



RICKERT.LAW

Rickert Rechtsanwaltsgesellschaft mbH · Colmantstraße 15 · 53115 Bonn

Oberlandesgericht Dresden
Schloßplatz 1
01067 Dresden

per beA

Ihr Zeichen: Sachbearbeiter: RA Thomas Rickert
Unser Zeichen: RIC-23/149/06/TR E-Mail: kanzlei@rickert.law

Bonn, den 27.06.2023

In dem Rechtsstreit
Sony Music Entertainment Germany GmbH ./.
Quad9 Stiftung
14 U 503/23

bedanken wir uns für die gewährte Fristverlängerung. Im Folgenden wird namens der Beklagten und Berufungsklägerin die mit Schriftsatz vom 09.03.2023 eingelegte Berufung gegen das Urteil des Landgerichtes Leipzig, Az. 05 O 807/22 vom 01.03.2023 mit folgenden Anträgen begründet:

Es wird beantragt werden,

unter Abänderung des Urteils des Landgerichts Leipzig vom 01.03.2023, Az. 05 O 807/22 die Klage abzuweisen.

Vorsorglich wird für den Fall des Unterliegens beantragt, die Revision zuzulassen.

Rickert Rechtsanwaltsgesellschaft mbH

Rechtsanwälte

Thomas Rickert¹
Patrick Jardin²
Carsten Toß²
Roman Wagner⁴
Matthias Bendixen³
Nicolas Golliart³
Lena Wassermann³
Sandra Schulte, LL.M.³
Theresa Müller-Sevindik³

Kanzlei

Colmantstraße 15
53115 Bonn
Tel.: +49.228.74 898.0
Fax: +49.228.74 898.66
www.rickert.law

HRB 9269
AG Bonn

Geschäftskonto

Commerzbank AG
IBAN: DE81 3804 0007 0241 4480 00
BIC: COBADEFF380

Deutsche Bank AG
IBAN: DE20 3807 0059 0053 1012 00
BIC: DEUTDE380

Anderkonto

Commerzbank AG
IBAN: DE55 3804 0007 0241 4480 80
BIC: COBADEFF380

¹Geschäftsführender Gesellschafter

²Senior Associate Partner

³Associate Partner

⁴Of Counsel

A. Vorbemerkung

Das Landgericht Leipzig hat den Dienst der Beklagten rechtsdogmatisch fehlerhaft eingeordnet, weil es annimmt, dass die Auflösung von Domain Namen in IP-Adressen eine täterschaftliche Haftung für urheberrechtsverletzende Inhalte begründen kann. Das Landgericht Leipzig wendet rechtsfehlerhaft Grundsätze an, die der Europäische- und der Bundesgerichtshof für bestimmte Kategorien von Hosting-Anbietern entwickelt haben. Hosting-Anbieter oder Plattformen, über die Inhalte zum Abruf über das Internet verfügbar gemacht werden, sind allerdings hinsichtlich ihrer technischen Funktionalität und auch der Möglichkeit der Einflussnahme des Anbieters auf von Kunden eingestellte Inhalte zum Betrieb eines DNS-Resolvers grundverschieden.

Ein DNS-Resolver ist ein Software-Modul, das von der Beklagten betrieben wird und als bloße technische Schnittstelle zwischen Nutzern, die DNS-Anfragen stellen und DNS-Servern, die über Informationen dazu verfügen, welche IP-Adresse der angefragten Domain zugeordnet ist, fungiert. Über diese Schnittstelle können Nutzer keine Inhalte hochladen oder auswählen, ob und gegebenenfalls mit wem sie Inhalte teilen möchten, was aber in den vom EuGH entschiedenen Fällen Voraussetzung war (vgl. EuGH, Urteil v. 22. Juni 2021, Rs. C682/18 und C683/18, Rn. 74 – YouTube/Cyando).

Außerdem können keine Links/Hyperlinks hochgeladen werden, die den Zugang zu Inhalten verschaffen. Nur solche Anbieter oder Plattformen, die ein Hochladen sowie die Verwaltung der hochgeladenen Inhalte ermöglichen bzw. Download-Links im Internet veröffentlichen, die Zugang zu den Inhalten auf der Plattform verschaffen, können eine „*Handlung der Wiedergabe*“ vornehmen, weil sie ohne Zustimmung der Rechtsinhaber anderen Internetnutzern über diese Plattformen Zugang zu geschützten Werken gewähren können, die jene anderen Internetnutzer, wären die erstgenannten Nutzer nicht tätig geworden, nicht hätten abrufen können (vgl. EuGH, Urteil v. 22. Juni 2021, Rs. C-682/18 und C-683/18, Rn. 75 – YouTube/Cyando).

Eine entsprechende Subsumtion für den DNS-Resolver-Dienst der Beklagten ist nicht im Ansatz möglich und wird auch nicht vom Landgericht Leipzig vorgenommen.

Schließlich sind die Ausführungen des Landgerichts unlogisch und widersprüchlich, wenn es einerseits eine täterschaftliche öffentliche Wiedergabe und damit eine zentrale Rolle des Diensteanbieters annimmt (Urteil, S. 11), gleichzeitig aber der Beklagten die Eigenschaft eines Diensteanbieters und damit die Haftungsprivilegierung nach § 8 Abs. 1 S. 2 TMG mangels hinreichender Möglichkeit der Einflussnahme abspricht (Urteil, S.10).

In einer kurzen Videopräsentation, die unter dem URL <https://www.youtube.com/watch?v=HdC7Dy7xLzU> abrufbar ist, wird die neutrale und automatische Funktionsweise eines DNS-Resolvers veranschaulicht. Es ist ersichtlich, dass keine Speicherung und kein Bereithalten von Inhalten durch einen DNS-Resolver erfolgt.

Da das Urteil gravierende Fehler in der Subsumtion des Dienstes der Beklagten aufweist, gesetzliche Regelungen, die für die Beklagte von Vorteil sind, völlig außer Acht lässt und den Vortrag der Beklagten aus der I. Instanz nicht hinreichend würdigt, wird das Urteil in vollem Umfang zur Überprüfung durch das Berufungsgericht gestellt.

B. Begründung

Das Urteil des Landgerichts Leipzig beruht auf einer rechtsfehlerhaften Anwendung des Rechts nach §§ 513 Abs. 1, 546 ZPO. Die Klägerin hat keine Ansprüche gegen die Beklagte auf Unterlassung oder Sperrung.

I. Unbestimmter Unterlassungstenor

Der Urteilstenor des Landgerichts Leipzig ist nicht hinreichend konkret, da dieser die Formulierung „und/oder der weiteren Domain(s)“ (Urteil, S. 2) aufweist. Unter Berücksichtigung des BGH-Urteils „DNS-Sperre“ (BGH, Urteil v. 13. Oktober 2022 - I ZR 111/21, GRUR 2022, 1812) ist ein Antrag bzw. Tenor unbestimmt, wenn keine Sperrung einer konkreten Domain verlangt wird (Duplik v. 30.01.2023, S. 18; BGH, a.a.O. Rn. 72f.).

Das Landgericht unterliegt der falschen Annahme, dass der zuletzt gestellte Antrag der Klägerin dem Bestimmtheitserfordernis des § 253 Abs. 2 Nr. 2 ZPO genügt. Dies widerspricht den eigenen rechtlichen Ausführungen des Landgerichts (Urteil, S. 9), wonach entsprechend der Entscheidung DNS-Sperre des Bundesgerichtshofs eine „konkrete Domain“ benannt werden muss (BGH, a.a.O.).

II. Keine Aktivlegitimation

Das Landgericht nimmt rechtsirrig eine Aktivlegitimation der Klägerin an. Eine Aktivlegitimation der Klägerin wurde vom Landgericht ohne Prüfung der tatsächlichen Voraussetzung lediglich pauschal auf das Vorliegen einer hier nicht relevanten Vermutungsregelung gestützt.

1. Keine Leistungsschutzrechte / Keine ausreichenden Nutzungsrechte

Das Landgericht geht von der Aktivlegitimation der Klägerin aus (Urteil, S. 10), weil diese auf Vervielfältigungsstücken des Tonträgers mit dem Streitgegenständlichen Musikalbum als Inhaberin ausschließlicher Nutzungsrechte bezeichnet ist. Zugleich sei die Klägerin aber auch Inhaberin der Leistungsschutzrechte des Tonträgerherstellers (Urteil, S.10).

Bei originärer und erworbener Rechtsinhaberschaft handelt es sich jeweils um verschiedene Sachverhalte, die sich denkbare ausschließen. So wird einerseits behauptet, die Voraussetzungen für die Entstehung des jeweiligen Schutzrechts selbst erfüllt zu haben und das andere Mal, dass ein Dritter diese Voraussetzungen erfüllt habe und dass dadurch entstandene Schutzrecht anschließend durch Abschluss eines Vertrages übertragen oder lizenziert worden sei. Mithin ergeben die unterschiedlichen Feststellungen des Landgerichts Leipzig keinen Sinn, da die Inhaberin von Leistungsschutzrechten bereits die ausschließlichen Rechte besitzt, mithin keine ausschließlichen Nutzungsrechte eingeräumt werden müssen.

Aus einem P-Vermerk ergibt sich nicht, ob der Benannte Hersteller, Rechtsnachfolger oder Inhaber ausschließlicher Nutzungsrechte ist. Folglich kommt der P-Vermerk für alle drei Funktionen in Betracht. Aus der Vermutung nach § 10 Abs. 3 UrhG kann nicht auf eine Vollrechtsübertragung geschlossen werden. Der BGH (BGH, Urteil v. 2. Juni 2022 – I ZR 140/15, Rn. 40 YouTube II) hat festgestellt, dass der P-Vermerk auch lediglich darauf

hindeuten kann, dass dem Unternehmen nur bestimmte ausschließliche Nutzungsrechte eingeräumt worden sind (Duplik v. 30.01.2023, S. 19).

Bereits in der Klageerwiderung erklärte die Beklagte (Klageerwiderung v. 29.07.2022, S. 25), dass aus dem P-Vermerk nicht auf die Rechteinhaberschaft an dem streitgegenständlichen Musikalbum geschlossen werden kann, zumal es vorliegend nicht um die physische Verbreitung des Tonträgers, sondern um eine vermeintliche Verletzung des Rechts der öffentlichen Zugänglichmachung an den streitgegenständlichen Tonaufnahmen geht.

2. Keine Verletzung des Rechts der öffentlichen Zugänglichmachung durch Hyperlinks auf streitgegenständlicher Webseite

Das Landgericht begründet die täterschaftliche Haftung der Beklagten mit einer Verletzung des Rechts der öffentlichen Zugänglichmachung gem. §§ 15, 19a, 85 UrhG (Urteil, S. 11). Es geht rechtsfehlerhaft davon aus, dass die Veröffentlichung von Hyperlinks auf der streitgegenständlichen Webseite die Tonträgerherstellerrechte der Klägerin gem. § 85 UrhG verletzt. Dies ist auch entscheidungserheblich, da das Landgericht annimmt, dass die Beklagte mit „einem Blick auf die Seite den Charakter der Seite hätte erkennen können“, dass sich auf der streitgegenständlichen Webseite offensichtlich ausschließlich illegale Angebote befänden (Urteil, S. 12).

Das Tonträgerherstellerrecht gem. § 85 UrhG gewährt dem Tonträgerhersteller indes – mit Ausnahme des Rechts der öffentlichen Zugänglichmachung – kein Recht der öffentlichen Wiedergabe. Inhaber von Leistungsschutzrechten können sich nicht auf das Recht der öffentlichen Wiedergabe gem. § 15 UrhG i.V.m. Art. 3 Abs. 1 InfoSoc-Richtlinie berufen, weil ihnen kein umfassendes Recht der öffentlichen Wiedergabe zukommt (Schulze in: Dreier/Schulze, Urheberrechtsgesetz, 7. Aufl. 2022, § 85 Rn. 38).

Das Landgericht verkennt, dass die Veröffentlichung von Hyperlinks auf der streitgegenständlichen Webseite das Recht der öffentlichen Zugänglichmachung nicht berührt. Das Setzen von Hyperlinks stellt nur dann eine öffentliche Zugänglichmachung gem. § 19a UrhG dar, wenn sich der Schutzgegenstand in der Sphäre des Vorhaltenden befindet. (BGH, Urteil v. 21. September 2017 – I ZR 11/16, Rn. 19, GRUR 2018, 178 – Vorschaubilder III). Den Betreibern der streitgegenständlichen Webseite kann daher keine öffentliche Zugänglichmachung vorgeworfen werden, da sich die Tonaufnahmen auf den Servern eines Dritten und somit außerhalb ihrer Zugriffssphäre befanden. Auf eine etwaige Verletzung des Rechts der öffentlichen Wiedergabe, zu dem das Landgericht die Rechtsprechung des EuGH in Bezug nimmt (Urteil, S. 11), kann sich die Klägerin nicht berufen, da das von ihr geltend gemachte Tonträgerherstellrecht dieses Recht nicht umfasst.

Diejenigen, die eine festgelegte Darbietung selbst zum Download bereitstellen, machen diese öffentlich zugänglich, da nur die Mitglieder der Öffentlichkeit bestimmen, ob, wann und wo sie darauf zugreifen. Folglich liegt die Entscheidung, dass der verwandte Schutzgegenstand den Besuchern der Plattform zugänglich gemacht wird, ausschließlich bei den Plattformnutzern bzw. den Betreibern dieser Plattformnutzer (vgl. Grünberger, Michael: Die Entwicklung des Urheberrechts im Jahr 2022; ZUM 2023, 309, 332).

„Daher ist zum einen festzustellen, dass die Nutzer der in den Ausgangsverfahren in Rede stehenden Plattformen eine „Handlung der Wiedergabe“ im Sinne der in Rn. 68 des vorliegenden Urteils angeführten Rechtsprechung vornehmen, wenn sie ohne Zustimmung der Rechtsinhaber anderen Internetnutzern über diese Plattformen Zugang zu geschützten Werken gewähren, die jene anderen Internetnutzer, wären die erstgenannten Nutzer nicht tätig geworden, nicht hätten abrufen können. Zum anderen besteht nur dann, wenn diese Nutzer die hochgeladenen Inhalte der „Öffentlichkeit“ im Sinne der in Rn. 69 des vorliegenden Urteils angeführten Rechtsprechung zugänglich machen, indem sie diese Inhalte mit jedem Internetnutzer auf der Plattform YouTube teilen bzw. die Download-Links, die Zugang zu den Inhalten auf der Plattform Uploaded verschaffen, im Internet veröffentlichen, die Möglichkeit, dass diese Nutzer und infolgedessen der Betreiber der Plattform, über die diese Zugänglichmachung erfolgt, eine „öffentliche Wiedergabe“ im Sinne von Art. 3 Abs. 1 der Urheberrechtsrichtlinie durchführen. (EuGH, Urteil v. 22. Juni 2021, Rs. C-682/18 und C-683/18, Rn. 75 – YouTube/Cyando).

Unterstellt, die Beklagte würde durch die Auflösung der Domains in eine IP-Adresse eine öffentliche Wiedergabe der Hyperlinks vornehmen, könnte die Klägerin daraus keine Berechtigung ableiten. Mithin hat das Landgericht aufgrund einer unzutreffenden Vermutung die Aktivlegitimation der Klägerin angenommen.

III. Keine Haftung der Beklagten für Rechtsverletzungen auf streitgegenständlicher Webseite

Die Klägerin kann keine Ansprüche auf Unterlassung, Schadensersatz und Beseitigung gegen die Beklagte geltend machen, da der Dienst der Beklagten gem. § 8 Abs. 1 S. 2 TMG haftungsprivilegiert ist.

1. Beklagte ist Diensteanbieterin gem. § 2 Nr. 1 TMG

Das Landgericht geht davon aus, dass die Haftungsprivilegierung gem. § 8 Abs. 1 S. 2 TMG nicht greife, weil es rechtsirrig annimmt, dass die Beklagte keine Diensteanbieterin i.S.v. § 2 Nr. 1 TMG sei und führt dazu aus (Urteil, S.10):

„Dies trifft auf einen DNS-Resolver aber nicht zu. Der Begriff des Diensteanbieters ist funktionell zu bestimmen (LG Hamburg, Beschl. v. 12.05.2021, Az. 310 O 99/21, Anlage K 1). Er muss durch seine Weisungen oder seine Herrschaftsmacht über Rechner und Kommunikationskanäle die Verbreitung oder das Speichern von Informationen ermöglichen und nach außen als Erbringer von Diensten auftreten. So ist etwa der Admin-C kein Diensteanbieter, weil er nur die Abwicklung der Domainregistrierung erleichtert, aber weder Informationen bereithält noch Zugang zu diesen vermittelt. Der Registrar stellt Nutzern ebenfalls keine Informationen bereit und vermittelt keinen Zugang zur Nutzung von Telemedien, sondern nimmt lediglich die administrative Abwicklung der Domainregistrierung vor, indem er der Registrierungsstelle die Registrierung der Domain erforderlichen Daten mitteilt. Er ist insbesondere kein Zugangsvermittler im Sinne von § 8 TMG, weil er weder Zugang zu

einem Netz vermittelt noch Informationen durchleitet (BGH, Urt. v. 15.10.2020-tzR13/19, GRUR 2021, 53,64 Rz. 15_17 m.w.N.). Das gleiche gilt jedenfalls für den hier streitgegenständlichen Fall des DNS-Resolvers (LG Hamburg, a.a.O.).“

Das Landgericht legt hier die zutreffende Definition des Bundesgerichtshofs zugrunde, unterlässt danach jedoch jegliche Subsumtion.

Die Beklagte ist Diensteanbieterin i.S.d. TMG, weil sie gem. § 2 Nr. 1 Alt. 2 TMG den Zugang zur Nutzung von Telemedien vermittelt. Der Dienst der Beklagten ist ein wesentlicher Bestandteil der Zugangsvermittlung zu Telemedien (MMR 2023, 378, 381), nämlich des Abrufs von Webseiten nach Aufruf einer Domain (Klageerwiderung v. 29.07.2022, S. 26f.). Anders als der Domain-Registrar ist der Dienst der Beklagten an der technischen Zugangsvermittlung selbst beteiligt und daher auch nach der Rechtsprechung des BGH als Diensteanbieter einzustufen (BGH, Urteil v. 15. Oktober 2020 – I ZR 13/19, Rn. 17). Die von dem Anfragenden gewünschte „Verbindung“ zur angefragten Domain wird automatisch durch die Eingabe der URL in das Browserfenster vorgenommen. Der DNS-Resolver als wesentliche Schnittstelle im DNS wandelt den in einem URL enthaltenen Hostnamen in eine IP-Adresse um, damit der Anfragende den Inhalt der Website abrufen kann, die über die Domain erreichbar ist. Ohne den DNS-Resolver würde keine Zuordnung der Domain zur IP-Adresse stattfinden, sodass kein Zugang zum gewünschten Telemedium auf diese Weise möglich wäre. Dass die Beklagte nicht unmittelbar den Zugang zur streitgegenständlichen Webseite eröffnet, ist unerheblich, da „Vermittlung“ schon dem Wortlaut nach gerade auch die mittelbare Eröffnung des Zugangs, also ein weites Begriffsverständnis nahelegt (Klageerwiderung v. 29.07.2022, S. 26f.). Zudem ist der „unmittelbare Zugang“ nur mittels der IP-Adresse möglich. Falls aber eine Domain aufgerufen wird, so ist es eine technische Notwendigkeit, dass zunächst deren Auflösung über das DNS erfolgt und in einem zweiten Schritt der Webserver abgerufen wird.

Diese Auslegung ergibt sich zudem aus den eindeutigen unionsrechtlichen Vorgaben (MMR 2023, 378, 380). In Art. 2 lit. b der E-Commerce-Richtlinie (Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates, im Folgenden: ECRL) wird „Diensteanbieter“ als jede natürliche oder juristische Person, die einen Dienst der Informationsgesellschaft anbietet, definiert. Der Begriff „Dienst der Informationsgesellschaft“ ist in Art. 1 Abs. 1 lit. b der RL (EU) 2015/1535 als „jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung“ legaldefiniert. Dies trifft auf den Dienst der Beklagten zu (MMR 2023, 378, 381). Die Unentgeltlichkeit ist dafür unbeachtlich (EuGH, Urt. vom 15. September 2016, Rs. C-484/14 – McFadden, Rn. 41, 43).

Auf den technischen Vorgang der Zugangsvermittlung kommt es nach dem Wortlaut des § 2 Nr. 1 TMG, Art. 2 lit. b der ECRL und Art. 1 Abs. 1 der RL 2015/1535 nicht an, damit ein Dienst als Dienst der Informationsgesellschaft und weiter als Telemediendienst gewertet werden muss. Einer erweiternden Auslegung bedarf es ebenfalls nicht (Klageerwiderung v. 29.07.2022, S. 26f.).

2. Erheblichkeit der unzutreffenden Würdigung des Begriffs des „Diensteanbieters“

Das Urteil beruht auch auf der erheblichen und fehlerhaften Würdigung des Begriffs des Diensteanbieters, da bei angemessener Berücksichtigung der Beklagten als Zugangsvermittlerin ein Unterlassungsanspruch gem. § 8 Abs. 1 S. 2 TMG entfielen.

3. Haftungsprivilegierung der Beklagten nach § 8 Abs. 1 TMG

Das Landgericht ist der Auffassung, dass die Haftungsprivilegierung gem. § 8 Abs. 1 TMG nicht eingreife, weil die Beklagte Inhalte durchleite, nicht den Zugang zu einem Netz vermittele und „jedenfalls das gleiche“ gelte wie für einen Domain-Registrar oder einen Admin-C.

a. Reine Durchleitung / Zugangsvermittlung durch den Dienst der Beklagten

Das Landgericht setzt sich nicht im Ansatz mit den Vorgaben von § 8 TMG und den Eigenschaften des Dienstes der Beklagten auseinander. Das Landgericht lehnt die Anwendbarkeit von § 8 Nr. 1 TMG mit einem einzigen Satz und dem pauschalen Hinweis darauf, dass für den DNS-Resolver „*jedenfalls das gleiche*“ wie für den Admin-C oder den Domain-Registrar gelte, ab (Urteil, S. 10).

Dabei verkennt das Landgericht grundsätzlich die Funktionalität des Dienstes der Beklagten, die sich wesensmäßig von der eines Domain-Registrars und des Admin-C unterscheidet (Klageerwiderung v. 29.07.2022S. 23ff.). Der BGH stuft Registrar und Admin-C nicht als Diensteanbieter ein, weil sie an dem technischen Vorgang des Abrufs einer Webseite nicht selbst beteiligt sind. Ihr Beitrag besteht in der einmaligen, administrativen Mitwirkung an der Registrierung einer Domain (BGH, Urteil v. 15. Oktober 2020 – I ZR 13/19, Rn. 16f. 28). Dies ist bei der Beklagten gerade nicht der Fall, die bei jedem Aufruf einer Webseite auf Veranlassung des Nutzers eine individuelle Leistung erbringt und somit an der Zugangsvermittlung fortlaufend beteiligt ist (MMR 2023, 378, 381).

Der Dienst der Beklagten ist als Zugangsvermittlung i.S.v. § 8 Abs. 1 TMG zu subsumieren. Wie bereits dargelegt, ist der Begriff der Zugangsvermittlung schon begrifflich weit zu verstehen. Sie setzt die Durchleitung von Informationen gerade nicht voraus. Wird eine Kette von Diensteanbietern für die Zugangsvermittlung genutzt, ist jeder Diensteanbieter in der Kette privilegiert (Klageerwiderung v. 29.07.2022, S. 24 ff.). Nach der klaren Vorgabe von Art. 12 ECRL ist bereits die Zugangsvermittlung zu einem Kommunikationsnetz, nicht erst zur Vermittlung des Zugangs zur Information selbst von der Haftungsprivilegierung umfasst (Klageerwiderung v. 29.07.2022, S. 25). So liegt der Fall bei der Beklagten, die unstreitig an der Vermittlung des Zugangs zum DNS beteiligt ist.

Auch wenn man auf die unmittelbare Durchleitung von Informationen bzw. die Vermittlung des Zugangs zu einem Netz abstellt, ist die Beklagte als Zugangsvermittlerin gem. § 8 TMG einzustufen. Die Klägerin nimmt die Beklagte auf die Unterlassung der Übermittlung von Domain-Namen und IP-Adressen in Anspruch. Bei dem maßgeblichen Lebenssachverhalt der Übermittlung von Domain-Namen und IP-Adressen zwischen den Rechnern der Anfragenden und den Name-Servern leitet die Beklagte unmittelbar Informationen durch, sodass es sich um

einen Fall der reinen Durchleitung gem. §§ 2 Abs. 1, 8 TMG handelt (Duplik v. 31.01.2022, S. 30, MMR 2023, 378, 381).

b. Anwendbarkeit der Haftungsprivilegierung folgt unmittelbar aus dem DSA

Das Urteil des Landgerichts lässt jegliche Auseinandersetzung mit den Vorgaben der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG, dem sog. Digital Services Act (DSA), vermissen. Die Beklagte hat in der Klageerwiderung (Klageerwiderung v. 29.07.2022, S. 27 ff.) und der Duplik (Duplik v. 31.01.2022, S. 25 ff.) ausführlich dargelegt, dass der DSA eindeutig klarstellt, dass die Haftungsprivilegierung für reine Durchleitungsdienste auf DNS-Resolver Anwendung findet.

Der Europäische Gesetzgeber hat die Haftungsprivilegierungen der E-Commerce-RL wortgleich in Art. 4 – 6 DSA nachgebildet, die bislang geltenden Art. 12 – 14 der E-Commerce-RL werden aufgehoben, vgl. Art. 89 DSA. Der Digital Services Act ist als Verordnung unmittelbar anwendbar.

Er hat mit dem DSA klargestellt, dass DNS-Resolver Dienste als reine Durchleitungsdienste gem. Art. 4 Abs. 1 DSA haftungsprivilegiert und mithin auch als Diensteanbieter gem. §§ 2 S. 1 Nr. 1 TMG, 8 Abs. 1 TMG einzustufen sind (MMR 2023, 378, 381).

In Erwägungsgrund 29 des DSA stellt der Gesetzgeber unmissverständlich fest, dass DNS-Resolver zu den gem. Art. 4 Abs. 1 DSA haftungsprivilegierten Diensten der reinen Durchleitung zählen:

*„Vermittlungsdienste umfassen ein breites Spektrum an wirtschaftlichen Tätigkeiten, die online stattfinden und sich kontinuierlich weiterentwickeln, um eine rasche, sichere und geschützte Übermittlung von Informationen zu ermöglichen und allen Beteiligten des Online-Ökosystems komfortable Lösungen zu bieten. Vermittlungsdienste einer **„reinen Durchleitung“** umfassen beispielsweise allgemeine Kategorien von Diensten wie Internet- Austauschknoten, drahtlose Zugangspunkte, virtuelle private Netze, **DNS-Dienste und DNS-Resolver**, Dienste von Namenregistern der Domäne oberster Stufe, Registrierungsstellen, Zertifizierungsstellen, die digitale Zertifikate ausstellen, Internet-Sprachtelefonie (VoIP) und andere interpersonelle Kommunikationsdienste; [...]“ (Hervorhebungen des Unterzeichners)*

Dass der Europäische Gesetzgeber damit keine konstitutive Rechtsänderung bewirken, sondern lediglich die geltende, wortgleich fortgeführte Rechtslage in Bezug auf seit Inkrafttreten der E-Commerce-RL technische Entwicklungen klarstellen wollte, ergibt sich, ebenfalls unmissverständlich, aus Erwägungsgrund 28:

*“In dieser Hinsicht sollte **darin erinnert werden**, dass Anbieter von Diensten zur Bereitstellung und Vereinfachung der zugrunde liegenden logischen Architektur und des reibungslosen Funktionierens des Internets, einschließlich technischer Hilfsfunktionen, ebenfalls die in dieser Verordnung festgelegten Haftungsausschlüsse in Anspruch nehmen können, sofern ihre Dienste als „reine Durchleitung“, „Caching“-Leistung oder „Hosting“-Dienst einzuordnen sind. Zu solchen Diensten gehören u. a. lokale Funknetze (WLAN), **DNS-Dienste** [...]“ (Hervorhebungen des Unterzeichners)*

Der Digital Services Act ist am 22. November 2022 in Kraft getreten und gilt gemäß Art. 93 DSA vollumfänglich ab dem 17. Februar 2024. Der Zeitpunkt, der für die Anwendbarkeit des Gesetzes, etwa hinsichtlich einzelner Sachverhalte, bestimmter Veranlagungszeiträume oder bestimmter Geschäftsjahre, festgelegt wird, kann vom Zeitpunkt des Inkrafttretens abweichen. Anwendungsbestimmungen haben eher die Funktion von Übergangsvorschriften (Handbuch der Rechtsförmlichkeit, 3. Auflage, Teil C, 11 Geltungszeitregeln, 11.1 Inkrafttretensregelung, Rn. 438).

Gesetze entfalten mit dem Inkrafttreten ihre Wirkung. Sie gestalten die Rechtsordnung für die Zukunft und erfassen daher regelmäßig alle künftig entstehenden Rechtsverhältnisse. Ein neues Gesetz kann jedoch auch bestehende Rechtsverhältnisse betreffen. Dabei ergeben sich Unterschiede, je nachdem ob es sich um abgeschlossene oder noch offene Sachverhalte handelt. Durch Übergangsvorschriften werden die Wirkungen des Gesetzes oder einzelner Regelungen klargestellt, verändert oder mit Blick auf die angestrebte künftige Ordnung besonders ausgestaltet (Handbuch der Rechtsförmlichkeit, 3. Auflage, Teil C, Rn. 412). Die nach dem Inkrafttreten des DSA festgelegte Anlaufzeit dient lediglich dazu, dass die betroffenen Vermittlungsdienste hinreichend Zeit haben, den angestrebten Rechtszustand zu erreichen, da dies unter Umständen erhebliche technische Änderungen von Systemen zur Folge haben kann, welche nicht sogleich vollständig erreicht werden können. Demnach bezieht sich die Anlaufzeit des DSA auf die Handlungsverpflichtungen der Vermittlungsdienste. Der Geltungsbereich der Verordnung für Vermittlungsdienste nach Art. 2 DSA gilt bereits mit Inkrafttreten der Verordnung, woraus sich ergibt, dass DNS-Resolver als Vermittlungsdienste vom Geltungsbereich erfasst sind. Dies folgt unzweifelhaft aus den oben genannten Erwägungsgründen.

Die Beklagte hat in der Duplik (Duplik v. 31.03.2023, S. 26 f.) auf Grundlage des als Anlage B 13 vorgelegten Gutachtens von Prof. Dr. Ruth Janal erläutert, dass der DSA eine Vorwirkung entfaltet und die gesetzgeberischen Wertungen bereits jetzt von mitgliedstaatlichen Gerichten berücksichtigt werden müssen. Aus dem unionsrechtlichen Frustrationsverbot aus Art. 4 Abs. 3 EUV folgt, dass die mitgliedstaatlichen Stellen verpflichtet sind, Maßnahmen zu vermeiden, die dazu geeignet sind, die Ziele des Unionsrechtsakts ernstlich zu gefährden. Eine Inanspruchnahme eines DNS-Resolvers auf Unterlassung der Auflösung bestimmter Domain Namen aus § 97 Abs. 1 UrhG ist in die Zukunft gerichtet. Eine entsprechende Unterlassungsanordnung wäre damit geeignet, die Wirkung des Art. 4 Abs. 1 DSA ernstlich zu gefährden, sofern sie nicht zeitlich auf den Beginn des zeitlichen Anwendungsbereichs des DSA befristet wird (Anlage B13, S. 14 f.).

Folglich hätte das Landgericht den von der Beklagte aufgezeigten Erwägungsrund 29 DSA nicht ignorieren dürfen, sondern diesen bei der Subsumtion der Auslegung der Anwendungsfrage des § 8 TMG zur Haftungsprivilegierung berücksichtigen müssen.

c. Ungleichbehandlung mit Access Providern führt zu Wertungswidersprüchen

Die Rechtsauffassung des Landgerichts, dass DNS-Resolver sich nicht auf die Haftungsprivilegierung gem. § 8 Abs. 1 TMG berufen können, führt zu dem zu Wertungswidersprüchen und einer sachlich nicht gerechtfertigten Ungleichbehandlung mit

Internetzugangsanbietern (Klageerwiderung v. 29.07.2022, S. 28f; Duplik v. 31.03.2023, S. 27f., Anlage B13, S. 12f.).

Internetzugangsanbieter erbringen im Rahmen ihres Dienstes stets auch DNS-Resolver-Dienste. Die Auflösung der IP-Adressen in Domain-Namen ist Teil des einheitlichen Lebenssachverhalts der Erbringung von Internetzugangsleistungen. Internetzugangsanbieter sind für diese Leistungen unstreitig gem. § 8 Nr. 1 TMG haftungsprivilegiert. Diese Privilegierung muss auch die DNS-Resolver-Leistungen miteinschließen, da das Haftungsprivileg ansonsten leerliefe (Klageerwiderung v. 29.07.2022, S. 28f; Duplik v. 31.03.2023, S. 27). Internetzugangsanbieter setzen DNS-Sperren, die etwa Gegenstand der BGH-Entscheidung „DNS-Sperre“ waren (BGH, Urteil v. 13. Oktober 2022 - I ZR 111/21, GRUR 2022, 1812– DNS-Sperre), ebenfalls durch eine Konfiguration der von ihnen betriebenen DNS-Resolver um. Fasst man den Schritt der DNS-Abfrage nicht unter den technischen Lebenssachverhalt der Zugangsvermittlung, würden die Privilegierung für Access Provider gem. § 8 Abs. 1 TMG ins Leere laufen, da die Anbieter sodann zwar nicht in ihrer Eigenschaft als Access Provider, wohl aber in ihrer Eigenschaft als Anbieter eines rekursiven DNS-Resolvers Haftungs- und Prüfungsrisiken ausgesetzt wären (Klageerwiderung v. 29.07.2022, S. 27f.).

Den Betrieb von DNS-Resolvieren von der Haftungsprivilegierung gem. § 8 TMG auszunehmen, führt nicht nur zu Wertungswidersprüchen, sondern zu einer sachlich nicht gerechtfertigten Ungleichbehandlung. Prof. Janal führt dazu aus:

„Zugangsprovider, die im Rahmen ihres Dienstes DNS-Resolving anbieten, sind in den Grenzen des § 8 Abs. 1 TMG von der Haftung privilegiert und können nur gemäß § 7 Abs. 4 TMG auf Sperre des Zugangs zu einer Domain in Anspruch genommen werden. Dabei ist das Sperrverlangen i.d.R. auf die Einrichtung einer DNS-Sperre gerichtet, d.h. auf Unterlassung der Auflösung bestimmter Domainnamen. Demgegenüber sollen Anbieter von unabhängigen DNS-Resolvieren nach Auffassung des LG Kölns als Täter einer Urheberrechtsverletzung haften, sofern sie nicht auf ein Sperrverlangen eines Rechteinhabers hin die Auflösung der genannten Domainnamen unterbinden. Das gleiche Verhalten – Durchführung des DNS-Lookups – wird demnach unterschiedlich behandelt. Für diese Ungleichbehandlung zwischen Zugangsanbieter und unabhängigem DNS-Resolver werden in der instanzgerichtlichen Rechtsprechung keine Sachgründe genannt, die dem Differenzierungsziel und dem Ausmaß der Ungleichbehandlung angemessen sind. So ist bspw. die Behauptung, die Haftungsprivilegien des TMG seien eng auszulegen, kein Sachgrund für eine Differenzierung. Ebenfalls lässt sich kein angemessener Sachgrund dafür erkennen, eine „Hilfsleistung“ einer strikteren Haftung zu unterziehen als eine Hauptleistung. Auch die Tatsache, dass Zugangsvermittler eine zusätzliche Leistung anbieten, nämlich die Vermittlung des Zugangs zum Internet und die Übermittlung der unter der IP-Adresse gespeicherten Inhalte, stellt keinen Sachgrund für eine Privilegierung eines Zugangsvermittlers dar. Denn beide Dienste sind für die Nutzung des World Wide Web unverzichtbar. Im Gegenteil ist die Zugangsvermittlung „näher“ an der Rechtsverletzung als die Auflösung der IP-Adresse durch einen Resolver, weil durch den Zugangsvermittler, nicht aber durch den DNS-Resolver, potenziell rechtsverletzende Inhalte übermittelt werden. Dies spricht für eine strengere Haftung

des Zugangsanbieters gegenüber einem unabhängigen DNS-Resolver, nicht für eine strengere Haftung des DNS-Resolvers.“ (Anlage B13, S. 13 m.w.N.)

4. Keine täterschaftliche Haftung der Beklagten

Das Landgericht hat die Beklagte als Täterin einer Urheberrechtsverletzung gem. § 97 Abs. 1 UrhG zur Unterlassung der Auflösung des streitgegenständlichen Domain-Namens verurteilt. Das Landgericht nimmt dabei in nicht vertretbarer Weise an, dass die Beklagte durch den Betrieb des DNS-Resolver-Dienstes eine öffentliche Wiedergabe der streitgegenständlichen Tonaufnahmen vornehme (Urteil, S. 11 f.).

Das Landgericht geht davon aus, dass die Ausübung einer Vermittlungstätigkeit sowie die bloße Kenntnis von einer Rechtsverletzung auf einer Plattform, die von einem Dritten betrieben wird, für die Handlung einer öffentlichen Wiedergabe ausreicht. Diese Auffassung verkennt grundsätzlich die Systematik der Haftungsprivilegierungen des TMG und der ECRL. Sie ist mit der Rechtsprechung des BGH und des EuGH zu Hosting- und Vermittlungsdiensten nicht vereinbar.

Das Landgericht überträgt die Rechtsprechung des EuGH zu bestimmten Hosting-Diensten (vgl. EuGH, Urteil v. 22. Juni 2021, Rs. C-682/18 und C-683/18, Rn. 75 – YouTube/Cyando) mit einem Satz auf den DNS-Resolver-Dienst der Beklagten. Das Landgericht stellt apodiktisch fest, dass die Beklagte eine zentrale Rolle bei der geltend gemachten Urheberrechtsverletzung spiele, in dem sie den Domain-Namen in eine IP-Adresse auflöse (Urteil, S. 11). Dabei verkennt das Landgericht, dass sich die Ausführungen des EuGH auf bestimmte Kategorien von Hosting-Diensten, und zwar auf eine Video- und eine Sharehosting-Plattform beziehen. Dabei verkennt das Landgericht, dass sich diese Rechtsprechung nicht ohne weiteres auf den technisch völlig anders gelagerten Sachverhalt der Auflösung von DNS-Anfragen übertragen lässt. Die Feststellung des Landgerichts, dass die Ausführungen nicht „ausschließlich auf den Fall des Hostproviders“ beschränkt seien (Urteil, S. 11), entbindet das Landgericht nicht von der Prüfung, ob die Leistung der Beklagten eine öffentliche Wiedergabe gem. Art. 3 Abs. 1 InfoSoc-RL darstellt.

Die Auffassung des Landgerichts, dass die Beklagte eine öffentliche Wiedergabe vornehme, weil sie eine zentrale Rolle bei der Rechtsverletzung spiele und vorsätzlich handle, begegnet durchgreifenden Bedenken. Der Entscheidung des EuGH i.S. YouTube/Cyando lassen sich keine generalisierungsfähigen Maßstäbe entnehmen, nach welchen Kriterien eine öffentliche Wiedergabehandlung anderer Diensteanbieter oder sonstiger Mittelspersonen der Informationsgesellschaft zu beurteilen sind. Sowohl der EuGH als auch der BGH differenzieren in ihrer Rechtsprechung strikt zwischen den unterschiedlichen Arten von Diensteanbietern. Der EuGH hat Internetzugangsanbieter und Anbieter von Vermittlungsdiensten und Vermittlungsleistungen stets als Mittelspersonen gem. Art. 8 Abs. 3 InfoSoc-RL, Art. 12 E-Commerce-RL und nicht als Täter der Handlung einer öffentlichen Wiedergabe betrachtet (EuGH, Urteil v. 27. März 2014 – C-314/12, GRUR 2014, 468 – UPC Telekabel; EuGH, Urteil v. 15. September 2016 – C-484/14, GRUR 2016, 1146 – McFadden, Duplik v. 31.03.2023, S. 22, Anlage B13, S. 7f.). Anhaltspunkte, dass der EuGH von dieser Rechtsprechung abweichen wollte, enthält die Entscheidung YouTube/Cyando nicht. Dementsprechend stellt auch der BGH in den Entscheidungen YouTube II und Uploaded III (BGH, Urteil v. 2. Juni 2022 – I ZR 140/15, Rn. 112

– YouTube II; BGH, Urteil v. 2. Juni 2022 – I ZR 135/18, – Uploaded III) klar, dass er seine Rechtsprechung zur öffentlichen Wiedergabe durch Vermittlungsdienste nur in Bezug auf Host Provider geändert hat. Dies ergibt sich aus den von Prof. Janal in Bezug genommenen Passagen der Entscheidungsbegründungen (Anlage B13, S. 8 f.). Die Entscheidungen des BGH beschränken sich ersichtlich auf die streitgegenständlichen Konstellationen, wie sich aus den Wendungen „in einem solchen Fall“, „in dieser Konstellation“ sowie „Hier tritt mithin die Haftung als Täter an die Stelle der bisherigen Störerhaftung“ ergibt. Für andere Diensteanbieter als Host Provider enthalten die Entscheidungen keine Aussage (Anlage B13, S. 9 m.w.N. und Verweis auf Ohly, NJW 2022, 2961, 2962 f.)

Die Auffassung des Landgerichts widerspricht zudem der Rechtsprechung des BGH in der Entscheidung DNS-Sperre (BGH, Urteil v. 13. Oktober 2022 – I ZR 111/21 – DNS-Sperre). Der BGH prüft die Verantwortlichkeit des Internetzugangsanbieters allein unter dem Gesichtspunkt des § 7 Abs. 4 TMG. Eine täterschaftliche Haftung des Internetzugangsanbieters, wenn er nach einem Hinweis auf rechtsverletzende Inhalte eine DNS-Sperre nicht einrichtet, zieht der BGH nicht in Betracht.

Die Ausführungen des EuGH und des BGH zur zentralen Rolle von bestimmten Hosting-Anbietern lassen sich nicht auf DNS-Resolver übertragen. Der EuGH und der BGH leiten die zentrale Rolle dieser Dienste insbesondere aus deren besonderen Zugriffsmöglichkeiten ab, da sich die rechtsverletzenden Inhalte in ihrer Sphäre befinden und Hosting-Dienste diese Inhalte gezielt und vollständig beenden können. Die vom EuGH geforderte „zentrale Rolle“ beim Zugänglichmachen von Werken kann bei diesen Diensteanbietern daher vorliegen, wenn Betreiber einer Online-Filesharing-Plattform durch deren Bereitstellung und den Betrieb ihren Nutzern einen Zugang zu den betreffenden Werken anbieten (EuGH, Urteil v. 22. Juni 2021, Rs. C-682/18 und C-683/18, – YouTube/Cyando, Rn. 77). Der EuGH stellt darauf ab, dass der unmittelbare Täter Nutzer des Hosting-Dienstes ist und die geschützten Inhalte über den Dienst des Hosting-Anbieters zugänglich gemacht werden (EuGH a.a.O. Rn 77, 83, 84). Die Rolle des DNS-Resolvers unterscheidet sich davon fundamental. Ein DNS-Resolver handelt als Vermittler, der die Anfrage zu einer Domain bzw. IP-Adresse abrufen und weitergeben kann (Klageerwiderung v. 29.07.2022, S. 2). Die Schutzgegenstände befinden sich weder in der Zugriffssphäre des DNS-Resolvers, noch nutzen die Täter der Rechtsverletzungen den Dienst der Beklagten, um geschützte Inhalte rechtswidrig öffentlich zugänglich zu machen. Der Dienst der Beklagten speichert keine Informationen, der Dienst ist auf die Übermittlung von Informationen (IP-Adressen und Domain-Namen) beschränkt. Anders als Host Provider kann die Beklagte Inhalte zudem nicht zielgenau löschen und sperren, eine Sperre im Dienst der Beklagten betrifft stets sämtliche Inhalte einer Domain (Klageerwiderung v. 29.07.2022, S. 38, Duplik v. 31.03.2023, S. 40).

Die Auffassung des Landgerichts, dass der Hinweis auf eine (vermeintliche) Rechtsverletzung auf einer Dritt-Plattform einen Vorsatz bezüglich einer Handlung der öffentlichen Wiedergabe begründet (Urteil, S. 11), begegnet ebenfalls durchgreifenden Bedenken. Das Landgericht verkennt die Systematik der Haftungsprivilegierungen des TMG. Das Haftungsprivileg für Host Provider entfällt gem. § 10 S. 1 Nr. 2 TMG, wenn diese auf eine rechtsverletzende Informationen hingewiesen wurden und diese nicht unverzüglich löschen. Das Haftungsprivileg für Zugangsanbieter gem. § 8 Abs. 1 TMG enthält eine solche Reaktionspflicht gerade nicht. Die Haftungsprivilegierung greift deshalb grundsätzlich auch dann, wenn der Diensteanbieter positive Kenntnis von der rechtswidrigen Information hat

(Anlage B13, S. 7f.). Würde nun mit der Auffassung des Landgerichts die fehlende Abhilfemaßnahme durch einen solchen Dienst als Handlung der öffentlichen Wiedergabe interpretiert, hätte dies nach der Entscheidung zur Folge, dass sich der Diensteanbieter nicht auf das Haftungsprivileg berufen könnte. Damit aber würden die spezifisch auf diese Diensteanbieter zugeschnittenen Haftungsprivilegien konterkariert und umgangen.

Unabhängig davon kommt eine öffentliche Wiedergabe durch die Beklagte schon aus dem Grund nicht in Betracht, dass die Beklagte nach der Verurteilung durch das Landgericht Hamburg im einstweiligen Verfügungsverfahren eine auf das Gebiet der Bundesrepublik Deutschland begrenzte Sperrung der streitgegenständlichen Domain durch eine geografische Zuordnung der IP-Adressen implementiert hat. Insofern hat sie die „erforderlichen Maßnahmen“ ergriffen, um die von der Klägerin begehrte Unterlassung der Auflösung der streitgegenständlichen Domains für das Gebiet der Bundesrepublik Deutschland zu bewirken (Duplik v. 30.01.2023, S. 23f.). Dass die geografisch begrenzte Sperre gezielt durch den Einsatz von VPN-Software umgangen werden kann, steht deren Wirksamkeit nicht entgegen (vgl. Klageerwiderung v. 29.07.2022, S. 23). In den Schlussanträgen zum Verfahren Grand Production (EuGH, C-423/21 – Grand Production, Schlussanträge v. 20.12.2022), legt Generalanwalt Szpunar dar, dass eine öffentliche Wiedergabe bei geografischen Zugangssperren für die Gebiete, für die die Sperre implementiert ist, nicht erfolgt. Eine Ausnahme davon gelte nur dann, wenn der jeweilige Dienst absichtlich eine unwirksame geografische Zugangssperre anwendet (EuGH, a.a.O., Rn. 36 ff.; 44).

Dies ist hier ersichtlich nicht der Fall, die Beklagte hat eine Zugangssperre nach höchsten technischen Standards eingerichtet. Demnach führt die vorsätzliche Verschleierung des Aufenthalts durch die Nutzung eines VPN-Dienstes durch den Zeugen Kunath nicht zu einer Wiedergabehandlung durch die Beklagte. Eine öffentliche Wiedergabe durch die Beklagte scheidet daher schon aus dem Grund aus, dass die Beklagte keinen Vorsatz für die Ermöglichung einer Wiedergabehandlung auf dem Gebiet der Bundesrepublik hat (Duplik v. 30.01.2023, S. 24). Mit diesem Vortrag hat sich das Landgericht Leipzig ebenfalls nicht auseinandergesetzt.

5. Weltweite DNS-Sperre unverhältnismäßig

Die Annahme des Landgerichts, dass es unschädlich wäre, wenn die Beklagte die streitgegenständlichen Domains global für sämtliche Internetnutzer, unabhängig vom jeweils anwendbaren Recht sperrt (Urteil, S. 12) begegnet ebenfalls durchgreifenden Bedenken.

Die vom Landgericht Leipzig kurz erwähnten „Einwände der Beklagten“ und die Bewertung, dass diese einem Anspruch nicht entgegenstehen (Urteil, S. 12) verdeutlicht, dass sich das Landgericht nicht im Ansatz mit dem Vortrag der Beklagten befasst hat (Klageerwiderung v. 29.07.2022, S. 9).

Die Beklagte hat mehrfach auf die gefestigte Rechtsprechung von EuGH und BGH hingewiesen, dass Sperrmaßnahmen gegen Urheberrechtsverletzungen stets streng zielorientiert sein müssen (Klageerwiderung v. 29.07.2022, S. 39f; BGH, Urteil v. 26 November 2015 – I ZR 174/14, GRUR 2016, 268 Rn. 53 – Störerhaftung des Access Providers; EuGH, Urteil v. 27. März 2014 – C-314/12, GRUR 2014, 468, Rn. 63- UPC Telekabel). Eine Sperrmaßnahme darf nicht dazu führen, dass der Zugang der Internetnutzer zu rechtmäßigen Informationen unverhältnismäßig beeinträchtigt wird.

Die pauschale Behauptung, dass ein Overblocking unschädlich sei, weil weltweit kein berechtigtes Interesse auf den Zugriff dieser Website bestehe (Urteil, S. 12), dehnen die Rechtsfolgen des Art. 8 Abs. 1 Rom-II-VO in einem nicht vertretbaren Maß aus. Nach dem Vortrag der Klägerin beschränken sich ihre Rechte auf das Gebiet der Bundesrepublik Deutschland (Klage v. 22.04.2022, S. 15). Demnach steht der Klägerin kein Anspruch auf Unterlassung außerhalb der Bundesrepublik Deutschland zu.

Die Beklagte legte in der Klageerwiderung dar (Klageerwiderung v. 29.07.2022, S. 41ff.), dass durch die weltweite Sperrwirkung eine erhöhte Gefahr besteht, dass der Zugang zu Informationen, die in anderen Jurisdiktionen nicht verboten sind, verhindert wird. Dabei ist es davon unabhängig, ob die rechtsverletzenden Inhalte, die über die beanstandete Domain zugänglich sind, auch in den Rechtsordnungen der TRIPS-Mitgliedstaaten rechtswidrig sind, die Frage ist danach zu beurteilen, ob die jeweiligen Rechtsordnungen eine Inanspruchnahme der Beklagten zugelassen hätten. Wie ausgeführt, sind gerichtliche Anordnungen gegen DNS-Resolver international bislang Einzelfälle geblieben (vgl. Schwemer, Copyright Content Moderation at Non-Content Layers, in: Rosati, Handbook of European Copyright Law (2021), S. 11). Das Landgericht setzt sich auch an dieser Stelle nicht mit den Argumenten der Beklagten (Klageerwiderung v. 29.07.2022, S. 41 ff.), dass etwa aus dem Verhältnismäßigkeits- und Subsidiaritätserwägungen eine Inanspruchnahme von DNS-Resolovern unter anderen Rechtsordnungen nicht möglich ist, auseinander. Nach dem Schweizer Recht, wo die Beklagte ihren Sitz hat, können Zugangsvermittler mangels eigenem Tatbeitrag nicht zur Einrichtung von DNS-Sperren aufgrund von Urheberrechtsverletzungen in Anspruch genommen werden (Bundesgericht, Urteil vom 4. Februar 2019, 4A_433/2018). Die weltweite Sperrwirkung führt dazu, dass eine Rechtsfolge eintritt, die nach anderen Rechtsordnungen nicht vorgesehen oder, wie im Falle der Schweiz, ausdrücklich ausgeschlossen ist. Die Beklagte wies daraufhin, dass die Mitgliedstaaten dafür Sorge tragen müssen, dass die von ihnen erlassenen Maßnahmen mit internationalem Recht vereinbar sind (a.a.O. Rn. 52). Ob eine Verfügung mit extraterritorialer Wirkung nach internationalem Recht zulässig ist, muss demnach im Einzelfall erst festgestellt werden und kann nicht pauschal vom Landgericht behauptet werden. Die Zulässigkeit extraterritorialer Anordnungen ist außerhalb besonderer Gestattung (insb. internationaler Verträge) nach internationalem Recht indes grundsätzlich zu verneinen (vgl. Krämer, EuR 2021, 137, 138). Zur Zulässigkeit der Sperrung mit weltweiter Wirkung nach internationalem Recht tätigt das Landgericht keine Ausführungen.

6. Keine gerichtlichen Rechtsschutzmöglichkeiten

Das Landgericht hat nicht gewürdigt, dass die Rechtmäßigkeit einer DNS-Sperre nach der Rechtsprechung des EuGH und des BGH voraussetzt, dass den betroffenen Internetnutzern ein wirksamer gerichtlicher Rechtsbehelf zur Verfügung steht, um ihre Rechte nach Bekanntwerden der vom Anbieter getroffenen Sperrmaßnahmen vor Gericht geltend zu machen (EuGH, Urteil v. 27. März 2014 – C-314/12, GRUR 2014, 468, Rn. 56 – UPC Telekabel; BGH, Urteil v. 26. November 2015 – I ZR 174/14, GRUR 2016, 268, Rn. 57 – Störerhaftung des Access Providers). Das Landgericht hat sich nicht damit auseinandergesetzt, dass die Beklagte ausführlich dargelegte, dass den Internetnutzern vorliegend kein Rechtsbehelf zur Verfügung steht, der es ihnen ermöglichen würde, die DNS-

Sperre gerichtlich überprüfen zu lassen (Klageerwiderung v. 29.07.2022, S. 38 f.; Duplik v. 30.01.2023, S. 33).

7. Kein Anspruch auf Ergreifung „zumutbarer Vorsorgemaßnahmen“

Das Landgericht legt der Beklagten mit Verweis auf die Entscheidung Uploaded III (BGH, Urteil v. 2. Juni 2022 – I ZR 135/18– Uploaded III) auf, „zumutbare Vorsorgemaßnahmen [zu] ergreifen, mit denen das Hochladen von Dateien mit vergleichbarem rechtsverletzenden Inhalt in Zukunft verhindert wird“ (Urteil, S. 12). Diese Ausführungen belegen, dass das Landgericht die Funktionalität des Dienstes der Beklagten grundsätzlich verkannt hat und auch hier unbesehen die Rechtsprechung des BGH zu Hosting-Anbietern auf den DNS-Resolver-Dienst der Beklagten übertragen will. Dieses fundamentale Missverständnis des Landgerichts wird in der Übertragung der Grundsätze zur Ergreifung von Vorsorgemaßnahmen besonders deutlich: Denn anders als der im Verfahren Uploaded III betroffene Sharehosting-Dienst kann die Beklagte das Hochladen von Dateien nicht verhindern, da das Hochladen von Dateien auf dem Dienst der Beklagten schlichtweg nicht möglich ist. Die Beklagte speichert, wie mehrfach dargelegt (Klageerwiderung v. 29.07.2022, S. 2; Duplik v. 30.01.2023, S. 6 ff.), keine Informationen, auch nicht die streitgegenständlichen Tonaufnahmen. Der Dienst der Beklagten besteht allein in der Übermittlung von Domain-Namen und IP-Adressen.

8. Kein Sperranspruch gem. § 7 Abs. 4 TMG

Das Landgericht prüft, obwohl es dazu wegen der Annahme einer täterschaftlichen öffentlichen Wiedergabe durch die Beklagte nicht verpflichtet wäre, zumindest teilweise die Voraussetzungen von § 7 Abs. 4 TMG. Dabei nimmt das Landgericht rechtsfehlerhaft an, dass die Klägerin ausreichende Bemühungen unternommen habe, um tatnähere Beteiligte vorrangig in Anspruch zu nehmen (Urteil, S. 13 f).

a. Inanspruchnahme wegen Subsidiarität ausgeschlossen

Der BGH hat in der Entscheidung DNS-Sperre erneut klargestellt, dass die Sperrung einer Webseite strengen Voraussetzungen unterliegt und der Sperranspruch gem. § 7 Abs. 4 TMG nur als ultima ratio in Betracht kommt, wenn der Rechteinhaber zuvor alle ihm zumutbaren Möglichkeiten der Inanspruchnahme tatnäherer Beteiligter ausgeschöpft hat. Der BGH stellt in dieser Entscheidung klar, dass dem Rechteinhaber unter Berücksichtigung seiner wirtschaftlichen Ressourcen erhebliche Anstrengungen zur Beseitigung der Rechtsverletzung durch tatnähere Beteiligte zumutbar sind. Der BGH bestätigt zunächst seine im Rahmen der Störerhaftung entwickelten Grundsätze zur subsidiären Inanspruchnahme von Zugangsvermittlern (BGH ZUM 2016, 349, Rn. 83 – Störerhaftung des Access-Providers; BGH ZUM 2021, 148, Rn. 27 – Störerhaftung des Registrars), wonach dem Rechteinhaber die Einschaltung staatlicher Ermittlungsbehörden und privater Detektive sowie die Geltendmachung von Auskunftsansprüchen gegen den Host Provider zur Ermittlung der Identität der Betreiber der Webseite zumutbar sind (vgl. dazu ausführlich Klageerwiderung v. 29.07.2022, S. 21, 33; Duplik v. 30.01.2023, S. 32f.). Ergänzend stellt der BGH klar, dass der Rechteinhaber grundsätzlich zuvor einen Drittauskunftsanspruch gegen im EU-Ausland

ansässige Host Provider vor einem Gericht der Bundesrepublik Deutschland geltend machen muss:

„Welche Anstrengungen zur Inanspruchnahme des Betreibers der Internetseite und des Host-Providers zumutbar sind, ist eine Frage des Einzelfalls.

*(1) Der Rechtsinhaber ist in zumutbarem Umfang dazu verpflichtet, Nachforschungen zur Ermittlung der vorrangig in Anspruch zu nehmenden Beteiligten anzustellen (vgl. BT-Drucks. 18/12202, S. 12). Dies umfasst insbesondere die **Einschaltung staatlicher Ermittlungsbehörden im Wege der Strafanzeige** (vgl. BGHZ 208, 82 [juris Rn. 87] - Störerhaftung des Access-Providers) und die außergerichtliche Geltendmachung eines Anspruchs auf Drittauskunft gegenüber dem Host-Provider, um den Betreiber der Internetseite zu ermitteln. Auch die **Vornahme privater Ermittlungen etwa durch einen Detektiv** oder andere Unternehmen, die Ermittlungen im Zusammenhang mit rechtswidrigen Angeboten im Internet durchführen, ist - unter Berücksichtigung der wirtschaftlichen Ressourcen des Rechtsinhabers - grundsätzlich zumutbar (vgl. BGHZ 208, 82 [juris Rn. 87] - Störerhaftung des Access-Providers).*

(2) Die außergerichtliche Inanspruchnahme eines bekannten Betreibers der Internetseite oder Host-Providers auf Entfernung der urheberrechtsverletzenden Inhalte ist dem Rechtsinhaber im Regelfall ebenfalls zumutbar.

[...]

Ein Verfahren des einstweiligen Rechtsschutzes gegen innerhalb der Europäischen Union ansässige Betreiber oder Host-Provider hat der Rechtsinhaber jedoch grundsätzlich anzustrengen (vgl. Spindler, GRUR 2014, 826, 832; ders., GRUR 2016, 451, 458; aA J. B. Nordemann in Fromm/Nordemann aaO § 97 Rn. 171a; wohl auch Weisser/Färber, BB 2016, 776, 777). Vor dem Hintergrund des Vertrauens, das die Mitgliedstaaten der Europäischen Union gegenseitig ihren Rechtssystemen und Rechtspflegeorganen entgegenbringen (vgl. hierzu auch BGH, Beschluss vom 17. November 2021 - I ZB 16/21, IWRZ 2022, 129 [juris Rn. 39 mwN]), ist grundsätzlich davon auszugehen, dass eine einstweilige Verfügung innerhalb der Europäischen Union zügig erwirkt und vollstreckt werden kann. Soweit Staaten außerhalb der Europäischen Union betroffen sind, **muss das Vorhandensein gleichwertiger Rechtsschutzmöglichkeiten jedoch im Einzelfall geprüft werden**, ohne dass dem Antragsteller hierfür überzogene Darlegungslasten aufgebürdet werden dürfen (vgl. Spindler, GRUR 2014, 826, 832; Leistner/Grise, GRUR 2015, 105, 107 f.).

[...]

*In die Beurteilung der Zumutbarkeit fließt auch ein, dass es sich bei den Klägerinnen um große und international tätige Wissenschaftsverlage handelt, die Rechte an einer Vielzahl von Werken halten. **Mit Blick auf die Verhinderung künftiger Rechtsverletzungen steht die Ermittlung der Identität der Betreiber der Internetdienste in ihrem Eigeninteresse** (vgl. dazu BGH, Urteil vom 12. Mai 2010 - I ZR 121/08, BGHZ 185, 330 [juris Rn. 22 und 34] = GRUR 2010, 633 - Sommer unseres*

Lebens.)” (BGH, Urteil v. 13 Oktober 2022 – I ZR 111/21, GRUR 2022, 1812 – DNS-Sperre, Rn. 38 ff., 55) (Hervorhebungen durch den Unterzeichner)

Die Beklagte hat ausführlich dazu vorgetragen, dass die Klägerin keine der ihr nach dieser Rechtsprechung zumutbaren Maßnahmen ergriffen hat. Weder hat die Klägerin eine Strafanzeige erstattet, noch einen privaten Ermittler eingeschaltet, noch hat sie versucht, im Wege des Eilrechtsschutzes einen gerichtlichen Anspruch auf Drittauskunft gegen den in der EU ansässigen Host Provider geltend zu machen, noch hat sie zu Rechtsschutzmöglichkeiten am Sitz des Host Providers in der Ukraine vorgetragen, noch hat sie ausreichende Bemühungen zur Inanspruchnahme weiterer tatnäherer Beteiligten unternommen (Klageerwiderung v. 29.07.2022, S. 33 ff.; Duplik v. 30.01.2023, S. 31 ff.).

Das Landgericht nimmt rechtsirrig an, dass der Klägerin die gerichtliche Geltendmachung eines Drittauskunftsanspruchs nicht zumutbar gewesen sei (Urteil, S. 14). Eine Auseinandersetzung mit den übrigen Subsidiaritätsanforderungen des BGH (BGH, a.a.O. Rn. 38) fehlt gänzlich.

Das Landgericht verkennt, dass nach der Rechtsprechung des BGH ein Verfahren des einstweiligen Rechtsschutzes nur dann unterbleiben darf, wenn aus vom Anspruchsteller darzulegenden Gründen dem Vorgehen jede Erfolgsaussicht fehlt (BGH, a.a.O. Rn. 42). Dies hat die Klägerin nicht im Ansatz darlegen können. Die Klägerin stellte erst im gerichtlichen Verfahren fest, dass sie die Host Provider nicht hinreichend in Anspruch genommen hat. Deshalb versucht sie mit ihrem Vortrag (Replik v. 17.10.2022, S.18), dass eine Drittpartei durch einen Kurier in einer anderen Angelegenheit einem Monat vor der Inanspruchnahme der Beklagten ein Schreiben nicht zustellen konnte, den Eindruck zu erwecken, eine Zustellung sei nicht erfolgsversprechend. Aus diesem Vortrag kann nicht darauf geschlossen werden, dass einer gerichtlichen Inanspruchnahme jegliche Erfolgsaussicht fehle. Auch der BGH unterscheidet dementsprechend trennscharf zwischen dem Erfordernis der außergerichtlichen Inanspruchnahme (BGH, a.a.O. Rn. 40) und dem *zusätzlichen* Erfordernis der gerichtlichen Inanspruchnahme (BGH, a.a.O. Rn. 42) mit einer etwaigen amtlichen Zustellung innerhalb der EU.

Woraus das Landgericht die Schlussfolgerung zieht (Urteil, S. 14), dass die Anschrift des Host Providers in Litauen und damit der EU nicht festgestellt werden könne, bleibt offen. Die Beklagte hat vorgetragen, dass der Host Provider unter der im Impressum angegebenen Adresse im Handelsregister eingetragen ist, dort in den vergangenen Jahren regelmäßig Umsätze und sozialversicherungspflichtig Beschäftigte gemeldet hat (Duplik v. 30.01.2023, S. 32, Anlage B23). Die Beklagte trug bereits in der Duplik (Duplik v. 30.01.2023, S.32) vor, dass der Klägerin bei der gebotenen Durchführung eines einstweiligen Verfügungsverfahrens offen gestanden hätte, die Verfügung nach der EU-Verordnung über die Zustellung in Zivil- und Handelssachen durch eine (Verordnung (EU) 2020/1784) durch einen litauischen Gerichtsvollzieher vornehmen zu lassen. Jenseits des einzigen, erfolglosen Zustellungsversuchs, der seit Klageeinreichung zudem eine erhebliche Zeit zurück liegt, kann die Klägerin nicht davon ausgehen, dass eine erneute Zustellung bzw. eine amtliche Zustellung mittels des Gerichtsvollziehers keinen Erfolg verspricht (MMR 2023, 378, 381).

Schließlich zeigt das Vorgehen der Klägerin im einstweiligen Verfügungsverfahren gegen die Beklagten, dass die gerichtliche Zustellung gegenüber privaten Zustellversuchen eine

besondere Qualität aufweist. Die Klägerin erklärte in ihrer Klageschrift, die Beklagte habe die postalische Zustellung der einstweiligen Verfügung des Landgerichts Hamburg durch eine Angabe einer falschen Adresse im Impressum vereitelt, (Klage v. 22.04.2022, S. 10). Dies hat die Klägerin aber nicht davon abgehalten, eine einstweilige Verfügung gegen die Beklagte zu beantragen und mithilfe des Landgerichts Hamburg außerhalb der EU zustellen zu lassen. Aus dem Subsidiaritätsprinzip muss dann auch folgen, dass eine einstweilige Verfügung vorerst gegen den Host Provider beantragt werden und ein Zustellversuch, wenn nötig mithilfe einer gerichtlichen Zustellung, unternommen werden muss, bevor ein Dienst gerichtlich in Anspruch genommen wird, der wenn überhaupt nur nachrangig in Anspruch zu nehmen ist und sich ebenfalls außerhalb der EU befindet.

Hinsichtlich des Zustellversuchs in der Ukraine reichte dem Landgericht Leipzig die von der Klägerin vorgetragene Annahmeverweigerung aus, um die vorrangige Inanspruchnahme für gescheitert zu erklären (Urteil, S.14). Die Vorgaben des BGH, auch die Möglichkeiten der gerichtlichen Inanspruchnahme in Ländern außerhalb der EU zu prüfen, beachtet das Landgericht nicht. Eine Vollstreckung deutscher Gerichtsurteile in der Ukraine ist indes auch ohne Abschluss eines internationalen Vertrags über Rechtshilfe möglich (<https://berlineranwaltsblatt.de/ce/deutsche-gerichtsurteile-in-der-ukraine/detail.html>).

Die Auffassung des Landgerichts, dass die Möglichkeiten einer Inanspruchnahme erschöpft seien, wenn ein unter einer Adresse unstreitig ansässiger Anbieter lediglich eine Zustellung ablehnt, würde dazu führen, dass die vom BGH geforderte vorrangige Inanspruchnahme tatnäherer Anbieter ausgehöhlt würde. Es würde dann in die Disposition des vorrangig in Anspruch zu nehmenden gestellt, sich seiner Verantwortung zu entziehen und die Bürde des Tätigwerdens dem Tatferneren aufzuerlegen. Dies führt, wie hier geschehen, zu nicht sachgerechten Ergebnissen.

Im Übrigen ignoriert das Landgericht den gesamten Vortrag der Beklagten zu der fehlenden Inanspruchnahme weiterer tatnäherer Beteiligten (Klageerwiderung v. 29.07.2022, S. 21f. und Duplik v. 30.01.2023, S. 33) und würdigt diesen in keiner Weise. Eine Erklärung in der Urteilsbegründung des Landgerichts, weshalb eine Inanspruchnahme dieser Beteiligten nicht in Betracht kommt, fehlt auch gänzlich. Das Landgericht würdigte insbesondere nicht, dass seitens der Klägerin gegenüber RIPE keine Maßnahmen ergriffen wurden, um entweder korrekte Kontaktdaten zu erhalten, damit eine erfolgreiche Zustellung vorgenommen werden kann oder dem Host Provider die IP-Adressen entziehen zu lassen, die für die behauptete Rechtsverletzung genutzt wurden (Duplik v. 30.01.2023, S. 31).

Die Beklagte wies zudem bereits ausdrücklich daraufhin (Duplik v. 30.01.2023, S. 32), dass weder der Vertreter der Klägerin noch die von ihm zur Dokumentation der geltend gemachten Rechtsverletzung beauftragten proMedia GmbH „private Ermittler“ sind, deren Einsatz der BGH in der Entscheidung *Störerhaftung des Access Providers* gefordert hat (BGH, Urteil v. 26 November 2015 – I ZR 174/14, GRUR 2016, 268, Rn. 87 – *Störerhaftung des Access Providers*). Der BGH hat in dieser Entscheidung mit dem Einsatz privater Ermittler oder der Einschaltung staatlicher Ermittlungsbehörden ausdrücklich Maßnahmen gefordert, die über die von der Klägerin dargelegten Maßnahmen zur Ermittlung der Identität der Betreiber der Webseite hinausgehen. Dementsprechend benennt der BGH als Beispiel für „privater Ermittler“ Privatdetektive oder Unternehmen, die Ermittlungen im Zusammenhang mit Rechtsverletzungen im Internet durchführen (BGH a.a.O.). Das Landgericht ist in der

Urteilsbegründung nicht auf Mängel der Ermittlungsversuche und der unzureichenden Umstände des einmaligen Zustellversuchs, trotz ausreichender Monierung durch die Beklagte, eingegangen.

b. Inanspruchnahme wegen Unverhältnismäßigkeit ausgeschlossen

Das Landgericht hat bei der Prüfung von § 7 Abs. 4 TMG nicht berücksichtigt, dass die Norm zwingend eine Prüfung der Verhältnismäßigkeit und Zumutbarkeit der Sperrmaßnahme vorsieht. Das Landgericht würdigt weder den ausführlichen Vortrag der Beklagten zur Unverhältnismäßigkeit der Einrichtung einer DNS-Sperre wegen der Auswirkungen auf die Leistung des Systems der Beklagten und den Geschäftsbetrieb (Klageerwiderung v. 29.07.2022, S. 12 ff. 41f. ; Duplik v. 30.01.2023, S. 7ff, 35) noch den ausführlichen Vortrag der Beklagten zur Unverhältnismäßigkeit der DNS-Sperre wegen des Eingriffs in die Informationsfreiheit der Anfragenden der Beklagten (Klageerwiderung v. 29.07.2022, S. 39 ff; Duplik v. 30.01.2023, S. 33 f.).

Ergänzend wird auf sämtlichen Vortrag in der ersten Instanz Bezug genommen.

Das Urteil des Landgerichts Leipzig ist aufzuheben, und die Klage ist vollumfänglich abzuweisen.

C. Zulassung der Revision

Die Zulassung der Revision wird im Hinblick auf die Notwendigkeit der Fortbildung des Rechts oder der Sicherung einer Einheitlichkeit der Rechtsprechung nach § 543 Abs. 2 S. 1 Nr. 2 ZPO beantragt. Der Rechtsstreit berührt Fragen, zu denen sich der Bundesgerichtshof nicht oder nicht abschließend geäußert hat (z.B. die Frage der Täterschaft von haftungsprivilegierten Diensteanbietern bei nicht unverzüglicher Sperrung von Domainnamen.)

D. Übertragung der Sache auf den Einzelrichter

Da der Rechtsstreit z.T. in der höchstrichterlichen Rechtsprechung noch nicht abschließend geklärte Fragen aufwirft, erscheint eine Übertragung der Sache auf den Einzelrichter nach § 526 Abs. 1 Nr. 2 ZPO nicht angezeigt (vgl. Wiczorek/Schütze/Gerken, aaO, § 526 Rn. 5; Thomas/Putzo/Seiler, aaO § 526 Rn. 7).

Rickert Rechtsanwaltsgesellschaft mbH
durch:

Thomas Rickert
(Rechtsanwalt)