezogen werden können, wenn

Rechtsverletzer und Host-Provider durch Anonymisierung nicht greifbar sind. Als Maßnahme kommt lediglich die Sperrung des Dienstes in Betracht.

Damit ist das Konzept der Steuerung von Providerhaftung aber noch nicht zu Ende gedacht. Wir glauben, dass bei einer optimalen Ausbalancierung dieser Haftungslogik über alle Ebenen der Provider damit sogar flächendeckenden Deanonymisierungskonzepten wie z. B. die Vorratsdatenspeicherung mittelfristig überflüssig gemacht werden können, ohne übermäßige Einschnitte in die Privatsphäre, den Datenschutz oder hohe Beeinträchtigungen des Niveaus der Rechtsdurchsetzung hinnehmen zu müssen. Alleine aufgrund dieses Ausblickes sollte man dem Haftungskonzept größtmögliche Beachtung widmen.

Die Weiterführung des A/B/C-Konzeptes kann de lege ferenda also eine Vielzahl von Problemen aus den immer mehr zunehmenden Rechtsverletzungen im Internet bewältigen, die zu enormen wirtschaftlichen Schäden führen. Die sinnvolle Austarierung von Anonymität mit einhergehender Haftungsabwägung hat so starke selbstregulatorische Effekte, dass nicht nur Verletzungen durch Informationen im Netz zurückgehen werden. Auch Phänomene wie Phishing-Emails, Scam- und Scareware oder sogar der Spamversand profitieren davon, dass die Anbieter, über die diese Rechtsverletzungen und Straftaten stattfinden, zwar öffentlich, die Täter aber wirksam anonymisiert sind. Eine minimalinvasive Auflösung dieser Anonymisierung und der damit entstehenden Verantwortungsdiffusion ist der zwingende Schritt zu einer nachhaltigen Rechtssicherheit für die Beteiligten.

Für Rückfragen:

Mindbase Strategic Consulting
Stefan Herwig
Horster Straße 31
45897 Gelsenkirchen
Tel: 0209 38 650 670
Fax: 0209 38 650 668
sherwig@mindbasesc.de
www.mindbasesc.de