

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 7. Juni 2022 einstimmig beschlossen:

Es wird empfohlen, für die Website

CINE.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 „Motion Picture Association“, der Partei des Verhaltenskodexes ist und der dem Antrag zugestimmt hat (Anlage IV).

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

C. Begründetheit des Antrags

Der Antrag auf Empfehlung der Sperrung der Website CINE.TO ist begründet. Die Website ist eine strukturell urheberrechtsverletzende Website (SUW). Es liegt eine klare Verletzung des Urheberrechts vor. Die Sperrung ist zumutbar und verhältnismäßig.

I. Antrag

Die Antragstellerin beantragt, für die strukturell urheberrechtsverletzende Website CINE.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, Ur. v. 01.02.2018 – 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 28.09.2017: BGH, Ur. v. 26.11.2015 – I ZR 174/14 GRUR 2016, 268 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, Ur. v. 17.10.2019 – 29 U 1661/19, MMR 2020, 35; betreffend sog. Tor-Exit-Nodes zum TOR-Netzwerk BGH, Ur. v. 26.07.2018 – I ZR 64/17 GRUR 2018, 1044 Rn. 42 – 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 Medienstaatsvertrag 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, Ur. v. 15.10.2020 – I ZR 13/19, NJW 2021, 311 Rn. 12 bis 35 – Störerhaftung des Registrars). Der Prüfungsausschuss legt auf der

Grundlage der Rechtsprechung des Bundesgerichtshofs (BGH, Urt. v. 26.07.2018 – I ZR 64/17, GRUR 2018, 1044 Rn. 42 und 45 bis 49 – Dead Island; Urt. v. 15.10.2020 – I ZR 13/19, NJW 2021, 311 Rn. 27 – 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. 2 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 nach der Rechtsprechung des Bundesgerichtshofs 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 Streaming (§ 19a UrhG) an dem am ***** veröffentlichten urheberrechtlich geschützten Film

*****.

Dabei handelt es sich um ein Filmwerk gem. § 2 Abs. 1 Nr. 6, Abs. 2 UrhG. Zu den Filmwerken im Sinne des § 2 Abs. 1 Nr. 6, Abs. 2 UrhG zählen Spiel- und Fernsehfilme (Loewenheim/Leistner in Schricker/Loewenheim, Urheberrecht, 6. Aufl., § 2 Rn. 215). Die Anforderungen an eine persönlich geistige Schöpfung und damit an einen urheberrechtlichen Schutz für Filmwerke sind gering. Es genügt jede individuelle Gestaltung, z.B. der Regie, die sich nicht in der bloß schematischen Aneinanderreihung von Lichtbildern erschöpft, sondern sich durch die Auswahl, Anordnung und Sammlung des Stoffes sowie durch die Art der Zusammenstellung der einzelnen Bildfolgen als das Ergebnis individuellen Schaffens darstellt (BGH, Urteil vom 24.11.1983 – I ZR 147/81, GRUR 1984, 730, 732 – Filmregisseur). Durch die Leistung der an der Filmherstellung Beteiligten kommt aufgrund der Gestaltungsmöglichkeiten des Films (Handlungsablauf, Regie, Kameraführung,

Schnitt, Szenenbild, Kostümgestaltung, Ton, Musik) eine persönlich geistige Schöpfung zustande. Spiel- und Fernsehfilme erfüllen regelmäßig die Voraussetzungen eines Filmwerks im Sinne von § 2 Abs. 1 Nr. 6 UrhG (BGH, Urteil vom 24.11.1983 – I ZR 147/81, GRUR 1984, 730, 732 - Filmregisseur). Jeder Film, der Ergebnis einer – wenn auch nur geringfügigen – gestalterischen Tätigkeit ist, genießt Schutz als Werk im Sinne des § 2 Abs. 1 Nr. 6, Abs. 2 UrhG (OLG München, Urteil vom 13.04.2017 – 6 U 3515/12, GRUR-RR 2017, 417 Rn. 22). Lediglich Bildsequenzen, denen jegliche Individualität fehlt, weil sie sich in der schematischen Aneinanderreihung von Lichtbildern erschöpfen, bei denen allein die gefilmte Wirklichkeit „Regie geführt“ hat, sind vom Werkschutz ausgenommen (OLG München, Urteil vom 13.04.2017 – 6 U 3515/12, GRUR-RR 2017, 417 Rn. 22). Der in Rede stehende Film stellt danach unproblematisch ein Filmwerk dar. Er verfügt über einen eigenen Handlungsablauf, eine Tongestaltung, eine Filmmusik sowie Regie- und Kameraführung, die dem Film eine Individualität verleihen, die über eine Aneinanderreihung von Lichtbildern deutlich hinausgehen.

Die Rechtsinhaberschaft der Antragstellerin ist belegt durch das ***** (Anlage II.1). Die Antragstellerin hat die Rechtsinhaberschaft zudem belegt durch die Anlage II.2.6 Seite 2, die die Antragstellerin im Abspann des Films als Rechtsinhaberin wie folgt ausweist: „*****“ (dazu OLG Köln, GRUR-RR 2011, 305, 306; Schulze in Dreier/Schulze, Urheberrechtsgesetz, 7. Aufl., 2022, § 10 Rn. 13, 43 f.; A. Nordemann in Fromm/Nordemann, Urheberrecht, 12. Aufl. 2018, § 10 UrhG Rn. 16).

2. Strukturell urheberrechtsverletzende Website (SUW)

Die Website ist in deutscher Sprache gehalten (Anl. II.2.4) und damit auf den deutschsprachigen Markt ausgerichtet.

Die klare Rechtsverletzung besteht im Bereithalten von Links, um den Film „*****“ für Nutzer über Fremdwebsites verfügbar zu machen (Anl. II.2.6). Darin liegt eine eindeutige Verletzung des Rechts des Öffentlich-Zugänglichmachens nach § 19a UrhG (vgl. BGH, Urt. v. 12.07.2012 – I ZR 18/11, GRUR 2013, 370 Rn. 16, 29 – Alone in the Dark; BGH, Urt. v. 15.08.2013 – I ZR 80/12, GRUR 2013, 1030 Rn. 23 ff., 46 – File-Hosting-Dienst). Durch die SUW wird das nach deutschem Urheberrechtsgesetz geschützte Recht verletzt, den in Rede stehenden Film an Orten und zu Zeiten

nach Wahl des Internetnutzers zum Streaming öffentlich zugänglich zu machen (vgl. OLG Hamburg ZUM 2009, 414, 415).

Ein auf der SUW zu dem Film „*****“ bereitgehaltener Link führte zur Cyberlocker-Website „*****“, auf der Dateispeicher und File-Sharing-Dienste angeboten werden, über die der Film am ***** im Wege des Streaming-Verfahrens angesehen werden konnte (Anl. II.2.6).

In Italien ist durch den behördlichen Bescheid der AGCOM (IT) vom 21. März 2019 – Delibera 78/19/CSP – gegen die SUW eine DNS-Sperre verhängt (Anl. II.2.7) und durch Schreiben der IGAC (Portugal) vom 8. Februar 2021 ist bestätigt worden, dass eine Sperrmaßnahme gegen die SUW der Netzneutralitäts-Verordnung nicht widerspricht (Anl. II.2.8).

3. Domains

Für die SUW werden die Domains „*****“ benutzt, die nach wie vor verfügbar sind (Anl. II.4).

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 Website 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, GRUR 2016, 268 Rn. 83, 87 – Störerhaftung des Access-Providers).

Diese Voraussetzung ist im vorliegenden Fall erfüllt.



Die Identität des Betreibers der SUW ließ sich aufgrund der auf der SUW bereitgehaltenen Informationen nicht feststellen. Sie enthält kein Impressum und keine anderen Informationen oder Hinweise, die eine Identifizierung ermöglichen (Anl. II.5.1.1). Sämtliche Ermittlungen zur Identifizierung der Betreiber der SUW brachten keine weiterführenden Erkenntnisse (Anl. II.5.1.3).

Um die Identität des Betreibers der SUW festzustellen, hat die Antragstellerin einen privaten Ermittler, *****, beauftragt, der Dienstleister der SUW ermittelt hat. Diese sind von den Rechtsanwälten der Antragstellerin auf Auskunft in Anspruch genommen worden. Ermittlungen erfolgten zu den Host-Anbietern, TLS-Zertifikat-Anbietern, Registraren und Registrierungsstellen der SUW (Anl. II.5.1.2a).

Der TLS-Zertifikatsanbieter des von der SUW verwendeten Zertifikats ist ***** (Anl. II.5.1.2a).

Der private Ermittler hat durch Whois-Abfragen als Registrar ***** identifiziert. Er hat nicht klären können, ob die Domain cine.to direkt bei ***** oder über einen anderen Registrar bei der Registrierungsstelle ***** angemeldet worden ist (Anl. II.5.1.2a).

Registrierungsstelle der Domain cine.to ist ***** (Anl. II.5.1.2a). ***** ist *****.

Die anwaltlichen Auskunftersuchen gegenüber dem TLS-Zertifikat-Provider ***** sowie gegenüber ***** als Registrar und als Registrierungsstelle führten nicht zur Identifizierung des SUW oder zu weiteren Ermittlungsansätzen (Anl. II.5.1.2b und Anl. II.5.1.3).

Die Identität des Host-Providers ließ sich nicht ermitteln (Anl. II.5.2.1). Die SUW nutzt die Dienste von *****, einem Unternehmen mit Sitz in *****, dem die IP-Adresse ***** zugeordnet werden konnte, die für cine.to in Anspruch genommen worden ist (Anl. II.5.2.1). Kontaktperson und CEO von ***** ist nach den Ermittlungen ***** (Anl. II.5.2.1; Anl. II.5.2.2). Ob ***** selbst Host-Provider ist oder den Host-Provider verschleiert, konnte nicht festgestellt werden (Anl. II.5.2.3). ***** wurde unter den ermittelten E-Mail-Adressen „*****“ am ***** erfolglos anwaltlich notifiziert und am ***** erfolglos abgemahnt (Anl. II.5.2.3). Die Notifizierung und die Abmahnung von ***** brachten keine Erkenntnisse über den Betreiber der SUW und führten nicht

zu einer Beendigung der Rechtsverletzungen. ***** hat seinen Sitz in *****. Die Inanspruchnahme in ***** bietet keine Aussicht auf Erfolg.

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, GRUR 2016, 268 Rn. 55 – 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 Rn. 63 – UPC Telekabel/Constantin Film ua [kino.to]).

Die Verhältnismäßigkeit ist vorliegend gegeben. Auf der SUW konnten im Rahmen einer Zufallsstichprobe von 100 Eintragungen aus der Grundgesamtheit aller Inhalte eine große Mehrheit als klare Urheberrechtsverletzungen ermittelt werden (Anl. II.3). Mit einer statistischen Wahrscheinlichkeit von 95,5 % liegt der Anteil urheberrechtswidriger Inhalte an der Grundgesamtheit zwischen 96,28 % und 100 % (Anl. II.3).
