Der Prüfungsausschuss

Empfehlung zur Umsetzung einer DNS-Sperre

Auf Antrag von

*****

Antragstellerin

*****

hat der Prüfungsausschuss durch

*****

Vorsitzenden

*****

Beisitzer

Aufgrund der Beratung in der Sitzung vom 26. Juli 2021 einstimmig beschlossen:

Es wird empfohlen, für die Website

BS.TO

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 des Verbands *****, 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 BS.TO 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 BS.TO 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 abzuhelfen, 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 Urheber- oder Leistungsschutzrechten rechten unter anderem im Hinblick auf die öffentliche Wiedergabe in Form des Öffentlich-Zugänglichmachens an Orten und zu Zeiten nach Wahl des Internetnutzers zum Streaming (§ 19a UrhG) des am ***** in den USA und am ****** in Deutschland veröffentlichten Filmwerks
*****

geschaffen von dem Regisseur, dem US-amerikanische Staatsangehörigen,

*****

der in der üblichen Weise als Inhaber der ausschließlichen Rechte bei erlaubter öffentlicher Wiedergabe sowie auf Vervielfältigungsstücken (inklusive auf Verpackungen von Vervielfältigungsstücken und im Abspann von Filmwerken) bezeichnet wird (Anl. II.1.a und b; II.2.b).

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

2. Strukturell urheberrechtsverletzende Website (SUW)

Die Webseite ist in deutscher Sprache gehalten (Anlage II.2.4 und damit klar auch auf den deutschsprachigen Markt ausgerichtet.

Die klare Rechtsverletzung besteht in dem Bereithalten von Links, um die TV-Serie ***** und dessen Folge ***** für Nutzer über FileHosting-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 Streaming (on demand) . 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 Filmwerk an Orten und zu Zeiten nach Wahl des

Internetnutzers zum permanenten Download öffentlich zugänglich zu machen (§ 19a UrhG).

Für die SUW wurde bereits in einem anderen EU-Mitgliedsstaat, nämlich in Österreich, durch eine Behörde, nämlich durch die Telekom-Controll-Kommission (TKK) durch Bescheid vom 20. Juli 2020 unter dem Az. R 1/20-14, durch Bescheid vom 22. Juni 2020 unter dem Az. R 15/19-14 und durch Bescheid vom 8. Juli 2019 unter dem Az. R 7/19-22 bestätigt, dass eine DNS-Sperre der Netzneutralität-VO EU 2015/2120 vom 25. November 2015 nicht widerspricht (Anl. II. 2.8.)

3. Domains

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

*****

Für sie ist ebenfalls die DNS-Sperre beantragt.

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 Identität der Betreiber der SUW ließ sich anhand der auf der SUW bereitgestellten Informationen nicht feststellen, da Sie weder ein Impressum noch rechtliche Hinweise o.ä. enthält (Anhang II.5.1.1). Um die Identität der Betreiber der Website festzustellen, wurden daher die Diensteanbieter der SUW identifiziert und schriftlich um die

entsprechende Auskunft ersucht (Anhang II.5.1.2.b). 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). Durch 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.

Der Host-Provider lässt sich nicht identifizieren. Die SUW nutzt den in Russland ansässigen Dienst *****. Die privaten Ermittler konnten nicht aufklären, ob *****tatsächlich die SUW hostet oder nur als Content-DeliveryNetwork die Identität des wahren Host-Providers verschleiert. Zudem ist die Inanspruchnahme von Host-Providern grundsätzlich aussichtslos, da Betreiber der SUW durch einfachen Wechsel zu anderen Host-Providern die SUW weiterbetreiben könnten. Bis zum Zeitpunkt der Einreichung des Antrags erhielten die Antragsteller keine Antwort auf die an *****gerichteten Notifizierungen, Abmahnungen und Auskunftsgesuche. Ausführliche Informationen und Belege sind in Anlage II.5.2.3. enthalten.

Als Domaininhaber konnte das Unternehmen ***** identifiziert werden. Die Dienste dieses auf der ***** ansässigen Unternehmens ermöglichen eine vollständige anonyme Registrierung von Domains und verschleiern hierüber den eigentlichen Domaininhaber (Anlage II.5.1.3). Auf eine anwaltliche Abmahnung hat dieses Unternehmen nicht reagiert.

Die erhöhten Subsidiaritätsanforderungen nach dem nicht rechtskräftigen Urteil des OLG München vom 27.05.2021 (Az. 29 U 6933/19), die ggf. auch eine gerichtliche Durchsetzung von Auskunftsansprüchen gegen Host-Provider mit Sitz im EU-Ausland erfordern, sind im Streitfall nicht anwendbar, weil DDoS-Guard seinen Sitz außerhalb der EU hat.

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 einer repräsentativen Stichprobe ausschließlich urheberrechtsverletzende Inhalte aufgefunden werden. Die statistische Wahrscheinlichkeit, dass der Anteil rechtsverletzende Inhalte über 90% liegt, liegt nahe 100%. Die entsprechenden Belege und statistischen Erläuterungen sind dem Antrag in Form des Statistical Analysis Reports des Dienstleisters Incopro Ltd. als Anl. II.3. beigefügt.

***** ***** *****