
Datum: 09.10.2020
Gericht: Oberlandesgericht Köln
Spruchkörper: 6. Zivilsenat
Entscheidungsart: Urteil
Aktenzeichen: 6 U 32/20
ECLI: ECLI:DE:OLGK:2020:1009.6U32.20.00

Vorinstanz: Landgericht Köln, 14 O 171/19

Tenor:

I. Die Berufung der Antragsgegnerin gegen das Urteil des Landgerichts Köln vom 30.1.2020 – 14 O 171/19 – wird zurückgewiesen. Die Anschlussberufung der Antragstellerin vom 11.7.2020 wird als unzulässig verworfen.

II. Die Kosten des Rechtsstreits beider Instanzen haben die Antragstellerin zu 1/3 und die Antragsgegnerin zu 2/3 zu tragen.

Gründe

- I. 1
- Die Antragstellerin ist eine bekannte Tonträgerherstellerin, die u.a. das am 31.5.2019 veröffentlichte Musikalbum HERZ KRAFT WERKE der Künstlerin Sarah Connor vertreibt. 2
- Die Antragsgegnerin bietet verschiedene Dienstleistungen im Internet an, u.a. als Nameserver, Betreiberin eines Netzwerks entsprechend dem eines Content-Delivery-Networks (CDN) sowie als Anbieterin von sog. DNS-Resolvern für Internetnutzer. Zur Funktionsweise dieser Dienstleistungen wird auf die Ausführungen im angefochtenen Urteil sowie ergänzend auf das Vorbringen der Parteien in ihren Schriftsätzen nebst Anlagen Bezug genommen. 3
- Bereits am 5.6.2019 war das o.g. Album als „Album der Woche“ u.a. unter Verweis auf die Seite Nitroflare wie im Tenor des angefochtenen Urteils wiedergegeben über die Seite „ddl-music.to“ abrufbar. Die Seite „ddl-music.to“ war Vertragspartnerin der Antragsgegnerin und nahm deren CDN-Dienstleistungen in Anspruch. Die Antragsgegnerin war für diese als 4
- 5

autoritativer Nameserver registriert.

Mit Urteil vom 31.1.2020 (Bl. 564 ff./25 ff. eA), auf das wegen der weiteren Einzelheiten und tatsächlichen Feststellungen gem. § 540 Abs. 1 S. 1 Nr. 1 ZPO verwiesen wird, hat das Landgericht die Antragsgegnerin als Störerin gem. dem 2. Hilfsantrag (Antrag zu 1c) sowie gem. den Anträgen zu 2 und 3 sinngemäß wie folgt verurteilt: 6

Der Antragsgegnerin wird im Wege der einstweiligen Verfügung verboten, 7

I. 8

1) es Dritten in der BRD zu ermöglichen das o.g. Werk bzw. die Deluxe Edition über den gegenwärtig „DDL-Music“ genannten Internetdienst wie mit der Domain „ddl-music.to“ öffentlich zugänglich zu machen wie geschehen unter den im Tenor des angefochtenen Urteils wiedergegebenen Hyperlinks; 9

2) in der BRD durch die Domain Name Server auf das o.g. Musikalbum über den gegenwärtig „DDL-Music“ genannten Internetdienst wie mit der Domain „ddl-music.to“ zu verweisen, wie geschehen unter den im Tenor des angefochtenen Urteils wiedergegebenen Hyperlinks. 10

II. Der Antragsgegnerin wird aufgegeben, Auskunft zu erteilen über Name und Anschrift der Betreiber des „DDL-Music“ genannten Dienstes, der am 5.6.2019 unter der Domain „ddl-music.to“ abrufbar war. 11

Im Übrigen (Haftung als Täter und Haftung als Gehilfe) hat das Landgericht den Antrag auf Erlass einer einstweiligen Verfügung zurückgewiesen. 12

Mit ihrer Berufung rügt die Antragsgegnerin, dass bereits die tatsächlichen Feststellungen des Landgerichts fehlerhaft seien, wie aus dem Tatbestandsberichtigungsantrag ersichtlich. 13

Die Aktivlegitimation der Antragstellerin ist unstreitig gestellt, die Verurteilung zur Auskunft nicht Gegenstand der Berufung. 14

Die Antragsgegnerin behauptet, dass sie Webseiten keinen Zugang zum Internet anbiete und auch deren Inhalte nicht hoste. Sie habe keine Kontrolle über den Inhalt von Webseiten, deren Betreiber ihre Dienste nutzten. Diese Webseiten seien auch ohne die Dienste der Beklagten weiter abrufbar. 15

Ihr CDN-Angebot richte sich an Betreiber von Webseiten und biete Infrastrukturleistungen zu Sicherheit und Performancesteigerung; der öffentliche DNS-Resolver sei ein kostenloser Dienst für einzelne Internetnutzer und biete diesen, wenn sie im World Wide Web bestimmte Webseiten aufrufen wollten, eine weltweite und schnelle Leistung zur Unterstützung bei der Auflösung von Domainnamen in numerische IP-Adressen aus dem von vielen unterschiedlichen Betreibern operierten Domain-Name-System an. 16

Ihr CDN-System schütze die Webseiten ihrer Kunden gegen Internetangriffe (Viren, Würmer, Botnet-Angriffe, DDoS), indem sie sich in den in beide Richtungen fließenden Datenverkehr zwischen der Webseite des Kunden (dem Server) und Internnutzern (Clients), die auf die Seite zugreifen wollen, einklinke. Der gesamte Datenverkehr müsse dazu über das Netzwerk der Antragsgegnerin laufen. Wenn ein Nutzer die Webseite eines Kunden aufrufen wolle, durchlaufe der Datenverkehr dieses Internetnutzers zunächst das Netzwerk der Antragsgegnerin. Bei großen Datenmengen steigere die Antragsgegnerin die Effizienz und 17

reduziere die Belastung der Netzwerke der Kunden, indem sie die Anzahl der Vorgänge, bei denen D. die identischen Daten von den Kunden abholen und an die Nutzer weiterleiten müsse, reduziere. Zu diesem Zweck könne das System der Antragsgegnerin gelegentlich Daten oder Informationen von den Webseiten der Kunden an einem bestimmten Punkt im Netzwerk (Point of Presence) vorübergehend speichern, wenn es zahlreiche und häufige Anfragen nach den Daten oder Informationen über diesen Point of Presence erhalte. Dann würden die angefragten Daten von diesem Punkt aus sofort an den Internetnutzer geliefert, wodurch Übertragungswege gespart würden und die Übertragungszeit verkürzt werde (= System-Caching). Dabei sei diese Speicherung nur vorübergehend. Wenn eine Webseite angefragte Inhalte übermittele, würde im sog. http-Header der Antwort zugleich angegeben, wie lange (Sekunden, Minuten, Stunden) der Inhalt gecacht werden kann (sog. Time-to-live). Da Inhalte auf den Ausgangsseiten sich änderten und es gewährleistet sein müsse, dass der Inhalt im Cache und auf der Ausgangsseite übereinstimme, müsse nach Ablauf des Time-to-Live der Cache den Inhalt entfernen.

Der DNS-Resolver sei eine Art Schnittstelle zwischen einer Anwendung und den von vielen unterschiedlichen Anbietern betriebenen Nameservern. Eine DNS-Sperre sei mit dem öffentlichen DNS-Resolver der Antragsgegnerin nicht vereinbar. Denn ein solcher Filter müsse für jede der – im Fall der Beklagten – täglich 200 Milliarden Anfragen an den DNS-Resolver angewendet werden, um zu prüfen, ob die Auflösung einer bestimmten Webseite angefragt wird. Solche Filterungen hätten erhebliche Auswirkungen auf die Latenz und führten zu einer schlechten Performance (Bl. 85 eA). Dies sei ihr auch deshalb nicht zuzumuten, weil eine Sperrung notwendigerweise in der gegenwärtigen Umsetzung weltweit erfolgen müsse. Eine Sperre auf geographischer Basis sei nicht möglich. Des weiteren sei eine Sperre der gesamten Domain nicht nur unverhältnismäßig im Sinne eines „overblocking“, sondern auch unwirksam, weil Internetnutzer für den Zugriff ohne weiteres andere DNS-Resolver als den der Antragsgegnerin wählen könnten. 18

Fehlerhaft sei die Annahme, dass es unstreitig sei, dass es sich bei der Seite ddl-music.to um eine strukturell urheberrechtsverletzende Seite handele. Das sei mit Nichtwissen bestritten worden. 19

Das Landgericht sei davon ausgegangen, dass mit einfachen technischen Mitteln wie Wortfiltern die eingeschränkte Auflösung der Domain mittels des DNS-Resolvers möglich sei. Dies sei weder unstreitiger noch glaubhaft gemachter Parteivortrag, sondern reine Vermutung. 20

Die Antragstellerin habe schließlich unstreitig nicht einmal versucht, den ihr bekannten Host-Provider zu kontaktieren. Es sei eine unzulässige Tatsachenschöpfung, wenn das Landgericht annehme, dass effektiver und zeitnaher Rechtsschutz in Russland oder Pakistan nicht gewährleistet sei. 21

Weiter sei die Darlegungs- und Beweislast verkannt worden. Nicht die Antragsgegnerin sei darlegungsbelastet für das Eingreifen der Haftungsprivilegierung nach §§ 8 ff. TMG, sondern nach BGH handele es sich bei den Voraussetzungen der Verantwortlichkeit nach dem TMG um anspruchsbegründende Merkmale, die der Kläger darzulegen und zu beweisen habe (noch zum TDG BGH GRUR 2004, 74 – rassistische Hetze). 22

§ 9 TMG sei vom Landgericht nicht geprüft worden, obwohl die Antragsgegnerin darauf hingewiesen habe, dass ihre Dienste unter § 8 und/oder § 9 TMG fielen. In Bezug auf die Performancesteigerung durch Zwischenspeicherung sei dieser Aspekt geradezu ein Musterbeispiel eines Caching-Dienstes iSd § 9 TMG. Die Erweiterung der Sicherheit und 23

Kapazität dürfe kein höheres Haftungsrisiko nach sich ziehen, wolle man das Wachstum des Internets nicht erheblich beeinträchtigen.

Im Rahmen der Prüfung des § 8 TMG gehe das Landgericht davon aus, dass nur eine „flüchtige“ Speicherung/Caching privilegiert sei, obwohl „flüchtig“ kein Kriterium der Haftungsprivilegierung darstelle. Es werde von § 8 TMG eine „automatische kurzzeitige Zwischenspeicherung“ verlangt, woraus folge, dass eine Speicherung nach § 9 TMG wesentlich länger erfolgen dürfe. Eine feste Zeitdauer lasse sich weder § 9 TMG noch der e-Commerce-RL nebst Erwägungsgründen entnehmen (mit Verweis auf Hoffmann/Volkmann in: Spindler/Schuster: Recht der elektronischen Medien, 4. Aufl. 2019, § 9 TMG Rn. 12) (Bl. 93 eA). Unabhängig von der gespeicherten Menge greife § 9 TMG, weil keine Umfangsbegrenzung enthalten sei. Das Ziel, Internetkapazitäten zu erhöhen, würde konterkariert, wenn die Haftungsprivilegierung des § 9 TMG nur das absolute Minimum an Zwischenspeicherung erfasste. 24

Sie habe nicht – wie das Landgericht angenommen habe – vorgetragen, „so viel wie möglich“ auf lokalen Speichern des CDN zu speichern, sondern nur, dass dem anfragenden Nutzer, so viel wie möglich vom Proxy-Cache Server zur Verfügung gestellt werde. Nur so sei die Eigenwerbung „Das D. Rechenzentrum unter xx.xx.xx.xx stellt so viel wie möglich von Ihrer Webseite von seinem lokalen Speicher zur Verfügung und fragt Ihren Webserver unter 1.1.1.1 für die übrigen Teile Ihrer Webseite, die es nicht bereits lokal gespeichert hat“ zu verstehen. 25

Außerdem speichere sie datenintensive Inhalte wie Audio- und Videodateien grundsätzlich nicht. 26

Das Vorhalten von Information auch für den Fall vorübergehender Nichterreichbarkeit einer Webseite sei das Kernmerkmal des Caching. Dabei werde jedoch keine Auswahl oder Veränderung vorgenommen. Als Veränderung würden nicht Eingriffe technischer Art im Verlauf der Übermittlung gelten, da sie die Integrität der übermittelten Informationen nicht veränderten (BT-Drs. 14/6098, S. 25). Entscheidend sei, dass keine inhaltlichen Veränderungen vorgenommen würden, sodass die Kopie dem Original entspreche. 27

Auch wenn – was streitig sei – die Inhalte der Seite „ddl-music.to“ erreichbar gewesen sein sollten, während die Webseite ihren Host-Provider wechselte, wäre dies ein Fall des § 9 S. 1 Nr. 5 TMG. Solange der Caching-Provider keine Kenntnis von der Entfernung der Inhalte am Ursprungsort habe, könne er sich auch auf die Haftungsprivilegierung stützen (BT-Drs. 14/6098, S. 25). Entscheidend für ein Tätigwerdenmüssen sei die positive Kenntnis davon, dass die Inhalte am Ursprungsort entfernt wurden (Spindler, aaO, Rn. 28). 28

Selbst wenn § 9 TMG nicht eingriffe, greife jedenfalls keine Störerhaftung. Ein CDN sei kein Hosting-Dienst. Die dazu ergangene Rechtsprechung sei nicht anwendbar. 29

Der Kläger trage die Darlegungs- und Beweislast, was möglich und zumutbar sei, um Rechtsverletzungen abzustellen. Dass zB Wortfilter eingesetzt werden könnten, habe die Antragstellerin nicht in Bezug auf die Antragsgegnerin, sondern auf die Betreiber der Webseite behauptet (Antrag v. 26.6.2019 S. 17). 30

Die Behauptung, die Dienste der Antragsgegnerin seien näher an der streitgegenständlichen Rechtsverletzung als die des Hostproviders, sei fehlerhaft. Die Antragsgegnerin habe keine direkte Möglichkeit der Unterbindung im Internet öffentlich zugänglich gemachter urheberrechtlich geschützter Inhalte. Die Anonymisierung von IP-Adressen stelle eine 31

urheberrechtlich neutrale Handlung dar ohne Bezug zu Inhalten auf einer bestimmten Webseite. Sie habe ein automatisiertes System eingerichtet, das Informationen zur Identifizierung des Host-Providers bereitstelle und unterhalte das „Trusted Reporter Programm“, das vertrauenswürdigen Rechteinhabern weitergehende Auskunft über die Webseiten erteile. Darüber hätte die Antragstellerin weitere Informationen bekommen können.

Die Antragsgegnerin habe nach Erhalt des erstinstanzlichen Urteils wegen eines Musikalbums die gesamte Webseite ddl-music.to für Nutzer mit einer IP-Adresse aus Deutschland gesperrt, weil ihr eine werkbezogene Umsetzung nicht möglich sei. Dadurch bestehe die Gefahr des Overblockings, indem die Antragsgegnerin unter Vorhalt einzelner Urheberrechtsverletzungen auf einer Webseite gedrängt würde, eine Webseite insgesamt zu blockieren.

32

Die Blockierung sei auch unwirksam, weil innerhalb weniger Tage ddl-music.to die Nutzung der Dienste der Beklagten einfach eingestellt habe, die Seite aber immer noch in Deutschland zugänglich sei. Dies zeige, dass die Antragsgegnerin keine Möglichkeit habe, die Urheberrechtsverletzung eines ihrer Kunden abzustellen. Auch wenn ihre Dienste nicht genutzt würden, bliebe die Verletzung bestehen.

33

Nach der Rechtsprechung des BGH sei die Haftung des Störers als subsidiär anzusehen, wenn nur gegen einen einzigen Webseitenbetreiber vorgegangen werden müsse (vgl. BGH GRUR 2016, 268 Rn. 81 ff. - Störerhaftung des Access-Providers). Die Rechtsprechung zu Host-Providern greife nicht, weil die Antragsgegnerin weder eine Internetplattform betreibe, auf die eine Vielzahl unterschiedlicher Anbieter Inhalte einstellten noch die Antragstellerin gegen eine Vielzahl unterschiedlicher Webseitenanbieter vorgehen müsse.

34

Das Landgericht habe sich bei der Prüfung des Antrags zu 2 (DNS-Resolver) nicht mit § 8 TMG auseinandergesetzt. Der DNS-Resolver werde Internetnutzern zur Verfügung gestellt, um URLs in IP-Adressen zu übersetzen. Der DNS-Resolver sei unabhängig von den CDN-Leistungen. Eine Störerhaftung scheide schon wegen § 8 Abs. 1 S. 2 TMG aus.

35

Hilfsweise gäbe es keinen adäquat kausalen Beitrag iSd Störerhaftung. Zwischen einer Urheberrechtsverletzung durch öffentliches Zugänglichmachen des Musikalbums durch Hyperlink von ddl-music.to auf einer Drittseite und dem Betrieb des DNS-Resolvers gäbe es nicht einmal eine Kausalität. Die öffentliche Zugänglichmachung geschehe unabhängig vom DNS-Resolver der Antragsgegnerin auf einer Unterseite von „ddl-music.to“ oder auf Drittseiten. § 19 a UrhG sei bereits erfüllt, wenn das Werk zum Abruf im Internet bereitgehalten werde (so Dustmann/Engels in: Fromm/Nordemann, Urheberrecht, 12. Aufl. 2018, 19a Rn. 7). Es komme nicht darauf an, dass tatsächlich abgerufen werde (EuGH GRUR 2018, 911 Rn. 20 – Renckhoff). Für die öffentliche Zugänglichmachung durch den Betreiber einer Webseite sei es gerade nicht erforderlich, dass ein Internetnutzer den DNS-Resolver der Antragsgegnerin verwende, um auf die Webseite „ddl-music.to“ zu gelangen.. Die Situation sei anders als der Beitrag eines Internetzugangsvermittlers, weil die Gewährung des Internetzugangs und die Durchleitung der Informationen bei der Übertragung der rechtsverletzenden Inhalte unmittelbar eingesetzt werde. Der DNS-Resolver sei daran nicht beteiligt. Dieser sei mit dem Betreiber eines Telefonbuchs vergleichbar.

36

Hilfsweise komme jedenfalls nur eine subsidiäre Haftung in Betracht, weil auch der Access-Provider nur subsidiär hafte.

37

38

Das Landgericht habe weiter rechtsfehlerhafte Zumutbarkeitserwägungen bzgl. einer Sperre mit Wortfiltern angestellt. Der Vortrag zum Wortfilter habe sich auf die Webseitenbetreiber bezogen. Eine Sperre bzw. ein Filter sei ein Eingriff in das Recht auf unternehmerische Freiheit aus Art. 16 EU-GR-Charta. Die weltweiten Auswirkungen seien offensichtlich unverhältnismäßig. Die Antragstellerin sei auch nicht rechtlos gestellt, weil gesetzlich vorgesehene Maßnahmen gerade für Fälle wie den vorliegenden existierten (§ 59 RStV).	
Schließlich sei die Dringlichkeit fehlerhaft bejaht worden.	39
Zur weiteren Substantiierung ihres Vorbringens nimmt sie Bezug auf das Privatgutachten von Prof. Dr. Spindler vom 1.9.2020 (Bl. 279 ff. eA) nebst Ergänzung vom 25.9.2020 (Bl. 384 ff. eA).	40
Die Antragsgegnerin beantragt,	41
unter Abänderung des am 30. Januar 2020 verkündeten Urteils des Landgerichts Köln, Aktenzeichen 14 O 171/19, die einstweilige Verfügung aufzuheben und den auf ihren Erlass gerichteten Antrag insgesamt zurückzuweisen.	42
Die Antragstellerin beantragt,	43
die Berufung zurückzuweisen.	44
Hilfsweise stellt sie zu den bisherigen Klageanträgen zu 1 a — c)	45
folgenden weiteren Antrag zu 1 d):	46
Der Verfügungsbeklagten wird aufgegeben, in ihren CDN-Dienst die Webseite DDL-Music.to zu sperren, soweit über diese das Musikalbum „HERZ KRAFT WERKE“ bzw. „HERZ KRAFT WERKE (Deluxe Edition)“ der Künstlerin Sarah Connor mit den Musikaufnahmen wie in den Hauptanträgen aufgelistet über den gegenwärtig „DDL—Musik“ genannten Internetdienst öffentlich zugänglich gemacht wird, wie geschehen unter den in den Hauptanträgen aufgeführten Hyperlinks.	47
Zum Antrag zu 2) formuliert sie sinngemäß weiteren folgenden Hilfsantrag:	48
Der Verfügungsbeklagten wird aufgegeben, in ihrem DNS-Resolver-Dienst die Auflösung des Domainnamens „DDL-Music.to“ in numerische IP-Adressen zu sperren, soweit über diese Domain das Musikalbum HERZ KRAFT WERKE“ bzw. „HERZ KRAFT WERKE“ (Deluxe Edition) der Künstlerin Sarah Connor mit den genannten Musikaufnahmen öffentlich zugänglich gemacht wird.	49
Die Antragsgegnerin beantragt,	50
auch die neu gestellten Hilfsanträge zurückzuweisen.	51
Sie rügt deren Unzulässigkeit, insoweit speziell deren mangelnde Dringlichkeit und weist darauf hin, dass diese Anträge nicht Gegenstand der bisherigen einstweiligen Verfügung seien, die sie mit der Berufung angegriffen habe.	52
Die Antragstellerin beantragt im Rahmen ihrer Anschlussberufung,	53
das angefochtene Urteil teilweise abzuändern und zu erkennen,	54
	55

es der Beklagten bei Vermeidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes und für den Fall, dass dieses nicht beigetrieben werden kann, einer Ordnungshaft oder Ordnungshaft bis zu 6 Monaten (Ordnungsgeld im Einzelfall höchstens € 250.000,00, Ordnungshaft insgesamt höchstens zwei Jahre, zu vollziehen an ihrem Geschäftsführer), zu verbieten,

das Musikalbum „HERZ KRAFT WERKE" bzw. „HERZ KRAFT WERKE (Deluxe Edition)" der Künstlerin Sarah Connor mit den Musikaufnahmen 56

1.1 Vincent 57

1.2 Ich wünsch dir 58

1.3 Ruiniert 59

1.4 Flugzeug aus Papier (Für Emmy) 60

1.5 Hör auf deinen Bauch 61

1.6 Keiner pisst in mein Revier 62

1.7 Mein Jetzt mein Hier 63

1.8 Unendlich 64

1.9 Zelt am Strand 65

1.10 Unter alten Jacken 66

1.11 Schloss aus Glas 67

1.12 Weisst du noch Herz 68

1.13 Kleinstadtsymphonie 69

1.14 Es war gut 70

1.15 Dank dir 71

2.1 Töten dafür 72

2.2 Drachen 73

2.3 Es war gut (Fan-Version) 74

2.4 Vincent (akustisch) 75

2.5 Ich wünsch dir (akustisch) 76

2.6 Zelt am Strand (akustisch) 77

2.7 Mein Jetzt mein Hier (akustisch) 78

2.8 Kleinstadtsymphonie (akustisch) 79

80

2.9 Hör auf deinen Bauch (akustisch)

über den gegenwärtig „DDL-Music“ genannten Internetdienst insbesondere mit	81
der Domain „ddl- music.to“ öffentlich zugänglich zu machen, wie geschehen unter den Hyperlinks	82
http://ddl-music.t/download/227112/Sarah Connor - HERZ KRAFT WERKE Deluxe Edition/	83
https://ddl-music.to/download/links/f13266beef1a3f1dfe8b2f691ce685f1/mirror/2/	84
http://nitroflare.com/view/FF060C685955F76/PTYfsGUybX.rar	85
http://ddl-music.to/download/227112/Sarah Connor - HERZ KRAFT WERKE Deluxe Edition/	86
https://ddl-music.to/download/links/f13266beef1a3f1dfe8b2f691ce685f1/	87
http://www.share-online.biz/dl/1P11QFSP83D;	88
hilfsweise	89
Dritten Hilfe zu leisten, das Musikalbum „HERZ KRAFT WERKE“ bzw. „HERZ	90
KRAFT WERKE (Deluxe Edition)“ der Künstlerin Sarah Connor mit den oben aufgeführten Musikaufnahmen über den gegenwärtig „DDL-Music“ genannten Internetdienst insbesondere mit der Domain „ddl-music.to“ öffentlich zugänglich zu machen, wie geschehen unter den bereits aufgeführten Hyperlinks.	91
Die Antragsgegnerin beantragt,	92
die Anschlussberufung der Antragstellerin zurückzuweisen.	93
Mit ihrer Anschlussberufung verfolgt die Antragstellerin die Verurteilung der Antragsgegnerin gem. ihren erstinstanzlichen Anträgen 1a, hilfsweise 1b als Mittäter bzw. Gehilfe weiter.	94
Die streitgegenständlichen Rechtsverletzungen seien auf der Webseite gelöscht worden und die Webseite werde nicht länger über den CDN-Dienst der Antragsgegnerin betrieben.	95
Die Antragsgegnerin hafte täterschaftlich, weil sie eigenständig in die Verletzung eines Dritten eintrete. Sie stelle so viel wie möglich an Inhalten zur Verfügung, was kein Caching nach Anfrage durch den Nutzer sei, sondern ein Bereithalten zum Abruf. Sie biete weiter Webcontent-Optimierung an (Anlage Ast 1 S. 4) und greife dadurch in Inhalte ein, etwa durch Komprimierung von Bildern und Bereinigung des Quelltextes (Ast 10 und 11). Dieses Recht lasse sie sich von ihren Kunden einräumen. Sie anonymisiere, indem sie sich an die Stelle des wahren Hostproviders setze. Dadurch werde der Betreiber der Webseite vor Inanspruchnahme bewahrt. Sie schirme Webseiten vor Angriffen ab. Dabei handele es sich um eine sog. deliberate intervention iSd EuGH-Rechtsprechung zur Seite „The Pirate Bay“ (Urt. v. 14.6.2017 – C 610/15 Rn. 26).	96
Die Antragsgegnerin handele auch vorsätzlich. Vom 1.1.2017 – 31.1.2020 habe sie von der Firma proMedia 566 Abuse-Meldungen mit Hinweisen auf urheberrechtsverletzende Angebote auf ddl-music.to erhalten.. Seit 6.6.2019 wisse die Antragsgegnerin von dem konkreten Verstoß, der erst am 17.2.2020 abgestellt worden sei. Die Antragsgegnerin sei auch in Italien mit Entscheidung des Handelsgerichts Rom v. 26.6.2019 R.G. 26942/2019 RTI	97

./ D. zur Sperrung von Piraterieseiten und Auskunft verurteilt worden (Ast. 15). In den USA liefen ebenso diverse Verfahren.

Indem die Antragsgegnerin trotz positiver Kenntnis von der Rechtsverletzung über einen Zeitraum von acht Monaten untätig geblieben sei, habe sie eine zentrale Rolle eingenommen wie im Vorlagebeschluss des BGH zu „Youtube“ und „Uploaded“ angenommen (BGH, Beschl. v. 13.9.2018 - I ZR 140/15 – juris Rn. 34 - YouTube). Ein Erwerbsinteresse sei ebenfalls gegeben. 98

Zur Berufung der Antragsgegnerin behauptet die Antragstellerin, dass sie nicht gegen die Betreiber der Seite direkt hätte vorgehen können, weil kein Impressum und kein Abuse-Formular vorhanden sei. Eine Kontaktaufnahme mit dem Host-Provider sei nicht erfolversprechend gewesen, weil zwar die Antragsgegnerin den Namen des Hosts mitgeteilt habe, aber nicht die IP-Adresse der Webseite. Ohne IP-Adresse sei es dem Host-Provider nicht möglich, den für die Rechtsverletzung genutzten Server in seinem Rechenzentrum ausfindig zu machen. Selbst mit IP-Adresse sei eine Inanspruchnahme überdies aussichtslos, weil der pakistanische Host-Provider gerade damit werbe, Urheberrechtsverletzungen zu ignorieren. 99

Die Darlegungslast bzgl. einer Haftungsprivilegierung liege bei der Antragsgegnerin. Die von dieser zitierte Entscheidung des BGH sei noch zu § 5 TDG ergangen. Mit dem abweichenden Wortlaut in § 8 TMG „nicht verantwortlich, sofern...“ werde ein Ausnahmefall beschrieben, für den die Antragsgegnerin als Diensteanbieterin darlegungsbelastet sei. 100

Wegen bestehender vertraglicher Beziehungen greife die Privilegierung ohnehin nicht. Die E-Commerce-RL 2000/31/EG Erwägungsgrund Rn. 43 führe aus, dass ein Dienstleister die Ausnahmeregelung für die „reine Durchleitung“ und das „Caching“ (nur) in Anspruch nehmen könne, wenn er in keiner Weise mit der übermittelten Information in Verbindung stehe. 101

Die Antragsgegnerin filtere zudem iS einer Firewall, was einen Ausschlussstatbestand darstelle (Spindler in: Spindler/Schmitz, TMG, 2. Aufl. 2018, § 8 TMG Rn. 14).(Bl. 216 eA). Außerdem verändere sie die Informationen. 102

Es liege auch kein Caching iSd § 9 TMG vor, weil nicht nach Anfrage des Nutzers gespeichert werde. Caching werde jedoch immer durch den Nutzer ausgelöst, hier erfolge dies durch den Kunden, also den Webseitenbetreiber. Ziel der Speicherung sei nicht nur Effizienzsteigerung, sondern auch Schutz der Webseite. 103

Schließlich liege zumindest eine Störerhaftung vor. Der Haftungsausschluss für Unterlassungsansprüche nach § 8 Abs. 1 S. 2 TMG beziehe sich nach dem gesetzgeberischen Willen sowie nach richtlinienkonformer Auslegung ohnehin nur auf die Haftung des WLAN-Betreibers und hätte bei § 8 Abs. 3 TMG geregelt werden müssen. Es handele sich um ein Redaktionsversehen, dass sich die Regelung in § 8 Abs. 1 TMG befinde. 104

Die Antragsgegnerin habe mittlerweile sogar territorial begrenzt die Rechtsverletzung abgestellt und ihre Dienste ab dem 17.2.2020 ausgesetzt, sodass die verletzende Seite nicht mehr unter Einschaltung ihrer Dienste abrufbar sei. 105

Die Sperre durch die Antragsgegnerin sei auch nicht unwirksam. Solange die Antragsgegnerin für die Domain „ddl-music.to“ als autoritativer Name-Server eingetragen sei, sei die Seite „ddl-music.to“ nach Sperrung durch die Antragsgegnerin nicht aufrufbar. Erst nach Umtragung könne die Seite wieder abgerufen werden. 106

Beim DNS-Resolver greife keine Haftungsprivilegierung.	107
Es liege auch ein adäquat kausaler Beitrag vor. Das Argument der Antragsgegnerin, dass die öffentliche Zugänglichmachung unabhängig von der Verwendung ihres DNS-Resolvers durch einen Internetnutzer geschehe, lege einen hypothetischen Verlauf zugrunde. Alle Internetnutzer, die den DNS-Resolver der Antragsgegnerin benutzten, könnten nur auf die Seite „ddl-music.to“ gelangen, wenn ihnen der DNS-Resolver dabei helfe, die Domain zu der zugehörigen IP-Adresse aufzulösen. Da beim Recht des öffentlichen Zugänglichmachens auch keine Erschöpfung eintrete, komme es nicht darauf an, ob die Inhalte bereits Nutzern anderer DNS-Resolver öffentlich zugänglich gemacht worden seien.	108
Adäquate Kausalität ergäbe sich auch entsprechend dem BGH-Urteil zu Access-Providern. Da danach der Zugang zu einer bereits erfolgten Verletzung des § 19a UrhG einen adäquaten kausalen Beitrag darstelle, müsse dies auch hier gelten. (Bl. 226 eA)	109
Hinsichtlich der Zumutbarkeit der Sperre unterliege die Antragsgegnerin einer sekundären Darlegungslast. Richtig sei, dass DNS-Resolver keine spezifischen URLs sperren könnten. Bestritten werde jedoch, dass man nicht einzelne Domains sperren könne. Bestritten werde auch, dass die Sperrung einer Domain signifikante Auswirkungen auf die Latenz des DNS-Resolvers hätte. Die technische Möglichkeit werde durch die gängige Praxis verdeutlicht, dass weltweit durch Einsatz von DNS-Filtern über 2600 Webseiten gesperrt würden. Insoweit verweist sie auch auf das Dokument „DNS over HTTPS“, in dem die Sperrmöglichkeit beschrieben werde.	110
Umgehungsmöglichkeiten sprächen nicht gegen die Zumutbarkeit einer Sperrung. Sie würden die Annahme hinreichender Effektivität nicht erschüttern (s. BGH Störerhaftung des Access-Providers Rn. 48).	111
Selbst wenn eine Sperre nur weltweit möglich sei, seien keine berechtigten Interessen ersichtlich, die gegen die Zumutbarkeit sprächen.	112
II.	113
1. Die Berufung der Antragsgegnerin ist unbegründet. Ohne Erfolg wendet sich die Antragsgegnerin gegen die Annahme des Landgerichts, dass die Antragsgegnerin als CDN-Dienstleisterin für die öffentliche Zugänglichmachung des streitgegenständlichen Musicalbums über die Webseite ddl-music.to mit verantwortlich ist.	114
a. Der Antragstellerin steht wegen der Zurverfügungstellung eines sog. CDN-Systems ein Unterlassungsanspruch aus dem Gesichtspunkt der Störerhaftung iVm §§ 97 Abs. 1, 19 a, 85 Abs. 1, 35 Abs. 3 UrhG zu.	115
aa. Die Aktivlegitimation der Antragstellerin steht nicht mehr im Streit.	116
bb. Die der Antragstellerin zustehenden Rechte als Tonträgerherstellerin hinsichtlich der streitgegenständlichen Musiktitel sind dadurch verletzt worden, dass diese über die Webseite „ddl-music.to“ über die im Tenor aufgeführten Hyperlinks öffentlich zugänglich gemacht worden sind. Insoweit wird auf die zutreffenden Ausführungen des Landgerichts (S. 27-31 des angefochtenen Urteils) verwiesen. Dieser Punkt wird von der Antragsgegnerin nicht angegriffen. Da die Antragsgegnerin jedoch selbst weder die Webseite betreibt noch die Hyperlinks eingestellt hat, sie es aber vertraglich den Betreibern der Webseite gegenüber übernommen hat, für die Webseite als sog. CDN-Server tätig zu werden, hat sie adäquat	117

kausal zur Rechtsverletzung beigetragen und ist daher für die Rechtsverletzung als Störer verantwortlich.

cc. Als Störer kann bei der Verletzung absoluter Rechte auf Unterlassung in Anspruch genommen werden, wer - ohne Täter oder Teilnehmer zu sein - in irgendeiner Weise willentlich und adäquat kausal zur Verletzung des geschützten Rechts beiträgt. Dabei kann als Beitrag auch die Unterstützung oder Ausnutzung der Handlung eines eigenverantwortlich handelnden Dritten genügen, sofern der Inanspruchgenommene die rechtliche und tatsächliche Möglichkeit zur Verhinderung dieser Handlung hatte. Da die Störerhaftung nicht über Gebühr auf Dritte erstreckt werden darf, die weder als Täter noch als Teilnehmer für die begangene Urheberrechtsverletzung in Anspruch genommen werden können, setzt die Haftung als Störer nach der Rechtsprechung des Bundesgerichtshofs die Verletzung zumutbarer Verhaltenspflichten, insbesondere von Prüfungspflichten, voraus. Ob und inwieweit dem als Störer Inanspruchgenommenen eine Verhinderung der Verletzungshandlung des Dritten zuzumuten ist, richtet sich nach den Umständen des jeweiligen Einzelfalls unter Berücksichtigung seiner Funktion und Aufgabenstellung sowie mit Blick auf die Eigenverantwortung desjenigen, der die rechtswidrige Beeinträchtigung selbst unmittelbar vorgenommen hat (st. Rspr.; vgl. BGH, Urt. v. 10.1.2019 – I ZR 267/15 -, juris Rn. 82 mwN – Cordoba II).

118

aaa. Die in § 8 Abs. 1 TMG geregelte und auf Art. 12 Abs. 1 der Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr (e-Commerce-Richtlinie) beruhende Haftungsprivilegierung des Diensteanbieters steht der Annahme nicht entgegen, dass die Antragsgegnerin als Anbieterin eines CDN-Systems für von Dritten begangene Rechtsverletzungen als Störer auf Unterlassung haftet, weil vorliegend bereits die Voraussetzungen des Ausschlussstatbestands nach § 8 TMG nicht erfüllt sind.

119

(1) Nach § 8 Abs. 1 S. 1 TMG sind Diensteanbieter für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie die Übermittlung nicht veranlasst, den Adressaten der übermittelten Informationen nicht ausgewählt und die übermittelte Informationen nicht ausgewählt oder verändert haben.

120

(2) Die Antragsgegnerin ist Diensteanbieterin iSd Legaldefinition des § 2 S. 1 Nr. 1 TMG, wonach Diensteanbieter jede natürliche oder juristische Person ist, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt. Zu den Telemedien zählen u.a. alle elektronischen Informations- und Kommunikationsdienste, § 1 Abs. 1 S. 1 TMG. Die Antragsgegnerin, die für ihre Kunden als „autoritativer Nameserver“ eingetragen wird, leitet für ihre Kunden den gesamten Datenverkehr zwischen Endnutzer und Webseite über ein eigenes Servernetz. Damit übermittelt sie fremde Informationen in einem Kommunikationsnetz iSd § 8 TMG.

121

(3) Sie beschränkt sich jedoch nicht auf die reine Übermittlung, sondern speichert unstreitig Inhalte der Webseiten ihrer Kunden auf ihren eigenen Servern zwischen. Nach § 8 Abs. 2 TMG erfasst die Übermittlung von Informationen nach Absatz 1 auch die kurzzeitige Zwischenspeicherung dieser Informationen, jedoch nur soweit dies zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Informationen nicht länger gespeichert werden als für die Übermittlung üblicherweise erforderlich ist. Aus dem eigenen Vortrag der Antragsgegnerin ergibt sich hingegen, dass sie die Inhalte der Kundenwebseiten nicht nur solange speichert, wie dies zur bloßen Übermittlung üblicherweise erforderlich ist. Sie behauptet in der Berufungsbegründung selbst, dass sie auch Speicherungen vornehme, um die Anzahl der Aufrufe auf die Seiten ihrer Kunden zu reduzieren. Da die Antragsgegnerin

122

als Vorteil ihrer Dienstleistung in ihrer Werbung sowohl auf die Beschleunigung als auch den Schutz der Kundenwebseiten abstellt, ergibt sich, dass das Speichern auf den Servern ihres Netzwerks nicht allein der Übermittlung der angefragten Informationen dient. Vielmehr ermöglicht - wie sie es selbst ausführt -, das „Speichern Ihrer Webseite auf lokalen Datenzentren und das Blockieren bössartiger Besucher (...) D., Ihre Bandbreitennutzung um über 60% und die Anzahl der Anfragen auf Ihre Webseite um 65% zu reduzieren.“ (Ast 1, Bl. 207 ff. dA). Damit dient das Speichern auf den lokalen Servern auch dazu, den Zugriff auf die Kundenwebseite zu verringern und wird danach nicht allein zum Zwecke der effizienteren Übermittlung vorgenommen. Da sich dies bereits aus der Eigenwerbung der Antragsgegnerin ergibt, kommt es auf die von der Antragsgegnerin aufgeworfene Frage der Darlegungs- und Beweislast an dieser Stelle nicht an.

(4) Vor diesem Hintergrund geht die Rüge, dass das Landgericht entgegen dem Wortlaut des § 8 TMG fehlerhaft eine „Flüchtigkeit“ der Zwischenspeicherung für erforderlich gehalten habe, ins Leere, weil jedenfalls nach der Eigenwerbung der Antragsgegnerin weder von einer „flüchtigen“ noch von einer „kurzzeitigen“ Zwischenspeicherung ausgegangen werden kann. Denn die Speicherung, wie sie die Antragsgegnerin vornimmt, geschieht offensichtlich nicht – wie es § 8 Abs. 2 TMG fordert – „nur zur Durchführung der Übermittlung im Kommunikationsnetz“ und es werden die Informationen auch länger gespeichert, „als für die Übermittlung üblicherweise erforderlich“. Dies ist im Grunde auch nicht streitig, weil die Antragsgegnerin sich zusätzlich auf die Haftungsprivilegierung nach § 9 TMG beruft, der gerade, anders als § 8 TMG, nicht die kurzzeitige Speicherung zum Zwecke der effizienteren Durchleitung von Informationen zum Gegenstand hat, sondern das sog. Caching. Dabei handelt es sich um die Zwischenspeicherung von Derivaten einer bereits an anderer Stelle verfügbaren Quelle, ohne dabei die Zuordnung zum Inhaber zu berühren oder die Inhalte zu modifizieren (vgl. Roggenkamp/Stadler in: Heckmann, jurisPK-Internetrecht, 5. Aufl. (Stand: 11.1.2019), Kap. 10 Rn. 197). Da die Datenpakete mitunter einen weiten Weg vom Host-Provider bis zum Nutzer zurücklegen, sparen dezentrale Kopien Ressourcen ein. Der Nutzer bekommt die Inhalte dabei nicht direkt vom Quellserver geliefert, sondern von einem näher an seinem Standort gelegenen lokalen Server (vgl. Roggenkamp/Stadler in: Heckmann, jurisPK-Internetrecht, 5. Aufl. (Stand: 11.1.2019), Kap. 10 Rn. 197). Dass das System der Antragsgegnerin diese Art der Zwischenspeicherung vornimmt, ergibt sich jedenfalls aus der Eigenwerbung der Antragsgegnerin:

„Das D. Rechenzentrum unter xx.xx.xx.xx stellt so viel wie möglich von Ihrer Webseite von seinem lokalen Speicher zur Verfügung und fragt Ihren Webserver unter 1.1.1.1 für die übrigen Teile ihrer Webseite, die es nicht bereits lokal gespeichert hat.“

Soweit die Antragsgegnerin meint, diese Aussage sei nur so zu verstehen, dass dem Nutzer nur so viel wie möglich vom lokalen Server zur Verfügung gestellt werde, nicht aber, dass so viel wie möglich auf dem lokalen Server gespeichert werde und sich daraus keine Schlussfolgerungen hinsichtlich der Dauer der Speicherung ziehen ließen, spielt die Frage der Auslegung im Rahmen des § 8 TMG keine Rolle, weil dadurch jedenfalls glaubhaft gemacht ist, dass die über die zur effizienteren Durchleitung erforderliche Dauer der Speicherung in jedem Fall überschritten wird, weil das Angebot der Antragsgegnerin gerade auch auf das Caching ausgelegt ist, mit dem Ziel, Schnelligkeit und Sicherheit für die Kundenwebseiten zu erreichen. Von einer „Kurzfristigkeit“ iSd § 8 TMG – die wohl nach hM bei einigen Stunden gegeben sein soll (s. Malek/Popp, Strafsachen im Internet, 2. Aufl. 2015, Rn. 103 mwN) – kann vor dem Hintergrund dieser Auslobung nicht mehr die Rede sein.

bbb. Auch die Privilegierung nach § 9 TMG steht einer Störerhaftung der Antragsgegnerin nicht entgegen. Zwar könnte möglicherweise wegen des Verweises in § 9 S. 2 TMG auf § 8 Abs. 1 S. 2 TMG dem reinen Wortlaut nach die Privilegierung des Caching-Providers nach § 9 TMG auch einem bloßen Unterlassungsanspruch entgegengehalten werden. Es spricht jedoch viel dafür, dass es sich um ein Redaktionsversehen handelt, weil jedenfalls nach der Gesetzesentstehung gezielt eine besondere Privilegierung von WLAN-Betreibern und daneben sonstigen Access Provider erreicht werden sollte (vgl. BT-Drs. 18/12202, 9f., 12). Eine Ausweitung auf Caching-Provider war jedenfalls nicht ausdrücklich angedacht worden.

(1) Wie der Verweis in § 9 S. 2 TMG letztlich zu verstehen ist, kann dahinstehen, weil vorliegend bereits nicht glaubhaft gemacht ist, dass überhaupt die Voraussetzungen der Haftungsprivilegierung des § 9 TMG vorliegen. Für das Bestehen des Haftungsprivilegs ist die Antragsgegnerin darlegungs- und beweisbelastet, weil nur sie über die entsprechenden technischen und organisatorischen Kenntnisse über den Einsatz der Verfahren, die sie bei der Zwischenspeicherung anwendet, verfügt (vgl. Roggenkamp/Stadler in: Heckmann, jurisPK-Internetrecht, 5. Aufl. (Stand: 11.1.2019), Kap. 10 Rn. 232 mwN). Anders als § 5 TDG Abs. 2 aF, in dem es hieß, dass „Diensteanbieter für fremde Inhalte nur verantwortlich sind, wenn (...)“, der also weitere anspruchsbegründende Merkmale formulierte, ist § 9 Abs. 1 TMG negativ formuliert dahingehend, dass Diensteanbieter für bestimmte Informationen „nicht verantwortlich sind, sofern (...)“. Insoweit werden in § 9 TMG keine zusätzlichen anspruchsbegründenden Voraussetzungen aufgestellt, für die der Anspruchsteller nach den allgemeinen Grundsätzen darlegungs- und beweisbelastet wäre, sondern es wird vielmehr unter bestimmten Voraussetzungen eine Haftungsprivilegierung gewährt, die der Antragsgegnerin günstig ist und für die sie nach den allgemeinen Grundsätzen darlegungs- und beweisbelastet ist (vgl. zum Streitstand: Paal in: Gersdorf/Paal, BeckOK InfoMedienR, TMG, 29. Edition (Stand: 1.2.2020), § 7 Rn. 74 f.) 127

(2) Nach § 9 S. 1 TMG sind Diensteanbieter für eine automatische, zeitlich begrenzte Zwischenspeicherung, die allein dem Zweck dient, die Übermittlung fremder Informationen an andere Nutzer auf deren Anfrage effizienter zu gestalten, unter den in den Nr. 1 – 5 aufgeführten Voraussetzungen nicht verantwortlich. 128

(3) Vorliegend ist bereits nicht glaubhaft gemacht, dass die Speicherung durch die Antragsgegnerin - wie nach dem Wortlaut des § 9 TMG vorausgesetzt - allein dem Zweck dient, die Übermittlung fremder Informationen an andere Nutzer auf deren Anfrage effizienter zu gestalten, wenn die Speicherung möglicherweise dem weiteren vertraglich vereinbarten Zweck des Schutzes der Webseite des Kunden dient. Ob bereits diese Verfolgung weiterer Zwecke der Haftungsprivilegierung entgegensteht, kann jedoch dahinstehen. 129

(4) Beim sog. Caching iSd § 9 TMG, der Art. 13 Abs. 1 der e-Commerce-Richtlinie umsetzt, geht es um die automatische Zwischenspeicherung von Informationen, um Nutzern auf deren Abfrage hin einen schnellen Zugang zu ermöglichen (s. Malek/Popp, aaO, Rn. 104). In Betracht kommen verschiedene Formen von Caching, zum einen mithilfe eines sog. Proxy-Cache-Servers und zum anderen mithilfe eines sog. Mirror-Servers. Bei beiden handelt es sich um leistungsstarke Rechner mit hoher Speicherkapazität, die mithilfe von eigens angelegten Zwischenkopien die unnötige Mehrfachübertragung von Internetinhalten verhindern. Räumlich gesehen stehen sie zwischen einer ausreichend großen Nutzergruppe und den Host Servern. Beim Proxy-Cache-Server wird anhand der von Internetbrowsern übermittelten URL abgeglichen, ob die angefragten Inhalte zuvor schon einmal übertragen wurden und noch im Speicher vorrätig sind. Ist dies der Fall, werden die Seiteninhalte direkt vom Proxy-Cache-Server an den Browser des Nutzers geliefert. Die Übertragung der Daten 130

vom ursprünglichen Host-Server ist dann nicht mehr erforderlich. Ist allerdings keine Zwischenkopie verfügbar und soll auch keine generiert werden, wird die Nutzeranfrage unverändert an den Host Server weitergeleitet (vgl. Roggenkamp/Stadler in: Heckmann, jurisPK-Internetrecht, 5. Aufl. (Stand: 11.1.2019), Kap. 10 Rn. 204 ff. mwN).

(5) Der Begriff Mirror-Server steht für Netzwerkserver mit hohen Speicherkapazitäten, die ein Abbild von häufig nachgefragten Datenbanken, ganzen Webauftritten oder einzelnen Dateien im Internet bereithalten. Vergleichbar mit Cache-Diensten steht auch hier die Effizienzsteigerung der Internetkommunikation durch die Dezentralisierung von Daten im Vordergrund. Anders jedoch als Proxy-Cache-Server stehen die Mirror-Server hauptsächlich im Interesse der Content- oder Host-Provider. Durch die Datenredundanz kann eine Lastverteilung erwirkt werden, die im Fall kritisch hoher Abfragekumulationen den Ausfall der Serversysteme verhindern soll. In der Regel besteht dazu eine Vereinbarung zwischen den Inhaltsanbietern und den Betreibern von Mirror-Servern (vgl. Roggenkamp/Stadler in: Heckmann, jurisPK-Internetrecht, 5. Aufl. (Stand: 11.1.2019), Kap. 10 Rn. 207 mwN). Nach überwiegender Ansicht soll auch das Betreiben von Mirror-Servern grundsätzlich unter das Tatbestandsmerkmal der automatischen, zeitlich begrenzten Zwischenspeicherung fallen können (vgl. noch zum TMG aF: Jandt in: BeckTMG, 1. Aufl. 2013, § 9 Rn. 8 mwN). 131

(6) Die Antragsgegnerin hat vorliegend schriftsätzlich als auch in der mündlichen Verhandlung vorgetragen, dass sie ein System mit Proxy-Cache-Servern der oben dargestellten Art vorhält. Es spricht nach Auffassung des Senats jedoch vieles dafür, dass sie darüber hinaus ihre Rechner auch als Mirror-Server betreibt. Die Eigenwerbung der Antragsgegnerin legt dies jedenfalls nahe, wenn es heißt: 132

„Das D. Rechenzentrum unter xx.xx.xx.xx stellt so viel wie möglich von Ihrer Webseite von seinem lokalen Speicher zur Verfügung und fragt Ihren Webserver unter 1.1.1.1 für die übrigen Teile Ihrer Webseite, die es nicht bereits lokal gespeichert hat. Das D. Rechenzentrum xx.xx.xx.xx stellt dann dem Besucher Ihre komplette Webseite zur Verfügung, so dass der Besucher nie direkt den Webserver 1.1.1.1 anspricht.“ 133

Das Ziel, Schnelligkeit und Sicherheit für die Kundenwebseite zu erreichen, soll danach ausdrücklich dadurch erreicht werden, dass „so viel wie möglich“ von der Kundenwebseite von einem lokalen Speicher der Antragsgegnerin zur Verfügung gestellt wird. Die lässt sich aus Sicht der angesprochenen Kunden, §§ 133, 157 BGB, jedenfalls so verstehen, dass nicht so viel wie nötig, sondern so viel wie möglich der Kundenwebseite auf Servern der Antragsgegnerin gespeichert werden soll. Da es jedenfalls beim Einsatz von Mirror-Servern, auch wenn er vom Grundsatz her, der Privilegierung nach § 9 TMG unterfallen kann, auf den Umfang und die Art und Weise der Zwischenspeicherung ankommt, hätte es näheren Vortrags und Glaubhaftmachung dazu bedurft, wie sich das Caching der Antragsgegnerin tatsächlich im Detail gestaltet. Neben dem allgemeinen Hinweis, dass die Kunden die „Time-to-live“-Vorgaben machen und die klassischen Dienstleistungen eines Proxy-Cache-Servers erbracht werden, fehlt es an konkretem Vortrag und Glaubhaftmachung, inwieweit es sich bei der Speicherung um einen automatisierten Vorgang handelt, welche vertraglichen Vereinbarungen es hierzu gibt und dass und in welchem Rahmen die Kunden, hier die Verantwortlichen der Seite „ddl-music.to“, die Zwischenkopien bei ihrer Anlegung dezidiert als zeitlich begrenzt widmen. Weiter fehlt es an Vortrag und Glaubhaftmachung, wie die konkrete Konfiguration der eigenen Server der Antragsgegnerin diesbezüglich aussieht und ob sich das „Ob“ und „Wie“ der Speicherung ganz im Sinne einer Effizienzsteigerung nach Speicherkapazität, der Größe und Aktivität der Nutzergemeinde sowie der Abrufhäufigkeit richten. 134

(7) Die Eigenwerbung der Antragsgegnerin lässt insgesamt den Eindruck aufkommen, dass durch die Zwischenspeicherung jedenfalls auch eine Lastverteilung bewirkt werden soll, die bei hohen Abfrageaufkommen seitens von Internetnutzern den Ausfall der Serversysteme der Kunden verhindern soll. Auch das Privatgutachten von Prof. Spindler, das als substantiiertes Parteivortrag zu berücksichtigen ist, gibt insoweit keine näheren Aufschlüsse über Art und Umfang der Speicherung und ihre tatsächliche Handhabung und insbesondere auch nicht hinsichtlich der vertraglichen Vereinbarungen mit den Kunden, denen die Antragsgegnerin in ihrer Werbung jedenfalls nicht nur Schnelligkeit, sondern vor allem auch Sicherheit und Stabilität verspricht. Mangels tatsächlichen Vortrags kann keine Abgrenzung durch das Gericht erfolgen, ob sich die Antragsgegnerin noch im Rahmen des nach § 9 TMG privilegierten Cachings bewegt oder ob sie ihre Rechner möglicherweise zu weitergehenden Zwischenspeicherungen zugunsten der Sicherheit und Stabilität ihrer Kundenwebseiten verwendet, zu denen sie sich gegenüber ihren Kunden verpflichtet hat und die evtl. über den zulässigen Rahmen des zeitlich begrenzten Cachings nach § 9 TMG hinausgehen. Jedenfalls dann, wenn eine ständige Spiegelung von Inhalten stattfindet und aufrecht erhalten bleibt, die gewährleistet, dass bestimmte Inhalte der Kunden gerade bei einem Ausfall des Ursprungsservers weiter zugreifbar bleiben, könnte die Grenze des § 9 TMG überschritten sein. Dass die Antragsgegnerin als Diensteanbieterin iSd § 9 TMG privilegiert ist, hat sie (s.o. zu § 8 TMG) darzulegen und zu beweisen, sodass die verbleibende Unklarheit zu ihren Lasten geht. Der Einwand der Antragsgegnerin, dass sie grundsätzlich keine datenintensive Informationen wie Audio- oder Videodateien speichere, hilft nicht weiter, weil die Seite „ddl-music.to“ prinzipiell nur mit Verlinkungen arbeitet und selbst keine Audio- oder Videodateien vorhält.

dd. Soweit danach die von der Antragsgegnerin angeführten Privilegierungen der §§ 8 und 9 TMG nicht in Betracht kommen, hat das Landgericht zu Recht eine Störerhaftung der Antragsgegnerin bejaht. Insoweit kann auf die zutreffenden Gründe des Landgerichts verwiesen werden (S. 33 ff., Bl. 580 ff. dA). Der Beitrag der Antragsgegnerin besteht darin, dass sie sich hinsichtlich des Datenverkehrs zwischen der Kundenwebseite und Nutzern mit ihrem Server-Netzwerk zwischenschaltet, sodass sämtlicher Internetverkehr von und zur Webseite des Kunden über die Server der Antragsgegnerin läuft. Die Einschaltung der Server der Antragsgegnerin ist damit adäquat kausal für die rechtswidrige öffentliche Zugänglichmachung des streitgegenständlichen Musikalbums über die Seite ihres Kunden. Da das Geschäftsmodell der Antragsgegnerin zunächst objektiv neutral und gesellschaftlich erwünscht ist und sie ein System von 194, weltweit auf 90 Länder verteilte und miteinander vernetzte Server-Präsenzpunkte unterhält, wäre eine allgemeine Prüfungs- und Überwachungspflicht hinsichtlich von Inhalten ihrer Kundendomains unverhältnismäßig (vgl. EuGH GRUR 2011, 1025 – L’Oréal/eBay -, juris Rn. 139). Denn diese richtet sich nach den jeweiligen Umständen des Einzelfalls unter Berücksichtigung der Funktion und Aufgabenstellung des als Störers in Anspruch Genommenen sowie mit Blick auf die Eigenverantwortung desjenigen, der die rechtswidrige Beeinträchtigung selbst unmittelbar vorgenommen hat (s. BGH, EuGH-Vorlagebeschl. v 13.9.2018 – I ZR 140/15 -, juris Rn. 49 mwN - YouTube). Ist ein Störer ein Diensteanbieter, dessen Dienst in der Speicherung von durch einen Nutzer eingegebenen Informationen besteht, kann er nach der Rechtsprechung des BGH grundsätzlich erst dann durch gerichtliche Anordnung zur Unterlassung verpflichtet werden, wenn es nach einem Hinweis auf eine klare Rechtsverletzung erneut zu einer derartigen Rechtsverletzung gekommen ist, weil der Diensteanbieter nicht unverzüglich tätig geworden ist, um den rechtsverletzenden Inhalt zu entfernen oder den Zugang zu diesem zu sperren und dafür zu sorgen, dass es zukünftig nicht zu derartigen Rechtsverletzungen kommt (vgl. BGH, Vorlagebeschl. v. 13.9.2018 – I ZR 140/15 -, juris Rn. 40 mwN - Youtube).

ee. Eine Prüfpflicht konnte daher nach der Rechtsprechung des BGH erst entstehen, nachdem die Antragsgegnerin Kenntnis von der konkreten Rechtsverletzung erhalten hat (vgl. BGH, Vorlagebeschl. v. 13.9.2018 – I ZR 140/15 -, juris Rn. 49 mwN – Youtube). Eine solche konkrete Kenntnis hatte die Antragsgegnerin hier ab dem Hinweis vom 6.6.2019. Ab diesem Zeitpunkt war sie verpflichtet, ihren Beitrag zur Aufrechterhaltung des rechtswidrigen Zustands zu unterlassen. Sie hat jedoch ca. acht Monate lang nichts unternommen, sodass ein Unterlassungsanspruch zu bejahen ist.

ff. Die im Rahmen der Zumutbarkeit vorzunehmende Interessenabwägung hat das Landgericht ebenfalls zutreffend vorgenommen. Im vorliegenden Fall ist auf Seiten der Antragsgegnerin ihr Recht auf unternehmerische Freiheit nach Art. 16 EU-Grundrechtecharta bzw. Art. 12 Abs. 1 GG (Berufsfreiheit) zu berücksichtigen. Auf Seiten der Antragstellerin geht es um die effektive Verfolgung von Urheberrechtsverstößen als Ausfluss des grundrechtlich gewährten Rechts am Eigentum aus Art. 14 GG bzw. Art. 17 Abs. 2 EU-Grundrechtecharta. Auch das Interesse der Internetnutzer an Informationsfreiheit ist mit zu berücksichtigen. Die Abwägung geht jedoch vorliegend aus den zutreffenden Gründen des landgerichtlichen Urteils zugunsten der Antragstellerin aus. Denn die Sperrung einer Domain, die – mit einem Blick auf die Seite, wie sie Inhalt der Akte geworden ist, erkennbar – fast ausschließlich auf illegale Download-Möglichkeiten verweist, berührt keine berechtigten Interessen der Internetnutzer. Die unternehmerische Freiheit der Antragsgegnerin ist insoweit nicht über Gebühr berührt, als sie selbst in ihren Verträgen sich das Recht vorbehält, bei rechtswidrigen Inhalten ihre Leistungen einzustellen. Dagegen hat die Antragstellerin keine effektive Möglichkeit, gegen den Webseitenbetreiber selbst vorzugehen, weil ihr dazu die Informationen fehlen und gerade auch durch die Eintragung der Antragsgegnerin als autoritativer Nameserver eine Anonymisierung eintritt. Die Antragsgegnerin hat auch nur den Namen des Host-Providers mitgeteilt, der wie aus seiner Eigenwerbung ersichtlich – offensichtlich auch nichts gegen Rechtsverletzungen unternehmen will. Der Antragsgegnerin ist – wie der Verlauf des Verfahrens zeigt – eine Sperre technisch möglich und - weil sie wegen der vertraglichen Regelungen keine wirtschaftlichen Nachteile zu befürchten hat - zumutbar.

gg. Dass Umgehungsmöglichkeiten im Internet bestehen und die streitgegenständliche Webseite auch ohne die Nutzung der Dienste der Antragsgegnerin etwa unmittelbar über ihre eigene IP-Adresse für Internetnutzer erreichbar bleibt, spricht –aus den zutreffende Gründen des landgerichtlichen Urteils – nicht gegen die Zumutbarkeit.

hh. Die Antragsgegnerin haftet auch nicht nur subsidiär. Die Störerhaftung ist zunächst grundsätzlich gegenüber der Haftung des Täters nicht subsidiär (BGH, Urt. v. 26.11.2015 – I ZR 174/14 -, juris Rn. 82 – Störerhaftung des Access-Providers).

Die Rechtsprechung des BGH zur (subsidiären) Störerhaftung des Access-Providers ist vorliegend nicht entsprechend anwendbar. Zwar verfolgt auch die Antragsgegnerin ein von der Rechtsordnung gebilligtes und in Bezug auf Rechtsverletzungen Dritter zunächst neutrales Geschäftsmodell. Sie ist jedoch, anders als ein Access-Provider, mit den Betreibern der streitgegenständlichen Webseite unmittelbar vertraglich verbunden und führt ihre Dienstleistungen des CDN-Systems für diese und zu deren Gunsten aus, indem sie mit ihrer Dienstleistung die Kundenwebseite effizienter macht und vor Angriffen schützt; anders dagegen der Access-Provider, der lediglich den Zugang zu einem Kommunikationsnetz vermittelt, indem er über die von ihm bereitgestellten Internetzugänge Dritten ermöglicht, von deren Endgeräten aus auf das Internet zuzugreifen (vgl. BGH, Urt. v. 26.11.2015 – I ZR 174/14 -, juris Rn. 24 – Störerhaftung des Access Providers unter Verweis auf: Hoffmann in

ii. Der Verweis auf § 59 RStV führt zu keiner anderen Bewertung. Zwar können – worauf die Antragsgegnerin zu Recht hinweist - nach § 59 Abs. 4 RStV grundsätzlich Maßnahmen zur Sperrung von Angeboten nach § 59 Abs. 3 RStV durch die jeweils zuständige Aufsichtsbehörde auch gegen den Diensteanbieter von fremden Inhalten nach den §§ 8 bis 10 TMG gerichtet werden. Wird durch ein Angebot aber in Rechte Dritter eingegriffen und ist für den Dritten hiergegen der Rechtsweg eröffnet, so sollen gem. § 59 Abs. 5 RStV Anordnungen der Aufsichtsbehörde im Sinne von Abs. 3 nur erfolgen, wenn dies aus Gründen des Gemeinwohls geboten ist. Da im vorliegenden Fall durch das Angebot auf der Seite „ddl-music.to“ Rechte der Antragstellerin betroffen sind, dieser aber der Rechtsweg offensteht und Gemeinwohlgründe weder vorgetragen noch ersichtlich sind, kann die Antragstellerin nicht auf den Weg über § 59 RStV verwiesen werden. 142

b. Hinsichtlich des Antrags zu 2 haftet die Antragsgegnerin ebenfalls als Störerin, weil sie Internetnutzern ihren DNS-Resolver zur Verfügung stellt. Mit dem DNS-Resolver wird denjenigen Nutzern, die den Resolver der Antragsgegnerin verwenden, erst ermöglicht, einen Domainnamen in eine numerische IP-Adresse aufzulösen und die hier streitgegenständliche Seite aufzufinden. 143

aa. Ein DNS-Resolver ist ein Softwaremodul, dass auf dem Rechner eines DNS-Teilnehmers installiert ist. Es hilft dem Internetnutzer dabei, Domainnamen in numerische IP-Adressen aufzulösen. Jeder Schritt im Internet beginnt mit einer DNS-Abfrage. Die für die Auflösung von Domainnamen erforderlichen Informationen sind in dem Domain Name System – nicht dem DNS-Resolver – weltweit auf Tausenden von Servern in hierarchischer Weise verteilt. Der DNS-Resolver ist der erste Anlaufpunkt im sog. DNS-Lookup und ist für den Umgang mit dem Nutzer verantwortlich, der die Abfrage gestellt hat. Der DNS-Resolver startet die Abfragefolge, die schließlich dazu führt, dass die vom Nutzer angefragte URL in die benötigte IP-Adresse übersetzt wird. Regelmäßig gibt es dabei bis zu 10 Schritte, die durchgeführt werden müssen. Wenn der Nutzer einen Domain-Namen eingibt, fragt der DNS-Resolver einen DNS-Root-Nameserver ab. Der antwortet dann mit der Adresse eines Top-Level-Domain-Servers (z. B. .com, .de), der die Informationen für seine Domains speichert. Bei einer .com –Seite wird die Suche auf die com.TLD verwiesen. Dieser antwortet mit einer IP-Adresse des Nameservers der gesuchten Domain. Sodann sendet der rekursive Resolver eine Anfrage an den Nameserver der Domain. Die IP-Adresse wird dann vom Nameserver an den Resolver zurückgegeben. Der DNS-Resolver antwortet dann auf den Webbrowser des Nutzers mit der IP-Adresse. Sobald die acht Schritte des DNS-Lookups die gesuchte IP-Adresse zurückgegeben haben, kann der Browser die Anfrage auf die Webseite stellen. 144

bb. Danach ist die Inanspruchnahme eines DNS-Resolvers bei dem sog. DNS-Lookup für den Internetnutzer unverzichtbar. Erst der DNS-Lookup ermöglicht dem Internetnutzer, dem die IP-Adresse der hier streitgegenständlichen Domain unbekannt ist, den Zugang zur Seite. Damit stellt sich die Handlung der Antragsgegnerin als adäquat kausal für die auf der Webseite stattfindende Rechtsverletzung dar. Die Annahme der Antragsgegnerin, dass die Seite ddl-music.to ohne Beteiligung und Zutun des DNS-Resolvers der Antragsgegnerin bereits öffentlich zugänglich gemacht sei, sobald die Webseite online sei, und damit sogar die Kausalität als solche fehle, geht fehl. Denn den Internetnutzern, die den DNS-Resolver der Antragsgegnerin nutzen, wird die Seite erst öffentlich zugänglich, wenn sie mit Hilfe des DNS-Resolvers die Übersetzung des Domainnamens in die IP-Adresse erreichen. Ohne den DNS-Resolver ist ihnen ein Zugriff verwehrt. Dass es im Internet eine Vielzahl von Anbietern von DNS-Resolovern gibt, spielt für die Frage der Kausalität ebenso wenig eine Rolle wie es eine 145

Vielzahl von Access-Providern gibt, auf die ausgewichen werden kann (vgl. BGH, aaO, - Störerhaftung des Access Providers).

cc. Die Antragsgegnerin traf als Störerin jedenfalls ab dem Hinweis auf die konkrete Rechtsverletzung eine Pflicht zur Überprüfung und Sperrung. Soweit die Antragsgegnerin mit Nichtwissen bestreitet, dass es sich um eine Seite mit (fast) ausschließlich illegalen Angeboten handelt, ist dieses Bestreiten unzulässig, weil der Hinweis konkret genug war, dass die Antragsgegnerin mit einem Blick auf die Seite den Charakter der Seite hätte erkennen können. Im Übrigen ist die Natur der Seite durch die vorgelegten Screenshots belegt. 146

dd. Im Fall des DNS-Resolvers richtet sich jedoch - anders als im Fall des Angebots des CDN-Systems - das Angebot der Antragsgegnerin an den einzelnen Internetnutzer, dem durch den DNS-Resolver und die damit eingeleitete „Übersetzung“ des Domain-Namens in die entsprechende IP-Adresse erst der Zugang zur gesuchten Seite ermöglicht wird. 147

aaa. Ein Vertragsverhältnis mit dem Webseitenbetreiber oder Host-Provider ist hier nicht gegeben, weshalb die Gründe des BGH aus der Entscheidung „Störerhaftung des Access Providers“ (Rn. 94) entsprechend anwendbar sind: 148

„Die Störerhaftung ist gegenüber der Inanspruchnahme des Täters im Grundsatz nicht subsidiär (BGH, Urteil vom 27. März 2007 - VI ZR 101/06, GRUR 2007, 724 Rn. 13 = WRP 2007, 795; Urteil vom 12. Juli 2007 - I ZR 18/04, BGHZ 173, 188 Rn. 40 - Jugendgefährdende Medien bei eBay). Soweit der Senat im Hinblick auf den Fall der Inanspruchnahme von Access-Providern ausnahmsweise eine vorrangige Rechtsverfolgung gegenüber denjenigen Beteiligten verlangt hat, die entweder die Rechtsverletzung selbst begangen oder zu der Rechtsverletzung als Dienstleister Hilfe geleistet haben, beruhte dies auf der Besonderheit, dass der Access-Provider ein von der Rechtsordnung gebilligtes und in Bezug auf Rechtsverletzungen Dritter neutrales Geschäftsmodell verfolgt und ihm daher keine Kontrollmaßnahmen auferlegt werden dürfen, die sein Geschäftsmodell wirtschaftlich gefährden oder seine Tätigkeit unverhältnismäßig erschweren (vgl. BGH, Urteil vom 26. November 2015 - I ZR 174/14, BGHZ 208, 82 Rn. 82 f. und 26 f. - Störerhaftung des Access-Providers).“ 149

bbb. Auch die Antragsgegnerin betreibt mit der Vermittlung des Zugangs zum Internet ein von der Rechtsordnung gebilligtes und gesellschaftlich erwünschtes Geschäftsmodell, das als solches nicht in besonderer Weise die Gefahr von Urheberrechtsverletzungen schafft. Mangels vertraglicher Verpflichtungen und Bindungen gegenüber dem rechtsverletzenden Webseitenbetreiber ist ihr Verhalten auch grundsätzlich neutral. Damit ist in diesem Fall eine vergleichbare Interessenlage wie im Fall des Access-Providers gegeben und von einer lediglich subsidiären Haftung auszugehen. Diese Frage kann jedoch letztlich dahingestellt bleiben, weil der Antragstellerin andere vorrangige Inanspruchnahmen Dritter ohnehin nicht möglich oder nicht zuzumuten sind. 150

ccc. Im vorliegenden Fall ist der Antragstellerin die IP-Adresse der Webseite nicht bekannt. Dass im vorliegenden Fall gerade die Anmeldung der Antragsgegnerin als autoritative Nameserver zur Anonymisierung geführt hat, ist dabei nicht entscheidend. Allein die Tatsache der Anonymisierung als solche und das fehlende Impressum der Seite „ddl-music.to“ führen dazu, dass der Antragstellerin der Betreiber der Webseite unbekannt ist und sie sich aller Voraussicht nach nicht erfolgreich an den Host-Provider in Pakistan wenden kann, weil dieser nach seiner Eigenwerbung nichts unternehmen wird. Dass die Antragstellerin die IP-Adresse über das seitens der Antragsgegnerin zur Verfügung gestellte 151

„Trusted Reporter Programm“ hätte erhalten können, ist nicht glaubhaft gemacht. Denn es ist bereits nicht erläutert und auch sonst nicht nachvollziehbar, weshalb die Antragsgegnerin bislang nicht bereit war, die IP-Adresse der Seite „ddl-music.to“ mitzuteilen, obwohl sie selbst darauf abstellt, dass die Antragstellerin nach ihren eigenen im „Trusted Reporter Programm“ aufgestellten Bedingungen von vornherein berechtigt gewesen sei, die IP-Adresse zu erfahren. Ob die Rechtsdurchsetzung generell in Pakistan erschwert ist, wofür einiges sprechen mag, kann danach dahinstehen. Der weitergehende Vortrag der Antragsgegnerin, dass der Host-Provider aus Pakistan auch Server in der EU betreibe, hat für die Frage einer aussichtsreichen Rechtsdurchsetzung keine Bedeutung, weil dafür der reine Rechnerstandort nicht maßgeblich ist.

ee. Die Antragsgegnerin behauptet des weiteren, dass ein Wortfilter bei einem DNS-Resolver 152 nicht möglich sei und es sich dabei lediglich um eine Vermutung des Landgerichts im Rahmen der Prüfung der technischen Möglichkeit handele. Die Antragstellerin hat im Termin zur mündlichen Verhandlung vor dem Senat unter Verweis auf S. 18 eines Diskussionspapiers mit dem Titel „DNS over HTTPS“ jedoch substantiiert behauptet, dass jedenfalls eine Domain-Sperre – ob über einen Wortfilter oder auf anderem Weg - technisch möglich sei. So heißt es im Papier: „blocking the resolution of the domain name in the ISP’s resolver is the quickest and cheapest method“. Vorab hatte sie auch darauf hingewiesen, dass es eine vierstellige Anzahl von Webseiten gäbe, die über DNS-Resolver gesperrt seien. Darauf, ob das „Blocking“ über einen Wortfilter funktioniert, kommt es nicht an, solange es einem Anbieter eines DNS-Resolvers technisch möglich ist, den rechtswidrigen Zugriff auf das geschützte Werk zu verhindern. Dass eine Domain-Namen-Sperre nicht möglich sei, behauptet die Antragsgegnerin nicht ernsthaft.

ff. Es ist schließlich nicht unzumutbar, vom Anbieter eines DNS-Resolvers eine Sperre zu 153 verlangen, auch wenn diese möglicherweise nur weltweit möglich ist. Die streitgegenständliche Webseite ist – wie sich den eigenen Verlautbarungen auf der Seite „ddl-music.to“ entnehmen lässt - in erster Linie auf die Ermöglichung von illegalen Downloads gerichtet. So werden auf der Webseite, wie sie als Screenshots zur Akte gereicht worden ist (Anlagenkonvolut Ast 4, Bl. 233 ff. dA), Rubriken wie „DDL-WAREZ“ und „WAREZKORB“ angeboten. Die Webseite wirbt zudem auf der ersten Startseite damit, „die aktuellste Warezeite im deutschsprachigen Raum“ zu sein. Weiter werden bestimmte User ausdrücklich aufgefordert, den DNS-Server zu ändern. Dann sei die Seite „ddl-music.to“ trotz Netzsperre wieder für diese User erreichbar. Weiter (Bl. 234 dA) findet sich die Aufforderung „Umgehe die Ländersperre bei Zippyshare jetzt mit deinem VPN-Zugang“. Angesichts dieser Eigenwerbung ist auch weltweit kein berechtigtes Interesse der Internetnutzer auf Zugriff auf diese Webseite mit offensichtlich ausschließlich illegalen Angeboten ersichtlich, so dass sich die Frage eines Overblockings nicht stellt.

gg. Der Inanspruchnahme auf Unterlassung als Störer steht auch nicht § 8 Abs. 1 S. 2 TMG 154 entgegen. Der § 8 TMG erfasst die Durchleitung von Informationen bzw. die Zugangsvermittlung. Da sich das Angebot der Antragsgegnerin aber auf die Abfrage der Übersetzungsleistung von Domain-Namen in numerische IP-Adresse beschränkt und damit technisch nicht der Zugang zur Internetseite ddl-music.to selbst vermittelt oder Informationen von oder zu dieser Seite übermittelt werden, ist zweifelhaft, ob es sachgerecht ist, den Betreiber eines DNS-Resolvers wie einen WLAN-Betreiber oder Access-Provider zu behandeln.

aaa. Unmittelbar findet § 8 Abs. 1 TMG auf DNS-Resolver auch nach Ansicht des 155 Privatgutachters der Antragsgegnerin keine Anwendung. Eine Anwendung wird daraus

abgeleitet, dass für DNS-Server die Anwendbarkeit zu bejahen sei und es sich bei der DNS-Resolver-Leistung um einen wesentlichen Bestandteil einer DNS-Serverleistung handele. Der DNS-Resolver leitet jedoch nur die Abfrage nach der passenden IP-Adresse an die DNS-Server weiter bzw. die ermittelten Antworten an den Webbrowser des Internetnutzers zurück, damit anderweitig - und gerade nicht über den DNS-Resolver, der nur für die IP-Adressen-Abfrage zuständig ist - eine Verbindung mit der gesuchten Internetseite hergestellt werden kann. Der DNS-Resolver macht zwar – wovon auch das Privatgutachten ausgeht – einen wichtigen Bestandteil bei der Übersetzung eines Domainnamens in eine IP-Adresse aus. Er übermittelt aber weder die Informationen auf der gesuchten Webseite weiter noch vermittelt der Resolver selbst einen Zugang dazu. Er stößt nur die IP-Adressen-Abfrage gegenüber den DNS-Servern an. Selbst wenn DNS-Server – wie im Privatgutachten ausgeführt - dem § 8 Abs. 1 TMG unterfallen sollten, ist eine Gleichbehandlung des DNS-Resolvers jedenfalls nicht angezeigt, weil die Vorschrift des § 8 TMG gerade die Haftung für fremde übermittelte Informationen bzw. für fremde Informationen, zu denen der Zugang vermittelt wird, regelt und die Privilegierung nicht jedweden adäquat kausalen Beitrag im Zusammenhang mit der Übermittlung/Zugangsvermittlung einbezieht. Als ausnahmsweise Haftungsprivilegierung lässt sich die Vorschrift auch nicht ohne weiteres dahingehend erweiternd auslegen, dass jede adäquat kausale Handlung im Zusammenhang mit der Übermittlung von Informationen oder der Zugangsvermittlung zu Informationen Dritter vom Haftungsausschluss erfasst würde. Anhaltspunkte für eine solche weite Auslegung lassen sich weder in der Gesetzesbegründung (BT-Drs. 18/12202) noch in der E-Commerce-Richtlinie finden.

bbb. Die Antragstellerin ist daher auch nicht auf eine Sperranordnung nach § 7 Abs. 4 TMG zu verweisen, auch wenn dieser entgegen seinem Wortlaut nicht auf WLAN-Betreiber beschränkt, sondern entsprechend auf Betreiber drahtgebundener Internetzugänge und evtl. auf alle Zugangsvermittler iSd § 8 TMG anzuwenden sein könnte (vgl. BGH, Urt. v. 26.7.2018 – I ZR 64/17 -, juris Rn. 43 ff. - Dead Island). Eine entsprechende Anwendung des nach seinem Wortlaut auf WLAN-Betreiber beschränkten Sperranspruchs auf Anbieter von bloßen Hilfeleistungen, die nicht den Zugang zum Internet selbst vermitteln oder fremde Informationen übermitteln, ist nicht angezeigt und im vorliegenden Fall eines DNS-Resolver-Anbieters auch nicht erforderlich, um den Regelungsgehalt 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 S. 2 der Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums zu wahren, weil mangels Einschlägigkeit des § 8 Abs. 1 S. 2 TMG die Möglichkeit des Rückgriffs auf die Störerhaftung verbleibt. 156

2. Der Verfügungsgrund ist ebenfalls zu Recht vom Landgericht bejaht worden. Hierzu kann auf die Ausführungen des Senats in seinem Beschluss zur einstweiligen Einstellung der Zwangsvollstreckung vom 16.6.2020 (Bl. 132 ff. eA) Bezug genommen werden. Denn selbst wenn man mit dem OLG München (Urt. v. 7.2.2019 -29 U 3889/18) davon ausgeht, dass im Ergebnis eine werkbezogene Sichtweise nicht in Betracht komme, weil das Unterlassungsbegehren letztlich auf die Sperre der Domain insgesamt hinauslaufe und der Antragstellerin bereits seit dringlichkeitsschädlicher Zeit bekannt sei, dass auf der Webseite Urheberrechtsverletzungen begangen werden, lässt sich jedenfalls vorliegend ein Eilbedürfnis wegen der hohen Bekanntheit der Künstlerin und der sich fast nahtlos an eine aktuelle Veröffentlichung anschließenden Rechtsverletzung nicht verneinen. 157

2. Die Anschlussberufung der Antragstellerin ist bereits wegen fehlender Beschwer unzulässig. In seinem Urteil vom 10. Januar 2019 – I ZR 267/15 – (juris Rn. 95 ff. - Cordoba II) hat der BGH wie folgt ausgeführt: 158

„II. Die Anschlussrevision des Klägers hat ebenfalls keinen Erfolg. Sie ist unzulässig, soweit sie sich gegen die Annahme des Berufungsgerichts richtet, der Unterlassungsantrag habe unter dem Gesichtspunkt der Störerhaftung Erfolg (dazu unter B II 1). Im Übrigen ist die Anschlussrevision unbegründet (dazu unter B II 2). 159

1. Soweit sich der Kläger gegen die Annahme des Berufungsgerichts wendet, der Beklagte sei zur Unterlassung nicht als Täter, sondern lediglich unter dem Gesichtspunkt der Störerhaftung verpflichtet, ist seine Anschlussrevision unzulässig, weil es am Rechtsschutzbedürfnis fehlt. 160

a) Das für die Zulässigkeit der Revision erforderliche Rechtsschutzbedürfnis setzt voraus, dass der Rechtsmittelführer durch die angefochtene Entscheidung beschwert ist und das Rechtsmittel dazu dient, diese Beschwer zumindest teilweise zu beseitigen (BGH, Urteil vom 21. Juni 1968 - IV ZR 594/68, BGHZ 50, 261, 263; MünchKomm.ZPO/Krüger, 5. Aufl., § 542 Rn. 18). Damit soll im Interesse der Gesamtheit der rechtsschutzsuchenden Bürger und des jeweiligen Prozessgegners ausgeschlossen werden, dass das Rechtsmittelgericht sich mit dem Rechtsstreit befassen muss, ohne dass der Rechtsmittelkläger ein schutzwürdiges Interesse an der von ihm erstrebten Entscheidung hat. Deswegen genügt auf Seiten des Rechtsmittelklägers die bloß formelle Beschwer nicht, um die Zulässigkeit des von ihm eingelegten Rechtsmittels zu bejahen. Vielmehr ist die für die Zulässigkeit des Rechtsmittels der klagenden Partei geforderte Beschwer nur gegeben, wenn ein Vergleich des rechtskräftigen Inhalts des angefochtenen Urteils mit dem Klagebegehren ergibt, dass die Entscheidung für den Rechtsmittelkläger in irgendeiner Weise sachlich nachteilig ist, seinem Begehren also nicht voll entsprochen worden ist (BGHZ 50, 261, 263; BGH, Beschluss vom 11. März 2015 - XII ZB 553/14, NJW-RR 2015, 1203 Rn. 8 mwN). Der Kläger ist dagegen nicht beschwert, wenn das Gericht ihm den geltend gemachten Anspruch zugesprochen und ihn lediglich anders zugeordnet hat, als es in der Klagebegründung geschehen ist (BGHZ 50, 261, 263 f.). Entsprechendes gilt für die - hier vorliegende - unselbständige Anschlussrevision. Sie ist zwar kein Rechtsmittel im eigentlichen Sinn, sondern lediglich ein angriffsweise wirkender Antrag innerhalb der gegnerischen Revision (BGH, Beschluss vom 11. März 1981 - GSZ 1/80, BGHZ 80, 146, 148 [juris Rn. 5] mwN; Urteil vom 26. Januar 2001 - V ZR 462/99, juris Rn. 28). Gleichwohl setzt auch ihre Zulässigkeit eine Beschwer durch das Berufungsurteil voraus (BGH, Urteil vom 17. Oktober 1986 - V ZR 268/85, WM 1987, 19, 21 [juris Rn. 41]). 161

b) Nach diesen Grundsätzen ist der Kläger im Hinblick auf den Unterlassungsantrag durch das Berufungsurteil nicht beschwert. Das Berufungsgericht hat den Unterlassungsantrag in Bezug auf den im Streitfall maßgeblichen Sachverhalt uneingeschränkt zugesprochen. Dass es den Verbotsausspruch auf den Gesichtspunkt der Störerhaftung und nicht - wie von der Anschlussrevision für richtig gehalten - auf eine täterschaftliche Haftung gestützt hat, begründet nach den dargelegten Grundsätzen keine Beschwer.“ 162

Der Antrag in Cordoba II (BGH, aaO, Rn. 5) war wie im vorliegenden Fall ausdrücklich als Hilfsantrag formuliert und lautete: 163

Der Kläger hat - soweit für das Revisionsverfahren noch relevant - zuletzt beantragt, dem Beklagten unter Androhung von Ordnungsmitteln zu verbieten, das [oben eingeblendete] Foto zu vervielfältigen/vervielfältigen zu lassen und/oder öffentlich zugänglich zu machen/machen zu lassen, hilfsweise, Schülerinnen und Schülern zu ermöglichen, das [oben eingeblendete] Foto zum Zwecke des Einstellens ins Internet zu vervielfältigen. 164

Damit kann ein Antragsteller zwar in seinen Anträgen ausdrücklich auf alle drei Haftungsformen Bezug nehmen und diese separat zum Gegenstand seines Begehrens machen. Da es jedoch nur um den Unterlassungsanspruch geht und dieser zugesprochen wurde, wenn auch in der Formulierung „ermöglichen“, hat die hiesige Antragstellerin bei einem Vergleich der ausgeurteilten Unterlassungspflicht und den im Rahmen der Anschlussberufung geltend gemachten Anträge kein Weniger erhalten. Die Handlung, an die die Verbote der „öffentlichen Zugänglichmachung“, des „Hilfeleistens zur öffentlichen Zugänglichmachung“ oder des „Ermöglichens der öffentlichen Zugänglichmachung“ anknüpfen, sind identisch, sodass der Antragsgegnerin mit allen drei Antragsfassungen dasselbe Verhalten verboten würde. Ein Weniger iSd einer Beschwer ist daher nicht ersichtlich.

3. Die Kostenentscheidung beruht auf § 97 Abs.1 ZPO. Das Urteil ist gemäß § 542 Abs. 2 S. 1 ZPO mit seiner Verkündung rechtskräftig. 166

Streitwert für das Berufungsverfahren: bis 100.000 € 167