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 2. April 2024 einstimmig beschlossen:

Es wird empfohlen, für die Website

ZIPERTO.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 des Verbands „game – Verband der Deutschen Games-Branche e.V.“, der Partei des Verhaltenskodexes ist und der dem Antrag zugestimmt hat (Anlage IV).

Die Prüfgebühren für den 2. Antrag sind vorab entrichtet. Die Einzahlung ist belegt.

C. Begründetheit des Antrags

Der Antrag auf Empfehlung der Sperrung der Website ZIPERTO.COM 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 ZIPERTO.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. 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, Urt. 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 (BGH, Urt. v. 13.10.2022 – I ZR 111/21, GRUR 2022, 1812 Rn. 18 und 19 – DNS-Sperre; 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 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, Urt. 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; BGH, Urt. v. 13.10.2022 – I ZR 111/21, GRUR 2022, 1812 Rn. 18 bis 21 – DNS-Sperre) 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; BGH, Urt. v. 13.10.2022 – I ZR 111/21, GRUR 2022, 1812 Rn. 21 – DNS-Sperre).

Daran hat sich durch das Inkrafttreten der Vorschriften der Verordnung (EU) 2022/2065 über einen Binnenmarkt für digitale Dienste (Digital Services Act) am 17.02.2024 nichts geändert. Zwar sieht der Gesetzentwurf der Bundesregierung vom 22.12.2023 zur Durchführung der Verordnung (EU) 2022/2065 (BR-Drucks. 676/23) in § 8 eine neue Rechtsgrundlage für den Anspruch auf Sperrung bei einer Rechtsverletzung vor. Die Bestimmungen sind aber noch nicht in Kraft getreten. Bis dies der Fall ist, ist die Vorschrift des § 7 Abs. 4 TMG für die Übergangszeit weiter direkt oder analog Rechtsgrundlage für den Sperranspruch.

Die Vorschriften der Verordnung (EU) 2022/2065 stehen einer nationalen Regelung, durch die die Vorgaben des Art. 8 Abs. 3 der Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft und des Art. 11 Satz 3 der Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums umgesetzt werden, nicht entgegen (Begründung des Regierungsentwurfs vom 22.12.2023 zur Durchführung der Verordnung (EU) 2022/2065 (BR-Drucks. 676/23 S. 75).

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. 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; BGH, Urt. v. 13.10.2022 – I ZR 111/21, GRUR 2022, 1812 Rn. 18 bis 25 – DNS-Sperre).

Dies entspricht inhaltlich den Vorgaben des § 8 Abs. 1 und 2 des Gesetzentwurfs der Bundesregierung vom 22. Dezember 2023 zur Durchführung der Verordnung (EU) 2022/2065. Diese Bestimmung sieht im Entwurf vor, dass der Inhaber eines Rechts am geistigen Eigentum in einem Fall, in dem ein digitaler Dienst, der darin besteht, von einem Nutzer bereitgestellte Informationen in einem Kommunikationsnetz zu übermitteln oder den Zugang zu einem Kommunikationsnetz zu vermitteln, von einem Nutzer in Anspruch genommen wurde, um das Recht am geistigen Eigentum zu verletzen, von dem betroffenen Diensteanbieter die Sperrung der Nutzung von Informationen verlangen kann, um die Wiederholung der Rechtsverletzung zu verhindern, wenn der Rechteinhaber über keine andere Möglichkeit verfügt, der Verletzung seines Rechts abzuhelfen, und wenn die Sperrung zumutbar und verhältnismäßig ist.

„Digitaler Dienst“ ist nach § 1 Abs. 4 Nr. 1 des Gesetzentwurfs ein Dienst i.S.d. Art. 1 Abs. 1 lit. b der Richtline (EU) 2015/1535 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft. Nach Art. 1 Abs. 1 lit. b der Richtline (EU) 2015/1535 ist „Dienst“ eine Dienstleistung der Informationsgesellschaft, d. h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung. Darunter fällt ein Dienst, der Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellt oder einen drahtgebundenen Zugang zum Internet eröffnet. Auf die Bestimmung des Art. 1 Abs. 1 lit. b der Richtline (EU) 2015/1535 stellt auch Art. 3 lit. a der Verordnung (EU) 2022/2065 zur Definition des Dienstes der Informationsgesellschaft ab. Danach steht die Bestimmung des § 7 Abs. 4 TMG auch insoweit mit der Verordnung (EU) 2022/2065 und der Regelung des § 8 Abs. 1 und 2 des Entwurfs in Einklang.

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 von Orten und zu Zeiten nach Wahl des Internetnutzers zum permanenten Download (§ 19a UrhG) an dem am ***** veröffentlichten urheberechtlich geschützten Videospiel

*****

geschaffen von den Spieleentwicklern ***** und den Komponisten der Musik *****. Die vorgenannten Personen sind ***** Staatsangehörige und Angestellte der Antragstellerin aufgrund von Anstellungsverträgen nach ***** Recht. Diese Angestellten haben das Werk in Erfüllung arbeitsvertraglicher Pflichten und Aufgaben geschaffen. Nach ***** des ***** Urheberrechtsgesetzes entstehen alle Urheberrechte an Werken, die ein Angestellter in Erfüllung seiner arbeitsvertraglichen Pflichten und Aufgaben schafft, automatisch bei seinem Arbeitgeber (hierzu eidesstattliche Versicherung des Rechtsanwalts ***** vom *****, Anl. II.1).

Der Antrag bezieht sich auf eine Verletzung der ausschließlichen Rechte der Antragstellerin an dem Videospiel *****. Dabei handelt es sich um ein nach § 2 Abs. 1 Nr. 1, 2 und 6, Abs. 2 UrhG geschütztes Werk (BGH, Urt. v. 6.10.2016 – I ZR 25/15, GRUR 2017, 266 Rn. 34 - World of Warcraft I; OLG Köln, GRUR 1992, 312, 313; Bullinger/Czychowski GRUR 2011, 19, 23 f).

Die Rechtsinhaberschaft der Antragstellerin ist belegt durch die übliche Angabe ihres Namens als Urheberin des erschienenen Werks auf den Vervielfältigungsstücken nach § 10 Abs. 1 UrhG (©-Vermerk auf den Vervielfältigungsstücken; hierzu LG Hamburg, Urteil vom 20.07.2012 – 308 O 76/11, BeckRS 2012, 212015 Rn. 42) sowie durch eidesstattliche Versicherung (Anl. II.1).

2. Strukturell urheberrechtsverletzende Website (SUW)

Die Website ist in englischer Sprache gehalten (Anl. II.2.4). Sie ist gleichwohl auf den deutschsprachigen Markt ausgerichtet (Anl. II.2.5). Die Seite bietet eine Suchfunktion für bestimmte Seiteninhalte an. Bei Eingabe des Begriffs „German“ in das Suchfeld werden Suchergebnisse angezeigt, die eine deutsche Sprachfassung oder die den Begriff „german“ im Namen aufweisen.

Zu dem Suchbegriff „German“ lieferte die Suchfunktion der SUW 3.205 Ergebnisse. Bei diesen über die Suchfunktion mit dem Begriff „German“ aufgerufenen Ergebnissen wies die weit überwiegende Zahl eine deutsche Sprachfassung auf und nur vereinzelte Suchergebnisse trugen den Begriff „german“ im Namen.

Eine statistische Auswertung der Nutzerzahlen für die SUW ZIPERTO.COM ergab folgendes Bild (Anl. II.2.5):

Die SUW ZIPERTO.COM belegte auf der Grundlage der vom Internetdienst ***** ermittelten Nutzerzahlen im ***** den Rang 27.842 der in Deutschland am häufigsten aufgerufenen Websites und weltweit Rang 35.644. Von ***** bis ***** erfolgten 325.613 Seitenbesuche von Deutschland aus. In diesem Zeitraum stellten deutsche Nutzer mit 5,13 % die viertgrößte Gruppe der Nutzer der SUW nach den Vereinigten Staaten, Indonesien und Japan dar.

Die klare Rechtsverletzung besteht im Bereithalten von Links, um das Videospiel „*****“ für Nutzer über File-Hosting-Dienste verfügbar zu machen (Anl. II.2.6). Darin liegt eine eindeutige Verletzung des Rechts des Öffentlich-Zugänglichmachens nach § 19a UrhG (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, das in Rede stehende Videospiel von Orten und zu Zeiten nach Wahl des Internetnutzers zum permanenten Download öffentlich zugänglich zu machen.

Ein auf der SUW zu dem Videospiel „*****“ bereitgehaltener Link führte zunächst zu einer Internetseite von ***** und von dort zum Webspeicheranbieter „*****“, wo Dateien zum Hauptspiel des Videospiels heruntergeladen und nach erfolgreichem Download entpackt werden konnten (Anl. II.2.6). Nach dem Entpacken konnte das Videospiel „*****“ auf der Spielekonsole „*****“ installiert und gespielt werden.

Gegen die Website besteht bereits in einem anderen Mitgliedstaat der EU, und zwar in Italien, eine behördlich angeordnete DNS-Sperre aufgrund der Entscheidung der Autorità per le garanzie nelle comunicazioni vom 15. April 2021 Nr. 191/21/DDA (Anl. II.2.7).

3. Domains

Für die SUW werden die Domains ***** benutzt, die nach wie vor verfügbar ist (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; Urt. v. 13.10.2022 – I ZR 111/21, GRUR 2022, 1812 Rn. 27 – 31, 39 – DNS-Sperre).

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 weiterführenden Informationen oder Hinweise, die eine Identifizierung ermöglichen (Anl. II.5.1.1).

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. Ermittelt wurden Daten zu den Host-Providern, TLS-Zertifikat-Providern, Registraren und Registrierungsstellen der SUW (Anl. II.5.1.2a).

Der Aussteller und Zertifikatsinhaber des von der SUW verwendeten Zertifikats war ***** (Anl. II.5.1.2a). Seit dem ***** setzt die SUW kein Sicherheitszertifikat mehr ein.

Die SUW nutzt den ***** Registrar „*****“ (Anl. II.5.1.2a und Anl. II.5.1.2b). Die Registrierungsstelle der Domain ist „*****“ (Anl. II.5.1.2a und Anl. II.5.1.2b). Registrant (Domaininhaber) der Domain „*****“ ist der Whois-Protection-Service „***** “ (Anl. II.5.1.2a).

Die anwaltlichen Auskunftsersuchen gegenüber dem Registrar, der Registrierungsstelle und dem Registranten führten nicht zur Identifizierung des Betreibers der SUW oder zu weiteren Ermittlungsansätzen (Anl. II.5.1.2b und Anl. II.5.1.3).

Über einen Metadaten-Sammler hat der private Ermittler der Antragstellerin Informationen über einen möglichen Betreiber von ZIPERTO.COM aus dem Jahr ***** festgestellt. Die ermittelten Informationen führten zu einer nicht existenten Anschrift (Anl. II.5.1.2a). Eine anwaltliche Abmahnung über eine E-Mail-Adresse brachte keinen Erfolg (Anl. II.5.1.3).

Der Betreiber der SUW ist über Angaben auf der SUW oder sonstige Erkenntnisse aus dem Ermittlungsverfahren nicht zu identifizieren (Anl. II.5.1.3). Anwaltliche Abmahnungen über ein Kontaktformular und eine E-Mail-Adresse waren erfolglos (Anl. II.5.1.3).

„*****“ mit Sitz in ***** konnte durch den privaten Ermittler als Host-Provider festgestellt werden (Anl. II.5.2.1). Der Host-Provider wurde anwaltlich erfolglos am ***** und ***** notifiziert und am ***** ebenfalls erfolglos abgemahnt (Anl. II.5.2.3). Die Antragstellerin hat den in ***** ansässigen Hostprovider im Wege des Verfügungsverfahrens vor dem Landgericht ***** auf Auskunft in Anspruch genommen und eine einstweilige Verfügung des Gerichts vom ***** erwirkt, durch die dem Host-Provider aufgegeben worden ist, Auskunft über die Namen und Anschriften aller Personen mitzuteilen, für die die Antragsgegnerin Dienstleistungen in Bezug auf die unter den Domains ***** gehosteten Internetangebote betreffend das Computerspiel „*****“ erbracht hat (Anlage 2 EV-Antrag, Anlage 3 EV Beschluss). Bei „*****“ handelt es sich um ein weiteres urheberrechtlich geschütztes Computerspiel der Antragstellerin (Anlage 2 EV-Antrag, Anlage 3 EV Beschluss). Die einstweilige Verfügung ist dem Host-Provider zugestellt worden (Anlagen 4 und 5). Zusätzlich ist der Host-Provider von den Anwälten der Antragstellerin am ***** notifiziert und am ***** abgemahnt worden (Anl. II.5.2.3 neu). Auch die erneute Notifizierung und Abmahnung des Host-Providers und die Zustellung der gegen ihn ergangenen einstweiligen Verfügung brachten keine Erkenntnisse über den Betreiber der SUW und führten nicht zu einer Beendigung der Rechtsverletzungen. Eine Zwangsvollstreckung ist wegen der unklaren Rechtslage im Hinblick auf deren Durchführung in ***** (Schreiben der Rechtsanwälte ***** vom ***** Abschnitt II) und der damit verbundenen Verzögerung unzumutbar und käme einer Rechtsschutzverweigerung

gleich. Einer weiteren Inanspruchnahme des Host-Providers fehlt jegliche Erfolgsaussicht (Anl. II.5.2.3 neu). Zudem ist die Inanspruchnahme von Host-Providern zur Beendigung der Rechtsverletzung regelmäßig ungeeignet. Betreiber der SUW können durch einfachen Wechsel zu anderen Host-Providern die SUW weiter betreiben.

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 gegeben. Auf der SUW konnten im Rahmen einer repräsentativen Stichprobe von 100 Eintragungen aus der um Duplikate bereinigten Grundgesamtheit aller Inhalte von 8.084 Einträgen 100 von 100 Eintragungen der repräsentativen Stichprobe als klare Urheberrechtsverletzungen ermittelt werden (Anl. II.3). Mit einer statistischen Wahrscheinlichkeit von 95,5 % liegt der Anteil urheberrechtswidriger Inhalte an der Grundgesamtheit zwischen mindestens 97,2 % und 100 %. Dieses Ergebnis hat der Geschäftsführer ***** des Internetermittlers ***** im Rahmen eines Statistical Analysis Reports ermittelt. Ausweislich des Reports ist das Ergebnis von dem Sachverständigen für Rechtsforschung ***** bestätigt worden (Anl. II.3).

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