MALTE BAUMANN

Haftung von Domain-Registraren

Geistiges Eigentum
und Wettbewerbsrecht

Mohr Siebeck

Geistiges Eigentum und Wettbewerbsrecht

herausgegeben von
Peter Heermann, Diethelm Klippel,
Ansgar Ohly und Olaf Sosnitza

166

Malte Baumann

Haftung von Domain-Registraren

Verantwortlichkeit eines neutralen Diensteanbieters für urheberrechtsverletzende Inhalte Dritter

Mohr Siebeck

Malte Baumann, geboren 1992; Studium der Rechtswissenschaft an der Humboldt-Universität zu Berlin; 2018 erstes juristisches Staatsexamen; Wissenschaftlicher Mitarbeiter im Bereich Technologie, Medien und Telekommunikation; 2020 Promotion (Halle-Wittenberg); seit 2020 Rechtsreferendariat am Kammergericht Berlin.

ISBN 978-3-16-160668-7 / eISBN 978-3-16-160669-4
DOI 10.1628/978-3-16-160669-4

ISSN 1860-7306 / eISSN 2569-3956 (Geistiges Eigentum und Wettbewerbsrecht)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über *http://dnb.dnb.de* abrufbar.

Das Buch wurde von Laupp und Göbel in Gomaringen auf alterungsbeständiges Werkdruckpapier gedruckt und dort gebunden.

Printed in Germany.

Meinen Eltern

Vorwort

Die vorliegende Arbeit wurde von der Juristischen und Wirtschaftswissenschaftlichen Fakultät der Martin-Luther-Universität Halle-Wittenberg im Juli 2020 als Dissertation angenommen.

Besonderer Dank gebührt meinem Doktorvater Herrn Prof. Dr. Malte Stieper für das entgegengebrachte Vertrauen, die Denkanstöße und hilfreichen Verbesserungsvorschläge sowohl inhaltlicher als auch stilistischer Art. Namentlich die Sorgfalt und Geschwindigkeit der Korrekturen und Anmerkungen sowie die ständige Ansprechbarkeit haben dazu beigetragen, dass ich das Promotionsvorhaben kontinuierlich fortführen und erfolgreich abschließen konnte.

Darüber hinaus möchte ich mich herzlich bei Herrn Prof. Dr. Daniel Ulber für die zügige Erstellung des Zweitgutachtens und Herrn Prof. Dr. Jan Bernd Nordemann für die wertvolle Unterstützung in der Findungsphase der Arbeit bedanken. Durch ihn wurde ich auf das Thema aufmerksam.

Freundschaftlicher Dank gebührt auch Timm Pravemann für den Austausch, die Korrekturen und kritischen Fragen. Er steht dabei exemplarisch für all diejenigen, welche diese Arbeit in ihrer Entstehung mitbegleitet und stets ein offenes Ohr und einen guten Rat hatten. Danken möchte ich schließlich meiner Familie für den Rückhalt und die bedingungslose Unterstützung.

Berlin, im März 2021 Malte Baumann

Inhaltsübersicht

Inhaltsverzeichnis

A. Einleitung

I. Problemaufriss

Die Informationsübertragung im Internet ist von einer Vielzahl an Intermediären geprägt. Darunter lassen sich all diejenigen Vermittler fassen, welche entweder die technischen Voraussetzungen dafür schaffen, dass Informationen übertragen werden können, oder das Finden und Übermitteln von Informationen erleichtern.

Host-Provider bieten Speicherplatz bis hin zu ganzen Plattformen, die Inhalte zusätzlich strukturieren und präsentieren. Suchmaschinen listen den Nutzern gerankte Hyperlinks zu Websites auf. Access-Provider eröffnen den Endkunden den Zugang zum Internet und Network-Provider betreiben die Infrastruktur zur Signalübertragung. Auch die Registries und Registrare unterstützen mittelbar beim Auffinden und Abrufen von Websiteinhalten.

Die Geschäftsmodelle der Intermediäre unterscheiden sich dabei zum Teil deutlich. Die Spannweite der Vermittlungshandlungen reicht vom neutralen Bereitstellen von Infrastruktur bis hin zu Geschäftsmodellen, die gerade auf Urheberrechtsverletzungen angelegt sind.[1] Selbst die Rolle neutraler Intermediäre ist ambivalent. Für die Funktionsfähigkeit des Internets sind die Nutzer auf sie angewiesen. Domains beispielsweise ermöglichen den Nutzern, Websites unter eingänglichen Namen statt komplexen Nummernkombinationen aufzurufen. Suchmaschinen wie Google erleichtern das Auffinden gewünschter Inhalte beträchtlich. YouTube bietet eine Plattform, die jeden Tag hunderte Stunden an Videos für Endnutzer in Kategorien und Rankings strukturiert. Insofern ist die Tätigkeit von Intermediären sozialadäquat und erwünscht. Nicht selten sind gerade die Intermediäre diejenigen Akteure, die den technologischen Fortschritt vorantreiben, Informationen bündeln und neue Nutzungsarten eröffnen.

Auf der anderen Seite ermöglichen Intermediäre aber auch Urheberrechtsverletzungen, die über ihre Dienste begangen werden, beziehungsweise verstärken sie, indem sie ein größeres Publikum zu ihnen führen. Eine Website mit urheberrechtsverletzenden Inhalten hat ein größeres Verletzungspotential, wenn sie unter einer eingängigen Domain zu finden ist oder von einer Suchmaschine angezeigt wird.

---

[1] *Ohly*, ZUM 2015, 308, 309.

Gleichzeitig ist die Inanspruchnahme von Intermediären für die Rechteinhaber besonders attraktiv, weil sie nicht aufwendig und kostenintensiv gegen eine unüberschaubare Vielzahl an Verletzern vorgehen müssen. Es ist effizienter, YouTube in Anspruch zu nehmen oder die Domain einer illegalen Streamingwebsite löschen zu lassen, als gegen die einzelnen Nutzer vorzugehen, die urheberrechtsverletzendes Material hoch- oder herunterladen. Zeitliche und finanzielle Ressourcen für die Rechtsverfolgung müssen nur gegen eine zentrale Schaltstelle aufgewendet werden und nicht für viele Einzelfälle.[2]

Zudem kann die Rechtsverletzung durch die Inanspruchnahme der einzelnen Verletzer nicht vergleichbar effektiv verhindert werden. Andere Nutzer werden auf diese Weise nicht gehindert, die Rechtsverletzung erneut vorzunehmen, und die Löschung der rechtsverletzenden Inhalte erfolgt immer erst nach Eintritt der Rechtsverletzung.[3] Demgegenüber können die Intermediäre gleichartigen Rechtsverletzungen regelmäßig vorbeugen. Sie haben aufgrund der Masse der gespeicherten oder durchgeleiteten Informationen sogar Rationalisierungspotenziale hinsichtlich der Verhinderung künftiger Rechtsverletzungen (Beispiel: Überwachungssoftware).[4] Dies hat zu einer zunehmenden Inanspruchnahme der Intermediäre geführt.[5]

Im Zuges dieses Trends nahmen die Rechteinhaber in jüngerer Vergangenheit auch verstärkt Domain-Registrare in Anspruch, um gegen Websites mit rechtsverletzenden Inhalten wie etwa Filesharing-Dienste vorzugehen.[6] Wenn ein Kunde eine Domain registrieren möchte, wendet er sich in der Regel an einen Registrar. Auf den Websites der Registrare kann der Kunde prüfen, ob die gewünschte Domain noch frei ist, unterstützende Zusatzdienste wie Speicherplatz für den eigenen Internetauftritt buchen und schließlich einen Registrierungsauftrag für die Domain erteilen. Der Registrar pflegt dann die Informationen zu Registrant und Domain in die Datenbanken der Registries ein (sogenannte Registrierung). Die Registries verwalten die Datenbanken und Nameserver für eine Top-Level-Domain wie „.de“ oder „.com“. In Deutschland übernimmt beispielsweise die DENIC eG diese Aufgabe.

---

[2] *Frey*, Die Haftung von Host-Providern für Immaterialgüterrechtsverletzungen, S. 57.

[3] BGH GRUR 2007, 890, 894 Rn. 40 – *Jugendgefährdende Medien bei eBay*.

[4] *Matthies,* Providerhaftung für Online-Inhalte, S. 108; zur ökonomischen Analyse der Providerhaftung *Matthies*, Providerhaftung für Online-Inhalte, S. 103 ff.

[5] *Frey*, Die Haftung von Host-Providern für Immaterialgüterrechtsverletzungen, S. 50 ff.; vgl. für alternative Ansätze statt der weitreichenden Inanspruchnahme von Intermediären *Lemley*/*Reese*, Law and Economics Working Paper No. 025, S. 149 ff.

[6] Vgl. etwa BGH ZUM 2021, 148 – *Störerhaftung des Registrars*; OLG Saarbrücken MMR 2019, 839 – *Bit-Torrent-Tracker*; OLG Köln ZUM 2019, 348 – *Registrar*; OLG Saarbrücken ZUM-RD 2015, 196.

In einem nächsten Schritt überträgt die jeweilige Registry die Daten zu der gebuchten Domain von ihren Datenbanken in ihre Nameserver (sogenannte Konnektierung). Auf diese Weise wird die IP-Adresse des Servers, auf dem die Inhalte der jeweiligen Website gespeichert sind, mit dem gewünschten Domainnamen verknüpft.

Die Registrare übernehmen also die Registrierung von Domainnamen und tragen auf diese Weise dazu bei, dass Internetnutzer zu den gewünschten Inhalten gelangen, wenn sie in ihren Browser eine Domain eingeben oder auf einen Hyperlink klicken, der mit einer URL verknüpft ist. Sie sind das Bindeglied zwischen den Endkunden, die eine Domain nutzen möchten und den Registries, welche die technische Infrastruktur für eine Top-Level-Domain betreiben.

Die Inanspruchnahme von Intermediären wie Host- und Access-Providern ist bereits umfassend begutachtet worden.[7] Die Haftung der Registrare und Registries wurde vertieft bisher nur für den Fall untersucht, dass der Domainname eine Kennzeichen- oder Namensverletzung oder Wettbewerbsverletzung darstellt.[8] Darum soll es in der vorliegenden Arbeit nicht gehen. Gegenstand der Untersuchung ist die Haftung von Registraren, wenn auf den Websites, deren Domains sie registriert haben, Urheberrechtsverletzungen begangen werden. Es geht um die Haftung für Inhalte und nicht für den Domainnamen.

Mit der Inanspruchnahme der Registrare zielen die Rechteinhaber auf die sogenannte Dekonnektierung der Domain ab. Die Dekonnektierung trennt die Verknüpfung zwischen der Domain und den Servern mit den Websiteinhalten, sodass die Website nur noch über die IP-Adresse des zugehörigen Servers erreichbar ist. Die Nutzer können die Website dann weder durch Eingabe der Domain noch über einen Hyperlink, der auf eine URL unter der Domain verweist, ansteuern. Davon versprechen sich die Rechteinhaber einen Einbruch des Traffics auf der rechtsverletzenden Website. Ansprüche

---

[7] Beispielhaft seien genannt *Weidert/Molle*, in: Ensthaler/Weidert (Hrsg.), Urheberrecht und Internet, Kap. 7 Rn. 175 ff. und Rn. 183 ff.; *Brinkel/Osthaus*, in: Hoeren (Hrsg.), Die Haftung im Internet, Kap. 3 Rn. 1 ff.; *Schwartmann/Polzin*, in: Hoeren (Hrsg.), Die Haftung im Internet, Kap. 6 Rn. 1 ff.; *Frey,* Die Haftung von Host-Providern für Immaterialgüterrechtsverletzungen, S. 61 ff.; *Frey*, ZUM 2019, 40; *Spindler*, GRUR 2018, 1012.

[8] Beispielhaft seien genannt *Bettinger*, in: Bettinger (Hrsg.), Handbuch des Domainrechts, Teil 2 Rn. DE 161 ff.; *Beier*, in: Lehmann/Meents (Hrsg.), Informationstechnologierecht, Kap. 19 Rn. 51 ff.; *Heckmann*, in: jurisPK Internetrecht, Kap. 2.2 Rn. 1 ff.; *Härting*, Internetrecht, Rn. 2252 ff.; *Viefhues*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimediarecht, Teil 6 Rn. 1 ff.; *Rau*, Der internationale Schutz von Domainnamen und Markenrechten im Internet, S. 46 ff.; *Deutsch/Ellerbrock*, Titelschutz: Werktitel und Domainnamen, S. 167 ff.; *Neumann*, Rechtliche Probleme im Streit um Internet-Domain-Names, S. 13 ff.; *Ruff*, DomainLaw, S. 43 ff.; *Krumpholz*, Rechtsfragen von Domain-Namen, S. 25 ff.

gegen die Registrare auf Dekonnektierung der Domain wurden in der Rechtsprechung bisher auf die Störerhaftung gestützt.[9] Insbesondere vor dem Hintergrund der Rechtsprechung des EuGH zu mittelbaren Wiedergabehandlungen[10] ist aber zu erwägen, ob Registrare nicht sogar als Täter einer öffentlichen Wiedergabe in Betracht kommen. Auch eine Teilnehmerhaftung ist vorrangig zu prüfen.

Darüber hinaus haben die Rechteinhaber ein Interesse daran, dass die Dekonnektierung nicht umgangen wird, indem ein anderer Registrar die dekonnektierte Domain wieder konnektiert. Aufgrund der Vielzahl der Anbieter am Markt ist der Domaininhaber grundsätzlich in der Lage, von einem Registrar zum nächsten zu ziehen und somit der Inanspruchnahme eines Registrars jegliche Wirksamkeit zu nehmen. Die Rechteinhaber versuchen daher, den Registrar nicht nur zur Dekonnektierung zu verpflichten, sondern auch zum dauerhaften Gesperrthalten der Domain. In der gerichtlichen Praxis wurde ein Anspruch auf Gesperrthalten der Domain bisher auf einen vorbeugenden Unterlassungsanspruch aus der Teilnehmerhaftung gestützt.[11]

Das Angebot der Registrare ist Teil eines legalen und unter Neutralitätsgesichtspunkten den Access-Providern nahestehenden Geschäftsmodells. Gerade aus diesem Grund ist die Inanspruchnahme aber auch vielversprechend. Unternehmen mit legalen Geschäftsmodellen sind regelmäßig leicht erreichbar. Die unmittelbar Verantwortlichen – die Betreiber der Websites und die Domaininhaber – verbergen oftmals ihre Identität durch falsche Angaben oder sind in Ländern ansässig, in denen die Rechtsdurchsetzung erheblich erschwert ist. Letzteres gilt auch für einige Host-Provider.

Das Vorgehen gegen ein urheberrechtsverletzendes Geschäftsmodell über die Dekonnektierung der Domain ist auch erfolgsversprechend. Der Domainname ist prägend für den Widererkennungswert einer Website und erleichtert deren Auffindbarkeit. Die zunehmend wichtige Rolle der Domain für die virtuelle Präsentation der Inhalte spiegelt sich auch in der gewachsenen wirtschaftlichen Bedeutung der Domainnamen und dem Handel mit ihnen wider.[12]

---

[9] Zu Urheberrechtsverletzungen BGH ZUM 2021, 148 – *Störerhaftung des Registrars*; OLG Saarbrücken MMR 2019, 839 – *Bit-Torrent-Tracker*; OLG Köln ZUM 2019, 348 – *Registrar*; OLG Saarbrücken ZUM-RD 2015, 196; zu Markenrechtsverletzungen OLG Hamburg MMR 2010, 470; OLG Karlsruhe ZUM-RD 2004, 125; zu Persönlichkeitsverletzungen OLG Frankfurt am Main MMR 2016, 139; KG ZUM-RD 2015, 216; zu illegalem Glücksspiel OLG Hamburg ZUM-RD 2000, 173.

[10] EuGH GRUR 2017, 790 – *The Pirate Bay*; EuGH GRUR 2017, 610 – *Filmspeler*; EuGH GRUR 2016, 1152 – *GS Media*.

[11] LG Köln GRUR-RS 2017, 144887 Rn. 99 ff.

[12] Vgl. dazu *Birner*, Die Internetdomain als Vermögensrecht, S. 2 f.; zur steigenden Zahl der Domain-Registrierungen vgl. Verisign, The Domain Name Industry Brief, Volume 15, Issue 4, December 2018.

An dieser Stelle offenbaren sich die oben genannten Interessenpole: Die Tätigkeit der Registrare ist gesellschaftlich wünschenswert und hilft den Nutzern bestimmte Websites zu finden und aufzurufen. Die Inanspruchnahme der Registrare kann auf der anderen Seite wesentlich zur Durchsetzung des Urheberrechts beitragen.

Im Ergebnis zielt diese Arbeit darauf ab, in dem Spannungsfeld zwischen den berechtigten Interessen der Rechteinhaber, der Vulnerabilität des Urheberrechts im Internet und den vernünftigen Grundbedingungen für legale Geschäftsmodelle ein praxistaugliches Haftungskonzept für Registrare zu entwickeln. Die Fragmentierung von Kommunikations- und Datenverarbeitungsprozessen stellt die Rechtswissenschaft vor eine besondere Abwägungsproblematik: Einerseits darf die Fragmentierung der Verantwortung nicht dazu führen, dass die Rechte des geistigen Eigentums faktisch nicht mehr durchgesetzt werden können. Andererseits darf die Verantwortlichkeit neutraler, technischer Unterstützungsdienstleister in einer modernen Informationsgesellschaft nicht überstrapaziert werden. Die Untersuchung weist in ihrer Bedeutung damit über die Haftung der Registrare hinaus. Im Rahmen der einzelnen Haftungsinstitute stellen sich Grundsatzfragen der Haftung neutraler und infrastruktureller Diensteanbieter und des Zusammenspiels der nationalen und unionsrechtlichen Haftungsnormen im Urheberrecht.

II. Gang der Untersuchung

Zunächst wird die Funktionsweise des Domain Name Systems (DNS) erläutert. In diesem Zusammenhang wird auf die Aufgabenteilung und das vertragliche Geflecht zwischen Registries, Registraren und Domaininhabern eingegangen.

Die rechtliche Bewertung ist von drei großen Strukturprinzipien geprägt: die Trennung von Haftungsbegründung und Haftungsprivilegierung, die Haftungszäsur durch die Mitteilung der Rechtsverletzung und die Subsidiarität der Haftungsinstitute.

Zunächst wird die Haftungsbegründung untersucht. Die Mitteilung der Rechtsverletzung stellt dabei eine wichtige Zäsur für subjektive Merkmale und Verkehrspflichten dar. Aus diesem Grund ist die Haftung vor Mitteilung der Rechtsverletzung von der Haftung nach Mitteilung der Rechtsverletzung zu trennen.

Die Prüfung der Haftung vor Mitteilung der Rechtsverletzung richtet sich nach der Hierarchie: Täter, Teilnehmer, Störer. Diese Reihenfolge ist aufgrund der Subsidiarität der Teilnehmer- und der Störerhaftung geboten. Alle drei Haftungsinstitute haben dabei unionsrechtliche Implikationen. Es stellt sich also stets die Frage, was unionsrechtlich zwingend geboten ist und ob die nationalen Regelungen mit diesen Vorgaben vereinbar sind.

Anschließend wird geprüft, wie sich die Mitteilung der Rechtsverletzung auf die Haftung auswirkt. Ein besonderer Fokus liegt dabei auf der Unterlassungshaftung. Chronologisch wird zunächst untersucht, ob die Rechteinhaber von den Registraren die Beseitigung der mitgeteilten Rechtsverletzung durch Dekonnektierung der Domain verlangen können. Im Urheberrecht spielen aber nicht nur die Beseitigung der konkreten Rechtsverletzung eine Rolle, sondern insbesondere auch vorbeugende Prüfpflichten hinsichtlich gleichartiger Verstöße. Es stellt sich also die Frage, in welchem Ausmaß Registrare die Websites auf Rechtsverletzungen prüfen müssen, um gleichartige Rechtsverletzungen zu verhindern. Dabei geht es nicht nur um die Frage, welche Inhalte sie unmittelbar nach Mitteilung der Rechtsverletzung prüfen müssen. Auch die Prüfpflichten, wenn sie eine Domain wieder konnektieren oder registrieren, werden untersucht.

Neben der Dekonnektierung der Domain sind die Rechteinhaber besonders an einem Gesperrthalten berüchtigter Domains interessiert. Auf diesem Wege lässt sich verhindern, dass Domains wie „kinox.to“ oder „thepiratebay.org“ wenige Tage nach der Dekonnektierung oder Löschung durch einen anderen Registrar erneut konnektiert oder registriert werden. Dieser Anspruch auf das Gesperrthalten der Domain wird abschließend geprüft.

An die Prüfung der Haftungsbegründung schließen sich die Privilegierungen des TMG im Lichte der E-Commerce-RL[13] an. Ein besonderer Fokus liegt dabei auf der Frage, ob Registrare das sogenannte Access-Provider-Privileg nach § 8 Abs. 1 S. 1 TMG genießen. Schlussendlich sind noch die etwaigen Folgen der Privilegierung zu erörtern. In diesem Zusammenhang spielen die durch das dritte TMG-Änderungsgesetz eingeführte weitreichende Haftungsfreistellung nach § 8 Abs. 1 S. 2 TMG und der neue Sperranspruch nach § 7 Abs. 4 TMG eine besondere Rolle. Insbesondere ist zu klären, ob der der Sperranspruch auf Registrare anwendbar ist, in welchem Verhältnis der Sperranspruch zu dem traditionellen Institut der Störerhaftung steht und inwieweit der Sperranspruch nach § 7 Abs. 4 TMG von demjenigen aus der Störerhaftung abweicht.

Nach der Fertigstellung der vorliegenden Arbeit hat der BGH zur Störerhaftung von Registraren eine wichtiges Grundsatzurteil gefällt.[14] Im Anschluss findet sich daher eine kurze Besprechung dieses Urteils als Nachtrag. Dort werden die wesentlichen Entscheidungen des BGH zur Haftung und Privilegierung von Registraren besprochen.

---

[13] 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 („Richtlinie über den elektronischen Geschäftsverkehr“).

[14] BGH ZUM 2021, 148 – *Störerhaftung des Registrars*.

B. Die technischen und vertraglichen Grundlagen

Um die Haftung der Registrare für urheberrechtsverletzende Inhalte bewerten zu können, ist es erforderlich, zu verstehen, welche Handlungen der Registrar technisch bei der Registrierung einer Domain vornimmt. Insbesondere muss geklärt werden, wie der Registrar die Verknüpfung von IP-Adresse und Domainname herbeiführt. Denn diese Handlung ist der maßgebliche Anknüpfungspunkt für die Haftung. Dafür bedarf es eines grundlegenden Verständnisses davon, wie eine Domain funktioniert und im Rahmen des Domain Name Systems (DNS) in eine konkrete Website auflöst. Anschließend werden die vertraglichen Grundlagen analysiert, die der Tätigkeit der Registrare und Registries zugrunde liegen. Auf diese Weise wird das notwendige Verständnis dafür entwickelt, welche Aufgaben und Pflichten die Registrare haben und welche Rolle sie in dem Beziehungsgeflecht zwischen den Domaininhabern, den Registries und den übergeordneten Institutionen spielen.

I. Das Domain Name System (DNS)

Ursprünglich erfolgte der Zugriff auf Server und die dort gespeicherten Inhalte ausschließlich durch die Eingabe von IP-Adressen. In der sechsten Version des Internet-Protokolls (IPv6) besteht eine IP-Adresse aus acht Blöcken mit Hexadezimalzahlen,[1] beispielsweise 2001:0db8:0000:0000:0000:54f3:dd6b:0001. So lange, zufällige Zahlenketten können sich Menschen naturgemäß schlecht merken.

Daher wurde 1983 das Domain Name System eingeführt, das bestimmte IP-Adressen eindeutig bestimmten Domainnamen zuordnet und die Navigation im Internet erleichtert.[2] Mittlerweile steuern Internetnutzer Websites im Internet fast ausschließlich über den Domainnamen an, wobei die eigentliche Adressierung auf der Vermittlungsschicht weiterhin über die IP-Adresse erfolgt.[3] Während Nutzer also den Domainnamen in den Webbrowser einge-

---

[1] Elektronik Kompendium, IPv6-Adressen.

[2] *Albrecht* (Hrsg.), Informations- und Kommunikationsrecht, S. 202.

[3] *Albrecht* (Hrsg.), Informations- und Kommunikationsrecht, S. 202.

ben, erfolgt die Wegfindung im Internet im Hintergrund weiterhin über die Ziffernfolge der IP-Adresse.

Die Übersetzung des eingegebenen Domainnamens in die jeweilige IP-Adresse übernehmen Nameserver (DNS-Server). Deren Funktion lässt sich mit der eines Telefonbuchs vergleichen, in dem die Domains mit den zugeordneten IP-Adressen hinterlegt sind.[4]

1. Die Domain

Eine Domain besteht aus einer Top-Level-Domain (länderspezifisch z.B. „.de" oder generisch z.B. „.org") und einer vom Nutzer im Grundsatz frei bestimmbaren Second-Level-Domain (z.B. „wikipedia").[5] Die generischen Top-Level-Domains werden gemeinhin als gTLDs abgekürzt und die länderspezifischen als ccTLDs, wobei „g" für generic und „cc" für country code steht.

Eine Third-Level-Domain ist optional und wird in der Regel von den Inhabern der Second-Level-Domain selbstständig verwaltet.[6] Wikipedia nutzt beispielsweise die Third-Level-Domain „en.", um eine eigene Domain für englischsprachige Inhalte zu betreiben. Die gesamte Domain lautet dann „en.wikipedia.org.". Die Third-Level-Domain hat den Vorteil, dass der Domaininhaber für bestimmte Inhalte eine eigene Domain schaffen kann, die auf einen eigenständigen Server mit einer eigenen IP-Adresse verweist.[7]

Im Kontext des Domainrechts ist auch oft von der URL die Rede („Uniform Resource Locator"). Unter einer URL versteht man den vollständigen Pfad, der auf eine bestimmte Website führt,[8] also beispielsweise „en.wikipedia.org/wiki/History_of_art". Während also die Domain „en.wikipedia.org" über die mit ihr verknüpfte IP-Adresse auf einen ganz bestimmten Rechner verweist, auf dem die gewünschten Inhalte liegen, verweisen die Angaben nach den Schrägstrichen auf konkrete Verzeichnisse oder Dateien auf diesem Rechner. Vereinfacht lässt sich also sagen, dass über die Domain der richtige Server gefunden wird und mit den weiteren Angaben der URL der Ort auf dem Server, wo die konkreten Inhalte abgespeichert sind. Somit bleibt dem Nutzer erspart, stets mit der Startwebsite unter der Domain „en.wikipedia.org" zu beginnen. Der Pfad in der URL ermöglicht dem Nutzer, gezielt bestimmte Inhalte, wie einen Artikel zur Kunstgeschichte, aufzurufen.

---

[4] *Bettinger*, in: Bettinger (Hrsg.), Handbuch des Domainrechts, Teil 1 Abschnitt A Rn. 3.

[5] *Albrecht* (Hrsg.), Informations- und Kommunikationsrecht, S. 203.

[6] *Bettinger*, in: Bettinger (Hrsg.), Handbuch des Domainrechts, Teil 1 Abschnitt A Rn. 16.

[7] *Cichon*, Internetverträge, Rn. 328.

[8] *Huber/Hitzelberger*, Ratgeber Domain-Namen, S. 20.

2. Das hierarchische System der Nameserver

Die Internet Corporation for Assigned Names and Numbers (ICANN), eine Non-Profit-Organisation mit Sitz in Los Angeles, verwaltet die oberste Hierarchieebene des DNS. Diese sogenannte „root-Zone" („root" für Wurzel) besteht aus 13 Root-Nameservern, in denen alle Top-Level-Domains mit ihren dazugehörigen Nameservern eingetragen sind.[9] Man könnte diese Ebene als eine Art Inhaltsverzeichnis des Telefonbuchs betrachten. Es wird nur gespeichert, welcher Server für welche Top-Level-Domain zuständig ist. Informationen zu den Domains unterhalb der Top-Level-Domains befinden sich nicht auf den Nameservern der root-Zone. Dort ist also beispielsweise hinterlegt, welcher Nameserver für die gTLD „.org" zuständig ist. Nicht hinterlegt ist, auf welchem Nameserver die zugeordnete IP-Adresse der Domain „wikipedia.org" gespeichert ist.

Rein theoretisch könnten alle DNS-Daten auf einem einzigen Nameserver liegen, der alle Domain-Anfragen in die entsprechende IP-Adresse aufschlüsselt. Aufgrund der vielen Millionen Einträge wäre dieser Server aber überladen und ein Absturz hätte zudem direkt globale Folgen.[10] Daher wird der DNS-Namensraum in viele kleinere Zonen aufgeteilt, für die jeweils ein oder mehrere Nameserver zuständig sind, auf denen die Daten für die jeweilige Zone liegen.[11] Es handelt sich somit um ein hierarchisches und dezentrales System. Die Nameserver der root-Zone wissen, welcher Nameserver für die Top-Level-Domain zuständig ist. Die Nameserver der Top-Level-Domain wissen, welche Nameserver für die jeweiligen Subdomains zuständig sind. Die Nameserver der Subdomains wissen, welche IP-Adresse der konkreten Subdomain zugeordnet ist.

Für „wikipedia.org" wissen beispielsweise die Nameserver „NS0.WIKIMEDIA.ORG", „NS1.WIKIMEDIA.ORG" und „NS2.WIKIMEDIA.ORG", dass die Inhalte zu der Domain „wikipedia.org" auf dem Server mit der IPv4-Adresse „91.198.174.192" zu finden sind. Der Nameserver für die Top-Level-Domain „.org" weiß hingegen nur, dass für „wikipedia.org" die Nameserver „NS0.WIKIMEDIA.ORG", „NS1.WIKIMEDIA.ORG" und „NS2.WIKIMEDIA.ORG" zuständig sind. Aus Gründen der Redundanz ist es üblich, dass nicht nur ein Nameserver über die Daten verfügt (Primary Nameserver), sondern zusätzliche Nameserver über die identischen Datensätze verfügen (Secondary Nameserver).

Diejenigen Nameserver, welche über originäre Informationen zu einer Domain verfügen und diese nicht lediglich von einem anderen Server ab-

---

[9] *Bettinger*, in: Bettinger (Hrsg.), Handbuch des Domainrechts, Teil 1 Abschnitt A Rn. 5.

[10] *Tanenbaum/Wetherall*, Computernetzwerke, S. 703.

[11] *Tanenbaum/Wetherall*, Computernetzwerke, S. 703 f.

fragen, werden als autoritative Nameserver bezeichnet. Der Name rührt daher, dass sie ihre Informationen „aus erster Hand" erhalten.[12] Das Gegenstück sind nicht-autoritative Nameserver, die ihre Informationen von den autoritativen Nameservern beziehen.[13] Diese nicht-autoritativen Nameserver fragen die Informationen zu den Domains bei den autoritativen Nameservern ab und speichern diese Informationen auf ihren lokalen Speichern temporär zwischen (sog. cachen). Dies ermöglicht eine schnellere Auflösung häufig angefragter Domains. Die Dauer der Zwischenspeicherung wird dabei durch den autoritativen Nameserver bestimmt (sog. TTL – time to live) und kann zwischen einigen Minuten oder auch mehreren Stunden oder Tagen liegen.[14]

Autoritativ sind die Nameserver der Registries, aber auch die untergeordneten Nameserver für die einzelnen Second-Level-Domains. Die autoritativen Nameserver für einzelne Second-Level-Domains werden auch als delegierte Nameserver bezeichnet. Die delegierten Nameserver für eine Domain müssen der Registry im Registrierungsprozess mitgeteilt werden. Diese delegierten Nameserver kann der Domaininhaber selbst betreiben oder dafür einen Diensteanbieter nutzen. Oft übernehmen Registrare den Betrieb der delegierten Nameserver für die Domains, die sie verwalten.

3. Die Verwaltung der Top-Level-Domains durch Registries

Die Top-Level-Domains mit ihren jeweiligen Nameservern werden von sogenannten Registries verwaltet. Ihre Hauptaufgaben sind der Betrieb der Nameserver für die Top-Level-Domain und die Bereitstellung von Informationen über die registrierten Domains (WHOIS-Service).[15] Über den WHOIS-Service können Internetnutzer abfragen, welche Nameserver für die Domain zuständig sind, wann die Domain abläuft und welcher Registrar die Domain verwaltet.[16] Ferner findet sich dort ein E-Mail-Kontakt für Missbrauchsmeldungen.

---

[12] *Pfitzmann/Köpsell/Kriegelstein*, Sperrverfügungen gegen Access-Provider – Technisches Gutachten, S. 16.

[13] *Pfitzmann/Köpsell/Kriegelstein*, Sperrverfügungen gegen Access-Provider – Technisches Gutachten, S. 17.

[14] United Domains, Was bewirkt die Time to live (TTL).

[15] Specification 6 Ziffer 2.1 ICANN Registry Agreement. Die Angaben zu dem Registry Agreement beziehen sich auf das aktuelle Base Registry Agreement vom 31.7.2017, das von der ICANN veröffentlicht wird. Für einzelne gTLDs können abweichende Regelungen gelten. Die konkreten Registry Agreements für jede gTLD finden sich auf der Website der ICANN.

[16] Beispielhaft sei der Domain Name Registration Data Lookup der ICANN genannt.

Sachregister