Aktuelle Fragen der strafrechtlichen Providerhaftung

insbesondere zur Haftung des Access-Providers

Inaugural-Dissertation

zur Erlangung der Würde eines
doctor iuris
der Juristischen Fakultät
der Bayerischen Julius-Maximilians-Universität
Würzburg

vorgelegt von

Michael Jan Werner Götze
aus Amberg

2015

Erstgutachter: Prof. Dr. Dr. Eric Hilgendorf
Zweitgutachter: Prof. Dr. Frank Peter Schuster
Dekan: Prof. Dr. Eckhard Pache
Tag der mündlichen Prüfung: 26.07.2017

Für Sabine und Reyli

Vorwort

Die vorliegende Dissertation wurde im Wintersemester 2015/2016 von der Juristischen Fakultät der Julius-Maximilians-Universität Würzburg als Dissertation angenommen. Die mündliche Prüfung fand am 26. Juli 2017 statt. Die Endfassung wurde im September 2015 fertiggestellt und berücksichtigt die bis zu diesem Zeitpunkt verabschiedete Gesetzgebung, erschienene Literatur sowie veröffentlichte Rechtsprechung.

Die Entstehung dieser Dissertation haben viele Personen gefördert, bei denen ich mich herzlich bedanken möchte. Dies gilt zuerst für meinen Doktorvater Herrn Prof. Dr. Dr. Eric Hilgendorf, dem ich für so vieles danke – für seinen interessanten Themenvorschlag, für seine Geduld während der Bearbeitungszeit und letztlich und vor allem für seine stete fachliche Unterstützung bei der Umsetzung des Vorhabens. Herrn Prof. Dr. Frank Schuster danke ich für die zeitnahe Erstellung eines ebenso detaillierten wie konstruktiven Zweitgutachtens.

Für die Durchsicht des Manuskripts bedanke ich mich im Besonderen bei meinen guten Freunden Herrn Prof. Dr. Brian Valerius und Herrn Andreas Zeller sowie meinem Vater, Herrn Studiendirektor a.D. Wolfgang Götze.

Mein größter Dank gilt allerdings Frau Sabine Stahl, der diese Arbeit auch gewidmet ist. Sie hat mich immer inspiriert, beflügelt und in meinem Tun ermutigt. Ihre zahlreichen Anmerkungen waren stets hilfreich. Herzlichen Dank.

Herrlingen, im November 2017 *Michael Götze*

Inhaltsübersicht

Teil 3: Haftung des Access-Providers

Teil 4: Gesamtergebnis der Arbeit und Ausblick

Inhaltsverzeichnis

Abkürzungsverzeichnis

a.A.	anderer Ansicht
a.a.O.	am angegebenen Ort
ABl. EG	Amtsblatt der Europäischen Gemeinschaften
Abs.	Absatz
a.E.	am Ende
AG	Amtsgericht
Art.	Artikel
AT	Allgemeiner Teil
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Sammlung der Entscheidungen des Bundesgerichtshofs in Strafsachen
BGHZ	Sammlung der Entscheidungen des Bundesgerichtshofs in Zivilsachen
BR-Drs.	Bundesratsdrucksache
bspw.	beispielsweise
BT	Besonderer Teil
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Sammlung der Entscheidungen des Bundesverfassungsgerichts
bzw.	beziehungsweise
CR	Computer und Recht
d.h.	das heißt
ECRL	Richtlinie über den elektronischen Geschäftsverkehr (E- Commerce-Richtlinie)
ECG	E-Commerce-Gesetz, Österreich
EG	Europäische Gemeinschaft
EGG	Elektronischer Geschäftsverkehr-Gesetz
ElGVG	Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz
etc.	et cetera

EU	Europäische Union
EuGH	Europäischer Gerichtshof
f.	folgende
ff.	fortfolgende
Fn.	Fußnote
GG	Grundgesetz
ggf.	gegebenenfalls
GrS	Großer Senat für Strafsachen
HADOPI	Haute Autorité pour la diffusion des oeuvres et la protection des droits sur l'Internet
Hrsg.	Herausgeber
IaaS	Infrastructure-as-a-Service
IuKDG	Informations- und Kommunikationsdienstegesetz
i.V.m.	in Verbindung mit
JA	Juristische Arbeitsblätter
JMStV	Jugendmedienschutz-Staatsvertrag
Jura	Juristische Ausbildung
JuS	Juristische Schulung
JuSchG	Jugendschutzgesetz
JZ	Juristenzeitung
K&R	Kommunikation & Recht
Kap.	Kapitel
KG	Kammergericht
KJM	Kommission für Jegendmedienschutz
KOM	Kommission der Europäischen Gemeinschaften
LES	Ley 2/2011, de 4 de marzo, de Economía Sostenible
LG	Landgericht
lit.	litera
LTE	Long Term Evolution
MDStV	Mediendienste-Staatsvertrag
MMR	Multimedia und Recht
m.w.N.	mit weiteren Nachweisen
NJW	Neue Juristische Wochenschrift
NJW-RR	Neue Juristische Wochenschrift – Rechtsprechungs-Report

Nr.	Nummer
Nrn.	Nummern
NStZ	Neue Zeitschrift für Strafrecht
OLG	Oberlandesgericht
PaaS	Platform-as-a-Service
PC	Personal Computer
PKS	Polizeiliche Kriminalstatistik
RGSt	Sammlung der Entscheidungen des Reichsgerichts in Strafsachen
Rn.	Randnummer
RStV	Rundfunkstaatsvertrag; Staatsvertrag für Rundfunk und Telemedien
S.	Seite
SaaS	Software-as-a-Service
sog.	so genannte(r/n)
Std.	Stunden
StGB	Strafgesetzbuch
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
u.a.	und andere
UMTS	Universal Mobile Telecommunications System
UrhG	Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz)
Var.	Variante
VG	Verwaltungsgericht
vgl.	vergleiche
wistra	Zeitschrift für Wirtschafts- und Steuerstrafrecht
WRP	Wettbewerb in Recht und Praxis
z.B.	zum Beispiel
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft
ZugErschwG	Zugangserschwerungsgesetz

Einleitung

Heutzutage wird es immer schwieriger, rechtswidrige Informationen und Handlungen im Internet haftungsrechtlich zu verfolgen und den Täter zur Rechenschaft zu ziehen. Die Täter, aber auch die von Ihnen benutzten Infrastrukturen sind über den Erdball verteilt. Hinzu kommt, dass es technisch versierten Tätern möglich ist, ihre Identität und ihre Lokalität zu verschleiern. Dadurch, aber auch durch die Beschränkung hoheitlicher Befugnisse fällt es u.a. Strafverfolgungsbehörden zunehmend schwerer, ihren originären Aufgaben nachzukommen bzw. zu einem erfolgreichen Abschluss zu führen.

Oftmals einzig greifbare Figur in der Reihe von ineinandergreifenden Zahnrädern ist diejenige des Access-Providers. Host-Provider können ihre Server überall auf der Welt vorhalten und die Content-Provider können die von ihnen erzeugten Inhalte von überall auf der Welt ins Internet einstellen. Als Herr über oder zumindest Bereitsteller des lokalen Internetzugangs jedes Einzelnen, steht er geradezu zwischen Täter und Opfer und erbringt einen Beitrag, der die Verletzung des Opfers begünstigt. Es erscheint daher zweckmäßig zu untersuchen, ob der Access-Provider, der grundsätzlich nicht belangt wird, nicht doch auch einen haftungsrechtlichen Tatbestand erfüllen kann.

Ziel und Zweck dieser folgenden Darstellung ist es, diese Haftungslücke aufzuzeigen und herauszuarbeiten, ob eine strafrechtliche Haftung möglich ist. Dazu wird zunächst einen Überblick über das Haftungssystem der Providerarten geben und anschließend aktuelle Rechtsprechungsentwicklungen auf diesem Gebiet dargestellt. Den Schwerpunkt der Arbeit bildet anschließend die Frage, ob im Lichte der aktuellen technischen Entwicklungen und der heute immer unüberschaubareren Datenflut des Internets eine strafrechtliche Inanspruchnahme auch des Access-Providers rechtlich möglich und sinnvoll ist und welche Regelungen in anderen europäischen Ländern bestehen.

Teil 1: Grundlagen der Providerhaftung

Das Internet, unendliche Weiten, die nie ein Mensch zuvor gesehen hat[1] – dies ist ein nicht ganz korrekt abgewandeltes Zitat, denn das Internet als technische Einheit auf der einen Seite, sowie die darin enthaltenen Inhalte auf der anderen Seite wurden vom Menschen geschaffen. Richtig an dieser Aussage sind lediglich die für einen Einzelnen kaum überschaubaren Weiten und Möglichkeiten des Internets, die viel Positives, aber auch viel Negatives beinhalten.

Das Internet ist aus dem heutigen Alltag sowohl im privaten als auch im geschäftlichen Bereich nicht mehr wegzudenken. Es schafft nicht nur neue Möglichkeiten der Kommunikation unter den Individuen, es ermöglicht auch den reibungslosen Ablauf der Konsumgesellschaft, z.B. im Zahlungsverkehr.

Im privaten Bereich surfen 77% der Deutschen regelmäßig im Internet, das entspricht einer Zahl von ca. 55 Mio. deutschen Internetnutzern. Bei den 14–39jährigen liegt die Zahl bei nahezu 100%. Aber auch die Gruppe der Unter-Sechzigjährigen hat die 90%-Schwelle bereits überschritten. Lediglich die Gruppe der Über-Sechzigjährigen kommt auf einen Anteil von nur knapp 40%.[2]

Derzeit dominieren zwei Schwerpunkte die Fortentwicklung des Internets. Zum einen die immer häufigere Nutzung des Internets im mobilen Bereich. Dies geht einher mit der Zunahme der Zugriffe auf das Internet über Smartphones und Tablet-PCs, die dies ermöglichen und damit eine Loslösung des Internets aus dem häuslichen Bereich herbeiführen.

Zum anderen wird das Internet stark geprägt von Internet-Communitys, allen voran den sozialen Netzwerken wie Facebook. Diese entstammen dem Web 2.0, dem sog. Mitmach-Internet, das von der aktiven Teilnahme der Nutzer lebt. Im Jahre 2012 sind bereits 43% der Internet-Nutzer Mitglieder in Online-Communitys, je jünger, desto höher die prozentuale Beteiligung.[3]

---

1 „*Der Weltraum, unendliche Weiten.[...] Viele Lichtjahre von der Erde entfernt dringt die Enterprise in Galaxien vor, die nie ein Mensch zuvor gesehen hat.*“, Intro der Fernsehserie „Raumschiff Enterprise“.

2 ARD/ZDF-Onlinestudie 2013, online unter: http://www.ard-zdf-onlinestudie.de (15.05.2014).

3 ARD/ZDF-Onlinestudie 2013, a.a.O. (15.05.2014).

Kapitel 1: Entwicklung des Haftungssystems

I. Provider

Die Nutzung des Internets ist jedoch nicht ohne Weiteres möglich. Ein Festnetztelefonanschluss reicht nicht aus, um an diesem (nicht mehr) exklusiven Klub teilnehmen zu können. Vielmehr bedarf es eines Dienstleisters, der dem (Internet-)Nutzer den nötigen Zugang verschafft sowie die nötigen Ressourcen in Form von Programmen oder Speicherkapazitäten zur Verfügung stellt.

Diese Aufgabe übernehmen im Netz die Provider. Provider – vom englischen Verb „to provide“ abgeleitet, welches „beschaffen“, „liefern“ und „bereitstellen“ bedeutet – stellen den Internetzugang bereit, liefern die nötigen Inhalte und beschaffen den notwendigen Speicherplatz für die Daten der Nutzer.

Sie lassen sich in folgende – auch haftungsrechtlich unterschiedlich zu behandelnde – Provider-Arten einteilen:

1. Access-Provider

Der Access-Provider ist die Schnittstelle des Nutzers zum Internet und eröffnet ihm den Zugang zu diesem Medium, indem er ihm den Internetzugang zur Verfügung stellt. Vertraglich ist er mit dem Internetnutzer über einen Providervertrag verbunden, der ihn dazu verpflichtet, dem Nutzer das notwendige Eintrittstor zum World-Wide-Web zu eröffnen.

Somit stellt er die eine technische Verbindung zu dem jeweiligen Host-Service-Provider her, bei dem die entsprechenden Inhalte hinterlegt sind. Durch den vom Access-Provider geschaffenen Zugang fließen dann die vom Nutzer angeforderten Informationen. Access-Providing ist somit reine Datendurchleitung von den in das Internet integrierten Servern an den User.

2. Host-Service-Provider

Der Host-Service-Provider, der durch die Internetverbindung des Access-Providers nun erreichbar ist, stellt dem Internet-Nutzer seine Server zur Verfügung. Er bietet Speicherplatz an und eröffnet damit dem Nutzer auf der einen Seite die Möglichkeit, seine eigenen Inhalte ins Internet hochzuladen. Auf der anderen Seite kann der Nutzer die öffentlich zugänglichen Inhalte, die beim Host-Service-Provider gespeichert sind, abrufen.

Der Host-Service-Provider stellt damit den Hardware-Lieferant für das Internet dar.

3. Content-Provider

Der Content-Provider ist verantwortlich für die Inhalte (engl.: content), die das Internet füllen. Er hält diese für den Nutzer auf seinen Servern oder denjenigen eines Host-Service-Providers bereit. Jeder Anbieter eines Internetauftritts ist somit als Content-Provider zu qualifizieren, denn jedem Internetauftritt ist es eigen, dass dort wie auch immer geartete Informationen für einen Nutzer bereit gehalten werden. Content-Provider sind somit das Ziel jedes Internetnutzers, die Quelle der Informationen, die Informationslieferanten[4]. Ohne Content-Provider wäre das Internet ein leerer Raum. Der Nutzer hätte kein Ziel, das er ansteuern könnte.

II. Bedeutung des Access-Providers

Der Access-Provider stellt derzeit den Türöffner für die Digitalisierung des privaten und wirtschaftlichen Lebens dar. Eine zunehmende Vernetzung kann erst möglich werden, wenn nicht nur alle Systeme und Dinge internetfähig und damit von überall erreichbar sind, sondern erst dann, wenn auch die notwendige Verbindung zum Internet hergestellt ist. Es soll daher an dieser Stelle anhand zweier Schlüsseltechnologien aufgezeigt werden, weshalb der Access-Provider wichtiger Akteur in Zukunft sein und bleiben wird.

1. Access-Provider-Schlüssel des Cloud-Computing

Nachdem eine Strafbarkeit des Access-Providers nicht nur denkbar, sondern auch möglich ist, soll an dieser Stelle das Zusammenspiel von Access-Provider und Cloud-Computing beleuchtet werden. In Zeiten des portablen Internets, insbesondere auf Smartphones und Tablet-PCs, und der zunehmenden Abdeckung des urbanen Raumes mit Hotspots für W-Lan spielt die Cloud-Computing-Technologie eine immer größere Rolle. Datenbestände, ob für gewerbliche oder private Zwecke, müssen von überall aus erreichbar und bearbeitbar sein. Die Schlüsseltechnologie, die ermöglicht, ohne viel Hardware-Equipment auf Datenbestände und Rechnerleistung zuzugreifen, ist dabei die Cloud-Computing-Technologie. Sie findet dabei nicht nur Anwendung als externer Speicher, sondern offeriert auch variable Rechen- und Pro-

[4] *Hoeren,* Internetrecht, S. 442 f.

grammleistung. Dies ist einerseits vorteilhaft, andererseits birgt diese Technologie auch Nachteile. Die Auslagerung von Leistungen an einen Cloud-Dienstleister führt zwingend zu einem Kontrollverlust sowohl über die Daten als auch die Steuerbarkeit eines Leistungsabrufes.

Der Access-Provider ist für diese Technologie das notwendige Bindeglied um die Vielzahl der angebotenen Dienste auch nutzen zu können. Er muss über die nötige Zuverlässigkeit seiner Systeme sorgen.

a) Cloud-Computing

Ein kurzer Überblick über die Funktionsweise des Cloud-Computing soll die Möglichkeiten, die der Einsatz dieser Technologie gewährt, aufzeigen.

Der Begriff des Cloud-Computing ist geprägt durch die Metapher der Wolke (engl. cloud). Diese beschreibt zum einen einen abgeschlossenen Raum, der von außen – aber auch von innen – nicht durchblickt werden kann. Der Inhalt bleibt somit im Verborgenen. Zum anderen stellt die Wolke ein schwebendes Gebilde dar, welches weithin wahrgenommen werden kann (und damit auch vom Nutzer angesteuert) und den Nutzer aufgrund seiner Beweglichkeit auch „begleiten“ kann.

Sinn und Zweck der Cloud-Computing-Technologie ist folglich, dem Nutzer den Zugriff auf seine Daten immer und überall zu gestatten, nicht nur, um diese abzurufen oder einzusehen, sondern auch um diese zu bearbeiten.

Grundsätzlich besteht eine Cloud aus drei technischen Ebenen, die vom Diensteanbieter jedoch auch einzeln, je nach Bedarf, angeboten werden können. Auf der ersten Ebene befinden sich die IaaS, die Infrastructure-as-a-Service Dienste. Die IaaS-Dienste bieten zum Beispiel die Nutzung eines virtuellen Servers oder von Nachrichtendiensten an. Der Vorteil für den User der Cloud besteht nicht nur darin, dass er selbst keine Hardware mehr kaufen, vorhalten und warten muss, sondern auch, dass je nach Auslastung auf eine optimale Rechnerleistung oder Speicherkapazität zugegriffen werden kann.

Die zweite Stufe von Cloud-Diensten, die auf diese erste Ebene aufgesetzt wird, sind die PaaS, die Platform-as-a-Service Dienste. Um die PaaS betreiben zu können, wird vom Diensteanbieter eine Infrastruktur bereits vorgehalten, auf die der Nutzer keinen Einfluss hat. Es handelt sich beim PaaS-Dienst um die sog. Programmier-Ebene, bei der die Cloud als Programmierschnittstelle für den Nutzer dient. Hier ist es einzig Aufgabe des Cloud-Diensteanbieters, die Daten und die Rechenleistung entsprechend der Anwendung bereitzustellen.

Die dritte Ebene der Cloud, die wiederum die beiden vorigen als Basis benötigt, ist jene, mit welcher der normale, private Internet-Nutzer am häufigsten in Berührung kommt und deren Dienste für den herkömmlichen Konsumenten von Bedeutung sind. Es handelt sich um SaaS, die Software-as-a-Service Dienste.[5] Dem Nutzer wird auf dieser Ebene ermöglicht, innerhalb der Cloud bereitgestellte Software zu nutzen, wie z.B. Textverarbeitungsprogramme oder E-Maildienste. Hier hat der Nutzer den Vorteil, dass er nicht nur keine kostspielige und schnell veraltende Hardware benötigt, sondern auch darüber hinaus die Kosten und den Aufwand der Softwareanschaffung sowie für Updates spart. Dem privaten Nutzer werden SaaS-Dienste heute weitgehend kostenneutral als Zusatzdienst oder werbefinanziert angeboten. Zudem besteht bei der Nutzung solcher Dienste die Möglichkeit nach Zeiteinheiten abzurechnen über sog. pay-as-you-go Abrechnungssysteme.

Die Cloud-Computing-Technologie kann nicht nur in diese drei technischen Ebenen aufgeteilt werden, sondern es ist auch eine organisatorische Aufteilung möglich. Zu unterscheiden ist zwischen einer Public-Cloud und einer Private-Cloud. An einer Public-Cloud kann grundsätzlich jeder teilhaben und die angebotenen Cloud-Dienste nutzen. Eine Private-Cloud ist demgegenüber darauf angelegt, nur einem geschlossenen Kreis ausgewählter Nutzer zur Verfügung zu stehen, z.B. einem Unternehmen oder einer öffentlichen Verwaltung.

b) Access-Provider und Cloud-Computing

Wie dargelegt basiert die Cloud-Computing-Technologie auf dem Internet und damit auch darauf, dieses möglichst immer erreichen zu können. Hierbei wird die Variante des portablen Internets, z.B. via UMTS oder LTE, immer wichtiger. Endgeräte werden bereits serienmäßig mit der Möglichkeit ausgestattet, eine SIM-Karte eines Mobilkommunikationsnetzbetreibers verwenden zu können.[6]

Der Schlüssel liegt daher bei den Access-Providern, die garantieren müssen, dass man von beinahe überall aus die Möglichkeit hat, online zu gehen. Ansonsten wäre die Cloud-Computing-Technologie unnütz.

Betrachtet man das Zusammenspiel von Access-Provider und Cloud-Computing in strafrechtlicher Hinsicht, so ist Folgendes festzustellen:

---

5 Zu den Ebenen des Cloud Computing ausführlich: http://de.wikipedia.org/wiki/Cloud-Computing (12.12.2014), m.w.N.

6 Z.B. sog. Cellular-Modelle von Apple.

c) Anwendbarkeit deutschen Strafrechtes

Problematisch hinsichtlich der Strafbarkeit innerhalb der Cloud ist grundsätzlich die Anwendung deutschen Strafrechts, da die Server, auf denen die Daten innerhalb der Cloud gespeichert werden, meist im Ausland stehen bzw. es für den Nutzer nicht einsehbar ist, wo sich diese befinden.[7]

Zunächst ist hierbei der Ubiquitätsgrundsatz des § 9 StGB zu beachten, der zu einer weiten Anwendung des deutschen Strafrechtes führt, nachdem grundsätzlich jede Handlung und jeder tatbestandliche Erfolg in Deutschland zu einer Strafbarkeit führen kann.[8]

Die vom Access-Provider vorgenommene Unterstützungshandlung, die im Aufbauen der Verbindung und deren Aufrechterhalten besteht, erfolgt im Inland, sodass sowohl seine Handlung im Inland stattfindet als auch der sich daran anknüpfende Erfolg im Inland eintritt.

Die Handlungen des Access-Providers sind auch nicht als bloße Unterstützungshandlung zu einem Transitdelikt zu qualifizieren, denn es handelt sich überwiegend um einen im Inland sitzenden Haupttäter, der die Unterstützung des Access-Providers in Anspruch nimmt.

d) Strafverfolgung des Access-Providers

Die Möglichkeiten der Strafverfolgungsbehörden im Zusammenhang mit Cloud-Computing sind eingeschränkt. Zum einen ist zumeist nur schwer zu ermitteln, wo die Daten innerhalb der Cloud abgelegt sind. Zum anderen ist auch die Zugriffsmöglichkeit bei Daten, die außerhalb des deutschen Hoheitsgebietes liegen, meist nicht gegeben. Darüber hinaus kann es sein, dass die Daten aufgrund der in der Cloud vorgenommenen Optimierungsprozesse nur fragmentarisch vorliegen.[9]

Der Access-Provider ist jedoch für die Strafverfolgungsbehörden deshalb so interessant, weil er zumeist im Inland sitzt und – um einen Internetzugang zu eröffnen – lokale Einwahlknotenpunkte betreiben muss und daher als lokaler Betreiber greifbar ist. Anders als bei den weiteren am Cloud-Computing Beteiligten ist der Aufenthaltsort seiner Infrastruktur bekannt und liegt im Inland, sodass gegen ihn ermittelt und auf seine Ressourcen zugegriffen werden kann.

---

7 Jones/Nobis/Röchner/Thal/*Jones*, S. 38.

8 *Hilgendorf/Valerius*, Rn. 133ff.

9 Ausführlich hierzu Jones/Nobis/Röchner/Thal/*Jones*, S. 38 f.

e) Fazit

Das Cloud Computing ist als zukunftsweisende Technologie nicht mehr wegzudenken. Die Vorteile, die es den Nutzern auf der einen Seite bietet, sämtliche Hard- und Softwareleistungen über die Cloud abzuwickeln, zieht jedoch auf der anderen Seite Schwierigkeiten im Rahmen der Strafverfolgung innerhalb dieser Dienste nach sich. Lediglich der Access-Provider bleibt auch an dieser Stelle der einzige Ansatzpunkt, um sowohl repressiv als auch präventiv in strafrechtlicher Hinsicht gegen diesen tätig zu werden.[10].

2. Industrie 4.0 und Access-Provider

Ein weiteres wachsendes Betätigungsfeld für Access-Provider wird die zukünftige Industrie 4.0 sein. Durch die Vernetzung von Industrieprozessen auf der einen und Produktionsmaschinen auf der anderen Seite soll zukünftig der Industriestandort Deutschland seine Vorreiterposition im Bereich Anlagenbau sichern und zusätzlich auch als Produktionsstandort wieder gestärkt werden.[11] Mit der Schaffung des Internet der Dinge[12], d.h. der direkten Kommunikation von in diesem Falle Produktionsmaschinen mit einem Unternehmensnetzwerk oder dem Internet, wird auch dem Access-Provider an dieser Stelle eine tragende Funktion zukommen.

a) Industrie 4.0

Mit dem Begriff *Industrie 4.0* wird eine neue, gerade beginnende vierte industrielle Revolution bezeichnet.[13] Nach der Einführung der Dampfmaschine als Zeichen der Industrialisierung, des Fließbandes für die Realisierung der Massenproduktion und der flächendeckenden Verwendung elektronischer Steuerungstechnik als Auslöser für die Automatisierung der Industrie, soll nun ein weiterer Meilenstein erreicht sein.[14]

Ausgangspunkt ist der Einsatz von cyber-physischen Systemen innerhalb der Produktionsstätten.[15] Bei diesen handelt es sich um kleinste Computereinheiten, die in sämtliche Maschinen implementiert sind, welche an der Produktion und der darüber

---

10 So auch zuletzt *Hilgendorf,* JZ 2012, 825, 831.

11 Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, S. 5.

12 Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, S. 17.

13 Produktionsarbeit der Zukunft – Industrie 4.0, S. 22.

14 Zukunftsbild „Industrie 4.0“, S. 10 (http://www.bmbf.de/de/19955.php).

15 Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, S. 18.

hinausgehenden Wertschöpfungskette beteiligt sind.[16] Durch deren Vernetzung soll Echtzeitkommunikation zwischen den Maschinen möglich werden, um diese den Herstellungsprozess vollständig autonom bestmöglich gestalten zu lassen.[17]

Mit der Art dieses vernetzten Informationsaustausches können räumliche Grenze beinahe überwunden und zwischen Unternehmen Kommunikationshindernisse minimiert werden.[18] Diese Form der zukünftig in allen Herstellungsschritten vernetzten Produktion soll den Unternehmen etliche Vorteile bringen: Durch die erlangte Flexibilität soll es zukünftig besser möglich sein, auf individuelle Kundenwünsche einzugehen und diese umzusetzen[19] sowie Geschäftsprozesse dynamisch zu gestalten. Eine kurzfristige Reaktion auf Preis- bzw. Lieferzeitschwankungen soll gewährleistet sein.[20] Auch Ressourcen sollen produktiver und effizienter eingesetzt werden, um die Produktionsprozesse anlassbezogen über die gesamte Wertschöpfungskette zu optimieren.[21]

Diese Vernetzung der Produktionsmaschinen und -abläufe führt zum Entstehen einer Smart Factory. Diese ist genauso wie z.B. das Smart Grid oder die Smart Mobility Teil des Internet der Dinge.[22] Damit dieses Internet der Dinge entstehen kann, ist es nicht nur notwendig, dass alle zu vernetzenden Teilnehmer mit cyber-physischen Systemen ausgestattet werden. Um wiederum Kommunikation mit dem Internet herstellen zu können, bedarf es eines Access-Providers.

b) Herausforderungen für Access-Provider in der Industrie 4.0

Hauptgefahren innerhalb der Industrie 4.0 sind die Industriespionage gefolgt von Manipulation, d.h. Sabotage des Betriebsablaufes. Bei kritischen Infrastrukturen ist auch die Gefahr eines terroristischen Anschlages zu nennen.[23] Ein sicherer Datentransfer, der den Schutz von Unternehmensdaten garantiert muss daher zwingend gewährleistet werden.[24] Dies muss jedoch grundsätzlich von dem jeweiligen Unternehmen selbst gewährleistet werden und ist nicht Aufgabe des Access-Providers.

---

16 Zukunftsbild „Industrie 4.0“, S. 6.

17 Zukunftsbild „Industrie 4.0“, a.a.O.

18 Zukunftsbild „Industrie 4.0“, a.a.O.

19 Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, S. 19; Zukunftsbild „Industrie 4.0“, S. 7.

20 Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, S. 20.

21 Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, a.a.O.

22 Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, S. 23.

23 Zukunftsbild „Industrie 4.0“, S. 26.

24 Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, S. 62 f.

Derzeit gestaltet sich die Rechtslage wie folgt: Bei den ausgetauschten Unternehmensdaten handelt es sich um fremde Inhalte, für deren Legalität der Access-Provider nach der hier vertretenen Ansicht nur haften soll, wenn er Kenntnis von der Rechtswidrigkeit der Informationen hat. Das bedeutet, dass erst nach einem von der unternehmensinternen IT-Security erkannten Angriff der vertraglich an das Unternehmen gebundene Access-Provider dazu angehalten werden kann, als angreifend erkannte Netzadressen zu sperren. Ob in Zukunft zum besseren Schutz der Industrie 4.0 eine proaktive Handlung des Access-Providers gefordert werden muss, ist derzeit noch nicht absehbar.

c) Fazit

Auch die Industrie 4.0 und das Internet der Dinge sind abhängig von den Dienstleistungen der Access-Provider. Bei der Erforschung und Umsetzung der Industrie 4.0 sollte daher auch dessen tragende Rolle nicht außer Acht gelassen werden. Es muss geprüft werden, ob die bestehenden Haftungsregelungen auf die entwickelten Szenarien anwendbar sind und ob ggf. von gesetzgeberischer Seite nachgesteuert werden muss.[25] Dieses neue Betätigungsfeld für Access-Provider, das einen hohen Stellenwert hat und zukünftig die Grundlage für Gemeinschaft und Wohlstand bilden soll, kann einen entsprechend hohen Stellenwert bieten, der gesetzgeberisches Handeln anstoßen könnte.

3. Zusammenfassung

Der Access-Provider stellt einen wichtigen Baustein bei der Entwicklung zukünftiger Technologien und deren Vernetzung dar, sodass es im Weiteren angezeigt ist, dessen Haftung aus strafrechtlicher Sicht näher zu betrachten.

III. Entwicklung des Haftungssystems

Vorausgeschickt werden soll nun ein Überblick über die Entwicklung der Providerhaftung hin zum heutigen Haftungssystem des Telemediengesetzes (TMG) gegeben werden.

---

[25] Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, S. 63.

1. Grundlegende Gesetzgebung in Bund und Ländern

Die Rechtsgrundlage, auf welcher die Haftung für Inhalte im Internet fußte, war in Deutschland bis zur Schaffung des heute gültigen, zum 01.03.2007 eingeführten Telemediengesetzes[26], aufgespalten. Es gab zum einen das seit 1997 gültige Teledienstegesetz (TDG) des Bundes und zum andern den Mediendienstestaatsvertrag der Länder (MDStV).

Diese zweigleisige Rechtsetzung war Konsequenz der seinerzeit auseinanderfallenden Gesetzgebungskompetenzen. Aufgrund der Rundfunkfreiheit der Länder, hatten diese die Gesetzgebungskompetenz nach Art. 70 Abs. 1 GG für die auf Massenkommunikation mit Meinungsrelevanz bezogenen Mediendienste inne. Zur Vereinheitlichung wurde ein Staatsvertrag beschlossen, um 16 unterschiedliche Regelungen zu vermeiden. Demgegenüber hatte der Bund die ausschließliche Gesetzgebungskompetenz des Bundes auf dem Gebiet der Telekommunikation gem. Art. 73 Abs. 1 Nr. 7 GG für die auf Individualkommunikation ausgerichteten Teledienste[27].

So entstand auf Länderebene der MDStV, auf Bundesebene wurde 1997 das TDG als Teil des Informations- und Kommunikationsdienstegesetzes[28] (IuKDG) geschaffen.

a) TDG

Das TDG, eingeführt durch das IuKDG, trat am 01.08.1997 in Kraft. Das IuKDG sollte einheitliche wirtschaftliche Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten der elektronischen Informations- und Kommunikationsdienste schaffen[29].

Ziel des Gesetzgebers war es, den Weg ins Informationszeitalter zu ebnen und die ggf. entstehenden Hindernisse zu beseitigen. Zudem sollte der mit Hilfe dieses Mediums im Entstehen befindliche Markt gefördert werden.[30] Die aus dem Boden sprießenden Informations- und Kommunikationsdienste sollten in kontrollierbare Bahnen geleitet werden.

---

[26] Telemediengesetz, im folgenden TMG; Art. 1 des Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungs-Gesetz ElGVG) v. 26.02.2007, BGBl. I S. 179.

[27] MüKo-StGB/*Altenhain*, TMG, § 1 Rn. 1.

[28] BT-Drs. 13/7385.

[29] Vgl. § 1 TDG a.F.

[30] BT-Drs. 13/7385, S. 16.

Hierzu wurden auch die in der vorliegenden Arbeit zu betrachtenden Regelungen zur Verantwortlichkeit dieser Informations- und Kommunikationsdienste eingeführt und im damaligen § 5 TDG festgeschrieben.

Das TDG erfuhr dann 2001 durch das EGG[31] eine strukturelle Änderung, da die 2000 erlassene E-Commerce-Richtlinie der Europäischen Union[32] (ECRL) in nationales Recht umgesetzt werden musste.

Dabei wurden auch die Regeln über die Verantwortlichkeit der Diensteanbieter an die entsprechenden europarechtlichen Vorgaben angepasst und mit den §§ 7–10 ins Telemediengesetz (TMG) übernommen, das 2007 das TDG ablöste.

b) MDStV

Der Mediendienstestaatsvertrag der Länder war das Gegenstück zum TDG des Bundes. Nachdem sich Bund und Länder nicht über die Gesetzgebungskompetenz bezüglich Internet und Mediendienste einig wurden und der Bund das Teledienstegesetz auf den Weg gebracht hatte, wurde von den Ländern, die die Gesetzgebungskompetenz im Bereich der Medien inne hatten, der MDStV beschlossen, der den Bereich der Mediendienste im Internet regelte – entsprechend dem TDG im Bereich der Teledienste.

Der MDStV trat zeitgleich mit dem TDG am 01.08.1997 in Kraft und erfuhr immer wieder Änderungen. Ebenso wie das TDG musste auch er an die ECRL angepasst werden. Die Regelungen, die der MDStV über die Verantwortlichkeit der Mediendiensteanbieter enthielt, entsprachen denen des TDG.

Mit der Einführung des TMG wurde der MDStV außer Kraft gesetzt und die Regelungen, die keine Telemedien betrafen, wurden in den Rundfunkstaatsvertrag aufgenommen.

2. E-Commerce-Richtlinie

Auf europäischer Ebene erließen das Europäische Parlament und der Rat am 8. Juni 2000 die Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr, kurz E-Commerce-Richtlinie genannt.[33]

---

[31] Elektronischer-Geschäftsverkehr-Gesetz, BGBl. 2001 I, Nr. 70, S. 3721 ff.

[32] ABl. EG Nr. L 178 v. 17.7.2000, „Richtlinie 2000/31/EG der europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr")".

Ziel der Richtlinie war die Harmonisierung der geltenden innerstaatlichen Regelungen der Mitgliedsstaaten für Dienste der Informationsgesellschaft und die Sicherstellung des freien Dienstleistungsverkehrs auch in diesem Bereich.

Mit dem Erlass der E-Commerce-Richtlinie musste der deutsche Gesetzgeber europäische Vorgaben, insbesondere zur Regelung des europäischen Geschäftsverkehrs im Binnenmarkt, umsetzen.

In Abschnitt 4 – Verantwortlichkeit der Vermittler – wurde mit den Art. 12–15 ECRL für die Haftung der Provider eine Mindestharmonisierung erreicht.

Die ECRL wurde in der Bundesrepublik Deutschland mit dem „Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr", kurz: Elektronischer-Geschäftsverkehr-Gesetz (EGG), in nationales Recht umgesetzt. Dessen Art. 1 regelte die Anpassung des TDG an die Vorgaben der E-Commerce-Richtlinie.[34]

3. TMG

Da die „neuen Dienste" der Informationsgesellschaft von den traditionellen – auf den Rundfunk zugeschnittenen – Vorgaben abgekoppelt werden sollten[35], war es zur Fortentwicklung der Regelungen zwingend erforderlich, diese in einem neuen, einheitlichen Gesetz zusammenzufassen und die zwar grundsätzlich gleichlaufenden und gleichlautenden Regelungen, die bisher aufgrund auseinanderfallender Gesetzgebungskompetenzen in TDG und in MDStV statuiert waren, zur Übersichtlichkeit in einem Gesetz zu vereinen.

Bund und Länder waren sich einig, dass die künftige Medienordnung unabhängig vom Verbreitungsweg und entwicklungsoffen sein sollte.[36] Im Jahre 2007 trat dann das TMG in Kraft. Damit wurde auch der Streit über die Gesetzgebungskompetenz beendet und dem Bund die Gesetzgebungskompetenz über den neuen Begriff der „Telemediendienste" eingeräumt. Dies gewährleistete eine bundesweit einheitliche Regelung auf diesem Gebiet.

Die Gesetzgebungskompetenz des Bundes hinsichtlich der Telemedien richtet sich nun nach Art. 74 Abs. 1 Nr. 11 GG. Von dieser machte der Bund im Elektronischer-

---

33 ABl. EG Nr. L 178/1 vom 17.07.2000.
34 BT-Drs. 14/6098, S. 5.
35 BT-Drs. 16/3078, S. 11.
36 BT-Drs. 16/3078, S. 11.

Geschäftsverkehr-Vereinheitlichungsgesetz[37] (ElGVG) Gebrauch, in dessen Art. 1 das Telemediengesetz eingeführt wurde.

Aus den Begriffen „Teledienste“ und „Mediendienste“ wurden die „Telemedien“, § 2 S. 1 Nr. 1 TMG. Die Gesetzgebungszuständigkeit für diese „neuen“ Telemedien richtete sich nicht mehr nach der Art der Verbreitung – Rundfunk oder Telekommunikation –, sondern nach den inhaltlichen Zielen der Regelungen. Dadurch wurden die bis dahin bestehenden Kompetenzstreitigkeiten zwischen Bund und Ländern beseitigt.

Nach der Übereinkunft von Bund und Ländern[38] waren im TMG die wirtschaftliche Fragen betreffenden Angelegenheiten zu regeln, wie Herkunftslandprinzip, Zulassungsfreiheit, Informationspflichten, Verantwortlichkeit und Datenschutz, entsprechend den Vorgaben der E-Commerce-Richtlinie.

Inhaltlich wurden im TMG die Vorschriften des TDG und des MDStV weitgehend unverändert übernommen. Die Vorschriften über die Providerhaftung bspw. wurden lediglich im Paragraphengefüge verschoben. Aus den §§ 8–11 TDG wurden die §§ 7–10 TMG. Auch in der Gesetzesbegründung für die §§ 7–10 TMG verweist der Gesetzgeber im ElGVG mit einem Satz auf die Begründung im EGG und damit auf diejenige des TDG.

Kapitel 2: Providerhaftung nach dem Telemediengesetz

I. Überblick

Das TMG, in Kraft getreten am 01.03.2007, definiert zuerst seinen Anwendungsbereich in § 1 TMG sowie weitere allgemeine Bestimmungen in den §§ 2, 3 TMG. Die §§ 5 und 6 TMG regeln die Informationspflichten der Diensteanbieter und den Datenschutz im Anbieter-Nutzer-Verhältnis die §§ 11–15 TMG. Die Verantwortlichkeit der Diensteanbieter wird in den §§ 7–10 TMG statuiert, die in der vorliegenden Arbeit näher zu behandelt wird.

Der Anwendungsbereich ist gem. § 1 TMG eröffnet, wenn ein Diensteanbieter Inhalte aus dem Bereich der Informations- und Kommunikationsdienste auf elektronischem Wege bereithält. Maßgebend ist die Bereitstellung elektronischer Inhalte, nicht der Übertragungsweg. Nach richtlinienkonformer Auslegung setzt eine elektro-

---

37 BGBl. 2007 I, Nr. 6, S. 179.

38 BT-Drs. 16/3078, S. 1, 11 f.

nische Bereitstellung voraus, dass die Inhalte über ein Kommunikationsnetz übertragen werden.[39]

Ein Diensteanbieter, legaldefiniert in § 2 Nr. 1 TMG, ist „jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt". Diensteanbieter sind daher bspw. auch die Anbieter von Auktions- und Verkaufsplattformen im Internet[40], die dem Nutzer den Zugang zu Inhalten Dritter vermitteln.

Dienst im Sinne des TMG bedeutet Dienstleistung, ebenso wie im europäischen Vorbild der ECRL.[41]

Die im Folgenden noch genauer zu beleuchtenden Vorschriften zur Haftung der Diensteanbieter finden sich in den §§ 7–10 TMG. Hierbei richtet sich die Frage der Haftung zum einen nach der Unterscheidung, ob eigene oder fremde Inhalte vorliegen und zum anderen danach, als welche Art von Diensteanbieter, d.h. Provider, der Verantwortliche einzuordnen ist.

II. Dogmatische Einordnung

Bei den Haftungsprivilegierungen der §§ 7–10 TMG handelt es sich nach den europarechtlichen Vorgaben der ECRL um Querschnittsregelungen für das gesamte Recht – diese finden daher nicht nur für das Zivil- und das Öffentliche Recht, sondern auch für das Strafrecht Anwendung.[42]

Um die haftungsrechtliche Verantwortlichkeit des Diensteanbieters beurteilen zu können, muss zum einen eine einschlägige Haftungsnorm aus dem Zivil-, Öffentlichen- oder Strafrecht tatbestandlich erfüllt sein. Zum anderen müssen zusätzlich die entsprechenden Privilegierungen aus dem Bereich der §§ 7–10 TMG geprüft werden, die dann ggf. die Haftung des Diensteanbieters einschränken. Umstritten ist, nach welcher Reihenfolge diese Prüfung ablaufen soll.[43]

Die horizontale, d.h. auf alle Rechtsgebiete gleichermaßen anwendbare, Querschnittsregelung der §§ 7–10 TMG umfasst heute unstreitig auch das Strafrecht.[44] Dem steht auch nicht der Erwägungsgrund 8[45] der ECRL entgegen, in dem es heißt,

---

39 *Gercke/Brunst*, Rn. 567.

40 Spindler/Schuster/*Holznagel/Ricke*, § 2 TMG, Rn. 2.

41 MüKo-StGB/*Altenhain*, § 1 TMG, Rn 7.

42 SSW/*Hilgendorf*, § 184 StGB, Rn 23; Spindler/Schuster/*Hoffmann*, vor § 7 TMG, Rn. 15.

43 Spindler/Schuster/*Holznagel/Ricke*, § 2 TMG, Rn. 2.

44 KG NJW 2014, 3798, 3799, m. Anm. Hassemer

45 Erwägungsgrund 8: *„Ziel dieser Richtlinie ist es, einen rechtlichen Rahmen zur Sicherstellung des*

dass der Bereich des Strafrechts als solcher nicht harmonisiert werden soll. Mit diesem Erwägungsgrund soll nur ausgedrückt werden, dass die ECRL keine besonderen nur für das Strafrecht relevanten Vorschriften enthält.[46]

Die §§ 7 ff. TMG stellen keine Haftungsnormen im eigentlichen Sinne dar denn sie wirken weder haftungs- noch anspruchsbegründend.[47] Vielmehr greifen sie nur privilegierend hinsichtlich des jeweiligen Haftungstatbestandes ein.[48] Sie formulieren lediglich, wann ein Diensteanbieter verantwortlich oder nicht verantwortlich für sein Handeln sein soll. Diese Vorschriften sind aber weder eigenständige Straftatbestände, noch stellen sie Ermächtigungsgrundlagen dar, noch bilden sie Ausgangspunkte für staatliches Handeln.[49] Ob tatsächlich ein zivil-, öffentlich- oder strafrechtlich als rechtswidrig einzustufendes Verhalten vorliegt, aufgrund dessen auch der Provider in die Haftung genommen werden kann, muss gesondert anhand der vorliegenden zivil-, öffentlich- oder strafrechtlichen Gesetze bestimmt werden.

Ebenso wenig begründen sie eine Garantenstellung der Provider im Sinne des § 13 StGB.[50] Der Gesetzgeber hat in seiner amtlichen Begründung zum TDG festgehalten – die entsprechend der Begründung zum TMG auch für diese unverändert gelten soll[51] – dass damit die Schaffung einer eigenständigen Garantenstellung nicht einhergehen sollte.[52]

Da es sich bei den Verantwortlichkeitsregeln nach den §§ 7 ff. TMG um horizontale Querschnittsregeln handelt, die auf die Gesamtheit der Rechtsgebiete, d.h. Zivilrecht, Öffentliches Recht und Strafrecht Anwendung finden[53], stellt sich für das Strafrecht die Frage, wo diese dogmatisch zu verorten sind, wenn sie keine Haftungstatbestände eigener Art darstellen. Diese Frage ist noch immer umstritten.

Hierzu gibt es zwei große Meinungsströmungen. Zum einen wird vertreten, dass es sich um sog. Filter-Regelungen handle, die vor oder nach dem jeweiligen Haftungstatbestand separat zu prüfen seien. Zum anderen wird vertreten, dass die Haftungsprivilegierungen in den jeweiligen Straftatbestand zu integrieren und innerhalb desselben zu prüfen seien.

---

freien Verkehrs von Diensten der Informationsgesellschaft zwischen den Mitgliedstaaten zu schaffen, nicht aber, den Bereich des Strafrechts als solchen zu harmonisieren."

46 MüKo-StGB/*Altenhain,* vor § 7 TMG, Rn 2.

47 Spindler/Schuster/*Hoffmann*, vor § 7 TMG, Rn. 31.

48 *Haug,* Rn. 272.

49 BGH NJW 2007, 2558.

50 MüKo-StGB/*Altenhain*, vor § 7 TMG, Rn. 4.

51 BT-Drs. 16/3078, S. 15.

52 BT-Drs. 14/6098, S. 37.

53 Spindler/Schuster/*Hoffmann*, vor § 7 TMG, Rn. 25.

1. Zweistufige Filtermodelle

Die Ansicht, welche die Haftungsprivilegierungen des TMG als Haftungsfilter verstehen will, geht von einer zweistufigen Prüfung der Haftung aus. Hierbei werden die Haftungstatbestände der §§ 7–10 TMG außerhalb der gesetzlichen Haftungstatbestände geprüft.

Nach der einen Unterauffassung wird in diesem zweistufigen Modell sodann auf erster Stufe der sog. Vor-Filter geprüft. Auf der zweiten Stufe werden dann, sofern eine Haftungsprivilegierung nicht eingreift, die allgemeinen Haftungstatbestände nach dem jeweiligen anwendbaren Gesetz geprüft.[54]

Nach anderer Auffassung ist der Haftungsfilter in umgekehrter Reihenfolge nach den möglichen Haftungsnormen zu prüfen, d.h. erst auf der zweiten Prüfungsstufe.[55]

Für die rechtliche Einordnung der Regelungen als Haftungsfilter spricht, dass die Gesetzesbegründung dies explizit ausführt. Nach der Gesetzesbegründung ist die Wirkungsweise der Haftungsprivilegierungen „untechnisch“ als „Filter“ zu bezeichnen.[56] Der Gesetzesbegründung kann demgegenüber allerdings nicht entnommen werden, ob es sich um einen Vor- oder Nach-Filter bei den Privilegierungen handeln soll. Daraus, dass „bevor“ der Provider zur Verantwortung gezogen wird, zu prüfen sei, ob er nicht privilegiert ist, kann nicht darauf geschlossen werden, dass der Gesetzgeber einen Vor-Filter installieren wollte. Im nächsten Satz stellt der Gesetzgeber nämlich darauf ab, dass soweit „im Einzelfall die Voraussetzungen der allgemeinen Vorschriften für eine Haftung erfüllt [sind], der Diensteanbieter für die Rechtsgutsverletzung gleichwohl nicht verantwortlich [ist], wenn er sich auf das Eingreifen der §§ 9, 10 oder 11 [TDG] berufen kann“[57], was für einen Nachfilter sprechen könnte.

Die Filterlösung sei auch deshalb vorzugwürdig, weil sie als einzige in der Lage wäre, die von der ECRL geforderte Rechtseinheit, Rechtsklarheit und auch Rechtssicherheit zu garantieren, die durch sie für die Diensteanbieter geschaffen werden sollte.[58]

---

54 BGH NJW 2003, 3764; so auch: MüKo-StGB/*Altenhain*, vor § 7 TMG, Rn. 5, m.w.N.

55 *Haug*, Rn. 287.

56 BT-Drs. 14/6098, S. 23.

57 A.a.O.

58 *Haug*, Rn. 287.

2. Integrationsmodell

Entgegen der Filtermodelle wird bei der Integrationslösung die Haftungsprivilegierung nach den §§ 7 ff. TMG direkt in den spezifischen Deliktsaufbau des zu prüfenden Tatbestandes hineingeprüft.[59]

Vorstellbar wäre somit eine Integration auf Ebene der Schuld, der Rechtswidrigkeit oder auch des objektiven Tatbestands.

Gegen eine Verortung der Haftungsprivilegierung auf Schuldebene spricht jedoch, dass die §§ 7–10 TMG objektiv bestimmte Pflichten der Diensteanbieter festlegen und nicht die subjektive persönliche Vorwerfbarkeit eines Verhaltens betreffen.[60]

Auch eine Verortung auf der Ebene der Rechtfertigungsgründe ist nicht zielführend, da es hier zu einem Verstoß gegen das Prinzip der Einheitlichkeit der Rechtsordnung kommen kann, sofern eine beispielsweise in § 10 Nr. 1 TMG weitergehende zivilrechtliche Verantwortlichkeit die strafrechtliche überholen würde.[61]

Innerhalb der Integrationsmodelle vorzugswürdig erscheint die Prüfung der Verantwortlichkeitsregeln auf Tatbestandsebene. Die Verantwortlichkeitsregeln des TMG beschreiben tatbestandsähnliche Verhaltensweisen, d.h. wann die Diensteanbieter typischerweise verantwortlich sind und wann nicht. Dies entspricht den Tatbestandsmerkmalen eines bestimmten Deliktes.

Mit der Verortung der Verantwortlichkeitsregeln im Tatbestand können diese auch gebietsspezifisch, d.h. egal ob im Zivilrecht, Strafrecht oder öffentlichem Recht, ausgelegt werden.[62]

3. Stellungnahme

Durch die tatbestandliche Integrationslösung geht die durch die Querschnittsregelungen geschaffene Rechtseinheit, Rechtsklarheit und auch Rechtssicherheit, die in den Erwägungsgründen 7 und 8 der ECRL als Ziele ausdrücklich genannt werden, nicht verloren.

Zum einen wird die Rechtseinheit dadurch gewahrt, dass die Vorschriften der §§ 7–10 TMG unverändert und gleich in den anderen Rechtsgebieten angewendet werden. Ebenso verhält es sich mit der Rechtsklarheit und der Rechtssicherheit. Die

---

59 *Valerius* BeckOK-StGB, Providerhaftung, Rn. 6; *Gercke/Brunst*, Rn. 580.

60 *Sieber*, in: Verantwortlichkeit im Internet, Rn. 243.

61 *Gercke/Brunst*, Rn. 580.

62 *Hilgendorf/Valerius*, Rn. 192.

Vorschriften werden durch die Verortung im Prüfungsaufbau nicht verändert. Die Prüfung der Querschnittsregelungen zwingend in einer Vorprüfung vorzunehmen, würde weder die Rechtsklarheit noch die Rechtssicherheit erhöhen. Auch bei der Verortung der Vorschriften im Tatbestand können die Diensteanbieter ihre Verantwortlichkeit anhand der Vorschriften der §§ 7 ff. TMG ablesen.[63]

Zum anderen ergibt sich aus den Gesetzesmaterialien auch nicht, dass der Gesetzgeber zwingend von einer Vor-Filter-Lösung ausgegangen ist. Dies ist schon daran zu erkennen, dass er bewusst das Wort „untechnisch" verwendet, woraus sich ergibt, dass der Gesetzgeber die dogmatische Einordnung gerade nicht selbst vornehmen wollte. Dadurch sollte lediglich die Wirkung der Haftungsprivilegierung veranschaulicht werden. Dass der Gesetzgeber eine neue dogmatische Kategorie einführen wollte, liegt fern.[64] Auch die Tatsache, dass mit der ECRL eine technik- und wirtschaftsfreundliche Regelung geschaffen werden sollte, steht der tatbestandlichen Integration dieser Vorschriften nicht entgegen. Wo die Vorschriften dogmatisch eingeordnet werden, spielt für die Ausübung der Geschäftstätigkeit der Diensteanbieter keine Rolle. Die Diensteanbieter kennen ihre Privilegierung und deren Grenzen.[65]

Dass die Integrationslösung als vorzugswürdig zu behandeln ist, ergibt sich auch daraus, dass dadurch die praktische Anwendbarkeit des deutschen Strafrechts nicht beeinträchtigt wird. Dies ist insbesondere vor dem Hintergrund der Teilnahme-Strafbarkeiten gemäß §§ 26, 27 StGB zu beachten. Eine Teilnehmerstrafbarkeit ist nur möglich, wenn auch eine tatbestandliche und rechtswidrige Vortat vorliegt. Dies ist bei der Vor-Filter-Lösung nicht möglich, da man gar nicht erst bis zur Prüfung des Tatbestandes des Delikts gelangt. Ebenso verhält es sich bei den Irrtumsregeln. Bei der Zuordnung der Haftungsregeln zum Tatbestand läge bei einem Irrtum über die Schäden ein Tatbestandsirrtum gem. § 16 StGB vor. Handelte es sich um eine Verortung in der Schuld, so wäre § 17 StGB anwendbar. Dafür spricht darüber hinaus auch, dass es sich bei den §§ 7–10 TMG um rein objektive Haftungsprivilegierungen handelt. Dies legt ebenso für eine Prüfung innerhalb des Tatbestandes nahe.[66]

Die Integrationslösung auf Tatbestandsebene ist somit vorzugswürdig und eine dogmatische Einordnung der Regelungen der §§ 7–10 TMG dort vorzunehmen.[67]

---

63 A.A. in MüKo-StGB/*Altenhain*, vor § 7 TMG, Rn. 7 f.

64 *Hilgendorf/Valerius*, Rn. 190.

65 MüKo-StGB/*Altenhain*, vor § 7 TMG, Rn. 7.

66 *Gercke/Brunst*, Rn. 580.

67 *Hilgendorf/Valerius*, Rn. 192; so auch zuletzt Spindler/Schuster/*Hoffmann*, vor § 7 TMG, Rn. 31a.

III. Providerhaftung

Das TMG regelt in seinem Abschnitt 3, Verantwortlichkeit, in den §§ 7–10 TMG die Haftung der Diensteanbieter, der Provider. Neben der technischen, d.h. funktionellen, Abgrenzung der Provider[68] in Host-, Content-, und Access-Provider, ist nach dem Gesetz zunächst zu unterscheiden zwischen der Haftung für eigene Informationen und der Haftung für fremde Informationen. Bei der Haftung für fremde Informationen unterscheidet das Gesetz weiter zwischen der reinen Durchleitung (§ 8 TMG), der kurzzeitigen Zwischenspeicherung (§ 9 TMG) und der (andauernden) Speicherung (§ 10 TMG) von fremden Informationen.

1. Eigene Informationen

Für eigene Informationen haftet der Diensteanbieter nach § 7 TMG. Insofern ist zunächst zu klären, was unter eigenen Informationen zu verstehen ist.

a) Informationen

Der im TMG verwendete Begriff der Informationen ist der Formulierung der Art. 12–15 der ECRL entnommen. Im § 5 TDG a.F. wurde demgegenüber noch der Begriff der Inhalte verwendet, zu welchem vertreten wurde, dass dieser sich nur auf rechtswidrige Inhalte beziehen sollte und rechtmäßige Inhalte nicht mitumfassen würde, was zu einer teilweise einschränkenden Auslegung des Begriffes der Inhalte führte.[69] Mit der Umsetzung der ECRL wurde der Begriff der „Inhalte“ durch den der „Informationen“ ersetzt, der nach dem Willen des Gesetzgebers weit auszulegen ist und damit sämtliche „Angaben, die im Rahmen des jeweiligen Teledienstes übermittelt und gespeichert werden“ umfasst[70]. Daher fallen alle von Telemediendiensten, d.h. von Diensteanbietern, übermittelten oder gespeicherten Daten unter den Anwendungsbereich des Informationsbegriffes. Unerheblich ist dabei, ob diese vom Webbrowser lesbar gemacht werden können oder hierzu zusätzliche Software eingesetzt werden muss.[71]

---

68 *Hilgendorf/Valerius*, Rn. 179; *Sieber*, in: Verantwortlichkeit im Internet, S. 261 ff.

69 Spindler/Schuster/*Hoffmann*, vor § 7 TMG, Rn. 12.

70 BT-Drs. 14/6098, S. 23.

71 Spindler/Schuster/*Hoffmann*, § 7 TMG, Rn. 10.

b) Eigene Informationen

Eigene Informationen sind zunächst vom Anbieter selbst erstellte Informationen.[72]

c) Haftung für eigene Informationen

Die Haftung für eigene Informationen, d.h. die Haftung des Content-Providers, der eigene Inhalte und damit eigene Informationen bereithält, richtet sich nach den allgemeinen Grundsätzen des § 7 Abs. 1 TMG.[73] Für eigene zur Nutzung bereitgehaltene Informationen ist ein Diensteanbieter demzufolge nach den allgemeinen Gesetzen verantwortlich. Der Content-Provider wird damit durch das TMG gar nicht privilegiert.[74] Seine Haftung wird ohne Einschränkung durch das TMG von dem jeweiligen Rechtsgebiet, dessen Norm betroffen ist, bestimmt, sei es das Zivilrecht, das öffentliche Recht oder das Strafrecht.[75] Das ist nur logisch, denn derjenige, der eigene verbotene Informationen für andere Teilnehmer bereithält, muss auch für diese zur Verantwortung gezogen werden können. Er ist quasi „Haupttäter".

d) Haftung für Zu-eigen-Gemachte Informationen

Eine Haftung nach den allgemeinen Gesetzen i.S.d. § 7 Abs. 1 TMG kommt darüber hinaus auch für jene Informationen in Betracht, die nicht der Anbieter selbst, sondern durch einen anderen erstellt wurden, die sich der Anbieter jedoch als eigene Informationen zu eigen gemacht. Nach dem Willen des Gesetzgebers soll der Anbieter für ursprünglich fremde Informationen wie für eigene Informationen haften[76], wenn er diese dergestalt bereithält und so in seinen Informationskontext eingebettet hat, dass ein Dritter diese für eigene Informationen des Anbieters halten muss.

Zu der Frage, wann zu eigen gemachte Informationen vorliegen, werden in der Literatur und Rechtsprechung unterschiedliche Ansätze vertreten. Grundsätzlich war jedoch eine Tendenz dahingehend festzustellen, dass dieser Begriff weit auszulegen ist.[77] Zum einen wird auf die Begründung des Gesetzgebers verwiesen, aus der sich ergibt, dass darauf abzustellen sei, auf welche Art und Weise ursprünglich fremde Informationen in einen neuen Kontext einbezogen werden.[78] Sei daraus erkennbar,

---

72 *Hilgendorf/Valerius*, Rn. 199.
73 BT-Drs. 14/6098, S. 23.
74 *Laufhütte/Roggenbuck* LK § 184a, Rn. 14.
75 *Gercke/Brunst*, Rn. 589.
76 BT-Drs. 14/6098, S. 23.
77 Spindler/Schuster/*Hoffmann*, § 7 TMG, Rn. 15.
78 BT-Drs. 13/8153, S. 13.

dass der Anbieter die ursprünglich fremden Inhalte billigt, so mache er sich diese auch zu eigen. Ebenfalls in diese Richtung geht eine in der Literatur vertretene Ansicht, die danach differenziert, ob die fremden Inhalte bewusst ausgewählt und von dem Anbieter übernommen werden.[79] Beiden Ansichten ist entgegenzuhalten, dass eine klare Distanzierung des Anbieters gefordert werden müsste, um eine eindeutige Zuordnung als fremde Inhalte feststellen zu können.[80] Eine Differenzierung allein am Kontext der Verwendung erscheint mit zu vielen Rechtsunsicherheiten belegt. Zudem kann es nicht ausreichend sein, dass der Anbieter von Inhalten – der ansonsten nicht haftungsprivilegiert ist – sich lediglich durch eine Kennzeichnung derselben als fremde Inhalte von einer Verantwortlichkeit freizeichnen kann.[81] Dadurch wäre die rechtliche Regelung quasi ausgehebelt.

Weiter wird daher vertreten, dass auch eine fehlende inhaltliche Distanzierung von Inhalten zu einer Umwandlung ursprünglich fremder in zu eigen gemachte Informationen führen kann.[82] Hierunter ist auch die Meinung zu fassen, die sich an einer bestimmten Zeitspanne orientiert, nach der die fremden Inhalte als gebilligt und daher als zu-eigen-gemacht angesehen werden sollen.[83] Dagegen ist ebenfalls anzuführen, dass es nicht allein auf eine fehlende oder bestehende Distanzierung ankommen kann.

Des Weiteren wird die Auffassung vertreten, dass schon das Unterlassen, fremde Inhalte regelmäßig zu kontrollieren, zu einem Zu-eigen-Machen führen soll.[84] Der Diensteanbieter trage hierfür die Verantwortung. Dieser letztgenannten Ansicht aus der Rechtsprechung, in der sehr extensiv die Voraussetzungen eines Zu-eigen-Machens bejaht werden, ist schon mit dem Wortlaut des Gesetzes nicht vereinbar, denn gem. § 7 Abs. 2 S. 1 TMG sind die Diensteanbieter von einer Pflicht zum proaktiven Suchen nach rechtswidrigen Inhalten freigestellt. Darüber hinaus ist den vorgenannten Ansichten gemein, dass sie von subjektiven Auslegungsgesichtspunkten abhängig sind, was in der Praxis dazu führt, dass sich Beweisprobleme stellen.[85] Diese Ansichten sind somit nicht zielführend.

Eine neuere Ansicht vertritt die Auffassung, dass die Figur des Zu-eigen-Machens von Informationen nach der Umsetzung der ECRL nicht mehr anzuwenden sei, da es nach der ECRL nicht mehr auf die Urheberschaft der Information und auf die Gene-

---

79 *Sieber*, MMR 1998, 438, 443; *Fleschig/Gabel*, CR 1998, 351, 354.
80 *Malek/Popp*, Rn. 80.
81 *Malek/Popp*, Rn. 80.
82 Hoeren/Sieber/Holznagel/*Sieber*, Kap. 19, Rn. 264.
83 Spindler/Schuster/*Hoffmann*, § 7 TMG, Rn. 16.
84 LG Trier, MMR 2002, S. 642 ff; LG Köln, MMR 2003, S. 601 ff.
85 *Hilgendorf/Valerius*, Rn. 200.

rierung als Urheber derselben ankomme, sondern darauf, ob vorliegend eine neue Datei erstellt worden ist.[86] Dies entspricht dem Wortlaut der ECRL, lässt jedoch außer Betracht, dass der Gesetzgeber in seiner Begründung zum TMG bewusst auf die Begründung zum TDG verweist, in der ein Zu-eigen-Machen vorgesehen ist, und somit an dieser Rechtsfigur festhalten möchte.[87]

Auch der Bundesgerichtshof verwendet dementsprechend das Zu-eigen-Machen weiterhin in seiner neueren Rechtsprechung.[88] Ausschlaggebend für den BGH bei der Beurteilung ist eine objektive Sicht auf der Grundlage einer Gesamtbetrachtung aller relevanten Umstände. Der BGH verweist an dieser Stelle ausdrücklich auf die Gesetzesbegründung zum IuKDG und macht damit klar, dass er an der Rechtsfigur des Zu-eigen-Machens festhalten will. Der BGH schränkt sich in dieser neueren Rechtsprechung allerdings dahingehend ein, dass er ein Zu-eigen-Machen lediglich dann annimmt, wenn bzgl. des Zu-eigen-Machens ein positives Handeln des Diensteanbieters vorliegt.[89] Im Falle des Unterlassens einer regelmäßigen Überprüfung der Inhalte verneint er zutreffend mit Blick auf § 7 Abs. 2 S. 1 TMG eine Haftung.

2. Stellungnahme

Dem Willen des Gesetzgebers entsprechend und auch in der Praxis anzuwenden ist somit diejenige Ansicht, die ein *Zu-eigen-Machen* dann annimmt, wenn ein Diensteanbieter die Entwicklung einer Situation zulässt, bei der für einen objektiven Dritten der Anschein entsteht, der Diensteanbieter würde bestimmte Inhalte billigen und wie eigene Inhalte behandeln.[90] Nur diese objektivierte Betrachtung des BGH führt zu einer konkreten Überprüfbarkeit für den Diensteanbieter selbst und die Gerichte im Zweifelsfall.

3. Fremde Informationen

Fremde Informationen liegen im Umkehrschluss dann vor, wenn es sich weder um eigene noch um zu eigen gemachte Informationen handelt. Dies sind daher Informationen eines anderen, bei denen der Diensteanbieter nicht den Anschein generiert, diese seien seine eigenen. Liegen fremde Informationen vor, so muss nach dem TMG die Haftung nach folgenden Kriterien unterschieden werden:

---

86 MüKo-StGB/*Altenhain*, TMG, vor § 7 Rn 21.

87 BT-Drs. 16/3078, S. 15.

88 BGH MMR 2010, 556, 557; Spindler/Schuster/*Hoffmann*, § 7 TMG, Rn. 17.

89 BGH MMR 2009, 752, 753.

90 *Hilgendorf/Valerius*, Rn. 200; Spindler/Schuster/*Hoffmann*, § 7 TMG, Rn. 17.

Geht es um den Zugang zu und die Durchleitung von fremden Informationen, so richtet sich die Haftung nach § 8 TMG. § 9 TMG regelt sodann die Haftung für die kurzzeitige Zwischenspeicherung von fremden Informationen zur Vermittlung schnelleren Zugriffs, das sog. Caching. Die Haftung für das einfache Speichern fremder Informationen, das sog. Hosting, wird von § 10 TMG geregelt.

a) Speicherung fremder Informationen, § 10 TMG

Ein Diensteanbieter, der fremde Informationen auf seinen Servern speichert, ein sog. Host-Service-Provider, ist gem. § 10 TMG privilegiert. Die Privilegierung greift aber nur ein, wenn er entweder von den rechtswidrigen Informationen keine Kenntnis hat gem. § 10 S. 1 Nr. 1 TMG oder er nach Kenntniserlangung umgehend tätig wird, um eine Weiterverbreitung zu verhindern gem. § 10 S. 1 Nr. 2 TMG.

aa) § 10 S. 1 Nr. 1 TMG

Voraussetzung für die Privilegierung nach § 10 S. 1 Nr. 1 TMG ist, dass der Host-Service-Provider keine Kenntnis von den rechtswidrigen Inhalten der bei ihm gespeicherten Informationen hat.

(1) Kenntnis der rechtswidrigen Informationen

Um die Privilegierung aufzuheben, bedarf es im Strafrecht – anders als im Zivilrecht – der positiven Kenntnis der rechtwidrigen Handlung oder Informationen.[91] Allein die bloße Kenntnis von Umständen, die auf rechtswidrige Informationen schließen lassen, reicht ebenso wenig aus wie fahrlässige Unkenntnis.[92] Dies wurde ausdrücklich so vom Gesetzgeber in der Neufassung des TDG durch die Umsetzung der ECRL in nationales Recht in der Gesetzesbegründung festgehalten.[93] Das Erfordernis der positiven Kenntnis des Diensteanbieters ist bereits daran festzumachen, dass der Gesetzgeber bei der Neufassung des TDG im Jahre 2001 ausdrücklich für Schadensersatzansprüche ein „Bekanntsein“ von Tatsachen mit aufnimmt, was dann zu einer Haftung führt.[94] Diese Unterscheidung zwischen Schadensersatzansprüchen und sonstigen Ansprüchen verdeutlicht, dass nur die positive Kenntnis ausreichend

---

91 *Hilgendorf/Valerius*, Rn. 208.

92 *Gercke/Brunst*, Rn.599.

93 BT-Drs. 14/6098, S. 25.

94 Spindler/Schuster/*Hoffmann*, § 10 TMG, Rn. 20.

sein kann. Dafür spricht ebenfalls die Gesetzesbegründung zu § 5 Abs. 4 TDG a.F., die explizit die positive Kenntnis aufführt.[95] Der BGH hat zur Frage der positiven Kenntnis ebenfalls entschieden, dass eine derartige Auslegung des § 10 TMG zur erforderlichen Rechtssicherheit für den Diensteanbieter nach Sinn und Zweck notwendig ist.[96]

(2) Kenntnis der Rechtswidrigkeit der Informationen

Streitig ist die Frage, ob es für die Kenntnis i.S.v. § 10 TMG genügt, dass der Diensteanbieter die rechtswidrigen Informationen kennt oder ob er gerade auch Kenntnis von der Rechtswidrigkeit der Information haben muss. Wie sind die Fälle zu behandeln, in denen er sehr wohl Kenntnis von den Informationen besteht, aber ihre Rechtswidrigkeit nicht erkannt wird? Betrachtet man den Wortlaut der Vorschrift des § 10 S. 1 Nr. 1 TMG so, besteht in der 1. Alternative eine Privilegierung, wenn keine Kenntnis von der rechtswidrigen Handlung besteht. Aus dieser Formulierung kann gefolgert werden, dass zumindest Kenntnis der Rechtswidrigkeit hinsichtlich der Handlung zu verlangen ist.[97] Dies ergibt sich zudem aus der Begründung des Gesetzgebers bei der Umsetzung der ECRL in deutsches Recht im Rahmen des TDG[98], auf die die Begründung zum TMG Bezug nimmt.[99] Nach der 2. Alternative von § 10 Abs. 1 Nr. 1 TMG besteht eine Privilegierung, wenn keine Kenntnis von der Information vorliegt. Es ist daher zu fragen, ob es auch hier darauf ankommt, dass sich die Kenntnis auch auf die Rechtswidrigkeit der Information bezieht. Der Gesetzgeber hält die bloße Kenntnis von Informationen für ausreichend, sofern diese rechtswidrig sind, um eine Kenntnis im Sinne des § 10 S. 1 Nr. 1 TMG zu bejahen.[100]

Nach einer anderen Ansicht soll die Kenntnis der Rechtswidrigkeit weder in Bezug auf Handlungen noch im Hinblick auf Informationen Tatbestandsmerkmal sein. Das Wörtchen „rechtswidrig“ sei nur deshalb als Klarstellung mit in den Normtext aufgenommen, um zu verdeutlichen, dass der Diensteanbieter gerade diejenigen Tatsachen kennen müsse, an welche die Wertung der Rechtswidrigkeit der Tätigkeit oder Information anknüpfe[101] – sozusagen die inkriminierte Handlung oder Information, nicht aber ihre Inkriminierung als solche. Lege man Art. 14 ECRL zugrunde, in welchem auch von der „rechtswidrigen Tätigkeit oder Information“ die Rede ist, so

95 BT-Drs. 13/8153, S. 9.
96 BGH MMR 2004, 166, 167; Spindler/Schuster/*Hoffmann*, § 10 TMG, Rn. 18.
97 MüKo-StGB/*Altenhain*, § 10 TMG, Rn 9.
98 BT-Drs. 14/6098, S. 25.
99 BR-Drs. 556/06, S. 22.
100 *Gercke/Brunst*, Rn. 601.
101 MüKo-StGB/*Altenhain*, § 10 TMG, Rn 9 a.E.

müsse nicht notwendig die Rechtswidrigkeit ein eigenes Tatbestandsmerkmal bilden. Vielmehr böte die ECRL keine Anhaltspunkte dafür, wann eine Information rechtswidrig ist. Dadurch müsste die ECRL mit Hilfe von nationalem Recht ausgelegt werden, was der ECRL als vorgelagerter, supranationaler Haftungsprivilegierung widerspräche.[102] Weiter sei es, sofern es sich um ein eigenes Tatbestandsmerkmal handelt, nur schwer für den Provider – aber auch für Juristen – zu beurteilen, wann tatsächlich eine so eindeutige Fallkonstellation vorliegt, dass tatsächlich von einer Kenntnis der Rechtswidrigkeit auszugehen sei.[103]

Nach einer weiteren und zuzustimmenden Ansicht soll sich das Merkmal der Kenntnis der Rechtswidrigkeit sowohl auf die der Handlung als auch auf die der Informationen beziehen.[104] Nach richtlinienkonformer Auslegung bezieht sich die Kenntnis der Rechtswidrigkeit sowohl auf die Tätigkeit als auch auf die Information. Dies ergibt sich insbesondere auch aus dem Vergleich der spanischen und der französischen Fassung der ECRL, welche die Rechtswidrigkeit auf Handlung und Information beziehen.[105] Der EuGH hat diesen Streitpunkt mit seinem Urteil *Google France and Google* nun geklärt[106]. Das Urteil des EuGH zur Zulässigkeit der Nutzung von sog. *AdWords*[107] stellt zwischenzeitlich klar, dass der Host-Service-Providers die Privilegierung nur verliert, wenn er gerade von der Rechtswidrigkeit der Informationen oder Handlungen Kenntnis hat.[108] Dieser Auffassung des EuGH hat sich auch der BGH angeschlossen[109]. Voraussetzung ist somit nicht nur positive Kenntnis der Handlung oder Information, sondern auch die positive Kenntnis der Rechtswidrigkeit. Die Privilegierung greift damit auch dann ein, wenn zwar Handlung oder Information positiv bekannt sind, der Host-Service-Provider deren Rechtswidrigkeit aber nicht positiv erkennt.

(3) Bezugspunkt der Kenntnis

Nachdem nun auch obergerichtlich geklärt ist, dass Voraussetzung für das Entfallen der Privilegierung des Host-Service-Providers das Vorliegen positiver Kenntnis der Rechtswidrigkeit ist, muss auch dieser Begriff der positiven Kenntnis ausgefüllt

---

102 MüKo-StGB/*Altenhain*, § 10 TMG, Rn 10.

103 MüKo-StGB/*Altenhain*, § 10 TMG, Rn 10 a.E.

104 *Valerius* BeckOK-StGB, Providerhaftung, Rn. 23.

105 *Gercke/Brunst*, Rn. 601.

106 Rechtssache des EuGH, *Google France and Google,* C-236/08 = MMR 2010, 315

107 AdWords bezeichnet eine schlüsselwortbasierte Werbemöglichkeit des Suchmaschinenanbieters Google, bei der anhand von gekauften Schlüsselwörtern (Keywords), die Suchanfragen der Nutzer mit Werbeanzeigen (Adverts) verknüpft werden (Adverts + Keywords = AdWords).

108 *Fitzner*, MMR 2011, 83, 85.

109 BHG - *Vorschaubilder* - NJW 2010, 2731 ff.

werden. Es stellt sich die Frage, ab wann der Host-Service-Provider positive Kenntnis der rechtswidrigen Handlungen oder Inhalte hat.

Die positive Kenntnis der rechtswidrigen Handlung oder Information muss sich auf konkrete Details beziehen.[110] Zudem muss dem Diensteanbieter die genaue Fundstelle der rechtswidrigen Inhalte bekannt sein.[111] Nicht ausreichend ist die Kenntnis, dass irgendwo auf dem Server rechtswidrige Informationen liegen. Dies deshalb, weil an dieser Stelle die Privilegierung des § 10 TMG sonst die Privilegierung des § 7 Abs. 2 S. 1 TMG, dass keine Verpflichtung für proaktives Suchen nach rechtswidrigen Informationen besteht, aushebeln würde. [112] Die Art der Kenntniserlangung des Diensteanbieters von den rechtswidrigen Inhalten ist unerheblich. Er kann die Kenntnis auch durch Dritte erworben haben.[113]

(4) Zurechnung von Wissen

Nachdem es sich bei den Diensteanbietern, den Host-Service-Providern, meist um Unternehmen handelt, stellt sich die Frage, inwiefern Wissen zugerechnet werden kann. Grundsätzlich sind hier die allgemeinen Grundsätze zur Wissenszurechnung in Unternehmen bzw. arbeitsteiligen Organisationen sowie der Rechtsgedanke des § 166 BGB anzuwenden.[114] Dem steht nicht entgegen, dass Art. 14 ECRL die tatsächliche Kenntnis des Diensteanbieters fordert. Würde eine Wissenszurechnung in diesem Rahmen nicht stattfinden, so würde die Haftungsprivilegierung zu weit greifen, der Diensteanbieter wäre auch bei positiver Kenntnis seiner Mitarbeiter oder von den handelnden Organen privilegiert. Dies würde eine übermäßige Ausdehnung der Haftungsprivilegierung darstellen.[115]

bb) Haftungsprivilegierung bei Kenntnis, § 10 S. 1 Nr. 2 TMG

Erlangt der Host-Service-Provider von den rechtswidrigen Inhalten Kenntnis, entfällt seine Haftungsprivilegierung nach § 10 S. 1 Nr. 1. Gemäß § 10 S. 1 Nr. 2 TMG bleibt ihm seine Haftungsfreistellung dann erhalten, wenn er unverzüglich tätig wird, um die rechtswidrigen Informationen zu entfernen oder den Zugang zu ihnen zu sperren. In diesem Fall der Kenntnis ist der Diensteanbieter verpflichtet, aktiv tätig

---

110 *Gercke/Brunst*, Rn. 600.
111 Spindler/Schuster/*Hoffmann*, § 10 TMG, Rn. 19.
112 *Hilgendorf/Valerius*, Rn. 208, m.w.N.
113 Spindler/Schuster/*Hoffmann*, § 10 TMG, Rn. 26; *Gercke/Brunst*, Rn. 597, *Malek/Popp*, Rn. 88 f.
114 MüKo-StGB/*Altenhain*, § 10 TMG, Rn. 18.
115 MüKo-StGB/*Altenhain*, § 10 TMG, Rn. 19.

zu werden und gegen die rechtswidrigen Informationen auf seinen Servern etwas zu unternehmen. Grundsätzlich besteht gemäß § 7 Abs. 2 S. 1 TMG keine Verpflichtung zum proaktiven Tätigwerden des Diensteanbieters. Erhält er jedoch Kenntnis von den rechtswidrigen Informationen, so hat er nun gem. § 10 S. 1 Nr. 2 TMG die Pflicht, aktiv tätig zu werden, sofern er seine Haftungsprivilegierung erhalten möchte.[116] Die Kenntnis von rechtswidrigen Informationen muss sich auch in diesem Falle – wie in § 10 S. 1 Nr. 1 TMG – wiederum auf positive Kenntnis, d.h. auf konkrete Details zu den Informationen sowie deren Speicherort beziehen.[117]

(1) Tätigwerden

Der Diensteanbieter muss, um in den Genuss der Privilegierung zu gelangen, lediglich tätig werden, d.h. den Versuch einer Löschung oder Sperrung unternehmen. Auf den tatsächlichen Erfolg der Maßnahmen – d. h. Entfernen der Inhalte oder Sperrung dieser beizeiten – kommt es nicht an. Dies ergibt sich schon aus der Formulierung des Gesetzestextes, der ein Tätigwerden mit dem Ziel des Entfernens oder Sperrens genügen lässt und nicht die tatsächliche Entfernung oder Sperrung verlangt.[118]

Das nicht von einem Erfolg gekrönte Tätigwerden reicht jedoch nur dann, sofern die vorgenommene Maßnahme zur auch geeignet war zu verhindern, dass die Inhalte weiterhin eingesehen werden können.[119] Die unternommene Maßnahme muss demnach so gestaltet sein, dass im Falle ihres Erfolges die Inhalte auch tatsächlich nicht mehr aufgerufen werden können. Von vornherein offensichtlich unzureichende Maßnahmen können den Host-Servide-Provider nicht mehr in den Genuss der Privilegierung bringen.

(2) Unverzügliches Tätigwerden

Der Diensteanbieter muss zudem unverzüglich tätig werden, d. h. ohne schuldhaftes Zögern.[120] Da die ECRL für das Tatbestandsmerkmal „unverzüglich“ keine Regelung aufweist, ist die Auslegung anhand § 121 Abs. 1 S. 1 BGB vorzunehmen. Dies verpflichtet den Diensteanbieter somit grundsätzlich zu einem Tätigwerden direkt nach Kenntniserlangung.[121] Meist stellt das Löschen oder die Sperrung von Inhalten,

---

116 *Gercke/Brunst*, Rn. 602.
117 MüKo-StGB/*Altenhain,* § 10 TMG, Rn. 23.
118 *Hilgendorf/Valerius*, Rn. 207.
119 MüKo-StGB/*Altenhain*, § 10 TMG, Rn. 24.
120 *Gercke/Brunst*, Rn. 602.
121 MüKo-StGB/*Altenhain,* § 10 TMG, Rn. 26.

d. h. von Dateien auf Servern keine mit großem Aufwand verbundene Handlung dar, sodass im Zweifelsfall der Host-Service-Provider sofort tätig werden kann und muss.

(3) Möglichkeit und Zumutbarkeit

Die Privilegierung nach § 10 TMG bleibt darüber hinaus auch dann bestehen, wenn dem Host-Service-Provider eine Entfernung oder Sperrung der rechtswidrigen Informationen nicht möglich oder unzumutbar ist. Die tatsächliche Möglichkeit der Entfernung oder Sperrung hängt in hohem Maße vom vorherrschenden Stand der Technik ab, der dies entweder zulässt oder nicht.[122] Auch im TMG gilt der Grundsatz „ultra posse nemo obligatur" – das Recht darf (technisch) Unmögliches oder Unzumutbares nicht verlangen.[123] Diese Herleitung aus dem allgemeinen Grundsatz war in § 5 TDG a.F. noch explizit geregelt. Die neue Regelung ohne diesen Zusatz im TMG soll jedoch nichts an dessen Gültigkeit ändern. Vielmehr ist diese den Regelungen der ECRL geschuldet und der Gesetzentwurf zum TDG im Jahre 2001 nimmt auf die Regelung des § 5 TDG a.F. explizit Bezug.[124] Ausgangspunkt für diese Regelung ist der über allem stehende Grundsatz, dass Strafrecht Handlungsstrafrecht und kein Gesinnungstrafrecht ist und daher nur das bestrafen kann, was jemand ändern oder verhindern kann.

cc) Ausschluss der Privilegierung, § 10 S. 2 TMG

Ein Diensteanbieter kann sich nicht auf die Privilegierung gem. § 10 S. 1 TMG berufen, wenn der Nutzer ihm gemäß § 10 S. 2 TMG untersteht oder er diesen beaufsichtigt und dieser die rechtswidrigen Informationen speichert oder die rechtswidrige Handlungen begeht. Wie ein Unterstehen eines Nutzers bzw. das Beaufsichtigen von Nutzern nach § 10 S. 2 TMG zu definieren ist, ergibt sich weder aus der Gesetzesbegründung zum TMG, noch aus der ECRL selbst.[125] Geht man vom Wortsinn der Begriffe „unterstehen" und „beaufsichtigen" aus, so ist mit dem Wort „unterstehen" grundsätzlich ein länger anhaltender Zustand zu verbinden, mit dem Wort „beaufsichtigen" eine punktuelle Situation gemeint.[126] Der Diensteanbieter muss sich gegenüber dem Nutzer in einer derart übergeordneten Position befinden, dass er über den Nutzer Einfluss auf die Speicherung fremder Informationen nehmen kann. Da

---

122 *Malek/Popp*, Rn. 90 ff.
123 *Hilgendorf/Valerius*, Rn. 209.
124 BT-Drs. 14/6098, S. 25.
125 MüKo-StGB/*Altenhain*, § 10 TMG, Rn. 28.
126 Spindler/Schuster/*Hoffmann*, § 10 TMG, Rn. 48.

eine Privilegierung gemäß Erwägungsgrund 42[127] der ECRL grundsätzlich nur dann eintreten soll, wenn es sich nur um eine rein technische Informationsdurchleitung oder Informationsspeicherung handelt, ist § 10 S. 2 TMG dahingehend zu verstehen, dass hier der Diensteanbieter auf den Nutzer soweit Einfluss nehmen können muss, dass von einer lediglich technischen, automatisierten und teilweise unkontrollierbaren Speicherung nicht mehr auszugehen ist.[128]

Der Diensteanbieter muss somit ein Weisungsrecht gegenüber dem Nutzer haben. Nach dem BGH besteht der Grund für die Privilegierung darin, dass der Host-Service-Provider aufgrund der Unüberschaubarkeit der in der Masse zu verarbeitenden Informationen privilegiert sein soll. Diese Privilegierung entfällt daher, wenn der Host-Service-Provider auf den Nutzer Einfluss nehmen kann und dadurch eine Unüberschaubarkeit der zu verarbeitenden Informationen nicht mehr gegeben ist.[129]

An dieser Stelle ist auch eine Abgrenzung dahingehend vorzunehmen, ob es sich bei den von den beaufsichtigten oder unterstehenden Nutzern gespeicherten Daten noch um fremde oder möglicherweise auch um sich zu eigen gemachte Informationen handelt, mit der Konsequenz, dass dann die Privilegierung nach § 10 TMG überhaupt nicht mehr eingreifen kann, sondern vielmehr eine unbeschränkte Haftung nach den allgemeinen Gesetzen gem. § 7 Abs. 1 TMG einschlägig wäre. Ausschlaggebend für das Vorliegen fremder oder zu eigen gemachter Informationen ist demnach die Intensität und die Reichweite der Einflussnahme des Host-Service-Providers auf die vom Nutzer gespeicherten Daten.[130] Hat der Diensteanbieter auf den Nutzer derart Einfluss genommen und damit die technische Speicherung zu einer untechnischen, d.h. bewussten Speicherung gemacht, so ist § 10 S. 2 TMG einschlägig und der Diensteanbieter haftet unprivilegiert als wären es nicht fremde, sondern eigene Informationen.

---

127 Erwägungsgrund 42: *„Die in dieser Richtlinie hinsichtlich der Verantwortlichkeit festgelegten Ausnahmen decken nur Fälle ab, in denen die Tätigkeit des Anbieters von Diensten der Informationsgesellschaft auf den technischen Vorgang beschränkt ist, ein Kommunikationsnetz zu betreiben und den Zugang zu diesem zu vermitteln, über das von Dritten zur Verfügung gestellte Informationen übermittelt oder zum alleinigen Zweck vorübergehend gespeichert werden, die Übermittlung effizienter zu gestalten. Diese Tätigkeit ist rein technischer, automatischer und passiver Art, was bedeutet, daß der Anbieter eines Dienstes der Informationsgesellschaft weder Kenntnis noch Kontrolle über die weitergeleitete oder gespeicherte Information besitzt.“*

128 MüKo-StGB/*Altenhain*, § 10 TMG, Rn. 28.

129 BGH MMR 2004, 166; Spindler/Schuster/*Hoffmann*, § 10 TMG, Rn. 49.

130 Spindler/Schuster/*Hoffmann*, § 10 TMG, Rn. 48.

b) Zwischenspeicherung fremder Informationen, § 9 TMG

§ 9 TMG privilegiert die Zwischenspeicherung zur beschleunigten Übermittlung von Informationen, d.h. von einem Haftungsausschluss profitiert auch das sog. Caching – das Einschalten von Proxy-Cache-Providern. Es werden hier auf Proxy-Servern Zwischenspeicherungen vorgenommen, um die Übermittlung fremder Informationen an andere Nutzer auf deren Anfrage hin effizienter zu gestalten. Dies ist insbesondere bei häufig genutzten Informationen der Fall. So muss bei der Übermittlung nicht jedes Mal auf den Content-Provider zurückgegriffen werden, der seine Server bzw. Host-Server ggf. am anderen Ende der Welt stehen hat. Beim Caching bzw. bei der Nutzung von Proxy-Servern werden die Daten des Content-Providers beim ersten Abrufen für den Nutzer auf einem dem Standort des Nutzers "näher" liegenden Server gespeichert und von dort abgerufen.[131] Es handelt sich hierbei um eine wirtschaftlich motivierte Zwischenspeicherung der Informationen, denn die Diensteanbieter müssten beim Abruf von Informationen ein volumenabhängiges Entgelt entrichten, welches mittels Caching reduziert werden kann.[132] Zudem wird, was für den Nutzer ausschlaggebend ist, die Ladezeit der abgerufenen Informationen durch das Caching bzw. das Einsetzen von Proxy-Cache-Servern verkürzt, weil der "Übertragungsweg" verkürzt ist.[133]

§ 9 TMG privilegiert die automatische Zwischenspeicherung, d.h. diejenige, bei welcher der technische Speichervorgang an sich ohne Kenntnis der Einflussmöglichkeit des Diensteanbieters abläuft.

aa) Zeitlich begrenzte Zwischenspeicherung

Voraussetzung für die Privilegierung ist, dass es sich um eine zeitlich begrenzte Zwischenspeicherung handelt. Wie diese zeitliche Begrenzung auszusehen hat, wird weder in der Gesetzesbegründung noch in der ECRL näher definiert. Auf der einen Seite lässt sich § 9 TMG bzgl. des Merkmals der zeitlichen Begrenzung von § 10 TMG sowie § 8 Abs. 2 TMG abgrenzen. § 8 Abs. 2 TMG spricht von einer kurzfristigen Zwischenspeicherung, d. h. es ist bei dieser auf den einmaligen Durchleitungs- bzw. Kommunikationsvorgang abzustellen.[134] Die Zwischenspeicherung gem. § 9 TMG dient somit dem Zugriff vieler verschiedener Nutzer und ist nicht nur für den einzelnen Übertragungsvorgang an sich relevant. Auf der anderen Seite ist § 9 TMG

---

131 *Hilgendorf/Valerius*, Rn. 181.
132 *Gercke/Brunst*, Rn. 21.
133 *Haug*, Rn. 279.
134 *Gercke/Brunst*, Rn. 623.

von § 10 TMG abzugrenzen. Wenn es sich um eine dauerhafte Speicherung von Daten handelt, so richtet sich die Haftung nach § 10 TMG nach der eines Host-Service-Providers.[135]

Die zeitliche Dimension der Zwischenspeicherung, die von § 9 TMG umfasst wird, ist somit nicht genauer zu fassen, als dass sie auf der einen Seite nicht dauerhaft sein darf und auf der anderen Seite jedoch eine mehr als kurzfristige Speicherung sein muss. Es ist davon auszugehen, dass eine kurzfristige Zwischenspeicherung gem. § 8 Abs. 2 TMG nur den Zeitraum umfasst, den eine Datenübertragung durchschnittlich benötigt.[136] Dies werden meist nur wenige Stunden sein.[137] Der Zeitraum, den § 9 TMG umschreibt, ist demgegenüber von längerer Dauer. Geht man vom Sinn der Proxy-Cache-Provider aus, so wäre dort eine nur kurzfristige – möglicherweise an § 8 Abs. 2 TMG orientierte – Speicherdauer nicht zielführend, denn es kommt gerade darauf an, Übertragungswege zu verkürzen und dadurch die Übertragungsgeschwindigkeit dauerhaft zu erhöhen. Dies kann nur durch ein längeres Vorhalten oft genutzter Webseiten herbeigeführt werden.[138]

Um in den Genuss der Haftungsprivilegierung zu gelangen, muss der Proxy-Cache-Provider zudem die Voraussetzungen des § 9 S. 1 Nr. 1–5 TMG erfüllen.

bb) Keine Veränderung der Information

Gemäß § 9 S. 1 Nr. 1 TMG darf der Diensteanbieter die Informationen nicht verändern. Die Informationen, die zwischengespeichert werden, müssen „in jedem Moment dem Original entsprechen."[139] An dieser Stelle muss jedoch unterschieden werden: Der Diensteanbieter darf die Informationen nicht inhaltlich verändern. Kommt es jedoch zu einer technisch bedingten Veränderung durch die Zwischenspeicherung, so ist diese unbeachtlich und hebt die Privilegierung in der Folge nicht auf. Dies ergibt sich aus Erwägungsgrund 43[140] der ECRL.[141]

---

135 MüKo-StGB/*Altenhain,* § 9 TMG, Rn. 11.

136 *Hilgendorf/Valerius*, Rn. 224 f.

137 BT-Drs. 13/7385, S. 20; *Malek/Popp*, Rn. 103, m.w.N.

138 *Malek/Popp*, Rn. 104; *Hilgendorf/Valerius*, Rn. 226.

139 BT-Drs. 14/6098, S. 25.

140 Erwägungsgrund 43: *„Ein Diensteanbieter kann die Ausnahmeregelungen für die „reine Durchleitung" und das „Caching" in Anspruch nehmen, wenn er in keiner Weise mit der übermittelten Information in Verbindung steht. Dies bedeutet unter anderem, daß er die von ihm übermittelte Information nicht verändert. Unter diese Anforderung fallen nicht Eingriffe technischer Art im Verlauf der Übermittlung, da sie die Integrität der übermittelten Informationen nicht verändern."*

141 MüKo-StGB/*Altenhain*, § 9 TMG, Rn. 13.

cc) Aufrechterhaltung der ursprünglichen Zugangsbedingungen

Zudem muss der Diensteanbieter gemäß § 9 S. 1 Nr. 2 TMG die Bedingungen für den Zugang zu den Informationen beachten, d.h. der Diensteanbieter darf durch das Caching bzw. das Speichern auf Proxy-Cache-Servern Zugangskontrollen und Zugangsbedingungen, die der Content-Provider aufgestellt hat, nicht unterlaufen.[142]

dd) Bereithalten der aktuellsten Version

Weiter muss der Diensteanbieter gemäß § 9 S. 1 Nr. 3 TMG die Regeln für die Aktualisierung der Informationen beachten, die als derzeit gängige Industriestandards festgelegt sind. Da der Diensteanbieter gemäß § 9 S. 1 Nr. 1 TMG die Informationen nicht verändern darf, muss er dafür sorgen, dass der Nutzer, der die betreffenden Inhalte abruft, auch immer die aktuelle Version der beim Content-Provider vorliegenden Informationen erhält. Würde über den Proxy-Cache-Server keine aktuelle Version der abgerufenen Informationen bereit gehalten, würde dies dem Sinn und Zweck des Caching widersprechen. Der Nutzer soll, auch wenn er lediglich eine Kopie der Informationen vom Proxy-Cache-Server abruft, immer die aktuellen Informationen des Content-Providers erhalten.[143]

ee) Keine Beeinträchtigung der wirtschaftlichen Auswertung

Darüber hinaus darf der Diensteanbieter gemäß § 9 S. 1 Nr. 4 TMG die erlaubte Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Informationen nicht beeinträchtigen. Hier stellt der Gesetzgeber insbesondere auf Zugriffszähler und Cookies ab, d.h. die Content-Provider sollen davor geschützt werden, dass die Anzahl der Aufrufe ihrer Seiten durch die Nutzung von Proxy-Cache-Servern verzerrt wird und dem Content-Provider durch falsche Zugriffszahlen Nachteile entstehen. Ebenso verhält es sich bei dem Einsatz von Cookies. Werden diese Programme zur Überwachung des Nutzerverhaltens vom Content-Provider eingesetzt, so muss gewährleistet sein, dass dies durch den Einsatz eines Proxy-Cache-Servers nicht unterbunden wird, um dem Content-Provider die durch das Cookie aufgezeichneten Daten nicht vorzuenthalten. Diese Regelung erklärt sich insbesondere vor dem Hintergrund, dass sich Internetinhalte meist über Werbung finanzieren

142 *Hilgendorf/Valerius*, Rn. 228, m.w.N.
143 BT-Drs. 14/6098, S. 25; *Gercke/Brunst*, Rn. 626.

und sich die Höhe der Werbeeinnahmen nach der Zahl der Zugriffe auf die bestimmten Websites richtet.[144]

ff) Reagieren bei Kenntnis von Sperrung oder Entfernung

Des Weiteren muss der Diensteanbieter gemäß § 9 S. 1 Nr. 5 TMG unverzüglich Informationen entfernen oder den Zugang zu diesen sperren, sobald er Kenntnis davon erlangt hat, dass die Informationen am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt wurden, der Zugang zu ihnen gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat. Hier ist ebenso wie bei § 10 TMG positive Kenntnis erforderlich.[145] Die Voraussetzungen entsprechen denen des § 10 TMG. Insbesondere muss die Entfernung oder Sperrung dem Diensteanbieter auch technisch möglich und zumutbar sein.[146]

gg) Ausschluss bei kollusivem Zusammenwirken

Darüber hinaus stellt § 9 S. 2 TMG – bezugnehmend auf § 8 Abs. 1 S. 2 TMG klar – dass, sobald der Diensteanbieter mit den Nutzern kollusiv zusammenarbeitet, um rechtswidrige Handlungen zu begehen, der Diensteanbieter seiner Privilegierung verlustig geht. Ist dies der Fall, so handelt es sich auch schon nicht mehr um eine automatische Zwischenspeicherung gemäß § 9 S. 1 TMG.[147]

c) Durchleitung fremder Informationen, § 8 TMG

Diensteanbieter, die fremde Informationen in einem Kommunikationsnetz übermitteln oder den Zugang zu diesen Informationen vermitteln, werden gemäß § 8 Abs. 1 TMG privilegiert. Diese Privilegierung betrifft insbesondere Access- bzw. Network-Provider. Die Diensteanbieter sind gem. § 8 Abs. 1 TMG privilegiert, wenn die Durchleitung rein technischer, automatischer und passiver Art ist und sie in keiner Weise mit der übermittelten Information in Verbindung stehen.[148] Diese Art der Privilegierung entspricht wieder dem Grundsatz der ECRL, nach dem auf den techni-

---

144 MüKo-StGB/*Altenhain*, § 9 TMG, Rn. 16; *Gercke/Brunst*, Rn. 624.

145 MüKo-StGB/*Altenhain*, § 9 TMG, Rn. 18; *Gercke/Brunst*, Rn. 627.

146 *Malek/Popp*, Rn. 105; *Hilgendorf/Valerius*, Rn. 231 a.E.

147 MüKo-StGB/*Altenhain*, § 9 TMG, Rn. 20.

148 BT-Drs. 14/6098 S. 24; vgl. ebenso *Paul*, Primärrechtliche Regelungen zur Verantwortlichkeit von Internetprovidern aus strafrechtlicher Sicht, S. 126 ff.

schen Verarbeitungsvorgang abstellt wird.[149] Die Haftungsprivilegierung gemäß § 8 Abs. 1 S. 1 TMG ist nur anzuwenden, sofern die Nummern 1–3 erfüllt sind.

aa) Keine Übermittlungsveranlassung

Der Diensteanbieter darf die Übermittlung der Informationen nicht veranlasst haben gem. § 8 Abs. 1 S. 1 Nr. 1 TMG, d.h. er darf zu diesen keinerlei Bezug haben.[150] Die Übermittlung von Daten muss aufgrund der Veranlassung durch einen Nutzer entstanden sein.[151] Hat der Diensteanbieter die Übermittlung veranlasst, so handelt es sich nicht mehr um eine lediglich technische und automatisierte Durchleitung von Daten, denn dann wurde vom Access-Provider aktiv in den technischen Übermittlungsprozess eingegriffen und dieser verändert.[152]

bb) Keine Auswahl des Adressaten der übermittelten Informationen

Zudem darf der Diensteanbieter den Adressaten, an den die Informationen übermittelt werden sollen, nicht ausgewählt haben, will er die Privilegierung nicht verlieren, § 8 Abs. 1 S. 1 Nr. 2 TMG. Auch hier muss die Auswahl des Adressaten ausschließlich vom Nutzer ausgehen. Der Diensteanbieter darf auf den Entschluss des einzelnen Nutzers keinen Einfluss nehmen, an wen die Informationen übermittelt werden sollen.[153] Durch diese Regelung entfällt für Dienstleistungen, die eine Filter- oder Blockierungsfunktion mitumfassen, die Privilegierung nach § 8 Abs. 1 S. 1 Nr. 2 TMG, da hier ein bewusster Eingriff des Diensteanbieters in den Übertragungsvorgang vorliegt.

cc) Keine Auswahl oder Veränderung der vermittelten Informationen

Des Weiteren darf der Diensteanbieter gemäß § 8 Abs. 1 S. 1 Nr. 3 TMG die übermittelte Information nicht ausgewählt oder verändert haben. Auch bei derartigem Verhalten wird der Diensteanbieter seiner passiven Rolle nicht gerecht und es

---

149 Erwägungsgründe 42 (Fn. 127) und 43 (Fn. 140) der ECRL.
150 Spindler/Schuster/*Hoffmann*, § 8 TMG, Rn. 21, m.w.N.
151 MüKo-StGB/*Altenhain*, § 8 TMG, Rn. 7.
152 *Gercke/Brunst*, Rn. 613.
153 MüKo-StGB/*Altenhain*, § 8 TMG, Rn. 8.

fehlt somit an einer rein technischen und automatischen Tätigkeit passiver Art, d.h. an der bloßen technischen Vermittlerrolle ohne Einwirkung auf die Informationen.[154]

dd) Ausschluss bei kollusivem Zusammenwirken

Gemäß § 8 Abs. 1 S. 2 TMG ist die Privilegierung der Durchleitung von Informationen auch dann ausgeschlossen, wenn der Diensteanbieter mit dem Nutzer kollusiv, d.h. absichtlich zusammenarbeitet, um rechtswidrige Handlungen zu begehen. Den Formulierungen „absichtlich" sowie „um zu" ist zu entnehmen, dass hier lediglich dolus directus ersten Grades ein kollusives Zusammenwirken begründet.[155] Ist dies gegeben, so besteht keine Veranlassung, den Access-Provider zu privilegieren.

ee) Haftung bei Kenntnis der rechtswidrigen Informationen

Keine Regelung zum Ausschluss der Haftungsprivilegierung gemäß § 8 TMG besteht für den Fall, dass der Access-Provider Kenntnis der rechtswidrigen Informationen erlangt, ähnlich wie zum Beispiel im Falle des Host-Providers. Heute wird es immer schwieriger, rechtswidrige Informationen und Handlungen im Internet zu verfolgen, denn die Host-Provider können ihre Server überall auf der Welt vorhalten und die Content-Provider können die von ihnen erzeugten Inhalte von überall auf der Welt ins Internet einstellen, wodurch sie für die Strafverfolgungsbehörden nur schwer greifbar sind.

Der Access-Provider hingegen, der dem Internetnutzer den lokalen Zugang zum Internet verschafft, ist von dieser Ungebundenheit weit weniger betroffen. Er ist auf die Ressourcen an dem Ort angewiesen, an dem er dem Nutzer den Zugang zum Internet eröffnet und muss daher vor Ort seine Dienste erbringen. Daher erscheint es sinnvoll und gleichzeitig notwendig, die Privilegierung des Access-Providers für den Fall zu hinterfragen, wenn er Kenntnis von der Rechtswidrigkeit der Informationen erhält, deren Transport er ermöglicht, vorausgesetzt ihm ist ein Einschreiten möglich.

Es ist höchst umstritten, ob die Privilegierung des Access-Providers entfallen soll, wenn er positive Kenntnis von der Durchleitung von rechtswidrigen Informationen erhält und er trotz einer Verhinderungsmöglichkeit ein Einschreiten unterlässt. In Betracht käme in diesem Fall eine Haftung des Access-Providers nach den allgemeinen Gesetzen bei entsprechender Anwendung des § 7 Abs. 2 S. 2 TMG.

---

154 *Gercke/Brunst*, Rn. 613.

155 MüKo-StGB/*Altenhain*, § 8 TMG, Rn. 11; *Kudlich* in JA 2002, 798, 801.

Diese Frage nach einer Haftung des Access-Providers soll an dieser Stelle zunächst unbeantwortet bleiben, um dann im Teil 4 der vorliegenden Arbeit umfassend vertieft und behandelt zu werden.

4. Zusammenfassung

Der Gesetzgeber hat nicht zuletzt unter europarechtlichem Einfluss und Vorgaben ein differenziertes Haftungssystem für die bestehenden Providerarten geschaffen. Dieses orientiert sich an deren originären Aufgaben und der Qualifizierung der durchgeleiteten Informationen als eigene, fremde oder zu-eigen-gemachte. Auch zukünftig wird diese Unterscheidung fortsetzen, wenn es im IoT-Umfeld um die Frage des Dateneigentums und die sich daraus ergebenden Rechte und Pflichten drehen wird.

Teil 2: Aktuelle Haftungsprobleme

Im Folgenden soll betrachtet werden, wie anhand der oben dargestellten Haftungssystematik, einzelne Fallgruppen zu behandeln sind unter Einbeziehung der aktuellen Rechtsprechung. Hierbei war teilweise auf zivilrechtliche Urteile zurückzugreifen, nachdem es aktuell an strafrechtlichen Urteilen zum TMG mangelt.

Kapitel 1: Hyperlinks

Die Verwendung von Hyperlinks ist von herausragender Bedeutung, da sich heutzutage jede Seite im Internet der Verweistechnik durch Hyperlinks bedient, um auf eigene oder dritte Informationsangebote zu gelangen.[156] Ein Hyperlink ist eine inhaltliche Verknüpfungen zwischen der Ausgangswebseite und einer – eigenen oder dritten – Verweisseite im Internet. Durch das Setzen von Verweisankern im Quelltext des HTML-Dokuments wird ein Hyperlink erzeugt. Dieser kann auf jegliche Art von Informationen bzw. Inhalte verweisen. Größtenteils wird mit diesem Instrument der Zugriff nicht auf eigene, sondern auf fremde Informationen im Internet ermöglicht.[157]

I. Keine gesetzliche Regelung

Die Haftung für Hyperlinks ist weder im TMG noch in der ECRL geregelt. Obwohl sich die Frage einer nationalen Einzelregelung bereits bei Umsetzung der E-CRL im Jahre 2001 stellte, die eine nationale Regelung zu diesem Problem durchaus erlaubt hätte, hat sich der nationale Gesetzgeber bewusst dagegen entschieden.[158]

1. Regelung in der ECRL

Die ECRL regelt die Haftung für Hyperlinks in den Art. 12–15 ECRL unter dem Abschnitt „Verantwortlichkeit der Vermittler“ nicht. Lediglich in den „Schlussbestimmungen“ bestimmt die ECRL in Art. 21 Abs. 2 ECRL, dass im Rahmen einer Evaluation der ECRL, die nach Art. 21 Abs. 1 ECRL durchzuführen ist, untersucht werden soll, ob eine Regelung bezüglich der Haftung von Verwendern von Hyper-

---

156 *Gercke/Brunst*, Rn. 629.

157 Hoeren/Sieber/Holznagel/*Höflinger*, Kap. 18.1, Rn. 102.

158 BT-Drs. 14/6098, S. 34, 37: entgegen der Empfehlung des Bundesrates, eine Regelung im TMG aufzunehmen, entschied sich der Gesetzgeber aufgrund des komplexen Regelungsinhaltes im Rahmen der Umsetzung der ECRL dagegen; *Hilgendorf/Valerius*, Rn. 178, m.w.N.

links erforderlich ist und die Richtlinie in diesem Punkt angepasst werden muss. Bei der Schaffung der ECRL war das Problem der Hyperlinks daher durchaus bekannt.

In ihrem ersten Evaluationsbericht hat die EU-Kommission allerdings lediglich festgestellt, dass durch eine gesetzliche Regelung der Haftung der Verwender von Hyperlinks – wie in einzelnen Mitgliedstaaten geschehen – der Binnenmarkt der europäischen Union nicht gefährdet sei.[159] Hintergrund hierfür war, dass Mitgliedsländer wie Österreich, Portugal und Spanien bei der Umsetzung in den nationalen Gesetzen Regelungen im Hinblick auf die Haftung für Hyperlinks geschaffen hatten, nachdem die Richtlinie keine Vollharmonisierung der Rechtslage in der Europäischen Union herbeigeführt hatte.[160]

2. Gesetzgebungsverfahren in Deutschland

Der deutsche Gesetzgeber hat, wie der Begründung zum TDG zu entnehmen ist, lediglich die Regelungen aus der ECRL, d.h. die Art. 12–15 ECRL, übernommen und diese bewusst nicht erweitert.[161] Der Bundesrat hatte zuvor im Gesetzgebungsverfahren zu den §§ 8–11 TDG n.F., bei dem die ECRL umgesetzt werden sollte, eine Regelung zur Haftung für Hyperlinks gefordert, da er eine Klärung durch den Gesetzgeber aufgrund der uneinheitlichen Behandlung in der Rechtsprechung und Lehre für geboten hielt.[162] Die Einführung einer nationalen Regelung, wie sie andere Mitgliedstaaten getroffen hatten, lehnte die Bundesregierung und mit ihr der Bundestag jedoch ab, da sie im Hinblick auf Art. 21 Abs. 2 ECRL zunächst abwarten wollte, wie sich die Haftung der Verwender von Hyperlinks in Lehre und Rechtsprechung

---

159 Erster Bericht über die Anwendung der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt vom 21.11.2003, S. 15,
online unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0702:FIN:DE:PDF (07.01.2014).

160 Vgl. z.B. § 17 ECG (Österreich), Ausschluss der Haftung bei Links:
(1) Ein Diensteanbieter, der mittels eines elektronischen Verweises einen Zugang zu fremden Informationen eröffnet, ist für diese Informationen nicht verantwortlich,
1. sofern er von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis hat und sich in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird, oder,
2. sobald er diese Kenntnis oder dieses Bewusstsein erlangt hat, unverzüglich tätig wird, um den elektronischen Verweis zu entfernen.
(2) Abs. 1 ist nicht anzuwenden, wenn die Person, von der die Informationen stammen, dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird oder der Diensteanbieter die fremden Informationen als seine eigenen darstellt.

161 MüKo-StGB/*Altenhain*, § 7 TMG, Rn. 54; BT-Drs. 14/6098, S. 37.

162 BT-Drs. 14/6098, S. 34.

weiterentwickelt, um dann auch in diesem Punkt eine einheitliche Regelung auf europäischer Ebene anzustreben.[163]

Darüber hinaus begründete die damalige Bundesregierung die Ablehnung einer Regelung der Frage der Haftung von Verwendern von Hyperlinks mit der Komplexität der damit in Zusammenhang stehenden Fragen, die sich aus der Vielzahl von Verwendungsmöglichkeiten für den Einsatz von Hyperlinks ergibt.[164]

3. Haftung für Hyperlinks nach deutschem Recht

Da der deutsche Gesetzgeber bei der Umsetzung der ECRL und auch bei der Neufassung des TMG im Jahre 2007 keine Veranlassung sah, eine ausdrückliche Haftungsregelung in das TMG mit aufzunehmen, obwohl diese Möglichkeit auch im Rahmen der Umsetzung der ECRL gerade bestanden hätte, steht die Frage immer noch in der Diskussion, nach welchen Vorschriften sich die Haftung für die Verwendung von Hyperlinks richtet. Diskutiert werden im Wesentlichen drei Lösungsansätze: Eine Anwendung der §§ 7–10 TMG direkt, eine analoge Anwendung der §§ 7–10 TMG sowie eine Haftung lediglich nach den allgemeinen Gesetzen in Betracht kommt.

a) Direkte Anwendung der §§ 7–10 TMG

aa) Meinungsstand

Teilweise wird in der Literatur die Ansicht vertreten, dass die §§ 7–10 TMG auf die Haftung für Hyperlinks anzuwenden seien.[165] Die im Rahmen des Gesetzgebungsverfahrens zur Umsetzung der ECRL in nationales Recht getroffene Aussage des Gesetzgebers in der Gesetzesbegründung, die Haftung für Hyperlinks richte sich „nach allgemeinen Vorschriften[166]“, ist der Ausgangspunkt für diese Ansicht. Die „allgemeinen Vorschriften“ sollen demnach auch das TMG bzw. TDG mitumfassen.

Als Argument führt diese Auffassung an, dass zwar die isolierte Betrachtung dieser Aussage auf eine Unanwendbarkeit des TMG schließen lasse, jedoch der Gesetzgeber, gerade im Lichte einer Vollharmonisierung in diesem Bereich, von den allge-

---

163 BT-Drs. 14/6098, S. 37.

164 BT-Drs. 14/6098, S. 37.

165 *Sieber/Liesching*, S. 8; *Kudlich* JA 2002, 798, 803; *Laufhütte/Roggenbuck* LK § 184a, Rn. 14 a.E. – Sie übersehen jedoch, dass das BVerfG in dem stattgebenden Kammerbeschluss vom 08. April 2009 (zit. juris) die Frage der Anwendbarkeit der §§ 8–10 TMG bewusst offen lässt und zudem auf die dies ablehnende h.M. verweist.

166 BT-Drs. 14/6098, S. 37.

meinen Vorschriften des TMG in der Haftungsfrage ausgegangen sei.[167] Dafür spreche auch die Tatsache, dass eine vollständige Ausklammerung der Frage der Haftung für Hyperlinks einer umfassenden Regelung der Haftung von Informations- und Kommunikationsdiensten widerspräche.[168] Dies ergebe sich auch daraus, dass der Gesetzgeber im Rahmen des IuKDG gerade auch von einer Subsumierbarkeit der Haftung für Hyperlinks unter den § 5 Abs. 3 TDG a.F. ausgegangen ist.[169]

bb) Kritik

Die vorgenannte Ansicht ist zu Recht auf kritische Ablehnung gestoßen. Denn, wie sich aus der Gesetzesbegründung zum TDG n.F. ergibt, steht einer Anwendung der §§ 7–10 TMG der klare und ausdrückliche Wille des Gesetzgebers entgegen. Die damalige Bundesregierung hat bei der Umsetzung der ECRL in nationales Recht explizit davon abgesehen, eine Regelung für Hyperlinks mit aufzunehmen.[170] Der Gesetzgeber hat ausdrücklich davon gesprochen, dass, solange eine spezielle Regelung nicht besteht, sich die Verantwortlichkeit nach den allgemeinen Vorschriften richtet[171], er also die Regelungen der §§ 7–10 TMG gerade nicht für einschlägig hält. An dieser Stelle einen derartigen Widerspruch des Gesetzgebers zwischen geschriebener Gesetzesbegründung und dessen tatsächlichem und europarechtlichem Willen erkennen zu wollen, entbehrt jeder Grundlage.[172] Aufgrund dieser Aussage des Gesetzgebers wird eine Anwendung der Haftungsprivilegierungen der §§ 7 ff. TMG auch zu Recht von der herrschenden Meinung auf die Haftung von Verwendern von Hyperlinks nicht abgelehnt.

b) Analoge Anwendung der §§ 7–10 TMG

aa) Meinungsstand

Teilweise wird in der Literatur auch vertreten, dass aufgrund einer Regelungslücke in der ECRL sowie im TMG bzw. TDG hinsichtlich der Haftung von Hyperlinks die §§ 7–10 TMG analog anzuwenden seien.[173] Voraussetzung für eine Analogie ist zum einen eine vergleichbare Interessenlage, bei der der Gesetzgeber im Rahmen einer

---

167 *Sieber/Liesching*, S. 8.
168 BT-Drs. 14/6098, S. 11 f.
169 BT-Drs. 13/8153, S. 13; *Sieber/Liesching*, S. 9.
170 *Haug*, Rn. 344.
171 BT-Drs. 14/6098, S. 37.
172 Müko-StGB/*Altenhain*, vor § 7 TMG, Rn. 55 f.
173 *Liesching*, MMR 2006, 387, 391.

Interessenabwägung unter Berücksichtigung der gleichen Grundsätze wie beim Erlass der Gesetzesvorschrift zu dem gleichen Abwägungsergebnis gekommen wäre[174] und zum anderen das Vorliegen einer planwidrigen Regelungslücke.[175]

Diese Auffassung argumentiert damit, dass eine planwidrige Regelungslücke auch dann vorliege, wenn der Gesetzgeber bewusst eine ausfüllungsbedürftige und ausfüllungsfähige Regelungslücke schaffe. Als Handlungsoptionen des Rechtsanwenders wären dann lediglich ein Umkehrschluss auf die nicht unmittelbar anzuwendenden Vorschriften oder eine Analogie zu den gesetzlichen Vorschriften in Betracht zu ziehen.[176] Maßgeblich für eine inhaltliche Entscheidung zwischen einer der beiden Möglichkeiten sei allein die Regelungsvorstellung des Gesetzgebers sowie die Rechtsähnlichkeit der zu vergleichenden Sachverhalte.[177] Eine analoge Anwendung der §§ 7–10 TMG wird im Hinblick auf diese Kriterien damit begründet, dass aus der Äußerung im Gesetzgebungsverfahren „die weitere Entwicklung in Wissenschaft und Rechtsprechung zu verfolgen“[178], die Intention des Gesetzgebers abzuleiten sei. Darin sei zu erkennen, dass sich der Gesetzgeber gerade nicht gegen eine analoge Anwendung ausspräche, was im Ergebnis zu der Möglichkeit einer analogen Anwendung führe.

bb) Kritik

Diese Ansicht geht jedoch fehl. Eine analoge Anwendung der Vorschriften der §§ 7–10 TMG auf die Haftung von Verwendern von Hyperlinks scheitert daran, dass die Voraussetzungen einer Analogie nicht vorliegen. Schon an einer planwidrigen Regelungslücke fehlt es offensichtlich. Der Gesetzgeber hat bei der Neuschaffung des TMG bewusst auf eine Regelung hinsichtlich der Haftung bei Verwendung von Hyperlinks verzichtet und somit eine gerade nicht planwidrige, sondern vielmehr bewusste Regelungslücke geschaffen.[179] Über diesen ausdrücklich erklärten Willen des Gesetzgebers kann nicht im Wege der Analogie hinweggegangen werden. Zudem verweist der Gesetzgeber eindeutig auf die Haftung nach den allgemeinen Gesetzen.[180] Auch an dieser Stelle ist der ausdrückliche Wille in der Gesetzesbegründung nicht über den Wortlaut hinaus ausdehnbar.[181]

---

174 BGH NJW 2003, 2061, 2063; BGH NJW 1997, 2683.
175 BGH NJW 2003, 2061, 2063; BGH NJW 1981, 1726, 1727.
176 *Sieber/Liesching*, S. 10.
177 *Sieber/Liesching*, a.a.O., m.w.N.
178 BT-Drs. 14/6098, S. 37.
179 Müko-StGB/*Altenhain*, vor § 7 TMG, Rn. 55; Spindler/Schuster/*Hoffmann*, vor § 7 TMG, Rn. 40
180 *Gercke/Brunst*, Rn. 630.
181 Müko-StGB/*Altenhain*, vor § 7 TMG, Rn. 56.

c) Haftung nach den allgemeinen Gesetzen

Die Haftung für die Verwendung von Hyperlinks richtet sich nach der herrschenden Meinung in Lehre und Rechtsprechung nach den allgemeinen Gesetzen.[182] Es seien die allgemeinen Grundsätze des jeweiligen Teils der Rechtsordnung anzuwenden, der gerade betroffen ist, d.h. Zivil-, Straf- oder öffentliches Recht. Im strafrechtlichen Sinne bedeutet dies das Vorliegen von Tatbestand, Rechtswidrigkeit und Schuld. Bei der Frage der strafrechtlichen Haftung der Verwender von Hyperlinks ist daher zu prüfen, ob eine Norm des Strafgesetzbuches oder eine sonstige Strafnorm durch die Verwendung bzw. das Setzen eines Hyperlinks tatbestandlich erfüllt ist.

Im Rahmen der Prüfung, ob der Link-Verwender eine strafbare Handlung begeht, ist zu differenzieren nach der Art des Hyperlinks, da es eine Vielzahl von Möglichkeiten gibt, einen Hyperlink zu setzen. Grundsätzlich kann ein Hyperlink auf eigene Inhalte innerhalb der eigenen Internetseite gesetzt werden oder als Verweis auf eine Internetseite eines Dritten. Wird auf eine fremde Internetseite verwiesen, so muss weiter danach differenziert werden, ob lediglich auf deren Startseite verwiesen wird oder ob ein „Deeplink“ auf bestimmte Informationen gesetzt wird.[183] Es kommt daher bei der Beurteilung der Strafbarkeit darauf an, ob es sich um eigene bzw. zu-eigen-gemachte Informationen des Link-Verwenders handelt und ob ein Straftatbestand erfüllt ist.[184]

II. Haftung für Hyperlinks in der aktuellen Rechtsprechung

Auch die Rechtsprechung geht wie die herrschende Meinung weitgehend davon aus, dass die §§ 7–10 TMG nicht auf die Haftung für Hyperlinks Anwendungen finden. Dies hat schon der BGH in seiner zivilrechtlichen „Schöner Wetten“-Entscheidung[185] im Jahre 2004 so festgehalten, die von der aktuellen Rechtsprechung bestätigt wird.

1. „Schöner Wetten“-Entscheidung

In dieser richtungsweisenden Entscheidung, entschied der Bundesgerichtshof u.a. über die Frage, ob durch das Setzen eines Hyperlinks eine zivilrechtliche Störerhaftung ausgelöst werden kann.

---

182 *Gercke/Brunst*, Rn. 630.
183 *Hilgendorf/Valerius*, Rn. 334.
184 MüKo-StGB/*Hörnle*, § 184, Rn. 48.
185 *Schöner Wetten,* BGH NJW 2004, 2158 ff.

a) Sachverhalt

Das beklagte Verlagshaus berichtete in einem seiner Artikel über ein in Salzburg ansässiges Unternehmen. Hauptgeschäftszweck des Unternehmens war das Anbieten jeglicher kommerzieller Wetten im Internet, darunter insbesondere Sportwetten. Der Bericht der Beklagten erschien auf ihrer Online-Präsenz. Dort war jedoch nicht nur der Artikel der Beklagten einsehbar. Um das Online-Angebot der Beklagten im Gegensatz zum herkömmlichen Druckwerk attraktiver zu gestalten, hatte diese neben dem Artikel einen Hyperlink zu den Angeboten des Unternehmens, über das berichtet wurde, eingefügt. Über den Aufruf des Hyperlinks gelangte man direkt auf die in Deutschland illegalen Angebote des Unternehmens. Eine Lizenz zur Veranstaltung von Wetten dieser Art in Deutschland besaß weder das österreichische Unternehmen noch das beklagte Verlagshaus.

Die Klägerin, die eine entsprechende Lizenz zum Vertrieb von Sportwetten in Deutschland besaß, nahm das Verlagshaus auf Unterlassen des Setzens eines Hyperlinks auf die Webseite des österreichischen Unternehmens in Anspruch.

b) Entscheidung des Bundesgerichtshofs

Die Entscheidung des Bundesgerichtshofs erging noch zum TDG. Im Ergebnis lehnte der BGH einen Unterlassungsanspruch ab. Der BGH hat zur Frage der zivilrechtlichen Störerhaftung entschieden, dass das TDG nicht anwendbar ist, wenn es um die Haftung für das Setzen eines Hyperlinks geht.[186]

Der BGH führt hierbei aus, dass mit der Umsetzung der Richtlinie für den elektronischen Geschäftsverkehr der § 5 TDG a.F. aufgehoben und durch die §§ 8–11 TDG ersetzt worden ist. Diese regeln, genauso wie die ECRL, eine Haftung für Hyperlinks gerade nicht. Der BGH nahm im Rahmen seiner Begründung hierfür ebenfalls Bezug auf die amtliche Gesetzesbegründung und den darin ausgedrückten Willen des Gesetzgebers.

---

[186] *Schöner Wetten,* BGH NJW 2004, 2158, 2160.

2. Entscheidung des OLG Stuttgart

Das OLG Stuttgart äußerte sich in strafrechtlicher Hinsicht im Rahmen einer Revisionsentscheidung, die noch zum TDG erging, im Jahre 2006 zur Anwendbarkeit der §§8–11 TDG im Rahmen der Haftung eines Link-Verwenders.[187]

a) Sachverhalt

Der Angeklagte, ein Anhänger der unbeschränkten Meinungsfreiheit im Internet, betrieb eine Homepage, auf der er auf gesperrte Webseiten sowie geplante Sperrungen von Webseiten hinwies. Im Rahmen der Dokumentation der Sperrtätigkeit der Behörden und im Sinne der von ihm verfochtenen Informationsfreiheit pflegte der Angeklagte diese von ihm entworfene Online-Dokumentation u.a. auch damit, dass er zu den jeweiligen gesperrten Webseiten Hyperlinks setzte, unter deren zu-Hilfe-Nahme die gesperrten Seiten dennoch abrufbar waren. Unter anderem befanden sich unter diesen gesperrten Webseiten auch zwei aus den USA, auf deren Unterseiten Kennzeichen und Symbole der NSDAP und deren Unterorganisationen zu sehen waren. Zudem wurden der Holocaust und die Existenz von Vernichtungslagern geleugnet.

Dem angeklagten Homepagebetreiber waren diese Inhalte bekannt, er billigte sie jedoch nicht. Vielmehr warnte er vor rechtsradikaler Propaganda und setzte zudem Hyperlinks auf Seiten, auf denen eine argumentative Auseinandersetzung mit diesen Inhalten erfolgte.

b) Urteil des OLG Stuttgart

Im Ergebnis sprach das OLG Stuttgart den Angeklagten aufgrund der Sozialadäquanzklausel des § 86 Abs. 3 StGB frei.

Die Anwendbarkeit der §§ 8–11 TDG auf Hyperlinks schloss das OLG Stuttgart aus. Es nahm in seinen Ausführungen Bezug auf die Gesetzesbegründung zum TDG und die vorgenannte *„Schöner Wetten“*-Entscheidung des BGH und kam zu dem Schluss, dass im Falle von Hyperlinks die allgemeinen Gesetze anzuwenden sind.[188] Auch eine analoge Heranziehung der §§ 8–11 TDG lehnte das OLG Stuttgart ab. Es könne eine unbewusst entstandene Regelungslücke durch den Gesetzgeber im Gesetzgebungsverfahren nicht erkennen. Das Gericht führte weiter aus, dass es auch

[187] OLG Stuttgart MMR 2006, 387.
[188] OLG Stuttgart MMR 2006, 387.

eine Vergleichbarkeit der Sachverhalte, d.h. zwischen der Tätigkeit eines Link-Verwenders und eines Providers, nicht gegeben sei. Das OLG Stuttgart prüfte daher im weiteren Verfahrensgang die allgemeinen Vorschriften.[189]

3. Entscheidung des LG Karlsruhe

Das LG Karlsruhe hat sich ebenfalls in einer strafrechtlichen Entscheidung mit der Haftung eines Link-Verwenders befasst. [190] Die Entscheidung erging dort zu den Vorschriften des TMG.

a) Sachverhalt

In der dem LG Karlsruhe zur Entscheidung vorliegenden Sache ging es inhaltlich um die Frage, wann kinderpornographisches Material zugänglich gemacht wird. Die streitgegenständliche Beschwerde richtete sich gegen einen Durchsuchungsbeschluss. Der Angeklagte hatte auf der von ihm betriebenen Webseite eine Verlinkung zu einer Webseite eines Dritten angebracht, die kinderpornographisches Material enthielt.

b) Beschluss des LG Karlsruhe

Das Landgericht Karlsruhe stellte in seinem Beschluss darauf ab, dass sich der Betreiber einer Homepage mit dem gezielten Setzen eines Hyperlinks zu einer Internetseite mit kinderpornographischem Inhalt diese Informationen zu-eigen-machte und somit gemäß § 7 TMG verantwortlich sei.[191] Es gelangte damit über § 7 Abs. 1 TMG zur Anwendbarkeit der allgemeinen Gesetze.

Aus dem Beschluss geht nicht hervor, ob das LG Karlsruhe von den beiden vorgenannten Entscheidungen, die eine Anwendbarkeit der Vorgänger-Vorschriften des TMG (TDG) verneint haben, bewusst abweichen und eine eigene Ansicht, die zu dem Schluss gelangt, dass die §§ 7–10 TMG auch im Falle von Hyperlinks einschlägig sind, begründen wollte oder aber ob das LG die entsprechenden Entscheidungen nicht präsent waren. Da das Landgericht in seinem Beschluss von zu-eigen-gemachten Informationen ausgeht und über § 7 Abs. 1 TMG auf die allgemeinen

---

189 OLG Stuttgart MMR 2006, 387, 388.
190 LG Karlsruhe, MMR 2009, 418.
191 LG Karlsruhe, MMR 2009, 418, 419.

Gesetze verweist, prüft es im Anschließenden ohne weitere Differenzierung nach den allgemeinen Vorschriften außerhalb des TMG den Sachverhalt weiter.

III. Stellungnahme

Nachdem der Gesetzgeber bewusst auf eine Regelung für Hyperlinks im TMG verzichtet hat und nur die zwingenden Vorgaben der ECRL umsetzen wollte, ist der herrschenden Lehre und Rechtsprechung zuzustimmen, die eine Anwendung der §§ 7–10 TMG verneinen.[192] Es kann nicht über die Ausführungen des Gesetzgebers im Gesetzgebungsverfahren hinweggegangen werden, der von der Anwendung der allgemeinen Gesetze ausgeht. Eine Auslegung dahingehend, der Normgeber würde in seiner Begründung mit dem Hinweis auf die allgemeinen Gesetze auch das TMG mit einschließen, erscheint an dessen Willen vorbeizugehen und stellt einen Zirkelschluss dar.

Wünschenswert wäre, dass der Gesetzgeber an dieser Stelle die Möglichkeit, die ihm die ECRL offen lässt, wahrnähme und eine gesetzgeberische Lösung durch die Einführung einer Regelung ins TMG träfe. Dies insbesondere vor dem Hintergrund, dass diese Streitfrage nun bereits seit der Umsetzung der ECRL besteht und eine weitere Evaluierung – 10 Jahre nach der ersten – von europäischer Seite in naher Zukunft nicht zu erwarten sein dürfte.

Kapitel 2: Haftung für Suchmaschinen

Suchmaschinen stellen für das Internet eines der bedeutendsten – wenn nicht das bedeutendste – Angebote dar. Nur anhand von Suchmaschinen ist eine gezielte Informationsbeschaffung im Internet möglich. Liegt die Ursprungs-URL einer Zieladresse nicht vor oder werden lediglich Informationen zu einem bestimmten Themenkreis gesucht, so wird heutzutage zwangsläufig eine Suchmaschine mit Schlüsselworten gefüttert. Diese muss nicht einmal mehr separat aufgerufen werden, sondern ist in den meisten Internet-Browsern schon fest als Eingabezeile integriert, sodass ohne Zeitverlust „gegoogelt“ werden kann. *Haug* spricht in diesem Zusammenhang von einer hohen systemischen Bedeutung der Suchmaschinen für das Internet.[193] Diese Sonderstellung besteht nicht nur gegenüber den eigentlich Suchenden, sondern auch gegenüber den gewerblichen Kunden der Suchmaschinenanbieter, die

[192] *Hilgendorf/Valerius*, Rn. 232; *Gercke/Brunst*, Rn. 630; Spindler/Schuster/*Hoffmann*, vor § 7 TMG, Rn. 40; zuletzt *ueber18.de*, BGH NJW, 2008, 1882, 1883.

[193] *Haug*, Rn. 358.

durch den Einsatz von Analysesoftware auf deren Webseiten ihr Angebot noch mehr an den Kunden orientieren wollen.

I. Funktionsweise

Zur Beurteilung Frage nach der Haftung von Suchmaschinenbetreibern ist kurz die Funktionsweise von Suchmaschinen zu klären. Bei dem Ergebnis einer Suchmaschine handelt es sich grundsätzlich um eine Sammlung von Hyperlinks, die der Suchmaschinenbetreiber für den Nutzer aufgrund dessen Suchanfrage zusammengestellt hat. Je nach Art der Suchanfrage wird das Suchergebnis, die sog. Trefferliste, nach dem Grad der Übereinstimmung sortiert. Grundlage für die Sortierung ist ein bestimmter, in einem Programm des Suchmaschinenbetreibers implementierter Suchalgorithmus, der anhand von geheim gehaltenen Kriterien den Grad der Übereinstimmung festlegt. Von technischer Seite funktioniert eine Suchmaschine überwiegend dergestalt, dass der Suchmaschinenbetreiber eine Datenbank unterhält, die Links mit potentiellen Zielen speichert, mit der die Anfrage des Nutzers abgeglichen wird.[194]

II. Haftungsgrundlagen

Die Haftung von Suchmaschinenbetreibern ist wie die Haftung für das Setzen von Hyperlinks gesetzlich nicht normiert. Auch die ECRL regelt diese Haftung nicht explizit. In Erwägungsgrund 20[195] jedoch wird der Begriff des Nutzers dahingehend definiert, dass dieser auch diejenigen Personen miteinschließt, die im Internet nach Informationen suchen, gleich ob für private oder berufliche Zwecke. Diese Definition übernahm der nationale Gesetzgeber bei der Umsetzung, sodass sich zumindest an dieser Stelle eine Beziehung des TMG zu Suchmaschinen als wichtigstes Werkzeug im Internet herstellen lässt.

1. Keine Anwendung des TMG

Nachdem es sich lediglich um eine Sammlung von Hyperlinks handelt, geht die herrschende Meinung davon aus, dass sich die Haftung des Suchmaschinenbetreibers

---

194 MüKo-StGB/*Altenhain*, vor § 7 TMG, Rn. 36.

195 Erwägungsgrund 20: *„Die Definition des Begriffs des Nutzers eines Dienstes umfasst alle Arten der Inanspruchnahme von Diensten der Informationsgesellschaft sowohl durch Personen, die Informationen in offenen Netzen wie dem Internet anbieten, als auch durch Personen, die im Internet Informationen für private oder berufliche Zwecke suchen."*

an der Haftung für Hyperlinks zu orientieren ist.[196] Weder im Gesetzgebungsverfahren wurde eine Regelung getroffen, noch lassen sich die Tätigkeiten des Suchmaschinenbetreibers unter einen Privilegierungstatbestand – auch bei potentieller Anwendbarkeit – fassen.

a) Gesetzgebungsverfahren

Ebenso wie die Haftung für das Setzen von Hyperlinks wird auch die Haftung der Suchmaschinenbetreiber in der Gesetzesbegründung zum TDG n.F. vom Gesetzgeber ausdrücklich ausgenommen.[197] Der Gesetzgeber umschreibt die Funktionsweise der Suchmaschinen als das Erstellen externer programmgesteuerter Links und gelangt zu dem Schluss, dass aufgrund der damit einhergehenden Komplexität der auftretenden Fallgestaltungen eine gesetzliche Regelung zum Zeitpunkt der Umsetzung der ECRL nicht geschaffen werden soll. Der Gesetzgeber verweist damit in seiner Begründung auch für die Suchmaschinen auf die allgemeinen Gesetze als Haftungsgrundlage.

b) Entgegenstehender Gesetzeswortlaut

Zudem kommt neben dem Vorgesagten auch eine Haftungsprivilegierung des Suchmaschinenbetreibers nach dem TMG schon deshalb nicht in Betracht, da dieser bereits der Wortlaut der europäischen Rechtsgrundlage entgegensteht. Erwägungsgrund 42[198] der ECRL stellt klar, dass die Privilegierung des Providers lediglich dann eingreifen soll, wenn es sich um eine automatische und passive Tätigkeit handelt. Dies ist beim Betreiben von Suchmaschinen gerade nicht der Fall. Durch den Abgleich der Suchanfrage mit seiner Datenbank und der Erstellung einer Trefferliste, die nach dem Grad der Übereinstimmung festgelegt wird, trifft der Suchmaschinenbetreiber eine inhaltlich wertende Auswahl und ist somit nicht nur passiv tätig.[199] Eine Heranziehung der Normen des TMG zur Beurteilung der Frage der Haftungsprivilegierung des Suchmaschinenbetreibers wäre damit bereits europarechtswidrig.

---

196 *Hilgendorf/Valerius*, Rn. 233; Spindler/Schuster/*Hoffmann*, vor § 7 TMG, Rn. 35; SSW/*Hilgendorf*, § 184 Rn. 27; *Gercke/Brunst* Rn. 632; *Marberth-Kubicki*, Rn. 382; MüKo-StGB/*Altenhain*, vor § 7 TMG, Rn. 37.

197 BT-Drs. 14/6098 S. 37.

198 vgl. Fn. 127.

199 Spindler/Schuster/*Hoffmann*, vor § 7 TMG, Rn. 39.

2. Keine Heranziehung des § 9 TMG

Ginge man davon aus, dass die Tätigkeit des Suchmaschinenbetreibers an den Vorschriften des TMG zu messen sei, ggf. auch analog, so käme § 9 TMG in Betracht. § 9 TMG, der das Caching regelt, ist allerdings nicht anwendbar, da das Caching nach § 9 TMG lediglich begriffliche Ähnlichkeiten aufweist. „Caching" ist nicht mit dem vom Suchmaschinenbetreiber verwendeten „Cache" in Übereinstimmung zu bringen ist. Hier handelt es sich lediglich um eine gleichlautende Terminologie.[200] Beim Caching nach § 9 TMG werden Webseiten zur beschleunigten Übermittlung von Informationen zwischengespeichert. Diese Informationen müssen immer dem aktuellen Stand der Ursprungswebsite entsprechen.

Dies ist beim „Cache" des Suchmaschinenbetreibers nicht der Fall. Hier werden von diesem zu einem bestimmten Zeitpunkt sämtliche Informationen zu den Inhalten von Webseiten gespeichert, unabhängig von deren Aktualität bezogen auf die Ursprungswebsite, teilweise auch abgekoppelt von deren Existenz oder Verfügbarkeit. Daher ist § 9 TMG nicht heranziehbar.

3. Keine Heranziehung des § 7 TMG

Zudem wird vertreten, dass es sich bei der vom Suchmaschinenbetreiber hergestellten Trefferliste nicht um das Bereitstellen fremder Informationen, sondern um eigene Informationen des Suchmaschinenbetreibers handele.[201] Durch das Generieren der Trefferliste anhand der Datenbank des Suchmaschinenbetreibers entstehe eine eigene Information des Suchmaschinenbetreibers. Die Haftung des Suchmaschinenbetreibers habe sich somit nach § 7 Abs. 1 TMG und folglich den allgemeinen Vorschriften zu richten. Diese Ansicht ist jedoch entsprechend der herrschenden Meinung abzulehnen, da der Wille des Gesetzgebers der Anwendung des TMG entgegensteht.[202]

4. Keine Heranziehung des § 8 TMG

§ 8 TMG ist darüber hinaus auch deshalb nicht anwendbar, weil der Suchmaschinenbetreiber nicht den Zugang zur Nutzung gemäß § 8 Satz 1 TMG vermittelt. Der vom Suchmaschinenbetreiber bereitgestellte Hyperlink in der Trefferliste erleichtert

---

200 Spindler/Schuster/*Hoffmann*, § 9 TMG, Rn. 11.
201 MüKo-StGB/*Altenhain*, vor § 7 TMG, Rn. 36.
202 *Hilgendorf/Valerius*, Rn. 178, m.w.N.

dem Nutzer lediglich einen bereits vom Host-Provider eröffneten Zugang zu der spezifischen Information ohne ihn selbst zu vermitteln.[203]

III. Stellungnahme

Die Haftung des Suchmaschinenbetreibers richtet sich nach den allgemeinen Vorschriften, da nach dem Vorstehenden die §§ 7–10 TMG nicht anwendbar sind. Dies entspricht auch der herrschenden Meinung, der zu folgen ist.[204] Der ausdrückliche Wille des deutschen Gesetzgebers lässt eine andere Interpretation nicht zu, ebenso wenig wie der Wortlaut des Gesetzes, das dem der ECRL entspricht. Da in diesem Punkt bisher eine europäische Vorgabe fehlt und der deutsche Gesetzgeber von einer eigenen Regelung abgesehen hat, ist die Entwicklung auf europäischer Ebene abzuwarten. Um Rechtssicherheit herbeizuführen, wäre eine Vollharmonisierung auch in diesem Punkt wünschenswert. Vorstellbar wäre beispielsweise eine Anlehnung an die Regelung des § 10 TMG, sodass der Suchmaschinenbetreiber bei Kenntnis von den rechtswidrigen Inhalten eine vorherige Privilegierung verlieren würde.

Kapitel 3: Haftung für Snippets und Thumbnails

Eng verbunden mit der Frage der Haftung für Suchmaschinen ist nunmehr die Frage der Haftung für das Bereitstellen von Snippets und Thumbnails. Bei Snippets handelt sich um Wörter und Text-Schnipsel, die auszugsweise mit dem Suchergebnis dargestellt werden.[205] Als Thumbnails bezeichnet man Vorschaubildchen in der Größe eines Fingernagels, die vom Suchmaschinenbetreiber eingeblendet werden, damit der Nutzer einen optischen Eindruck des Suchergebnisses erhält.

Um dem Nutzer der Suchmaschine möglichst schnell eine Vorschau über die gefundenen Suchergebnisse zu präsentieren und ihm durch die auszugsweise Darstellung von Textteilen und Bildern aus den verlinkten Treffer-Inhalten einen ersten Überblick zu ermöglichen, bilden viele Suchmaschinen nach der Überschrift einzelne Wörter bzw. Textbausteine aus der verlinkten Internetseite ab. Diese Text-Schnipsel können bereits rechtswidrige Informationen enthalten, wie z.B. rechtsradikale Propaganda und volksverhetzende Aussagen. Im Rahmen der Darstellung von Thumbnails können z.B. verbotene rechtsradikale Symbole oder Kinderpornographische Photos gezeigt werden.

---

[203] BGHZ 156,1; Spindler/Schuster/*Hoffmann*, vor § 7 TMG, Rn. 39.
[204] *Hilgendorf/Valerius*, Rn. 232
[205] *Ott* in WRP 2011, 655, 675, m.w.N.

Problematisch ist die Verwendung sog. Snippets insbesondere dann, wenn die nur in Textteilen wiedergegebene Information den Sinn der zugrunde liegenden Website entstellt – z.B. durch das einfache Weglassen des Wortes „nicht“ – oder in Textteilen Aussagen wiedergegeben werden, von denen sich jedoch auf der verlinkten Internetseite distanziert wird, oder es sich um Auszüge und Zitate handelt, die in einem wissenschaftlichen Kontext stehen, was nur bei Aufruf der Website erkannt werden kann.

Im folgenden soll die Haftung der Suchmaschinenbetreiber für das Wiedergeben von Snippets weiter beleuchtet werden, da hier Literatur und Gerichte zu unterschiedlichen Ergebnissen in der Behandlung gelangen und der Schwerpunkt in der wissenschaftlichen Betrachtung liegt. Die Verwendung von Thumbnails ist grundsätzlich aus strafrechtlicher Sicht gleich zu behandeln.[206] Bei der Betrachtungsweise der Haftung für Thumbnails liegt das Hauptaugenmerk jedoch auf der Frage der urheberrechtlichen Zulässigkeit der Verwendung durch den Suchmaschinenbetreiber. Hierauf kann an dieser Stelle nicht weiter eingegangen werden, um den strafrechtlichen Fokus der vorliegenden Arbeit beizubehalten. Der BGH hat sich bereits in seinen Entscheidungen „Vorschaubilder I“ und „Vorschaubilder II“ mit den urheberrechtlichen Fragestellungen befasst.[207]

I. Haftung für den rechtswidrigen Inhalt von Snippets

Die Haftung für wiedergegebene Snippets ist umstritten. Literatur und Rechtsprechung sind hier geteilter Meinung.

1. In der Literatur vertretene Ansichten

In der Literatur werden mehrere Ansätze vertreten, die jeweils eine andere Rechtsgrundlage hinsichtlich der Frage der Haftungsprivilegierung des Suchmaschinenbetreibers anwenden wollen.

---

206 MüKo-StGB/*Altenhain*, vor § 7 TMG, Rn. 37.

207 In der Entscheidung des BGH, *Vorschaubilder I*, NJW 2010, 2731, kommt dieser zu dem Ergebnis, dass auch eine Darstellung von Bildern in den Suchergebnissen einer Internetsuchmaschine ein rechtswidriger Eingriff in urheberrechtliche Befugnisse ist. In der Folgeentscheidung BGH, *Vorschaubilder II*, NJW 2012, 1886, wird das Ergebnis der Entscheidung *Vorschaubilder I* dahingehend relativiert, dass mit dem Einstellen eines urheberrechtlich geschützten Werkes in das Internet gleichzeitig eine Einwilligung in die Nutzung durch den Suchmaschinenbetreiber anzunehmen ist.

a) Analoge Anwendung des § 9 TMG

Sieber/Liesching gelangen in ihrer Untersuchung zu dem Ergebnis, dass § 9 TMG analog anwendbar sei, wenn es um Snippets oder Thumbnails gehe.[208] In diesem Fall sei das Handeln des Suchmaschinenbetreibers mit dem eines Proxy-Cache-Providers vergleichbar. Dieser nimmt inhaltlich auf die Informationen keinen Einfluss und speichert diese zeitlich begrenzt, um die Effizienz der Übertragung zu steigern. Auch für den Snippet-Verwender handle es sich um fremde Informationen, denn der Suchmaschinenbetreiber habe kein Interesse daran, sich die Inhalte zu-eigen-zu-machen. Eine ihm zurechenbare Wertung läge daher nicht vor.[209] Nachdem es sich um fremde Inhalte handele, wenden *Sieber/Liesching* den § 9 TMG analog an. Die Ausgangssituation sei vergleichbar. *Sieber/Liesching* gehen dabei davon aus, dass auch der Suchmaschinenbetreiber seine Performance durch die Inhaltsvorschau steigern wolle und die kurzzeitige Speicherung nur für den Fall der konkreten Suchanfrage erfolge. § 9 TMG sei daher im Falle von Snippets analog anzuwenden.[210]

b) Anwendung des § 8 TMG

Zudem wird teilweise für das Einblenden von Snippets im Suchergebnis die Anwendung des § 8 TMG, d.h. eine Haftungsprivilegierung als Access-Provider diskutiert. Der Suchmaschinenbetreiber eröffne dem Nutzer durch die Anzeige der um den Textschnipsel erweiterten Suchergebnisse lediglich den Zugang zu fremden Inhalten.[211]

Als Access-Provider greife der Suchmaschinenbetreiber nicht aktiv in die Auswahl der angezeigten Vorschau ein, sondern es handele sich auch in diesem Falle um eine automatische, lediglich technisch ablaufende Generierung von Trefferlisten, ohne dass hierauf von außerhalb Einfluss genommen würde. Aufgrund einer vorzunehmenden Wertung der vorliegenden Handlung sei daher § 8 TMG anwendbar.[212]

c) Haftung nach den allgemeinen Gesetzen

Die überwiegende Meinung in der Literatur behandelt Snippets haftungsrechtlich gesehen wie die Ergebnisse von Suchmaschinen. Das TMG finde nach dieser Auf-

---

208 *Sieber/Liesching*, S. 14 ff.
209 *Sieber/Liesching*, S. 16.
210 *Sieber/Liesching*, S. 22.
211 Spindler/Schuster/*Hoffmann*, § 8 Rn. 19 ff.
212 Spindler/Schuster/*Hoffmann*, § 8 Rn. 23.

fassung auch hier keine Anwendung, die Haftung richte sich nach den allgemeinen Gesetzen.[213] Nachdem es sich um einen Bestandteil der Ergebnisse von Suchmaschinenanfragen handele, auf die die Vorschriften des TMG ebenfalls nicht anwendbar seien, sei konsequenterweise davon auszugehen, dass auch hier eine Haftung nach den allgemeinen Gesetzen anzunehmen sei.[214]

Hinzu komme, dass es sich um eigene Kopien des Suchmaschinenbetreibers zum Zweck der Ergebnisoptimierung handele und diese auf dessen Servern gespeichert werden. Damit lägen auch eigene Informationen vor, was in jedem Falle zur Anwendung der allgemeinen Vorschriften außerhalb des TMG führt.[215]

2. Stellungnahme zu den in der Literatur vertretenen Ansichten

Gegen eine Anwendung des § 9 TMG, wie *Sieber/Liesching* dies vorschlagen, spricht, dass die Ausgangslage von Proxy-Cache-Provider und Suchmaschinenbetreiber zwar auf den ersten Blick gleich anmutet, jedoch bei genauerer Betrachtung eine Vergleichbarkeit gerade nicht vorliegt. Der Proxy-Cache-Provider strebt nur eine Verbesserung der technischen Performance an. Der Suchmaschinenbetreiber hingegen möchte das Ergebnis der Suchanfrage des Nutzers dahingehend optimieren, dass diesem die Auswahl unter den angezeigten Links erleichtert wird. Von einer Effizienzsteigerung allein im technischen Bereich kann also nicht ausgegangen werden. Außerdem ist von keiner nur automatischen Speicherung durch den Suchmaschinenbetreiber auszugehen. Der vorgegebene Suchalgorithmus trifft bereits eine vorgefertigte Wertung der zu erwartenden Suchergebnisse und die Suchmaschine lädt die aus der verlinkten Webseite ausgesuchten Inhalte als Snippets in das Suchmaschinenergebnis. Die Vergleichbarkeit der Interessenlagen im Rahmen der Analogieprüfung ist daher abzulehnen.

Auch die Ansicht, nach der § 8 TMG als Ergebnis der Bewertung der Handlung des Suchmaschinenbetreibers anwendbar sei, ist abzulehnen. Selbst wenn die Anwendbarkeit des TMG an dieser Stelle angenommen werden könnte, handelt es sich doch um eine Auswahl, die nicht bar jeglichen äußeren Einflusses ist. Eine reine Durchleitung technischer Natur ist daher zu verneinen und § 8 TMG deshalb nicht einschlägig.[216] Überzeugend ist die herrschende Meinung, die eine Haftung nach den allgemeinen Gesetzen vertritt. Die §§ 7–10 TMG sind nicht passend – weder inhalt-

---

213 *Gercke/Brunst*, Rn. 632.

214 MüKo-StGB/*Altenhain*, vor § 7 TMG, Rn. 37.

215 MüKo-StGB/*Altenhain*, a.a.O.

216 Im Ergebnis auch *Malek/Popp*, Rn. 98, der die Grenze zur automatischen Durchleitung spätestens bei Vorliegen sog. „abstracts“ (umfassen auch Snippets) als überschritten ansieht.

lich noch im Hinblick auf ihre gesetzgeberische Entstehung. Der Suchmaschinenbetreiber gibt zum einen schon den Suchalgorithmus vor. Zum anderen ist auch in diesem Falle wieder auf die Gesetzesbegründung zu verweisen, die eine Haftungsregelung für Suchmaschinenergebnisse bewusst nicht mitregelt. Hierunter fallen auch die Snippets, sodass es bei der Haftung nach den allgemeinen Gesetzen verbleibt.

3. Snippets in der Rechtsprechung

Die Gerichte entscheiden in dieser Frage uneinheitlich. Ein Urteil des BGH zu diesem Thema liegt bislang noch nicht vor.

a) Entscheidung des Kammergerichts

Die Haftung des Suchmaschinenbetreibers für in den Suchergebnissen enthaltene Snippets war entscheidungserhebliche Frage des Kammergerichts in einer zivilrechtlichen Entscheidung des Jahres 2009.

aa) Sachverhalt

Dem Fall lag zugrunde, dass die im Rahmen des Textschnipsels angezeigte Aussage den Sinngehalt der tatsächlich getroffenen Aussage im ursprünglichen Textdokument entstellt hatte. In Wahrheit war das Suchergebnis mit der Internetseite einer Satire-Zeitschrift verlinkt, der Inhalt also grundsätzlich als satirische Äußerung zu verstehen. Dies ergab sich jedoch aus dem im Suchmaschinenergebnis angezeigten Snippet nicht. Die Aussage, die dem Textschnipsel zu entnehmen war, war objektiv betrachtet persönlichkeitsrechtsverletzend.

bb) Beschluss des Kammergerichts

Das Kammergericht ging entgegen der herrschenden Lehre zunächst davon aus, dass die §§ 8–10 TMG auch auf die Betreiber von Suchmaschinen Anwendung finden, und grenzt sodann fremde von eigenen Informationen anhand der Entscheidung des BGH „Internetversteigerung I[217]“ ab. Es gelangt dann zu dem Ergebnis, dass es sich nicht um eigene Informationen des Suchmaschinenbetreibers handelte, sondern dass für die Nutzer der Suchmaschine erkennbar sei, dass es sich um fremde Infor-

[217] BGH NJW 2004, 3102.

mationen handelte.[218] Durch das Einbinden der Snippets in das Suchergebnis sei vom objektiven Empfängerhorizont eines durchschnittlichen Internetnutzers davon auszugehen, dass sich der Betreiber der Suchmaschine die fremden Inhalte nicht z eigene machen wollte.

Das Gericht führt seine Prüfung der Haftungsprivilegierung durch das TMG sodann jedoch nicht weiter, weil der ihm vorliegende Fall und deshalb auch die vorliegende Entscheidung Unterlassungsansprüche gegen den Diensteanbieter betrifft, auf welche nach der Rechtsprechung des BGH die §§ 8–10 TMG aber keine Anwendung finden.[219] Würde man den Gedankengang des Kammergerichts konsequent zu Ende führen, so müsste man in strafrechtlicher Hinsicht nun die Privilegierungstatbestände des TMG heranziehen, da es sich nach dem Kammergericht um fremde Informationen handeln soll, deren Anwendungsbereich daher grundsätzlich eröffnet ist.

b) Entscheidung des Hanseatischen Oberlandesgerichts

Auch das OLG Hamburg hatte in einer Entscheidung die Haftung des Suchmaschinenbetreibers für Snippets zu prüfen.

aa) Sachverhalt

Der dem OLG Hamburg vorliegende Sachverhalt gründete auf der Tatsache, dass das Ergebnis einer Suchmaschinenanfrage Textteile eines Internet-Blogs enthielt. Gegen diese Inhalte richtete sich die Klage des Betroffenen, der sein allgemeines Persönlichkeitsrecht durch die Behauptung unwahrer Tatsachen verletzt sah. Auf Unterlassung nahm der Kläger dann auch den Betreiber der Suchmaschine in Anspruch, bei der die fraglichen Snippets auftauchten.

bb) Urteil des Hanseatischen Oberlandesgerichts

Das OLG Hamburg geht bei der Beurteilung des Tatbeitrages eines Suchmaschinenbetreibers noch einen Schritt weiter als das Kammergericht. Das OLG schließt eine Haftung desselben für die Verwendung von Snippets schon deshalb aus, weil der Nutzer der Suchmaschine wissen müsse, dass es sich hier lediglich um unvollständige Textteile, generiert in einem automatisierten Verfahren, handele und der

---

[218] KG Berlin MMR 2010, 495.
[219] KG Berlin MMR 2010, 495, 496.

Text der Suchergebnisse, d.h. der Snippets, somit immer nur im Zusammenhang mit der tatsächlichen Ursprungsseite zu lesen sei, welcher er entstammt.[220]

Abgestellt wird vom OLG Hamburg dabei darauf, dass der Nutzer der Suchmaschine weiß, dass es sich bei den Suchergebnissen, insbesondere den Textschnipseln, um offensichtlich unvollständige Textauszüge handele. Das Oberlandesgericht schließt somit eine Haftung des Suchmaschinenbetreibers für Snippets generell aus und kommt im Folgenden denklogisch zu dem Ergebnis, dass die Frage, ob Suchmaschinenbetreiber nach den Privilegierungen des §§ 7–10 TMG zu behandeln sind, offen gelassen werden könne. Das OLG Hamburg nimmt somit eine Gesamtbetrachtung vor, indem es dem Nutzer das Wissen um die Beispielhaftigkeit unterstellt, mit der die Textteile und Wörter wiedergegeben werden.

4. Stellungnahme zu den Entscheidungen der Rechtsprechung

Sowohl die Entscheidung des Kammergerichts als auch die Entscheidung des Hanseatischen Oberlandesgerichts sind kritisch zu betrachten. Das Kammergericht hält die Anwendung der §§ 7–10 TMG grundsätzlich für möglich. Wäre dieser Punkt entscheidungserheblich gewesen, so hätte sich das Kammergericht gegen die h.M. in der Literatur gestellt und es hätte einer obergerichtlichen Klärung bedurft. Weshalb das Kammergericht in seiner Entscheidung von der Anwendbarkeit des TMG ausgeht, begründet es jedoch nicht. Gerade dies wäre aufgrund der umstrittenen Rechtslage notwendig und wünschenswert gewesen. Auch das Urteil des OLG Hamburg ist durchaus differenziert zu sehen. Eine generelle Gesamtbetrachtung zwischen gesamt angezeigtem Suchergebnis und verlinkter Zielseite erscheint bei näherer Betrachtung als problemorientierte Lösung.

Jedoch ist fraglich, ob generell jedem Internetnutzer dieses Wissen um die Tatsache, dass es sich hier lediglich um Auszüge handelt, unterstellt werden kann. Dies ist wohl aufgrund der Vielzahl der Internetnutzer und der weitgehend wenig vertiefen Kenntnisse derselben zu pauschal. Dies insbesondere vor dem Hintergrund, dass das Suchergebnis eine Vielzahl von Treffern darstellt, welche sicher nicht alle vom Nutzer mit der verlinkten Hauptseite überprüft werden. In strafrechtlicher Hinsicht ist hier durchaus eine Differenzierung geboten.

---

[220] OLG Hamburg MMR 2010, 490.

II. Stellungnahme zur Haftung für Snippets und Thumbnails

Die herrschende Meinung, die eine Haftung nach den allgemeinen Gesetzen vertritt, hat die besseren Argumente, denn die §§ 7–10 TMG passen in ihrer Zielrichtung nicht. Nachdem wie bereits erläutert eine vergleichbare Ausgangslage hinsichtlich der §§ 8 und 9 TMG nicht gegeben ist, erscheint eine Beurteilung der Haftung nach den allgemeinen Gesetzen angebracht. Die Gesetzesbegründung lässt eine Haftungsregelung für Suchmaschinenergebnisse und daher auch für Snippets und Thumbnails bewusst offen.

Kapitel 4: Haftung bei Internetplattformen

Die Frage nach der Haftung für die auf einer Internetplattform eingestellten Informationen, insbesondere durch den Forenbetreiber, bedarf hier zunächst der weiteren Auslegung dahingehend, was unter einer Internetplattform zu fassen ist. *Haug* stellt seine Abhandlung zu diesem Thema unter den Oberbegriff „Haftung für Usergenerated Content".[221] Er fasst darunter Meinungs- und Diskussionsforen, Auktions- und Verkaufsplattformen, etc. Die Beschreibung „Usergenerated Content" eignet sich auch für die nachstehende Arbeit, denn der gemeinsame Nenner besteht darin, dass im Internet Plattformen angeboten werden, auf denen die User eigene Informationen einstellen.

I. Internetplattform

Das Grundkonzept der Internetplattform gestaltet sich generell so, dass der Plattformbetreiber eine Website anbietet. Auf dieser Oberfläche wird dem Internetnutzer ermöglicht – meist nach erforderlicher Anmeldung – Beiträge zu verfassen, Waren anzubieten, oder Dateien hochzuladen. Dadurch entsteht eine Vielzahl von rechtlichen Beziehungen, die auch strafrechtliche Bedeutung haben können.

Die erste Verbindung besteht zwischen dem Plattformbetreiber und dem Nutzer der Plattform, der sich dieser als Kommunikationsbasis bedient. In bürgerlichrechtlicher Hinsicht besteht zwischen beiden ein Nutzungsvertrag. Strafrechtlich stellt sich die Frage, ob der Plattformbetreiber durch die von ihm betriebene Plattform z.B. an einem Aussage- oder Verbreitungsdelikt des Nutzers mitwirkt. Als zweiter Anknüpfungspunkt sind die Beziehungen der einzelnen Nutzer untereinander zu beleuchten. Auch zwischen ihnen können zivilrechtliche Verträge entstehen, z.B.

---

[221] *Haug*, Rn. 295 f.

Kaufverträge auf ebay. In strafrechtlicher Hinsicht kommen z.B. internettypische Beleidigungsdelikte wie Flaming oder Cybermobbing in Betracht. Zudem kommt als dritte Möglichkeit auch die Verbindung von Plattformbetreiber und Nutzer einerseits und außenstehenden Dritten andererseits in Betracht. Diese können z.B. Unterlassungsansprüche gegen Nutzer und Betreiber haben. Auch Straftaten gegenüber Nicht-Nutzern sind denkbar.

II. Haftung des Nutzers

Der Nutzer einer Internetplattform stellt in diese eigene Informationen ein und haftet damit vollumfänglich.[222] Er ist als Content-Provider einzustufen, der für seine Inhalte nach den allgemeinen Gesetzen gem. § 7 Abs. 1 S. 1 TMG haftet. Ob dieser dann tatsächlich für rechtswidrige Inhalte belangt werden kann, ist eine Frage, die in der Praxis nicht einfach zu beantworten ist. Um den Nutzer zu ermitteln, müssen die Nutzerdaten beim Plattformanbieter abgefragt werden. Problematisch ist nicht die mangelnde Vorhersehbarkeit, sondern dass oft eben keine verwertbaren Informationen bereitgehalten werden. Dies macht ein Vorgehen der Ermittlungsbehörden schwierig. Hinzu kommt die zunehmende Anonymisierung des Internets, aufgrund deren sich der Nutzer sich nicht mit seinen richtigen Daten auf der Plattform anmeldet. Teilweise ist dies gar nicht notwendig, ausreichend ist oft die Hinterlegung einer E-Mail-Adresse und eines Spitznamens.

Die Haftbarmachung des Nutzers gestaltet sich somit theoretisch eindeutig, praktisch jedoch umso schwieriger. Dies stellt insbesondere die Strafverfolgungsbehörden – deren Tätigkeit in der Praxis auch der zivilrechtlichen Inanspruchnahme z.B. in Filesharing-Fällen zur Ermittlung des Rechteverletzers vorangeht – vor immer größere Herausforderungen. Die Ermittlung eines Täters muss dann anhand der IP-Adresse oder über eine möglicherweise falsche (Fake-)E-Mail-Adresse erfolgen.

III. Haftung des Plattformbetreibers

Die Haftung des Plattformbetreibers, der gleichzeitig Diensteanbieter im Sinne von § 2 TMG ist, ist jedoch nicht so einfach zu beurteilen wie die der Nutzer solcher Dienste. Der Plattformbetreiber, der dem Nutzer auf seiner Website die Möglichkeit gibt, eigene Beiträge zu verfassen, leistet dem potentiell rechtswidrigen Verhalten des Nutzers dadurch Vorschub. Denn ohne diese Möglichkeit wäre der Nutzer nicht in der Lage, ein derart breites Publikum für sein Verhalten zu finden.

---

[222] *Haug*, Rn. 296.

1. Haftung für eigene Informationen

Die Informationen, die auf der Plattform von den Nutzern eingestellt oder verfasst werden, sind für den Plattformbetreiber grundsätzlich fremde Informationen. Der Plattformbetreiber kann sich diese jedoch zu eigen machen, mit der Folge, dass er dafür wie für eigene Informationen unbeschränkt gem. § 7 Abs. 1 TMG einzustehen hat.[223]

a) Zustimmung

Ein Zu-eigen-Machen liegt insbesondere dann vor, wenn der Plattformbetreiber die rechtswidrigen Informationen gutheißt bzw. diesen zustimmt oder sich mit ihnen identifiziert. Durch dieses aktive Tun macht sich der Plattformbetreiber die Inhalte zu eigen.[224]

b) Billigung rechtswidriger Inhalte

Ausreichend soll jedoch auch sein, wenn der Plattformbetreiber die fremden Inhalte billigt und diese wie eigene behandelt.[225] Dadurch mache er sich diese ebenfalls zu eigen. Zur Beurteilung, ob der Plattformbetreiber die Inhalte billigt, soll maßgeblich sein, ob aus der Sicht eines unbefangenen Dritten eine Identifikation des Plattformbetreibers mit den rechtswidrigen Inhalten objektiv erkennbar sei.[226]

c) Themenstruktur

Zudem ist es nach der Rechtsprechung möglich, dass fremde Inhalte zu eigen gemacht werden, wenn der Plattformbetreiber eine Themenstruktur seines Angebotes vorgibt.[227] Indem der Plattformbetreiber dem Nutzer einen festen Platz für seinen Beitrag vorgibt, kann bereits derart in die Vermittlung der Information eingegriffen werden, dass dem entsprechenden Beitrag eines Nutzers eine bestimmte Wertung zukommt, die auf den Plattformbetreiber und die von diesem vorgenommene Einordnung zurückzuführen ist. Hierdurch macht sich der Plattformbetreiber die frem-

---

223 SSW/*Hilgendorf*, § 184 StGB, Rn. 25.
224 Ausführlich s.o. S. 35.
225 SSW/*Hilgendorf*, § 184 StGB, Rn. 25.
226 *Hilgendorf/Valerius*, Rn. 200.
227 OLG Köln, MMR 2002, 548.

den Inhalte zu eigen. Er wertet sie und bringt seine Wertung dem Nutzer zur Kenntnis.

2. Haftung für fremde Informationen

Werden dem Plattformbetreiber fremde Informationen nicht zugerechnet, fehlt es also an einem Zu-eigen-Machen, so kommt eine Haftung für fremde Informationen in Betracht, die an den Privilegierungen der §§ 7–10 TMG zu messen ist. Die herrschende Meinung stuft die Handlung des Forenbetreibers als Host-Provider ein[228], nachdem der Plattformbetreiber dem Nutzer die Möglichkeit der Hinterlegung von Informationen gibt und diese auf seinen Servern und seiner Website speichert. Sie haften daher nur bei positiver Kenntnis der rechtswidrigen Inhalte der von ihnen betriebenen Seiten, sofern sie nicht nach Kenntniserlangung unverzüglich tätig werden gem. § 10 TMG.

3. Rechtsprechung

Die zivilrechtliche Rechtsprechung geht mit der herrschenden Meinung im Schrifttum davon aus, dass der Anbieter sich die Inhalte – je nach Intensität der Themenstruktur und objektiver Erkennbarkeit der Billigung nach außen – zu eigen macht und dafür wie für eigene Informationen gem. § 7 Abs. 1 TMG nach den allgemeinen Gesetzen haftet.[229]

Diese Rechtsprechung geht auf eine Entscheidung des OLG Köln aus dem Jahre 2002 zurück, die zwischenzeitlich vom LG Hamburg in einer Entscheidungen aus dem Jahre 2008 bestätigt[230] und auch vom BGH dergestalt übernommen wurde.

a) Entscheidung des BGH – Marions-kochbuch.de

In seiner Entscheidung „Marions-kochbuch.de“ hat auch der BGH die untergerichtliche Rechtsprechung bestätigt.[231] Eigene Informationen können danach auch zu eigen gemachte Informationen sein.

---

228 *Gercke/Brunst*, S. 247f, Rn. 595; MüKo-StGB/*Altenhain*, vor § 7 TMG, Rn. 28; SSW/*Hilgendorf*, § 184 StGB, Rn. 26.

229 SSW/*Hilgendorf*, § 184 StGB, Rn. 26; OLG Köln, MMR 2002, 548.

230 LG Hamburg ZUM-RD 2009, 407 f.

231 *marions-kochbuch.de* BGH MMR 2010, 556.

aa) Sachverhalt

In dem vom BGH zu entscheidenden Fall wurde der Betreiber einer Internetplattform in Anspruch genommen, welcher auf der von ihm angebotenen Website Fotos veröffentlichte, deren Urheber der Kläger war. Auf der Internetplattform des Beklagten konnten Nutzer Kochrezepte hochladen nebst dazugehöriger Fotos. Diese Inhalte wurden erst veröffentlicht, nachdem sie von der Redaktion des Plattformbetreibers auf Richtigkeit und Vollständigkeit überprüft worden waren. Es wurde insbesondere versucht darauf zu achten, ob die Fotos einen professionellen Eindruck machten. Bei der Freischaltung wurde dem hochgeladenen Foto dann noch ein Kochmützensymbol, nämlich dasjenige des Plattformbetreibers, hinzugefügt.

bb) Urteil des Bundesgerichtshofes

Der Bundesgerichtshof setzte sich in dieser Entscheidung mit der Frage auseinander, wann ein Zu-eigen-Machen von fremden Inhalten durch den Betreiber einer Internetplattform vorliegt. Die Frage ist objektive Grundlage einer Gesamtbetrachtung aller relevanten Umstände zu beurteilen.[232] Der BGH verweist in den Gründen seiner Entscheidung insbesondere auf die Begründung des Regierungsentwurfs zum IuKDG[233].

Im vorliegenden Fall war eine Stellungnahme zur Strukturierung des Inhaltes nach Themenkomplexen nicht vorzunehmen, denn der BGH ging vielmehr davon aus, dass die hochgeladenen Kochrezepte der Nutzer zum redaktionellen Kerngehalt der Internetseite zählten und somit dem Diensteanbieter objektiv zurechenbar waren. Dies begründet der BGH damit, dass der Diensteanbieter die eingestellten Inhalte erst nach eigener Überprüfung freigeschaltet hatte.[234] Darüber hinaus hatte sich der Diensteanbieter auch unmissverständlich die von den Nutzern hochgeladenen Abbildungen zu eigen gemacht, indem er die Fotos mit seinem Kochmützenemblem versehen hatte, sodass sie sich für den Nutzer als eigene Bilder des Anbieters darstellten. Der BGH bejahte damit eine Haftung für eigene – zu eigen gemachte – Informationennach § 7 Abs. 1 TMG des Plattformbetreibers in diesem Fall.[235]

---

232 *marions-kochbuch.de* BGH MMR 2010, 556.
233 *marions-kochbuch.de* BGH MMR 2010, 557; BT-Drucks. 13/7385, S. 19 f.
234 *marions-kochbuch.de* BGH MMR 2010, 557.
235 *marions-kochbuch.de* BGH MMR 2010, 558.

b) Entscheidung des hanseatischen Oberlandesgerichtes – „Sevenload“

Das hanseatische Oberlandesgericht folgt in seiner Entscheidung dem Urteil des BGH in Sachen „Marions-kochbuch.de“. Auch in diesem Fall war die Grenze eines Zu-eigen-Machens durch den Betreiber einer Website zu ermitteln.

aa) Sachverhalt

In dem vorliegenden Fall betrieb die Antragsgegnerin eine Internetplattform auf der Nutzer u.a. Video- und Audiodateien hochladen und damit jedermann frei zugänglich machen konnten. Die Musik- und Filmtitel der Nutzer standen damit allen registrierten Nutzern zum Ansehen und teilweise auch Herunterladen zur Verfügung. Das Online-Abspielen erfolgte über eine Oberfläche, auf der kontinuierlich Werbung für die Antragsgegnerin eingeblendet wurde. Zur Verfolgung von Straftaten gegen das Urheberrecht hatte die Plattformbetreiberin ein „notice-and-takedown“-Verfahren eingerichtet, über das illegale Inhalte gemeldet werden konnten und diese dann gesperrt wurden.

bb) Urteil des hanseatischen Oberlandesgerichtes

Mit der Entscheidung „sevenload“ hat das OLG Hamburg die vom BGH im o.g. Urteil aufgestellten Grundsätze verfestigt.[236] Es orientiert sich eng an der Entscheidung „Marions-kochbuch“, von der es den ihm vorliegenden Fall abgrenzte. Das OLG Hamburg nimmt an dieser Stelle eine umfassende Prüfung der Frage vor, ob sich der Plattformbetreiber von „sevenload“ die Inhalte seiner Nutzer zu Eigen gemacht hat oder nicht. In Anlehnung an die soeben erörterte BGH Entscheidung geht auch das OLG von einer objektiven Betrachtungsweise aus und würdigt jedes einzelne Anzeichen eigenständig und ausführlich. Es kommt sodann zu dem Schluss, dass zu viele Punkte gegen ein Zu-eigen-Machen der Plattformbetreiberin sprächen.[237] Insbesondere sei das Kennzeichnen der Dateien mit einem Wiedergabe- bzw. Abspielsymbol verbunden mit dem Namen der Plattform, das zum Starten des Abspielens angeklickt werden muss, nicht mit der dauerhaften Kennzeichnung durch das Anbringen des Kochmützensymbols im Fall „Marions-kochbuch“ vergleichbar. Darin sah das OLG keine vergleichbare Übernahme der Inhalte als eigene durch sevenload erkennen. Zudem nehmen die Betreiber der Videoplattform sevenload keine

[236] *sevenload* OLG Hamburg, MMR 2011, 49.
[237] *sevenload* OLG Hamburg, MMR 2011, 49, 51.

vorherige Prüfung der Informationen vor, sodass von einem Zu-eigen-Machen auch deshalb nicht auszugehen sei.[238]

IV. Stellungnahme

Mit der Entscheidung „Marions-kochbuch" bekräftigt der Bundesgerichtshof die Qualifizierung von zu-Eigen-gemachten Informationen als eigene Informationen. Die Entscheidung zugunsten dieses Rechtsinstitutes ist zu begrüßen, da dies bereits in der Gesetzesbegründung angelegt war. Ebenfalls positiv ist die Festlegung der Gerichte auf den objektiven Beurteilungsmaßstab. Nur anhand dessen ist praktisch nachvollziehbar und nachprüfbar, wann Inhalte als eigene gelten sollen. Ein innerer Wille ist daher nicht beachtlich. Dies entspricht dem praxisorientierten Ansatz des BGH und trägt zur Rechtsklarheit bei.

Kapitel 5: Hot-Spots und Internetcafés

Im Folgenden soll nur überblicksartig auf die Haftung der Anbieter von Hot-Spots eingegangen werden. Es handelt sich hier zumeist um das Zur-Verfügung-Stellen von W-LAN-Netzwerken in Hotels, Bars, Cafés oder Flug- und Bahnhöfen, über die sich jeder Nutzer ins Internet einwählen kann. In diesem Kontext soll auch kurz auf den Betrieb von Internetcafés eingegangen werden, bei dem zusätzlich zum Internetzugang auch die dazugehörige Hardware zur Verfügung gestellt wird.

I. Haftung für Hot-Spots

Der Betreiber eines Hot-Spots, d.h. eines W-LAN-Netzwerks vermittelt denjenigen Nutzern, die sich in Reichweite seines Funknetzes befinden, den Zugang zum Internet. Dies geschieht teilweise kostenlos, teilweise aber auch gegen Entgelt. Teilweise wird vertreten, dass es sich bei einem Anbieter von Infrastruktur, der lediglich den Kontakt zwischen dem Nutzer und dem tatsächlichen Internetprovider herstellt, nicht um einen Diensteanbieter gem. § 2 S. 1 Nr. 1 TMG handele, der nach den Verantwortlichkeitsregelungen der §§ 7–10 TMG zu behandeln sei. Vielmehr handele es sich hierbei um einen Anbieter außerhalb des Internets.[239] Die derzeit überwiegende Meinung vertritt die Ansicht, dass sich die Tätigkeit des Anbieters eines Hot-Spots lediglich in dem Zur-Verfügung-Stellen erschöpft und seine Tätigkeit rein techni-

---

238 *sevenload* OLG Hamburg, MMR 2011, 49, 50 f.

239 *Hilgendorf/Valerius*, Rn. 183 a.E.; *Hornung* CR 2007, 88, 90.

scher Natur sei, bei der die Inhalte nicht entsprechend § 8 Abs. 1 S. 1 Nr. 3 TMG verändert werden. Nach dieser Ansicht ist der Anbieter von W-LAN-Hot-Spots daher als Access-Provider gem. § 8 TMG einzustufen.[240]

II. Internet-Cafés

Betrachtet man die Frage der Haftung von Internet-Café Betreibern, so ist festzustellen, dass diese ebenfalls weiterhin umstritten ist.[241] In Betracht kommt eine Privilegierung der Internet-Café-Betreiber nach § 8 TMG, da diese durch die Bereitstellung von Rechnerarbeitsplätzen die Möglichkeit des Zugangs zum Internet eröffnen. Umstritten ist, ob eine Privilegierung gemäß § 8 TMG auch dann anzunehmen ist, wenn nicht der Zugang zur Nutzung vermittelt wird, sondern lediglich die Nutzung eines Zugangs ermöglicht wird.[242] Es wird insbesondere vertreten, dass § 8 TMG dahingehend richtlinienkonform auszulegen sei, dass auch die Ermöglichung der Nutzung eines Zugangs hierunter zu subsumieren ist. Hierfür spreche, dass Art. 12 der ECRL auch die Vermittlung des Zugangs zu einem Kommunikationsnetz mitumfasst.[243] Zudem handele es sich auch nicht um eine reine Telekommunikationsdienstleistung, sodass die Anwendbarkeit des TMG nicht gem. § 1 Abs. 1 S. 1 TMG ausgeschlossen sei.[244]

Die gegenteilige Ansicht meint, dass diejenigen, die nicht den Zugang zur Nutzung, sondern nur die Nutzung eines Zugangs vermitteln, nicht als Diensteanbieter im Sinne des § 8 TMG zu qualifizieren seien. Begründet wird diese Ansicht damit, dass diese nicht Bestandteil des Kommunikationsnetzes seien, sondern außerhalb des Kommunikationsnetzes stünden und lediglich die Infrastruktur zur Nutzung der Leistung von Access-Providern bereitstellten.[245]

III. Stellungnahme

Vorzugswürdig ist die letztgenannte Ansicht, die die Betreiber nicht als Diensteanbieter einstuft. Sowohl der europäische als auch der deutsche Gesetzgeber haben bei der Schaffung der ECRL und des TDG n.F. immer den technischen Zusammen-

---

240 MüKo-StGB/*Altenhain*, vor § 7 TMG, Rn. 50; Spindler/Schuster/*Hoffmann*, § 8 TMG, Rn. 17 f.

241 *Gercke/Brunst*, Rn. 609.

242 *Gercke/Brunst*, Rn. 612.

243 *Gercke/Brunst*, a.a.O.

244 Spindler/Schuster/*Hoffmann*, § 8 TMG, Rn. 17.

245 *Hilgendorf/Valerius*, Rn. 183; SSW/*Hilgendorf* § 184 Rn. 30; *Kessler*, Zur strafrechtlichen Verantwortlichkeit von Zugangsvermittlern, S. 44 ff.; *Liesching/Günter* MMR 2000, 260 264 f.

hang im Auge gehabt. Es sollte gezielt eine Regelung geschaffen werden, die gerade an das Vorliegen eines Kommunikationsnetzes und den darin enthaltenen Datenaustausch anknüpft. Nicht darunter zu fassen sein und damit geschützt, sollten damit Angebote sein, die außerhalb des Kommunikationsnetzes stehen. Der Kreis der Diensteanbieter würde ansonsten zu weit gefasst werden. Dies betrifft sowohl die Frage der W-LAN-Hot-Spots, als auch das Zugänglichmachen durch einen Internet-Café-Betreiber.

Teil 3: Haftung des Access-Providers

Wie in der Einleitung bereits dargelegt, ist das Internet aus dem Leben vieler Menschen, egal ob jung oder alt, heute kaum noch wegzudenken. Damit im Internet jedoch kein rechtsfreier Raum entsteht, ist es umso wichtiger, Möglichkeiten zu ergründen, mit denen Missbrauch im Internet Einhalt geboten werden kann. Der Access-Provider bietet sich als Mittel zum Zweck der Eingrenzung rechtswidriger Tendenzen deshalb an, weil er die Schnittstelle zwischen „Offline“ und „Online“ darstellt. Jeder Internetnutzer ist darauf angewiesen, dass ihm der Zugang zum Internet von einem Access-Provider vermittelt wird. Anders als bei Content- oder Host-Providern, die aus der ganzen Welt und von jedem Eiland aus ihre Dienste anbieten können und ihren Standort sowie den Ort, an welchem die von ihnen zur Verfügung gestellten Informationen gespeichert werden, ständig wechseln können, ist der Access-Provider immer auch gezwungen, hiesige inländische Datennetze und Einwahlpunkte zu nutzen, um dem Endverbraucher den Zugang zu ermöglichen. Will man nun missliebige Daten und Informationen aus dem Netz heraushalten oder diese zumindest für die Nutzer unzugänglich machen, so ist es sinnvoll, hierbei den Access-Provider in die Pflicht zu nehmen. Im Folgenden soll geprüft werden, inwiefern es auch im bestehenden System des TMG durchaus möglich ist, eine Haftung des Access-Providers herzuleiten.

Kapitel 1: Haftung nach „den allgemeinen Gesetzen“

Wie bereits erörtert, richtet sich die Haftung des Access-Providers grundsätzlich nach § 8 TMG. Diese Norm führt zu einer weitgehenden Privilegierung des Access-Providers. Solange es sich um eine rein technische und automatisiert ablaufende Datenübertragung handelt, in die vom Access-Provider nicht eingegriffen wird, ist dieser von jeglicher Haftung freigestellt. Der Access-Provider haftet erst, wenn er bei der Datenübertragung von einer passiven in eine aktive Rolle wechselt, d.h. wenn er selbst entweder die Übermittlung fremder Informationen veranlasst, § 8 Abs. 1 S. 1 Nr. 1 TMG, den Adressaten dafür aktiv auswählt, § 8 Abs. 1 S. 1 Nr. 2 TMG, die übermittelten Informationen ausgewählt oder verändert hat, § 8 Abs. 1 S. 1 Nr. 3 TMG, oder kollusiv mit einem seiner Nutzer zusammenarbeitet, um Straftaten zu begehen, § 8 Abs. 1 S. 2 TMG. Aufgrund dieser weitgehenden Privilegierung des Access-Providers durch § 8 TMG wird er zumeist von den Strafverfolgungsorganen im Rahmen ihrer Tätigkeit bereits von vorneherein nicht als Täter wahrgenommen,

sondern lediglich als Informationsbeschaffer, z.B. wenn es um die Ermittlung von zugehörigen Daten zu einer bestimmten IP-Adresse geht.

Der Access-Provider kann jedoch im Falle eines Unterlassens außerhalb seiner Privilegierung auch nach den allgemeinen Gesetzen gem. § 7 Abs. 2 S. 2 TMG haftbar gemacht werden. § 7 Abs. 1 TMG regelt, wie bereits an anderer Stelle erläutert, die Haftung für eigene Informationen, d.h. solche, deren Urheber der Diensteanbieter selbst ist oder welche er sich zu eigen gemacht hat. Im Abschnitt 3 „Verantwortlichkeit“ steht § 7 TMG unter der Überschrift „Allgemeine Grundsätze“. Er hält in seinem Absatz 2 drei weitere allgemeine Regeln für die Haftung des Internetproviders fest. § 7 Abs. 2 S. 1 TMG statuiert, dass die Diensteanbieter im Sinne der §§ 7–10 TMG sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen, denn die Datenmengen, die im Internet versendet oder abgerufen werden, sind in der Regel zu umfangreich. Es handelt sich hierbei um den Grundsatz „ultra posse nemo obligatur“, der als allgemeiner Grundsatz im Rechtsverkehr anerkannt ist und hier daher nicht gesondert hätte festgehalten werden müssen.[246] Ebenso von rein deklaratorischer Bedeutung erscheint § 7 Abs. 2 S. 3 TMG, der die Geltung des Fernmeldegeheimnisses entsprechend § 88 TKG hervorhebt.[247] Eine Haftung der Diensteanbieter nach den allgemeinen Gesetzen, unabhängig von einer Haftungsprivilegierung nach den §§ 8–10 TMG, regelt jedoch § 7 Abs. 2 S. 2 TMG für den Fall, dass eine Verpflichtung zur Entfernung oder Sperrung von Informationen besteht.

Nach der hier vertretenen Ansicht handelt es sich bei dieser Vorschrift um eine spezielle Vorschrift für den Fall des Unterlassens, die insbesondere auch im Strafrecht Anwendung findet und dadurch im Einzelfall bei Vorliegen der gesetzlichen Voraussetzungen zu einer Strafbarkeit eines Access-Providers führt. Dies wird im Nachfolgenden zu erläutern sein:

I. Spannungsverhältnis zu § 7 Abs. 2 S. 1 TMG

Vorab soll zunächst das Verhältnis zwischen § 7 Abs. 2 S. 1 und S. 2 TMG beleuchtet werden, denn diese Normen stehen sich auf den ersten Blick diametral entgegen. § 7 Abs. 2 S. 1 TMG statuiert, dass für die Diensteanbieter keine Verpflichtung zur proaktiven Überprüfung der von ihnen verwendeten Informationen besteht. Diese Norm basiert auf Art. 15 ECRL, den der nationale Gesetzgeber an dieser Stelle

246 *Hilgendorf/Valerius*, Rn. 205.
247 Spindler/Schuster/*Hoffmann*, § 7 TMG, Rn. 38.

ins TMG eingefügt hat. Demgegenüber regelt § 7 Abs. 2 S. 2 TMG, dass für Beseitigungs- und Unterlassungsansprüche die allgemeinen Gesetze zur Frage der Haftung heranzuziehen sind und die Privilegierungen in den §§ 8–10 TMG keine Anwendung finden.[248] Diese Regelung setzt die vom Richtliniengeber in den Art. 12 Abs. 3, 13 Abs. 2 und 14 Abs. 3 ECRL eröffnete Möglichkeit in innerstaatliches Recht um.

Unabhängig von der Verantwortlichkeitsprüfung nach §§ 8–10 TMG ist somit denkbar, dass ein Beseitigungsanspruch aus der unterlassenen Befolgung der Verpflichtung zur Überwachung besteht, obwohl dies gerade nach § 7 Abs. 2 S. 1 TMG nicht der Fall sein soll. Um diesen Konflikt zu lösen, müssen diese Normen richtlinienkonform entsprechend der ECRL und nach ihrem Sinn und Zweck ausgelegt werden. Dem Willen des Gesetzgebers bei der Umsetzung der ECRL ist zu entnehmen, dass eine allgemeine aktive Überwachungspflicht nicht bestehen soll, was gerade in § 7 Abs. 2 S. 1 TMG zum Ausdruck kommt. Dies wurde nun ausdrücklich vom Europäischen Gerichtshof auch so bestätigt.[249] Erlangt der Diensteanbieter jedoch konkrete Kenntnis über rechtswidrige Informationen, die Beseitigungs- oder Unterlassungsansprüche auslösen, so soll der Diensteanbieter dann dafür nach den allgemeinen Gesetzen in die Haftung zu nehmen sein entsprechend § 7 Abs. 2 S. 2 TMG. Dies entspricht dem Willen des nationalen Gesetzgebers in seiner Begründung zum EGG[250]. Diese Auslegung erscheint auch vor der hier vertretenen Ansicht sinnvoll. Um einen Wertungswiderspruch zu vermeiden, muss die Vorschrift des § 7 Abs. 2 S. 2 TMG dahingehend einschränkend ausgelegt werden, dass eine unterlassene proaktive Überwachung nur dann an den allgemeinen Gesetzen zu messen ist, sofern der Diensteanbieter konkrete Kenntnis von den rechtswidrigen Inhalten hat.[251]

II. § 7 Abs. 2 S. 2 TMG als lex specialis

Nachdem die grundsätzliche Anwendbarkeit der Norm, wenn auch im Lichte des europäischen Gesetzgebers richtlinienkonform ausgelegt, geklärt ist, muss ihre Einordnung in das Haftungssystem erfolgen. Nach der hier vertretenen Auffassung ist § 7 Abs. 2 S. 2 TMG eine spezialgesetzliche Regelung, die über den Anwendungsbe-

---

248 Spindler/Schuster/*Hoffmann*, § 7 TMG, Rn. 32 f.

249 In der Rechtssache *Scarlet/SABAM*, Az. C-70/10, hat der EuGH in dem zugrundeliegende Vorabentscheidungsverfahren bestätigt, dass dem Access-Provider entsprechend der ECRL (RL 2000/31/EG) eine proaktive Überwachungspflicht nicht obliegt, dass die Einrichtung einer solchen gerade zu „*verboten*“ ist. (Rz. 40).

250 BT-Drs. 14/6098, S. 23.

251 Spindler/Schuster/*Hoffmann*, § 7 TMG, Rn. 36 f.

reich der §§ 8–10 TMG hinausgeht. Diese Vorschrift stellt eine Ausprägung des Grundsatzes *lex specialis derogat legi generali* dar.[252]

1. Lex specialis derogat legi generali

Bei der Regelung des § 7 Abs. 2 S. 2 TMG handelt es sich um eine Sonderregelung für den Fall, dass eine Verpflichtung zur Entfernung oder Sperrung von Informationen besteht, d.h. auch wenn der Diensteanbieter grundsätzlich die Voraussetzungen für eine Privilegierung nach den § 8–10 TMG erfüllt. Der „lex specialis“-Grundsatz stellt heraus, dass eine generelle Regelung von einer spezielleren verdrängt wird. Im Strafrecht liegt eine lex specialis insbesondere dann vor, wenn eine Norm den Grundtatbestand einer allgemeineren Norm aufweist und diesen Grundtatbestand zusätzlich noch um ein oder mehrere darüber hinausgehende Tatbestandsmerkmale erweitert und damit den Grundtatbestand auf ein gewisses Merkmal hin konkretisiert.[253]

Den Grundtatbestand die Access-Provider betreffend stellt § 8 TMG dar. Diesen bezieht die Regelung des § 7 Abs. 2 S. 2 TMG mit in seinen Tatbestand über die Formulierung „auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 bis 10“ ein. Die §§ 8–10 TMG müssen somit als Grundtatbestand erfüllt sein, damit eine „Nichtverantwortlichkeit des Diensteanbieters“ vorliegt. Die Regelung des § 7 Abs. 2 S. 2 TMG fügt diesem Grundtatbestand dann ein weiteres Merkmal hinzu: „Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben [...] unberührt“. Dabei handelt es sich um eine Erweiterung des Grundtatbestandes dahingehend, dass bestimmte Rechtsfolgen – „Verpflichtungen zur Entfernung oder Sperrung nach den allgemeinen Gesetzen bleiben [...] unberührt“ – auch eintreten sollen, wenn der Grundtatbestand erfüllt ist und dieser den Diensteanbieter grundsätzlich von sämtlicher Haftung freistellen würde.

Bereits aus dem Wortlaut des § 7 Abs. 2 S. 2 TMG, subsumiert unter die Definition des Grundsatzes lex specialis derogat legi generali, ergibt sich somit, dass diese Vorschrift der Haftungsprivilegierung nach § 8 TMG vorgeht.

---

252 *Hilgendorf/Valerius*, Rn. 217; *Valerius* BeckOK-StGB, Providerhaftung, Rn. 27; *Hilgendorf*, K&R 2011, 229, 232.

253 *Fischer*, vor § 52, Rn. 40.

2. Systematische Betrachtung

Betrachtet man die Reglung des § 7 Abs. 2 S. 2 TMG weiter systematisch, so ist kein anderes Ergebnis als die Einordnung als lex specialis zu erzielen. Dazu muss die Regelung im Kontext des Gesetzes und dessen Entstehung gesehen werden[254] sowie der europarechtlichen Grundlagen, auf der sie basiert.

a) § 7 Abs. 2 S. 2 TMG im Kontext des Gesetzes

Nimmt man die Stellung der Norm im Gefüge des Gesetzestextes, so ist festzustellen, dass diese unter der Überschrift „Allgemeine Grundsätze" zu finden ist. Diese allgemeinen Grundsätze bilden den ersten Paragraphen im „Abschnitt 3 Verantwortlichkeit", in dem die Haftung und Haftungsprivilegierung der Diensteanbieter geregelt ist. Es handelt sich somit um eine vorangestellte Regelung, bei der grundsätzlich zu erwarten ist, dass sie genereller als die nachfolgende Regelung ist. Diese Stellung die eher auf das Vorliegen einer allgemeinen Regelung schließen lässt, spricht gegen die Annahme einer lex specialis. Die speziellere Regelung ist üblicherweise nach der generelleren Regelung zu erwarten.

Dass § 7 TMG allgemeine Regelungen gegenüber den nachfolgenden trifft, mag grundsätzlich bei den übrigen Absätzen und Sätzen des § 7 TMG der Fall sein. Nicht jedoch bei der Regelung des § 7 Abs. 2 S. 2 TMG. Diese ist den §§ 8–10 TMG vorangestellt, um Wiederholungen zu vermeiden. Dies ergibt insbesondere ein Blick auf die ECRL als Rechtsgrundlage. Betrachtet man die Regeln der Art. 12–15 ECRL des Abschnittes 4, „Verantwortlichkeit der Vermittler", welche in den Regelungen der §§ 7–10 TMG in nationales Recht umgesetzt wurden, so findet man die europäische Vorlage, auf der § 7 Abs. 2 S. 2 TMG beruht[255], jeweils im letzten Absatz der Art. 12–14 ECRL statuiert[256]. Die vom nationalen Gesetzgeber im Zuge der Umsetzung geschaffene Vorschrift wurde in die allgemeinen Grundsätze von § 7 TMG aufgenommen und den übrigen Privilegierungen vorangestellt. Dadurch sollte auch eine Wiederholung am Ende jedes einzelnen Privilegierungstatbestandes vermieden werden entsprechend dem in der Rechtsetzung üblichen Grundsatz des „Vor-die-Klammer-Ziehens."

---

254 *Zippelius*, S.43.

255 Art. 12 Abs. 3, 13 Abs. 2, 14 Abs. 3 ECRL: „*Dieser Artikel läßt die Möglichkeit unberührt, daß ein Gericht oder eine Verwaltungsbehörde nach den Rechtssystemen der Mitgliedstaaten vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern.*"

256 Art. 12 Abs. 3, 13 Abs. 2, 14 Abs. 3 ECRL.

Rein die Stellung von § 7 Abs. 2 S. 2 TMG im Gesetzestext spricht daher nicht gegen die Annahme als lex specialis. Hätte der nationale Gesetzgeber diese Regelung entsprechend den Vorgaben in der ECRL am Ende jeder einzelnen Privilegierung hinzugefügt, so würde ohne Weiteres schon aus der Stellung folgen, dass es sich um eine lex specialis handelt.

b) Entstehung der Regelung des § 7 Abs. 2 S. 2 TMG

Wie bereits soeben ausgeführt, füllt diese Vorschrift den Spielraum des nationalen Gesetzgebers dahingehend aus, eine Regelung für den Fall zu schaffen, dass eine Pflicht zur Entfernung oder Sperrung von Informationen besteht. Betrachtet man die Entwicklung hin zur aktuellen Regelung des § 7 Abs. 2 S. 2 TMG, so setzt diese zum einen die Artikel 12 Abs. 3, 13 Abs. 2 und 14 Abs. 3 ECRL in nationales Recht um.[257] Bei den vorgenannten Absätzen handelt es sich um Ausnahmeregelungen über den jeweiligen Tatbestand der Grundnorm hinaus, sodass bei diesen eine *lex specialis* im Verhältnis zum Grundtatbestand der jeweiligen Privilegierungsnorm zu bejahen ist.[258] Dieser Ansicht steht auch die ECRL und insbesondere Erwägungsgrund 45[259] nicht entgegen. Dieser setzt gerade explizit die Möglichkeit der Entfernung oder Sperrung durch eine Behörde voraus. Auch die Gliederung der Erwägungsgründe, in der Erwägungsgrund 45 als Ausnahme von der Ausnahmeregelung zur Verantwortlichkeit der Diensteanbieter für Zugangsvermittler in Erwägungsgrund 43[260] genannt wird und damit eine Rückausnahme darstellt, stärkt die hier vertretene Ansicht.[261] Mit dieser Einstufung als Ausnahme von der Ausnahmeregelung macht der europäische Gesetzgeber deutlich, dass es sich um eine speziellere Norm handelt.

Zum anderen handelt es sich bei der Regelung des § 7 Abs. 2 S. 2 TMG um die der nationalen Vorgängernorm – § 5 Abs. 4 TDG a.F. – entsprechende Vorschrift.[262] Diese wurde bei der Umsetzung der ECRL im Jahre 2001 in § 8 Abs. 2 S. 2 TDG n.F. übernommen.

---

257 BT-Drs. 14/6098, S. 23.

258 Vgl. oben II.2.a.

259 Erwägungsgrund 45: *„Die in dieser Richtlinie festgelegten Beschränkungen der Verantwortlichkeit von Vermittlern lassen die Möglichkeit von Anordnungen unterschiedlicher Art unberührt. Diese können insbesondere in gerichtlichen oder behördlichen Anordnungen bestehen, die die Abstellung oder Verhinderung einer Rechtsverletzung verlangen, einschließlich der Entfernung rechtswidriger Informationen oder der Sperrung des Zugangs zu ihnen.“*

260 Vgl. Fn. 140.

261 ABl. EG Nr. L 178/1 vom 17. Juli 2000, L 178/6.

262 BT-Drs. 14/6098, S. 23.

Ebenso lässt sich aus der Stellung dieser Regelung als letzter Absatz in § 5 TDG a.F. – unter Beachtung des üblichen Gesetzesaufbaus, bei welchem die lex generalis der lex specialis vorangestellt ist[263] – auf eine lex specialis schließen, welche auch bei Vorliegen der Voraussetzungen einer Haftungsprivilegierung im Ausnahmefall doch wiederum eine Haftung zulässt, sofern die Voraussetzungen von § 5 Abs. 4 TDG a.F. vorliegen.

3. Ergebnis

Es handelt sich somit bei § 7 Abs. 2 S. 2 TMG um eine lex specialis zu den nachfolgenden Privilegierungen der §§ 8–10 TMG.[264] Dies ergibt sich zum einen aus dem Regelungsinhalt des § 7 Abs. 2 S. 2 TMG und zum anderen aus dessen systematischer Stellung im Hinblick auf die Entwicklung dieser Vorschrift aus der Vorgängernorm des § 5 Abs. 4 TDG und den europäischen Grundlagen der ECRL.

III. Anwendbarkeit im Strafrecht

Wie bereits oben erläutert, handelt es sich bei den Regelungen des TMG um Querschnittsregelungen, die grundsätzlich in allen Rechtsgebieten Anwendung finden. Dennoch gibt es einige Stimmen, die eine Anwendbarkeit im Strafrecht verneinen. Im Folgenden soll aufgezeigt werden, dass diesen jedoch zu widersprechen ist.

1. Strafgesetze als „allgemeine Gesetze“

§ 7 Abs. 2 S. 2 TMG stellt eine spezielle Regelung im Falle des Unterlassens dar. Liegen die Voraussetzungen für die Anwendung dieser Vorschrift vor, so ist die Rechtsfolge, die § 7 Abs. 2 S. 2 TMG trifft, dass der betroffene Diensteanbieter nach den *allgemeinen Gesetzen* haften soll. Umstritten ist, ob die allgemeinen Gesetze im Sinne von § 7 Abs. 2 S. 2 TMG auch die Strafgesetze umfassen sollen. Zum Teil wird vertreten, dass es sich bei den Strafgesetzen nicht um allgemeine Gesetze i.S.v. § 7 Abs. 2 S. 2 TMG handeln soll.[265] Dies wird von dieser Ansicht insbesondere damit zu begründen versucht, dass dagegen die E-Commerce-Richtlinie spreche, die

---

263 Ausgehend von der Vorstellung: die allgemeinere Norm vor der spezielleren Norm.

264 *Valerius* BeckOK-StGB, Providerhaftung, Rn. 27; *Hilgendorf/Valerius*, Rn. 217.

265 Gegen die Subsumierung der Strafgesetze unter die allgemeinen Gesetze *Leible* während des 6. Bayreuther Forums für Wirtschafts- und Medienrecht am 5./6.11.2010 im Anschluss an den Vortrag von *Hilgendorf*; ebenso MüKo-StGB/*Altenhain*, § 7 TMG, Rn. 8, m.w.N.; *Paul* in Primärrechtliche Regelungen zur Verantwortlichkeit von Internetprovidern aus strafrechtlicher Sicht.

das Strafrecht nicht betreffe.[266] Nach der hier vertretenen Ansicht sind die Strafgesetze jedoch auch im Falle des § 7 Abs. 2 S. 2 TMG unter die allgemeinen Gesetze zu fassen.[267] Dies ergibt sich wiederum aus der Auslegung des Normtextes, sodass die Strafgesetze ebenfalls unter die allgemeinen Gesetze zu subsumieren sind.

a) Grammatikalische Auslegungsmethode

Als erster Schritt muss die Auslegung nach der grammatikalischen Bedeutung vorgenommen werden, da sich eine weitergehende Auslegung verbieten würde, wenn der Gesetzestext eindeutig ist.[268] Nach der grammatikalischen Auslegungsmethode ist auf den Wortsinn im allgemeinen Sprachgebrauch abzustellen. Es gilt den Bedeutungsumfang der Gesetzesworte zu ermitteln.[269] Grundsätzlich ist zu unterscheiden zwischen generellen und speziellen Gesetzen. Betrachtet man den Wortlaut, die „Haftung nach den allgemeinen Gesetzen“, so ist lediglich festzustellen, dass der Gesetzgeber an dieser Stelle darauf verweisen wollte, dass keine Privilegierungstatbestände des TMG eingreifen und sich die Haftung nach den verwirklichten Haftungstatbeständen außerhalb des TMG richten soll. Dies ergibt auch die Gesetzesbegründung, wenn sie sich an der ECRL orientiert, die eine Beurteilung anhand der Verantwortlichkeit nach den Rechtssystemen der Mitgliedstaaten für die Haftung vorsieht.[270] Hieraus nimmt der nationale Gesetzgeber die Formulierung der Haftung nach den allgemeinen Gesetzen.[271] Da es sich hierbei um einen unbestimmten Rechtsbegriff handelt, den man mit einer Auslegung lediglich nach seinem Wortlaut nicht erfassen kann, bedarf es somit eines weiteren Auslegungsschrittes.

b) Systematische Auslegungsmethode

Nach der grammatikalischen Auslegungsmethode ist im nächsten Schritt die systematische Auslegungsmethode heranzuziehen. Die systematische Auslegungsmethode stellt den zu untersuchenden Begriff in den Kontext des zu betrachtenden Gesetzes und der gesamten Rechtsordnung.[272] Zudem sollen sich nach der systematischen Auslegungsmethode die einzelnen Normen grundsätzlich logisch zueinander verhalten. Es sollen damit Widersprüche zwischen den einzelnen Normen ausge-

---

266 Vgl. dazu unten 3.

267 So auch zuletzt *Hilgendorf*, K&R 2011, 229, 232.

268 *Bleckmann*, JuS 2002, 942, 943; BVerfGE 19, 147 (251); 47, 82; 71, 105; 78, 357.

269 *Zippelius*, S.43.

270 BT-Drs. 14/6098, S. 23.

271 A.a.O.

272 *Zippelius*, S.43.

räumt werden. Dies basiert der auf der Annahme, dass der Gesetzgeber bei Fassung eines Gesetzes logisch und rational vorgeht.[273]

Nimmt man den gesamten § 7 TMG in den Fokus, so stellt man fest, dass der Gesetzgeber den Begriff der allgemeinen Gesetze nicht nur im zu untersuchenden § 7 Abs. 2 S. 2 TMG sondern auch in § 7 Abs. 1 TMG verwendet. Die herrschende Meinung geht davon aus, dass der in § 7 Abs. 1 TMG gebrauchte Begriff der allgemeinen Gesetze auch das Strafrecht mitumfasst. Die aus diesem Abschnitt entwickelte „Lehre von der Querschnittsregelung" der Verantwortlichkeitsbestimmungen in den §§ 7–10 TMG schließt auch das Strafrecht mit ein.[274] An dieser Stelle bestand auch in der Lehre bisher kein Zweifel daran, dass auch das Strafrecht zu den allgemeinen Gesetzen zählt.[275] Die Frage, die nun aufzuwerfen ist, ist diejenige, ob tatsächlich einen Begriff, der an mehreren Stellen eines Gesetzes – vorliegend sogar in der gleichen Norm – vom Gesetzgeber bewusst verwendet wird, tatsächlich zwei verschiedene Bedeutungen beigemessen werden können.

aa) Methode des Bundesverfassungsgerichtes

Das Bundesverfassungsgericht greift bei der Auslegung eines Begriffes insbesondere auf die systematische Auslegungsmethode zurück.[276] Nach der Rechtsprechung des BVerfG gilt die Vermutung, dass dasselbe Wort in verschiedenen Vorschriften eines Gesetzes dieselbe Bedeutung hat. Betrachtet man exemplarisch die Entscheidung des BVerfG vom 30.10.1963 zur Erfassung und Auslegung des Wortes „Vereinigung" in § 129 StGB, so nimmt es einen dezidierten Vergleich mit der Verwendung dieses Begriffes in anderen Normen, z.B. §§ 92 bzw. 129a StGB vor. Das BVerfG geht dabei davon aus, dass ein bestimmter, auszulegender Ausdruck nur innerhalb der in „unserer Rechtsordnung ausgeprägten Vorstellungen verstanden werden kann.[277]" Das BVerfG legt folglich seiner Interpretation eines Begriffes die Auslegung desselben Begriffes in einer anderen Norm zugrunde und gelangt damit zu einem Gleichlauf der Verwendung eines Begriffes in demselben Gesetz.[278] Dies verlange auch der Grundsatz von der „Einheitlichkeit der Rechtsordnung".

---

273 *Bleckmann*, JuS 2002, 942, 944.

274 SSW/*Hilgendorf*, § 184 StGB, Rn 23; Spindler/Schuster/*Hoffmann*, vor § 7 TMG, Rn. 15.

275 So auch schon Spindler/Schmitz/Geis/*Spindler*, vor § 8 TDG, Rn. 13, m.w.N.; an dieser Stelle sieht dies auch MüKo-StGB/*Altenhain*, vor § 7 TMG, Rn. 2, der jedoch dann im Rahmen des § 7 Abs. 2 S. 2 TMG widersprüchlich die Strafgesetze nicht mehr unter die *allgemeinen Gesetze* fasst.

276 BVerfGE 19, 147, 151; 47, 82; 71, 105; 78, 357; *Bleckmann*, JuS 2002, 942, 943.

277 BVerfGE 17, 164, 166.

278 BVerfGE 17, 164, 167; 26, 27, 28; 71, 53, 55.

Die Methode des Verfassungsgerichtes zielt darauf ab, aus der gemeinsamen Betrachtung aller Normen eines bestimmten Gesetzes gemeinsame Rechtsauslegungsgrundsätze zu schöpfen und diese dann auf alle Normen des gleichen Gesetzes anzuwenden, um einzelne Begriffe oder Normen auszulegen.[279]

bb) Stellungnahme

Betrachtet man nun die vorliegende Formulierung des Begriffes der „allgemeinen Gesetze“, so ist im Rahmen der systematischen Betrachtung zunächst auf die Stellung im Gesetzestext einzugehen. Die Vorschrift des § 7 Abs. 2 S. 2 TMG ist in § 7 TMG in den allgemeinen Vorschriften aufgeführt, die den spezielleren Haftungsprivilegierungen vorangestellt ist. Schon dies spricht für eine weite Auslegung des Begriffes der allgemeinen Gesetze. Hinzu kommt, dass nach dem BVerfG eine Vermutung dafür spricht, dass ein Begriff, der in mehreren Normen ein und desselben Gesetzes verwendet wird, nicht unterschiedlich auszulegen ist. Dieses Argument trifft hier im Besonderen zu, denn wenn schon in dem selben Gesetz in verschiedenen Normen ein Begriff gleich auszulegen ist, so muss dies hier umso mehr gelten, wenn es sich um die Auslegung eines Begriffes in dem selben Paragraphen handelt.

cc) Vergleich mit Art. 5 Grundgesetz

Anstrengen lässt sich im Rahmen der systematischen Auslegung auch ein Vergleich mit Art. 5 GG. Das Grundrecht der Meinungs- und Pressefreiheit findet seine Schranken gem. Art. 5 Abs. 2 GG in den allgemeinen Gesetzen, welche damit den Rahmen dieses Grundrechtes bilden. Eine abstrakt-generelle Formulierung reicht im Anwendungsbereich des Art. 5 Abs. 2 GG noch nicht aus, um ein Gesetz als allgemein im Sinne dieser Vorschrift zu fassen.[280] Hinzukommen muss nach der schon im Rahmen der Weimarer Reichsverfassung vorherrschenden und vom Bundesverfassungsgericht übernommenen Sonderrechtslehre in diesem Zusammenhang eine Meinungsneutralität dieser allgemeinen Gesetze.[281] Unter diesen Begriff werden grundsätzlich auch die Strafgesetze subsumiert, denn sie zielen nicht auf eine bestimmte Meinungsindoktrination, gleich in welche Richtung, ab.[282]

---

279 *Bleckmann*, JuS 2002, 942, 943.
280 *Pieroth/Schlink*, Rn. 632.
281 *Pieroth/Schlink*, Rn. 633.
282 *Pieroth/Schlink*, Rn. 642 f.

Es ist somit festzuhalten, dass unter den grundgesetzlich verwendeten Begriff der allgemeinen Gesetze die Strafgesetze zu fassen sind. Dem ist zu entnehmen, dass der Gesetzgeber bei der Verwendung dieses Begriffes grundsätzlich davon ausgeht, dass von diesem die Strafgesetze mitumfasst sind.

dd) Stellungnahme

Zieht man nun die Auslegungsmethode des BVerfG heran und legt den Begriff der *allgemeinen Gesetze* in § 7 Abs. 2 S. 2 TMG unter Heranziehung der grundgesetzlichen Bedeutung des Begriffes *allgemeine Gesetze* in Art. 5 Abs. 2 GG aus, so ist auch hier davon auszugehen, dass der Gesetzgeber eine einheitliche Auslegung dieses Begriffes wollte. Wäre etwas anderes vom Gesetzgeber gewollt gewesen, so wäre zu erwarten, dass sich dies aus der Gesetzesbegründung ergibt und der Gesetzgeber einen entgegenstehenden Willen zumindest dort zum Ausdruck gebracht hätte.

c) Ergebnis

Die besseren Argumente sprechen an dieser Stelle für eine Subsumierbarkeit der Strafgesetze unter den Begriff der allgemeinen Gesetze in § 7 Abs. 2 S. 2 TMG. Die gegenteilige Ansicht ist abzulehnen. Betrachtet man § 7 Abs. 2 S. 2 TMG systematisch, so ist der Begriff der allgemeinen Gesetze nicht anders als in § 7 Abs. 1 TMG auszulegen. Dies ergibt sich insbesondere aus dem Vergleich mit Art. 5 GG, bei welchem unter den Begriff der allgemeinen Gesetze nach der herrschenden Meinung auch die Strafgesetze zu fassen sind, und zum anderen aus dem noch näher liegenden Vergleich mit § 7 Abs. 1 TMG, bei welchem auch nach der herrschenden Meinung unter den Begriff der allgemeinen Gesetze die Strafgesetze zu subsumieren sind. Nimmt man nun hierzu die Vermutung des BVerfG, dass ein Begriff in einem Gesetz grundsätzlich nicht unterschiedlich auszulegen ist, so muss dies auch in diesem Falle gelten, wenn zum einen ein Vergleich mit dem Grundgesetz an sich angestellt werden kann und zum anderen ein Begriff innerhalb der selben Norm zweimal verwendet wird. Dies gebietet auch die Einheit der Rechtsordnung. Unter den Begriff der allgemeinen Gesetze in § 7 Abs. 2 S. 2 TMG sind daher auch die Strafgesetze zu fassen.

2. Keine Bedeutung des § 7 Abs. 2 S. 2 TMG im Strafrecht

Eine noch weitergehende Ansicht zu der vorliegenden Frage, ob § 7 Abs. 2 S. 2 TMG auch im Strafrecht Anwendung findet, verneint dies von Anfang an. § 7 Abs. 2 S. 2 TMG betreffe das Strafrecht schon gar nicht.[283] Diese Ansicht stützt sich insbesondere auf die zu § 5 Abs. 4 TDG a.F. in einem großen Teil der Literatur vertretenen Meinung, § 5 Abs. 4 TDG a.F. sei nicht auf strafrechtliche Tatbestände anwendbar und treffe keine Regelungen hierfür.

a) § 5 Abs. 4 TDG a.F.

Die Vertreter der Ansicht, dass § 7 Abs. 2 S. 2 TMG auf die Strafgesetze nicht anwendbar sei, begründen ihre Auffassung mit einem Blick auf § 5 Abs. 4 TDG a.F.[284] Bei dieser Regelung, der ersten Fassung des TDG im Rahmen des IuKDG von 1997, sind die Verantwortlichkeitsregelungen noch einzig in § 5 TDG a.F. verankert. Diese Ansicht stellt darauf ab, dass schon zu § 5 TDG a.F. vertreten wurde, dass lediglich die Absätze 1–3 auch eine strafrechtliche Bedeutung hätten, nicht jedoch § 5 Abs. 4 TDG a.F.[285] Dieser regele lediglich schuldunabhängige Verpflichtungen und schließe somit die Heranziehung des Strafrechts aus. Damit scheide auch die Subsumierung der Strafgesetze unter den Begriff der allgemeinen Gesetze i.S.v. § 5 Abs. 4 TDG a.F. aus, da im Strafrecht das Vorliegen des Merkmales der Schuld immer Voraussetzung sei. Diese Ansicht erklärt sich insbesondere mit einem Blick in die Begründung des IuKDG. Hier wird zu § 5 Abs. 4 TDG a.F. ausgeführt, dass die Absätze 1–3 die „strafrechtliche und deliktische Verantwortlichkeit der Diensteanbieter für eigenes Verschulden zum Gegenstand haben“, § 5 Abs. 4 TDG a.F. hingegen die verschuldensunabhängige Verantwortlichkeit.[286] Daraus sei zu schließen, dass hier auf Gesetze mit verschuldensunabhängigen Anspruchsgrundlagen verwiesen wird, zu denen die Strafgesetze bekanntlich nicht gehörten, da sie immer eine Schuldkomponente benötigen.[287] Darüber hinaus handele es sich um für den Einzelfall getroffene Anordnungen, die zwar im Zivil-, Ordnungs- und Sicherheitsrecht

---

283 MüKo-StGB/*Altenhain* § 7 TMG, Rn. 8.

284 MüKo-StGB/*Altenhain* § 7 TMG, Rn. 8.

285 *Kudlich*, Jura 2001, 305, 310, m.w.N.

286 BT-Drs. 13/7385, S. 20 f.

287 Mit dieser Begründung auch zuletzt *Leible* während des 6. Bayreuther Forums für Wirtschafts- und Medienrecht am 5./6.11.2010 im Anschluss an den Vortrag von *Hilgendorf* (Fn. 265); ebenso MüKo-StGB/*Altenhain*, § 7 TMG, Rn. 8; *Paul*, Primärrechtliche Regelungen zur Verantwortlichkeit von Internetprovidern aus strafrechtlicher Sicht; *Bleisteiner,* Rechtliche Verantwortlichkeit im Internet, S. 205ff; *Hoeren*, MMR 1998, 97, 98.

vorkommen, die aber im Strafrecht nicht denkbar sind, da dort generelle Regelungen getroffen werden, die nicht lediglich einzelfallbezogen sind.[288]

b) Stellungnahme

Diese Ansicht, die sich auf die Begründung des IuKDG bezieht, übersieht jedoch, dass der Wortlaut der Erklärung zu § 5 Abs. 4 TDG a.F. überwiegend auf die Formulierung „Verschulden" bzw. „verschuldensunabhängig" abstellt. Es handelt sich hierbei um einen zivilrechtlich geprägten Begriff, der sich auf Vorsatz und Fahrlässigkeit bezieht. Damit bringt der Gesetzgeber seinen Willen zum Ausdruck, dass für die Verpflichtung zur Entfernung und Sperrung rein objektive Gründe ausreichen sollen und es auf eine subjektive Komponente grundsätzlich nicht ankommt, d.h. diese nicht Voraussetzung sein soll.[289]

Aus der von dieser o.g. Ansicht vielfach zitierten Formulierung, § 5 Abs. 4 TDG a.F. betreffe „die objektiven, d.h. keine Schuld voraussetzenden Verpflichtungen der Diensteanbieter", kann jedoch die Anwendbarkeit des Strafrechtes nicht geschlossen werden. Dies insbesondere auch aufgrund der Tatsache, dass bei einem unechten Unterlassungsdelikt die Garantenstellung und die Garantenpflicht gerade im objektiven Tatbestand zu prüfen sind, d.h. eine Verpflichtung zur Entfernung oder Sperrung, auch unabhängig von der Schuldfrage des Täters stehen kann.[290] Damit kann vorliegend nicht auf § 5 Abs. 4 TDG a.F. zur Begründung der Aussage, § 7 Abs. 2 S. 2 TMG betreffe die Strafgesetze nicht, rekurriert werden.

c) Gesetzesbegründung zum TDG

Ein weiteres Argument, das gegen die Ansicht spricht, dass § 7 Abs. 2 S. 2 TMG nicht für das Strafrecht gelte, ergibt sich aus der Gesetzesbegründung zum TDG.[291] Der Gesetzgeber hat einen solchen Willen schon nicht explizit zum Ausdruck gebracht. Dass § 7 Abs. 2 S. 2 TMG das Strafrecht nicht betreffe, ist der Gesetzesbegründung nicht zu entnehmen. Es darf jedoch davon ausgegangen werden, dass der Gesetzgeber eine von ihm gewünschte Ausnahme von der alle Rechtsgebiete erfassenden Querschnittsregelung, wenn schon nicht im Gesetzestext selbst, dann doch zumindest in die Gesetzesbegründung aufgenommen hätte. Dies ist jedenfalls in aus-

---

288 *Kudlich*, Jura 2001, 305, 310, m.w.N.

289 *Hilgendorf*, NStZ 2000, 518, 520.

290 *Hilgendorf*, NStZ 2000, 518, 520.

291 Auf diese nimmt auch die Begründung des TMG Bezug, die zur Frage der Verantwortlichkeit auf die Begründung zum TDG n.F. verweist, vgl. BT-Drs. 16/3078, S.15.

drücklicher Form nicht der Fall. Der Gesetzgeber hat vielmehr in der Begründung zum TDG n.F. in den Vorbemerkungen zu den §§ 8–11 TDG auf die Geltung dieser Regelungen in strafrechtlicher Hinsicht hingewiesen.[292]

Darüber hinaus ergibt sich auch noch aus einem weiteren Grund, weshalb der Gesetzgeber von der Anwendbarkeit von § 7 Abs. 2 S. 2 TMG auch im Strafrecht ausgeht. Vor dem eben dargelegten Hintergrund, dass es sich bei den Regelungen zur Verantwortlichkeit im TMG um Querschnittsregeln handelt, die auf sämtliche Rechtsgebiete Anwendung finden, sind auch die Stellungnahme des Bundesrates im Gesetzgebungsverfahren zum TDG und die Gegenäußerung der Bundesregierung einzuordnen und zu deuten. Der Bundesrat äußerte in seiner Stellungnahme die Auffassung, dass zur Klarstellung der Bedeutung der Verantwortlichkeitsregelungen im strafrechtlichen Sinne ein Satz aufgenommen werden müsse, aus dem eindeutig hervorgehe, dass in der Regel eine Garantenstellung i.S.v. § 13 StGB bestünde, wenn eine Verantwortlichkeit für fremde Informationen gegeben sei.[293] Die Bundesregierung stellte in ihrer Gegenäußerung fest, dass eine Garantenpflicht nach § 13 StGB dadurch in der Regel gerade nicht entstehen solle.[294]

Konkludent geht der Gesetzgeber damit davon aus, dass – unabhängig von einer Garantenpflicht – die Strafgesetze uneingeschränkt anwendbar sein sollen.[295] Durch die Einschränkung „in der Regel“ wird klargestellt, dass auch eine Haftung für Unterlassungsdelikte dadurch nicht ausgeschlossen wird. Auch hier hätte der Gesetzgeber die Möglichkeit gehabt klarzustellen, dass er die spezielle Regelung des § 7 Abs. 2 S. 2 TMG für Unterlassungstaten nicht für eine Anwendung im Strafrecht statuiert hat. Dies hat er wiederum nicht getan.

d) Ergebnis

Die Ansicht, die eine Anwendung des § 7 Abs. 2 S. 2 TMG im Strafrecht ausschließt, ist abzulehnen. Die zu § 5 Abs. 4 TDG a.F. vertretene Ansicht übersieht, dass gerade die Garantenstellung ein im objektiven Tatbestand zu prüfendes Merkmal darstellt und damit eine objektive Tatbestandserfüllung – wie von § 7 Abs. 2 S. 2 TMG vorausgesetzt – zulässt. Die Frage der strafrechtlichen Schuld ist hiervon unabhängig, sodass dieser Ansicht nicht zu folgen ist.

---

[292] BT-Drs. 14/6098 S. 22 f.
[293] BT-Drs. 14/6098, S. 34, *Nr. 11*.
[294] BT-Drs. 14/6098, S. 37, *Zu Nummer 11*.
[295] Spindler/Schuster/*Hoffmann*, vor § 7 TMG, Rn. 15 a.E.

Des Weiteren ergibt sich aus der Gesetzesbegründung zum TDG, welche auch für das TMG weiter Geltung beansprucht, dass die Normen zur Verantwortlichkeit in ihrer Gesamtheit entsprechend der vom Gesetzgeber gewollten Querschnittsregelung auch die Strafgesetze mitumfassen.

3. E-Commerce-Richtlinie schließe die Anwendbarkeit im Strafrecht aus

Eine weitere Meinung vertritt die Ansicht, § 7 Abs. 2 S. 2 TMG sei im Rahmen der Strafgesetze nicht anzuwenden, weil die E-Commerce-Richtlinie dies ausschließe.[296] Ein Teil dieser wenig differenzierenden Ansicht vertritt die Auffassung, aus der ECRL selbst sei zu entnehmen, dass diese nicht im Zusammenhang mit den Strafgesetzen anzuwenden sei.[297] Ein anderer Teil beruft sich darauf, dass die Regelungen des TMG richtlinienkonform auszulegen sind, und kommt so zu der Auffassung, dass § 7 Abs. 2 S. 2 TMG keine Anwendung im Rahmen der strafrechtlichen Access-Provider Haftung finden kann.[298]

a) Direkter Ausschluss durch die E-Commerce-Richtlinie

Wie bereits angeführt, vertritt ein Teil der an dieser Stelle zu behandelnden Ansicht, dass sich aus dem Wortlaut der E-Commerce-Richtlinie selbst bzw. den Erwägungsgründen derselben ergebe, dass eine Anwendung des § 7 Abs. 2 S. 2 TMG nicht in Betracht komme.[299]

aa) Ausschluss anhand der E-Commerce-Richtlinie

Begründet wird dies teilweise mit einem Verweis auf Erwägungsgrund 8[300] der ECRL, der vorgibt, dass es nicht Ziel der ECRL sein soll, „den Bereich des Strafrechts als solchen zu harmonisieren“. Daraus wird dann der Schluss gezogen, dass die ECRL von sich aus die Anwendbarkeit ihrer Regelungen für das Strafrecht ausschließe, was sich unmissverständlich aus dem zitierten Halbsatz entnehmen lasse.

---

296 MüKo-StGB/*Altenhain*, § 7 TMG, Rn. 8.
297 *Gercke/Brunst*, Rn. 616; *Kudlich*, JA 2002, 798, 802.
298 *Kudlich*, JA 2002, 798, 802
299 *Gercke/Brunst*, Rn. 616; *Kudlich*, JA 2002, 798, 802.
300 Vgl. Fn. 45.

bb) Stellungnahme

Diese Mindermeinung ist von vornherein abzulehnen. Sie spiegelt sich weder in der Intention des europäischen Richtliniengebers noch in den Regelungen der ECRL selbst wider. Die ECRL nimmt in den Erwägungsgründen an mehreren Stellen auf das nationale Strafrecht der Mitgliedstaaten Bezug. Auch ist den Art. 12 Abs. 3, 13 Abs. 2 und 14 Abs. 3 ECRL sowie dem dazugehörigen Erwägungsgrund 45[301], die in § 7 Abs. 2 S. 2 TMG ihre nationale Umsetzung gefunden haben, nicht zu entnehmen, dass diese nicht für das Strafrecht gelten sollen. Zudem beruht diese Meinung auf der unrichtigen Folgerung, dass aus einer nicht gewünschten Vollharmonisierung im strafrechtlichen Bereich auf einen generellen Ausschluss des § 7 Abs. 2 S. 2 TMG für das gesamte Strafrecht geschlossen werden kann.[302] Eine Vollharmonisierung schließt mitnichten die Regelung einzelner Teilgebiete oder gar die Anwendung der ECRL auf ein gesamtes Teilrechtsgebiet wie das Strafrecht aus. Diese Ansicht ist damit abzulehnen.

b) Richtlinienkonforme Auslegung des § 7 Abs. 2 S. 2 TMG

Eine weitaus bedeutsamere Ansicht, die auch schon zu § 8 Abs. 2 S. 2 TDG[303] vertreten wurde, stellt größtenteils darauf ab, dass diese Norm vor dem Hintergrund der Umsetzung der ECRL im nationalen Recht richtlinienkonform ausgelegt werden muss. Bei der Umsetzung der Art. 12 Abs. 3, 13 Abs. 2 und 14 Abs. 3 ECRL sei es vom nationalen Gesetzgeber unterlassen worden die spezielle Formulierung der E-CRL,

„...ein Gericht oder Verwaltungsbehörden nach den Rechtssystemen der Mitgliedsstaaten vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern...“,

ausreichend präzise zu übernehmen. Der Passus soll nach dieser Ansicht dafür sprechen, dass nur zivilrechtliche oder sicherheitsbehördliche Unterlassungsverfügungen in Betracht kommen, diese Norm zu erfüllen. Dies ergebe sich zudem aus der norminternen Systematik des § 8 Abs. 2 S. 2 TDG, nämlich aus der Verwendung des Begriffes „Verpflichtung“ durch den Gesetzgeber im Zuge der Umsetzung in das nationale Recht, welcher von dem Begriff der „Verantwortlichkeit“ zu unterscheiden sei. Letztere hätte möglicherweise auch das Strafrecht mitumfasst, der Begriff der „Verpflichtung“ jedoch sei zukunftsgewandt und betreffe lediglich Vorschriften aus

[301] Vgl. Fn. 259.
[302] MüKo-StGB/*Altenhain*, vor § 7 TMG, Rn. 2; Spindler/Schuster/*Hoffmann*, vor § 7 TMG, Rn. 15.
[303] § 8 Abs. 2 S. 2 TDG entspricht dem aktuellen, hier behandelten § 7 Abs. 2 S. 2 TMG.

dem Zivil- bzw. dem Verwaltungsrecht.[304] Diesem Versäumnis des Gesetzgebers sei nur mit richtlinienkonformer Auslegung des § 8 Abs. 2 S. 2 TDG[305] beizukommen. Die richtlinienkonforme Auslegung hätte zudem auch schon vor der Umsetzung angewendet werden müssen.[306]

aa) Methode der richtlinienkonformen Auslegung

Nach den Vorgaben des Europäischen Gerichtshofes erfordert das Unionsrecht, dass nationale Rechtsnormen soweit möglich europarechts- und damit richtlinienkonform auszulegen sind.[307] Die nationalen Gerichte müssen dabei alle Auslegungsspielräume ausschöpfen, damit die entsprechende Richtlinie im nationalen Recht Wirkung entfalten kann.[308] Die Pflicht zur richtlinienkonformen Auslegung besteht grundsätzlich erst nach Ablauf der Umsetzungsfrist.[309] Die Reichweite der richtlinienkonformen Auslegung umfasst alle Rechtsnormen, gleich ob sie vor oder nach der Richtlinie erlassen wurden.[310] Auch im hier vorliegenden Fall, in welchem die nationale Vorschrift bereits die Umsetzung der europäischen Richtlinie darstellt, ist nach dem EuGH eine richtlinienkonforme Auslegung durchaus noch von Nöten. Die Umsetzung einer Richtlinie in nationales Recht entbindet nicht von der Auslegung dieser Rechtsnorm selbst im Sinne des Wortlauts und des Zwecks der Richtlinie.[311]

bb) Richtlinienkonforme Auslegung anhand der E-Commerce-Richtlinie

Betrachtet man nun den § 7 Abs. 2 S. 2 TMG im Lichte der ECRL, so sind zum einen die expliziten Regelungen der Richtlinie und zum anderen deren Erwägungsgründe zu beleuchten.

---

304 *Kudlich* in JA 2002, 798, 802; *Kudlich*, Die Unterstützung fremder Straftaten durch berufsbedingtes Verhalten, S. 505; mit dieser Begründung auch zuletzt *Kudlich* während des 6. Bayreuther Forums für Wirtschafts- und Medienrecht am 5./6.11.2010 in der Diskussion im Anschluss an den Vortrag von *Hilgendorf* (vgl. auch Fn. 265 und 287).

305 *Kudlich*, JA 2002, 798, 802.

306 *Satzger*, CR 2001, 109, 110; ebenso *Kudlich*, JA 2002, 798, 802.

307 EuGH, verb. Rs. C-397/01 – C-403/01, Slg. 2004, I-8835 Rn. 113 ff. – *Pfeiffer.*

308 *Herdegen*, § 8, Rn. 42.

309 EuGH, Rs. C-212/04, Slg. 2006, I-6057 Rn. 115 – *Adeneler.*

310 *Herdegen*, § 8, Rn. 41.

311 EuGH, Rs. 14/83, Slg. 1984, 1891ff – *von Colson & Kamann.*

(1) Artikel 12 Abs. 3, 13 Abs. 2 und 14 Abs. 3 E-Commerce-Richtlinie

Die Art. 12 Abs. 3, 13 Abs. 2 und 14 Abs. 3 ECRL wurden zur Umsetzung in nationales Recht in der heutigen Vorschrift des § 7 Abs. 2 S. 2 TMG[312] festgeschrieben.[313] Die bereits dargelegte Ansicht[314] geht davon aus, dass die Vorschriften nicht ordnungsgemäß umgesetzt wurden und es deshalb einer Korrektur über das Werkzeug der richtlinienkonformen Auslegung bedürfe. Diese Ansicht ist jedoch abzulehnen. An dieser Stelle müssen die Vorschriften der ECRL im Zusammenhang mit ihren Erwägungsgründen betrachtet werden. Zieht man zu deren Auslegung Erwägungsgrund 45[315] heran, so sind diesem mehrere Anhaltspunkte zu entnehmen, die gegen diese Ansicht sprechen.

(a) „Anordnungen unterschiedlicher Art“

Im ersten Satz des Erwägungsgrundes 45, auf den die Art. 12 Abs. 3, 13 Abs. 2 und 14 Abs. 3 ECRL zurückgehen, wird zunächst einmal klargestellt, dass die in der Richtlinie festgelegten Beschränkungen hinsichtlich der Diensteanbieter „die Möglichkeit von Anordnungen unterschiedlicher Art unberührt“ lassen. Eine Einschränkung auf solche von Gerichten und Verwaltungsbehörden, wie sie im Normtext[316] vorgenommen wird, ist hier noch nicht angelegt. Vielmehr verwendet der Richtliniengeber die Formulierung „Anordnungen unterschiedlicher Art“, was dafür spricht, dass er es nicht mit der beispielhaften Ausführung im Normtext bewenden lassen möchte.

Unter den Begriff der „Anordnungen unterschiedlicher Art“ lassen sich Verpflichtungen zum Handeln bzw. Tätigwerden, die aufgrund des Vorliegens einer Garantenstellung entstehen, ebenfalls subsumieren. Durch die Formulierung „Anordnungen unterschiedlicher Art“ wird die etwas starre Verwendung des Wortes „Anordnung“ aufgebrochen und damit die Möglichkeit einer weiten Auslegung geschaffen.

---

312 § 7 Abs. 2 S. 2 TMG ist die gleichlautende Nachfolgeregelung von § 8 Abs. 2 S. 2 TDG, der ursprünglich bei der Umsetzung der ECRL geschaffen wurde.

313 BT-Drs. 14/6098, S. 23.

314 Vgl. Fn. 305.

315 Vgl. Fn. 259.

316 *„...Gericht oder Verwaltungsbehörden...“.*

(b) Insbesondere gerichtliche oder behördliche Anordnungen

Im zweiten Satz des Erwägungsgrundes 45[317] findet sich die Formulierung, dass diese Anordnungen unterschiedlicher Art „insbesondere in gerichtlichen oder behördlichen Anordnungen bestehen“ können. Beachtlich ist hier die Verwendung des Wortes „insbesondere“ durch den europäischen Richtliniengeber. Betrachtet man die Wortbedeutung, so ist festzustellen, dass das Wort „insbesondere“ eine nicht abschließende Aufzählung einleitet.

Das bedeutet, dass vorliegend mit dieser Formulierung zum Ausdruck gebracht werden soll, dass gerade nicht nur gerichtliche oder behördliche Anordnungen in Betracht kommen, sondern auch vergleichbare bzw. darüberhinausgehende Alternativen, die eine Verpflichtung zum Tätigwerden generieren. Die Intention des europäischen Richtliniengebers bei der Schaffung der Art. 12 Abs. 3, 13 Abs. 2 und 14 Abs. 3 ECRL ist daher entsprechend dem Erwägungsgrund 45[318] dahingehend auszulegen, dass auch andere Anordnungen vorliegen können, die zu einem Wiederaufleben der Haftung führen.

(2) Stellungnahme

Zieht man zur Ermittlung des Willens des europäischen Richtliniengebers die Art. 12 Abs. 3, 13 Abs. 2 und 14 Abs. 3 ECRL und deren korrespondierenden Erwägungsgrund 45 heran, um zu einer richtlinienkonformen Auslegung des § 7 Abs. 2 S. 2 TMG zu gelangen, so ist die oben dargelegte Meinung abzulehnen, denn auch im Rahmen richtlinienkonformer Auslegung sprechen die besseren Argumente für die Anwendbarkeit des § 7 Abs. 2 S. 2 TMG auch im Strafrecht.

Die Anwendung der Strafgesetze im Rahmen des § 7 Abs. 2 S. 2 TMG ist nicht richtlinienwidrig, denn es ist nach dem Willen des europäische Richtliniengebers nicht ausgeschlossen, auch andere Anordnungen als gerichtliche oder behördliche heranzuziehen, um die in § 7 Abs. 2 S. 2 TMG statuierte „Verpflichtung zur Entfernung oder Sperrung“ zu begründen. Es ist daher keineswegs ausgeschlossen, diese Verpflichtung auch in einer aus einer Garantenstellung abgeleiteten Pflicht zum Tätigwerden zu sehen.

---

317 Vgl. Fn. 259.

318 Vgl. Fn. 259.

c) Erwägungsgrund 42 der E-Commerce-Richtlinie

Ein weiteres Argument, welches an dieser Stelle genannt werden muss und gegen den Ausschluss der strafrechtlichen Haftung spricht, ergibt sich aus Erwägungsgrund 42[319] der ECRL. Auch dieser muss zumindest im Rahmen der richtlinienkonformen Auslegung herangezogen werden.

aa) Funktionale Betrachtungsweise

Nach Erwägungsgrund 42 tritt eine Privilegierung des Diensteanbieters dann ein, wenn die Tätigkeit „rein technischer, automatischer und passiver Art“ *ist*, worauf sich das Augenmerk dieser Ansicht richtet. Sie geht von einer funktionalen Betrachtungsweise anhand der vom Zugangsvermittler vorgenommenen Handlungen aus.[320] Erwägungsgrund 42[321] definiert im folgenden selbst, was unter Zugangsvermittlung in „rein technischer, automatischer und passiver Art“ zu verstehen ist:

„Diese Tätigkeit ist rein technischer, automatischer und passiver Art, was bedeutet, dass der Anbieter eines Dienstes der Informationsgesellschaft weder Kenntnis noch Kontrolle über die weitergeleitete oder gespeicherte Information besitzt.“

Somit gibt der europäische Richtliniengeber vor, dass ab Kenntnis, dass rechtswidrige Informationen durchgeleitet werden, und bei vorausgesetzter Kontrollmöglichkeit – was technisch heute aufgrund der Möglichkeit von Deep-Packet-Inspections unproblematisch sein dürfte – die Tätigkeit des Diensteanbieters bzw. Access-Providers nicht mehr als „rein technischer, automatischer und passiver Art“ anzusehen ist. Damit begibt sich der Diensteanbieter seiner Privilegierung, da seine Tätigkeit nicht mehr auf den technischen Vorgang beschränkt ist, wie der erste Satz von Erwägungsgrund 42 fordert. Folglich ist zumindest auch im Rahmen der richtlinienkonformen Auslegung davon auszugehen, dass die Privilegierung des § 8 TMG die Anwendung des § 7 Abs. 2 S. 2 TMG nicht gänzlich verdrängen kann.[322]

---

319 Vgl. Fn. 127.

320 *Hilgendorf/Valerius*, Rn. 221; *Kessler*, Zur strafrechtlichen Verantwortlichkeit von Zugangsvermittlern, S.87.

321 Vgl. Fn. 127.

322 Diese Ansicht vertritt wie bereits oben unter Fn. 304 ausgeführt insb. immer noch *Kudlich.*

bb) Handeln durch Unterlassen

Die auf dieser Ansicht fußende Meinung, die insbesondere von *Kessler*[323] vertreten wird, differenziert weiter nach der Art der Handlung des Diensteanbieters.

(1) Differenzierende Ansicht

Die differenzierende Ansicht stellt die einzelne Tätigkeit des Diensteanbieters heraus und dann anhand der Tatbestandsmerkmale geprüft. Dies erfolgt grundsätzlich losgelöst von der starren Einteilung der Provider nach dem System der ECRL bzw. des TMG. Betrachtet wird nicht zuerst der Typus des Diensteanbieters, um schließlich anhand der Vorschriften des TMG eine quasi vorsortierte und vorprivilegierte Einordnung zu treffen, sondern betrachtet wird unabhängig davon die konkrete Handlung, um dann erst anhand dieser eine Einordnung als entsprechender Provider vorzunehmen.

(2) Handlung des Access-Providers

Wendet man nun diese Ansicht auf das Kernproblem der vorliegenden Arbeit an, so muss zunächst die Handlung herausgestellt werden. Hier zu behandeln ist, wie bereits erörtert, das Unterlassen einer Handlung durch den Access-Provider. Die vorgenannte Ansicht gelangt dabei zu dem Ergebnis, dass das Unterlassen von Sperrmaßnahmen oder der Entfernung von rechtswidrigen Inhalten eine Handlung darstellt, die nicht im Sinne der ECRL und folglich den §§ 7–10 TMG privilegiert ist. Vorausgesetzt natürlich, es besteht eine Verpflichtung zum Handeln, welche sich aus einer behördlichen Anordnung, gerichtlichen Verfügung, aber auch aus einer Garantenstellung ergeben kann.[324]

Unter der Prämisse, dass es sich um eine von vorneherein nicht privilegierte Tätigkeit handelt, und damit § 8 TMG nicht einschlägig ist, stellt sich bei dieser Ansicht die Frage, wie nun der nächste Prüfungsschritt zu vollziehen ist. Betrachtet man die Regelungen des TMG, so stellt man fest, dass nun diese Tätigkeit, das Unterlassen von Sperrmaßnahmen bzw. der Entfernung dieser fremden Informationen, nicht mehr unter § 7 Abs. 1 TMG – es handelt sich nicht um eigene Informationen – aber auch nicht mehr unter § 7 Abs. 2 S. 2 TMG – es handelt sich nicht um eine privilegierte Tätigkeit – subsumiert werden kann.

---

323 *Kessler*, Zur strafrechtlichen Verantwortlichkeit von Zugangsvermittlern, S. 87 ff.

324 Zum Vorliegen einer Garantenstellung vgl. unten IV. Garantenstellung.

Die Beurteilung der Strafbarkeit wäre danach ausschließlich ohne die Heranziehung des TMG zu treffen.

cc) Stellungnahme

Diese von *Kessler* entwickelte, rein nach der Handlung differenzierende Meinung ist so im Rahmen des TMG kaum vertretbar. Sie verfehlt den Regelungszweck des TMG, denn es kann nicht einzig und allein nach der auszuführenden Tätigkeit differenziert werden, sondern es muss auch die subjektive Seite der Kenntnis des Vorliegens rechtswidriger Informationen betrachtet werden. Damit würde die von der E-CRL vorgenommene Unterteilung in verschiedene Providerarten und die Differenzierung nach eigenen und fremden Informationen unterlaufen. Das widerspricht dem Zweck des Gesetzes, nachdem mit der ECRL und dem TMG eine einheitliche Regelung für die Verantwortlichkeit entstehen sollte. Damit wäre auch deren Funktion als horizontale Querschnittsregelung aufgehoben. Dies kann vom Gesetzgeber nicht gewünscht gewesen sein, der eine umfassende Regelung im Auge hatte. Diese allzu sehr differenzierende Ansicht ist daher abzulehnen.

d) Ergebnis

Nimmt man eine funktionale Betrachtungsweise vor, so ist dies, unter Heranziehung von Erwägungsgrund 42[325], ein weiteres Argument, welches die Ansicht stützt, dass auch das Strafrecht nicht im Rahmen des § 7 Abs. 2 S. 2 TMG auszuschließen ist. Gerade das Abstellen des Erwägungsgrundes 42 auf Kenntnis und Kontrollmöglichkeit des Diensteanbieters spricht dafür, dass, sofern diese beiden Punkte vorliegen, eine Privilegierung nicht mehr bestehen kann und damit auch ein Eingreifen der Strafgesetze über die Ausnahme des § 7 Abs. 2 S. 2 TMG möglich sein muss.[326]

4. Gesamtergebnis

Es ist somit als Gesamtergebnis festzuhalten, dass die Argumente gegen eine Anwendung des Strafrechtes im Rahmen des § 7 Abs. 2 S. 2 TMG abzulehnen sind.[327] Vielmehr sprechen nach einer kritischen Analyse derselbigen die besseren Argumente für eine Anwendung des Strafrechtes.

---

325 Vgl. Fn. 127.

326 *Hilgendorf,* K&R 2011, 229, 233.

327 A.A. MüKo-StGB/*Hörnle*, § 184, Rn. 48, m.w.N.

Zum einen sind die Strafgesetze logischerweise nach Sinn und Zweck, aber auch nach der systematischen Stellung, unter die „allgemeinen Gesetze“ im Sinne des § 7 Abs. 2 S. 2 TMG – insbesondere nach der heutigen Fassung des TMG – zu subsumieren. Die sehr kritische Anmerkung von *Hoeren* im Anschluss an die Einstellungsverfügung des Generalbundesanwaltes 1998[328] ist damit nicht mehr haltbar. Zum anderen ist auch die bereits zu § 5 Abs. 4 TDG a.F. vertretene Ansicht abzulehnen, das Strafrecht sei im Rahmen des § 7 Abs. 2 S. 2 TMG ausgeschlossen. Hier wird verkannt, dass grundsätzlich im Prüfungsaufbau des unechten Unterlassungsdeliktes die Garantenstellung ein im objektiven Tatbestand zu prüfendes Merkmal darstellt und somit auch nicht in Konflikt mit der Formulierung „Verpflichtung“ kommt.

Zudem ist nach europarechtskonformer Auslegung des § 7 Abs. 2 S. 2 TMG nicht ersichtlich, weshalb hier auf Grundlage der ECRL eine Anwendung des Strafrechts im Rahmen des § 7 Abs. 2 S. 2 TMG ausgeschlossen sein sollte. Vielmehr sprechen die besseren Argumente anhand der Erwägungsgründe 42 und 45 für die Anwendung auch des Strafrechts. Damit bleibt festzuhalten, dass nach Entkräftung der Argumente gegen die Anwendung des Strafrechts gerade eine Strafbarkeit des Access-Providers auch im Rahmen des § 7 Abs. 2 S. 2 TMG geprüft werden kann.

[328] Anmerkung von *Hoeren*, im Anschluss an MMR 1998, 93, 97f: Hier führt *Hoeren* teilweise die oben erörterten Argumente auf und wirft dem Generalbundesanwalt letztendlich sogar Rechtsbeugung vor.

Kapitel 2: Haftung nach den Strafgesetzen

Wie bereits soeben festgestellt, haftet der Access-Provider auch außerhalb der Privilegierung des § 8 TMG nach den allgemeinen gesetzlichen – im vorliegenden Falle strafrechtlichen – Vorschriften, wenn ein Fall des § 7 Abs. 2 S. 2 TMG bejaht werden kann. Daher sind im Weiteren die Voraussetzungen einer Haftung nach den Strafgesetzen zu untersuchen. Nachdem überblicksmäßig die für einen Access-Provider typischerweise (mit)zuverwirklichenden Strafgesetze angesprochen werden sollen, muss im Anschluss die Art der strafbaren Handlung und ggf. eine Garantenstellung ermittelt werden, um das Vorliegen einer nicht privilegierten Unterlassungsstraftat entsprechend § 7 Abs. 2 S. 2 TMG annehmen zu können.

I. Straftatbestände

Es soll nun vorab ein kurzer Überblick über die in Frage kommenden Delikte gegeben werden, die typischerweise durch einen Access-Provider verwirklicht bzw. unterstützt werden können. Dazu zählen nicht nur solche des Strafgesetzbuches, sondern insbesondere auch solche des Urheber(straf)rechts sowie die im Jugendmedienschutz-Staatsvertrag festgelegten. Der Überblick teilt die Delikte gängigen Verwirklichungsgruppen zu.

1. Straftaten der extremistischen Szene

Eine der Tätergruppen, die sich zur Erreichung ihrer Ziele gerne des Internets bedient, ist die der Täter aus einem extremistischen Umfeld. Hierzu zählen nicht nur die rechtsextremen und neonazistischen Gruppierungen, sondern ebenso die linksradikal und sonstig politisch motivierten Vereinigungen, genauso wie alle Arten von religiös motiviertem Extremismus.

Hier findet über das Medium Internet eine weltweite Verbreitung von ideologischem Anschauungs- und politischem Hetzmaterial statt. Hinzu kommt der Meinungsaustausch über Internetforen und Chatrooms. Die meist auf ausländischen Servern eingerichteten „Vertriebs“-Plattformen bieten die Grundlage, um von dort aus größtenteils unbehindert – da entweder in einem „sicheren“ Drittstaat untergebracht oder anonymisiert – Informationen zu Weltanschauungen bis hin zur Anleitung zum Bombenbau und deren „richtigem“ Einsatz zu veröffentlichen.

In diesen Fällen kommen die Straftatbestände der Bildung einer kriminellen oder terroristischen Vereinigung, §§ 129, 129a StGB, die Volksverhetzung, § 130 StGB, oder die Anleitung zu Straftaten, § 130a StGB, in Betracht. Anfang 2015 wurden zudem mit dem 49. Strafrechtsänderungsgesetz die §§ 130 Abs. 5, 130a Abs. 3 und 131 Abs. 1 Nr. 2 StGB dahingehend geändert und ergänzt, dass auch die Verbreitung mittels Telemedien ausdrücklich unter Strafe gestellt wurde.[329]

Nachdem § 129 StGB überwiegend zur Verfolgung von politisch motivierten Vereinigungen herangezogen wird,[330] ist § 129a StGB mit seinen Qualifikationstatbeständen durch das Terrorismusbekämpfungsgesetz als Ausfluss der Terroranschläge des 11. September 2001 eingeführt worden. Beide Tatbestände dienen dem Schutz der öffentlichen Sicherheit und Ordnung. Ebenfalls dem Schutz der öffentlichen Ordnung und des öffentlichen Friedens – aber auch dem von Individualrechtsgütern – dient der Tatbestand der Volksverhetzung, § 130 StGB. Tatsächlich werden vor diesem Hintergrund überwiegend rechtsradikale Taten verfolgt. Zur Gruppe der Straftatbestände, die den öffentlichen Frieden als zu schützendes Rechtsgut innehaben, zählt auch derjenige, der die Anleitung zu Straftaten unter Strafe stellt, § 130a StGB. Dieser umstrittene Tatbestand, der als abstraktes Gefährdungsdelikt nach h.M. überflüssig erscheint[331], ist jedoch gerade im Bezug zum Internet und seinen sich daraus ergebenden Verbreitungsmöglichkeiten beachtenswert.

Straftaten extremistischer Gruppen richten sich jedoch nicht nur gegen die öffentliche Ordnung an sich, wie von den vorgenannten Straftatbestände inkriminiert, sondern können darüber hinausgehend auch gegen den demokratischen Rechtsstaat in seiner Natur gerichtet sein. Hier sind im Rahmen der Access-Providerhaftung insbesondere die Tatbestände der §§ 86 und 86a StGB zu nennen, das Verbreiten von Propagandamitteln verfassungswidriger Organisationen und das Verwenden von Kennzeichen derselben. Verhindert werden soll mit diesen Tatbeständen die inhaltliche Werbung für solche Organisationen und das Entstehen des Eindruckes, diese würden nicht an ihrer Betätigung gehindert. Die im Zuge des § 86a StGB entstehende Tabuisierung ist umstritten, da immer dann ein Problem auftritt, wenn diese Kennzeichen von Gegnern dieser Organisationen aus Protest verwendet werden. § 86a StGB muss daher nach dem Schutzzweck seiner Norm einschränkend im Lichte der Meinungsfreiheit ausgelegt werden.[332]

---

329 BT-Drs. 18/2601 S. 6 f.

330 *Fischer*, § 129 Rn. 4.

331 *Fischer*, § 130a Rn. 2 ff.

332 BGHSt 25, 30, 33; 25, 13, 136; 52, 364, 375; *Fischer*, § 86a, Rn. 18.

2. Verbreitung pornographischer Schriften

Die zweite Gruppe von Straftatbeständen, die im Rahmen der Access-Providerhaftung in Erwägung zu ziehen ist, sind diejenigen aus dem Bereich der Verbreitung von Pornographie. Es handelt sich dabei grundsätzlich um Straftaten gegen die sexuelle Selbstbestimmung.

Pornographische Inhalte nehmen bereits einen großen Teil aller im Internet angebotenen Inhalte ein. Die hierzu vorliegenden Zahlen sind unterschiedlich, es kann jedoch davon ausgegangen werden, dass es bereits über 4 Mio. pornographische Inhalte im Internet gibt und diese einen Gesamtanteil von über 10 Prozent darstellen.[333] Auch die Angebote von kinder- und jugendpornographischen Schriften steigen. Allein in Deutschland wurden im Jahr 2011 ca. 3.000 Angebote über jugendschutz.net verzeichnet. Größtenteils erfolgt in diesem Feld eine Weitergabe der illegalen Inhalte über Downloadbereiche.[334] Die Verbreitung von Pornographie war bis Anfang 2015 an den Schriftenbegriff gebunden (Verbreitung Pornographischer Schriften). Aufgrund der Tatsache, dass Pornographie heutzutage überwiegend online verbreitet wird und dies die Fixierung der Strafbarkeitsnormen auf das Verbreiten von Schriften nicht mehr rechtfertigte, hat der Gesetzgeber mit dem 49. StrÄndG beschlossen, die Strafbarkeit vom Schriftenbegriff zu entkoppeln und damit einige, nicht unerhebliche dogmatische Schwierigkeiten zu entflechten.

a) Verbreitung pornographischer Schriften über Tele- und Mediendienste, § 184 StGB a.F.

Der Tatbestand der Verbreitung gem. § 184 Abs. 1 Nr. 1 StGB a.F. erfasste zwei grundlegend von einander zu unterscheidende Handlungsvarianten. Zum eine das Anbieten und Überlassen von pornographischen Schriften gem. § 11 Abs. 3 StGB und zum anderen das Zugänglichmachen des Inhalts der Schriften.[335] Das Anbieten und Überlassen, das Verbreiten im engeren Sinne setzt die körperliche Weitergabe voraus.[336] Verkörpert sind Daten jedoch erst dann, wenn sie auf Datenträgern gespei-

---

[333] Zahlen bspw. online unter http://www.nacktetatsachen.at/statistiken-pornographie.html (07.01.2014).

[334] Jugendschutz.net, Ergebnisse der Recherchen und Kontrollen, Bericht 2011, online unter http://jugendschutz.net/pdf/bericht2011.pdf (07.01.2014).

[335] *Hilgendorf/Valerius*, Rn. 291; *Laubenthal*, Rn. 936 ff.

[336] LK-StGK/*Laufhütte*/*Roggenbuck* § 184 Rn. 15 f.; *Hilgendorf/Valerius*, Rn. 301; *Laubenthal*, Rn. 1078.

chert sind. Eine Verbreitung pornographischer Schriften war daher über Telemedien nicht möglich, da es an der Weitergabe eines Trägermediums scheiterte.[337]

Anders verhält es sich mit dem Tatbestandsmerkmal des Zugänglichmachens. Notwendig hierfür ist lediglich die Möglichkeit der Kenntnisnahme des expliziten Inhalts durch das Opfer.[338] Dies ist auch im Bereich der Verbreitung durch Tele- und Mediendienste durchaus möglich.[339]

b) Spezifischer Verbreitungsbegriff im Internet

Der BGH entwickelte einen eigenen, internetspezifischen Verbreitungsbegriff, um der Verbreitung von pornographischen Inhalten über Telemedien im Rahmen des § 184 StGB a. F. gerecht zu werden.[340] Für den BGH kam es danach nicht mehr auf die körperliche Weitergabe der Schrift an, sondern es sollte die Manifestation auf dem Computer des Nutzers ausreichen. Der sich an der Verkörperung orientierende Verbreitungsbegriff sollte damit im Internet nicht gelten.[341] Der BGH begründet seine Entscheidung damit, dass ansonsten der gesetzgeberisch gewollte effektive Jugendschutz im Bereich der Tele- und Mediendienste an dieser Stelle lückenhaft wäre und daher eine internetspezifische Auslegung des Verbreitensbegriffes geboten sei.[342]

Diese Entscheidung des BGH wurde vielfach von der Literatur kritisiert. Insbesondere wurde argumentiert, dass der BGH in seiner Entscheidung die Übertragung von verkörperten Inhalten nicht dogmatisch richtig von einer körperlichen Weitergabe trenne[343] und dass ein fehlender effektiver Jugendschutz ebenso über das Tatbestandsmerkmal des Zugänglichmachens erreicht werden könnte.[344]

c) Verbreitung pornographischer Darbietungen, § 184d StGB a.F.

Vom Straftatbestand des § 184d StGB a.F. erfasst wurden Darbietungen in Tele- und Mediendiensten sowie im Rundfunk. Der Begriff der Darbietung sollte sich von demjenigen der Schriften i.S.d § 11 Abs. 3 StGB unterscheiden. Erfasst werden soll-

---

337 *Hilgendorf/Valerius*, Rn. 301.
338 SSW/*Hilgendorf* § 184 Rn. 15; *Malek/Popp* Rn. 311.
339 *Hilgendorf/Valerius*, Rn. 291 f.
340 BGH NJW 2001, 3558, 3559.
341 BGH NJW 2001, 3558, 3559.
342 BGH a.a.O.
343 *Hilgendorf/Valerius*, Rn. 303; *Fischer,* § 184 Rn. 35; Schönke/Schröder/*Perron/Eisele*, § 184b Rn. 5; *Gercke/Brunst* Rn. 312.
344 *Bornemann*, MMR 2012, 157, 159; *Kudlich*, JZ 2002, 310, 311; *Hilgendorf/Valerius*, Rn. 305.

ten Live-Übertragungen, z.B. über Webcams.[345] Diese waren aufgrund mangelnder Dauerhaftigkeit – es handelte sich um keine Wiedergabe von vorher fixierten Aufzeichnungen – nicht unter den Schriftenbegriff zu subsumieren. Das Verbreiten i.S.d. § 184d StGB a.F. war folglich an dieser Stelle anders zu definieren. Darunter zu subsumieren war das Zugänglichmachen von Inhalten, das sich an die Allgemeinheit richtete.[346]

d) Zugänglichmachen pornographischer Inhalte mittels Rundfunk oder Telemedien, § 184d Abs. 1 StGB

Mit dem In-Kraft-Treten des 49. StrÄndG am 27.01.2015 wurden auch die Vorschriften über die Verbreitung von Pornographie mittels Telemedien reformiert. § 184d StGB wird hierbei zu einer Norm erhoben, die die Verbreitung sämtlicher pornographischer Inhalte über Telemedien unter Strafe stellt, im Gegensatz zur Verbreitung verkörperter Schriften in den §§ 184a-c StGB.[347] Unverändert bleibt an dieser Stelle die Möglichkeit einfache Pornographie innerhalb geschlossener Benutzergruppen unter Einsatz entsprechender Altersverifikationssysteme zugänglich zu machen, § 184d Abs. 1 S. 2 StGB. Der Begriff der Telemedien ersetzt nun die Begrifflichkeit der Tele- und Mediendienste und wurde folglich zeitgemäß an die Formulierung im TMG angepasst.[348]

e) Pornographische Inhalte

Tatobjekt sind nun im § 184d StGB nicht mehr die Schriften sondern es wird statt derer auf den Ausdruck „Inhalte“ zurückgegriffen.[349] Der Gesetzgeber wollte an dieser Stelle weg von dem bisher verwendeten Tatbestandsmerkmal der Schrift. Der Schriftenbegriff schließt lediglich verkörperte Inhalte ein.[350] Der Gesetzgeber will nun für das Pornographiestrafrecht hin zu einer Mitumfassung von nicht verkörperten Inhalten, um die Frage der Strafbarkeit auf diesem Gebiet den heutigen techni-

345 *Hilgendorf/Valerius*, Rn. 313.

346 *Bornemann,* MMR 2012, 157 160 f.; Schönke/Schröder/*Perron/Eisele* § 184d Rn. 5; BeckOK-StGB/*Ziegler* § 184d Rn. 4.

347 *Gercke*, ZUM 2014, 641; *Hörnle*, Stellungnahme zum Gesetzentwurf, S. 9.

348 S. oben S. 8; *Hörnle*, Stellungnahme zum Gesetzentwurf, S. 9; BT-Drs. 18/2601 S. 16.

349 BT-Drs. 18/2601 S. 24; *Gercke*, ZUM, 641,645.

350 Siehe oben S. 7.

schen Gegebenheiten anzupassen und um bisherigen Schwierigkeiten in der Rechtsprechung zu begegnen.[351]

Der verwendete Begriff der Inhalte soll deckungsgleich mit dem der „Informationen“ gem. § 2 S. 1 Nr. 3 TMG sein und nur deshalb im StGB verwendet werden, um sprachliche Unpässlichkeiten zu vermeiden.[352] Der im TMG verwendete Begriff der Informationen ist der Formulierung der Art. 12–15 der ECRL entnommen. Im § 5 TDG a.F. wurde demgegenüber noch der Begriff der Inhalte verwendet, zu welchem vertreten wurde, dass dieser sich nur auf rechtswidrige Inhalte beziehen sollte und rechtmäßige Inhalte nicht mitumfassen würde, was zu einer teilweise einschränkenden Auslegung des Begriffes der Inhalte führte.[353] Mit der Umsetzung der ECRL wurde der Begriff der „Inhalte“ durch den der „Informationen“ ersetzt, der nach dem Willen des Gesetzgebers weit auszulegen ist und damit sämtliche „Angaben, die im Rahmen des jeweiligen Teledienstes übermittelt und gespeichert werden“ umfasst[354]. Daher fallen alle von Telemediendiensten, d.h. von Diensteanbietern, übermittelten oder gespeicherten Daten unter den Anwendungsbereich des Informationsbegriffes. Unerheblich ist dabei, ob diese vom Webbrowser lesbar gemacht werden können oder hierzu zusätzliche Software eingesetzt werden muss.[355]

f) Einer anderen Person oder der Öffentlichkeit zugänglich machen

Das Zugänglich-Machen i.S.d. § 184d StGB soll nach dem Willen des Gesetzgebers keiner Änderung unterliegen und wie bisher verwendet werden. Danach soll darunter die Möglichkeit der Wahrnehmung verstanden werden.[356] Ebenso verhält es sich beim Zugänglich-Machen von Inhalten der Öffentlichkeit. Auch hier zieht der Gesetzgeber die ursprüngliche Auslegung des Begriffes heran und stellt darauf ab, dass die Möglichkeit der Wahrnehmung für eine unbestimmte Vielzahl von Personen bestehen muss.[357]

---

[351] BT-Drs. 18/2601 S. 2; *Hörnle*, Stellungnahme zum Gesetzentwurf, S. 9.
[352] BT-Drs. 18/2601 S. 24.
[353] Spindler/Schuster/*Hoffmann*, vor § 7 TMG, Rn. 12.
[354] BT-Drs. 14/6098, S. 23.
[355] Spindler/Schuster/*Hoffmann*, § 7 TMG, Rn. 10.
[356] *Fischer*, § 74d Rn. 6; siehe zu Zugänglich-Machen auch oben S. 9.
[357] *Fischer*, § 74d Rn. 6; BT-Drs. 18/2601, S. 24.

g) Abruf kinder- und jugendpornographischer Inhalte mittels Telemedien, § 184d Abs. 2 StGB

Eine zusätzliche Novellierung, die der § 184d StGB erfahren hat, ist, dass mit dessen Abs. 2 auch der Abruf von kinder- und jugendpornographischen Inhalten unter Strafe gestellt wird. Dies soll den Streitpunkt erledigen, wann eine Besitzverschaffung solchen Inhalts anzunehmen ist.[358] Notwendig ist eine Besitzverschaffung, die zu einer Verkörperung führt nun nicht mehr, ausreichend ist die bloße Betrachtung entsprechender Informationen.[359]

Die Definition des Abrufs soll auch an dieser Stelle der des TMG entsprechen.[360] Nachdem die Gesetzesbegründung zum TMG auf die des TDG verweist, ist dieses heranzuziehen. Danach ist für den „Abruf" typischerweise notwendig, dass die Informationen so zur Verfügung stehen, dass sie „auf Anforderung" übermittelt werden können.[361] Ein Abrufen kinder- oder jugendpornographischen Inhalts liegt folglich dann vor, wenn der Täter die Übertragung der Inhalte veranlasst und sich somit die Möglichkeit der Kenntnisnahme verschafft.[362] Die Verwendung des Begriffes des „Abrufs" ist jedoch nicht unumstritten. Kritisiert wird, dass diese Formulierung zu weit vom in der „Lanzarote-Konvention" verwendeten Begriff des „Zugriffs" – in der Ausgangsversion „access" – abweiche.[363] Zugriff und Abruf seien nicht vergleichbar, insbesondere sei der Nachweis eines Abrufs schwieriger zu führen, als der des Zugriffs.[364] Die Gesetzesbegründung hingegen setzt sich mit der „Zugangsverschaffung" auseinander und führt an, dass diese Begrifflichkeit zu nicht unerheblichen Abgrenzungsschwierigkeiten führen würde, da darunter die Möglichkeit der Wahrnehmung zu verstehen sei, diese Möglichkeit aber bereits mit dem Vorhandensein des notwendigen technischen Equipments bestehe und damit der Straftatbestand nicht konkret genug gefasst wäre.[365] Die Zugangsverschaffung und damit auch der Zugriff implizierten die Kenntnisnahme der Inhalte, was der Abruf nicht zwingend voraussetze.[366]

---

358 BT-Drs. 18/2601 S. 33f; zum bisherigen Streitstand um die Besitzverschaffung vgl. LK-StGB/ *Laufhütte/Roggenbuck*, § 184b Rn. 8; *Hilgendorf/Valerius*, Rn. 306ff, m. w. N.

359 *Hörnle*, Stellungnahme zum Gesetzentwurf, S. 9; *Titz*, Stellungnahme DRB, S. 8 f.

360 BT-Drs. 18/2601, S. 34.

361 BT-Drs. 14/6098, S. 16.

362 BT-Drs. 18/2601, S. 34.

363 Übereinkommen des Europarates zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch, ETS 201, Art. 20 Abs. 1 Buchstabe f; *Gercke*, ZUM 2014, 645.

364 *Gercke*, ZUM 2014, 645.

365 BT-Drs. 18/2601, S. 34.

366 BT-Drs. 18/2601, S. 34.

h) „Posing“

Eine weitere, immer mehr zunehmende Art der Pornographie ist die der virtuellen Pornographie und das sog. „Posing“. Nachdem das Internet immer mehr Möglichkeiten in virtuellen Räumen eröffnet, droht auch von dort aus die Gefahr der Verwirklichung pornographie-strafrechtlicher Tatbestände. Es handelt sich bei der virtuellen Pornographie um einen Unterfall der fiktiven Pornographie, der ebenfalls – zumindest als reale bzw. wirklichkeitsnahe Pornographie – von den Straftatbeständen umfasst ist.[367] Einbezogen wird die fiktive Pornographie durch eine grammatikalische und systematische Auslegung der §§ 184b, 184c StGB.[368] Auch in diesen virtuellen Räumen lässt sich z.B. Sex mit kindlichen Avataren beobachten.[369]

Das sog. „Posing“ zeigt Kinder und Jugendliche in unnatürlichen, geschlechtsbetonten Haltungen und umfasst die aufreizende Zurschaustellung der Genitalien und der Schamgegend. Das „Posing“, welches bereits durch § 4 Abs. 1 S. 1 Nr. 9 JMStV verboten ist, wird ebenfalls von den §§ 184b, 184c StGB mitumfasst.[370] Nachdem die Grenzen in diesen Fällen fließend sind, ist gerade hier ein nachdrückliches Einschreiten erforderlich, um den pädophilen Straftätern zu begegnen.

3. Ehrverletzung – „Flaming“

Eine weitere Gruppe der vom Internet geförderten und daher auch im Rahmen der Access-Providerhaftung in Betracht kommenden Straftatbestände sind die der §§ 185 ff. StGB.

Straftaten gegen die persönliche Ehre spielen im Zeitalter des Web 2.0 eine immer größere Rolle. Das „Mitmach-Internet“, d.h. die sozialen Netzwerke, allen voran Facebook, eröffnet dem Einzelnen nicht nur die Möglichkeit, sich dort zu präsentieren, sondern er (oder sie) sitzt auch auf dem sprichwörtlichen Präsentierteller und wird so zur Zielscheibe von Anfeindungen. Diese können vom spitzen Kommentar zu einem Benutzereintrag oder Foto, dem Flaming, über eine Beleidigung durch einen Einzelnen bis hin zum Shit-Storm führen, in dem ganze Hundertschaften von Nutzern großenteils in beleidigender Form über den User mittels seines Profils herfallen. Dabei werden Opfer wie Täter immer jünger, teilweise werden die Profile einzelner Mitschüler von ganzen Klassen mit Beleidigungen, Verleumdungen oder

---

367 *Sieber*/*Nolde*, S. 10 f.

368 *Fischer*, § 184b, Rn. 5 ff.

369 Hierzu ausführlich *Hopf/Braml* ZUM 2007, 354, 358, Zur Strafbarkeit von Darstellungen mit kindlichen Avataren in Online-Welten wie „Second Life“.

370 *Hilgendorf/Valerius*, Rn. 278.

Hassparolen überschwemmt, wobei weder Täter noch Opfer strafmündig sind. Diese ehrverletzenden Taten nehmen deshalb so stark zu, weil die Hemmschwelle der Täter aufgrund der räumlichen und technischen Trennung stark herabgesetzt ist und die Selbstwahrnehmung in sozialen Netzwerken verzerrt ist.[371]

Eine weitere Verstärkung erfahren die Beleidigungsdelikte auch hinsichtlich ihrer Intensität. Die über soziale Netzwerke geäußerten Beleidigungen sind jedermann zugänglich, sodass davon eine viel größere Zahl von Personen Kenntnis nimmt und dies zu einer seelisch weitaus größeren Belastung des Opfers führt. Hinzu kommt, dass auch über das mobile Internet via Smartphones und Tablets die ständige Möglichkeit besteht, zu agieren und zu reagieren – auch aus einem angespannten Gemütszustand heraus, z.B. in einer Diskothek.

Ist eine Beleidigung einmal im Internet veröffentlicht, so ist diese tatsächlich kaum mehr zu entfernen. Das soziale Netzwerk Facebook zum Beispiel speichert jeden Vorgang und behält auch vom Benutzer „gelöschte" Vorgänge auf seinen Servern. Der Straftatbestand des § 185 StGB ist erfüllt, wenn die herabwürdigende Äußerung gegenüber dem Opfer selbst getätigt wird. Die §§ 186, 187 StGB hingegen setzen eine Äußerung gegenüber Dritten voraus. Innerhalb sozialer Netzwerke wird zumeist ein direktes Ansprechen des Opfers aufgrund der niedrigen Hemmschwelle anzutreffen sein. Werden jedoch verleumderische Aussagen gegenüber Dritten getätigt, so stehen die Delikte in Tateinheit, wenn auch das Opfer Zugriff auf den „Post" bzw. die Äußerung hat.[372]

4. Unerlaubte Verwertung urheberrechtlich geschützter Werke

Eine weitere Gruppe von Straftatbeständen, die im Zusammenhang mit der Access-Providerhaftung genannt werden muss, sind die des Urheberstrafrechts. Der Schaden, welcher der Musik- und Softwareindustrie jährlich durch illegale Downloads und Verbreitung entsteht, ist beträchtlich.[373] Wegen der in allen gesellschaftlichen Ebenen Einzug haltenden Digitalisierung ist sogar das Weiterbestehen althergebrachter Tonträger wie der Audio-CD fraglich. Nachgefragt wird heute nicht mehr Musik im kb-lastigen *.wav-Format wie auf einer Audio-CD sondern in komprimierten *.mp- bzw. *.aac-Formaten.[374] Nachdem Mobiltelefone durch Smartphones ver-

[371] Ausführlich hierzu *Hilgendorf*, ZIS 2010, 208, 209 f.

[372] *Hilgendorf/Valerius*, Rn. 346, m.w.N.

[373] Der geschätzte Schaden der Musikindustrie betrug laut dem Spiegel allein 2010 geschätzt 680 Mio. Euro, http://www.spiegel.de/spiegel/print/d-86402970.html (07.08.2013).

[374] Die von Apple verwendete Software iTunes wandelt Audiodateien nicht in mp- sondern in aac-Dateien.

drängt werden und diese über das bloße Telefonieren hinaus auch für Unterhaltung sorgen sollen, ggf. auch als portabler Festplattenersatz, werden digitalisierte, komprimierte Musikdaten benötigt, um möglichst viele Musiktitel verfügbar zu haben, sei es zum Anhören oder als Klingelton. Im Jahre 2012 haben die polizeilich registrierten Zahlen zu Straftaten aus dem Urheberrecht sowie die herkömmliche wie auch die gewerbliche Softwarepiraterie im Vergleich zum Vorjahr zugenommen.[375]

Die entsprechenden Straftatbestände, die bei Straftaten gegen das Urheberrecht verletzt werden, sind im Urheberrechtsgesetz geregelt. In Betracht kommen die Normen der §§ 106, 107, 108 und 108b UrhG. Nachdem noch immer die Mehrzahl der Urheberrechtsverletzungen, die mit Hilfe des Internet begangen werden, aus dem Bereich des Filesharing stammen, soll vorliegend nur diese auch für den Access-Provider in Betracht kommende Straftat näher beleuchtet werden. Das Filesharing wird unter die wichtigste Norm innerhalb dieser Tatbestände, den § 106 UrhG subsumiert. Dieser stellt die unerlaubte Verwertung urheberrechtlich geschützter Werke unter Strafe. Tathandlung ist die Vervielfältigung, die Verbreitung oder die öffentliche Wiedergabe eines urheberrechtlich geschützten Werkes ohne Einwilligung des Rechteinhabers. Von einer Vervielfältigung gem. § 106 Abs. 1 Alt. 1 UrhG ist auszugehen, wenn ein Vervielfältigungsstück – dauerhaft oder auch nur vorübergehend – hergestellt wird. Dieses bedarf einer körperlichen Fixierung und muss für die menschlichen Sinne unmittelbar oder mittelbar wahrnehmbar gemacht werden können.[376] Vorliegend kommt dieser Straftatbestand dann in Betracht, wenn eine Datei auf einen Server hochgeladen oder von diesem auf ein anderes Medium, z.B. einen User-PC, wieder heruntergeladen wird.[377] Hierbei muss wieder zwingend ein Access-Provider mitwirken, um dem User den entsprechenden Zugang zum Internet zu verschaffen. Es handelt sich dabei jedoch noch nicht um die übliche und überwiegende Filesharing-Praxis, bei der ein Datenaustausch peer-to-peer, d.h. direkt von User-PC zu User-PC, stattfindet.

Das Verbreiten urheberrechtlich geschützter Werke gem. § 106 Abs. 1 Alt. 2 UrhG setzt voraus, dass ein Vervielfältigungsstück in Verkehr gebracht wird und dass das Eigentum an diesem übergeht.[378] Angewendet auf die Filesharing Praxis ist jedoch festzustellen, dass § 106 Abs. 1 Alt. 2 UrhG nicht einschlägig ist. Betrachtet man nämlich diese Konstellation bezogen auf die in § 15 UrhG festgeschriebenen Verwertungsmöglichkeiten, die auch den Tatbestand der Verbreitung aufzählen, so ist Voraussetzung die Verwertung und damit die Verbreitung in körperlicher Form. Dies

---

375 PKS 2012, S. 65.

376 BGH NJW 1991, 1231 (1234); *Gercke*/*Brunst*, Rn. 431.

377 *Hilgendorf/Valerius*, Rn. 702.

378 *Hilgendorf/Valerius*, Rn. 704.

würde die Fixierung auf einem Datenträger voraussetzen. Nachdem beim Filesharing jedoch nicht die Datenträger ausgetauscht werden, sondern das Werk lediglich in unkörperlicher Form vorliegt, ist beim Filesharing im Rahmen des peer-to-peer § 106 Abs. 1 Alt. 2 UrhG nicht verwirklicht. Für den Access-Provider bedeutet dies, dass auch eine Strafbarkeit nach § 106 Abs. 1 Alt. 2 UrhG nicht in Betracht kommt, da der Access-Provider nicht am Austausch von Datenträgern beteiligt ist, sondern nur Daten an sich durchleitet.[379]

Weitere Tatvariante der unerlaubten Verwertung urheberrechtlich geschützter Werke stellt die öffentliche Wiedergabe gem. § 106 Abs. 1 Alt. 3 UrhG dar. In dieser Alternative wird Unkörperliches wahrnehmbar und zugänglich gemacht, so § 15 Abs. 2 UrhG. Eine öffentliche Wiedergabe ist zu bejahen, wenn eine Wiedergabe für eine Mehrzahl von Mitgliedern der Öffentlichkeit bestimmt ist. Der Öffentlichkeit gehören Personen dann nicht an, wenn sie in einer persönlichen Beziehung zu dem Rechteinhaber stehen.[380] Um das Filesharing in peer-to-peer-Netzwerken ebenfalls unter die öffentliche Wiedergabe zu fassen, wurde vom Gesetzgeber der Tatbestand des Öffentlich-zugänglich-Machens gem. §§ 15 Abs. 2 S. 2 Nr. 2 i.V.m. 19a UrhG eingeführt. Dadurch wurde die Frage, ob beim Filesharing eine Wiedergabe an eine Mehrzahl von Mitgliedern der Öffentlichkeit vorliegt, obsolet. Die Verwertung eines Werkes durch den Rechteinhaber in Online-Medien wurde durch die Einführung des § 19a UrhG ausdrücklich geschützt. Das Filesharing und damit die unerlaubte Verwertung in digitalen Medien stellt daher einen Straftatbestand gem. § 106 Abs. 1 Alt. 3 UrhG dar. Daran ist der Access-Provider auch wieder nicht ganz unbeteiligt, da er die Voraussetzungen für den Datentransfer peer-to-peer schafft und die unerlaubte Verwertung durch seine Infrastruktur ermöglicht. Es besteht daher auch im Rahmen der Filesharing-Delikte ein Interesse, den Access-Providers mit in die Haftung zu nehmen.

5. § 23 Jugendmedienschutz-Staatsvertrag

Bei § 23 JMStV handelt es sich um eine Norm des Sonderstrafrechts, die der Gesetzgeber zum Schutz von Kindern und Jugendlichen im JMStV geschaffen hat.[381] Unter Strafe gestellt wird das Verbreiten oder Zugänglich-Machen von Angeboten, die offensichtlich dazu geeignet sind, die Entwicklung von Kindern und Jugendlichen oder ihre Erziehung zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit unter Berücksichtigung der besonderen Wirkungsform des Verbrei-

379 *Hilgendorf/Valerius*, Rn. 705; m.w.N.
380 *Hilgendorf/Valerius*, Rn. 706.
381 *Hilgendorf*, K&R 2011, 229, 231.

tungsmediums schwer zu gefährden. Als Strafmaß nennt das Gesetz Freiheitsstrafe bis zu einem Jahr, im Falle der fahrlässigen Tatbegehung bis zu 6 Monaten, sowie Geldstrafe. Diese strafrechtliche Norm weist aufgrund der für das Strafrecht untypischen Formulierung etliche Unklarheiten auf, die an dieser Stelle jedoch nicht vertieft werden sollen.[382]

Auch Access-Provider fallen unter den Anwendungsbereich dieser Norm. Tatbestandlich statuiert die Norm, dass bestimmte inkriminierte Angebote verbreitet oder zugänglich gemacht werden. Hierunter lässt sich ohne weiteres die Tätigkeit eines Access-Providers subsumieren, dessen Tätigkeit gerade darin liegt, dem Nutzer Angebote aus dem Internet zugänglich zu machen.

II. Tun oder Unterlassen

Nachdem in einem kurzen Überblick die häufigsten von Providern realisierbaren Straftatbestände, vorgestellt wurden, stellt sich nun die Frage, worin die strafbare Handlung des Access-Providern liegt. Es besteht für den Access-Provider ebenso wie bei natürlichen Personen die Möglichkeit, einen Straftatbestand durch aktives Tun zu verwirklichen oder durch ein Unterlassen, d.h. die Nicht-Vornahme einer gebotenen Handlung. Dann käme eine Strafbarkeit über § 13 StGB in Betracht im Sinne eines unechten Unterlassungsdeliktes.

1. Abgrenzung von Tun und Unterlassen

Bevor abschließend geklärt werden kann, ob sich ein Access-Provider überwiegend durch aktives Tun oder im Rahmen eines pflichtwidrigen Unterlassens strafbar macht, muss zunächst geklärt werden, anhand welcher objektiver Kriterien die Handlungen des Access-Providers gemessen werden müssen. Dazu wurden in Rechtsprechung und Literatur unterschiedliche Abgrenzungskriterien entwickelt, die kurz erläutert werden sollen.

a) Energieeinsatz

Ein Teil der Literatur nimmt die Abgrenzung von Tun und Unterlassen innerhalb des tatbestandlichen Handelns im Rahmen einer naturwissenschaftlichen Betrachtung

[382] Vgl. ausführlich dazu *Hilgendorf*, K&R 2011, 229, 231 f.

anhand des Kriteriums des Einsatzes von Energie vor.[383] Wird vom Täter Energie aufgewandt bzw. eingesetzt, so liegt nach dieser Ansicht ein aktives Tun vor, bleibt der Täter untätig und wendet keine Energie auf, so handelt er durch Unterlassen.

b) Kausalität

Eine weitere Meinung grenzt aktives Tun von Unterlassen anhand der Kausalität ab. Sie stellt darauf ab, ob eine Handlung conditio-sine-qua-non für eine äußerliche Veränderung des Geschehensablaufes war.[384] Verändert eine kausale Handlung einen Geschehensablauf, sei von einem aktiven Tun auszugehen, wird nicht in den Handlungsverlauf eingegriffen, von einem Unterlassen.

c) Kombination aus Energieeinsatz und Kausalität

Eine andere Ansicht kombiniert die beiden vorgenannten Abgrenzungsmöglichkeiten des Energieeinsatzes und der Kausalität.[385] Es bedarf nach dieser Ansicht eines finalen, d.h. zweckgerichteten Energieeinsatzes, der kumulativ einen Kausalverlauf entweder anstoßen oder in eine bestimmte Richtung lenken muss. Sind diese Voraussetzungen erfüllt, so handelt es sich um eine aktives Tun. Fehlt es an diesen kumulativen Bedingungen, so liegt nach dieser Ansicht ein Unterlassen vor.

d) Internetspezifische Lösung

Altenhain hält die vorgenannten Ansichten auf dem Gebiet des Internets für unzulänglich und schlägt eine alternative Lösung für diese Art von Fällen vor. Das Medium Internet verlange eine Modifizierung, denn hierin könnten die oben beschriebenen Abgrenzungskriterien nicht übernommen werden.[386] Dabei solle das Kriterium des Energieeinsatzes dahingehend modifiziert werden, dass mit Blick auf das Medium Internet als Anknüpfungspunkt für den Einsatz von Energie nicht der Einsatz menschlicher Energie sondern vielmehr von beherrschbarer maschineller Energie von dienen soll. Beherrschen solle dann bedeuten, dass der Mensch die Möglichkeit besitzt, in den maschinellen Arbeitsprozess einzugreifen.[387]

---

383 SK-StGB/*Rudolphi/Stein*, vor § 13, Rn. 6.

384 *Kühl*, S. 644, Fn. 22, 23.

385 *Wessels/Beulke*, Rn. 699

386 *Altenhain*, CR 1997, 485, 487 f.

387 *Altenhain* gelangt damit stets zu einem aktiven Tun des Providers.

e) Schwerpunkt der Vorwerfbarkeit

Die herrschende Meinung sowie die ständige Rechtsprechung des Bundesgerichtshofes stellen bei der Abgrenzung von aktivem Tun und Unterlassen auf den Schwerpunkt der Vorwerfbarkeit der Handlung ab.[388] Der Tatrichter prüft dabei im Einzelfall, auch anhand der unten genannten Kriterien *aa)–cc)*, wo bei normativer Betrachtung und bei Berücksichtigung des sozialen Handlungssinns in dem konkreten Täterverhalten der Schwerpunkt des strafrechtlich relevanten Handelns liegt.

f) Stellungnahme

In den Fällen, in denen nicht schon dem äußeren Erscheinungsbild nach entschieden werden kann, ob ein Tun oder Unterlassen vorliegt bzw. in denen eine mehrdeutige Verhaltensweise beurteilt werden muss, ist die h.M. zur Abgrenzung heranzuziehen. Nur diese gelangt zu einem differenzierenden Ergebnis, bei dem das Täterverhalten ausreichend Würdigung findet. Die Abgrenzung nach dem Energieeinsatz greift zu kurz, da auch in mehrdeutigen Fällen ein Energieeinsatz vorliegen kann, eine Bewertung nach dem sozialen Handlungssinn jedoch zu einem anderen Ergebnis als aktivem Tun gelangt.[389] Ebenso verhält es sich mit der Abgrenzung nach der Kausalität. Auch hier ist eine Bewertung der Tat lediglich nach der Änderung des Kausalverlaufes nicht in der Lage den Sachverhalt in seiner gesamten Dimension zu erfassen.[390] Kein anderes Ergebnis lässt auch die Kumulation beider Merkmale zu, sodass auch diese impraktikabel ist.

Die Ansicht von *Altenhain* versucht zwar speziell auf die Erfordernisse des Internets einzugehen, sie führt jedoch zu einer zu weiten Fassung des aktiven Tuns und zu einer Quasi-Aufhebung der Differenzierung. Konsequenz dessen ist eine faktische Aushebelung des § 13 Abs. 2 StGB.[391] Es muss daher auch bei Straftaten, die im Internet stattfinden oder über das Medium Internet begangen werden, anhand von normativer Betrachtung und unter Berücksichtigung des sozialen Handlungssinns in dem konkreten Täterverhalten der Schwerpunkt des strafrechtlich relevanten Handelns ermittelt werden.

---

388 *Fischer*, § 13 Rn. 5; *Wessels/Beulke*, Rn. 700; Hoeren/Sieber/Holznagel/*Sieber*, Multimediarecht, Kap. 19.1, Rn. 22; BGHSt 6, 59, 40, 257; BGH NStZ 1999, 607.

389 Z.B. ist die Aufgabe von Rettungsmaßnahmen nach h.M. als Unterlassen weiterer Rettungsbemühungen zu qualifizieren.

390 Z.B. stellt die Aufgabe von Rettungsmaßnahmen eine Handlung dar, die den Kausalverlauf ändert und damit immer eine Strafbarkeit wegen aktiven Tuns nach sich ziehen würde.

391 BGH NStZ 1999, 607, hier wird ausdrücklich betont, dass § 13 StGB aufgrund seines geänderten Strafmaßes nicht unterlaufen werden darf.

2. Handlung des Access-Providers

Um die Handlung des Access-Providers anhand der eben erörterten Kriterien nach einem Tun oder Unterlassen abgrenzen zu können, muss an dieser Stelle die tatsächliche Handlung des Access-Providers herausgearbeitet werden.

Hilgendorf/Valerius sehen im Rahmen des Internets immer zwei Anknüpfungspunkte, an denen eine Handlung festgemacht werden kann. Zum einen eine inhaltliche Komponente, z.B. durch das Veröffentlichen von Informationen, und zum andern eine rein technische Mitwirkung.[392] Für den Access-Provider ist danach davon auszugehen, dass dieser immer anhand seines technischen Mitwirkens zu beurteilen ist.[393] Es sind mehrere Blickwinkel denkbar, aus denen die Tätigkeit eines Access-Providers betrachtet werden kann. Dabei sind insbesondere folgende Handlungen zu unterscheiden:

a) Eröffnen des Internetzugangs

Eine Handlung des Access-Providers besteht darin, den potentiellen Nutzern den Zugang zum Internet zu verschaffen. Der Access-Provider stellt dafür die notwendige Infrastruktur zur Verfügung. Hierbei wird dem Nutzer eine jeweils neu generierte IP-Adresse zur Verfügung gestellt, welche es ihm ermöglicht, mit den jeweiligen Servern eine Verbindung herzustellen und zu kommunizieren. Diese erfolgt grundsätzlich durch die Übertragung von IP-Paketdatensätze.

b) Durchleiten von Informationen

Durch die Eröffnung des Internetzuganges, den der Access-Provider so lange wie vom Nutzer gewünscht aufrecht erhält, schafft der Access-Provider nicht nur ein „Tor“ zum World Wide Web, er leitet zudem auch jene Daten des Nutzers – fremde und/oder eigene – durch dieses „Tor“, die dieser up- oder downloadet. Diese Handlung stellt die überwiegende Tätigkeit des Access-Providers dar, denn es kommt bei der virtuellen Kommunikation gerade darauf an, dass der Nutzer in der Lage ist, immer schneller Datensätze zu empfangen und zu senden.

---

392 *Hilgendorf/Valerius*, Rn. 236.
393 *Hilgendorf/Valerius*, Rn. 239.

c) Bereitstellen von Infrastruktur

Ein weiteres Betätigungsfeld für den Access-Provider ist das Bereitstellen und Betreiben der zum von ihm ermöglichten Datentransfer notwendigen Kommunikationsnetze oder zumindest der notwendigen Einwahlpunkte. Dies ist jedoch dem Access-Providing nicht wesensimmanent, sodass nicht jeder als Access-Provider einzustufende Diensteanbieter auch ein eigenes Datennetz betreibt. Aufgrund der ehemals zentralen Postverwaltung, die ursprünglich die Leitungsnetze betrieb, hat sich in Deutschland – zwar kontrolliert durch die Bundesnetzagentur – eine grundsätzlich monopolartige Struktur erhalten, die dazu führt, dass sich das Datennetz überwiegend in der Hand eines einzigen Konzerns befindet.

d) Keine Entfernung oder Sperrung rechtswidriger Informationen

Eine weitere zu untersuchende Handlung des Access-Providers stellt sein Untätigbleiben im Falle des Wissens, dass durch seine Datenleitungen rechtswidrige Informationen transportiert werden, dar. Betrachtet werden muss dieses Geschehen vor dem rechtlichen Hintergrund, dass der Access-Provider gem. § 7 Abs. 2 S. 1 TMG zum proaktiven Suchen nicht verpflichtet ist, er jedoch dennoch, auch über Handlungen Dritter – vom einfachen Hinweis eines Dritten bis hin zum Erlass einer Entfernungs- oder Sperrverfügung – von der Durchleitung rechtswidriger Informationen erfahren kann.

3. Bewertung der Handlungen

Die soeben aufgezeigten Handlungen des Access-Providers sind anhand ihres jeweiligen Schwerpunkts der Vorwerfbarkeit zu bewerten und in das System von Tun und Unterlassen einzuordnen.

a) Eröffnen des Internetzugangs

Das Eröffnen eines Internetzuganges, d.h. der Möglichkeit des Zugriffes auf einen Einwahlknoten, stellt objektiv ein aktives Tun dar. Der Access-Provider ermöglicht durch seine Handlung den Zugang zum Internet. Er stellt die notwendige Hardware zur Verfügung und teilt dem User die zur Benutzung notwendige IP-Adresse zu. Der Schwerpunkt ist folglich in einem Tun zu sehen, nicht in einem Unterlassen.

Was bei der vorliegenden Handlung des Access-Providers dennoch nicht außer Acht gelassen werden darf und was letztendlich zu einem Ausschluss der Vorwerfbarkeit überhaupt führen wird, ist die nach der h.M. bei der Abgrenzung nach dem Schwerpunkt der Vorwerfbarkeit zu beachtende Prüfung des sozialen Handlungssinns, d.h. der Sozialadäquanz der Handlung.

Die Eröffnung des Internetzugangs ist gesellschaftlich gewünscht.[394] Gerade im heutigen beinahe schon Post-Informationszeitalter, in dem das Internet auf Smartphones und Tablet-PCs allgegenwärtig ist, ist die Ermöglichung eines Zugangs zu diesen durch den Access-Provider nicht mehr wegzudenken. Daher ist, auch wenn diese Tätigkeit des Access-Providers als aktives Tun einzustufen ist, eine Strafbarkeit aufgrund des sozialadäquaten Verhaltens ausgeschlossen. Dies wurde vom Gesetzgeber so auch in der Privilegierung nach § 8 TMG festgelegt.

b) Durchleiten von Informationen

Auch das Durchleiten von Informationen ist im Rahmen der Frage nach dem Schwerpunkt der Vorwerfbarkeit als aktives Tun zu werten. Das Durchleiten benötigt zum einen den Einsatz von Energie und setzt zum anderen einen kausalen Tatbeitrag. Daher ist auch hier von aktivem Tun auszugehen. Jedoch ist auch diese Tätigkeit des Access-Providers unter dem Gesichtspunkt der Sozialadäquanz betrachtet gesellschaftlich erwünscht. Damit fehlt es auch in diesem Fall an der Vorwerfbarkeit und folglich an einer strafrechtlich relevanten Handlung.

c) Bereitstellen von Infrastruktur

Das Bereitstellen von Infrastruktur, das eine Handlung mit Dauerwirkung darstellt, ist ebenfalls im Schwerpunkt der Vorwerfbarkeit aktives Tun. Hier wird mit Energieaufwand ein der Informationsdurchleitung dienendes, kausales Geschehen aufrechterhalten. Doch auch hier handelt es sich um ein sozialadäquates Handeln. Das Bereitstellen von Infrastruktur zur Datenübertragung ist ein zentrales Thema im urbanen[395] und ländlichen[396] Raum. Somit ist auch hier nicht von einem strafbaren Handeln auszugehen.

---

394 *Frey/Rudolph*, S.9, S. 174 Rn. 392; *Kessler*, Zur strafrechtlichen Verantwortlichkeit von Zugangsvermittlern, S. 72, m.w.N.

395 Der Ausbau im urbanen Raum läuft nach dem Motto: „Höher, schneller, weiter".

396 Der Ausbau des Breitbandnetzes im ländlichen Raum verläuft nur langsam und ist deshalb immer noch allerorten Parteiprogramm und beliebtes Wahlkampfthema, vgl. hierzu http://www1.wdr.de/themen/politik/sp_neuwahl/programme/medien116.html (08.01.2014).

d) Keine Entfernung oder Sperrung rechtswidriger Informationen

Werden vom Access-Provider Maßnahmen nicht ergriffen, wenn rechtswidrige Informationen von ihm durchgeleitet werden, so liegt der Schwerpunkt der Vorwerfbarkeit in einem Unterlassen. Hat der Access-Provider konkrete Kenntnis davon, dass durch seine Leitungen rechtswidrige Informationen fließen, so liegt der Schwerpunkt der Vorwerfbarkeit nicht darin, dass er den Zugang dazu eröffnet hat oder er das Leitungsnetz unterhält, sondern darin, dass er untätig bleibt. Grundsätzlich könnte man natürlich auch die Zugangseröffnung und deren Aufrechterhaltung als Anknüpfungspunkt in Betracht ziehen, denn gerade hierin steckt der Energieaufwand des Access-Providers und auch ein kausaler Eingriff in den Handlungsverlauf.

Betrachtet man in dieser Konstellation zusätzlich den sozialen Handlungssinn, so ist der Schwerpunkt der Vorwerfbarkeit nicht in aktivem Tun des Access-Providers zu sehen, sondern in dem Unterlassen, geeignete Gegenmaßnahmen zu ergreifen. Dies ist ihm erst mit konkreter Kenntnis von den rechtswidrigen Informationen möglich. Diese Kenntnis kann der Access-Provider entweder aus einer gerichtlichen oder behördlichen Verfügung erlangen, aber auch durch Hinweise Dritter, z.B. im Rahmen eines sog. *notice-and-take-down* Verfahrens. Sie könnte sich aber auch durch zufällige Erkenntnis ergeben. Der Hinweis bzw. die Umstände der Erkenntnis müssen jedoch geeignet sein, dem Access-Provider ohne weitere Nachforschungen – um nicht in Widerspruch zu § 7 Abs. 2 S. 1 TMG zu stehen – ein Tätigwerden zu ermöglichen.

Die Tätigkeit des Access-Providers im Rahmen dieser Konstellation ist in diesem Moment auch nicht mehr gesellschaftlich gewünscht und hinsichtlich der rechtswidrigen Information auch nicht erwünscht, sodass der Vorwerfbarkeits-Vorwurf bestehen bleibt.[397] Vielmehr hat die Gesellschaft den Wunsch und den Anspruch, dass rechtswidrige Handlungen unterbunden werden. Der Schwerpunkt liegt daher in dem Unterlassen des Ergreifens von geeigneten Gegenmaßnahmen, sodass nur eine Strafbarkeit wegen Unterlassen der gebotenen Handlungen in Betracht kommt.

4. Ergebnis

Betrachtet man die grundlegenden Handlungen des Access-Providers, so sind diese überwiegend als aktives Tun einzustufen, welches zudem überwiegend sozialadäquat ist. Diese Handlungen, wie das Eröffnen des Zugangs, das Durchleiten von Informationen und das Bereitstellen der Infrastruktur, sind daher auch gem. § 8 TMG

[397] So auch *Hilgendorf* während des 6. Bayreuther Forums für Wirtschafts- und Medienrecht am 5./6.11.2010 in der Diskussion im Anschluss an den Vortrag von *Hilgendorf*.

privilegiert. Lediglich wenn rechtswidrige Informationen durchgeleitet werden und der Access-Provider davon Kenntnis erlangt, liegt der Schwerpunkt der Vorwerfbarkeit in dem Unterlassen von gebotenen Abwehrhandlungen und damit im nicht privilegierten Anwendungsbereich des § 7 Abs. 2 S. 2 TMG.

III. Tatbeteiligung

Die Handlung des Access-Providers, der wie soeben herausgearbeitet durchaus einen Tatbeitrag in Form eines Unterlassens leisten kann, muss nun vor dem Hintergrund der Beteiligungsformen betrachtet werden. Die Intensität des Tatbeitrages lässt dann den Schluss auf die Begehungsform, d.h. Täterschaft oder Teilnahme, zu.

1. Abgrenzung von Täterschaft und Teilnahme

Wie die Abgrenzung von Täterschaft und Teilnahme vorzunehmen ist, ist im Einzelnen umstritten. Nicht nur vertreten Rechtsprechung und herrschende Meinung in der Literatur unterschiedliche Ansatzpunkte, auch innerhalb der Literatur selbst gibt es verschiedene Lösungsansätze. An dieser Stelle sollen nur die beiden meistvertretenen Ansatzpunkte kurz dargestellt werden.

a) Tatherrschaftslehre

Die in der Literatur stärkste Meinung bildet die Lehre von der Tatherrschaft. Tatherrschaft bedeutet das vom Vorsatz umfasste In-den-Händen-Halten des tatbestandsmäßigen Geschehensablaufes.[398] Täter ist danach, wer das Tatgeschehen planvoll lenkt oder eine mitgestaltende Tatherrschaft besitzt und dadurch die Tatbestandsverwirklichung nach seinem Willen hemmen oder ablaufen lassen kann.[399] Teilnehmer hingegen ist nur derjenige, der ohne eigne Tatherrschaft den Geschehensablauf veranlasst oder fördert.[400]

b) Subjektive Theorie

In der Rechtsprechung wird überwiegend die subjektive Theorie vertreten. Diese bewertet den Tatbeitrag anhand der inneren Einstellung der Beteiligten und nach

[398] *Wessels/Beulke*, Rn. 512, m.w.N.
[399] BGHSt 32, 38; 35, 347.
[400] *Roxin*, S. 546 f.

deren Willensrichtung.[401] Täter ist, wer die Tat als eigene will und mit Täterwillen, sog. animus auctoris, handelt. Teilnehmer hingegen ist, wer die Tat nicht als eigene, sondern als fremde will und lediglich mit Teilnehmerwillen, sog. animus socii, handelt[402]. Die Anwendung dieser Formel in der Rechtsprechung war immer unterschiedlich, die neuere Entwicklung geht jedoch in die Richtung einer Objektivierung derselben und nimmt eine wertende Betrachtung der Vorstellung der Beteiligten anhand objektiver Tatumstände vor. Damit nähert sich die Rechtsprechung der Lehre von der Tatherrschaft an.[403]

c) Stellungnahme

Für die Heranziehung der Tatherrschaftslehre spricht, dass sie nicht den Ungenauigkeiten der subjektiven Theorie ausgesetzt ist. Die Rechtsprechung muss bei Anwendung der subjektiven Theorie die innere Willensrichtung des Täters beurteilen, was sich als schwierig erweist. Der innere Willen und das Wollen eines Täters zum Tatzeitpunkt lassen sich nur schwer nachvollziehen. Eine Beurteilung anhand objektiver Kriterien, die auch äußerlich erkennbar sind, erscheint daher zweckmäßiger. Gegen eine rein objektive Bestimmung der Täterschaft anhand der Tatherrschaftslehre ist auf der anderen Seite einzuwenden, dass § 25 Abs. 2 StGB gerade ein bewusstes und gewolltes Zusammenwirken bei gemeinschaftlicher Begehung fordert[404] und so eine lediglich objektive Bestimmung der Täterschaft möglicherweise gesetzeswidrig wäre. Dass eine rein objektive Betrachtung auch praktisch nicht unproblematisch ist, zeigen die Fälle organisierter Kriminalität, bei denen auch ein nicht den Tatplan ausführender, hierarchisch übergeordneter Chef einer kriminellen Vereinigung Täter sein soll.[405]

Der Bundesgerichtshof beurteilt die Frage der Täterschaft nunmehr aufgrund aller von der Vorstellung der Beteiligten umfassten Umstände in wertender Betrachtung.[406] Dieser sich der objektiven Tatherrschaftslehre annähernden Lösung, die als zentrale Kriterien das Maß des eigenen Interesses am Taterfolg, den Umfang der Tatbeteiligung und die Tatherrschaft bzw. den Willen dazu heranzieht[407], ist zu folgen, denn durch sie werden sowohl die Schwächen der Tatherrschaftslehre einerseits aber auch der subjektiven Theorie andererseits reduziert.

---

401 *Wessels/Beulke*, Rn. 515.
402 RGSt 37, 58.
403 *Fischer*, § 25 Rn. 4.
404 *Wessels/Beulke*, Rn. 517.
405 BGHSt 32, 165.
406 BGHSt 28, 346, 349; 48, 52, 56.
407 BGHSt 37, 291; *Wessels/Beulke*, Rn. 516.

d) Besonderheiten beim Unterlassen

Handelt es sich wie vorliegend um eine mögliche Strafbarkeit des Access-Providers aufgrund eines Unterlassens, so gibt es im Rahmen der Abgrenzung zwischen Täterschaft und Teilnahme dort teilweise weitergehende Theorien, die hier kurz erörtert werden sollen. Zum einen ist hier die Pflichtdeliktstheorie von *Roxin* zu nennen, nach der jeder Garant Täter ist, sofern nicht subjektive oder persönliche Merkmale fehlen.[408] Eine Täterschaft ist danach dann gegeben, wenn der Garant eine Erfolgsabwendungspflicht verletzt, die aus seiner Garantenpflicht erwächst. Beihilfe liegt danach nur vor, sofern sich die Erfolgsabwendungspflicht selbst wieder auf eine Beihilfetat bezieht. Dagegen wird zurecht eingewandt, dass das Bestehen einer Garantenpflicht nichts über die Rolle des Handelnden im Tatgeschehen aussagen könne.[409] Auch würde der Unterlassende gegenüber dem aktiveren Tatbeteiligten benachteiligt, der ebenfalls nur Beihilfe leisten könnte.[410] Des Weiteren wird vertreten, dass ein Unterlassen stets nur eine Beihilfe-Strafbarkeit nach sich ziehen könne, denn die Tatherrschaft liege immer beim aktiv handelnden Täter.[411] Hiergegen spricht jedoch das Argument, dass ein Nicht-Handelnder, der im Falle der Beteiligung Dritter gegen diesen eine Handlung unterlässt, besser gestellt wäre als derjenige, der aufgrund eines natürlichen Ereignisses (z.B. Ertrinken) in einen Kausalverlauf nicht eingreift.[412] Eine weitere Ansicht stellt auf den Pflichteninhalt des Garanten ab, der Beschützergarant sei – ob seiner Nähe zum Opfer – stets Täter, der Überwachergarant stets Teilnehmer.[413] Die Rechtsprechung hingegen weicht bei der Abgrenzung zwischen Täterschaft und Teilnahme auch beim Unterlassungsdelikt nicht von der oben bereits dargestellten Abgrenzungsmethode ab. Auch in diesem Fall nimmt die Rechtsprechung eine wertende Betrachtung anhand objektiver Kriterien vor.[414]

2. Einordnung der Handlung des Access-Providers

Nimmt man nun das Unterlassen des Access-Providers und betrachtet es anhand der Tatherrschaftslehre sowie der subjektiven Theorie der Rechtsprechung, so ist die Handlung des Access-Providers wie folgt zu bewerten:

---

408 *Roxin* AT II, § 31, Rn. 140ff; *Fischer*, § 13, Rn. 50, m.w.N.
409 *Kühl*, § 20, Rn. 230.
410 *Hilgendorf/Valerius*, Rn. 245.
411 *Lackner*/*Kühl*, § 27, Rn. 5, m.w.N.
412 *Hilgendorf/Valerius*, Rn. 245.
413 Schönke/Schröder/*Heine*, vor § 25, Rn. 101 ff.
414 *Fischer*, § 13, Rn. 52.

a) Tatherrschaftslehre

Nach der Tatherrschaftslehre scheidet eine Allein-Täterschaft des Access-Providers aus. Der Access-Provider hält den Geschehensablauf nicht selbst in Händen. Ausgangspunkt für die Erfüllung ist immer eine Verfügungsmacht über das Verbreitungsgut – z.B. Pornographie – welche der Access-Provider nicht innehat. Hinsichtlich einer möglichen Mittäterschaft des Access-Providers könnte ein arbeitsteiliges Vorgehen, wie es bei Mittätern meist der Fall ist, durchaus angenommen werden. Jedoch scheitert auch eine Mittäterschaft schon am Fehlen eines gemeinsamen Tatplans sowie einer irgendwie gearteten Beuteteilungsabsicht. Vielmehr ist zwischen den Tatbeteiligten eine Kommunikation nicht erkennbar. Zudem fehlt auch das finanzielle Motiv des Access-Providers, der grundsätzlich nicht mehr für das Durchleiten rechtswidriger Informationen erhält als das übliche Leitungsentgelt für das Durchleiten rechtmäßiger Informationen. Es kommt daher i.S. der Tatherrschaftslehre in der Regel lediglich eine Form der Beteiligung in Betracht.

b) Subjektive Theorie

Nach der subjektiven Theorie ist festzustellen, dass der Access-Provider keinen Täterwillen besitzt. Der Access-Provider hat kein Interesse an der rechtswidrigen Tat. Ihm kommt es lediglich darauf an, mit den von ihm erbrachten Leistungen Profit zu erzielen. Auch ein Wille des Access-Providers, eine eigene Straftat zu begehen, ist nicht ersichtlich. Danach scheidet auch nach der subjektiven Theorie eine Täterschaft des Access-Providers aus. Auch eine Mittäterschaft kommt nicht in Betracht, denn der Access-Provider hat auch keinen dahingehenden Mittäterwillen.

c) Ergebnis

Der Access-Provider handelt nicht täterschaftlich. Sowohl nach der Tatherrschaftslehre der Literatur als auch nach der subjektiven Theorie der Rechtsprechung scheidet Täterschaft aus, denn der Access-Provider hält weder das Tatgeschehen aktiv in Händen noch besitzt er einen erforderlichen Täterwillen.

3. Teilnahme des Access-Providers

Nachdem soeben festgestellt worden ist, dass der Access-Provider nicht täterschaftlich handelt, kommt für sein Verhalten nur noch die Bewertung als Teilnahmehandlung im Rahmen der Beteiligungsformen in Betracht. Nicht näher untersucht

werden soll die Strafbarkeit des Access-Providers als Anstifter gem. § 26 StGB. Eine Anstiftung durch den Access-Provider kommt in der Regel nicht in Betracht, denn im klassischen Fall wird durch den Access-Provider niemand zu einer Handlung bestimmt. Der Access-Provider fördert lediglich die durch einen Dritten begangene Haupttat durch die Zugänglichmachung des Internet und die Durchleitung der Daten. Zu prüfen ist daher das Vorliegen der Voraussetzungen der Beihilfe gem. § 27 StGB.

a) Akzessorietät

Erste Voraussetzung für eine vom Access-Provider zu realisierende Beihilfe ist, wie bei allen Teilnahmedelikten, das Bestehen einer rechtswidrigen Haupttat, die vom Teilnehmer gefördert wird. Vorliegend kommen insbesondere die bereits oben dargestellten Straftaten in Betracht.Ausreichend ist nach dem StGB das Vorliegen ei ner limitierten Akzessorietät, d.h. die Haupttat muss lediglich rechtswidrig sein, i.S.v. § 11 Abs. 1 Nr. 5 StGB. Der Haupttäter muss jedoch nicht schuldhaft handeln. Abgeleitet wird dieser Gedanke von § 29 StGB, nachdem jeder Beteiligte nach seiner Schuld bestraft wird.[415] Handelt ein Haupttäter ohne Schuld, so ist ein schuldhaft handelnder Teilnehmer trotzdem zu bestrafen.

b) Hilfeleisten

Der Teilnehmer muss dem Haupttäter zu seiner Tat Hilfe leisten. Als *Hilfeleisten* ist jeder Tatbeitrag zu bewerten, der die Haupttat ermöglicht, erleichtert oder fördert.[416] Auch durch ein Unterlassen kann der Teilnehmer Hilfe leisten, aber nur dann, wenn auch der Teilnehmer eine Garantenstellung entsprechend § 28 Abs. 1 StGB inne hat. Fehlt diese, so kommt eine Beihilfe durch Unterlassen nicht in Betracht. Die Form der Hilfeleistung wird generell in zwei Arten aufgeteilt:

Zum einen kann der Gehilfe physische Beihilfe zur Haupttat leisten. Die physische Beihilfe des Teilnehmers drückt sich dabei entweder in einer nach außen gerichteten Handlung aus, welche die Umsetzung der Haupttat unterstützen soll, oder im Falle des Unterlassens die Nicht-Ausführung einer nach den äußerlichen Umständen gebotenen Handlung.[417]

Zum andern kommt die Form der psychischen Beihilfe in Betracht. Hierbei wird der Haupttäter durch den Gehilfen nicht durch einen äußerlich erkennbaren Tatbei-

---

415 *Wessels/Beulke*, Rn. 553.
416 *Fischer*, § 27, Rn. 14.
417 *Fischer*, § 27, Rn. 10.

trag unterstützt, sondern durch die Stärkung des Willens des Haupttäters, die Tat durchzuführen. Sie kann ebenfalls entweder durch aktives Tun oder durch Unterlassen geleistet werden.[418]

c) Beihilfe des Access-Providers

Auch der Access-Provider kann im Rahmen seiner Handlungen Beihilfe zu einer Haupttat leisten. Wie bereits oben festgestellt, kommt ein Tatbeitrag des Access-Providers nicht durch aktives Tun, sondern durch ein Unterlassen in Betracht, nämlich indem er es unterlässt, bei Kenntnis der Rechtswidrigkeit von durchgeleiteten Informationen geeignete Gegenmaßnahmen zu ergreifen. Dieses Unterlassen des Access-Providers kann nicht als psychische Beihilfe ausgelegt werden. Dazu müsste der Access-Provider mit seiner Handlung insbesondere den subjektiven Willensentschluss des Haupttäters fördern. Dies kommt jedoch schon deshalb nicht in Betracht, da nicht davon auszugehen ist, dass der Haupttäter Kenntnis davon hat oder erlangt, dass der Access-Provider selbst Kenntnis vom Inhalt der durchgeleiteten Informationen hat. Da die psychische Beihilfe zwingend voraussetzt, dass dem Haupttäter zumindest ein Gefühl von Sicherheit suggeriert wird[419], scheidet sie vorliegend aus. Aufgrund der fehlenden Kenntnis des Haupttäters von einer Unterstützungshandlung durch den Access-Provider und wird daher auch nicht in seinem Willensentschluss bestärkt.

Somit kommt nur eine physische Beihilfe in Betracht, bei der per se die Haupttat gefördert wird. Der Access-Provider unterstützt die rechtswidrige Haupttat, von der er Kenntnis erlangt hat, indem er es unterlässt, eine gebotene Handlung vorzunehmen, die die Übertragung von rechtswidrigen Informationen verhindert oder beendet.

d) Ergebnis

Im Ergebnis stellen die Handlungen des Access-Providers folglich physische Beihilfe zu einer rechtswidrigen Haupttat dar. Diese wird vom Access-Provider durch ein Unterlassen von zumutbaren Gegenmaßnahmen verwirklicht. Ein Unterlassen ist jedoch einer aktiven Handlung nur dann gleichgestellt, wenn der Unterlassende im Rahmen einer Garantenstellung verpflichtet ist, den tatbestandlichen Erfolg abzuwenden, der durch die Haupttat eintreten soll. Dies ist nun im Nachfolgenden noch näher zu erörtern.

---

418 BGHSt 40, 315.

419 *Fischer*, § 27, Rn. 12.

IV. Garantenstellung

Der Access-Provider muss eine Garantenstellung innehaben, die eine Garantenpflicht nach sich zieht, aufgrund deren er rechtlich dafür einzustehen hat, dass der tatbestandliche Erfolg nicht eintritt. Eine Garantenstellung ist notwendig, da der Unrechtsgehalt der Nicht-Vornahme einer gebotenen Handlung anders einzuschätzen ist als derjenige bei einer aktiven Erfolgsherbeiführung, § 13 StGB. Deshalb ist bei unechten Unterlassungsdelikten eine Modalitätenäquivalenz zu fordern[420], d.h. der Unrechtsgehalt des Unterlassens muss dem der Verwirklichung des Tatbestandes durch ein aktives Tun entsprechen. Dies wird durch das Vorliegen einer Garantenstellung erreicht. Nur wenn der Access-Provider also eine Garantenstellung innehat, kann sein Unterlassen gem. § 13 StGB einem aktiven Tun gleichgestellt werden und er damit eines unechten Unterlassungsdeliktes strafbar sein. Das Vorliegen einer Garantenstellung stellt im Rahmen des unechten Unterlassungsdeliktes ein ungeschriebenes Tatbestandsmerkmal dar.[421] Die bloße Möglichkeit der Erfolgsverhinderung oder eine sittliche Pflicht hierzu genügen als Anforderungen nicht.[422]

1. Entstehen der Garantenstellung

Die Begründung einer Garantenstellung ist in Rechtsprechung und Lehre umstritten und die Entstehung einer Garantenstellung, aus der sich ein rechtliches Dafür-Einstehen-Müssen, dass der verbotene Erfolg nicht eintritt, ergibt, ist nicht abschließend geklärt.[423] Früher wurde insbesondere in der Rechtsprechung zwischen Garantenstellungen aus enger Lebensgemeinschaft, aus Vertrag, aus Gesetz und aus Ingerenz unterschieden. Diese förmliche Einteilung in Unterscheidungsmerkmale wird in der neueren Lehre, aber auch die Rechtsprechung, durch eine Unterteilung in materielle Entstehungsgründe ersetzt.[424]

Diese neuere Ansicht ordnet die Entstehungsgründe der Garantenstellung in zwei grundlegende Kategorien ein. Die Einteilung erfolgt dabei nach materiellen Kriterien der Pflichtbegründung. Zum einen wird nach besonderen Schutzpflichten für bestimmte Rechtsgüter unterschieden, den Beschützergaranten. Zum anderen wird unterschieden nach der Verantwortlichkeit für bestimmte Gefahrenquellen, den Überwachergaranten.[425] Legt man diese Zweiteilung zugrunde, so ergibt sich folgendes

---

[420] BGHSt, 28, 300, 307.
[421] BGHSt GrS 16, 155, 158.
[422] *Fischer*, § 13, Rn. 8.
[423] *Wessels/Beulke*, Rn. 716.
[424] *Fischer*, § 13, Rn. 11, 12, 13.
[425] BGHSt 48, 77, 82ff; 48, 301.

Ordnungsbild: In die Gruppe der Beschützergaranten fallen denjenigen, die freiwillig besondere Schutzpflichten für bestimmte Rechtsgüter inne haben. Hierzu zählen die freiwillige Übernahme von Schutz- und Beistandspflichten, die Stellung als Amtsträger oder Organ juristischer Personen, die Lebens- oder Gefahrgemeinschaft und besonderer Rechtssätze oder enge natürliche Verbundenheit. Zu der Gruppe der Überwachergaranten, d.h. denjenigen mit besondere Verantwortlichkeit für bestimmte Gefahrenquellen, zählen die Entstehungsgründe der Verkehrssicherungspflichten, der Inverkehrbringung von Produkten, der Pflicht zur Beaufsichtigung Dritter und der Ingerenz.[426] Nahm die ältere Lehre eine Unterscheidung nach förmlichen Kriterien vor, so unterscheidet die heute überwiegende Ansicht die Garantenstellungen nach materiellen Kriterien. Die Abgrenzung zwischen den einzelnen Gruppen ist jedoch nicht starr, und es kann somit zu Überschneidungen einzelner Garantenstellungen kommen.

2. Die einzelnen Garantenstellungen

Um untersuchen zu können, ob auch ein Access-Provider eine Garantenstellung innehaben kann, die eine Erfolgsabwendungspflicht nach sich zieht, werden die einzelnen Entstehungstatbestände der Garantenstellungen im Folgenden kurz dargestellt:

a) Beschützergaranten

Der Beschützer- oder Obhutsgarant hat besondere Schutzpflichten inne oder übernimmt solche für bestimmte Rechtsgüter. Dem Beschützergarant haftet folglich eine Vertrauensstellung gegenüber der zu beschützenden Person an. Mit diesem gegenüber der zu beschützenden Person erweckten Vertrauen, muss diese Person selbst oder ein Dritter, der ebenfalls zum Schutze verpflichtet sein muss, rechnen. Unterlässt der zu Beschützende oder der dazu verpflichtete Dritte aufgrund des vom Beschützergarant erweckten Vertrauens Maßnahmen, die notwendig gewesen wären, um die zu beschützende Person vor Verletzung zu bewahren, so ergibt sich für den Beschützergarant daraus eine Garantenstellung, die ihn zum Handeln verpflichtet.[427] Eine Garantenpflicht als Beschützergarant folgt insbesondere aus Gesetz, Vertrag, einer Gefahrgemeinschaft oder deren Übernahme.

---

[426] Übersicht bei *Wessels/Beulke*, a.a.O.

[427] *Popp*, Die strafrechtliche Verantwortlichkeit von Internet-Providern, S. 130 ff.

aa) Gesetz

Zunächst kann eine Stellung als Garant aus gesetzlichen Vorschriften erwachsen.[428] Je nach Ausgestaltung der Norm ist die Reichweite der daraus entstehenden Schutzpflicht unterschiedlich und muss am jeweiligen Einzelfall geprüft werden. Häufig werden hier die Normen zur Regelung der Ehe, § 1353 BGB, des Eltern-Kind-Verhältnisses, § 1626 BGB, oder der Lebenspartnerschaft, § 2 LPartG, genannt, aus denen sich Garantenpflichten ergeben. Aber auch aus öffentlich-rechtlichen Vorschriften können grundsätzlich Garantenstellungen hervorgehen.[429]

bb) Vertrag

Eine Garantenstellung als Beschützergarant kann zudem aus der vertraglichen Übernahme von Schutzpflichten entspringen. In diesem Fall verpflichtet sich der eine Vertragspartner gegenüber dem anderen, Pflichten zu übernehmen, die zum Schutze des anderen bestimmt sind.[430] Diese Pflichten können sowohl Hauptpflichten des Vertrages sein, die Garantenstellung kann sich jedoch auch aus Nebenpflichten ergeben.[431] Die vertragliche Verpflichtung muss zum Tatzeitpunkt bereits bestehen, um eine für das Strafrecht relevante Garantenstellung zu begründen.

cc) Lebens- oder Gefahrengemeinschaft

Ebenso kann eine Garantenstellung als Beschützergarant aus einer Lebens- und Gefahrengemeinschaft entstehen.[432] Eine Gewähr für gegenseitige Hilfe und Fürsorge, die in diesem Fall die Garantenstellung begründet, entsteht nicht schon durch das Eingehen einer Ehe- oder Lebensgemeinschaft.[433] Notwendig zur Begründung einer Garantenstellung ist über das bloße bestehen der Ehe oder Lebensgemeinschaft hinaus, dass durch diese ein Vertrauensverhältnis entstehen soll, aus dem sich gegenseitige Fürsorgepflichten ergeben.[434]

---

428 BGHSt 19, 168; 7, 271.
429 *Wessels/Beulke*, Rn. 718; *Fischer*, § 13, Rn. 19ff, m.w.N.
430 *Wessels/Beulke*, Rn. 719a; *Fischer*, § 13, Rn. 36 ff.
431 BGHSt 46, 196.
432 BGHSt 2, 153; 17, 359; 19, 167.
433 *Fischer*, § 13, Rn. 43ff, m.w.N.
434 *Wessels/Beulke*, Rn. 719; *Fischer*, § 13, Rn. 44.

dd) Freiwillige Übernahme von Schutz- und Beistandspflichten

Des Weiteren kann die Stellung als Beschützergranat auch aus der freiwilligen Übernahme von Schutz- und Beistandspflichten herrühren.[435] Für die Entstehung der Erfolgsabwendungspflicht ausschlaggebend ist hier die Übernahme dieser Schutzpflichten im Tatsächlichen.[436]

Wann bei dieser Fallgruppe eine Garantenstellung entsteht, muss maßgeblich daran gemessen werden, ob im Vertrauen auf die übernommenen Schutz- und Beistandspflichten andere Schutzmaßnahmen unterblieben sind. Ist dies der Fall und hat der Geschädigte auf die Gewährsübernahme vertraut, so ist eine Garantenstellung zu bejahen.

ee) Stellung als Amtsträger oder Organ einer juristischen Person

Eine Garantenstellung kann sich zudem auch aus einer Stellung als Amtsträger oder als Organ einer juristischen Person ergeben. Diese Ämter können mit einem besonderen Pflichtenkreis verbunden sein, der zu einer Garantenstellung führt. Die Tatsache, dass es sich um einen Amtsträger handelt, löst jedoch für sich noch nicht automatisch eine Garantenstellung aus. Denn die Verpflichtung des Staates zur präventiven Vorsorge für die Sicherheit von Rechtsgütern ist für das Auslösen einer Garantenstellung zu allgemein gehalten. Entscheidend muss hier immer eine Einzelfallbetrachtung sein.[437] Ebenso ist auch die Garantenstellung von Organen juristischer Personen zu beurteilen. Auch hierbei muss im Einzelfall geprüft werden, ob bestimmte Schutzpflichten vorliegen, aus denen sich eine Garantenstellung ergeben kann.

b) Überwachergaranten

Die zweite Personengruppe für eine Garantenstellung ist die der Überwachergaranten. Ihre Garantenstellung entspringt einer bestimmten Verantwortlichkeit für eine Gefahrenquelle, über die der Überwachergarant Kontrolle ausübt. Im Einzelnen ergeben sich die Garantenstellungen aus Gründen der Sachherrschaft, dem Inverkehrbringen von Produkten, einer Beaufsichtigungspflicht oder einer Ingerenz:

---

435 BGH NJW 1979, 1258.

436 *Wessels/Beulke*, Rn. 720; *Fischer*, § 13, Rn. 44.

437 *Fischer*, § 13, Rn. 29, m.w.N.

aa) Sachherrschaft über eine Gefahrenquelle

Eine Garantenstellung kann sich zunächst aus dem Bestehen einer Verkehrssicherungspflicht ergeben. Diese folgt zumeist aus der Sachherrschaft über eine Gefahrenquelle bzw. aus der Eröffnung derselbigen. Wer die faktische Herrschaft über eine Gefahrenquelle inne hat oder eine Gefahrenquelle eröffnet ist verpflichtet die Gefahren abzuwehren, die auf den Zustand dieser Sache zurückzuführen sind.[438] Bei dieser Fallgruppe ist nicht von Belang, ob die Gefahr auf pflichtwidrigem Verhalten beruht oder durch ein sozialadäquates Handeln geschaffen wurde. Dies ist bei den Verkehrssicherungspflichten deshalb nicht relevant, weil Dritte sich darauf verlassen können müssen, dass Gefahrenquellen, auf die sie nicht einwirken dürfen, durch den tatsächlich Verfügungsberechtigten ordnungsgemäß überwacht werden, so dass für sie keine Gefahr von diesen ausgeht.[439]

bb) Inverkehrbringen von Produkten

Auch durch das Inverkehrbringen von Produkten kann eine Garantenstellung im Rahmen einer strafrechtlichen Produkthaftung entstehen. Nicht erforderlich an dieser Stelle ist, dass das Vorverhalten des Garanten pflichtwidrig war.[440] Auch bei rechtmäßigem Vorverhalten kann eine Garantenstellung entstehen, wenn der Hersteller es unterlässt, eine aus Produktfehlern entstehende Gefahr für Dritte abzuwenden. Den Hersteller trifft dann eine Garantenpflicht.[441] Nach der h.L. soll es in diesem Falle ausreichen, dass der Gefährdungserfolg rechtlich zu missbilligen ist. Ein zumindest fahrlässiges pflichtwidriges Vorverhalten sei nicht notwendig.[442]

cc) Pflicht zur Beaufsichtigung Dritter

Darüber hinaus kann sich eine Garantenstellung als Überwachergarant aus der Pflicht zur Beaufsichtigung Dritter ergeben. Voraussetzung ist, dass von dem Dritten eine Gefahr ausgeht und der Garant rechtlich in einer solchen Beziehung zu dem Dritten steht, aus der eine Verpflichtung für den Garanten erwächst, eine erforderli-

---

438 BGHSt 53, 38, 41 f.

439 *Wessels/Beulke*, Rn. 723; *Fischer*, § 13, Rn. 60 ff.

440 BGHSt 37, 106, 115 f.

441 *Wessels/Beulke*, Rn. 728.

442 *Fischer*, § 13, Rn. 71; ausführlich hierzu *Hilgendorf*, in: Strafrechtliche Produzentenhaftung in der „Risikogesellschaft“.

che Erfolgsabwendungshandlung zu tätigen.[443] Auch in diesem Fall hat der Garant rechtlich dafür einzustehen, dass der Erfolg nicht eintritt.

dd) Ingerenz

Als letzte Fallgruppe, aus der eine Garantenstellung entsteht, ist die Ingerenz zu nennen. Die Garantenstellung entsteht hier durch ein pflichtwidriges Vorverhalten des Garanten.[444] Derjenige, der durch sein objektiv pflichtwidriges Handeln eine Gefahr für Rechtsgüter Dritter geschaffen hat, ist verpflichtet, den aus dieser Gefahr drohenden Erfolg abzuwenden. Im Fall der Ingerenz kommt es gerade auf die Pflichtwidrigkeit des Vorverhaltens an.[445] Ob auch rechtmäßiges Vorverhalten eine Garantenstellung nach sich ziehen kann, ist umstritten. Die h.M. scheint diese bei rechtmäßigem Vorverhalten wohl abzulehnen. Die Erfolgsabwendungspflicht entstehe gerade aus der Pflichtwidrigkeit des Vorverhaltens.[446] Eine differenzierende Ansicht hingegen möchte auch das Entstehen einer Garantenstellung bei rechtmäßigem Vorverhalten in engen Grenzen zulassen, z.B. durch die Eröffnung einer Gefahrenquelle durch den Betrieb eines Kraftfahrzeuges.[447]

3. Garantenstellung des Access-Providers

Auch die Tätigkeit des Access-Providers kann unter einzelne Punkte des soeben vorgestellten Systems zur Entstehung von Garantenstellungen gefasst werden. Anhand der aufgezeigten Systematik muss daher die Tätigkeit des Access-Providers in dieses Schema eingeordnet werden.

a) Access-Provider als Beschützergarant

Teilweise wird in diesem Zusammenhang vertreten, dass der Access-Provider kein Beschützergarant sein könne. Angeführt wird dafür das Argument, die bzgl eines Access-Providers überwiegend in Betracht kommenden Verbreitungsdelikte schützten mehrheitlich abstrakte Rechtsgüter. Der Access-Provider habe keine andere Schutzpflicht als andere in Betracht kommende Garanten.[448] Diese Beurteilung ver-

---

443 *Wessels/Beulke*, Rn. 724, m.w.N.
444 RGSt 24, 339; 64, 276.
445 *Wessels/Beulke*, Rn. 725; *Fischer*, § 13, Rn. 52.
446 *Fischer*, § 13 Rn. 52ff m.w.N.
447 *Wessels/Beulke,* Rn. 727, m.w.N.
448 *Sieber*, JZ 1996, 494, 500.

kennt jedoch, dass die in Betracht kommenden Straftatbestände – insbesondere die der §§ 184 ff StGB – zumindest auch dem Schutz von Kindern, Jugendlichen und Heranwachsenden dienen. Dem damit einhergehenden gewollten Schutz der ungestörten Entwicklung dieser Gruppe durch den Gesetzgeber ist eine differenzierte Betrachtung geschuldet.[449] Daher kann eine Stellung des Access-Providers als Beschützergarant nicht von vornherein ausgeschlossen werden.

Der Access-Provider kann – wie nachfolgend dargestellt – durchaus eine Stellung als Beschützergarant innehaben. Nicht in Betracht kommen jedoch die Garantenstellungen aus einer Lebens- oder Gefahrengemeinschaft und aus einer Stellung als Amtsträger oder Organ einer juristischen Person. Der Access-Provider unterhält weder eine Nähebeziehung zu seinem Kunden/Nutzer, noch bildet er mit diesem keine Gefahrengemeinschaft hinsichtlich der Gefahrenquelle des Internets.

aa) Garantenstellung aus Gesetz

Im Rahmen einer Garantenpflicht als Beschützergarant kommt für den Access-Provider durchaus eine Garantenstellung, beruhend auf einer gesetzlichen Grundlage, in Betracht.

(1) Garantenstellung aus dem TMG

Direkt aus dem Telemediengesetz ist eine Garantenstellung für den Access-Provider nicht herzuleiten. Die sich aus dem TMG ergebenden Rechtsfolgen stellen Haftungserleichterungen für die Diensteanbieter dar und sollen die Haftung insofern einschränken, nicht erweitern. Dies gilt auch im Hinblick auf eine mögliche Garantenstellung, die sich daraus herleiten ließe.[450] Es ergibt sich jedoch auch schon aus der Begründung zum TDG a.F., dass der Gesetzgeber eine Haftungserweiterung oder -begründung durch die Vorschriften zur Privilegierung der Diensteanbieter nicht wollte.[451]

---

449 *Popp*, Die strafrechtliche Verantwortlichkeit von Internet-Providern, S. 130.

450 *Blanke*, Über die Verantwortlichkeit des Internet-Providers, S. 95; *Satzger*, in: Strafrechtliche Providerhaftung, S. 171.

451 BT-Drs. 14/6098, S. 23.

(2) § 5 Abs. 1 Jugendmedienschutz-Staatsvertrag

Eine Garantenstellung aus dem Gesetz kann sich für den Access-Provider jedoch aus § 5 Abs. 1 JMStV[452] ergeben. Ziel des JMStV ist es, Kinder und Jugendliche vor entwicklungs- oder erziehungsgefährdenden Inhalten in elektronischen Informations- und Kommunikationsmedien zu schützen. Die Vorschrift des § 5 Abs. 1 JMStV erlegt dem Anbieter eine Schutzpflicht gegenüber Kindern und Jugendlichen auf, derzufolge er verpflichtet ist, entwicklungsbeeinträchtigende Inhalte so anzubieten, dass sie für Kinder und Jugendliche nicht zugänglich sind. Als entwicklungsbeeinträchtigend sind Angebote immer dann anzusehen, wenn sie die Entwicklung zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit hemmen. Ob es sich um ein entwicklungsgefährdendes Angebot handelt, ist an einem durchschnittlich entwickelten Minderjährigen zu messen.[453]

Wer Anbieter im Sinne des JMStV ist, richtet sich nach der Legaldefinition des § 3 Abs. 2 Nr. 2 JMStV[454], demzufolge sind es Rundfunkveranstalter oder Anbieter von Telemedien. Der Access-Provider ist „Anbieter" im Sinne des § 3 Abs. 2 Nr. 2 JMStV.[455] Nachdem auch der JMStV auf die allgemeinen medienrechtlichen Begriffe abstellt[456] und daher der Begriff der Telemedien in § 2 Abs. 2 Nr. 2 JMStV ebenso zu definieren ist wie in § 1 Abs. 1 S. 1 TMG[457], ist der Access-Provider auch nach dem JMStV unter den „Anbieter von Telemedien" zu subsumieren. Die Anwendbarkeit auf den Access-Provider lässt sich auch aus der Vorschrift des § 5 Abs. 1 JMStV selbst herleiten. Die Vorschrift stellt explizit auf das Zugänglichmachen der inkriminierten Angeboten ab. Werden diese im Internet veröffentlicht, so ist es erst der Access-Provider, der ein Zugänglichmachen ermöglicht, indem er den Zugang zum Internet herstellt und aufrechterhält.

Nachdem eine Anwendbarkeit des § 5 Abs. 1 JMStV auf Access-Provider zu bejahen ist, ist ebenso eine sich aus dieser Vorschrift für den Access-Provider ergebende Garantenstellung festzustellen.[458] Wie bereits oben erläutert, setzt die Stellung als

---

[452] § 5 Abs. 1 JMStV: *„Sofern Anbieter Angebote, die geeignet sind, die Entwicklung von Kindern oder Jugendlichen zu einer eigenverantwortlichen oder gemeinschaftsfähigen Persönlichkeit zu beeinträchtigen, verbreiten oder zugänglich machen, haben sie dafür Sorge zu tragen, dass Kinder oder Jugendliche der betroffenen Altersstufen sie üblicherweise nicht wahrnehmen."*

[453] Spindler/Schuster/*Erdemir*, § 5 JMStV, Rn. 8.

[454] Spindler/Schuster/*Erdemir*, § 5 JMStV, Rn. 4.

[455] § 3 Abs. 2 Nr. 1 JMStV: *„Im Sinne dieses Staatsvertrages sind (...) 2. „Anbieter" Rundfunkveranstalter oder Anbieter von Telemedien."*

[456] *Paschke*, § 21, Rn. 1228.

[457] *Frey/Rudolph*, Rn. 49ff, m.w.N. zum gewünschten Gleichlauf zwischen den Regelwerken siehe dort Rn. 51.

[458] Ebenso *Hilgendorf*, K&R 2011, 229ff, 233.

Beschützergarant voraus, dass dieser eine Vertrauensposition gegenüber dem Opfer oder zum Schutz des Opfers verpflichteten Dritten erwirbt.

Der Jugendmedienschutz-Staatsvertrag schafft für die Exekutive ein Mittel, das Zugänglichmachen von nach diesen Vorschriften inkriminierten Inhalten im Rahmen von Bußgeld- bzw. Strafvorschriften zu sanktionieren. Damit wurde ein Instrument geschaffen, auf welches insbesondere Aufsichtspersonen wie Eltern vertrauen, die originär zuständig sind für den Schutz von Kindern und Jugendlichen vor Inhalten, die deren Entwicklung beeinträchtigen. Nachdem sich die Länder durch den Jugendmedienschutz-Staatsvertrag verpflichtet haben, ihre ebenfalls originäre Schutzpflicht gegenüber den schwächsten Mitgliedern der Gesellschaft zu konkretisieren, haben die Länder eine vertrauensbildende Ursache gesetzt. Hieraus folgt, dass nun von Aufsichtspersonen darauf vertraut wird, dass auch ein Access-Provider diese Vorschriften einhält und damit Maßnahmen ergreift, die Kinder und Jugendliche vor entwicklungsbeeinträchtigenden Inhalten schützen, und mit denen er selbst einer Sanktionierung entgeht.[459]

Die Garantenpflicht entsteht jedoch nicht aus einem gesetzten Vertrauenstatbestand alleine. Hinzu kommen muss, wie bereits oben ausgeführt, dass durch die geschaffene Vertrauensposition eine Gefährdungssituation hervorgerufen wird. Diese Gefährdungssituation entsteht erst durch die Inanspruchnahme des gesetzten Vertrauenstatbestands durch das Opfer zum einen und zum anderen durch das Unterlassen von Schutzmaßnahmen durch einen schutzbereiten Garanten – gerade aufgrund des hervorgerufenen Vertrauens.[460] Diese Gefährdungssituation entsteht auch insbesondere in Bezug auf den Access-Provider, da es sich bei diesem immer um einen aus dem Inland agierenden Diensteanbieter handelt, mit dem ein Providervertrag besteht. Zudem wird der Nutzer gerade bei einem aus dem Inland agierenden Diensteanbieter davon ausgehen dürfen, dass dieser die nationalen Gesetze beachtet. Dem Access-Provider kann daher eine nicht unerhebliche Vertrauensstellung zukommen.

Durch den § 5 Abs. 1 JMStV kann folglich beim Access-Provider eine Garantenpflicht entstehen, wenn seitens des Minderjährigen oder seitens eines entsprechend schutzbereiten Garanten das Vertrauen darauf gegeben ist, der Access-Provider werde entwicklungsbeeinträchtigende Inhalte von dem Minderjährigen fernhalten und seiner Verpflichtung aus § 5 Abs. 1 JMStV nachkommen und deshalb von diesen eigene Schutzmaßnahmen unterlassen werden.

---

459 *Kessler*, Zur strafrechtlichen Verantwortlichkeit von Zugangsvermittlern, S. 101, gelangt sogar zu dem Ergebnis, dass der Internet-Nutzer gerade darauf vertrauen dürfe, von inkriminierten Inhalten verschont zu bleiben.

460 *Popp*, Die strafrechtliche Verantwortlichkeit von Internet-Providern, S. 132.

(3) § 4 Jugendmedienschutz-Staatsvertrag

Eine weitere Vorschrift, die aufgrund des vorausgegangenen Ergebnisses eine Garantenstellung als Beschützergarant für den Access-Provider auslöst, ist § 4 JMStV. Nachdem § 5 JMStV bereits seit längerem Eingang in die Diskussion in der Literatur und Lehre gefunden hat[461], sei an dieser Stelle auch der § 4 JMStV durchleuchtet, ob er sich als eine Garantenstellung auslösende Vorschrift entpuppt. § 4 JMStV betrifft „unzulässige Angebote", die Kindern und Jugendlichen nicht zugänglich gemacht werden dürfen. Im Gegensatz zu den „lediglich" entwicklungsbeeinträchtigenden Inhalten des § 5 JMStV handelt es sich bei denen des § 4 JMStV um schwer jugendgefährdende Angebote[462], bei denen es nicht ausreichend ist, dass sie Minderjährige üblicherweise nicht wahrnehmen, sondern die Minderjährigen überhaupt nicht zugänglich gemacht werden dürfen.

Unterschieden wird innerhalb des § 4 JMStV zwischen den „absolut" verbotenen Angeboten, deren Kriterien die Vorschrift des § 4 Abs. 1 JMStV katalogartig aufzählt, und den „relativ" verbotenen Angeboten des § 4 Abs. 2 JMStV, die unter weiteren Voraussetzungen in sog. „geschlossenen Benutzergruppen" i.S.v. § 4 Abs. 2 S. 2 JMStV öffentlich zugänglich gemacht werden können, wenn sichergestellt ist, dass der geschlossenen Benutzergruppe nur Erwachsene angehören.[463] Verglichen mit § 5 JMStV handelt es sich bei § 4 JMStV folglich um die einschneidendere Regelung. Es ist daher möglich, dass im Hinblick auf die soeben bejahte Möglichkeit der Garantenstellung aus § 5 JMStV sich erst recht auch aus § 4 JMStV eine Garantenstellung herleiten lässt.

Es gilt festzuhalten, dass auch diese Vorschrift auf Access-Provider anwendbar ist. Zwar wurde das Zugänglichmachen nicht derart explizit im Normtext festgehalten wie in § 5 Abs. 1 JMStV. Nachdem sich der Access-Provider aber unter den Anbieterbegriff des § 3 Abs. 2 Nr. 2 JMStV subsumieren lässt und es daher auf eine ausdrückliche Nennung nicht ankommt, ist diese Regelung auch auf Access-Provider anzuwenden. Die unzulässigen Angebote, die § 4 JMStV aufzählt, dürfen vielmehr von keinem Anbieter eingestellt oder zugänglich gemacht werden. Erst recht im Hinblick auf diese Vorschrift darf, sowohl vom Minderjährigen als auch vom schutzbereiten Garanten, darauf vertraut werden, dass die Anbieter keine unzulässigen Angebote verbreiten. Dies nicht zuletzt deshalb, weil § 4 Abs. 1 JMStV Angebote in Ver-

---

461 Vgl. z.B. *Hilgendorf*, in: Jugendmedienschutz im Informationszeitalter, S. 117.

462 *Gierschmann*, S. 123.

463 *Paschke*, § 21, Rn. 1230.

bindung mit Straftatbeständen aufzählt, die insbesondere auch das Erwachsenenstrafrecht mitumfassen.[464]

Damit besteht auch im Lichte dieser Vorschrift die Gefahr, dass aufgrund dies hervorgerufenen Vertrauens eine Gefährdungssituation entsteht, wenn tatsächlich darauf vertraut wird, dass die Anbieter diese Vorschrift befolgen. Dies um so mehr, da es bei § 4 JMStV aufgrund der Aufzählung der Straftatbestände in Absatz 1 auch für einen Laien ersichtlich wird, dass er im Besonderen darauf vertrauen kann, dass der Anbieter sich nicht strafwürdig verhält. Eine durch diese Vertrauensposition geschaffene Gefährdungssituation kann daher im Rahmen des § 4 JMStV schneller eintreten, da der Minderjährige oder der schutzbereite Garant hier schneller zu dem Entschluss gelangen, dass sie auf das Tätigwerden des Anbieters vertrauen dürfen und dadurch eigene Abwehrhandlungen oder Vorkehrungen unterlassen.

(4) Ergebnis

Im Ergebnis ist daher auch für § 4 JMStV festzuhalten, dass sich hieraus eine Garantenstellung für den Access-Provider ergeben kann. Ebenso wie bei § 5 JMStV kann hier eine Vertrauensposition hinsichtlich des Access-Providers entstehen, die eine Gefährdungssituation nach sich ziehen kann, aus der schließlich die Garantenpflicht für den Access-Provider erwächst.

bb) Garantenstellung aus Vertrag

Eine Garantenstellung kann sich für den Access-Provider auch aus einer vertraglichen Übernahme von Schutzpflichten ergeben.[465] Grundsätzlich wäre eine vertragliche Übernahme durch den Access-Provider im Rahmen seines Providervertrages mit dem Nutzer denkbar. Der Access-Provider könnte sich vertraglich verpflichten, geeignete Maßnahmen zu ergreifen, um das Durchleiten von inkriminierten Inhalten, wie z.B. Kinderpornographie oder volksverhetzende Inhalte, zu unterbinden. Dies wäre durch ein Filtersystem zu bewerkstelligen, was heutzutage auch technisch möglich ist. Denkbar wäre zum Beispiel der Einsatz von Proxy-Servern durch den Access-Provider, mit deren Hilfe dann inkriminierte Inhalte aussortiert werden[466] oder der Einsatz von hybriden Filtersystemen, wie z.B. sog. „Clean-Feed“ Systemen.[467]

---

464 *Paschke*, a.a.O., Rn. 1231.
465 *Hilgendorf/Valerius*, Rn. 220, 240; *Hilgendorf*, K&R 2011, 229, 233.
466 *Frey/Rudolph*, Rn. 171 ff.
467 *Frey/Rudolph*, Rn. 181 ff.

In der Praxis ist jedoch festzustellen, dass eine vertragliche Verpflichtung des Access-Providers in diesem Maße nicht anzutreffen ist. Vielmehr bieten die Provider lediglich Kinderschutzsoftware an, die auf den entsprechenden Internetseiten heruntergeladen werden kann. Hierbei handelt es sich um ein kostenfreies Zusatzangebot der Provider, das unverbindlich zur Verfügung gestellt wird und aus dem sich eine vertragliche Verpflichtung nicht ergibt. Mit dieser Ausgestaltung als kostenfreies, freiwilliges Zusatzangebot, soll eine vertragliche Bindung gerade vermieden werden, um keine Haftungsgrundlage zu schaffen.

Im Ergebnis ist daher festzuhalten, dass eine Garantenstellung des Access-Providers aus einer vertraglichen Übernahme von Schutzpflichten durchaus in Betracht kommt. In der Praxis ist jedoch festzustellen, dass Access-Provider davon absehen, Schutzpflichten vertraglich zu übernehmen und vielmehr dazu übergegangen sind, lediglich Software-gestützte Filtersysteme anzubieten, mit deren Nutzung sie nach dem Download nichts mehr zu tun haben, sondern für dessen Verwendung der User verantwortlich ist.[468]

cc) Ergebnis zum Beschützergarant

Der Access-Provider kann eine Garantenstellung als Beschützergarant innehaben. Diese kann sich entweder aus Gesetz oder Vertrag ergeben. Nicht in Betracht kommt eine Mitgliedschaft in einer Gefahrengemeinschaft des Access-Providers, da ihm hierfür die persönliche Bindung fehlt. Auch andere oben angeführte Entstehungsmöglichkeiten kommen für den Access-Provider nicht in Betracht. Wenn schon eine vertragliche Übernahme von Schutzpflichten in der Praxis nicht durchgeführt wird, so ist auch die freiwillige Übernahme solcher Pflichten fernliegend.

Die Vorschriften des JMStV können eine Garantenpflicht beim Access-Provider begründen, insofern er Kenntnis von den inkriminierten Inhalten hat und auf sein Tätigwerden vertraut wird. Nachdem ein proaktives Tätig werden vom Access-Provider aber nicht verlangt werden darf,[469] kommt zusätzlich hinzu, dass er auf diese Inhalte aufmerksam gemacht werden muss. Die vorausgesetzte Kenntnis der konkret inkriminierten Inhalte muss dem Access-Provider daher von dritter Seite verschafft werden, da das Gewinnen eigener Erkenntnisse nicht vorausgesetzt werden kann. Das Erfordernis, dass der Access-Provider auf die inkriminierten Inhalte durch einen Dritten aufmerksam gemacht werden muss, ist erforderlich, um zu verhindern, dass

---

[468] Bspw.: http://tarife-und-produkte.t-online.de/mit-kinderschutz-software-surfen-ihre-kinder-sicher-im-internet-/id_12727562/index (07.01.2014).

[469] EuGH, *Scarlet/SABAM,* (Fn. 249).

auf diese Art und Weise das Verbot des proaktiven Tätigwerden-Müssenn – i.S.v. § 7 Abs. 2 S. 1 TMG – ausgehebelt wird. Ist der Access-Provider jedoch über die rechtswidrigen Inhalte in Kenntnis gesetzt worden, so kann auch ihn eine Garantenpflicht als Beschützergarant treffen.

b) Access-Provider als Überwachergarant

Auch in den Fallgruppen, die den Überwachergaranten zugerechnet werden, gibt es Ansatzpunkte, die eine Garantenstellung für den Access-Provider begründen können. In Betracht kommt zum einen die Eröffnung einer Gefahrenquelle und zum anderen ein pflichtwidriges Vorverhalten.

aa) Eröffnung einer Gefahrenquelle

Der Access-Provider, dessen Wirtschaftsmodell darauf ausgerichtet ist, den Zugang zum Internet zu eröffnen und diesen Zugang aufrecht zu erhalten, schafft dadurch auch den Zugang zu einer Gefahrenquelle. Die Garantenstellung entsteht hier, anders als im Falle der Ingerenz, lediglich durch die Eröffnungshandlung und die daraus entstehenden Pflicht, die Umwelt vor den davon ausgehenden Gefahren zu schützen.[470] Nicht notwendig ist, dass diese Handlung objektiv pflichtwidrig ist.[471] Sie kann sogar erwünscht und sozialadäquat sein. Einschränkungen aufgrund der Weite dieses Merkmals und der darin nicht vorausgesetzten objektiven Pflichtwidrigkeit erfährt diese Garantenpflicht über die Frage der Zumutbarkeit der Gefahrenabwehr, das bereits erörterte Kriterium des Vertrauens hinsichtlich der Beherrschbarkeit dieser Gefahrenquelle sowie über das Prüfungsmerkmal des Zurechnungszusammenhangs.

(1) Gefahrenquelle

Die Gefahrenquelle, die der Access-Provider seinem Nutzer eröffnet, ist das Internet selbst. Ob dieses per se als Gefahrenquelle angesehen werden kann, ist umstritten.

Zunächst sei an dieser Stelle kurz in Erinnerung gerufen, dass insbesondere das Internet andauernden Fortentwicklungen unterliegt und mit der vorliegenden Arbeit nur

---

[470] *Blanke*, Über die Verantwortlichkeit des Internet-Providers, S. 96f, m.w.N.

[471] *Kessler*, Zur strafrechtlichen Verantwortlichkeit von Zugangsvermittlern, S. 94, m.w.N.

eine derzeitige Momentaufnahme skizziert werden kann. Zu beobachten ist jedoch, dass das Internet in seiner Fortentwicklung und seiner immer weiteren Verbreitung auch der Kriminalität dadurch eine wachsende Plattform bietet. Hinzu kommt, dass die breite Masse an Nutzern ein immer geringeres Maß an Medienkompetenz mit sich bringt. Die „digital natives" waren in den 1980er Jahren eine noch eher kleine Gruppe – heute würde man wohl den Begriff der Computer-Nerds verwenden – die zum einen für das große kriminelle Geschäft uninteressant waren und zum anderen allen anderen auch technisch überlegen waren.

Heutzutage macht das Internet weder vor dem Kinderzimmer noch vor der Senioren-WG halt. Festzustellen ist jedoch, dass die Verbreitung des Internets nicht dafür sorgt, dass auch die Netz-Kompetenz, d.h. der Grad der Aufgeklärtheit über Nutzungen und Gefahren, in demselben oder jedenfalls einem ausreichenden Maße mitwächst. Dies macht das Internet für Kriminelle interessant, die insbesondere die Anonymität und die grenzüberschreitenden Spielräume für sich nutzen, für Straftaten von Betrug über Flaming[472] zu Pornographie und Volksverhetzung. Platz für Kriminalität entsteht, wo Webspace zur Verfügung steht und immer dort, wo die Handlung keinen Tatbestand erfüllt, denn auch die Entwicklung der Strafgesetze hat Mühe mit der Entwicklung des Internets Schritt zu halten, oder die Anonymität den Täter schützt.

Betrachtet man allein die polizeiliche Kriminalstatistik 2011 für Deutschland, so liegt die Anzahl der mit dem Tatmittel Internet begangenen Straftaten unvermindert hoch bei 222.267 Delikten. Dreiviertel dieser mit Hilfe des Internets begangen Straftaten stellen Betrugsdelikte dar. Zieht man die Gesamtzahl der Waren- und Kreditbetrugsfälle heran, so ist festzustellen, dass dreiviertel der Straftaten mit Hilfe des Tatmittels Internet begangen werden. Pornographische Schriften werden zu fast 60 Prozent über das Internet verbreitet.[473]

Auch die Fälle des Cybercrime bleiben mit fast 60.000 konstant hoch.[474] Hierbei werden die Straftaten unter Ausnutzung der Informations- und Kommunikationstechnik begangen. Nicht ungewöhnlich ist auch hier die schnelle Anpassung der Kriminalität an neue Tatmittel und Möglichkeiten, insbesondere über mobile Endgeräte wie Smartphones oder Tablets.[475] Hinzu kommt, dass sich der Kreis der potentiellen Täter nicht nur durch die Ausbreitung des Internets vergrößert, sondern auch dadurch, dass sich ein Markt für entsprechend neue Schadsoftware bis hin zur Zur-

---

472 Sog. *Flaming* bezeichnet die Straftaten im Zusammenhang mit Beleidigungsdelikten im Web 2.0 (s.o.), vgl. hierzu ausführlich *Hilgendorf*, ZIS, 2010, 208 ff.

473 PKS 2011, S. 261 f.

474 Bundeslagebild Cybercrime 2011, S. 6, online unter www.bka.de (10.01.2014).

475 A.a.O., S. 18.

verfügungstellung ganzer krimineller Infrastrukturen entwickelt hat und dadurch auch technisch nicht versierte Täter Straftaten leicht begehen können.[476]

Der Schaden, der allein in Deutschland durch Internetkriminalität entsteht, ist enorm. Im Jahre 2012 war dieser bereits im September um 16 Prozent im Vergleich zum Vorjahr auf 71,2 Millionen Euro angestiegen. Von mindestens 8,5 Millionen Internetnutzern waren in diesem Zeitraum 2012 bereits Zugangsdaten aller Art ausspioniert worden. 52 Prozent der privaten Internetnutzer in Deutschland hatten im Jahre 2012 bereits persönlich Erfahrungen mit Internetkriminalität gemacht.[477] Betrachtet man die wachsende Internetkriminalität verbunden mit der immer einfacher werdenden Missbrauchsmöglichkeit und der wegen der Anonymität des Internets niedrigen Hemmschwelle bei der Begehung von Straftaten[478], so ist das Internet durchaus als Gefahrenquelle einzustufen.[479]

(2) Herrschaft über eine Gefahrenquelle

Schwieriger zu beantworten ist die Frage, ob der Access-Provider auch eine ausreichende Sachherrschaft über das Internet besitzt und dadurch eine Einwirkungsmöglichkeit hat, die eine Garantenstellung voraussetzt. Durch seine hervorgehobene Stellung bei der Schaffung der Internetverbindung erlangt der Access-Provider eine besondere Beziehung zu der Gefahrenquelle, die es rechtfertigt, ihm eine Garantenpflicht aufzuerlegen. Teilweise wird dies in der Literatur lapidar verneint und eine Garantenstellung damit ausgeschlossen. Das Internet sei nicht kontrollierbar, schon gar nicht für den Access-Provider, der lediglich den Zugang eröffnet und Daten durchleitet. Die geforderte Kontrollmöglichkeit des Garanten sei aufgrund vieler Umgehungsmöglichkeiten der zu verwendenden Filter- und Sperrsysteme nur gering bis gar nicht vorhanden.[480] Als weiteres Argument wird vorgetragen, das Internet an sich sei schon einer umfassenden Kontrolle und damit einer ausreichenden Sachherrschaft für den Garanten entzogen.[481] Mit der Umschreibung des Internet an sich wird

---

476 A.a.O., S. 18.

477 Presseinformation des BKA und des BITKOM vom 17.09.2012, online unter www.bitkom.org (10.01.2014).

478 Vgl. hierzu *Heckmann*, NJW 2012, 2631, 2632 f.

479 Ebenso *Hilgendorf/Valerius*, Rn. 242; *Kessler*, Zur strafrechtlichen Verantwortlichkeit von Zugangsvermittlern, S. 94; *Blanke*, Über die Verantwortlichkeit des Internet-Providers, S. 96ff; *Popp*, Die strafrechtliche Verantwortlichkeit von Internet-Providern, S. 138f, m.w.N.; **a.A.** *Finke*, Die strafrechtliche Verantwortung von Internet-Providern, S. 129; *Pelz*, wistra 1999, 53, 56.

480 *Kessler*, Zur strafrechtlichen Verantwortlichkeit von Zugangsvermittlern, S. 94; *Satzger*, in: Strafrechtliche Providerhaftung, S. 172.

481 *Kessler*, Zur strafrechtlichen Verantwortlichkeit von Zugangsvermittlern, S. 94.

auf den Aufbau des Internet selbst abgestellt, d.h. auf dessen Umfang, Größe und dessen dezentrale, weltweite Struktur.

Andere Teile der Literatur bejahen je nach Providerart eine Kontrollmöglichkeit und damit auch eine ausreichende Sachherrschaft. So sollen Host-Service-Provider über eine ausreichende Sachherrschaft verfügen, da bei ihnen Daten gespeichert werden, auf die sie – aufgrund der tatsächlichen Sachherrschaft über die Datenträger – auch Kontrolle haben. Daran fehle es jedoch beim Access-Provider, der lediglich Zugang vermittelt und Daten leitet.[482] Die Frage, die sich daher an dieser Stelle stellt, ist, wie umfassend die Kontrollmöglichkeit des Garanten sein muss. Grundsätzlich ist es dem Access-Provider von vorneherein lediglich möglich, die konkret durch seine Verbindungen durchgeleiteten Daten zu kontrollieren, denn in erster Linie hat er nur auf diese Zugriff. Dem Access-Provider ist es von seiner Grundkonstruktion her gar nicht möglich, das *gesamte* Internet zu kontrollieren, da er lediglich einen Zugangspunkt schafft und seine Infrastruktur zum Datentransfer zur Verfügung stellt. Die bisher überwiegende Meinung ging bislang deshalb davon aus, dass es dem Access-Provider an der realen und physischen Eingriffsmöglichkeit in den Datenverkehr, zu welchem er den Zugang eröffnet und das Durchleiten ermöglicht, fehlt. Verwiesen wird an diesem Punkt größtenteils auf die fehlenden technischen Möglichkeiten des Access-Providers, einen effektiven Kontrollmechanismus einzusetzen.[483] Diese bisher vorherrschende Ansicht stellt darauf ab, dass die eingesetzten Kontrollmechanismen leicht zu umgehen sind, zum Beispiel durch das bloße Benutzen eines anderen Access-Providers oder das Umgehen eines gesperrten Domainnamens durch die Eingabe der IP-Adresse mit Hilfe eines Whois-Dienstes.

(3) Access-Provider – Herrscher über die Gefahrenquelle

Gegen diese bisher vorherrschende Meinung sind zwei tragende Argumente vorzubringen, die in ihrer Zusammenschau zum heutigen Zeitpunkt eine andere Bewertung der Frage zulassen, ob der Access-Provider aufgrund der Eröffnung einer Gefahrenquelle eine Garantenstellung inne hat oder nicht. Zum einen ist darauf hinzuweisen, dass es in keinem Lebensbereich möglich ist, einen absoluten Schutz vor jeglicher Gefahr zu generieren. Dies ist weder vor dem Hintergrund des Mediums Internet möglich, noch in einem anderen Lebensbereich denkbar. Eine hundertprozentige Reduzierung der von einer Gefahrenquelle ausgehenden Gefahr lässt sich nur

---

482 *Blanke*, Über die Verantwortlichkeit des Internet-Providers, S. 99.

483 *Satzger*, in: Strafrechtliche Providerhaftung, S. 172; *Kessler*, Zur strafrechtlichen Verantwortlichkeit von Zugangsvermittlern, S. 94; *Blanke*, Über die Verantwortlichkeit des Internet-Providers, S. 99, m.w.N.

durch ihre Eliminierung erzielen. Dann bedürfte es aber auch keines Garanten mehr und die gesamte oben geführte Diskussion wäre hinfällig. Die Eliminierung der Gefahrenquelle Internet ist jedoch nicht Sinn und Zweck, nachdem das Internet nicht nur gesellschaftlich gewünscht, sondern heute auch eine gesellschaftliche Basis darstellt, die nicht nur den privaten Bereich, sondern auch den wirtschaftlichen immer mehr betrifft, vereinnahmt und verändert. Der Schluss, der aus der Forderung nach einer vollständigen Sicherheit zu ziehen wäre, wäre somit, dass auch eine Garantenstellung für den Eröffner einer Gefahrenquelle nur dann entstünde, wenn er jegliche davon ausgehenden Gefahren vollständig beherrschen könnte.[484] Erst dann wäre er verpflichtet, geeignete Gegenmaßnahmen zu ergreifen. Das würde bedeuten, dass das Institut der Garantenstellung aus der Eröffnung einer Gefahrenquelle nur noch in den Lehrbüchern zu finden wäre.

Zum anderen ist anzuführen, dass die Argumente der bisher herrschenden Meinung – zumindest derzeit – auch aus technischer Sicht überholt sind. Zwar hat der EuGH in rechtlicher Hinsicht letztinstanzlich bestätigt, dass der Access-Provider zu einem proaktiven Überprüfen der durchgeleiteten Inhalte nicht verpflichtet ist.[485] Jedoch stehen zur Zeit technische Mittel zur Verfügung, die es dem Access-Provider erlauben, seine Datenströme schnell und in großem Umfang zu kontrollieren. Durch den Einsatz neuartiger Filtersysteme, sog. Deep-Packet-Inspections, ist es heute möglich, auch große Datenpakete schnell auf inkriminierte Inhalte zu durchsuchen.[486] Hierbei wird, entgegen dem herkömmlichen Filterverfahren, der Stateful-Packet-Inspection, nicht der aufwendig zu prüfenden Datenteil überprüft. Vielmehr beschränkt sich die Methode der Deep-Packet-Inspections auf die Überprüfung des Header-Teiles des Datenpaketes auf inkriminierte Inhalte.[487] Diese Filtertechnik ist in der Lage, große Datenmengen schnell zu überprüfen und eignet sich daher insbesondere für den Einsatz durch Access-Provider.[488] Wie bei allen Techniken, die auf einem Eingriff in den Datentransfer basieren und die die Unversehrtheit der Daten berühren, wird auch die Methode der Deep-Packet-Inspections nicht unerheblich angegriffen. Kritiker fürchten bei einem flächendeckenden Einsatz erhebliche Eingriffe in die Netzneutralität und eine verstärkte Zensur des Internets.[489]

---

484 *Popp*, Die strafrechtliche Verantwortlichkeit von Internet-Providern, S. 143f, m.w.N.

485 EuGH, *Scarlet/SABAM,* (Fn. 249).

486 Hierzu ausführlich *Mochalski/Schulze.*

487 Vgl. de.wikipedia.org/wiki/Deep_Packet_Inspection; ausführlich zur Methode der Deep-Packet-Inspections *Mochalski/Schulze.*

488 Zu diesem Ergebnis gelangt auch *Sieber*, in Straftaten und Strafverfolgung im Internet, der die Regelung des TMG zur Haftung der Access-Provider für die Zukunft in Frage gestellt sieht.

489 Vgl. de.wikipedia.org/wiki/Deep_Packet_Inspection, m.w.N., 14.12.14

Die bisher herrschende Meinung, die immer auf die Tatsache abstellte, dass es dem Access-Provider technisch nicht möglich ist, geeignete Kontrollmaßnahmen zu ergreifen, ist daher von den heutigen technischen Möglichkeiten überholt worden. Der Access-Provider ist somit nach dem aktuellen Stand der Technik Herrscher über eine Gefahrenquelle. Dies gilt zumindest soweit, als er Herrschaft über die Informationen hat, die er durchleitet. Dies ist ihm nicht zuletzt mit der Durchführung einer Deep-Packet-Inspection möglich, sodass er auch in der Lage ist, den Datenfluss zu kontrollieren.

(4) Vertrauensstellung des Access-Provider

Die Garantenstellung aus der Eröffnung einer Gefahrenquelle bedarf, wie oben aufgezeigt, zu ihrer Eingrenzung des zusätzlichen Vorliegens einer durch den Access-Provider entstandenen Vertrauensstellung sowie der sich auf dieser Vertrauensstellung gründenden Gefährdungssituation. Hier gilt das bereits oben zum Access-Provider Ausgeführte.[490] Insbesondere ist die Vertrauensstellung aufgrund der Eröffnung einer Gefahrenquelle als noch stärker einzustufen als diejenige, die aufgrund eines Gesetzes entsteht, da der Access-Provider derjenige ist, der auch eine Kontrolle über die von ihm eröffnete Gefahrenquelle hat.

(5) Ergebnis

Damit kann an dieser Stelle festgehalten werden, dass für den Access-Provider zumindest vor dem heutigen Stand der technischen Entwicklung eine Garantenstellung aufgrund Herrschaft über eine Gefahrenquelle bejaht werden muss. Das Internet ist mittlerweile aufgrund vielerlei Aspekte als Gefahrenquelle anzusehen und wird aufgrund der dortigen laxen Handhabe der Behörden und der schweren Verfolgbarkeit von Straftaten teilweise sogar als rechtsfreier Raum betrachtet. Der Access-Provider, der die Gefahrenquelle Internet eröffnet, indem er den Zugang dazu vermittelt und aufrecht erhält, ist technisch dazu in der Lage, die Informationen zu filtern und dadurch zumindest zu blockieren. Ebenso wird in ihn ein ausreichendes Vertrauen auf sein Handeln zumindest dann zu setzen sein, wenn er von den inkriminierten Inhalten Kenntnis erlangt hat.

---

[490] Vgl. oben S. 122.

bb) Garantenstellung des Access-Providers aus Ingerenz

Unter den denkbaren Garantenstellungen des Access-Providers ist auch die Möglichkeit der Entstehung einer Garantenpflicht aus Ingerenz in Betracht zu ziehen. Wie bereits oben ausgeführt ist für eine aus Ingerenz entstehende Garantenpflicht ein objektiv pflichtwidriges Vorverhalten des Access-Providers notwendig. Denkbar wäre z.B. die Eröffnung des Internetzugangs oder das nicht Vorhalten entsprechender Sicherheitsstandard, die rechtswidrige Inhalte auf Seiten des Access-Providers herausfiltern.

Dies ist für die Tätigkeit des Access-Providers jedoch abzulehnen. Zwar bewirkt die eigentliche Tätigkeit des Access-Providers, das Zugänglich-Machen und Aufrecht-Erhalten, dass die geforderte Gefahrerhöhung entsteht[491]. Wie bereits soeben ausgeführt, stellt das Internet eine Quelle dar, aus der sich für den Nutzer der Leistung des Access-Providers mannigfaltige Gefahren ergeben. Es fehlt jedoch für die Garantenstellung aus Ingerenz an der objektiven Pflichtwidrigkeit des Vorverhaltens des Access-Providers. Das Eröffnen der Internetverbindung ist grundsätzlich ein gesellschaftlich erwünschter Vorgang,[492] der ein sozialadäquates[493] Handeln darstellt.

Zudem ist diese Tätigkeit ein Ausfluss eines berufsbedingten Verhaltens des Access-Providers. Strafrechtliche Würdigung erfährt ein berufsbedingtes Verhalten überwiegend dann, wenn es auf der Ebene der Unterstützung fremder Straftaten durch eben dieses berufsbedingte Verhalten zu überprüfen ist. Mit der h.M. ist für den Access-Provider im Rahmen eines objektiv pflichtwidrigen Vorverhaltens kein strafbares Verhalten anzunehmen.[494] Eine Garantenstellung aus Ingerenz ist daher für den Access-Provider abzulehnen. Dessen Tätigkeit ist heute gesellschaftlich gewollt und aus vielen Bereichen des Lebens nicht mehr wegzudenken, sodass ein objektiv pflichtwidriges Vorverhalten auszuschließen ist.

c) Garantenstellung aus einer Sperrverfügung

Des Weiteren kann sich eine Garantenstellung des Access-Providers auch aus einer behördlichen Sperrverfügung ergeben.[495]

---

491 *Fischer*, § 13, Rn. 48.

492 *Frey/Rudolph*, Rn. 392; *Kessler*, Zur strafrechtlichen Verantwortlichkeit von Zugangsvermittlern, S. 72, m.w.N.

493 *Satzger*, Strafrechtliche Providerhaftung, S. 171, m.w.N.

494 Hierzu siehe auch ausführlich *Kudlich*, Die Unterstützung fremder Straftaten durch berufsbedingtes Verhalten, S. 505.

495 *Hilgendorf/Valerius*, Rn. 220.

Die zuständige Behörde erlässt durch die Sperrverfügung ein Handlungsgebot. Handelt der Access-Provider nicht entsprechend, d.h. richtet er keine Internetsperre bzgl. derjenigen Seiten ein, die von der Anordnung der Behörde betroffen sind, so stellt sein Unterlassen eine strafbare Handlung dar. Der Access-Provider erhält durch die Sperrverfügung eine hervorgehobene Stellung als Mittel zur Bekämpfung von Straftaten und erfährt dadurch einen Vertrauensvorschuss – wenn auch nicht ganz freiwillig –, der zu der für die Garantenstellung notwendigen Vertrauensstellung führt, sodass dies auch eine Garantenpflicht nach sich zieht. Nachdem behördliche Sperrverfügungen jedoch nur selten rechtswirksam erlassen werden, sollen im Anschließenden kurz deren Voraussetzungen und Probleme skizziert werden.

aa) Rechtsgrundlage

Die Rechtsgrundlagen behördlicher Sperrverfügungen sind heute im JMStV und RStV angesiedelt. Überwiegend ergeben sich diese aus § 20 Abs. 4 JMStV i.V.m. § 59 Abs. 3 und 4 RStV. Eine Sperrverfügung ist nach dieser Rechtsgrundlage dann zulässig, wenn jugendgefährdende Inhalte i.S. der §§ 4 und 5 JMStV[496] vorliegen. Nachdem die Kataloge dieser Vorschriften äußerst umfangreich sind und damit beinahe sämtliche strafbaren Tatbestände aus dem StGB umfassen, bedarf es meist keiner Heranziehung anderer Rechtsgrundlagen.[497] Zuständig für die Einhaltung der Bestimmungen des JMStV ist die Kommission für Jugendschutz der Landesmedienanstalten. Diese prüft und bewertet die Inhalte auf ihre Rechtswidrigkeit und beschließt entsprechende Maßnahmen. Aber auch Fallgestaltungen, in denen die Vorschriften des Jugendschutzes i.S.v. § 20 Abs. 4 JMStV keine Rechtsgrundlage darstellen, sind in Betracht zu ziehen und benötigen eine Rechtsgrundlage. Als von der Politik geschaffenes Werkzeug sollte das 2009 verkündete Zugangserschwerungsgesetz[498] den Erlass oder die Durchsetzung von Internetsperren erleichtern. Aufgrund eines Erlasses der Bundesregierung wurde die Möglichkeit, Internetsperren zu erlassen von vornherein auf Eis gelegt. 2011 wurde das umstrittene Gesetz wieder aufgehoben.

Die Rechtsgrundlage für eine Sperrverfügung außerhalb des JMStV war vor der Aufhebung der Differenzierung zwischen Tele- und Mediendiensten § 22 Abs. 3 MDStV. Des Weiteren wurde auch vielfach die polizeirechtlichen Generalklausel als Rechtsgrundlage diskutiert. Nachdem heute einheitlich unter den Begriff der Tele-

---

496 Zu §§ 4 und 5 JMStV s.o.

497 *Sieber*/*Nolde*, S. 93 f.

498 Gesetz zur Erschwerung des Zugangs zu Kinderpornographie in Kommunikationsnetzen vom 17.02.2010, BGBl. I 78.

medien subsumiert wird, ist nun für alle Verstöße außerhalb der Anwendbarkeit des JMStV einheitlich § 59 RStV i.V.m. § 54 Abs. 1 RStV als Rechtsgrundlage heranzuziehen.[499] Zuständig für den Erlass einer etwaigen Sperrverfügung ist in diesem Falle gem. § 59 Abs. 2 RStV eine nach Landesrecht zu bestimmende Behörde.

bb) Subsidiarität der Sperrverfügung bei fremden Inhalten

Die Anordnung von Sperrmaßnahmen gegen Diensteanbieter fremder Inhalte ist lediglich ein subsidiäres Mittel der Behörden. Dies ergibt sich unmittelbar aus § 59 Abs. 4 RStV, der ein Tätigwerden der zuständigen Behörde gegenüber den Diensteanbietern fremder Inhalte nur dann zulässt, sofern Maßnahmen gegenüber Diensteanbietern eigener Inhalte nicht durchführbar oder nicht erfolgversprechend sind. Diese Begriffe verkörpern das an dieser Stelle vom Gesetzgeber statuierte „ultima ratio"-Prinzip des Strafrechts.[500] Erst wenn hinsichtlich der Diensteanbieter eigener Inhalte die Eingriffs- bzw. Zugriffsmöglichkeiten erschöpft sind, sollen auch gegen Diensteanbieter fremder Inhalte Sperrverfügungen möglich sein.

Nachdem ein Einwirken auf die Gruppe der Diensteanbieter eigener Inhalte, also der Content-Provider, aufgrund der unbeschränkten Möglichkeiten, von überall in der Welt aus Inhalte einzuspeisen, meist äußerst schwierig ist und für die deutschen Behörden auch territoriale Grenzen in Sachen Rechtsdurchsetzung schwer überwindbar sind, ist ein Einwirken auf den lokalen Access-Provider meist ein willkommenes Mittel. Die Nichtdurchführbarkeit einer Maßnahme gegen den Diensteanbieter eigener rechtswidrige Inhalte im Internet kann und wird insbesondere darin begründet sein, dass der Content-Provider entweder anonym ist oder der deutschen Gerichtsbarkeit durch seine Exterritorialität entzogen ist. Bei der Beantwortung der Frage, ob eine konkrete Maßnahme erfolgversprechend ist, kommt der zuständigen Behörde einen Einschätzungsspielraum zu. Zum Verneinen der Erfolgsversprechendheit einer Maßnahme ausreichend ist eine negative Prognose hinsichtlich der Eingriffsmöglichkeit – auch in Bezug auf die Möglichkeiten in einem Drittland.[501]

cc) Verhältnismäßigkeit der Sperrverfügung

Die Sperrverfügung muss auch verhältnismäßig sein. Dies ist eine weitere Folge dessen, dass die Sperrverfügung aufgrund ihrer Subsidiarität grundsätzlich nur als

499 *Sieber*/*Nolde*, S. 94.
500 *Sieber*/*Nolde*, S. VI, Rn. 2.
501 *Sieber*/*Nolde*, S. 153 f.

ultima ratio eingesetzt werden soll, nicht nur aus dem „ultima ratio"-Gedanken, sondern auch schon aus § 59 Abs. 3 S. 3 RStV selbst. Die Verhältnismäßigkeit der Sperrverfügung setzt voraus, dass diese geeignet, erforderlich und angemessen ist. Ob die Sperrverfügung ein geeignetes Mittel darstellt, ist umstritten, nachdem sich – wie bereits dargestellt – vielfältige Umgehungsmöglichkeiten auftun.[502]

Die Geeignetheit wird zwar grundsätzlich für jede Art der Internetsperre von der h.M. bejaht, da zumindest für den durchschnittlichen, normalen Internetnutzer das Umgehen von Sperrmaßnahmen grundsätzlich nicht möglich ist, sollte er nicht eine tiefergehende Beschäftigung mit den Umgehungsmöglichkeiten auf sich nehmen wollen.[503] Damit ist das Kriterium der Zweckförderlichkeit der Sperrmaßnahmen erfüllt, was für die Annahme der Geeignetheit der Maßnahme ausreichend ist.

Ebenso sind behördliche Sperrverfügungen auch erforderlich, da ein milderes Mittel gleicher Wirksamkeit ausscheidet. Meist kommen alternative, weniger belastende Maßnahmen nicht in Betracht, da gerade der Access-Provider vor Ort greifbar ist, nachdem Host- und Content-Provider entweder gleich aus der Anonymität heraus oder nicht selten vom Ausland aus agieren.[504] Für eine grundsätzlich angelegte Überprüfung sorgt auch die gesetzlich angeordnete Subsidiarität dieser Maßnahme gegenüber Access-Providern gem. § 59 Abs. 4 RStV und das bereits angesprochene „ultima ratio"-Prinzip.

Die meisten behördlichen Sperrverfügungen scheitern jedoch daran, dass diese nicht angemessen, d.h. verhältnismäßig im engeren Sinne sind. Eine Sperrverfügung greift schwerwiegend in die Grundrechte des Access-Providers ein, was zu einer strengen Handhabe innerhalb der gerichtlichen Kontrolle geführt hat. Im Anschluss sollen kurz die wichtigsten Grundrechte den Access-Provider betreffend angeführt werden.

(1) Gleichheitssatz, Art. 3 GG

Der allgemeine Gleichheitsgrundsatz, der erfordert, wesentlich Gleiches nicht ungleich zu behandeln[505], kann bezogen auf Access-Provider auf unterschiedliche Arten verletzt werden.

---

502 Vgl. hierzu ausführlich *Sieber*/*Nolde*, S. 180 ff.

503 *Peifer*/*Dörre*, S. 209, m.w.N.; *Sieber*/*Nolde*, S. 193 ff.

504 Vgl. zu den unterschiedlichen ebenfalls in Betracht kommenden *milderen Mitteln* und deren Wirksamkeit ausführlich *Sieber*/*Nolde*, S. 196 ff.

505 BVerfGE 49, 148, 165.

Da jeder Access-Provider den Zugang zum Internet eröffnet, muss bei im Internet abrufbaren rechtswidrigen Inhalten grundsätzlich jeder Access-Provider gleichermaßen herangezogen werden, nachdem diese den Zugang grundsätzlich unbeschränkt eröffnen. Ergeht eine Sperrverfügung, so muss diese gegen sämtliche im Hoheitsgebiet der erlassenden Behörde ansässigen Access-Provider gerichtet werden, d.h. soweit der Zuständigkeitsbereich der erlassenden Behörde reicht. Nur soweit geht auch ihre Möglichkeit, den Gleichheitssatz zu beachten. Nicht ausreichend für die Beachtung des Gleichheitssatzes ist in diesem Zusammenhang der Erlass einer Sperrverfügung gegenüber lediglich zwei Access-Providern im Hoheitsgebiet, auch wenn diese mehr als 50 Prozent des Marktes beherrschen.[506]

Andererseits kann sich ein Verstoß gegen den Gleichheitssatz auch dann ergeben, wenn alle Access-Provider gleichermaßen in Anspruch genommen werden. Hier kann eine Ungleichbehandlung daraus resultieren, dass die vorzunehmenden Sperrmaßnahmen zu einer faktischen Ungleichbehandlung führen, indem diese Maßnahmen die Access-Provider ungleich treffen, z.B. einige Access-Provider finanziell über Gebühr belasten.[507] Es besteht dann die Möglichkeit, dass es sich bei allen herangezogenen Access-Providern von vornherein nicht um Gleiches handelte oder ein Rechtfertigungsgrund in Form eines anderen Grundrechtes, wie die Berufsausübungsfreiheit oder das Recht am eingerichteten und ausgeübten Gewerbebetrieb, bestehen.

(2) Meinungsäußerungs-, Presse- und Wissenschaftsfreiheit, Art. 5 GG

Ebenfalls im Rahmen der Prüfung der Angemessenheit einer Sperrverfügung gegen Access-Provider heranzuziehen sind die in Art. 5 GG niedergelegten Grundrechte. Der Schutzbereich der Meinungsäußerungsfreiheit gem. Art. 5 Abs. 1 S. 1 Alt. 1 GG ist für den Access-Provider jedoch nicht eröffnet. Er ist kein Inhaltsanbieter, sondern lediglich auf die Durchleitung fremder Inhalte beschränkt. Ein Kundtun von Äußerungen und Meinungen, gleich einem Content-Provider, liegt im Falle des Access-Providers nicht vor, da in der Zugangseröffnung oder der Durchleitung nicht die Kundgabe oder Unterstützung einer Meinung zu sehen ist.[508]

Auch bezüglich der Freiheit der Presse gem. Art. 5 Abs. 1 S. 2 Alt. 1 GG kommt eine Eröffnung des Schutzbereiches für den Access-Provider als Transporteur fremder Inhalte aus vorgenannten Gründen grundsätzlich nicht in Betracht. Zwar erwei-

---

506 VG Düsseldorf, CR 2012, 155, 158.

507 *Sieber*/*Nolde*, S. 66, m.w.N.

508 *Spindler/Volkmann*, K&R 2002, 398, 406; *Sieber*/*Nolde*, S. 66f, m.w.N.

tert das BVerfG den Schutzbereich dahingehend, dass auch inhaltsferne Hilfsfunktionen vom Grundrechtsschutz miteingeschlossen sein sollen.[509] Diese umfassen insbesondere Meinungsverbreitung und -beschaffung. Gefordert wird jedoch ein organisatorischer Verbund mit einem Presseunternehmen als Grundrechtsträger. Ein solcher ist für den Access-Provider nicht anzunehmen. Nachdem der Pressemarkt gerade für Printerzeugnisse immer mehr rückläufig ist, muss die Presse ihre Online-Präsenz ausbauen. Dies bedingt natürlich auch eine verstärkte Inanspruchnahme der Dienste von Access-Providern, es führt aber nicht gleichzeitig zu der vom BVerfG geforderten Organisationseinheit. Die Einbeziehung von Access-Providern in den Schutzbereich des Grundrechtes der Pressefreiheit wäre daher zu weitgehend und ist abzulehnen.[510]

Die Wissenschaftsfreiheit, die Art. 5 Abs. 3 GG gewährleistet, umfasst den freien Zugang zu originalen Quellen, um mit diesen zu arbeiten. Ein Beispiel hierfür stellt die Erforschung und Bearbeitung neuer nationalsozialistischer Quellen über das Internet dar. Als Access-Provider und Grundrechtsträger muss dann die wissenschaftliche Forschungseinrichtung, d.h. i.d.R. die Universität, herangezogen werden. Lässt man die Frage der Einstufung als Access-Provider einmal außer Betracht, liegt in einer umfassenden Sperrverfügung gewiss eine nicht unerhebliche Beeinträchtigung dieses Grundrechtes, welches ansonsten nur verfassungsimmanente Schranken kennt.

Die Universitäten und Forschungseinrichtungen müssen daher von einer Sperrverfügung ausgenommen werden. Eine Möglichkeit bestünde darin, auf die Schutzrichtung der Sperrverfügung abzustellen. Soll durch diese z.B. dem Schutz der Jugend Rechnung getragen werden, so richtet sich diese nicht gegen Universitäten, da sich deren Zugangsvermittlung grundsätzlich nur an Studenten und Mitarbeiter und daher Volljährige richte.[511] Dieser Ansatz ist durch die deutschlandweite Einführung des achtjährigen Gymnasiums mittlerweile nicht mehr haltbar. Weite Teile der Studienanfänger sind –aufgrund dessen und zusätzlich durch die Aussetzung der Wehrpflicht – nicht volljährig sondern minderjährig, was den Jugendschutz an dieser Stelle nicht obsolet werden lässt.

Diese Handhabe war äußerst praktisch, da als Rechtsgrundlage – wie bereits erläutert – in den überwiegenden Fällen die Vorschriften aus dem JMStV heranzuziehen sind, nachdem die Kataloge der jugendgefährdenden Inhalte der §§ 4 und 5 JMStV beinahe sämtliche in Betracht kommenden Straftatbestände umfassen. Die For-

---

509 BVerfGE 10, 118, 121.

510 Vgl. auch *Sieber*/*Nolde*, S. 67 ff.

511 *Sieber*/*Nolde*, S. 70.

schungseinrichtungen wären dann in den überwiegenden Fällen auch von der Sperrverfügung ausgenommen gewesen.

Es wird jedoch außer Acht gelassen, dass Sperrverfügungen immer auch dem Jugendschutz dienen, aber die Schutzrichtung, die sich aus der Intention des Erlassenden ergibt, meist auch eine andere ist. Im Vordergrund steht nicht der Schutz der Jugend, sondern in erster Linie die Strafverfolgung. Aus diesem Gesichtspunkt heraus scheint es nicht angebracht, bei einer Ausnahme für Forschungseinrichtungen lediglich auf das Alter der potentiellen Mitarbeiter und Studierenden abzustellen. Die Frage, ob es sinnvoll ist, als Anspruchsgrundlage einer Sperrverfügung und der sich daraus ergebenden Folgen immer auf den JMStV zurückzugreifen, auch wenn die Schutzrichtung eine andere ist, soll jedoch hier nicht vertieft werden. Es ist Aufgabe des Gesetzgebers, entsprechende Rechtsgrundlagen zu schaffen. Dies gilt umso mehr, da der Ansatzpunkt über die Altersgruppe der Studierenden wir aufgezeigt nicht mehr weiterverfolgt werden kann.

(3) Berufsausübungsfreiheit, Art. 12 GG

Weiter kommt innerhalb der Verhältnismäßigkeitsprüfung auch Art. 12 GG mit seiner darin statuierten Berufsfreiheit als entgegenstehendes Grundrecht in Betracht. Es ist nicht unumstritten, ob mittels einer Sperrverfügung ein Eingriff nicht nur in die Berufsausübungsfreiheit, sondern ebenso in die Berufswahlfreiheit vorliegt, der dann nur unter äußerst engen Grenzen zulässig wäre.[512] Grundsätzlich ist der Schutzbereich des Art. 12 GG eröffnet, nachdem der Access-Provider durch die ihm auferlegte Sperrverfügung technische Maßnahmen ergreifen muss, um eine bestmögliche Nichterreichbarkeit der gesperrten Webadresse herbeizuführen. Diese Maßnahmen können finanzielle Auswirkungen nach sich ziehen, sei es als Aufwendungen für die zur Durchführung der Sperrung notwendigen Maßnahmen oder als finanzielle Gewinneinbuße in Folge derselben.

(4) Eigentumsfreiheit, Art. 14 GG

Zu guter Letzt kommt auch ein Eingriff in die Freiheit des Eigentums in Betracht. Hier stellt sich bereits bei der Eröffnung des Schutzbereiches die Frage, ob dieses Grundrecht neben dem der Berufsausübungsfreiheit eröffnet sein kann und in welchem Verhältnis diese Grundrechte zueinander stehen. Maßgebend für die Abgrenzung ist grundsätzlich, ob das bereits Erworbene eingesetzt werden muss (dann Ei-

[512] Siehe ausführlich zur Frage der Intensität des Eingriffes, *Sieber*/*Nolde*, S. 61 ff.

gentumsfreiheit) oder es um den Erwerbsvorgang an sich geht (dann Berufsausübungsfreiheit).[513] Nimmt man nun die Tätigkeit des Access-Providers, so ist grundsätzlich beides in Erwägung zu ziehen. Die h.M. bejaht die Eröffnung des Schutzbereiches[514] und gelangt darüber zu einem Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb, sodass auch Art. 14 GG im Rahmen der Verhältnismäßigkeitsprüfung beachtet werden muss.

dd) Zusammenfassung

Eine behördliche Sperrverfügung kann zu einer Garantenstellung des Access-Providers führen. Eine Sperrverfügung muss jedoch vor ihrem Erlass einer umfangreichen Grundrechtsprüfung unterzogen werden, nachdem durch sie in eine Vielzahl von Grundrechten eingegriffen wird. Zudem erscheint es auch ratsam, einige Grundrechtsträger von den Wirkungen der Sperrverfügung freizustellen. Der Erlass einer Sperrverfügung bleibt daher ein probates Mittel zur Bekämpfung von Straftaten, jedoch mit vielen Angriffspunkten und der immerwährenden Frage ihrer Sinnhaftigkeit.

4. Ergebnis zur Garantenstellung

Der Access-Provider kann eine Garantenstellung innehaben. Wie soeben dargelegt, kann er sowohl als Beschützer- als auch als Überwachergarant gehalten sein, notwendige Maßnahmen zu ergreifen, um die Verwirklichung eines Straftatbestandes zu verhindern. In Betracht kommen die Garantenstellungen aus Gesetz – hier insbesondere aus dem JMStV – oder aus einer vertraglichen Übernahme von Schutzpflichten. Hinzu kommen Garantenstellungen aus der Eröffnung einer Gefahrenquelle – in diesem Fall zumindest bei Kenntnis des Access-Providers von der tatsächlichen Durchleitung rechtswidriger Inhalte – und aus einer bestehenden Sperrverfügung.

V. Kenntnis und Vorsatz

Liegen die Voraussetzungen des objektiven Tatbestandes vor und ist insbesondere eine Garantenstellung des Access-Providers zu bejahen, so müssen für eine Strafbarkeit auch die subjektiven Tatbestandsvoraussetzungen vorliegen. Das vorsätzliche

---

513 BVerfGE 88, 366, 377.

514 *Schmidt-Preuß*, Die verfassungsrechtlichen Anforderungen an die Entschädigung für Leistungen der Telekommunikationsüberwachung, S.7 f.

Unterlassen besteht darin, dass der Täter – hier der Access-Provider – sich bei der Wahl zwischen Untätigbleiben und möglichem Handeln für das Nichtstun entscheidet.[515]

Das bedeutet für den Access-Provider zunächst, dass er überhaupt Kenntnis von den inkriminierten Inhalten haben muss. Nachdem eine Pflicht zum proaktiven Überwachen des Datenflusses entsprechend § 7 Abs. 2 S. 1 TMG nicht angeordnet wird und nach der *Scarlet/SABAM* Entscheidung des EuGH[516] auch nicht geboten ist, stellt sich zunächst die Frage, wie der Access-Provider zu der Kenntnis gelangen soll, dass er inkriminierte Inhalte durchleitet. Da der Access-Provider selbst nichts unternehmen muss, um den Datenfluss zu kontrollieren, bedarf es jeweils eines Hinweises von Dritten. Diese Aufgabe übernimmt teilweise die KJM[517], die die Provider regelmäßig auf das Vorliegen von rechtswidrigen Inhalten hinweist. Die KJM prüft die Inhalte in Fernsehen und Internet anhand des JMStV. Da dieser bereits einen umfassenden Katalog an inkriminierten Inhalten enthält, ist ihre Prüfung daher relativ umfassend. Jedoch bedarf es auch für die Fälle, in denen der JMStV keine Katalogtat enthält, einer warnenden, zumindest hinweisenden Einrichtung. Grundsätzlich läge es nahe, die Kompetenzen der KJM dahingehend zu erweitern und dort mehr Mittel für entsprechende Ressourcen zur Verfügung zu stellen.

Hat der Access-Provider davon Kenntnis erlangt, dass rechtswidrige Inhalte von einem seiner Access-Points durchgeleitet werden, so muss beim Access-Provider hinsichtlich seiner Strafbarkeit auch einen Unterlassungsvorsatz feststellbar sein. Der Unterlassungsvorsatz muss in Bezug auf alle objektiven Tatbestandsmerkmale bestehen sowie auf sämtliche die Garantenstellung begründenden Umstände. Notwendig ist der Wille zum Untätigbleiben und das Bewusstsein, dass eine Erfolgsabwendung möglich wäre. Für den Unterlassungsvorsatz ist auch dolus eventualis ausreichend.[518]

Es genügt für eine Strafbarkeit des Access-Providers also, wenn er die Unterstützung einer Straftat, von der er in Kenntnis gesetzt wurde, billigend in Kauf nimmt. Wird er z.B. von der KJM auf die inkriminierten Inhalte hingewiesen, so hat er auch davon Kenntnis, dass diese an dem Katalog des JMStV gemessen wurden und für ihn eine Garantenstellung aus Gesetz in Betracht kommt. Unternimmt er keine Handlung, um diesen Transport inkriminierter Inhalte zu unterbinden, und ist es ihm gleichgültig, dass dann Strafgesetze verletzt werden, so kann von einem billigenden

---

515 BGHSt 19, 295, 299; 46, 373, 379.

516 EuGH, *Scarlet/SABAM,* (s.a. Fn. 249).

517 Die Kommission für Jugendmedienschutz der Landesmedienanstalten ist die zentrale Aufsichtsstelle für den Jugendschutz im privaten bundesweiten Fernsehen sowie im Internet. Ihre Aufgabe ist es, für die Einhaltung der Jugendschutzbestimmungen zu sorgen und im Rahmen der regulierten Selbstregulierung die Selbstverantwortung der Anbieter zu fördern.

518 *Wessels/Beulke*, Rn. 732, m.w.N.

In-Kauf-Nehmen und damit vom Vorliegen eines dolus eventualis ausgegangen werden. Der Access-Provider handelt damit vorsätzlich, sodass eine Haftbarmachung desselbigen in Betracht kommt.

VI. Gesamtergebnis zur strafrechtlichen Haftung des Access-Providers

Wie soeben erläutert, ist eine strafrechtliche Haftung des Access-Providers nach den allgemeinen Gesetzen und damit insbesondere nach dem Strafgesetzbuch möglich. Unterlässt der Access-Provider eine zumutbare Handlung und hat er eine Garantenstellung inne, so ist er nicht mehr gem. § 8 Abs. 1 TMG privilegiert, sondern er haftet gem. § 7 Abs. 2 S. 2 TMG nach den allgemeinen Gesetzen.

Kapitel 3: Spezielle Haftungsregelungen in Europa

Nachdem nun ein Überblick über die deutschen Haftungsfragen hinsichtlich der verschiedenen Internetprovider mit besonderem Augenmerk auf die Person des Access-Providers gegeben wurde und die Schlussfolgerung zu ziehen ist, dass diese auch über ihre Privilegierung durch § 8 TMG hinaus im Falle eines vorsätzlichen Unterlassens nach den allgemeinen Strafvorschriften gem. § 7 Abs. 2 S. 2 TMG haften, soll auf einzelne Haftungsregime in anderen EU-Mitgliedsstaaten eingegangen werden. Behandelt wird die Rechtslage in Spanien und Frankreich – Länder, die jeweils spezielle Regelungen zur Verfolgung von Straftaten im Internet, insbesondere denjenigen auf dem Gebiet des Urheberrechts, erlassen haben.

I. Spanien

In Spanien ist im Jahre 2011 die Ley 2/2011, de 4 de marzo, de Economía Sostenible (LES), die „Ley Sinde“, verabschiedet. Sie trat zum 01.03.2012 in Kraft und sollte als Anti-Piracy-Gesetz die in Spanien sehr hohe Zahl von Urheberrechtsverletzungen eindämmen.[519] Benannt wurde das Gesetz nach der damaligen Ministerin für Kultur Ángeles González Sinde.[520] Das immer noch sehr umstrittene Gesetz, welches die Rechte der Urheber besser schützen sollte, wurde angeblich auf Druck

[519] Vgl. http://es.wikipedia.org/wiki/Ley_Sinde (12.12.2014).

[520] Nachdem Frau Ángeles González Sinde zum Zeitpunkt des In-Kraft-Tretens nicht mehr im Amt war, wird es teilweise unter einem Doppelnamen aus ihrem und dem ihres Nachfolgers José Ignacio Wert auch das Ley Sinde Wert genannt.

der USA erlassen, nachdem sich Spanien auf der schwarzen Liste der Länder mit einer hohen Anzahl an Urheberrechtsverletzungen weit vorne befand.[521]

Bereits die Zielrichtung der spanischen Ley Sinde birgt Zündstoff. Mit diesem Gesetz soll in erster Linie nicht gegen private Nutzer vorgegangen werden, das Gesetz richtet sich vielmehr auch gegen Internet-Provider selbst. Der spanische Minister für Kultur José Ignacio Wert sieht eine wirksame Strategie zur Bekämpfung von Urheberrechtsverstößen darin, gegen diejenigen vorzugehen, die es den Nutzern erst ermöglichen, über ihre Infrastruktur Urheberrechtsverstöße zu begehen.[522]

1. Ley Sinde

Das Verfahren des Ley Sinde zur Sperrung von Websiten oder Entfernung von illegalen Inhalten ist in Art. 19 ff. des LES[523] geregelt. Es handelt sich um ein sehr gestrafftes Verfahren, mit dem ein schnelles Handeln durch die Behörden gewährleistet werden soll. Nicht richtig ist jedoch die pauschale Aussage, innerhalb von 72 Stunden sei es möglich[524], eine Website zu sperren.

Zuständig für die Sperrung ist die Sección Segunda der Kommission für Urheberrecht. Diese setzt sich zusammen zu 25% aus Repräsentanten aus dem Kultusministerium, ebenfalls zu 25% aus Vertretern der Verwertungsindustrie und zu 50% aus Vertretern der Verwertungsgesellschaften. Wird ein Antrag zur Durchführung eines Prüfungsverfahrens durch einen potentiell Betroffenen gem. Art. 19 LES gestellt, wird der Antrag dem entsprechenden Provider von der Sección Segunda zugeleitet.

Dieser erhält dann die Möglichkeit, innerhalb von 48 Stunden die inkriminierten Inhalte zu sperren oder zu beseitigen oder aber den Beweis zu erbringen, dass eine Urheberrechtsverletzung nicht vorliegt, Art. 20 Nr. 1 LES. Kommt der Provider diesem Verlangen nach und entfernt die Inhalte oder sperrt den Zugang, so wird angenommen, dass tatsächlich ein Verstoß bestand. Dies wird dann aktenkundig gemacht, das restliche Verfahren jedoch eingestellt, Art. 20 Nr. 2 LES. Kommt der Provider dem Ersuchen im Antrag jedoch nicht nach, so prüft ein Ermittlungsrichter gem. Art. 21 LES innerhalb von zwei weiteren Tagen, wie weiter verfahren werden soll.

---

521 Vgl. online unter: http://flaschenpost.piratenpartei.de/2012/07/20/spaniens-ley-sinde-der-feuchte-traum-der-verwertungsindustrie/ (07.01.2014); http://derstandard.at/1341526783247/Druck-aus-den-USA-Spanien-sperrt-erste-Downloadseiten (07.01.2014).

522 Vgl. online unter: http://www.musikmarkt.de/Aktuell/News/Spanien-implementiert-umstrittenes-Anti-Piraterie-Gesetz (07.01.2014).

523 Vgl. http://www.boe.es/boe/dias/2011/12/31/pdfs/BOE-A-201–20652.pdf (07.01.2014).

524 Vgl. http://flaschenpost.piratenpartei.de/2012/07/20/spaniens-ley-sinde-der-feuchte-traum-der-verwertungsindustrie/ (07.01.2014).

Kommt er zu dem Ergebnis, dass es eines gerichtlichen Handelns bedarf, so stehen ihm weitere 3 Tage zu, um eine entsprechende Verfügung zu erlassen.

Sind diese insgesamt maximal 5 Tage vorbei, muss der Richter zu dem Schluss gekommen sein, ob eine Urheberrechtsverletzung vorliegt oder nicht. Dies teilt er sodann dem Provider sowie dem Antragsteller mit, Art. 22 Nr. 1 LES, und erlässt eine Verfügung zum Entfernen oder Sperren der inkriminierten Inhalte, Art. 22 Nr. 2 LES oder lehnt deren Erlass ab. Der Provider hat dann 24 Stunden Zeit, die Anordnung selbst zu vollziehen.

Kommt der Provider dem nicht nach, so wird die Angelegenheit dem Verwaltungsgericht vorgelegt, welches innerhalb von 72 Stunden eine Sperr- oder Entfernungsverfügung erlässt gem. Art. 22 Nr. 3 LES aufgrund der Anordnung des Ermittlungsrichters. Ergeht die Sperr- oder Entfernungsverfügung jedoch nicht innerhalb von 3 Monaten, dann gilt der Antrag auf Sperrung oder Beseitigung als abgelehnt, Art. 22 Nr. 4 LES. Erlässt das Verwaltungsgericht jedoch eine entsprechende Verfügung, so wird diese innerhalb von 24 Stunden vollzogen, Art. 23 LES.

2. Bilanz des Ley Sinde

Sofort nach dem Inkrafttreten des Gesetzes wurde eine Flut von Anträgen zur Löschung oder Sperrung gestellt, das Procedere schien sich zu bewähren. Bereits Anfang Juli 2012 wurden die ersten spanischen Websites gesperrt.[525] Bereits im April 2012 gab es mehr als 300 Anträge, von denen 79 auf eine Sperrung abzielten.[526]

Die anfängliche Euphorie von Rechteinhabern war jedoch nur von kurzer Dauer. Aufgrund der Vielzahl von Anträgen ist die Bearbeitungsdauer zu lang, die vorgesehene kurze Verfahrensdauer kann nicht erreicht werden[527]. Zudem zeigen Studien, dass auch im Jahre 2012 ein Schaden von über 15 Mio. Euro durch die Aktivitäten spanischer Filesharer entstanden ist. Hinzu kommt, dass Spanien auch wieder auf der Blacklist 301 der USA aufgeführt ist als eines der Länder mit den meisten Urheberrechtsverletzungen.[528]

---

525 *Matzellner, Peter*, Erste Sperraktivität auf Grundlage des Filesharing-Gesetzes „Ley Sinde“, in: Europäisches Medienrecht – der NEWSLETTER, online unter http://www.emr-sb.de/tl_files/EMR-SB/content/PDF/EMR-Newsletter/EMR_Newsletter_2012-06-07.pdf (07.01.2014).

526 Vgl. http://www.unwatched.org/EDRigram_10.7_Erste_Sperrverfuegungen_nach_dem_spanischen_Sinde-Gesetz_stehen_an (07.01.2014).

527 Vgl. http://www.pcactual.com/etiqueta/5107/ley_sinde-wert.html (07.01.2014).

528 Vgl. http://www.pcactual.com/etiqueta/5107/ley_sinde-wert.html (07.01.2014).

3. Fazit

Spanien hat versucht, die Verletzung von Urheberrechten mit einem eigens dafür geschaffen Gesetz zu bekämpfen und die Rechte der Urheber dadurch zu stärken. Dies ist jedoch nicht gelungen, nachdem auch im Jahre der Einführung des *Ley Sinde* der Schaden, der durch die Verletzung von Urheberrechten entstanden ist, beträchtlich ist. Zudem wurden zu wenige der durch das *Ley Sinde* ermöglichten Anträge zur Entfernung oder Sperrung tatsächlich erfolgreich abgeschlossen. Das von Spanien entwickelte Verfahren, das die Sperrung von Websites und Entfernung illegaler Inhalte beschleunigen sollte, hat sich in der Praxis nicht bewährt.

II. Frankreich

Bereits im Jahr 2009, d.h. einige Jahre vor dem spanischen *Ley Sinde*, wurde in Frankreich ein Gesetz zur Bekämpfung der Internet-Piraterie und zum Schutz der Inhaber von Urheberrechten erlassen. Das „Loi n°2009–669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet“[529], nach der eigens zur Umsetzung dieses Gesetzes geschaffenen Behörde „HADOPI“ benannt, trat im Juni 2009 in Kraft. Das Gesetz ordnete die Gründung der „Haute Autorité pour la diffusion des oeuvres et la protection des droits sur internet“ (HADOPI) an, einer Behörde, der Urheberrechtsverstöße im Internet gemeldet werden und die diese dann nach dem im Loi n°2009–669 du 12 juin 2009 festgeschriebenen Verfahren verfolgt.

1. Three-Strikes-and-Out

Das Verfahren der HADOPI basiert auf dem Prinzip der Sportart Baseball, bei dem der Schlagmann nach drei nicht getroffenen Schlagversuchen aus dem Spiel genommen werden muss. Über die von den Inhabern der Urheberrechte ermittelten IP-Adressen ermittelt die HADOPI bei den Access-Providern selbst bzw. mit Hilfe der Staatsanwaltschaft die Daten der Urheberrechtsverletzer.

Diese werden bei einem erstmals festgestellten Verstoß von der HADOPI per Mail darüber informiert, sog First Strike, dass eine Urheberrechtsverletzung über ihren Internetzugang registriert wurde. Wird im folgenden erneut eine weitere Urheberrechtsverletzung über denselben Internetanschluss erfasst, so wird der Verletzer erneut, diesmal per Einschreiben, sog. Second Strike, verwarnt.

---

[529] Vgl. online unter: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020735432&categorieLien=id (07.01.2014).

Wird später die IP-Adresse eines bestimmten Internetanschlusses ein drittes Mal als Ausgangspunkt einer Urheberechtsverletzung festgehalten, so kann die HADOPI den Fall an die Staatsanwaltschaft übergeben, die sodann ein vereinfachtes Gerichtsverfahren durchführen kann, sog Third Strike. Hierbei können Verwarnungen ausgesprochen, Geldstrafen verhängt, aber auch Internetsperren gegen den jeweiligen Nutzer verhängt werden.

2. Bilanz der HADOPI

Ebenso wie in Spanien, ist die Bilanz der Arbeit der HADOPI äußerst mager. Es wurden zwar über 1,2 Mio. Nutzer angeschrieben, zu Gerichtsverfahren kam es jedoch nur in drei Fällen.[530] Zum Erlass von Netzsperren kam es sogar erstmals im Juni 2013.[531] Nachdem die Arbeit der HADOPI wenig effizient war und auch nicht zu den gewünschten Ergebnissen geführt hat, dabei aber ein jährliches Budget von 12 Mio. Euro bei 60 Mitarbeitern verbraucht, hat die französische Regierung die Abwicklung der HADOPI beschlossen.[532] Das Three-Strikes Verfahren soll zwar weitergeführt werden, jedoch sollen die Websperren durch einfache Geldstrafen ersetzt und das Procedere dadurch weiter vereinfacht werden.

3. Fazit

Auch das in Frankreich eingeführte Verfahren, das von einer eigens dafür gegründeten Behörde durchgeführt wird, war grundsätzlich bislang wenig erfolgreich im Kampf gegen die Verletzung von Urheberrechten im Internet. Es lässt sich daher feststellen, dass gezielte Gesetzgebung an diese Stelle nicht effektiv ist. Jedoch wird auch in Deutschland die Schaffung eines Verfahrens auf der Grundlage des Three-Strikes-Systems diskutiert. Im Gespräch ist die Einführung eines Two-Strikes-Verfahrens, das den Internet-Nutzer bei der ersten Urheberrechtsverletzung verwarnen soll. Bei der zweiten Verletzung soll der Nutzer dann eine zivilrechtliche Abmahnung durch den Rechteinhaber erhalten.[533] *Sieber* wendet dagegen zurecht ein, dass ein solches Verfahren mit zu viel Rechtsunsicherheit verbunden wäre. Zum einen ist es fraglich, ob und wie lange die beim ersten Verstoß aufgezeichneten Daten

---

[530] Vgl. online unter: http://de.wikipedia.org/wiki/Hadopi (07.01.2014).

[531] Vgl. online unter: http://www.heise.de/newsticker/meldung/Hadopi-Behoerde-Kurz-vor-dem-Exitus-noch-die-erste-Websperre-1887955.html (07.01.2014).

[532] Vgl. online unter: http://www.heise.de/newsticker/meldung/Frankreich-rueckt-von-Netzsperren-ab-1875868.html/from/related (07.01.2014).

[533] Ausführlich hierzu *Schwartmann*, in: Vergleichende Studie über Modelle zur Versendung von Warnhinweisen durch Internetzugangsanbieter an Nutzer bei Urheberrechtsverletzungen.

der Nutzer gespeichert werden dürfen. Zum anderen ist die Ermittlung der Nutzer anhand dynamisch vergebener IP-Adressen fehlerträchtig. Hinzu kommen nicht zuletzt auch die dadurch entstehenden Eingriffe in die Persönlichkeitsrechte der Nutzer sowie die Übertragung hoheitlicher Befugnisse auf private Diensteanbieter.[534]

Es ist daher äußerst fraglich, ob es bei einer derart schwer in den Griff zu bekommenden Vielfalt von rechtlichen Ansatz- und Kritikpunkten zu einer Einführung eines ähnlichen Verfahrens in Deutschland kommen kann. *Sieber* befürwortet dies wie oben aufgezeigt nicht.[535]

[534] *Sieber*, in Straftaten und Strafverfolgung im Internet, S. C 97.
[535] *Sieber,* in Straftaten und Strafverfolgung im Internet, S. C 98.

Teil 4: Gesamtergebnis der Arbeit und Ausblick

Die Providerhaftung, die sich derzeit nach dem TMG richtet, ist ein differenziertes Haftungssystem, für welches die vorliegenden Informationen nach deren Art, eigene, fremde oder zu-eigen-gemachte qualifiziert werden müssen. Zudem richtet sich die Haftung dann an der tatsächlichen Tätigkeit des Providers nach den §§ 7–10 TMG.

In Rechtsprechung und Literatur sind die einzelnen Betätigungsfelder der Dienstanbieter bereits mehrfach Gegenstand höchstrichterlicher Rechtsprechung gewesen. Dies führt zum vorliegen einer ausreichend umfangreichen Kasuistik, die bspw. die Tatbestandsmerkmale des Zu-Eigen-machens ursprünglich fremder Informationen, durch einen Host-Provider herausdifferenziert hat. Derzeit höchstrichterlich ungeklärt bleibt allerdings die Frage, ob der Access-Provider im Rahmen eines strafrechtlichen Unterlassungsvorwurfes nicht doch über die allgemeinen Vorschriften strafbar sein kann.

Als Gesamtergebnis dieser Arbeit ist daher festzuhalten, dass eine allumfassende Haftungsprivilegierung des Access-Providers durch § 8 TMG nicht besteht. Vielmehr sprechen die besseren Argumente für eine Anwendung des § 7 Abs. 2 S. 2 TMG auch im Rahmen des Strafrechts. Hat der Access-Provider Kenntnis davon, dass rechtswidrige Informationen durch seine Leitungen transportiert werden, so kann er im Falle des Vorliegens einer Garantenstellung auch strafrechtlich haftbar gemacht werden. Es besteht daher ein probates Mittel, wie das Internet über die strafrechtliche Inanspruchnahme des Access-Providers bzw. über die Bedrohung desselben damit, sicherer werden kann. Droht dem Access-Provider die strafrechtliche Ahndung seines Untätigbleibens im Falle positiver Kenntnis, so ist zu erwarten, dass dies den Access-Provider zukünftig zum Handeln bewegen wird. Voraussetzung hierfür ist, dass die Strafverfolgungsbehörden, wie schon von *Hilgendorf* gefordert, in der Zukunft durch mutige Rechtsanwendung und Rechtsprechung die entsprechenden Signale an die Access-Provider senden.[536] Hinzu kommt, dass das Internet als Quelle des Wissens und des Fortschrittes auf seiner Kehrseite auch eine Gefahrenquelle darstellt, mittels derer Straftaten begangen werden. Damit kein rechtsfreier Raum entsteht, was durch die Neuerungen des Cloud Computing und des Web 2.0 weiter gefördert wird, ist es zudem erforderlich, dass die juristische Handhabe auch auf diejenigen Teilnehmer beim Betrieb des Internets erstreckt wird, die als Haftungsadressaten greifbar sind. Hierzu zählen letztendlich immer auch die Access-Provider, die die Infrastruktur vor Ort betreiben.

---

[536] *Hilgendorf*, K&R 2011, 229, 234.

Sieber, der Sperrverfügungen gegen Access-Provider derzeit als kein probates Mittel erachtet[537], und dem im Hinblick auf die einfache Umgehbarkeit derselbigen einerseits und die unzähligen Grundrechtseingriffe andererseits insofern grundsätzlichzuzustimmen ist, sieht als Ansatzmöglichkeit für die Zukunft nicht den Access-Provider, sondern den Hostprovider. Ausgangspunkt für *Sieber* ist hierbei die Verpflichtung des Host-Providers, bei der Kenntnis von rechtswidrigen Informationen einschreiten zu müssen, d.h. diese nach Kenntniserlangung zu löschen oder den Zugang zu ihnen zu sperren. Aufbauend auf dieser in § 10 S. 1 Nr. 1 TMG statuierten Regelung empfiehlt *Sieber* die Intensivierung der Bemühungen des Gesetzgebers dahingehend, private Vereine zu unterstützen, die rechtswidrige Informationen ermitteln und sich mit den erworbenen Erkenntnissen im Folgenden direkt an den – zunächst noch zu eruierenden – Host-Provider wenden, sodass dieser zu einem Tätigwerden gezwungen wird.[538] Wie sich bereits aus dem vorhergehenden Satz ergibt, ist auch dieses Procedere durchaus als umständlich zu bewerten. Nicht übersehen werden darf auch, dass der Host-Provider sich in vielen Fällen im Ausland befinden wird, was dazu führt, dass dieser entweder schon gar nicht ermittelt oder jedenfalls nicht hoheitlich auf diesen zugegriffen werden kann. Dies gilt im Besonderen für Cloud-Computing-Dienste.

Dieser deshalb zu kritisierende Vorschlag von *Sieber* bestärkt nichtsdestoweniger die hier vertretene – und bereits zuvor von *Hilgendorf* entwickelte – Ansicht, dass auf die Unterlassungsstrafbarkeit des räumlich und damit hoheitlich greifbaren Access-Providers nach § 7 Abs. 2 S. 2 TMG abgestellt werden muss. Die Empfehlung von *Sieber* muss derweil nicht vollständig von der Hand gewiesen werden. Das in dem Vorschlag beschriebene Vorgehen macht aber lediglich gegenüber dem Access-Provider Sinn. Hierauf könnte es übertragen werden. Bereits oben wurde im Rahmen der Vorstellung der KJM empfohlen, diese dahingehend zu sensibilisieren, auch Access-Provider ins Visier zu nehmen. Hinsichtlich der Frage, ob es eines gesetzgeberischen Gestaltungshandelns bedarf, ist mit *Sieber*[539] festzuhalten, dass es einer Erneuerung der Gesetzgebung im Hinblick auf die bestehenden Regelungen des TMG nicht dringend bedarf, würde § 7 Abs. 2 S. 2 TMG von den staatlichen Behörden in der hier vertretenen Art und Weise auf die Access-Provider angewandt.

Betrachtet man aber die tatsächliche Vorgehensweise der Strafverfolgungsorgane, die § 7 Abs. 2 S. 2 TMG auf Access-Provider unangewendet lässt, so muss mit *Hilgendorf* dennoch die Schaffung eines „differenzierenden Instrumentariums“ durch den Gesetzgeber zur besseren Kontrolle des Internets an greifbaren Ansatzpunkten

537 *Sieber*, in Straftaten und Strafverfolgung im Internet, S. C 136 ff.
538 *Sieber*, in: Straftaten und Strafverfolgung im Internet, S. C 138 f.
539 *Sieber*, a.a.O., S. C 62.

wie dem Access-Provider gefordert werden.[540] Um zu einer plastischeren Haftungsregelung für den Access-Provider zu gelangen, wäre es z.B. schon ausreichend innerhalb des § 8 TMG einen Verweis auf § 10 S. 1 Nr. 2 TMG zu schaffen. Abschließend gilt es festzuhalten, dass aber auch derzeit mit § 7 Abs. 2 S. 2 TMG ein Werkzeug besteht, welches der Gesetzgeber geschaffen hat und welches nur noch von den Strafverfolgungsbehörden richtig angewendet werden muss.

[540] *Hilgendorf*, K&R 2011, 229, 234; darüber hinaus lehnt *Hilgendorf*, JZ 2012, 825, 832 zu Recht die von *Sieber*, a.a.O., vorgeschlagene Schaffung eines Informationsstrafrechts ab.

Literaturverzeichnis

Altenhain, Karsten

Die strafrechtliche Verantwortung für die Verbreitung mißbilligter Inhalte in Computernetzen, CR 1997, 485–496.

Beck'scher Online-Kommentar zum Strafgesetzbuch

von Heintschel-Heinegg, Bernd (Hrsg.), 1. Auflage, München 2010, online unter http://beck-online.beck.de, 35. Edition (Stand: 01.11.2017) (zit.: *Bearbeiter* BeckOK-StGB).

Blanke, Isabel

Über die Verantwortlichkeit des Internet-Providers, Marburg 2006

Bleckmann, Albert

Zu den Methoden der Gesetzesauslegung in der Rechtsprechung des BVerfG, JuS 2002, 942–947.

Bleisteiner, Stephan

Rechtliche Verantwortlichkeit im Internet, München 1999.

Bornemann, Roland

Der „Verbreitensbegriff" bei Pornografie in audiovisuellen Mediendiensten. Straferweiternd im Internet und strafverkürzend im Rundfunk?, MMR 2012, 157–161.

Finke, Thorsten

Die strafrechtliche Verantwortung von Internet-Providern, Tübingen 1998.

Fischer, Thomas

Strafgesetzbuch und Nebengesetze, 62. Auflage, München 2015 (zit.: *Fischer*).

Fitzner, Julia

Fortbestehende Rechtsunsicherheit bei der Haftung von Host-Providern, MMR 2011, 83–86.

Flechsig, Norbert/Gabel, Detlev

Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks, CR 1998, 351–358.

Frey, Dieter/Rudolph, Matthias

Haftungsregimes für Host- du Access-Provider im Bereich der Telemedien, Rechtsgutachten im Auftrage des Bundesverband Digitale Medien e.V., Norderstedt 2009 (zit.: *Frey/Rudolph*).

Gercke, Marco/Brunst, Phillip
Praxishandbuch Internetstrafrecht, 1. Auflage, Stuttgart 2009 (zit.: *Gercke/-Brunst*).

Gierschmann, Sybille
Was ist eine geschlossene Benutzergruppe?, in Bosch/Leible (Hrsg.), Jugendschutz im Informationszeitalter, Jena 2012 (zit.: *Gierschmann*).

Haug, Volker
Internetrecht, 2. Auflage, Stuttgart 2010 (zit.: *Haug*).

Heckmann, Dirk
Persönlichkeitsschutz im Internet, NJW 2012, 2631–2635.

Herdegen, Matthias
Europarecht, 13. Auflage, München 2011 (zit.: *Herdegen*).

Hilgendorf, Eric
- Strafrechtliche Produzentenhaftung in der "Risikogesellschaft", Berlin 1993.
- Zur Anwendbarkeit des § 5 TDG auf das Strafrecht, NStZ 2000, 518–523.
- Ehrenkränkungen („flaming“) im Web 2.0, ZIS 2010, 208–215.
- Strafrechtliche Anforderungen an den Jugendmedienschutz im Internet, K&R 2011, 229–234.
- Strafrechtliche Anforderungen an den Jugendmedienschutz im Internet, in Bosch/Leible (Hrsg.), Jugendschutz im Informationszeitalter, Jena 2012 (zit.: *Hilgendorf*, in: Jugendschutz im Informationszeitalter).
- Die strafrechtliche Regulierung des Internet als Aufgabe eines modernen Technikrechts, JZ 2012, 825–832.

Hilgendorf, Eric/Valerius, Brian
Computer- und Internetstrafrecht, 2. Auflage, Berlin 2012 (zit.: *Hilgendorf/-Valerius*).

Hoeren, Thomas
- Anmerkung im Anschluss an: Generalbundesanwalt: Haftung eines Access Providers für rechtswidrigen Inhalt, MMR 1998, 93–98.
- Internetrecht, Münster 2013, http://www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript_Internetrecht_Oktober_2014.pdf (01.11.2017) (zit.: *Hoeren*, Internetrecht).

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.)
Handbuch Multimedia-Recht. Rechtsfragen des elektronischen Geschäftsverkehrs, Loseblattsammlung, Stand: 41. Ergänzungslieferung, München 2015 (zit. Hoeren/Sieber/Holznagel/*Bearbeiter*).

Hopf, Kristina/Braml Birgit
Virtuelle Kinderpornographie vor dem Hintergrund des Online-Spiels „Second Life“, ZUM 2007, 354–363.

Hornung, Gerrit
Die Haftung von W-LAN Betreibern, CR 2007, 88–94.

Hörnle, Tatjana
Stellungnahme für die öffentliche Anhörung im Rechtsausschuss am 13. Oktober 2014 zum Gesetzentwurf der Fraktionen der CDU/CSU und SPD: Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Umsetzung europäischer Vorgaben zum Sexualstrafrecht BT-Drucksache 18/2601; abrufbar unter https://www.bundestag.de/blob/338850/f0532cb0f8b2a123177e9f837ccd5f69/hoernle-data.pdf (01.11.2017) (zit.: *Hörnle*, Stellungnahme zum Gesetzentwurf).

Jones, Christopher/Nobis, Ralf/Röchner, Susanne/Thal, Paul
Internet der Zukunft. Ein Memorandum, Würzburg 2010, online unter: http://opus.bibliothek.uni-wuerzburg.de/volltexte/2011/5573/pdf/Internet_der_Zukunft.pdf (01.11.2017) (zit.: Jones/Nobis/Röchner/Thal/*Bearbeiter*).

Kagermann, Henning/Wahlster, Wofgang/Helbig, Johannes (Hrsg.)
Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, Frankfurt 2013, https://www.bmbf.de/files/Umsetzungsempfehlungen_Industrie4_0.pdf (01.11.2017).

Kessler, Clemens
Zur strafrechtlichen Verantwortlichkeit von Zugangsprovidern, Berlin 2003.

Kudlich, Hans
- Altes Strafrecht für Neue Medien?, Jura 2001, 305–310.
- Die Neuregelung der strafrechtlichen Verantwortung von Internet-Providern, JA 2002, 798–803.
- Die Unterstützung fremder Straftaten durch berufsbedingtes Verhalten, Berlin 2004.

Kühl, Kristian
Strafrecht. Allgemeiner Teil, 7. Auflage, München 2012 (zit.: *Kühl*).

Lackner, Karl/Kühl, Kristian
Strafgesetzbuch. Kommentar, 28. Auflage, München 2014 (zit.: *Lackner/Kühl*).

Laubenthal, Klaus
Handbuch Sexualstraftaten, Die Delikte gegen die sexuelle Selbstbestimmung, München 2012 (zit.: *Laubenthal*).

Leipziger Kommentar zum Strafgesetzbuch
Laufhütte, Heinrich Wilhelm/Rissing-van Saan, Ruth/Tiedemann, Klaus (Hrsg.), 6. Band, 12. Auflage, Berlin 2009 (zit.: *Bearbeiter* LK).

Liesching, Marc
Strafrechtliche Verantwortlichkeit für Hyperlinks, MMR 2006, 387–392.

Liesching, Marc/Günter Thomas
Verantwortlichkeit von Internet-Café-Betreibern, MMR 2000, 260–266.

Malek, Klaus/Popp, Andreas
Strafsachen im Internet, 2. Auflage, Heidelberg 2015 (zit.: *Malek/Popp*).

Marberth-Kubicki, Annette
Computer- und Internetstrafrecht, 2. Auflage, München 2010, (zit.: *Marberth-Kubicki*).

Mochalski, Klaus/Schulze, Hendrik
Deep Packet Inspection, Leipzig 2009, online unter www.ipoque.com/sites /default/mediafiles/documents/white-paper-deep-packet-inspection.pdf (30.06.2015) (zit.: *Mochalski/Schulze*).

Münchner Kommentar zum Strafgesetzbuch
Joecks, Wolfgang/Miebach, Klaus (Hrsg.), Band 3, §§ 80–184g StGB, 2. Auflage, München 2012; Band 7, Nebenstrafrecht II, München 2015 (zit.: MüKo-StGB/*Bearbeiter*).

Nomos Kommentar zum Strafgesetzbuch
Kindhäuser, Urs/Neumann, Ulfrid/Paeffgen, Hans-Ullrich (Hrsg.), 4. Auflage, Baden-Baden 2013 (zit.: *Bearbeiter* NK).

Ott, Stephan
Die Entwicklung des Suchmaschinen- und Hyperlink-Rechts im Jahr 2011, WRP 2011, 655–684.

Paul, Tobias
Primärrechtliche Regelungen zur Verantwortlichkeit von Internetprovidern aus strafrechtlicher Sicht, Baden-Baden 2005.

Paschke, Marian
Medienrecht, 3. Auflage, Heidelberg 2009 (zit.: *Paschke*).

Pelz, Christian
Die Strafbarkeit von Online-Anbietern, wistra 1999, 53–59.

Peifer, Karl-Nikolaus/Dörre, Tanja
Übungen im Medienrecht, 2. Auflage, Berlin 2011 (zit.: *Peifer/Dörre*).

Pieroth, Bodo/Schlink, Bernhard/Kingreen, Thorsten/Poscher, Ralf
Grundrechte. Staatsrecht II, 29. Auflage, Heidelberg 2013 (zit.: *Pieroth/Schlink*).

Popp, Martin
Die strafrechtliche Verantwortlichkeit von Internet-Providern, Berlin 2002.

Roxin, Claus
- Strafrecht Allgemeiner Teil, Band II, München 2003 (zit.: *Roxin* AT II).
- Täterschaft und Tatherrschaft, 8. Auflage, Berlin 2006 (zit.: *Roxin*).

Satzger, Helmut
- Strafrechtliche Verantwortlichkeit von Zugangsvermittlern, CR 2001, 109–117
- Strafrechtliche Providerhaftung, in: Heermann/Ohly (Hrsg.), Verantwortlichkeit im Netz – Wer haftet wofür?, Boorberg 2003, S. 161–180 (zit.: *Satzger*, in: Strafrechtliche Providerhaftung).

Satzger, Helmut/Schmitt, Bertram/Widmaier, Gunter
Strafgesetzbuch. Kommentar, 2. Auflage, Köln 2014 (zit.: SSW/*Bearbeiter*).

Schmidt-Preuß, Matthias
Die verfassungsrechtlichen Anforderungen an die Entschädigung für Leistungen der Telekommunikationsüberwachung und der Auskunftserteilung, online unter: http://www.sfu.ca/cprost/prepaid/relateddocs/Germany/Schmidt-PreuB_and_
German_Constitution.pdf (01.11.2017).

Schönke, Adolf/Schröder, Horst
Strafgesetzbuch. Kommentar, 29. Auflage 2014 (zit.: Schönke/Schröder/*Bearbeiter*).

Schwartmann, Rolf
Vergleichende Studie über Modelle zur Versendung von Warnhinweisen durch Internetzugangsanbieter an Nutzer bei Urheberrechtsverletzungen, 2012, online unter: https://www.bmwi.de/Redaktion/DE/Publikationen/Technologie/https://www.bmwi.de/Redaktion/DE/Publikationen/Technologie/warnhinweise.pdf?__blob=publicationFile&v=3warnhinweise.pdf?__blob=publicationFile&v=3 (01.11.2017).

Sieber, Ulrich
- Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (2), JZ 1996, 494–507.
- Anmerkungen zum AG München, MMR 1998, 438–448.
- Verantwortlichkeit im Internet, 1. Auflage, München 1999 (zit.: *Sieber*, in: Verantwortlichkeit im Internet).

– Straftaten und Strafverfolgung im Internet, in: Gutachten C zum 69. Deutschen Juristentag, München 2012 (zit.: *Sieber*, in: Straftaten und Strafverfolgung im Internet).

Sieber, Ulrich/Liesching, Marc
Die Verantwortlichkeit der Suchmaschinenbetreiber nach dem Telemediengesetz, MMR-Beilage 2007 (zit.: *Sieber/Liesching*).

Sieber, Ulrich/Nolde, Malaika
Sperrverfügungen im Internet, Berlin 2008 (zit.: *Sieber/Nolde*).

Spath, Dieter (Hrsg.)
Produktionsarbeit der Zukunft – Industrie 4.0, Studie, Stuttgart 2013.

Spindler, Gerald/Schuster, Fabian (Hrsg.)
Recht der elektronischen Medien, 2. Auflage, München 2011 (zit.: Spindler/-Schuster/*Bearbeiter*).

Spindler, Gerald/Schmitz, Peter/Geis, Ivo
Teledienstegesetz, Teledienstedatenschutzgesetz, Signaturgesetz, 1. Auflage, München 2004 (zit.: Spindler/Schmitz/Geis/*Bearbeiter)*.

Spindler, Gerald/Volkmann, Christian
Die öffentlich-rechtliche Störerhaftung der Access-Provider, K&R 2002, 398–409 (zit.: *Spindler/Volkmann*).

Systematischer Kommentar zum Strafgesetzbuch
Rudolphi, Hans-Joachim/Horn, Eckhard/Samson Erich (Hrsg.), Loseblattsammlung, Stand: 148. Ergänzungslieferung, Köln 2014, (zit.: SK-StGB/*Bearbeiter*).

Titz, Andrea
Stellungnahme des Deutschen Richterbundes zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs – Umsetzung europäischer Vorgaben zum Sexualstrafrecht sowie zum Entwurf eines Gesetzes zu dem Übereinkommen des Europarats vom 25. Oktober 2007 zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch, online unter: http://www.drb.de/?id=869 (01.11.2017) (zit.: *Titz*, Stellungnahme DRB).

Wessels, Johannes/Beulke, Werner/Satzger, Helmut
Strafrecht Allgemeiner Teil, 44. Auflage, Heidelberg 2014 (zit.: *Wessels/Beulke*).

Zippelius, Reinhold
Juristische Methodenlehre, 11. Auflage, München 2012 (zit.: *Zippelius*).

Über den Verfasser

Der Verfasser wurde am 09. Juli 1981 in Amberg in der Oberpfalz geboren, wo er im Jahre 2001 am Gregor-Mendel-Gymnasium die Allgemeine Hochschulreife erwarb. Seinen Grundwehrdienst leistete er beim 5. Gebirgstransportbatallion 83 in der Schweppermannkaserne Kümmersbruck.

Im Wintersemester 2002/03 begann er das Studium der Rechtswissenschaft an der Bayerischen Julius-Maximilians-Universität Würzburg. Von September 2004 arbeitete er für die Juristen ALUMNI Würzburg, von Juli 2005 bis zum Ende seiner Tätigkeit dort im Juni 2007 sogar als Chief Executive Officer (CEO). Sein Studium beendete der Verfasser im Februar 2007 mit der Ersten Juristischen Staatsprüfung, Prüfungstermin 2006/II. Im Anschluss hieran absolvierte er das Referendariat beim Landgericht Aschaffenburg, welches er mit dem Zweiten Juristischen Staatsexamen im Mai 2009, Prüftermin 2008/II, abschloss.

Von 2010 bis 2013 arbeitete der Verfasser als Rechtsanwalt in einer Kanzlei in Memmingen; seine Schwerpunkte bildeten hierbei die Bereiche des IT-Rechts und des privaten Bau- und Architektenrechts, währenddessen absolvierte er erfolgreich eine Fachanwaltsfortbildung für Bau- und Architektenrecht. Seit Ende 2013 widmet er sich der Unternehmensberatung auf dem Gebiet des Datenschutzrechts. Ende 2015 absolvierte er ebenso erfolgreich eine Fachanwaltsfortbildung für Arbeitsrecht. Derzeit begleitet der Verfasser seine Kunden bei der Umsetzung der Anforderungen der europäischen Datenschutz-Grundverordnung.