

Antrag 4/2021

Der Prüfungsausschuss
Empfehlung zur Umsetzung einer DNS-Sperre

Auf Antrag von

Antragstellerin

hat der Prüfungsausschuss durch

als Vorsitzenden

als Beisitzer

Aufgrund der Beratung in der Sitzung vom 6. April 2021 einstimmig beschlossen:

Es wird empfohlen, für die Website

NSW2U.COM,

verfügbar unter

eine DNS-Sperre umzusetzen.

Begründung:

A. Tätigkeit des Prüfungsausschusses

- I. Der Prüfungsausschuss wird tätig aufgrund Nr. 3 des Verhaltenskodexes i.V.m. §§ 6, 7 der Verfahrensordnung (Anl. 1 des Verhaltenskodexes).**
- II. Die Empfehlung zur Sperrung der Website erfolgt ausschließlich aufgrund gesetzlicher Vorschriften. Sie erfolgt nur, wenn eine klare Verletzung des deutschen Urheberrechtsgesetzes festgestellt ist.**

B. Zulässigkeit des Antrags

Der Prüfantrag ist zulässig.

Nach § 7 Abs. 3 Verfahrensordnung ist jeder Rechteinhaber antragsberechtigt, der Partei des Verhaltenskodexes ist, oder Mitglied eines Verbandes ist, der Partei des Verhaltenskodexes ist und der dem Antrag zugestimmt hat. Diese Voraussetzungen sind erfüllt. Die Antragstellerin ist Mitglied eines Verbandes, der Partei des Verhaltenskodexes ist und der dem Antrag zustimmt.

Die Prüfgebühren sind vorab entrichtet. Die Einzahlung ist belegt (Anlage I.2).

C. Begründetheit des Antrags

Der Antrag auf Empfehlung der Sperrung der Website NSW2U.com ist begründet. Die Website ist eine strukturell urheberrechtsverletzende Website. Es liegt eine klare Verletzung des Urheberrechts vor. Die Sperrung ist zumutbar und verhältnismäßig.

I. Antrag

Die Antragstellerin beantragt, für die strukturell urheberrechtsverletzende Website NSW2U.com eine DNS-Sperre gemäß dem Verhaltenskodex umzusetzen, unabhängig von dem durch die strukturell urheberrechtsverletzende Website gewählten http-Protokoll.

Bedenken hinsichtlich der Bestimmtheit des Antrags bestehen nicht.

II. Voraussetzungen der Empfehlung

Nach Art. 8 Abs. 3 der Richtlinie 2001/29/EG stellen die Mitgliedstaaten sicher, dass die Rechtsinhaber gerichtliche Anordnungen gegen Vermittler beantragen können, deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandter Schutzrechte genutzt werden. Art. 11 S. 3 der Richtlinie 2004/48/EG sieht vor, dass die Mitgliedstaaten unbeschadet des Art. 8 Abs. 3 der Richtlinie 2001/29/EG ferner sicherstellen, dass die Rechtsinhaber eine Anordnung gegen Mittelspersonen beantragen können, deren Dienste von einem Dritten zwecks Verletzung eines Rechts des geistigen Eigentums in Anspruch genommen werden. Gemäß ihrem Art. 17 Abs. 2 wird geistiges Eigentum durch die EU-Grundrechtecharta geschützt.

Zum Teil wird die Auffassung vertreten, als Rechtsgrundlagen für eine DNS-Sperre seien die Grundsätze der Störerhaftung heranzuziehen (LG München I, Urt. v. 1.2.2018 – 7 O 17752/17, CR 2018, 611 – kinox.to; für die Zeit vor Neufassung des § 7 Abs. 4 TMG durch das Dritte Gesetz zur Änderung des Telemediengesetzes vom 28.9.2017: BGH, Urt. v. 26.11.2015 – I ZR 174/14 Rn. 20 ff. – Störerhaftung des Access-Providers), teilweise wird § 7 Abs. 4 TMG direkt oder analog für einen gesetzlichen Anspruch gegen einen Zugangsanbieter zur Verhängung einer DNS-Sperre herangezogen (OLG München, Urt. v. 17.10.2019 – 29 U 1661/19, MMR 2020, 35; betreffend sog. Tor-Exit-Nodes zum TOR-Netzwerk BGH, Urt. v. 26.07.2018 – I ZR 64/17 Rn. 42 GRUR 2018, 1044 – Dead Island) oder es wird angenommen, Art. 8 Abs. 3 der Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft könne als unmittelbare Anspruchsgrundlage dienen. Daneben sieht § 109 Abs. 3 Medien-Staatsvertrag Maßnahmen gegen Diensteanbieter von fremden Inhalten nach den §§ 8 bis 10 des Telemediengesetzes vor. Die Voraussetzungen aller Rechtsgrundlagen sind weitgehend deckungsgleich.

Der Prüfungsausschuss lässt offen, ob eine DNS-Sperre gegen einen Zugangsvermittler nach den Maßstäben der Störerhaftung verhängt werden kann (zu den Grundsätzen zuletzt BGH, Urt. v. 15.10.2020 – I ZR 13/19 Rn. 12 bis 35, NJW 2021, 311 – Störerhaftung des Registrars). Der Prüfungsausschuss legt auf der Grundlage der Rechtsprechung des Bundesgerichtshofs (BGH, Urt. v. 26.07.2018 – I ZR 64/17 Rn. 42 und 45 bis 49, GRUR 2018, 1044 – Dead Island; Urt. v. 15.10.2020 – I ZR 13/19 Rn. 27, NJW 2021, 311 – Störerhaftung des Registrars) seiner Prüfung, ob die Voraussetzungen einer DNS-Sperre vorliegen, § 7 Abs. 4 TMG zugrunde. § 7 Abs. 4 TMG ist nach der Rechtsprechung für den Sperranspruch gegen den Betreiber eines Internetzugangs direkt anwendbar, wenn der Zugang drahtlos vermittelt wird; entsprechend ist er anzuwenden, wenn der Sperranspruch gegen den Betreiber eines drahtgebundenen Zugangs gerichtet ist (BGH, Urt. v. 26. 7.2018 – I ZR 64/17 GRUR 2018, 1044, Rn. 49 – Dead Island).

1. § 7 Abs. 4 TMG

Der Antrag auf Empfehlung zur Umsetzung einer DNS-Sperre ist begründet, wenn die Voraussetzungen des § 7 Abs. 4 TMG vorliegen. Wurde ein Telemediendienst von einem Nutzer in Anspruch genommen, um das Recht am geistigen Eigentum eines anderen zu verletzen und besteht für den Inhaber dieses Rechts keine andere Möglichkeit, der Verletzung seines Rechts abzuwehren, so kann der Inhaber des Rechts nach § 7 Abs. 4 S. 1 TMG von dem betroffenen Diensteanbieter nach § 8 Abs. 3 TMG die Sperrung der Nutzung von Informationen verlangen, um die Wiederholung der Rechtsverletzung zu verhindern. Die Sperrung muss zumutbar und verhältnismäßig sein, § 7 Abs. 4 S. TMG. Diensteanbieter im Sinne des § 8 Abs. 3 TMG ist ein Diensteanbieter, der Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellt. § 8 Abs. 3, § 7 Abs. 4 TMG sind beim Diensteanbieter eines drahtgebundenen Zugangs zum Internet analog anwendbar (BGH, Urt. v. 26.07.2018 – I ZR 64/17, GRUR 2018, 1044 Rn. 49 und 54 bis 57 – Dead Island).

2. Voraussetzungen für die Verhängung einer DNS-Sperre

Die Voraussetzungen für die Verhängung einer DNS-Sperre – und entsprechend die Grundsätze, die für die Empfehlung einer DNS-Sperre durch den Prüfungsausschuss mit Ausnahme der Einschränkung unter lit. c) gelten – sind danach:

- a) Der Anspruchsteller muss aktivlegitimiert sein,
- b) der Diensteanbieter muss Nutzern einen Zugang zum Internet vermitteln (diese Voraussetzung wird nachfolgend nicht weiter geprüft, weil alle Internetzugangsanbieter, die Partei des Verhaltenskodex sind, die Voraussetzung erfüllen),
- c) ein Diensteanbieter muss von einem Nutzer in Anspruch genommen werden, um das Recht am geistigen Eigentum eines anderen zu verletzen, wobei der Prüfungsausschuss eine Empfehlung zur DNS-Sperre nur dann ausspricht, wenn eine klare Rechtsverletzung vorliegt,
- d) für den Inhaber des Rechts darf keine andere Abhilfemöglichkeit bestehen und
- e) die Sperrung muss zumutbar und verhältnismäßig sein.

III. Vorliegen der Voraussetzungen

1. Aktivlegitimation des Anspruchstellers

Die Antragstellerin ist aktivlegitimiert. Sie ist Inhaberin von Urheberrechten im Hinblick auf das Öffentlich-Zugänglichmachen an Orten und zu Zeiten nach Wahl des Internetnutzers zum permanenten Download (§ 19a UrhG) und/oder zum Streaming (§ 19a UrhG) an dem am 28. April 2017 veröffentlichten urheberrechtlich geschützten Videospiel

*****,

geschaffen von ***** und ***** (S Spieleentwickler) und von den Komponisten der Musik des Spiels *****, *****, *****, *****, *****, *****, *****, *****. Sämtliche genannten Personen sind japanische Staatsangehörige und Angestellte der Antragstellerin im Rahmen von Anstellungsverträgen nach japanischem Recht; diese Angestellten haben das Werk in Erfüllung ihrer arbeitsvertraglichen Pflichten und Aufgaben geschaffen; nach § 15 des japanischen Urheberrechtsgesetzes entstehen alle Urheberrechte an Werken, die ein Angestellter in Erfüllung seiner arbeitsvertraglichen Pflichten und Aufgaben schafft, automatisch bei seinem Arbeitgeber (vgl. eidesstattliche Versicherung, Anl. II.1.).

Der Antrag bezieht sich auf eine Verletzung der ausschließlichen Rechte der Antragstellerin an dem Videospiel *****; dabei handelt es sich um einen nach § 2 Abs. 1 und 2 UrhG geschütztes Werk. Die Rechteinhaberschaft der Antragstellerin ist belegt durch die übliche Angabe ihres Namens Inhaberin ausschließlicher Rechte auf den einzelnen Vervielfältigungsstücken (§ 10 Abs. 1 UrhG) sowie durch die eidesstattliche Versicherung (Anl. II.1.)

2. Strukturell urheberrechtsverletzende Website (SUW)

Die Webseite ist zwar in englischer Sprache gehalten (Anlage II.2.4), jedoch klar auch auf den deutschsprachigen Markt ausgerichtet, da die Webseite einerseits einen Filter für deutschsprachige Inhalte enthält und zudem zahlreiche Inhalte in deutscher Sprachversion angeboten werden (Anlage II.2.5).

Die klare Rechtsverletzung besteht in dem Bereithalten von Links, um das Videospiel ***** für Nutzer über File-Hosting-Dienste verfügbar zu machen. Darin liegt eine eindeutige Verletzung des Rechts des Öffentlich-Zugänglichmachens nach § 19a UrhG (BGH GRUR 2013, 370 Rn. 16, 29 – Alone in the Dark; BGH GRUR 2013, 1030 Rn. 23 ff., 46 – File-Hosting-Dienst).

Die Website, deren Sperrung die Antragstellerin begehrt, betreibt im Hinblick auf die unerlaubte öffentliche Wiedergabe das Modell des Direct Download und setzt das kollaborative Filesharing-Protokoll BitTorrent ein. Die SUW ist unter mindestens einer Domain abrufbar (Anl. II.2.3.).

Durch die SUW wird das nach deutschem Urheberrechtsgesetz geschützte Recht verletzt, die in Ziff.1 genannte Videospiele an Orten und zu Zeiten nach Wahl des Internetnutzers zum permanenten Download öffentlich zugänglich zu machen (§ 19a UrhG).

3. Domains

Für die SUW wird eine Reihe weiterer Domains genutzt, für die die Umsetzung der DNS-Sperre beantragt wird.

4. Subsidiarität

Die Antragstellerin muss zunächst vorrangig ihre Rechte gegenüber denjenigen Beteiligten verfolgen, die – wie die Betreiber beanstandeter Websites – entweder die Rechtsverletzung selbst begangen oder zu der Rechtsverletzung – wie der Host-Provider der beanstandeten Websites – durch die Erbringung von Dienstleistungen beigetragen haben. Ein Antrag auf Sperrung einer SUW ist daher nur zulässig, wenn der Inanspruchnahme des Betreibers der Webseite jede Erfolgsaussicht fehlt und deshalb andernfalls eine Rechtsschutzlücke entstünde. Der Antragsteller muss zumutbare Maßnahmen zur Aufdeckung der Identität des Betreibers der Website unternommen haben. Hier kommen insbesondere die Einschaltung der staatlichen Ermittlungsbehörden im Wege der Strafanzeige und auch die Vornahme privater Ermittlungen etwa durch einen Detektiv oder andere Unternehmen, die Ermittlungen im Zusammenhang mit rechtswidrigen Angeboten im Internet durchführen, in Betracht (vgl. BGH, Urt. v. 26.11.2015 – I ZR 174/14, Rn. 83, 87, GRUR 2016, 268 – Störerhaftung des Access-Providers).

Diese Voraussetzung ist im vorliegenden Fall erfüllt.

Die Rechtsdurchsetzung gegenüber dem Betreiber und Hostprovider hat sich als aussichtslos erwiesen. Der Betreiber ist über Angaben auf der SUW nicht identifizierbar. Die SUW verfügt nicht über ein Impressum o.Ä. (vgl. Anlage II.5.1.1). Die Einschaltung weiterer Ermittler wurden weitere Anstrengungen unternommen, um den Betreiber der SUW zu identifizieren; auf diesem Wege konnte kein Betreiber identifiziert werden (Anl. II.5.1.2). Da die Betreiber nicht zu ermitteln sind, fehlt einer Inanspruchnahme des oder der Betreiber der SUW jede Erfolgsaussicht.

Unter den Anlagen befindet sich ein Screenshot (Anl. II.5.1.1., S. 2), wo behauptet wird, der Betreiber hoste keine urheberrechtlich geschützten Werke. Nach allfällig dennoch notwendig werdenden Beanstandungen werde der Betreiber angemessene Maßnahmen ergreifen. Da sich aus den Unterlagen, die die Antragstellerin vorgelegt hat, und aus ihrem Vortrag nicht ergab, ob die Antragstellerin dieser Anregung

nachgekommen ist, hat der Prüfungsausschuss bei dem Vertreter der Antragstellerin noch einmal nachgefragt. Dieser hat mitgeteilt, es sei versäumt worden, die entsprechende Abmahnung vorzulegen, die am 10. März 2021 ausgesprochen worden sei. Eine Kopie des Vermerks über das Gespräch, das der Vorsitzende des Prüfungsausschusses am 7. April 2021 mit dem Vertreter der Antragstellerin geführt hat sowie eine Kopie der daraufhin eingegangenen Nachricht mit der angehängten Kopie der Abmahnung ist zu den Akten genommen worden. Mit E-Mail vom 10. März 2021 hat die Antragstellerin dem Administrator von ***** mitgeteilt, sie habe Kenntnis davon erhalten, dass der Internet-Dienst ***** über eine Reihe von Domains die Möglichkeit zur Verfügung stelle, Videospiele herunterzuladen, die urheberrechtlich geschützt seien und hinsichtlich deren die Antragstellerin über die ausschließlichen Nutzungsrechte verfüge. Zusätzlich stelle ***** eine Suchmaschine zur Verfügung zum Auffinden spezifischer Videospiele. Der Internet-Dienst mache somit die Werke der Antragstellerin öffentlich zugänglich, weswegen der Antragstellerin nach deutschem Urheberrecht u.a. Unterlassungs- und Schadensersatzansprüchen zustünden. Ferner forderte die Antragstellerin den Internet-Dienst zur Abgabe einer Unterwerfungserklärung („cease and desist undertaking“) auf und setzte ihr hierfür eine Frist bis 12. März 2021, 14:00 Uhr CET. Der Vertreter der Antragstellerin hat in seiner Antwort auf die Anfrage des Vorsitzenden des Prüfungsausschusses mitgeteilt, dass der Internet-Dienst auf diese Aufforderung nicht reagiert habe.

Als Hostprovider konnten einerseits ***** (erreichbar unter ***** und *****) für die Domain ***** und ***** (erreichbar unter ***** und *****) für die weiteren Domains ermittelt werden (vgl. Anlagen II.5.2.1. und II.5.2.2.).

Die SUW nutzt den Anonymisierungsdienst Cloudflare, der auf Anfrage mitteilte, dass ***** beim niederländischen Provider ***** gehostet wird und die anderen Domains beim französischen Dienstleister ***** liegen. Auf je eine Notifizierung und anwaltliche Abmahnung reagierten beide Provider nicht. Im Übrigen ist eine Inanspruchnahme von Host-Providern stets aussichtslos, weil diese sehr einfach gewechselt werden können (sog. Hosting-Nomadismus).

Für die Antragstellerin besteht unter all diesen Umständen keine andere Möglichkeit, der Verletzung ihres Rechts entgegenzuwirken, als die Verhängung einer Sperrmaßnahme.

5. Zumutbarkeit und Verhältnismäßigkeit

Die DNS-Sperre ist zumutbar und verhältnismäßig.

Legale Inhalte, die auf einer SUW auch öffentlich wiedergegeben werden, stehen einer Einordnung als SUW nicht entgegen, wenn es sich in Bezug auf das Gesamtverhältnis

von rechtmäßigen zu rechtswidrigen Inhalten um eine nicht ins Gewicht fallende Größenordnung von legalen Inhalten handelt (vgl. BGH, Urt. v. 26.11.2015 – I ZR 174/14, Rn. 55, GRUR 2016, 268 – Störerhaftung des Access-Providers) und den Internetnutzern durch eine Sperre der Webseite nicht unnötig die Möglichkeit vorenthalten wird, in rechtmäßiger Weise Zugang zu den verfügbaren Informationen zu erlangen (vgl. EuGH, Urt. v. 27. März 2014 – C-314/12, GRUR 2014, 468 – UPC Telekabel/Constantin Film ua [kino.to] Rn. 63).

Die Verhältnismäßigkeit ist gegeben. Auf der SUW konnten im Rahmen eines sog. "Dumps", d.h. einem vollständigen Auslesen der auf der Website verfügbar gemachten Daten, ermittelt werden, dass der Anteil urheberrechtsverletzender Inhalte bei über 98 Prozent liegt (vgl. die entsprechenden Belege und statistischen Erläuterungen des privaten Ermittlungsunternehmens *****, Anlage II.3.). Damit ist die Sperrung nach den geforderten Kriterien verhältnismäßig.

6. Entscheidungen aus anderen EU-Mitgliedstaaten

Für die SUW wurde bereits in einem anderen EU-Mitgliedsstaat durch ein Gericht in Textform bestätigt, dass eine DNS-Sperre oder eine andere Sperrmaßnahme der Netzneutralitäts-Verordnung EU 2015/2120 v. 25. November 2015 nicht widerspricht: Urteil v. ***** des Handelsgerichts Nr. 6 Barcelona (Sentencia No. ***** Belege in Anl. II.2.7. [Kopie des Originals, mit englischer Übersetzung]).
