digital | recht

Schriften zum Immaterialgüter-, IT-,
Medien-, Daten- und Wettbewerbsrecht

Martina Kasch

Auskunftsansprüche gegen Diensteanbieter der Informationsgesellschaft

Band 8

Martina Kasch

Auskunftsansprüche gegen Diensteanbieter der Informationsgesellschaft

digital | recht
Schriften zum Immaterialgüter-, IT-, Medien-, Daten- und Wettbewerbsrecht

Herausgegeben von Prof. Dr. Maximilian Becker, Prof. Dr. Katharina de la Durantaye, Prof. Dr. Franz Hofmann, Prof. Dr. Ruth Janal, Prof. Dr. Anne Lauber-Rönsberg, Prof. Dr. Benjamin Raue, Prof. Dr. Herbert Zech

Band 8

Martina Kasch, geboren 1995, Studium an der Universität Bayreuth, Wissenschaftliche Mitarbeiterin und Doktorandin an der Universität Bayreuth bis 2022, Referendariat in Bayreuth seit 2022

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Angaben sind im Internet über http://dnb.d-nb.de abrufbar.
Dieses Buch steht gleichzeitig als elektronische Version über die Webseite der Schriftenreihe: http://digitalrecht-z.uni-trier.de/ zur Verfügung.

Umschlagsgestaltung von Monika Molin

ISBN: 9783757550974
URN: urn:nbn:de:hbz:385-2023052209
DOI: https://doi.org/10.25353/ubtr-xxxx-9e76-9cf3

Die Schriftenreihe wird gefördert von der Universität Trier und dem Institut für Recht und Digitalisierung Trier (IRDT).
Anschrift der Herausgeber: Universitätsring 15, 54296 Trier.

UNIVERSITÄT TRIER

IRDT Institut für Recht und Digitalisierung Trier

Vorwort

Die vorliegende Arbeit wurde im Januar 2023 als Dissertation bei der rechts- und wirtschaftswissenschaftlichen Fakultät der Universität Bayreuth eingereicht und im Mai 2023 verteidigt. Die Arbeit und die entsprechenden Nachweise beruhen im Wesentlichen auf dem Stand vom Januar des Jahres 2023. Vor der Veröffentlichung wurde jedoch das dritte Kapitel dieser Arbeit auf Anregung der beiden Gutachter in Teilen überarbeitet.

Ich möchte mich zunächst herzlich bei Prof. Dr. Ruth Janal, LL.M bedanken, die mir die Anfertigung dieser Arbeit durch Ihre Betreuung erst ermöglicht hat. Dabei hat sie mr jederzeit mit Ratschlägen und Anregungen zur Verfügung ge-standen, aber mir zugleich viel Freiheit bei der Bearbeitung gelassen. Bei Prof. Dr. Michael Grünberger, LL.M möchte ich mich für die schnelle Erstellung des Zweitgutachtens bedanken.

Zudem bedanke ich mich bei Herrn Prof. Dr. Raue und sämtlichen Herausgebern der Schriftenreihe digital | recht für die Aufnahme in die Schriftenreihe und die großartige Möglichkeit der Open-Access-Veröffentlichung.

Ein weiterer Dank geht an das gesamte Team des Lehrstuhls Zivilrecht VIII an der Universität Bayreuth für die schöne gemeinsame Zeit, in der diese Arbeit überwiegend entstanden ist.

Zuletzt gilt mein Dank meiner gesamten Familie und insbesondere meinen Eltern, meinen beiden Schwestern und meiner Tante Susanne Kasch, die mich bereits mein ganzes Leben lang begleiten und unterstützen.

Bayreuth, Mai, 2023 Martina Kasch

Inhaltsverzeichnis

Abkürzungsverzeichnis

a.A.	andere Ansicht
Abs.	Absatz
a.F.	alte Fassung
AG	Amtsgericht
Alt.	Alternative
Anm.	Anmerkung
Art.	Artikel
Aufl.	Auflage
Az.	Aktenzeichen
Bd.	Band
BDSG	Bundesdatenschutzgesetz
Bearb.	Bearbeiter
BeckOK	Beck'scher Online-Kommentar
betr.	betreffend
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BReg	Bundesregierung
BT-Drucks.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
bzw.	beziehungsweise
CR	Computer und Recht
DesignG	Gesetz über den rechtlichen Schutz von Design
DSGVO	Datenschutz-Grundverordnung
etc.	et cetera
EuGH	Europäischer Gerichtshof
f., ff.	Folgende
Fn.	Fußnote
GebrMG	Gebrauchsmustergesetz
GG	Grundgesetz
ggf.	gegebenenfalls
GRUR	Gewerblicher Rechtsschutz und Urheberrecht

GRUR-Prax	Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter- und Wettbewerbsrecht
GRUR-RR	GRUR Rechtsprechungs-Report
GVG	Gerichtsverfassungsgesetz
Hrsg.	Herausgeber
i.V.m.	in Verbindung mit
JuS	Juristische Schulung
JZ	Juristenzeitung
K&R	Kommunikation & Recht
KUG	Gesetz vom 9.1.1907 betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie
LG	Landgericht
lit.	littera
MarkenG	Gesetz über den Schutz von Marken und sonstigen Kennzeichen
MMR	MultiMedia und Recht
MüKoBGB	Münchener Kommentar zum BGB
m.w.N.	mit weiteren Nachweisen
n.F.	neue Fassung
NJW	Neue Juristische Wochenschrift
NJW-RR	NJW-Rechtsprechungs-Report
Nr.	Nummer
OLG	Oberlandesgericht
PatG	Patentgesetz
RefE	Referentenentwurf
RegE	Regierungsentwurf
RL	Richtlinie
Rn.	Randnummer
S.	Seite
s.a.	siehe auch
sog.	sogenannte/sogenannter/sogenannten
SortenG	Sortenschutzgesetz
str.	strittig
stRspr.	ständige Rechtsprechung
TMG	Telemediengesetz
u.a.	und andere

UrhG	Gesetz über Urheberrecht und verwandte Schutzrechte
Urt.	Urteil
u.v.m.	und vieles mehr
UWG	Gesetz gegen den unlauteren Wettbewerb
vgl.	vergleiche
VO	Verordnung
WRP	Wettbewerb in Recht und Praxis
WWW	World Wide Web
z.B.	zum Beispiel
Ziff.	Ziffer
zit.	zitiert
ZPO	Zivilprozessordnung
z.T.	zum Teil
ZUM	Zeitschrift für Urheber- und Medienrecht
ZUM-RD	ZUM-Rechtsprechungsdienst

Kapitel 1

Einführung und Gang der Untersuchung

Das Internet ist inzwischen längst ein fester Bestandteil des gesellschaftlichen Lebens. Für viele Menschen ist die Internetnutzung selbstverständlich geworden und begleitet sie überall im Alltag und wirkt sich teils bis tief in den privaten Bereich hinein aus. Durch die stetig fortschreitende technische Entwicklung lassen sich heutzutage eine Vielzahl von Informationen in Echtzeit in die ganze Welt übermitteln.

Im Laufe der Zeit hat sich die Rolle der Endnutzer aber verändert: Während private Nutzer früher vor allem Empfänger von Informationen waren, werden sie im Web 2.0 immer stärker auch selbst aktiv.[1] Zahlreiche Internetdienste ermöglichen es ihren Nutzern, selbst eigene Inhalte zu erstellen, mit anderen zu teilen und so Informationen zu verbreiten. Das Internet dient verstärkt der globalen Vernetzung und der Interaktion von Nutzern.

Neben den vielen Vorteilen, die das Internet zweifelsohne bietet, eröffnet es zwangsläufig auch Raum für Rechtsverletzungen: Sei es etwa die Verletzung von Persönlichkeitsrechten durch ehrverletzende Äußerungen in sozialen Netzwerken – oder die Verletzung von Rechten des geistigen Eigentums durch das Austauschen urheberrechtlich geschützter Werke im Internet. Neben vielen positiven und kreativen Nutzungsmöglichkeiten besteht daher auch immer das Risiko, dass Nutzer von Internetdiensten die Rechtsgüter anderer beeinträchtigen.

---

[1] S. zum Begriff des Web 2.0 etwa *Schmidt/Pruß* in: Auer-Reinsdorff/Conrad, § 3 Rn. 121 ff.; *Stanoveska-Slabeva* in: Meckel/ Stanoveska-Slabeva, Web 2.0, S. 13.

A. Das Problem der Identifizierung anonymer Rechtsverletzer im Internet

Sehr häufig können Internetdienste anonym beziehungsweise unter der Verwendung von Pseudonymen genutzt werden. Dies stellt Rechteinhaber regelmäßig vor erhebliche Probleme. Um im Falle einer Rechtsverletzung ihre Rechte gegenüber dem verantwortlichen Nutzer durchsetzen zu können, sind sie zwingend auf die Kenntnis von dessen Identität angewiesen. Um etwaige Ansprüche - zum Beispiel auf Unterlassung oder Schadensersatz - geltend zu machen, benötigen sie den Namen und die Anschrift des rechtsverletzenden Nutzers.

Die Identifizierung eines anonymen Rechtsverletzers im Internet ist nicht nur ein wichtiges Instrument zur Rechtsdurchsetzung, sondern könnte auch zu einer sinnvolleren Verteilung von Verantwortlichkeit zwischen Diensteanbietern und ihren Nutzern beitragen. Oft werden nämlich anstelle der Nutzer die Diensteanbieter in Anspruch genommen, da dies aufgrund der Anonymität der Nutzer häufig der einfachere Weg ist. Auch bei Verwendung des Klarnamens durch den Nutzer wenden sich die Rechteinhaber häufig an den Diensteanbieter, da ohne ladungsfähige Anschrift ein juristisches Vorgehen gegen den Nutzer nicht möglich ist. Selbst wenn dadurch den Rechteinhabern erst einmal Abhilfe geleistet werden kann, besteht die Gefahr, dass den Nutzern das Internet wie ein rechtsfreier Raum erscheint. Es ist naheliegend anzunehmen, dass die Anonymität im Internet rechtsverletzende Handlungen zumindest begünstigt. Dies gilt insbesondere, wenn der Eindruck entsteht, unter dem Deckmantel der Anonymität ohnehin nicht für Rechtsverletzungen belangt werden zu können. Dadurch ist zu befürchten, dass die Anonymität zur Verrohung der Kommunikation im Internet beiträgt.[2]

Ohne die Hilfe der Diensteanbieter besteht meist keine Möglichkeit für die betroffenen Personen, die Identität anonymer Nutzer zu ermitteln. Eine Identifizierung des Rechtsverletzers ist aber gegebenenfalls möglich, wenn die

---

[2] Dies veranlasste beispielsweise den Gesetzgeber zur Schaffung des NetzDG, S. *Regierungsentwurf*, BT-Drs.18/12356, S. 1: „Die Debattenkultur im Netz ist oft aggressiv, verletzend und nicht selten hasserfüllt.“. S. auch *Kühling*, ZUM 2021, 461, 462 f.; *Nolte,* ZUM 2017, 552, 553; *Pille*, NJW 2018, 3545, 3546.

Rechteinhaber die Internetdiensteanbieter auf Auskunft über personenbezogene Daten der Nutzer in Anspruch nehmen könnten. Dies würde die Rechtsdurchsetzung gegenüber anonymen Nutzern ermöglichen. Zudem können Auskunftsansprüche zu einer gerechteren Verantwortungsverteilung führen und die Gefahren zukünftiger Verletzungen reduzieren.

B. Gegenstand der Untersuchung und rechtlicher Rahmen

Die Arbeit befasst sich aus rechtlicher wie technischer Perspektive mit der Frage, wie im Internet anonym bzw. unter einem Pseudonym auftretende Rechtsverletzer identifiziert werden können. Der zentrale Gegenstand der Untersuchung sind die nach geltendem Recht bestehenden Auskunftsansprüche gegen die Anbieter von Internetdiensten.

Sämtliche der zu untersuchenden Auskunftsansprüche knüpfen an eine Rechtsverletzung zum Beispiel nach dem Urheberrechts- oder Markengesetz beziehungsweise eines der in § 823 Abs. 1 BGB geschützten Rechtsgüter an. Aufgrund der besseren Vergleichbarkeit insbesondere im Hinblick auf den Interessenskonflikt zwischen den Beteiligten bleiben über diese Rechtsverletzungen hinausgehende lauterkeitsrechtliche Verstöße, sowie reine Vermögensbeeinträchtigungen in dieser Arbeit außer Betracht.

Teile der untersuchten nationalen Regelungen werden erheblich durch das Unionsrecht beeinflusst. Die vorliegende Arbeit befasst sich schwerpunktmäßig mit Auskunftsansprüchen, die sich im Bereich des geistigen Eigentums etwa aus § 101 UrhG oder § 19 MarkenG, sowie für Verletzungen anderer absoluter Rechte aus § 21 Abs. 2 S. 2 TTDSG oder dem aus § 242 BGB abgeleiteten allgemeinen Auskunftsanspruch ergeben. Im Verhältnis zu anderen Rechtsmaterien ist der Einfluss des Unionsrecht im Bereich des geistigen Eigentums besonders stark ausgeprägt. So dienen etwa die Auskunftsansprüche aus § 101 UrhG und § 19 MarkenG der Umsetzung der Enforcement-Richtlinie.[3] Diese sieht in

[3] Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums, Abl. 2004 L 195, S. 16. S. zur Umsetzung das Gesetz zur Verbesserung der Durchsetzung der Rechte des geistigen Eigentums, BGBl. I 2008, S. 1191.

Art. 8 Abs. 1 lit. c) Enforcement-Richtlinie unter anderem die Einführung eines Anspruchs auf Auskunftserteilung gegen Personen vor, deren Dienste für rechtsverletzende Tätigkeiten genutzt werden.

Das Unionsrecht wirkt sich dabei besonders auf das nationale Urheberrecht aus. Dies gilt vor allem im digitalen Kontext. So dient die InfoSoc-Richtlinie[4] der Harmonisierung bestimmter Aspekte des Urheberrechts und verwandter Schutzrechte in der Informationsgesellschaft und der Erreichung eines hohen Schutzniveaus für Urheber.[5] Dies führte im Jahr 2003 zu einer Modifikation und Ergänzung des nationalen Urheberrechtsgesetzes.[6] Im Jahr 2019 wurden Teile der InfoSoc-Richtlinie durch die DSM-Richtlinie[7] überarbeitet und teilweise ersetzt.[8] Die Umsetzung ins deutsche Recht erfolgte durch das Gesetz zur Anpassung des Urheberrechts an die Erfordernisse des digitalen Binnenmarktes vom 20. Mai 2021. Im Zuge dessen wurden auch das neue Urheberrechts-Diensteanbieter-Gesetz (UrhDaG) geschaffen, das am 01. August 2021 in Kraft getreten ist.[9] Das Unionsrecht wirkt sich insbesondere auf die urheberrechtlich relevanten Verwertungsrechte,[10] auf die urheberrechtlichen Schranken,[11] aber

---

[4] Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, Abl. 2001 L 167, 10.

[5] Vgl. *EuGH,* Urt. v. 26.4.2017 – C-527/15, ZUM 2017, 587 Rn. 27 – Stichting Brein/Wullems; *EuGH,* Urt. v. 14.6.2017 – C-610/15, ZUM 2017, 746 Rn. 22 – Stichting Brein/Ziggo BV (The Pirate Bay); *Grünberger,* ZUM 2018, 271, 279.

[6] *Regierungsentwurf*, BT-Drs. 684/02, S. 1.

[7] Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17. April 2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG, Abl. 2019 L 130, 92.

[8] Allgemein zu DSM-RL siehe etwa *Dreier,* GRUR 2019, 771, 771 ff.; *Spindler,* CR 2019, 277, 277 ff.; *Steinbrecher,* MMR 2019, 639, 639 ff. Zur erheblichen öffentlichen Kritik vor allem zu Art. 17 DSM-RL siehe exemplarisch nur *Weidert/Uhlenhut/von Lintig*, GRUR-Prax 2019, 295, 296 f.

[9] S. dazu z.B. *Frey/Rudolph,* MMR 2021, 671, 672 ff.; *Hofmann,* NJW 2021, 1905, 1906; *Rauer/Bibi,* BB 2021, 1475, 1477; *Waiblinger/Pukas,* MDR 2021, 1489, 1490; *Wandtke/Hauck,* ZUM 2020, 671, 673 ff.; *von Welser,* GRUR-Prax 2021, 463, 463 f.

[10] So dient beispielsweise die Einführung von § 19 a UrhG der Umsetzung von Art. 3 Abs. 1, 2 InfoSoc-Richtlinie mit dem Zweck, der Informationsgesellschaft und den technischen Besonderheiten des Internets und anderer Netzwerke Rechnung zu tragen, S. dazu etwa *Götting* in: BeckOK Urheberrecht, § 19a UrhG Rn. 1.

[11] S. zur Schranke des § 51a UrhG für Karikatur, Parodie und Pastiche etwa *Dreier* in: Dreier/Schulze, § 51 a UrhG Rn. 3.

auch auf die Verantwortlichkeit und Haftung der Diensteanbieter für Urheberrechtsverletzungen ihrer Nutzer aus.[12]

Die Haftung von Internetdiensteanbietern ist aber auch allgemein und über das Urheberrecht hinaus durch die E-Commerce-Richtlinie[13] harmonisiert.[14] Diese sieht Haftungsprivilegierungen für Diensteanbieter vor, die in den §§ 7-11 TMG ins nationale Recht umgesetzt wurden. Perspektivisch wird dieser Bereich durch den Digital Services Act (DSA) noch stärker durch das Unionsrecht reguliert.[15] Der DSA ist am 16.11.2022 in Kraft getreten und gilt gemäß Art. 93 Abs. 2 DSA – abgesehen von einzelnen Regelungen, die bereits vorher zu berücksichtigen sind – ab dem 17. 02.2024. Nach Art. 89 DSA werden die Haftungsprivilegierungen des E-Commerce-Richtlinie durch den DSA gestrichen und ersetzt.

Neben den Vorschriften über die Verletzung absoluter Rechte und den Regelungen zur Haftung und Verantwortlichkeit von Diensteanbietern, müssen auch datenschutzrechtliche Regelungen im Rahmen dieser Arbeit Beachtung finden. Voraussetzung für die Identifizierung eines Rechtsverletzers mittels eines Auskunftsanspruchs ist, dass die Diensteanbieter über die benötigten Daten verfügen und befugt sind, diese an Dritte zur Rechtsdurchsetzung weiterzugeben. Regelungen, die derartige Pflichten und Befugnisse vorsehen, können jedoch im Konflikt mit dem Recht des Verletzers auf Schutz seiner persönlichen Daten und dem Telekommunikationsgeheimnis stehen. Den Ausgangspunkt

---

[12] S. etwa zur Umsetzung der umstrittenen Regelungen des Art. 17 DSM-RL zur Verantwortlichkeit von Online-Plattformen für das Teilen von Online-Inhalten im neuen UrhDaG *Frey/Rudolph,* MMR 2021, 671, 671 ff.; *Hofmann,* NJW 2021, 1905, 1905 ff.; *Rauer/Bibi,* BB 2021, 1475, 1475 ff.; *Waiblinger/Pukas,* MDR 2021, 1489, 1489 ff.; *Wandtke/Hauck,* ZUM 2020, 671, 671 ff.; *von Welser,* GRUR-Prax 2021, 463, 463 ff.

[13] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), Abl. 2000 L 178, 1.

[14] S. zum Verhältnis zwischen Art. 17 DSM-RL und der ECRL etwa *Hofmann,* GRUR 2019, 1219, 1222 f.; *Wandtke/Hauck*, ZUM 2019, 627, 629 ff.

[15] Verordnung (EU) 2022/2065 des europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG. S. noch zum Entwurf des Digital Services Acts etwa *Gielen/Uphues*, EuZW 2021, 627, 627 ff.; *Janal,* ZEuP 2021, 227, 227 ff.; *Kühling*, ZUM 2021, 461, 461 ff.; *Spindler*, GRUR 2021, 545, 545 ff.; *Spindler,* GRUR 2021, 653, 653 ff.

für die Zulässigkeit jeglicher Datenverarbeitung stellt die im Jahr 2018 in Kraft getretene Datenschutzgrundverordnung (DS-GVO) dar.[16] Spezielle Regelungen für die Anbieter von Telemedien- und Telekommunikationsdiensten enthalten zudem die Vorschriften des neuen TTDSG und des TKG. Die dort aufgeführten Regelungen für Telekommunikationsdienste beruhen größtenteils auf Vorschriften der e-Privacy-Richtlinie.[17]

C. Ziel der Untersuchung

Das Ziel der Arbeit ist es, einen allgemeinen Auskunftsanspruch gegen Internetdiensteanbieter zu entwickeln, mit dem Rechteinhaber die Identität eines anonymen rechtsverletzenden Nutzers ermitteln können. Dabei wird eine weitgehende Gleichbehandlung der Rechteinhaber verschiedener absoluter Rechte angestrebt. Es sollen zum einen die materiellen Voraussetzungen eines solchen Anspruchs entwickelt werden, zum anderen aber auch die notwendigen Rahmenbedingungen für die Durchsetzbarkeit und Praktizierbarkeit eines solchen Anspruchs erläutert werden. Dazu werden prozessuale und datenschutzrechtliche Aspekte betrachtet, um ein für die Rechteinhaber möglichst effektives, aber dennoch für Internetnutzer möglichst grundrechtsschonendes Rechtsdurchsetzungsinstrument zu schaffen.

D. Gang der Untersuchung

Im Anschluss an die Einführung wird im 2. Kapitel der Arbeit zunächst das Problem anonymer Rechtsverletzungen im Internet näher betrachtet. Dazu wird der Begriff der Anonymität erläutert. Zudem werden die beteiligten

---

[16] Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Abl. 2016 L 119, 1.

[17] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), Abl. 2002 L 201, 37.

Parteien einer Rechtsverletzung im Internet - also Diensteanbieter, Rechteinhaber und Nutzer – dargestellt. Darüber hinaus soll die Arbeit einen Überblick über die in der Praxis häufig bei der Nutzung von Internetdiensten auftretenden Rechtsverletzungen absoluter Rechte geben.

Daran anknüpfend wird im 3. Kapitel der Interessenskonflikt, der bei einer Rechtsverletzung durch anonyme Nutzer zwischen den beteiligten Parteien entsteht, beleuchtet. Auf der Seite aller beteiligten Parteien stehen durch die Grundrechtecharta der europäischen Union und das Grundgesetz geschützte Interessen, die sich auch auf die zivilrechtliche Rechtsdurchsetzung auswirken. Die Darstellungen in diesem Teil sollen Anhaltspunkte geben für einen angemessenen Ausgleich der widerstreitenden Interessen und stellen somit die Basis für den am Ende dieser Arbeit zu entwickelnden Auskunftsanspruch de lege ferenda dar.

Das 4. Kapitel der Arbeit setzt sich mit den technischen Begebenheiten einer anonymisierten Nutzung von Internetdiensten auseinander. Vor allem werden die tatsächlichen Möglichkeiten der Identifizierung eines anonymen Rechtsverletzers im Internet analysiert.

Diese an der Praxis orientierten Ausführungen bilden die Grundlage für die sich im 5. Kapitel der Arbeit anschließende Untersuchung der de lege lata existierenden rechtlichen Möglichkeiten zur Identifizierung von anonymen Rechtsverletzern. So werden die je nach beeinträchtigtem Rechtsgut möglicherweise in Betracht kommenden Anspruchsgrundlagen für einen Auskunftsanspruch gegen Internetdiensteanbieter erörtert. Hierbei gilt es unter anderem zu beurteilen, inwieweit diese Anspruchsgrundlagen bei der Identifizierung von Rechtsverletzern im Internet Anwendung finden und tatsächlich zu einer Identifizierung eines Rechtsverletzers führen können. Die de lege lata bestehenden Auskunftsmöglichkeiten werden zu diesem Zweck untersucht und miteinander verglichen. Besonderes Augenmerk liegt dabei auch auf dem Konflikt der Auskunftsansprüche mit dem Datenschutzrecht. Zudem werden prozessuale Besonderheiten von Auskunftsverfahren in den Blick genommen.

Das 6. Kapitel der Arbeit beschäftigt sich mit der Frage, ob anderweitige Möglichkeiten der Rechtsdurchsetzung existieren, die eine Identifizierung von

Rechtsverletzern mittels zivilrechtlicher Auskunftsansprüche überflüssig machen könnten. Dabei wird die Möglichkeit untersucht, ein Strafverfahren gegen anonyme Rechtsverletzer im Internet einzuleiten. mit dem Ziel, die Identität der Rechtsverletzer durch Akteneinsicht in dem Strafverfahren zu ermitteln. Daneben kommt außerdem eine Inpflichtnahme der Diensteanbieter als Alternative zur Identifizierung der anonymen Nutzer in Betracht. Dies hätte den Vorteil, dass keinerlei Einschränkungen hinsichtlich der Anonymität der Nutzer von Internetdienstleistungen erforderlich wären. Allerdings ist fraglich, ob die alleinige Inanspruchnahme der Diensteanbieter im Einklang mit dem Rechtsschutzinteresse des Verletzten steht und rechtspolitisch sinnvoll ist. Die Ausführungen in diesem Kapitel stellen die Grundlage für die anschließend angestellten Überlegungen dar, wie de lege ferenda die verschiedenen Rechtsdurchsetzungsinstrumente miteinander in Einklang gebracht werden können.

Die in den ersten Teilen der Arbeit gewonnenen Erkenntnisse sollen insgesamt dazu beitragen, im 7. Kapitel einen allgemeinen Auskunftsanspruch gegen Internetdiensteanbieter zur Identifizierung von anonymen Rechtsverletzern de lege ferenda zu entwickeln. Das Hauptaugenmerk liegt darauf, die widerstreitenden Interessen zu einem angemessenen Ausgleich zu bringen. Dazu werden die materiellen Voraussetzungen, Inhalt und Umfang eines solchen Anspruchs erarbeitet, sowie die notwendigen prozessualen und datenschutzrechtlichen Rahmenbedingungen erörtert.

Die Ergebnisse dieser Untersuchungen und die gewonnenen Erkenntnisse werden anschließend (8. Kapitel) zusammengefasst.

Kapitel 2

Anonyme Rechtsverletzungen im Internet

Die vorliegende Arbeit versucht eine Lösung für den Umgang mit Rechtsverletzungen durch anonyme Nutzer von Internetdiensten zu finden und widerstreitende Interessen zu einem angemessenen Ausgleich zu bringen. Daher gilt es zunächst den Begriff der Anonymität zu definieren (A.), die beteiligten Parteien näher zu bestimmen (B.) und typische Rechtsverletzungen im Internet zu untersuchen. (C.)

A. Anonymität im Internet

Häufig ist es möglich, Internetdienste anonym zu nutzen. Das bedeutet aber nicht, dass die Nutzung keinerlei Spuren hinterlässt. Die Anonymität von Internetnutzern kann jedoch die Rechtsdurchsetzung erheblich erschweren. Damit stellt sie den Ausgangspunkt der dieser Arbeit zugrundeliegenden Problematik dar.

I. Begriff der Anonymität

Der Begriff der Anonymität stammt vom altgriechischen Wort ἀνώνυμος (anonymos) ab und bedeutet so viel wie „namenlos".[1] Demnach spricht man von Anonymität, wenn ein Sachverhalt oder eine Handlung keiner bestimmten Person zugeordnet werden kann.[2] Aus diesem Umstand ergibt sich aber auch, dass Anonymität sich stets aus dem Verhältnis zu einer Person ableiten lässt, die diese Zuordnung nicht vornehmen kann.[3] Dies setzt jedoch nicht zwingend voraus, dass die Person keinerlei Informationen über die andere Partei besitzt, sondern lediglich, dass die vorhandenen Informationen für die Identifizierung einer

---

[1] *Rost* in: Bäumler/Mutius, Anonymität, S. 63; Vgl. *Schaar*, Datenschutz im Internet, S. 157.

[2] *Brunst,* Anonymität im Internet, S. 7; *Nietsch*, Anonymität und Durchsetzung, S. 14.

[3] Ähnlich auch *Nietsch*, Anonymität und Durchsetzung, S. 18.

Person nicht ausreichen.[4] Ebenso spielt es zunächst keine Rolle, ob ein Dritter über entsprechende Kenntnisse verfügt und die Zuordnung vornehmen kann.[5]

Allerdings wirken sich etwaige Identifizierungsmöglichkeiten auf den Grad der Anonymität aus. Je mehr Menschen in der Lage sind, ein bestimmtes Verhalten oder einen Sachverhalt der Identität einer Person zuzuordnen, und je mehr Informationen über diese Person bekannt sind, desto niedriger ist der Grad der Anonymität.[6]

Der dieser Arbeit zugrundeliegende Begriff umfasst als Sonderfall grundsätzlich auch die Pseudonymität. Pseudonyme dienen dazu, die Identität einer Person mittels einer Kennung zu verschleiern, die nicht dem tatsächlichen Namen entspricht.[7] Hierbei lässt sich zwar ebenfalls die Identität der hinter dem Pseudonym stehenden Person zumindest nicht auf den ersten Blick aufdecken, allerdings lassen sich bestimmte Handlungen dem entsprechendem Pseudonym zuordnen.[8] Sofern es sich nicht um „öffentliche Pseudonyme" handelt, bei denen für jedermann einsehbar ist, welche Person hinter dem Pseudonym steht, kann auch bei der Verwendung eines Pseudonyms zumindest von einem gewissen Grad der Anonymität ausgegangen werden.[9]

II. Anonymität bei der Nutzung von Internetdiensten

Die gesellschaftliche Konnotation des Begriffs der Anonymität hat sich mit dem zunehmenden Wandel hin zu digitalen Kommunikationsformen und dem erhöhten Bewusstsein für den Schutz personenbezogener Daten erkennbar verändert.[10] Wer sich in der Öffentlichkeit anonym äußerte, sah sich früher wohl

---

[4] Vgl. *Brunst, Anonymität im Internet*, S. 7.

[5] *Nietsch*, Anonymität und Durchsetzung, S. 18.

[6] So auch *Nietsch*, Anonymität und Durchsetzung, S. 18.

[7] *Nietsch*, Anonymität und Durchsetzung, S. 18; *Schaar,* Datenschutz im Internet, Rn. 161.

[8] S. dazu *Brunst,* Anonymität im Internet, S. 27 m.w.N.

[9] Ein Beispiel für ein öffentliches Pseudonym ist eine Telefonnummer, die in einem öffentlichen Telefonbuch aufgeführt ist, S. *Nietsch*, Anonymität und Durchsetzung, S. 19. S. zur Unterscheidung zwischen öffentlichen, nicht öffentlichen und anonymen Pseudonymen *Pfitzmann/Waidner/Pfitzmann*, DuD 1990, 243, 247 f.; *Roßnagel/Scholz*, MMR 2000, 721, 725.

[10] *Brunst*, Anonymität im Internet, S. 9 f; *Kersten*, JuS 2017, 193.

häufiger der Kritik ausgesetzt, er stünde nicht zu seiner Meinung.[11] Anonyme Meinungsäußerungen wurden entsprechend eher als unhöflich angesehen. Auch veröffentlichen die meisten traditionellen Printmedien in der Regel keine anonymen Leserbriefe.[12] Im Internet verhält sich dies jedoch anders: Die Möglichkeit der anonymen Meinungskundgabe wird als wichtiges Instrument zur Sicherung grundrechtlicher Freiheiten und insbesondere als Ausprägung der Meinungsfreiheit angesehen.[13]

Aber auch über Meinungsäußerungen hinaus kommt der Anonymität im Internet eine besondere Bedeutung zu. So spricht beispielsweise der *BGH* davon, dass die anonyme Nutzung „dem Internet immanent" sei.[14] Gestützt wird diese Aussage von der Regelung des § 19 Abs. 2 TTDSG.[15] Danach müssen die Anbieter von Telemediendiensten ihren Nutzern die anonyme Nutzung des Dienstes oder die Nutzung unter einem Pseudonym ermöglichen, sofern dies technisch möglich und zumutbar ist.

Dennoch besteht kaum eine „vollständige Anonymität" im Internet, da im Unterschied zur analogen Welt nahezu jede Handlung im Online-Bereich ihre Spuren hinterlässt.[16] Während im alltäglichen Leben Aktivitäten wie zum Beispiel

---

[11] *Bernreuther*, AfP 2011, 218, 222 f.; *Greve/Schärdel*, MMR 2008, 644, 648; *Kühling*, NJW 2015, 447, 448.

[12] S. dazu exemplarisch bei den drei größten überregionalen Tageszeitungen https://www.faz.net/hilfe/richtlinien-fuer-lesermeinungen-160626.html; https://www.sueddeutsche.de/service/brief-schreiben-schreiben-sie-uns-ihre-meinung-1.1284148; https://www.bild.de/corporate-site/kontakt/bildchannel-home/kontakt-43829628.bild.html (Stand jeweils: 24.05.2022)

[13] BGH, Urt. v. 23.6.2009 - VI ZR 196/08, NJW 2009, 2888 Rn. 38 - Spickmich; BVerfG, NJW 1997, 386; *Lagasnerie*, Die Kunst der Revolte, 80 ff., 96 ff., 140, 145 f; Ohly, AfP 2011, 428, 436; Kühling, NJW 2015, 447, 448; Rössler in: Bäumler/Mutius, S. 28 f. S. auch Thiel, zfmr 1/2016, 9, 13 ff, der die Bedeutung der Anonymität in der „Offline-Gesellschaft" mit dem Stellenwert der Anonymität im digitalen Zeitalter vergleicht.

[14] *BGH*, Urt. v. 23. 6. 2009 - VI ZR 196/08, NJW 2009, 2888 Rn. 38 - Spickmich.

[15] S. aber zur restriktiven und unionsrechtskonformen Auslegung von damals noch § 13 Abs. 6 TMG *Bock*, GRUR-Prax 2021, 30, 30 mit Anmerkung zu *OLG München*, Urt. v. 8.12.2020 – 18 U 2822/19, BeckRS 2020, 34203. S. auch *Kersten,* JuS 2017, 193, 195 f.

[16] *Brunst,* Anonymität im Internet, S. 9; *Härting,* NJW 2013, 2065, 2069; *Nietsch,* Anonymität und Durchsetzung, S. 59. Kritisierend *Thiel*, zfmr 1/2016, 9, 13 ff.

das Einkaufen in der Regel anonym ablaufen,[17] wird im Internet bei jedem Aufruf einer beliebigen Webseite eine Vielzahl an Daten an den Server der Webseite übertragen. Sobald jemand eine Internetseite aufruft, überträgt beispielsweise der Browser die IP-Adresse an den entsprechenden Server. Dazu zählen zum Beispiel IP-Adressen, Namen, Wohnanschriften, Kontodaten, Telefonnummern und E-Mail-Adressen. Teilweise legen sich Nutzer – z.B. von sozialen Netzwerken, Foren oder Online-Plattformen – Profile an, mit denen sie nach außen hin nur unter einem Pseudonym auftreten, während sie gegenüber dem Diensteanbieter verschiedene personenbezogene Daten angegeben haben.

Je mehr Daten die Diensteanbieter über ihre Nutzer erheben, desto vielfältiger können die Möglichkeiten der Reidentifizierung sein. Entsprechend ist auch die Wahrscheinlichkeit höher, dass Dritten – hier den Rechteinhabern – eine Deanonymisierung gelingen kann. Um dem entgegenzuwirken, ermöglichen Anonymisierungsdienste den Nutzern, ihre Identität den Diensteanbietern gegenüber zu verschleiern, indem zum Beispiel die IP-Adresse verborgen wird.

III. Anonymität im Verhältnis zu den Rechteinhabern

Die für diese Arbeit maßgebliche Definition der Anonymität ergibt sich aus dem Verhältnis zwischen dem (rechtsverletzenden) Nutzer und dem Inhaber des beeinträchtigten Rechtsguts. Die anonyme Nutzung des Internets i.S.d. § 19 Abs. 2 TTDSG wirkt sich unmittelbar auf dieses Verhältnis aus, da die Nutzer vor allem nach außen hin – also auch gegenüber den Rechteinhabern – anonym oder nur unter einem Pseudonym auftreten können.[18]

Von Anonymität ist entsprechend der oben genannten Begriffsbestimmung dann auszugehen, wenn die Rechteinhaber ein Verhalten oder eine Handlung nicht einer Person zuordnen können. Identifizierungsmöglichkeiten der Diensteanbieter spielen nur im Zusammenhang mit dem Grad der Anonymität

---

[17] *Brunst,* Anonymität im Internet, S. 9. Ähnlich auch *Thiel*, zfmr 1/2016, 9, 13 ff., der die Bedeutung der Anonymität in der „Offline-Gesellschaft" mit dem Stellenwert der Anonymität im digitalen Zeitalter vergleicht.

[18] S. noch zu § 13 Abs. 6 TMG a.F. *OLG Düsseldorf,* Urt. v. 7.6.2006 - I-15 U 21/06, MMR 2006, 618, 620 m. Anm. *Eichelberger*; *OLG Hamburg*, Urt. v. 4.2.2009 – 5 U 180/07, ZUM 2009, 417, 420 – Long Island Ice Tea; *Lauber-Rönsberg*, MMR 2014, 10, 13; Zu § 19 Abs. 2 TTDSG *Schwartmann,* ZD 2022, 133, 133 f.

eine Rolle. Um ihre Rechte gerichtlich durchsetzen zu können, ist für die Rechteinhaber vor allem die Kenntnis von Namen und ladungsfähiger Anschrift des Nutzers entscheidend. Dementsprechend spricht *Nietsch* von einer juristischen Anonymität, da im Rechtsverkehr sonstige Identifizierungsmerkmale – wie beispielsweise E-Mail-Adressen – als solches nicht ausreichend sind.[19]

Anonymität im Sinne dieser Arbeit liegt also immer dann vor, wenn die Rechteinhaber der Handlung keinen Nutzer zuordnen können, dessen Identität ihnen bekannt ist.[20]

B. Beteiligte

Die vorliegende Arbeit befasst sich mit der Identifizierung anonymer Rechtsverletzer mittels Auskunftsansprüchen. Deshalb konzentrieren sich die Ausführungen ausschließlich auf Dreieckskonstellationen, bei denen die Rechteinhaber von Internetdiensteanbietern Auskunft über personenbezogene Daten eines - mit dem Diensteanbieter nicht identischen - Rechtsverletzers erhalten könnten.[21]

Zu den Beteiligten gehören in diesen Fällen daher die Rechteinhaber, sowie die rechtsverletzenden Internetnutzer und mindestens ein Diensteanbieter, der die rechtsverletzende Handlung seines Nutzers ermöglicht hat.

I. Rechteinhaber

Rechteinhaber im Sinne dieser Arbeit können alle natürlichen und juristischen Personen, sowie rechtsfähige Personenvereinigungen sein, die Träger absolut geschützter Rechte sind. Zu den betroffenen Rechtsgütern zählen etwa

---

[19] *Nietsch*, Anonymität und Durchsetzung, S. 16 f.

[20] Vgl. auch die Definition zur Anonymität in der juristischen Praxis bei *Nietsch*, Anonymität und Durchsetzung, S. 22.

[21] Daher spielen etwa die Anbieter von Suchmaschinen keine besondere Rolle im Rahmen dieser Arbeit, da sie nicht zur Identifizierung der Anbieter von über die Suchmaschine abrufbaren Inhalten beitragen können. Davon unabhängig ist außerdem, ob auch die Diensteanbieter selbst in irgendeiner Weise für die Rechtsverletzung verantwortlich gemacht werden können.

Persönlichkeitsrechte, Rechte des geistigen Eigentums, Leben, körperliche Unversehrtheit und das Recht am eingerichteten und ausgeübten Gewerbebetrieb.

II. Diensteanbieter

Der Begriff des Diensteanbieters taucht in verschiedenen nationalen und unionsrechtlichen Regelungen auf. Vor allem ist er Grundlage für die Anwendbarkeit der Haftungsprivilegierungen der §§ 7-10 TMG. Nach der Legaldefinition in § 2 Nr. 1 TMG ist ein Diensteanbieter „jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt". Art. 2 lit. a) der E-Commerce-RL, deren Umsetzung die Haftungsregelungen des TMG dienen, greift wiederum auf die Definition des Begriffs des „Dienstes der Informationsgesellschaft" aus Art. 1 Abs. 1 lit. b) der Info-Richtlinie[22] zurück. Eine Dienstleistung der Informationsgesellschaft ist demnach „jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung".

Die für diese Arbeit maßgebliche Definition des Diensteanbieters geht noch über dieses Begriffsverständnis hinaus. Es ist weder eine entgeltliche Erbringung des Dienstes erforderlich, wie es etwa die E-Commerce-RL vorsieht,[23] noch ist die Tätigkeit auf die Bereitstellung oder Vermittlung von Informationen beschränkt, sodass anders als nach § 2 Nr. 1 TMG auch Dienste erfasst werden, die rein administrative Aufgaben erfüllen. Diensteanbieter im Sinne dieser Arbeit sind alle natürlichen und juristischen Personen, sowie rechtsfähigen Personenvereinigungen, die Internetdienste jeglicher Art anbieten. Rundfunkdienste im Sinne des § 2 RStV sind allerdings zum Zweck der besseren Vergleichbarkeit vom Anwendungsbereich dieser Arbeit ausgenommen.[24]

---

[22] Richtlinie (EU) 2015/1535 des europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft, Abl. 2015 L 241, 1.

[23] Auch nach der E-Commerce RL ist es jedoch ausreichend, wenn kommerzielle Absichten vorliegen, und kommt es nicht auf eine Entgeltzahlung durch die Nutzer an; S. dazu Erwägungsgrund 18 der E-Commerce-RL; *EuGH,* Urt. v. 15.9.2016 – C-484/14, NJW 2016, 3503, Rn. 40 - McFadden.

[24] S. zur Abgrenzung von Rundfunk und Telemediendiensten *Martini* in: BeckOK Informations- und Medienrecht, § 1 TMG Rn. 15.

Die Erscheinungsformen von Internetdiensten sind sehr vielfältig. Zudem bringen technischer Fortschritt, Innovation und ein geändertes Nutzerverhalten auch immer wieder neue Formen von Internetdiensten hervor. Die Anbieter von Internetdiensten unterscheiden sich sowohl in Bezug auf den Grad ihrer Verantwortlichkeit für eine Rechtsverletzung als auch in dem Beitrag, den sie für eine Identifizierung ihrer Nutzer leisten könnten, erheblich voneinander. Daher ist es erforderlich, eine Kategorisierung von Internetdiensten vorzunehmen. Ein Internetdienstleister kann dabei verschiedene Arten der Internetdienstleistung gleichzeitig erbringen. Für die Abgrenzung kommt es stets auf die im konkreten Einzelfall genutzte Funktion an.

Einen ersten Anhaltspunkt für die Abgrenzung bieten die auf der E-Commerce-RL basierenden Regelungen zu den Haftungsprivilegien von Diensteanbietern aus den §§ 8-10 TMG. Die Vorschriften unterscheiden zwischen der Durchleitung (Zugangsanbietern), der Zwischenspeicherung (Cache-Providern) und der Speicherung von Informationen (Host-Providern).

1. Zugangsanbieter

Zugangsanbieter im Sinne des § 8 TMG vermitteln ihren Nutzern den Zugang zum Internet und damit sämtlichen Online-Diensten. Als „Schnittstelle" zwischen den Nutzern und dem Internet nehmen sie daher unter den Internet-Diensteanbietern eine herausragende Stellung ein und können für die Identifizierung von Internetnutzern eine zentrale Funktion innehaben. [25]

In erster Linie handelt es sich hierbei um Access-Provider, die ihren Kunden – meist auf vertraglicher Basis und gegen Entgelt – Zugang zum Internet gewähren, indem sie eine entsprechende „Netzwerkinfrastruktur" unterhalten.[26] In Deutschland erbringt zum Beispiel die Telekom eine entsprechende Dienstleistung. Access-Provider stellen einen Einwahlknoten zur Verfügung, der die Verbindung der Nutzer mit dem betreffenden Computernetz herstellt.[27] Dabei

---

[25] *Brunst,* Anonymität im Internet, S. 47.

[26] *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 4, 47; *Jones,* Urheberrechtliche Haftung, S. 8; *Pfitzmann/Köpsell/Kriegelstein,* Sperrverfügungen, S. 21; *Wehr/Ujica,* MMR 2010, 667, 668.

[27] *Sandor,* Datenspeicherung, Rn. 421 f.; *Welp,* Auskunftspflicht von Access-Providern, S. 6; *Wehr/Ujica,* MMR 2010, 667, 668.

weisen sie ihren Nutzern eine IP-Adresse zu, die zu jedem Zeitpunkt nur einmal vergeben ist und ermöglichen so den Datenaustausch im Internet.[28]
Neben den Access-Providern sind auch die Betreiber von WLAN-Netzwerken den Zugangsanbietern zuzuordnen.[29] Hierbei handelt es sich häufig um Privatpersonen oder Unternehmen, die durch den Betrieb eines WLAN-Routers einen lokalen Zugang zum Internet einrichten.[30] Privatpersonen stellen Dritten diese Zugriffspunkte teilweise wissentlich, teilweise aber auch unwissentlich zur Verfügung, wenn der WLAN-Zugang nicht oder nur unzureichend gesichert ist.[31]

Ebenfalls um Zugangsanbieter handelt es sich bei Institutionen wie Schulen oder Universitäten und Internet-Cafés, insofern sie durch das Bereitstellen einer entsprechenden Infrastruktur Zugang zum Internet verschaffen.[32]

2. Host-Provider

Host-Provider speichern die Inhalte ihrer Nutzer und können diese wiederum Dritten zugänglich machen. In dieser Gruppe von Diensteanbietern haben sich neben Diensten, die klassisches Webhosting leisten oder ihren Kunden und Nutzern lediglich Speicherplatz zur Verfügung stellen, auch Dienste etabliert,

---

[28] Vgl. *Bange,* Von SoPA zum Copyright Alert System, S. 40; *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 47; *Heid,* Haftung bei Urheberrechtsverletzungen im Netz, S. 1; *Jones,* Urheberrechtliche Haftung, S. 8; *Paal/Hennemann* in: BeckOK Informations- und Medienrecht, § 8 TMG Rn. 15.

[29] WLAN-Betreiber können nach einem weiten Begriffsverständnis ebenso den Access-Providern zugeordnet werden, allerdings werden, um Missverständnissen vorzubeugen, im Folgenden WLAN-Betreiber gesondert behandelt und der Begriff des Access-Provider entsprechend enger gefasst; S. dazu auch *EuGH,* Urt. v. 15.9.2016 – C-484/14, GRUR 2016, 1146 Rn. 66 ff. – McFadden; *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 50, der WLAN-Betreiber als „Access-Provider im weiteren Sinne" bezeichnet. S. auch *Hartmann*, Unterlassungsansprüche, S. 12.

[30] Vgl. *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 50.

[31] *Habermann,* Zivilrechtliche Störerhaftung, S. 8. S. zur Frage der Diensteanbietereigenschaft i.S.v. § 2 Nr. 1 TMG bei unwissentlich agierenden privaten WLAN-Betreibern *Brüggemann,* Drittauskunftsanspruch, S. 98 f.

[32] Vgl. *Feldmann,* K&R 2011, 225, 226; *Liesching/Knupfer,* MMR 2003, 562, 565 ff.

die stärker auf einem Austausch der Nutzer basieren.[33] Die Nutzer haben dabei oft die Möglichkeit eigene Inhalte zu erstellen und mit anderen zu teilen (sog. nutzergenerierte Inhalte).[34]

Besonders im Fokus der juristischen Diskussion stehen Online-Plattformen. So sieht etwa der Digital Services Act der europäischen Kommission (DSA) spezielle Regelungen für Online-Plattformen in den Art. 16 ff. DSA vor.[35] Plattformen werden nach Art. 3 lit. i) DSA als Unterfall von Host-Providern definiert, „der im Auftrag eines Nutzers Informationen speichert und öffentlich verbreitet". Der Unterschied zu anderen Host-Providern besteht demnach im Wesentlichen darin, dass Inhalte im Auftrag der Nutzer öffentlich zugänglich gemacht werden.[36]

Über diese sehr weitreichenden Definition hinaus lassen sich Plattformen aber gut anhand der Funktionsweise und äußeren Merkmalen stärker eingrenzen:[37] Die Nutzung einer Plattform setzt regelmäßig die Eingabe von Zugangsdaten voraus.[38] Häufig erstellen die Nutzer dabei Profile, denen die Inhalte zugeordnet werden können.[39] Plattformen speichern Nutzerinhalte, indem sie es ihren Nutzern ermöglichen, Inhalte hochzuladen und zu teilen. Andere Nutzer erhalten Zugriff auf diese Inhalte und können sie gegebenenfalls herunterladen. Die Plattformen schaffen die technische Infrastruktur dafür und stellen meist Regeln für die Aktivitäten der Nutzer auf.

---

[33] Vgl. *Askani,* Private Rechtsdurchsetzung, S. 53 f.; *Bange,* Von SoPA zum Copyright Alert System, S. 40; *Fischer,* Einbindung von Providern, S. 19.

[34] S. dazu *Habermann,* Zivilrechtliche Störerhaftung, S. 13 ff.; *Jones*, Urheberrechtliche Haftung, S. 10 f.

[35] Vorschlag der europäischen Kommission für eine Verordnung des europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG, COM (2020) 825 final. Der Entwurf unterscheidet zwischen Regelungen für alle Provider und spezielle Regelungen für Plattformen große und besonders große Plattformen.

[36] Vgl. *Spindler,* GRUR 2021, 653, 653 f.

[37] S. dazu *Janal,* ZEuP 2021, 227, 273, die die fehlende „Trennschärfe" der Abgrenzung von Plattformen und Host-Providern im DSA-E kritisiert.

[38] Vgl. *Schmittmann* in: Hoeren/Sieber/Holznagel, Teil 9 Rn. 7.

[39] Vgl. *Schmittmann* in: Hoeren/Sieber/Holznagel, Teil 9 Rn. 7.

Dazu zählen etwa soziale Netzwerke[40] wie „Facebook“, „Twitter“ und „Instagram“ und Chatrooms,[41] Streamingdienste wie „YouTube“, Bewertungsportale wie „golocal“ und „TripAdvisor“ und Online-Marktplätze oder Online-Auktionshäuser wie „eBay“. Aber auch Sharehosterdienste wie „Flickr“, die im Auftrag ihrer Nutzer deren Dateien speichern und es ermöglichen, diese - meist mittels einem Link - mit anderen zu teilen, können als Plattform angesehen werden.

Neben den Plattformen können auch Kommentarspalten, Gästebücher, etc. einen Hosting-Dienst darstellen.

3. Cache-Provider

Während Host-Provider die Inhalte ihrer Nutzer langfristig speichern, nehmen Cache-Provider lediglich eine automatische kurzzeitige Zwischenspeicherung mit dem Zweck, die Übermittlung von Inhalten effizienter zu gestalten, vor.

Diesen Zweck erfüllen vor allem Proxy-Cache-Server, die auf Veranlassung ihrer Nutzer Informationen in einem Cache zwischenspeichern. Möchte ein Nutzer auf einen Inhalt zugreifen, der bereits im Cache vorhanden ist, erhält er die Daten direkt vom Proxy-Cache-Server. Andernfalls fordert der Proxy die Inhalte neu an und leitet sie weiter. Die Anfrage an den Zielserver erfolgt unter der IP-Adresse des Proxy-Cache-Servers, der die Inhalte wiederum an die IP-Adresse des Nutzers weiterleitet. Proxy-Cache-Server sind also der Kommunikation zwischen Client und Server zwischengeschaltet.

4. Weitere Diensteanbieter und Sonderfälle

Die Differenzierung zwischen Access-, Host- und Cache-Providern ist nicht ausreichend, um alle in dieser Arbeit behandelten Internetdienste zu erfassen. Manche Dienste lassen sich nämlich gar nicht oder nicht eindeutig in eine der genannten Kategorien einordnen.

---

[40] S. zur Einordnung sozialer Netzwerke als Host-Provider *EuGH,* Urt. v. 16. 2. 2012 - C-360/10, GRUR 2012, 382 – Netlog/SABAM.

[41] Ausführlich zu den Chatrooms, S. *Spindler* in: Spindler/Schmitz, § 10 TMG Rn. 77 ff.

a) Content-Provider

Anders als Zugangsanbieter, Host- und Cache-Provider stellen Content-Provider ihren Nutzern eigene Inhalte zur Verfügung. Dies sind zum Beispiel Betreiber eines Blogs, einer Website, eines Streamingdienstes oder Webshops oder Nutzer einer Plattform, über die nutzergenerierte Inhalte verbreitet werden.[42] Bezogen auf die Inhalte selbst, spielen Content-Provider in der Rolle als Diensteanbieter im Rahmen dieser Arbeit eine eher untergeordnete Rolle, da sie zwar gegebenenfalls selbst rechtsverletzende Inhalte zur Verfügung stellen, dies aber nicht ihren Nutzern ermöglichen. Insofern steht in den meisten Fällen ihre Rolle als Nutzer zum Beispiel von Webhosting- oder Zugangsdiensten und Diensten des Domain Name Systems im Vordergrund. Etwas anderes gilt aber, wenn (auch) die Nutzung der Inhalte selbst rechtswidrig ist. Dies kann etwa der Fall sein, wenn Nutzer urheberrechtlich geschütztes Material des Content-Providers streamen. In diesen Fällen wird aber das Vorgehen gegen den Content-Provider selbst und nicht gegen dessen Nutzer im Vordergrund stehen.

b) Interpersonelle Kommunikationsdienste

Eine ähnliche Differenzierung ist auch bei interpersonellen Kommunikationsdiensten vorzunehmen. Diese Dienste bieten basierend auf dem Internet eine Alternative zu traditionellen Telekommunikationsdiensten wie der Post und klassischer Telefonie.[43] Neben Mail-Diensten zählen dazu auch Messenger- und Internettelefonie-Dienste wie Skype, WhatsApp, der Facebook-Messenger, Telegram, etc.

Bei interpersonellen Kommunikationsdiensten muss zwischen den konkreten Tätigkeiten des Dienstes unterschieden werden. Das bloße Weiterleiten von Nachrichten oder Mails fällt unter die Zugangsverschaffung im Sinne des

---

[42] Vgl. *Jones,* Urheberrechtliche Haftung, S. 11.

[43] Im Falle eines Mail-Dienstes werden beispielsweise den Mailadressen die IP-Adressen der Endgeräte zugeordnet; vgl. *EuGH,* Urt. v. 13.6.2019 – C-193/18, MMR 2019, 514 – Google LLC; *OVG Münster*, Urt. v. 05.02.2020 - 13 A 17/16, BeckRS 2020, 2401, Rn. 30 – Meldepflicht von Gmail.

§ 8 TMG.[44] Soweit die Nachrichten aber für die Nutzer zum Beispiel bei einem Web-Mail-Dienst gespeichert werden, handelt es sich um Host-Provider.[45]

c) Anonymisierungsdienste

Anonymisierungsdienste werden vor allem von Endnutzern eingesetzt, um sich sicher oder unerkannt im Internet zu bewegen. Auch wenn sich ihre Funktionsweise unterscheidet, sind Anonymisierungsdienste meist dem unmittelbaren Datenaustausch zwischen Nutzer und dem aufgerufenen Server zwischengeschaltet. Sie dienen in der Regel dem Zweck, die IP-Adresse des Nutzers zu verschleiern. Damit sorgen sie für einen deutlich höheren Grad an Anonymität der Internetnutzer.

Solche Anonymisierungsdienste beteiligen sich an der Datenübertragung bei der Kommunikation im Internet und sind damit Zugangsanbieter i.S.d. § 8 TMG, auch wenn sie dafür i.S.d. § 8 Abs. 2 TMG automatisch zur Übermittlung Informationen kurzzeitig zwischenspeichern.[46] Werden wie bei einem Proxy-Cache-Server auch über die Übertragung von Informationen hinaus Daten in einem Cache zeitlich begrenzt zwischengespeichert, erfüllt der Dienst die Funktion eines Cache-Providers.[47]

Anonymisierungsdienste werden aber auch von Domaininhabern und Anbietern von Webseiten genutzt. Zum Beispiel stellen CDN-Provider (content delivery network) die Webseiten ihrer Nutzer unter ihrer eigenen IP-Adresse zur Verfügung.[48] Dabei fungieren sie als Host- oder Cache-Provider, indem sie die Webseiten auf ihren eigenen Servern (zwischen-)speichern.[49]

---

[44] Vgl. hinsichtlich der E-Mails *Spindler* in: Spindler/Schmitz, § 10 TMG Rn. 84.

[45] *Spindler* in: Spindler/Schmitz, § 8 TMG Rn. 84.

[46] Vgl. *Thiesen,* MMR 2014, 803, 805.

[47] S. zur Abgrenzung zwischen § 8 Abs. 2 und § 9 TMG *Spindler* in: Spindler/Schmitz, § 9 TMG Rn. 3 ff.

[48] *Nordemann,* GRUR 2021, 18, 18. S. auch *OLG Köln*, Urt. v. 9.10.2020 – 6 U 32/20, GRUR 2021, 70, 70 ff. – Herz Kraft Werke.

[49] Zur Einordnung als Cache-Provider S. *OLG Köln*, Urt. v. 9.10.2020 – 6 U 32/20, GRUR 2021, 70 Rn. 71 ff. – Herz Kraft Werke.

Anbieter von Privacy Domains ermöglichen die anonyme Registrierung einer Domain, indem anstelle des Domaininhabers die Daten des Anbieters in die whois-Datenbank eingetragen werden.[50] Diese Dienste lassen sich nicht in eine der genannten Kategorien aus dem Telemediengesetz einordnen, da sie lediglich administrative Aufgaben übernehmen.

d) Dezentrale Netzwerke

Einen weiteren Sonderfall stellen Netzwerke dar, bei denen die Diensteanbieter stark in den Hintergrund treten und lediglich organisatorisch die Handlungen ihrer Nutzer unterstützen.[51]

Dies ist etwa der Fall bei Peer-to-Peer-Systemen (P2P). Anders als beim Client-Server-Modell sind alle Teilnehmer untereinander gleichberechtigt und können gleichermaßen als Anbieter und Empfänger von Informationen agieren. Den bekanntesten Anwendungsbereich für P2P-Systeme dürften Filesharing-Netzwerke darstellen.[52] Die meisten der heute noch nutzbaren Filesharing-Netzwerke sind inzwischen vollständig dezentral organisiert, sodass die Vernetzung und Kommunikation der Teilnehmer allein durch die entsprechende Filesharing-Software erfolgt.[53] In diesem Fall existiert überhaupt kein Diensteanbieter, der durch den Betrieb eines zentralen Servers die organisatorische Verantwortung für das Netzwerk übernimmt. Vielmehr verbleiben lediglich noch die Anbieter der Filesharing-Software.[54]

Anders verhält es sich aber bei Filesharing-Netzwerken, die einen zentralen Server einsetzen, der die Verbindung zwischen den verschiedenen Teilnehmern

---

[50] *Brunst,* Anonymität im Internet, S. 93 f.

[51] Vgl. zur Definition des Begriffs des „Netzwerks" *Golland,* Datenverarbeitung in sozialen Netzwerken, S. 10; *Schmittmann* in: Hoeren/Sieber/Holznagel, Teil 9 Rn.1.

[52] Ein anderes Beispiel für die Nutzung der Peer-to-Peer-Technik ist der VoIP-Dienst Skype.

[53] Vgl. *Brüggemann,* Drittauskunftsanspruch, S. 83. Ein Beispiel für ein Filesharing-Netzwerk mit zentraler Komponente ist die ursprüngliche Form des Dienstes Napster, S. dazu *Kreutzer,* GRUR 2001, 193, 194 f.; *Kreutzer,* GRUR 2001, 307, 307 ff.; *Schmidt/Pruß* in: Auer-Reinsdorff/Conrad, § 3 Rn. 189.

[54] *Brüggemann,* Drittauskunftsanspruch, S. 84; *Solmecke,* K&R 2007, 138, 139. Die Anbieter der Software sind keine Diensteanbieter im Sinne des TMG, S. dazu *Spindler* in: Spindler/Schmitz, § 8 TMG Rn. 42.

herstellt.[55] Dadurch besteht die Möglichkeit der Nutzer, über den zentralen Server nach konkreten Inhalten zu suchen, um anschließend gezielt den Zugang zu den angefragten Informationen vermittelt zu bekommen. Der eigentliche Datenaustausch erfolgt allerdings auch in diesen Fällen nur unter den Teilnehmern selbst. Daher lassen sich die Anbieter solcher zentraler Komponenten in der Regel als Zugangsanbieter einstufen.[56]

Eine ähnliche Organisationsstruktur wie P2P-Netzwerke weist das Usenet auf. Hier erfolgt der Informationsaustausch in Newsgroups, die ebenfalls auf einer dezentralen Verbindung von Servern basieren, die durch verschiedene Provider betrieben werden.[57] Usenet-Provider stellen die dafür erforderliche technische Infrastruktur zu Verfügung und verschaffen so ihren Nutzern Zugang zum Usenet. Dennoch lassen sie sich nicht pauschal als Zugangsanbieter einordnen, da Usenet-Provider Daten sehr häufig auch über den bloßen Übertragungsvorgang hinaus für ihre Nutzer bereithalten.[58] Dies ist unter anderem darauf zurückzuführen, dass diese ihren Nutzern ermöglichen, Inhalte des Usenets zu suchen. Dafür werden Inhalte auf ihren eigenen Servern gespeichert und Inhalte von anderen Servern zur Durchsuchung gespiegelt.[59] Für die Einordnung erscheint es sinnvoll danach zu differenzieren, ob eine Datei erstmalig auf den „Ausgangsserver" hochgeladen wird, oder ob die Datei auf einem anderen Server gespiegelt wird.[60] Der Provider des Ausgansservers speichert die Inhalte längerfristig und ermöglicht den Nutzern des Usenets den Zugang zu den Inhalten. Damit ist er

---

[55] S. etwa *Brüggemann,* Drittauskunftsanspruch, S. 83; *Spindler* in: Spindler/Schmitz, § 8 TMG Rn. 41.

[56] S. auch *Dustmann,* Die privilegierten Provider, S. 211 f. Ähnlich auch *Spindler* in: Spindler/Schuster, § 8 TMG Rn. 41, der allerdings im Hinblick auf die Suchfunktion eine Ähnlichkeit zu Suchmaschinen problematisiert.

[57] *Brüggemann,* Drittauskunftsanspruch, S. 39; *Helmschrot* in: Handbuch IT-Recht, Teil 5.3 Rn. 70; *Schmidt/Pruß* in: Auer-Reinsdorff/Conrad, § 3 Rn. 164.

[58] S. *Helmschrot* in: Handbuch IT-Recht, Teil 5.3 Rn. 71. Anders aber *OLG Hamburg*, Urt. v. 14. Januar 2009 – 5 U 113/07, ZUM-RD 2009, 246, 257 – Usenet I; *OLG Hamburg, Urt. v. 28.1.2009 - 5 U 255/07,* MMR 2009, 405, 407 f. – Alphaload; *LG Hamburg*, Urt. v. 22.6.2018 – 308 O 314/16, ZUM 2018, 814, 814; *Bosbach/Wiege,* ZUM 2012, 293, 298.

[59] *Spindler* in: Spindler/Schuster, § 9 TMG Rn. 10.

[60] So *Kitz,* CR 2007, 603, 604. Ähnlich auch *Brüggemann,* Drittauskunftsanspruch, S. 81; S. auch *Spindler* in: Spindler/Schuster, § 9 TMG Rn. 10.

als Host-Provider zu klassifizieren.[61] Durch den Anbieter des „Spiegelservers" wird dagegen nur eine vorübergehende, automatische Speicherung vorgenommen, sodass diese als Cache-Provider agieren.[62]

e) DENIC, Domain-Registrare und Admin C

Diensteanbieter, die ausschließlich administrative Aufgaben übernehmen, aber weder Zugang zu Informationen verschaffen noch eigene oder fremde Informationen vorhalten, passen nicht in die genannten Kategorien der §§ 8-10 TMG. Das betrifft sowohl die DENIC, Domain-Registrare,[63] sowie den offiziellen Ansprechpartner einer Domain (Admin C)[64] aber auch die oben aufgeführten Anbieter von Privacy Domains.
Die Registrierung einer Domain bei einem Registrar ist erforderlich, damit Inhalte unter der Domain abgerufen werden können. Hierfür übersetzt das Domain-Name-System die Domainnamen in IP-Adressen (Konnektierung).[65] Dies ist essenziell dafür, dass ein Datenaustausch auch ohne Kenntnis der Nutzer von der IP-Adresse einer aufgerufenen Website möglich wird.[66] Eine Second-Level-Domain kann unter einer länderspezifischen Top-Level-Domain nur einmalig vergeben werden. Es gilt das Prioritätsprinzip („first come, first served").[67] Das heißt, dass die Registrierung einer Domain nur möglich ist, wenn nicht bereits eine identische Domain existiert.[68]

---

[61] *Kitz,* CR 2007, 603, 604. S. auch *OLG Hamburg*, Urt. v. 14. Januar 2009 – 5 U 113/07, ZUM-RD 2009, 246, 265 – Usenet I.

[62] *Kitz,* CR 2007, 603, 604.

[63] *Hofmann,* NJW 2021, 274, 274 ff.; *Nordemann,* GRUR 2021, 18, 18 ff.; jeweils m. Anm. zu *BGH,* Urt. v. 15.10.2020 – I ZR 13/19, NJW 2021, 63 – Störerhaftung des Domain-Registrars.

[64] *BGH,* Urt. v. 9. 11. 2011 - I ZR 150/09, GRUR 2012, 304 Rn. 54 – Basler Haarkosmetik; *Martini* in: BeckOK Informations- und Medienrecht, § 2 TMG Rn. 8.

[65] Ausführlich zur Funktionsweise des Domain Name Systems S. *Bertermann*, MMR 2015, 524, 525; *Welp,* Auskunftspflicht von Access-Providern, S. 14

[66] *Bettinger/Freytag*, CR 1999, 28, 29.

[67] *OLG Frankfurt a. M.,* Urt. v. 26.10.2010 - 11 U 29/10, BeckRS 2011, 01267, 01268; *Habermann,* Zivilrechtliche Störerhaftung, S. 22. S. auch Ziffer III Abs. 1 der DENIC-Domainrichtlinie abrufbar unter https://www.denic.de/domains/de-domains/domainrichtlinien/ (Stand: 24.05.2022).

[68] *Habermann,* Zivilrechtliche Störerhaftung, S. 22.

Die weltweite Koordinierung und technische Organisation des Domain Name System übernimmt die Internet Corporation for Assigned Names and Numbers (ICANN).[69] Das Deutsche Network Information Center (DENIC) ist die zentrale Vergabestelle (Domain Registry) für die Top-Level-Domain .de.[70]

Domain Registrys führen außerdem sogenannte Whois-Datenbanken, in denen Informationen über die Inhaber einer Domain, aber auch der Admin C verzeichnet sind.[71] Domain Registrare sind dabei die Vermittler zwischen den zukünftigen Domaininhabern und den Registries, indem sie als Dienstleistung nach verfügbaren Domainnamen suchen und die Registrierung der Domain vornehmen. Der Admin C ist der administrative Ansprechpartner einer Domain, der bei der Registrierung angegeben wird. Er ist als Bevollmächtigter entscheidungsbefugt und gegenüber den Domain-Registries verpflichtet.[72]

III. Nutzer

Der Begriff des Nutzers korreliert mit dem des Diensteanbieters. Nutzer ist jede Person, die die oben genannten Internetdienste nutzt. Die Nutzung besteht häufig darin, Informationen zu erlangen oder eigene Inhalte zugänglich zu machen.[73] Dabei ist es unerheblich, ob es sich um eine gewerbliche oder private und ob es sich um eine „aktive" oder „passive" Nutzung handelt.[74]

Die Einordnung einer Person als Nutzer hängt somit unmittelbar mit der des Diensteanbieters zusammen und ist anhand der im konkreten Einzelfall maßgeblichen Funktion zu bestimmen. Ein Nutzer kann nämlich selbst gleichzeitig auch als Diensteanbieter auftreten. Dies ist zum Beispiel der Fall, wenn er einen Inhalt auf einem fremden Server - zum Beispiel eines Online-Marktplatzes - für Dritte anbietet. In diesem Fall nutzt er die Dienste der Online-Plattform, tritt

---

[69] *Härting*, Internetrecht, Rn. 2214; *Hoeren,* Internetrecht, Rn. 30; *Holznagel,* MMR 2003, 219.

[70] *Habermann,* Zivilrechtliche Störerhaftung, S. 20; *Härting,* Internetrecht, Rn. 2216; *Hoeren,* Internetrecht, Rn. 40.

[71] S. auch Ziffer VII Abs. 2 der DENIC-Domainrichtlinie abrufbar unter https://www.denic.de/domains/de-domains/domainrichtlinien/ (Stand: 24.05.2022).

[72] *Habermann,* Zivilrechtliche Störerhaftung, S. 24 f.

[73] Vgl. die Definition in Art. 2 lit. d) ECRL und § 2 Nr. 3 TMG.

[74] Ausführlicher dazu S. *Ricke* in: Spindler/Schuster, § 2 TMG Rn. 11.

aber gleichzeitig den Dritten gegenüber auch als Diensteanbieter (Content-Provider) auf. Aus der Perspektive eines Rechteinhabers, der sich durch die Auskunft des Plattform-Betreibers Erkenntnisse über die Identität des Anbieters eines rechtsverletzenden Inhalts erhofft, ist der Inhalteanbieter aber Nutzer der Plattform. Auch für den Betreiber handelt es sich bei dem Inhalteanbieter um einen Nutzer des angebotenen Dienstes und im Falle einer Auskunftserteilung um die Weitergabe von Nutzerdaten.

C. Verletzung absoluter Rechte im Internet

Rechtsverletzungen im Internet sind sehr vielfältig. Dies ergibt sich aus der Vielfalt der Internetdienste, durch die Diensteanbieter ihren Nutzern auch eine Vielzahl unterschiedlicher Einwirkungsmöglichkeiten auf fremde Rechtsgüter schaffen. Die nachfolgenden Ausführungen geben einen Überblick über Rechtsverletzungen, die in der Praxis häufig vorkommen.

I. Fallkonstellationen

Rechtsverletzungen durch Nutzer von Internetdiensten lassen sich überwiegend in drei verschiedene Fallkonstellationen einsortieren: Eine der häufigsten Fallgruppen betrifft eigene rechtsverletzende Inhalte der Nutzer. Diese werden häufig durch die Diensteanbieter gespeichert oder zwischengespeichert und Dritten zugänglich gemacht. Darunter fallen vor allem nutzergenerierte Inhalte wie Äußerungen, Links, Texte, Bilder und Videos, durch die Rechteinhaber in ihren Rechten verletzt werden. Solche Inhalte werden oft zum Beispiel über Plattformen verbreitet. Ermöglicht wird dies meist durch Host-Provider wie die Betreiber einer Webseite, eines Blogs, sozialer Netzwerke, von Sharehoster-Diensten, Foren und Kommentarspalten, sowie von Online-Marktplätzen. Diese stellen die entsprechenden Dienste zur Verfügung und speichern die Inhalte ihrer Nutzer. Auch Webhosting-Anbieter tragen zur Verbreitung rechtswidriger Inhalte ihrer Nutzer bei, wenn sich solche auf den Webseiten ihrer Nutzer befinden. Einen Unterfall stellt die Verbreitung rechtswidriger Inhalte per Mail oder über Messenger-Dienste dar. Auch die Mailanbieter und die Anbieter von Messenger-Diensten, ermöglichen die Weitergabe rechtswidriger Inhalte und speichern diese teilweise auch auf ihren Servern.

Internetnutzer können die Rechte anderer aber nicht nur durch eigene Inhalte, sondern auch durch die Verwendung von fremden Inhalten verletzen. Zum Beispiel kann auch das Streaming urheberrechtlich geschützten Materials oder der Download eines Werks beim Filesharing eine Rechtsverletzung darstellen.

Eine weitere Fallgruppe stellen Rechtsverletzungen durch Domaininhaber dar. Durch die Registrierung und Verwendung einer Domain kann es insbesondere zu namens- oder markenrechtlichen Verstößen kommen. Daneben können unter einer Domain rechtswidrige Handlungen ermöglicht werden oder der Domaininhaber rechtswidrige Inhalte bereitstellen. Dabei stehen vor allem strukturell rechtsverletzende Webseiten im Vordergrund. Als rechtsverletzender Nutzer ist in diesem Fall der Domaininhaber zu verstehen, der die Domain angemeldet hat. In der Funktion des Diensteanbieters treten in dieser Fallgruppe vor allem die DENIC, Domain-Registrare, der Admin C, aber gegebenenfalls auch die Anbieter einer Privacy Domain auf.

II. Häufige Rechtsverletzungen im Internet

Rechtsverletzendes Nutzerverhalten in den drei genannten Fallgruppen kann verschiedene Rechtsgüter der Rechteinhaber betreffen. Diese Arbeit beschränkt sich auf absolute Rechte wie IP-Rechte, Persönlichkeitsrechte, das Recht am eingerichteten und ausgeübten Gewerbebetrieb, aber auch das Recht auf Eigentum, Leben, Gesundheit und körperliche Unversehrtheit. Die nachfolgenden Ausführungen behandeln exemplarisch die typischen Beeinträchtigungen solcher Rechtsgüter durch Nutzer im Internet.

1. Verletzungen des Urheberrechts und verwandter Schutzrechte

Besondere Aufmerksamkeit im Zusammenhang mit Rechtsverletzungen im Internet erzielten die Beeinträchtigungen von Urheberrechten und verwandten Schutzrechten. Die Klagen gegen die massenweise – überwiegend durch spezialisierte Anwaltskanzleien – verschickten Filesharing-Abmahnungen führten zu zahlreichen Gerichtsverfahren in diesem Bereich. Die möglichen Verletzungen des Urheberrechts und der verwandten Schutzrechte im Internet sind aber natürlich deutlich vielgestaltiger und nicht auf Filesharing-Netzwerke beschränkt.

a) Urheberrechtsverletzungen

Viele verschiedene Handlungsweisen im Online-Bereich können urheberrechtlich relevant sein.[75] Von besonderer Bedeutung sind dabei die Verwertungsrechte des Urhebers aus den §§ 16, 19a und 23 UrhG.

aa) Öffentliche Zugänglichmachung

Besonders relevant im Online-Bereich ist das Recht des Urhebers auf öffentliche Zugänglichmachung aus § 19a UrhG. Ein Eingriff in das Verwertungsrecht kann jedenfalls durch Einstellen eines urheberrechtlich geschützten Werkes ins Internet begründet werden. Dazu zählen beispielsweise: Der Upload eines Werks in Tauschbörsen oder Filesharing-Netzwerken,[76] das Anbieten eines On-Demand-Streams[77] sowie der Upload von Inhalten auf Plattformen und in sozialen Netzwerken.

Wird das Werk dabei – anders als bei einer für jedermann zugänglichen Website – nur einem begrenzten Personenkreis zugänglich gemacht, kann es an dem Merkmal der Öffentlichkeit fehlen. Dabei ist die Anzahl der Nutzer, die Zugriff auf ein Werk erhalten, und die Art der persönlichen Beziehungen zwischen den Nutzern entscheidungsrelevant.[78]

Das Setzen eines Links auf einen fremden urheberrechtlich geschützten Inhalt verletzt dagegen in der Regel das Recht des Urhebers auf öffentliche

---

[75] *Fischer,* Einbindung von Providern, S. 22.

[76] S. etwa *EuGH,* Urt. v. 17.6.2021 – C-597/19, MMR 2022, 30, 30 – Mircom.

[77] Live-Streams werden dagegen von § 20 UrhG erfasst, S. etwa *Ernst* in: Hoeren/Sieber/Holznagel, Teil 7.1 Rn. 70 m.w.N. S. zum On-Demand-Streaming *OLG Stuttgart*, Beschl. v. 21.01.2008, CR 2008, 319; *OLG Hamburg,* 7.7.2005 - 5 U 176/04, MMR 2006, 173 – staytuned.de; *Werner* in: Ensthaler/Weidert, Kap. 3 Rn. 47 f.

[78] S. allgemein *Wiebe* in Spindler/Schuster, § 15 UrhG Rn. 9 ff. m.w.N. S. im Besonderen zur öffentlichen Zugänglichmachung bei Facebook-Freunden *Ziegler*, Urheberrechtsverletzungen durch Social Sharing, S. 86 ff. S. zum Filesharing *Brüggemann,* Drittauskunftsanspruch, S. 57 ff.

Zugänglichmachung nicht.[79] Der Urheber hat in diesem Fall nämlich durch Löschen oder Verändern des Ziels des Links grundsätzlich weiterhin die Kontrolle über den Inhalt. Eine Ausnahme gilt, wenn der Inhalt durch die Verlinkung einem neuen Publikum zugänglich gemacht wird und der Linksetzer mit Gewinnerzielungsabsicht handelte oder die Rechtswidrigkeit des verlinkten Inhalts kannte oder kennen musste.[80] Gleiches gilt im Wesentlichen auch für das Einbinden eines fremden Inhalts mittels Framing-Technik in die eigene Website oder in Beiträge in sozialen Netzwerken.[81] Ähnlich verhält es sich auch beim Teilen von Links durch Nutzer sozialer Netzwerke, wenn dabei – wie beispielsweise auf Facebook- automatisch sogenannte Thumbnails oder Snippets (Vorschaubilder und -texte) erstellt werden.[82]

Anders sind – zumindest nach der jüngeren Rechtsprechung des *EuGH* – Fälle zu beurteilen, bei denen ein im Internet bereits veröffentlichtes Werk in kopierter Form auf der eigenen Website hochgeladen wird.[83] Hier wird regelmäßig eine Verletzung des Rechts auf öffentliche Zugänglichmachung anzunehmen sein. Anders als bei der Verlinkung würde der Urheber andernfalls die Kontrolle darüber verlieren, ob sein Werk online verfügbar bleibt.[84]

bb) Vervielfältigung

Häufig verstoßen notwendige Handlungen im Vorfeld der öffentlichen Zugänglichmachung gegen das Vervielfältigungsrecht des Urhebers aus § 16 UrhG.

---

[79] *EuGH*, Urt. v. 13.2.2014 – C-466/12, NJW 2014, 759, 360 – Svensson; *BGH*, Urt. v. 17. 7. 2003 - I ZR 259/00, GRUR 2003, 958 – Paperboy. Ausführlicher zu den technischen Aspekten von Verlinkung, Thumbnails und Snippets *Askani,* Private Rechtsdurchsetzung, S. 64 ff.

[80] *EuGH,* Urt. v. 8.9.2016 – C-160/15, GS– GS Media/Sanoma ua.

[81] Das Einbinden eines Inhalts in eine Internetseite verletzt nur dann das Recht auf öffentliche Zugänglichmachung, wenn ein anderes Publikum erreicht wird oder eine neue Technik eingesetzt wird, S. dazu *EuGH,* Urt. v. 8.9.2016 – C-160/15, MMR 2017, 95 – GS Media; *EuGH,* Beschl. v. 21.10.2014 - C-348/13, MMR 2015, 46 – Bestwater International; *EuGH*, Urt. v. 13.2.2014 – C-466/12, NJW 2014, 759, 360 – Svensson. S. auch zur Umgehung technischer Schutzmaßnahmen gegen Framing *BGH,* Urt. v. 9.9.2021 – I ZR 113/18, MMR 2021, 965 – Deutsche digitale Bibliothek II.

[82] S. dazu *Ziegler*, Urheberrechtsverletzungen durch Social Sharing, S. 124 ff.

[83] *EuGH*, Urt. v. 7.8.2018 – C-161/17, GRUR 2018, 911 - Cordoba.

[84] S. auch *Pfeifer*, NJW 2018, 3490, 3490 f.

Beispielsweise stellt die Digitalisierung[85] und das Überspielen der Daten eines Werks auf einen Server[86] im Vorfeld eines Uploads selbst eine Vervielfältigung dar. Dies ist auf den weiten Begriff der Vervielfältigung des § 16 UrhG zurückzuführen, nach dem auch kurzfristige oder vorübergehende Speicherungen auf einem Arbeitsspeicher, auf einer Festplatte oder auf einem Datenträger erfasst werden.[87] Auch das Browsing[88] und der Download, bei dem digitale Kopien eines Werks entstehen, können dementsprechend unter den Begriff subsumiert werden.[89] Auch beim Upload selbst handelt es sich um eine Vervielfältigung durch die entstehenden digitalen Kopien.[90]

Eine sehr kurzfristige Speicherung kann aber nach § 44a UrhG zulässig sein.[91] Dasselbe gilt unter den entsprechenden Umständen für eine Vervielfältigung zum rein privaten Gebrauch nach § 53 UrhG. Besteht von vornherein die

---

[85] *Askani,* Private Rechtsdurchsetzung, S. 63; *Ernst* in: Hoeren/Sieber/Holznagel, Teil 7.1 Rn. 50; *Fischer,* Einbindung von Providern, S. 22 f.; *Loewenheim* in: Schricker/Loewenheim, § 16 UrhG Rn. 20; *Nordemann* in: Fromm/Nordemann, § 16 UrhG R. 2; *Werner* in: Ensthaler/Weidert, Kap. 3 Rn. 30.

[86] *Ernst* in: Hoeren/Sieber/Holznagel, Teil 7.1 Rn. 55; *Fischer,* Einbindung von Providern, S. 24 ff.

[87] *BGH*, Beschl. v. 3. 2. 2011 - I ZR 129/08, GRUR 2011, 418, 419 – Used Soft; *OLG Hamburg*, Urt. v. 22. 2. 2001 - 3 U 247/00, GRUR 2001, 831 – Roche Lexikon Medizin; *Schulze* in: Dreier/Schulze, § 16 UrhG Rn. 7; *Werner* in: Ensthaler/Weidert, Kap. 3 Rn. 31.

[88] *OLG Hamburg*, Urt. v. 22. 2. 2001 - 3 U 247/00, GRUR 2001, 831 – Roche Lexikon Medizin; *Askani*, Private Rechtsdurchsetzung, S. 61; *Dustmann* in: Fromm/Nordemann, § 16 Rn. 13, 25; *Heerma* in: Wandtke/Bullinger, § 16 UrhG Rn. 13; *Fischer,* Einbindung von Providern, S. 34 f.; *Loewenheim* in: Schricker/Loewenheim, § 16 UrhG Rn. 22; a.A. *Galetzka/Stamer*, MMR 2014, 292, 294 f.

[89] *BGH,* Urt. v. 6.10.2016 – I ZR 25/15, MMR 2017, 171 m. Anm. *Biehler* – World of Warcraft; *KG*, Urt. v. 24. Juli 2001 – 5 U 9427/99, ZUM-RD 2001, 485, 488; *Askani*, Private Rechtsdurchsetzung, S. 62; *Brüggemann*, Drittauskunftsanspruch, S. 60 ff.; *Ernst* in: Hoeren/Sieber/Holznagel, Teil 7.1 Rn. 56; *Werner* in: Ensthaler/Weidert, Kap. 3 Rn. 82.

[90] *OLG München*, Urt. v. 8. 3. 2000 - 29 U 3282/00, GRUR 2001, 499, 503; *Werner* in: Ensthaler/Weidert, Kap. 3 Rn. 37; S. auch *EuGH*, Urt. v. 16. 7. 2009 - C-5/08, GRUR 2009, 1041 - Infopaq/DDF.

[91] S. dazu Erwägungsgrund 30, 33 der InfoSoc-Richtlinie. S auch *EuGH*, Urt. v. 5.6.2014 – C-360/13, EuZW 2014, 637 – Public Relations Consultants Association; *Solmecke/Dam*, MMR 2014, 544, 545; *Werner* in: Ensthaler/Weidert, Kap. 3 Rn. 78; *Wiebe* in: Spindler/Schuster, § 44 a Rn. 1 ff.

Absicht, die digitalisierten Dateien zu veröffentlichen, erfüllt deren Digitalisierung aber keinen rein privaten Zweck.[92]

Vor dem Hintergrund des Vervielfältigungsrechts ist besonders das Streaming problematisch. Beim Anschauen eines Videos im Internet beispielsweise werden codierte Datenpakete an den Rechner übertragen, die eine Vervielfältigung des Werks darstellen können.[93] Unabhängig von der Frage ob beim Streaming die Voraussetzungen des § 44a UrhG vorliegen,[94] wird eine rechtmäßige Nutzung – beispielsweise eine Gestattung des Betrachtens nach § 53 UrhG - vorausgesetzt.[95] Der *EuGH* hat dazu entschieden, dass das Anschauen eines illegalen Streams keine rechtmäßige Nutzung darstellt, wenn der Nutzer Kenntnis von der Rechtswidrigkeit des illegalen Streams hat.[96] Dies kann beispielsweise der Fall bei eindeutig illegalen Angeboten (z.B. kinox.to) oder bei Streams von ganz aktuellen Kinofilmen der Fall sein.[97]

cc) Bearbeitung und Umgestaltung

Bearbeitungen und Umgestaltungen eines Werks spielen vor allem im Zusammenhang mit nutzergenerierten Inhalten eine Rolle. Dadurch kann das Recht auf öffentliche Zugänglichmachung, das Vervielfältigungsrecht, beziehungsweise das Recht des Urhebers aus § 23 UrhG betroffen sein. Häufig werden fremde Werke von Nutzern für das Erstellen und Teilen von Inhalten – beispielsweise Memes, Remixe, Fan Fiction, Mashups und GIFs – verwendet. Die urheberrechtliche Zulässigkeit solcher modernen Ausdrucks- und Kommunikationsformen lässt sich nicht allgemeingültig beurteilen. Relevant ist dabei insbesondere das Verhältnis zu § 51a UrhG. Die am 07.06.2021 in Kraft getretene Schrankenregelung dient der Umsetzung von Art. 17 Abs. 7 lit. b) DSM-RL.[98] Entsprechend gestattet § 51a die Nutzung urheberrechtlich geschützter Werke

---

[92] *Freiwald*, Private Vervielfältigung, S. 141; *Hoeren* in: Hoeren/Sieber/Holznagel, Teil 18.2 Rn. 61.

[93] *Askani,* Private Rechtsdurchsetzung, S. 62; *Wiebe* in: Spindler/Schuster, § 44 a Rn. 8.

[94] Ausführlicher dazu etwa *Wiebe* in: Spindler/Schuster, § 44 a Rn. 7 ff. m.w.N.

[95] *Fischer,* Einbindung von Providern, S. 36; *Werner* in: Ensthaler/Weidert, Kap. 3 Rn. 88 ff.

[96] *EuGH,* Urt. v. 26.4.2017 – C-527/15, ZUM 2017, 587 – Stichting Brein/Wullems.

[97] *Ernst* in: Hoeren/Sieber/Holznagel, Teil 7.1 Rn. 52.

[98] Vorher war die Umsetzung aus Art. 5 Abs. 3 lit. k) der InfoSoc-Richtlinie noch optional; S. etwa *Lauber-Rönsberg* in: BeckOK Urheberrecht, § 51 a Rn. 7.

zum Zwecke der Karikatur, Pastiches oder Parodie.[99] Dennoch lässt sich die Rechtmäßigkeit nutzergenerierter Inhalte nur anhand des konkreten Einzelfalls und unter Berücksichtigung der wechselseitigen Interessen beurteilen.[100] Die Interessensabwägung stellt insofern ein ungeschriebenes Tatbestandsmerkmal des § 51 a UrhG dar.[101]

b) Urheberpersönlichkeitsrecht

Das Urheberrecht schützt sowohl materielle Interessen als auch Interessen, die ihren Ursprung in der Persönlichkeit des Urhebers haben.[102] Neben den genannten Beeinträchtigungen der Verwertungsrechte des Urhebers, können auch Urheberpersönlichkeitsrechte verletzt sein.[103] Häufig kommt es dabei auch zu Überschneidungen. Die öffentliche Zugänglichmachung eines Werks im Internet ohne Bezeichnung des Urhebers beispielsweise greift auch in das Recht des Urhebers auf Anerkennung seiner Urheberschaft nach § 13 UrhG ein. Dasselbe kann auch für das unerlaubte Vervielfältigen eines Werkes gelten.[104] Die erstmalige Veröffentlichung eines Werks ohne die Zustimmung des Urhebers verbietet § 12 UrhG. Aus dem unbefugten Gebrauch eines Werks im Internet kann sich zudem eine Entstellung, Beeinträchtigung oder Verfremdung i.S.v. § 14 UrhG ergeben.[105]

c) Verwandte Schutzrechte

Ein mit den Urheberrechtsverletzungen vergleichbarer Anwendungsbereich ergibt sich auch bei den verwandten Schutzrechten, sodass es zu Überschneidungen kommen kann. Die Rechte des Lichtbildners (§ 72 UrhG), Tonträgerherstellers (§ 85 UrhG) und Film- oder Laufbildherstellers (§§ 94, 95 UrhG)

---

[99] S. zu den Begriffen etwa *Lauber-Rönsberg* in: BeckOK Urheberrecht, § 51 a Rn. 11 ff. m.w.N.

[100] S. dazu *Regierungsentwurf,* BT-Drs. 19/27426, 90; *Stieper*, GRUR 2020, 792, 797. S. auch *EuGH, Urt. v. 3.9.2014 – C-201/13,* ZUM-RD 2014, 613 Rn. 34 – Deckmyn.

[101] *Lauber-Rönsberg* in: BeckOK Urheberrecht, § 51 a Rn. 11.

[102] *Fischer,* Einbindung von Providern, S. 22.

[103] S. dazu auch *Werner* in: Ensthaler/Weidert, Kap. 3 En. 111 ff.; *Ziegler*, Urheberrechtsverletzungen durch Social Sharing, S. 134 ff.

[104] *Fischer*, Einbindung von Providern, S. 23.

[105] S. dazu etwa *Bullinger* in: Wandtke/Bullinger, § 14 UrhG En. 62 ff.; *Werner* in: Ensthaler/Weidert, Kap. 3 Rn. 122 ff.

können beispielsweise durch Zugänglichmachung oder Vervielfältigung im Internet ebenfalls beeinträchtigt sein. Als relevant kann sich auch der Schutz des Sendeunternehmens vor Weitersendung und öffentlicher Zugänglichmachung – zum Beispiel mittels eines Streams – und Aufnahme der Sendung erweisen.

2. Verletzung gewerblicher Schutzrechte

Die gewerblichen Schutzrechte umfassen das Patent-, Gebrauchsmuster-, Geschmacksmuster- und Markenrecht sowie den Halbleiter- und Sortenschutz. Im Kontext anonymer Rechtsverletzungen im Internet ist vor allem das Markenrecht relevant. Andere gewerbliche Schutzrechte spielen dagegen – wenn überhaupt - eine eher untergeordnete Rolle.

Die Verletzung gewerblicher Schutzrechte im Internet wird vor allem bei der Veräußerung schutzrechtsverletzender Ware über Verkaufsplattformen und Internet-Marktplätze relevant.[106] Voraussetzung für eine Markenrechtsverletzung nach §§ 14, 15 MarkenG ist ein Handeln im geschäftlichen Verkehr.[107] Das verbreitetste Phänomen dürfte der Handel mit gefälschter Markenware sein. Ein Markenrechtsverstoß ergibt sich nach § 14 Abs. 2 Nr. 1 MarkenG etwa aus der Verwendung eines geschützten Zeichens für Waren oder Dienstleistungen, das mit demjenigen identisch ist, für das die Marke Schutz genießt. Es existieren zahlreiche Plattformen wie ebay, aliexpress, rakuten, etc., bei denen das Kaufen und Verkaufen für die Nutzer meist sehr schnell und einfach ausgestaltet ist. Verwendet der Anbieter solcher Plagiate dabei nicht seinen echten Namen, kann dem Rechteinhaber nicht nur die Rechtsdurchsetzung gegen diesen als Rechtsverletzer erschwert werden, sondern auch die Kenntniserlangung über Herkunft und Vertriebswege der Markenfälschungen.

Verstöße gegen das Markengesetz ergeben sich häufig im Zusammenhang mit Domains. Das Registrieren und Verwenden einer Domain, die ein geschütztes Kennzeichen beinhaltet, kann Vorschriften des MarkenG verletzen. Voraussetzung hierfür ist jedenfalls, dass die Verwendung im geschäftlichen Verkehr und

---

[106] S. dazu auch *Welp*, Auskunftspflicht von Access-Providern, S. 23 f; S. auch *BGH*, Urt. v. 30. 4. 2008 - I ZR 73/05, GRUR 2008, 702 ff. – Internet-Versteigerung III.

[107] Zur Problematik bei privaten Verkäufen über das Internet S. *Mielke* in: BeckOK Markenrecht, § 14 MarkenG Rn. 66 ff.

kennzeichenmäßig erfolgt und Zeichenidentität oder Verwechslungsgefahr besteht.[108] Eine markenmäßige Verwendung liegt zum Beispiel beim Domain-Parking vor, wenn unter der Domain abrufbaren Website Produktangebote verlinkt sind („sponsored links").[109]

Eine Rechtsverletzung kann es auch darstellen, wenn bekannte Marken als Domainnamen verwendet werden und dabei der Bekanntheitsgrad des Kennzeichens zur Erhöhung der Aufmerksamkeit für die eigene Website genutzt werden.[110] Häufig werden zu diesem Zweck auch Tippfehler-Domains – beispielsweise „kwwick" statt „kwick"[111] - eingesetzt, um versehentlich falsche Eingaben von Nutzern auszunutzen, um die Besucherzahlen der eigenen Seite anzuheben. In einem ähnlichen Zusammenhang kann zudem der Einsatz der Domain de.de in Verknüpfung mit der Erstellung einer sog. Catch-All-Funktion je nach der vom Nutzer eingegebenen Third-Level-Domain und der sonstigen Umstände des Einzelfalls eine Markenrechtsverletzung bewirken.[112]

Auch das sogenannte Domainname-Grabbing kann je nach Einzelfall einen Verstoß gegen das MarkenG begründen.[113] Darunter wird die Registrierung oder Reservierung eines bekannten Kennzeichens als Domainnamen verstanden mit dem Zweck, dem Inhaber dieses Kennzeichens die Freigabe der Domain gegen eine Bezahlung anzubieten.[114] Die Möglichkeit hierzu entsteht durch das bei der Domainvergabe vorherrschende Prioritätsprinzip.[115] Neben Vorschriften der §§

---

[108] S. etwa *Härting*, Internetrecht, Rn. 2269.

[109] *BGH*, Urt. v. 18.11.2010 - I ZR 155/09, MMR 2011, 459 – Sedo; *Hoeren* in: Hoeren/Sieber/Holznagel, Teil 18.2 Rn. 87.

[110] Ausführlicher *Müller* in: Spindler/Schuster, § 14 MarkenG Rn. 110 ff.

[111] *LG Stuttgart*, Urt. v. 28.7.2011 - 17 O 73/11, MMR 2012, 43 – Kwick/Kwwick.

[112] *KG*, Urt. v. 23.5.2012 - 5 U 119/11, MMR 2012, 757.

[113] Das bloße Registrieren einer Domain ohne Bezug zu einem Produkt oder Gewerbe stellt noch keine Markenrechtsverletzung dar, s. etwa *OLG Karlsruhe*, Urt. v. 12.9.2001 - 6 U 13/01, MMR 2002, 118 – dino.de. Bei bekannten Marken kann es zu einem Verstoß gegen § 14 Abs. 2 Nr. 3 MarkenG kommen, S. etwa *OLG Karlsruhe*, Urt. v. 24.6.1998 - 6 U 247/97, MMR 1999, 171 – zwilling.de. Im Übrigen bedarf es wohl eines konkreten Angebots der streitgegenständlichen Domain, S. etwa *LG Berlin*, Urt. v. 21.2.2008 - 52 O 111/07, MMR 2008, 484, 485 – naeher.de*; Viefhues* in: Hoeren/Sieber/Holznagel, Teil 6 Rn. 180.

[114] *Müller* in: Spindler/Schuster, § 14 MarkenG Rn. 131 f.

[115] S. dazu oben unter Kap. 2 § 2 B. IV. 5.

14, 15 MarkenG werden im Zusammenhang mit Kennzeichenbeeinträchtigungen im Domain-Bereich häufig auch lauterkeitsrechtliche Vorschriften des UWG oder das Namensrecht aus § 12 BGB relevant.

Vor dem Inkrafttreten der DS-GVO spielte ein anonymes Auftreten der Domaininhaber und möglichen Rechtsverletzer keine besondere Rolle, da diese registriert sind und sich über eine Whois-Abfrage im Internet meistens leicht selbstständig ermitteln ließen. Mittlerweile werden diese Daten von den Registrierungsstellen allerdings nicht mehr öffentlich einsehbar zur Verfügung gestellt. Die DENIC als zentrale Vergabestelle für die Top-Level-Domain .de beispielsweise erteilt nach eigenen Angaben zwar bei namensrechtlichen- und markenrechtlichen Verletzungen entsprechend Auskunft. Welche genauen Voraussetzungen dafür erfüllt sein müssen, ist jedoch für Rechteinhaber nicht auf den ersten Blick ersichtlich.[116]

Eine Kennzeichenrechtsverletzung kann sich auch aus der unbefugten Verwendung fremder Kennzeichen innerhalb einer Webseite ergeben: Metadaten von Websites werden teilweise mit irreführenden Schlagwörtern notiert, um – beispielsweise durch Verwenden eines geschützten Kennzeichens – die Trefferliste einer Suchmaschine zu beeinflussen.[117] Da viele Suchmaschinen inzwischen allerdings verstärkt auf den eigentlichen Inhalt der Seite reagieren, dürfte mittlerweile das sogenannte Keyword-Advertising im Vordergrund stehen. Problematisch ist in diesem Zusammenhang, ob das Verwenden eines fremden geschützten Kennzeichens als Schlüsselwort, durch das bei Eingabe des Suchbegriffs in einer Suchmaschine der bezahlte Treffer gesondert als Anzeige erscheint, eine Kennzeichenrechtsverletzung darstellt.[118] Unabhängig von der Frage nach einem Verstoß gegen das MarkenG, dürfte die Anonymität bei den möglichen Rechtsverletzungen durch Metadaten und Keyword-Advertising auf Grund der Impressumspflicht im Rahmen des Anwendungsbereich des § 5 TMG keine

---

[116] Ziffer VII Abs. 3 der DENIC-Domainrichtlinien abrufbar unter https://www.denic.de/domains/de-domains/domainrichtlinien/ (Stand: 24.05.2022); https://www.denic.de/service/whois-service/anfragen-dritter-zu-inhaberdaten (Stand: 24.05.2022).

[117] *Kaufmann*, MMR 2005, 348; s. auch *BGH*, Urt. v. 8.2.2007 - I ZR 77/04, GRUR 2007, 784 – AIDOL; *BGH*, Urt. v. 30.7.2015 – I ZR 104/14, NJW-RR 2016, 673 - Posterlounge.

[118] Ausführlicher dazu *Müller* in: Spindler/Schuster, § 14 MarkenG Rn. 147 ff. m.w.N.

größere Rolle spielen, da sich zumindest die geschäftsmäßigen Betreiber einer Internetseite leicht selbstständig ermitteln lassen.

3. Recht am eingerichteten und ausgeübten Gewerbebetrieb

Rechtsverletzungen im Internet können auch das Recht am eingerichteten und ausgeübten Gewerbebetrieb beziehungsweise das Unternehmenspersönlichkeitsrecht beeinträchtigen. Hiervon können auch juristische Personen betroffen sein. Das Recht am eingerichteten und ausgeübten Gewerbebetrieb können auch Angehörige freier Berufe für sich anführen.[119]

Das Unternehmenspersönlichkeitsrecht schützt den „sozialen Geltungsanspruch von Kapitalgesellschaften als Wirtschaftsunternehmen", und damit insbesondere die Reputation des Unternehmens, vor negativen Außendarstellungen.[120] Insofern ergeben sich Überschneidungen mit dem Schutzbereich des Rechts am eingerichteten und ausgeübten Gewerbebetrieb. Dieses wird vom BGH als sonstiges Recht im Sinne von § 823 Abs. 1 BGB angesehen und soll den Gewerbebetrieb in seiner wirtschaftlichen Tätigkeit und Funktionsfähigkeit vor widerrechtlichen Eingriffen bewahren.[121] Auch der Ruf des Unternehmens soll von dessen Schutzbereich erfasst werden.[122] Teilweise wird das Unternehmenspersönlichkeitsrecht daher auch als Teil des Rechts am eingerichteten und ausgeübten Gewerbebetrieb und nicht als selbstständig geschütztes Rechtsgut verstanden.[123]

Im Hinblick auf die Anonymität der Internetnutzer wird das Recht am eingerichteten und ausgeübten Gewerbebetrieb bzw. das Unternehmenspersönlichkeitsrecht vor allem bei negativen Bewertungen von Unternehmen relevant.

---

[119] *OLG Hamburg*, Urt. v. 4. 6. 1998 - 3 U 246–97, NJW-RR 1999, 1060, 1060 ff..

[120] *BGH*, Urt. v. 14.1.2020 – VI ZR 496/18, ZUM-RD 2020, 181, 181 ff.; *BGH*, Urt. v. 8.7.1980 - VI ZR 177/78, NJW 1980, 2807, 2807 ff.; *BGH, Urt. v. 8.2.1994 - VI ZR 286/93*NJW 1994, 1281, 1282.

[121] S. etwa *BGH*, Urt. v. 15.1.2019 – VI ZR 506/17, ZUM 2019, 435, 435 ff.; *BGH*, Urt. v. 6.2.2014 – I ZR 75/13, GRUR 2014, 904, 904 ff.

[122] *BGH*, Urt. v. 24.1.2006 - XI ZR 384/03, NJW 2006, 830, 839.

[123] So wohl *BGH*, Urt. v. 14.1.2020 – VI ZR 495/18, ZUM 2020, 331 Rn. 35 – yelp.de; *Koreng*, GRUR 2010, 1065, 1069 f.

Solche finden sich zum Beispiel auf Produkt- und Dienstleistungsbewertungsportalen wie beispielsweise Jameda, golocal, TripAdvisor und Yelp.

Neben den klassischen Bewertungsportalen besteht sehr häufig auch die Möglichkeit, eine Kundenrezension in Kommentarspalten und auf Verkaufs- und Auktionsplattformen zu hinterlassen. Zudem hält beispielsweise Google-Maps eine Bewertungs- und Kommentarfunktion bereit, wodurch den Nutzern die Bewertung von Unternehmen und Dienstleistungen in Bezug auf deren Standort angezeigt wird. Teilweise werden auch soziale Netzwerke genutzt, um Produkte und Dienstleistungen zu bewerten. In allen genannten Fällen erfolgt die Bewertung durch die Nutzer sehr häufig anonym.

Die Konsequenzen negativer Kundenrezensionen können im Einzelfall gravierend sein. Die Reputation eines Unternehmens oder Dienstleisters wirkt sich auf das Verhalten von Kunden, Geschäftspartnern und Kreditgebern aus.[124] Negative Bewertungen können abschreckend auf mögliche Geschäftspartner oder Abnehmer wirken und dem Image des betroffenen Betriebs schaden.[125] Dies kann eine Verminderung des Absatzes, sowie wirtschaftliche Einbußen des Gewerbebetriebs zur Folge haben.[126] Eine Häufung schlechter Bewertungen kann beispielsweise auch zur Sperrung eines Verkäufers auf ebay führen.[127]

Nicht jede negative Äußerung über Waren, Dienstleistungen oder ein Unternehmen als Ganzes verletzt das Recht am eingerichteten und ausgeübten Gewerbebetrieb oder das Unternehmenspersönlichkeitsrecht. Kritische Werturteile werden vom Schutzumfang der Meinungsfreiheit nach § 5 Abs. 1 GG erfasst und sind rechtmäßig, sofern nicht eine unzulässige Schmähkritik vorliegt. Letzteres ist der Fall, wenn die Diffamierung und nicht die Auseinandersetzung mit der Sache erkennbar im Vordergrund steht und die Zielsetzung des

---

[124] Ausführlich dazu *Klöhn/Schmolke*, NZG 2015, 689, 691 ff. m. w. N.

[125] Vgl. *Schmidt*, Äußerungsrechtlicher Schutz, S. 44.

[126] *Spindler*, ZUM 2020, 433, 436 f.

[127] § 5 Nr. 2 ebay-AGB abrufbar unter https://www.ebay.de/help/policies/member-behavior-policies/allgemeine-geschftsbedingungen-fr-die-nutzung-der-deutschen-ebay-dienste?id=4259#%C2%A75%20Sanktionen,%20Sperrung%20und%20K%C3%BCndigung (Stand: 24.05.2022).

Bewertenden darstellt.[128] Die Rechtsprechung verhält sich hierbei erkennbar zurückhaltend, sodass Kritik an einem Gewerbebetrieb in der Regel hinzunehmen ist.[129]

Eine Rechtsverletzung kann deshalb vor allem die Verbreitung falscher Tatsachen darstellen. Etwaige Ansprüche richten sich hierbei häufig schon nach § 824 BGB, sodass ein Rückgriff auf das Unternehmenspersönlichkeitsrecht oder das Recht am eingerichteten und ausgeübten Gewerbebetrieb nicht erforderlich ist. Allerdings ist abzugrenzen, ob überhaupt eine Tatsachenbehauptung vorliegt oder vielmehr die wertende Beurteilung im Vordergrund steht.[130] Äußerungen über wahre geschäftsschädigende Tatsachen greifen nur in Ausnahmefällen in das Recht am eingerichteten und ausgeübten Gewerbebetrieb ein.[131]

Negative und geschäftsschädigende Äußerungen können sich auch dann als rechtsverletzend erweisen, wenn der Bewertung des Unternehmens jegliche Grundlage fehlt. Dies ist zum Beispiel der Fall bei einer Restaurantbewertung, bei der der Bewertende das entsprechende Restaurant überhaupt nicht besucht hat. Zudem besteht die Gefahr, dass durch anonyme Mehrfachbewertungen das Meinungsbild nach außen hin verfälscht wird.[132] Werden bewusst solche falschen Bewertungen eingesetzt, um die Konkurrenz zu schwächen, kommt auch ein Verstoß gegen lauterkeitsrechtliche Vorschriften in Betracht. [133]

---

[128] S. etwa *BVerfG*, Beschl. v- 2.7.2013 – 1 BvR 1751/12, NJW 2013, 3021, 3021; *BVerfG*, Beschl. v. 26.06.1990 - 1 BvR 1165/89, NJW 1991, 95, 95; *BVerfG*, Beschl. v. 22.06.1982 - 1 BvR 1376/79, NJW 1983, 1415, 1415; *BGH*, Urt. v. 29.1.2002 - VI ZR 20/01, NJW 2002, 1192, 1193; *BGH*, Urt. v. 30.5.2000 - VI ZR 276/99, NJW 2000, 3421; *BGH*, Urt. v. 10.11.1994 - I ZR 216/92, NJW-RR 1995, 301, 301; *BGH*, Urt. v. 5.2.1980 - VI ZR 174/78, NJW 1980, 1685, 1685.

[129] S. auch *Förster* in: BeckOK BGB, § 823 Rn. 222.1 f. m.w.N.

[130] Ausführlicher etwa *Schmidt*, Äußerungsrechtlicher Schutz, S. 53 ff.

[131] *Volkmann* in: Spindler/Schuster, § 1004 Rn. 6.

[132] *Schmidt,* Äußerungsrechtlicher Schutz, S. 37.

[133] S. zur Problematik der Anonymität im Hinblick auf lauterkeitsrechtliche Verstöße *Schmidt,* Äußerungsrechtlicher Schutz, S. 37.

4. Eigentum

Eine eigenständige Bedeutung des Eigentumsrechts - neben den Überschneidungen mit anderen Rechtsgütern - ergibt sich vor allem im Zusammenhang mit dem Eigentum an einem Datenträger und den darauf enthaltenen Daten, das durch das Löschen der Daten - zum Beispiel durch einen per Mail versandten Computervirus – verletzt werden kann.[134]

Zudem kann das Fotografieren eines im fremden Eigentum stehenden Gebäudes oder Grundstücks mit anschließendem Upload des Fotos die Rechte des Eigentümers beeinträchtigen, wenn die Fotografie unter Verletzung der Intim- oder Privatsphäre oder des Hausrechts durch Betreten des Grundstücks entstanden ist.[135]
Außerdem können im Internet verbreitete Falschinformationen – beispielsweise fehlerhafte Gebrauchsanleitungen – eine mittelbare Eigentumsverletzung bewirken.[136]

5. Persönlichkeitsrechtsverletzungen

Von besonders großer Bedeutung im Zusammenhang mit Rechtsverletzungen im Internet sind Beeinträchtigungen von Persönlichkeitsrechten. Einzelne besondere Persönlichkeitsinteressen sind speziell gesetzlich normiert. Dazu gehören das Namensrecht in § 12 BGB, das Recht am eigenen Bild in §§ 22 ff. KUG, der Schutz der Ehre in §§ 185 ff. StGB und das oben bereits untersuchte Urheberpersönlichkeitsrecht gemäß §§ 12-14, 23, 25 UrhG.[137]

Daneben existiert das allgemeine Persönlichkeitsrecht, dessen verfassungsrechtliche Verankerung in dem aus Art. 1 I i.V.m. Art. 2 Abs. 1 GG abgeleiteten

---

[134] S. etwa *OLG Karlsruhe*, 07.11.1995 - 3 U 15/95, NJW 1996, 200, 201; *LG Kaiserslautern*, Urt. v. 18.03.1999 - 2 O 966/97, DAR 2001, 225; *Koch*, NJW 2004, 801, 802; *Spindler/Klöhn*, CR 2003, 81, 82; a.A. *LG Konstanz*, 10.05.1996 - 1 S 292/95, NJW 1996, 2662, 2262; *AG Brandenburg*, Urt. v. 22.4.2002 - 32 C 619/99, ITRB 2002, 199, 199.

[135] *BGH*, 17.12.2010 - V ZR 44/10, GRUR 2011, 321, 321 – Preußische Gärten; *BGH*, Urt. v. 17.12.2010 – V ZR 45/10, NJW 2011, 749, 749.

[136] *Hoeren* in: Hoeren/Sieber/Holznagel, Teil 18.2 Rn. 122.

[137] Zum Urheberpersönlichkeitsrecht s. oben unter Kap. 2 § 3 B. I. 2.

Schutzauftrag besteht.[138] Das allgemeine Persönlichkeitsrecht stellt ein sonstiges Recht im Sinne von § 823 Abs. 1 BGB dar. Es handelt sich um ein einheitliches subjektives Recht auf Achtung und Entfaltung der individuellen Persönlichkeit und umfasst das Recht auf Selbstentfaltung und Selbstdarstellung.[139]

Die von der Rechtsprechung ausgearbeiteten Fallgruppen bieten Anhaltspunkte für die Auslegung des Schutzbereichs des Allgemeinen Persönlichkeitsrechts, allerdings sind diese nicht als abschließend anzusehen.[140] Nachstehende Ausführungen untersuchen die einzelnen Ausprägungen des allgemeinen Persönlichkeitsrechts, sowie der speziell geregelten Persönlichkeitsinteressen.

a) Speziell geregelte Ausprägungen

aa) Schutz der persönlichen Ehre vor Äußerungen

Der strafrechtliche Ehrschutz aus den §§ 185 ff. StGB wird auch im Zivilrecht durch § 823 Abs. 2 BGB in Verbindung mit der strafrechtlichen Schutzvorschrift oder ggf. durch § 824 BGB oder § 826 BGB gewährleistet.

Beleidigungen im Sinne von § 185 StGB sind Meinungsäußerungen, durch die die Missachtung einer anderen Person zum Ausdruck gebracht wird.[141] Die Vorschriften zur Verleumdung und übler Nachrede aus §§ 186, 187 StGB richten sich dagegen gegen ehrrührige Tatsachenbehauptungen, die entweder erweislich unwahr sind oder deren Wahrheitsgehalt nicht nachweisbar ist.[142]

---

[138] S. etwa *BVerfG*, Beschl. v. 27.11.1990 - 1 BvR 402/87, NJW 1991, 1471, 1472 – Josephine Mutzenbacher; *BVerfG*, Beschl. v. 19.12.1991 - 1 BvR 382/85, NJW 1992, 815, 815; *BVerfG*, Beschl. v. 24.6.1996 - 2 BvR 2137/95, NJW 1997, 185, 186; *BVerfG*, Beschl. v. 15.8.1996 - 2 BvR 1833/95, NJW 1997, 1632, 1633.

[139] *Mann* in: Spindler/Schuster, § 823 Rn. 2 ff. m.w.N.

[140] *BVerfG*, Beschl. v. 25.02.1993 - 1 BvR 172/93, NJW 1993, 1463, 1464; *BVerfG*, Urt. v. 5.6.1973 - 1 BvR 536/72, NJW 1973, 1226, 1227 – Lebach-Fall; *BGH*, Urt. v. 19.12.1978 - VI ZR 137/77, NJW 1979, 647, 647.

[141] S. etwa *Kühl* in: Lackner/Kühl, § 185 StGB Rn. 3.

[142] S. etwa *Kühl* in: Lackner/Kühl, § 186 StGB Rn. 3; § 187 StGB Rn. 1.

Ob eine Äußerung eine Meinung oder Tatsachenbehauptung darstellt, ist im Wege der Auslegung zu ermitteln.[143] Auch für die Beurteilung des ehrverletzenden Charakters kommt es auf die Deutung und den Kontext einer Äußerung im Einzelfall an.[144] Dies gilt auch dann, wenn eine textbasierte Äußerung etwa durch kleine Bilder oder Zeichen wie Emojis ersetzt wird.[145] Wenn die Zustimmung zu einem Inhalt durch „Liken" zum Ausdruck gebracht wird oder der Inhalt lediglich geteilt wird, liegt in der Regel aber keine Rechtsverletzung vor.[146]

Ehrverletzende Äußerungen spielen eine unrühmliche Rolle beispielsweise in Bewertungsplattformen, sozialen Netzwerken, Chats und Foren.[147] Das Ausmaß und die Häufigkeit solcher Rechtsverletzungen zeigt sich auch dadurch, dass sich Begriffe wie „Cybermobbing" und „Shitstorm" in unserem Sprachgebrauch etabliert haben. Die psychischen Folgen für die Betroffenen können vor allem bei immer wiederkehrenden Rechtsverletzungen gravierend sein.[148] Zudem kann sich durch wiederkehrende herabwürdigende Äußerungen ein negatives Bild in der Öffentlichkeit festsetzen.[149]

Die Anonymität begünstigt dabei die Verbreitung von ehrverletzenden Äußerungen im Internet, was zur Verrohung der Online-Kommunikation führen kann.[150] Unter dem Deckmantel der Anonymität lassen sich im Internet schnell und gegebenenfalls unüberlegt Äußerungen verbreiten, die man vielleicht von Angesicht zu Angesicht nicht vorgenommen hätte. Dennoch besteht die Gefahr, dass sich eine aufgeheizte Stimmung im Internet auch auf die analoge Welt

---

[143] *BGH*, Urt. v. 16.11.2004 - VI ZR 298/03, NJW 2005, 279, 279 ff.; *Härting*, Internetrecht, Rn. 467 ff.

[144] Ausführlich zur Bestimmung des Aussagegehalts einer Äußerung im Internet *Seitz* in: Hoeren/Sieber/Holznagel, Teil 8 Rn. 15 ff.

[145] *Wandtke/Ostendorff,* ZUM 2021, 26, 35. S. zum „Mittelfinger-Emoji" *AG Bergheim*, Beschl. v. 1.10.2018 – 61 F 219/18, BeckRS 2018, 23574, 23574; *Burschel,* NZFam 2018, 1056, 1056.

[146] S. ausführlich zum Meinungsstreit im Hinblick auf die Strafbarkeit beim Liken und Teilen von Inhalten im Internet *Eckel/Rottmeier,* NStZ 2021, 1, 2 ff.

[147] S. auch *Gounalakis/Rhode*, Persönlichkeitsschutz, Rn. 155.

[148] S. etwa *Richter/Geschke/Klaßen,* ZJJ 2020, 148, 152.

[149] Vgl. *Großmann,* GA 2020, 546, 550 f.

[150] S. *Regierungsentwurf*, BT-Drs.18/12356, S. 1; *Kühling*, ZUM 2021, 461, 462 f.; *Pille,* NJW 2018, 3545, 3546.

überträgt. Deshalb sind etwa rassistische, sexistische oder antisemitische Inhalte im Internet kein rein individuelles Problem, sondern vielmehr ein gesellschaftliches Phänomen.[151] Auch der Gesetzgeber hat diese Problematik erkannt und versucht mit dem Netzwerkdurchsetzungsgesetz entgegenzuwirken.[152]

Zudem wurde kürzlich § 192a StGB eingeführt, der die sogenannte „verhetzende Beleidigung" unter Strafe stellt.[153] Damit werden Inhalte erfasst, die geeignet sind die Menschenwürde einer Person anzugreifen, die einer im Hinblick auf ihre Herkunft, Weltanschauung, Behinderung oder sexuellen Orientierung bestimmten Gruppe angehört, indem diese Gruppe beschimpft, böswillig verächtlich gemacht oder verleumdet wird. Bestraft wird, wer einen entsprechenden Inhalt an eine zu einer der aufgeführten Gruppen zugehörigen Person gelangen lässt. Damit sollten insbesondere zur Volksverhetzung geeignete Inhalte, die bisher weder von § 130 StGB, noch von § 185 StGB erfasst wurden, unter Strafe gestellt werden.[154]

bb) Recht am eigenen Bild

Das Recht am eigenen Bild ist als spezielle Ausprägung des allgemeinen Persönlichkeitsrechts in den §§ 22 ff. KUG normiert. § 22 KUG enthält ein generelles Verbot des Verbreitens oder öffentlich Zurschaustellens von Bildnissen ohne Einwilligung des Abgebildeten. Ausnahmen von diesem Verbot enthalten die Erlaubnistatbestände des § 23 und § 24 KUG.

Insbesondere dürfen nach § 23 Abs. Nr. 1 KUG Bildnisse auch ohne Einwilligung verbreitet werden, die aus dem Bereich der Zeitgeschichte stammen oder die nach § 23 Abs. 1 Nr. 4 KUG einem höheren Interesse der Kunst dienen.[155] Einer Einwilligung bedarf es gemäß § 23 Abs. 1 Nr. 2 und 3 KUG darüber hinaus nicht, wenn die abgebildeten Personen nur als Beiwerk neben einer Örtlichkeit erscheinen oder im Zusammenhang mit der Teilnahme an einer

---

[151] *Wandtke/Ostendorff,* ZUM 2021, 26, 26 f.; *Hoven/Witting*, NJW 2021, 2397, 2398.

[152] S. *Regierungsentwurf*, BT-Drs. 18/12356, S. 1 f.

[153] S. dazu *Ebner/Kulhanek*, ZStW 133 (2021), 984, 984 ff.; *Valerius,* ZStW 132 (2020), 666 ff.

[154] S. *Bericht des Ausschusses für Recht und Verbraucherschutz*, BT-Drs. 10/31115, S. 15; *Valerius* in: BeckOK StGB, § 192a StGB Rn. 1 f.

[155] Ausführlicher *Härting,* Internetrecht, Rn. 602 ff.

Versammlung abgebildet wurden. Diese Erlaubnistatbestände gelten jedoch nicht, wenn durch die Verbreitung oder Schaustellung ein berechtigtes Interesse des Abgebildeten verletzt wird.

Verletzungen des Rechts am eigenen Bild können im Internet eine vielfältige Rolle spielen. Zu nennen sind hier vor allem das Teilen und Verbreiten von Bildern über soziale Netzwerke und Kommunikationsplattformen oder auch Bildberichterstattungen in Online-Medien.[156] Zunehmend ist auch die Manipulation von Bildern oder Videos mittels sogenannter Deepfake-Technologie besorgniserregend.[157] Dadurch kann eine Person durch täuschend echte Darstellung fälschlicherweise in Zusammenhang etwa mit pornographischen Inhalten oder falschen Aussagen gebracht werden.
Beim Veröffentlichen oder Verbreiten von Bildern kann das öffentliche Interesse an Bildnissen aus dem Bereich der Zeitgeschichte (§ 23 Abs. 1 Nr. 1 KUG) das Recht am eigenen Bild des Betroffenen jedoch überwiegen. Prominente und Politiker trifft hierbei anders als Privatpersonen eine erweiterte Duldungspflicht.[158] Dennoch erkennt das *BVerfG* zutreffend, dass der Schutz des Persönlichkeitsrechts von Politikern auch im öffentlichen Interesse liegt:[159]

„Denn eine Bereitschaft zur Mitwirkung in Staat und Gesellschaft kann nur erwartet werden, wenn für diejenigen, die sich engagieren und öffentlich einbringen, ein hinreichender Schutz ihrer Persönlichkeitsrechte gewährleistet ist."[160]

Je nach Einzelfall ist eine Abwägung zwischen der Meinungs- bzw. Pressefreiheit einerseits und den Persönlichkeitsrechten der abgebildeten Person andererseits

---

[156] S. dazu etwa *Härting/Schätzle*, ITRB 2010, 39, 41; S. zu Persönlichkeitsrechtsverletzungen in sozialen Netzwerken *Verheijden*, Rechtsverletzungen auf YouTube und Facebook, S. 37 ff. Zur Bildberichtserstattung in Online-Medien *Wandtke*, MMR 2019, 142, 144 ff.

[157] S. dazu etwa *Hinderks*, ZUM 2022, 110, 110 ff.

[158] S. *BGH*, Urt. v. 6.2.2018 – VI ZR 76/17, GRUR 2018, 549, 551 – Christian Wulff im Supermarkt; *BGH*, Urt. v. 27.9.2016 – VI ZR 310/14, ZD 2017, 137, 137 – Klaus Wowereit.

[159] *BVerfG,* Beschl. v. 19.12.2021 – 1 BvR 1073/20, NJW 2022, 680 Rn. 35 - Beleidigende Äußerungen über bekannte Politikerin in sozialen Netzwerken; *BVerfG,* Beschl. v. 6.11.2019 – 1 BvR 276/17, NJW 2020, 314 Rn. 108 – Recht auf Vergessen II; *BVerfG,* Beschl. v. 19.5.2020 – 1 BvR 2397/19, NJW 2020, 2622 Rn. 32.

[160] *BVerfG,* Beschl. v. 19.12.2021 – 1 BvR 1073/20, NJW 2022, 680 Rn. 35 - Beleidigende Äußerungen über bekannte Politikerin in sozialen Netzwerken; *BVerfG,* Beschl. v. 6.11.2019 – 1 BvR 276/17, NJW 2020, 314 Rn. 108 – Recht auf Vergessen II; *BVerfG,* Beschl. v. 19.5.2020 – 1 BvR 2397/19, NJW 2020, 2622 Rn. 32.

erforderlich.[161] Bei redaktionellen Beiträgen im Internet spielt die Anonymität der möglichen Rechtsverletzer im Gegensatz zur Kommunikation in sozialen Medien allerdings wohl nur eine untergeordnete Rolle, da der Verantwortliche meist leicht zu ermitteln sein dürfte.

Eine Verletzung des Rechts am eigenen Bild kommt auch in Form von sogenannten Rache-Pornos (revenge porn) vor.[162] Dabei handelt es sich um pornographische oder intime Bilder oder Videos einer Person, die ohne deren Einwilligung häufig zu Rachezwecken in sozialen Netzwerken, über Messenger-Dienste oder auf Pornoseiten veröffentlicht werden. Ähnlich verhält es sich auch mit Bildnissen, die zwar nicht pornographischer Natur, aber anderweitig kompromittierend sind und beispielsweise im Zusammenhang mit Cyber-Mobbing-Attacken zur Diffamierung einer Person eingesetzt werden. Nicht immer ist dabei der Anbieter solcher Inhalte dem Betroffenen bekannt oder lässt es sich nachweisen, wer für den Inhalt verantwortlich ist. Im Hinblick auf die hohe Intensität solcher intimer Eingriffe ist kaum ein Fall denkbar, bei dem eine Interessensabwägung zulasten der betroffenen Person ausfallen könnte, zumal bereits das Vorliegen eines berechtigten Interesses an einer Veröffentlichung äußerst fragwürdig erscheint.[163]

Das Recht am eigenen Bild kann auch durch sogenannte Memes beeinträchtigt werden. Dabei handelt es sich um häufig humoristische, nutzergenerierte kleinere Inhalte, die zumeist über Internetplattformen verbreitet werden und weiterbearbeitet und kombiniert werden können.[164] Als Grundlage für ein Memes können auch Bilder von Personen dienen. Beispielsweise werden dabei häufiger auch Bildnisse von bekannten Personen und Politikern verwendet.[165] Neben der oben bereits beschriebenen urheberrechtlichen Problematik kann daher auch

---

[161] *BGH,* Urt. v. 29.5.2018 – VI ZR 56/17, GRUR 2018, 964, 966 – Tochter von Prinzessin Madeleine; *BGH*, Urt. v. 6.2.2018 – VI ZR 76/17, GRUR 2018, 549 – Christian Wulff im Supermarkt; *BGH*, Urt. v. 27.9.2016 – VI ZR 310/14, ZD 2017, 137, 137 – Klaus Wowereit. Zu den wichtigsten Kriterien der Abwägung s. etwa *Mann* in: Spindler/Schuster, § 823 BGB Rn. 57.

[162] S. etwa *LG Köln*, Urt. v. 15.11.2017 - 28 O 146/17, BeckRS 2017, 154937.

[163] S. etwa LG Köln, Urt. v. 15.11.2017 - 28 O 146/17, BeckRS 2017, 154937.

[164] *Maier*, GRUR-Prax 2016, 397, 397 f.

[165] S. auch *Wandtke*, MMR 2019, 142, 143 f.

das Recht der abgebildeten Person am eigenen Bild berührt sein.[166] Zur Beurteilung der Zulässigkeit eines Memes muss im konkreten Einzelfall eine Abwägung mit der Meinungs- und Kunstfreiheit des Nutzers vorgenommen werden.[167]

cc) Recht am eigenen Namen

Der Schutz des eigenen Namens ist in § 12 BGB geregelt und adressiert Rechtsverletzungen, bei denen das Recht zum Gebrauch eines Namens dem Berechtigten abgestritten wird oder dass ein anderer unbefugt den Namen des Berechtigten gebraucht. Im medienspezifischen Kontext ist vor allem die Namensanmaßung –also der unbefugte Gebrauch eines fremden Namens- relevant.[168]

Zur Anwendung kommt § 12 BGB dabei vor allem im Zusammenhang mit Domainnamen. Dadurch, dass eine Second-Level-Domain nur einmalig vergeben werden kann, hat der Namensinhaber ein schutzwürdiges Interesse gegenüber einem Nichtberechtigten, seinen Namen für eine Domain nutzen zu können.[169] Daneben kann gegebenenfalls auch der Inhaber eines Unternehmenskennzeichens auf § 12 BGB zurückgreifen, wenn sich nicht schon aus §§ 14, 15 MarkenG ein Anspruch ergibt – vor allem, wenn die Unternehmensbeziehung außerhalb des gesetzlichen Verkehrs benutzt wird.[170] Der Inhaber des Namensrechts kann gegen einen Domaininhaber vorgehen, sofern eine unbefugte Namensnutzung vorliegt, durch die eine Zuordnungsverwirrung eintritt und der Namensinhaber dadurch in seinen Rechten verletzt wird.[171] Ähnlich wie

---

[166] Zur urheberrechtlichen Problematik bei Memes, S. oben unter Kap. 2 § 3 B. I. 1. c).

[167] *BGH*, Urt. v. 8.11.2005 - VI ZR 64/05, NJW 2006, 603, 605; *Wandtke*, MMR 2019, 142, 144 ff.

[168] S. *Meyer,* Identität und und virtuelle Identität natürlicher Personen im Internet, S. 73.

[169] Vgl. *Sandor,* Datenspeicherung, S. 58.

[170] Zur Anwendbarkeit des § 12 BGB neben §§ 14, 15 MarkenG S. *BGH*, Urt. v. 6.11.2013 – I ZR 153/12, GRUR 2014, 506 Rn. 8 - sr.de; *BGH*, Urt. v. 9. 11. 2011 - I ZR 150/09, GRUR 2012, 304 Rn. 32 – Basler Haarkosmetik; *BGH*, Urt. v. 24.4.2008 - I ZR 159/05, GRUR 2008, 1099 Rn. 10 – afilias.de; *BGH*, Urt. v. 9.9.2004 - I ZR 65/02, GRUR 2005, 430, 430 f. – mho.de; *BGH*, Urt. v. 22.11.2001 - I ZR 138/99, GRUR 2002, 622, 623 – shell.de; *Thalmaier* in: BeckOK Markenrecht, § 15 Rn. 130.

[171] *Becker*, WRP 2010, 467, 473; Härting, Internetrecht, Rn. 2339 ff.; *Müller* in: Spindler/Schuster, § 12 BGB Rn. 66; Thalmaier in: BeckOK Markenrecht, § 15 MarkenG Rn. 139 ff.

bereits zu den Markenrechtsverletzungen im Domainbereich erläutert,[172] lassen sich seit dem Inkrafttreten der DS-GVO die persönlichen Daten von Domaininhabern nicht mehr einfach über eine Whois-Abfrage im Internet abrufen, sodass die Rechteinhaber verstärkt auf eine entsprechende Auskunft der Registrierungsstelle angewiesen sind.

Zum Anwendungsbereich des § 12 BGB zählen auch Namensrechtsverletzungen im Zusammenhang mit Identitätsdiebstahl und Identitätsmissbrauch. Dazu gehören Fälle, in denen unbefugt unter einem fremden Namen - häufig auch unter Verwendung weiterer persönlicher Daten (Wohnanschrift, Telefonnummern, Kontodaten, etc.) - im Internet agiert wird: Beispiele sind das Handeln unter fremden Namen auf Internetmarktplätzen und in Internetauktionshäusern,[173] das Erstellen von Fake-Profilen in sozialen Netzwerken, und das Versenden von Nachrichten über Messenger-Dienste.[174] Der Missbrauch solcher persönlicher Daten und vor allem die Namensanmaßung kann für den Betroffenen sehr schwer wiegen. Die fremden Daten werden entweder zum eigenen Vorteil eingesetzt oder auch um bewusst dem Betroffenen dadurch zu schaden. Letzteres ist beispielsweise der Fall, wenn im Zusammenhang mit Cybermobbing-Attacken unter falschem Namen oder unter falschem Profil Äußerungen verbreitet werden, die zur einer Rufschädigung oder Diffamierung des Namensinhabers führen.

b) Relevante Fallgruppen des allgemeinen Persönlichkeitsrechts

Auch wenn keine der besonderen Ausprägungen des Persönlichkeitsrechts einschlägig ist, kann eine Verletzung des allgemeinen Persönlichkeitsrechts gegeben sein. Bei Rechtsverletzungen im Internet sind vor allem die Fallgruppen des Rechts auf informationelle Selbstbestimmung und der Schutz vor Unwahrheit und das Recht auf Selbstdarstellung von Bedeutung.

---

[172] S. oben unter Kap. 2 § 3 B. II.

[173] S. zum Identitätsdiebstahl im Rahmen einer Internetauktion etwa *OLG Brandenburg*, Urt. v. 16.11.2005 - 4 U 5/05, NJW-RR 2006, 1193, 1193 ff.

[174] Ausführlicher zu Namensrechtsverletzungen im Internet *Meyer*, Identität und virtuelle Identität, S. 68 ff. S. zum Account Grabbing *Solmecke* in: Hoeren/Sieber/Holznagel, Teil 21.1 Rn. 10 ff. S. zu Fake-Profilen *OLG Köln,* Urt. v. 16.11.2017 – 15 U 71/17, BeckRS 2017, 163837.

aa) Recht auf informationelle Selbstbestimmung

Eine besonders medienrelevante Ausprägung des allgemeinen Persönlichkeitsrechts ist das Recht auf informationelle Selbstbestimmung. Es dient dazu den Einzelnen mit Blick auf die immer weiter fortschreitende Digitalisierung weitgehend zu ermächtigen, selbst über die Verbreitung und Offenbarung persönlicher Sachverhalte zu entscheiden.[175] Dieses Recht ist beeinträchtigt, wenn beispielsweise in sozialen Netzwerken persönliche Daten wie Geburtsdatum, Wohnanschrift, Telefonnummern oder Informationen darüber, wann sich eine Person an einem bestimmten Ort aufgehalten hat, ohne Erlaubnis des Betroffenen weitergegeben werden.

Dazu gehört etwa die Veröffentlichung von Feindeslisten oder das Doxing, bei dem in böswilliger Absicht personenbezogene Daten und Informationen einer Person gesammelt werden, zum Beispiel um diese Person anschließend in der Öffentlichkeit bloßzustellen.[176] Der Gesetzgeber hat auf derartige Herausforderungen durch die Einführung eines neuen Tatbestands in § 126a StGB reagiert, der das gefährdende Verbreiten personenbezogener Daten unter Strafe stellt.[177]

Ebenso tangiert aber auch das Verbreiten eines Trojaners per Mail, durch den ein Dritter Zugriff auf vertrauliche Daten des Empfängers erhält, das Recht auf informationelle Selbstbestimmung.[178] Dasselbe gilt für das Veröffentlichen vertraulicher Mails oder Nachrichten.[179]

Wie allgemein bei den verschiedenen Ausprägungen der Persönlichkeitsrechte gilt, ergeben sich hierbei natürlich auch Überschneidungen mit anderen Fallgruppen – zum Beispiel mit dem Recht am eigenen Bild oder am eigenen Namen.

---

[175] S. etwa *BVerfG*, Beschl. v. 9.3.1988 - 1 BvL 49/86, NJW 1988, 2031, 2031 f.

[176] S. *Hoven/Witting*, NJW 2021, 2397, 2401. S. zum Doxing *Kubiciel/Großmann*, NJW 2019, 1050, 1050 ff.

[177] S. *Regierungsentwurf,* BT-Drs. 19/28678, S. 1; S. auch *Beukelmann,* NJW-Spezial 2021, 248, 248; *Vassilaki,* K&R 2021, 763.

[178] *LG Berlin*, Beschl. v. 14.5.1998 - 16 O 301–98, NJW 1998, 3208, 3208 f.; *Koch*, NJW 2004, 801, 803.

[179] *LG Köln,* Urt. v. 6.9.2006 - 28 O 178/06, CR 2007, 195, 195 f.; Ausführlicher *Härting,* Internetrecht, Rn. 536 ff.

bb) Schutz vor Unwahrheit und Recht auf Selbstdarstellung

Weiterhin schützt das allgemeine Persönlichkeitsrecht in verschiedenen Ausprägungen auch vor der Verbreitung von Unwahrheit.[180] Grundsätzlich ist es das Recht einer jeden Person, sich nach außen hin selbst darzustellen und zu entscheiden, ob und ggf. in welchem Umfang persönliche Informationen öffentlich dargestellt werden können. Natürlich ist dies nicht gleichbedeutend mit dem Schutz vor jeglicher öffentlicher Kritik oder Meinungsäußerung. Ein ausschließliches Verfügungsrecht über die öffentliche Selbstdarstellung beinhaltet das allgemeine Persönlichkeitsrecht dementsprechend nicht.[181]

Allerdings schützt es den Einzelnen vor der Verbreitung unwahrer Tatsachen, die die eigene Person betreffen.[182] Dazu zählen zum Beispiel die Äußerung falscher Tatsachen über einen anderen in Personenbewertungsportalen,[183] sozialen Netzwerken und Kommunikationsplattformen. Von besonderer Bedeutung ist in diesem Zusammenhang auch das bewusste Veröffentlichen von Falschmeldungen und Desinformationen über andere Personen (sog. Fake-News), die einer gezielten meist politischen Agenda dienen und sich besonders über soziale Netzwerke sehr leicht verbreiten lassen.[184] Die Gefahr, die vom bewussten Einsatz solcher Falschmeldungen für den Betroffenen, aber auch für die Gesellschaft ausgeht, kann dabei gravierend sein.[185] Sie können beispielsweise im Rahmen von Wahlkämpfen gezielt eingesetzt werden, um die gegnerische Position zu schwächen. Aufsehen erregten in der jüngeren Vergangenheit vor allem Fake-News im Zusammenhang mit der amerikanischen Präsidentschaftswahl im Jahr 2016.

---

[180] S. auch *Müller* in: Spindler/Schuster, § 823 BGB Rn. 67 f.

[181] *BVerfG*, Beschl. v. 26.2.2008 - 1 BvR 1602/07 u.a., NJW 2008, 1793, 1793 ff. – Caroline von Hannover; *BVerfG*, Beschl. v. 18.2.2010 - 1 BvR 2477/08, NJW 2010, 1587, 1587 ff.

[182] In strafrechtlicher Hinsicht ergibt sich ein Schutz vor ehrenrührigen unwahren Tatsachen auch aus § 186 StGB; S. oben unter Kap. 2 § 3 B.V. 1. a).

[183] Häufig handelt es sich bei Bewertungen auf Personenbewertungsportalen aber nicht um Tatsachen, sondern um Meinungsäußerungen, deren Zulässigkeit schwieriger zu beurteilen ist, S. dazu etwa *Härting,* Internetrecht, Rn. 550 ff.

[184] S. dazu auch *Wandtke/Ostendorff,* ZUM 2021, 26, 34 f.

[185] Ausführlicher etwa *Holznagel*, MMR 2018, 18, 18 ff.

Eine ähnliche Schutzrichtung ergibt sich auch aus dem vom allgemeinen Persönlichkeitsrecht erfassten Recht am eigenen Wort. Davon wird unter anderem der Schutz vor einer unrichtigen Wiedergabe einer angeblichen Äußerung und davor, falsch zitiert zu werden, umfasst.[186] Aufmerksamkeit erregte beispielsweise ein Beitrag auf Facebook mit einem angeblichen Zitat der Politikerin Renate Künast, das zu vielen ehrverletzenden Kommentaren führte.[187]

c) Interessensabwägung

Sehr häufig ist bei einer möglichen Persönlichkeitsrechtsverletzung eine umfangreiche Abwägung des allgemeinen Persönlichkeitsrechts mit den Interessen der möglichen Rechtsverletzer (Meinungsfreiheit, Pressefreiheit, Kunstfreiheit) oder auch öffentlichen Interessen durchzuführen. Die Intensität des Eingriffs in das allgemeine Persönlichkeitsrecht spielt dabei eine wichtige Rolle. Anhaltspunkte für die Beurteilung der Schwere eines Eingriffs bietet die Unterscheidung zwischen der Intim-, Privat- und Sozialsphäre eines Menschen.[188] Die Anforderungen an eine Rechtmäßigkeit des Eingriffs sind umso höher, je stärker der Kernbereich der Persönlichkeit betroffen ist.[189] Die Interessensabwägung bei bekannten Persönlichkeiten geht dagegen eher zu Lasten des Persönlichkeitsrechts als bei unbekannten Personen.[190]

Bei der Abwägung mit der Meinungsfreiheit des Nutzers ist zu berücksichtigen, dass Kritik an einer Person auch in überspitzter Weise geäußert werden darf. Auch eine satirische Auseinandersetzung ist grundsätzlich möglich.[191] Zwar ist eine bloße Schmähkritik, bei der es vordergründig auf die bloße Herabwürdigung oder Diffamierung einer Person ankommt, unzulässig. Ansonsten ist allerding stets eine Abwägung erforderlich, selbst wenn eine Äußerung die Ehre

---

[186] BGH, Urt. v. 21.6.2011 - VI ZR 262/09, GRUR-RR 2012, 83 – Das Prinzip Arche Noah; *Müller* in: Spindler/Schuster, § 823 BGB Rn. 59.

[187] S. dazu *LG Berlin*, Beschl. v. 9.9.2019 – 27 AR 17/19, MMR 2019, 754, 754 ff.

[188] S. dazu etwa *Härting,* Internetrecht, Rn. 432 ff. m.w.N.

[189] *BGH*, Urt. v. 6.3.2007 - VI ZR 51/06, NJW 2007, 1977, 1979 – Caroline von Hannover.

[190] S. dazu *Wandtke/Ostendorff,* ZUM 2021, 26, 34.

[191] *BVerfG*, Beschl. v. 19.5.2020 – 1 BvR 1094/19, ZUM 2021, 45, 45 ff.; *Wandtke/Ostendorff*, ZUM 2021, 26, 33.

einer Person erheblich herabsetzt.[192] Das Gewicht der Meinungsfreiheit ist allerdings geringer, wenn lediglich die „emotionalisierende Verbreitung von Stimmungen gegen einzelne Personen" im Vordergrund steht.[193]

4. Leben, Gesundheits- und Körperverletzung

Das Recht auf Leben, Gesundheit und körperliche Unversehrtheit spielt im Rahmen dieser Arbeit eher eine untergeordnete Rolle. Dennoch können beispielsweise Persönlichkeitsrechtsverletzungen auch zu körperlichen und gesundheitlichen Beeinträchtigungen führen. Zum Beispiel können sich durch Cybermobbing oder Cyberstalking Depressionen, Angststörungen oder andere psychische Erkrankungen entwickeln, die eine Körper- beziehungsweise Gesundheitsverletzung begründen. [194]

Auch mittelbare Rechtsverletzungen durch das Verbreiten gefährlicher (z.B. medizinischer) Falschinformationen können zu körperlichen und gesundheitlichen Beeinträchtigungen führen.[195] Etwas Ähnliches gilt auch bei Aufrufen zu Gewalt gegen bestimmte Personen oder einen bestimmten Personenkreis, wenn Dritte diesen Aufrufen nachkommen.

Teilweise wird in sozialen Netzwerken und Foren auch zu gefährlichen Mutproben oder im schlimmsten Fall sogar zum Suizid aufgerufen. In der jüngeren Vergangenheit erregten gefährliche – meist über den WhatsApp-Messenger verbreitete - Kettenbriefe Aufsehen, die die überwiegend jungen Empfänger unter Druck setzten und zu gefährlichen Aufgaben oder sogar zum Suizid aufforderten.[196] Ob es in solchen Fällen wirklich zu einer zurechenbaren Rechtsverletzung kommt, lässt sich nur anhand des Einzelfalls bestimmen.

---

[192] *BVerfG*, Beschl. v. 19.5.2020 – 1 BvR 1094/19, ZUM 2021, 45; *Wandtke/Ostendorff*, ZUM 2021, 26, 33.

[193] *BVerfG,* Beschuss. v. 19.12.2021 – 1 BvR 1073/20, GRUR 2022, 335 Rn. 31 – Fall Künast; BVerfG, Beschl. v. 19.5.2020 – 1 BvR 2397/19, MMR 2020, 834 Rn. 29.

[194] *Bieszk/Stadtler*, NJW 2007, 3382, 3383; *Jansen/Hartmann*, NJW 2012, 1540, 1541; *Keiser*, NJW 2007, 3387, 3388 ff.

[195] *Hoeren* in: Hoeren/Sieber/Holznagel, Teil 18.2 Rn. 122.

[196] S. zur sog. Momo-Challenge https://de.wikipedia.org/wiki/Momo_Challenge (Stand: 24.0.2022). S. zur sog. Blue Wales Challenge https://de.wikipedia.org/wiki/Blue_Whale_Challenge (Stand: 24.05.2022).

III. Besonderheiten bei Rechtsverletzungen im Internet

Rechtsverletzungen im Internet wirken im Vergleich zur analogen Welt in besonderer Weise in die Rechte der Betroffenen ein. Die Anonymität der Nutzer erschwert die Rechtsdurchsetzung und kann das Auftreten von Rechtsverletzungen im Internet begünstigen.[197] Ohne die Handlung des Rechtsverletzers mit dessen Identität verknüpfen zu können, kann der Inhaber des beeinträchtigten Rechtsguts seine Rechte nicht gerichtlich durchsetzen.[198] Auch eine strafrechtliche Verfolgung kann an der Anonymität der Nutzer scheitern. Nicht nur private Nutzer, sondern auch Anbieter von Webseiten wie kinox.to, die gezielt illegale Inhalte anbieten, sind häufig nur schwer ermittelbar.[199] Dies birgt die Gefahr, dass rechtsverletzende Handlungen im Internet zunehmen und das Internet im Vergleich zur analogen Welt als rechtsfreier Raum wahrgenommen wird, sodass die Hemmschwelle der Nutzer sinkt.[200] Zudem ermöglicht die Anonymität zum Beispiel Äußerungen über Personen, deren Identität erkennbar ist, ohne dass der Äußernde selbst seine Identität preisgeben muss. Der betroffenen Person wird es so erschwert, sich zu wehren, weil sie die Umstände, unter denen es zur Äußerung kam, gegebenenfalls gar nicht kennt.[201]

Neben der Anonymität, die die Zunahme von Rechtsverletzungen zumindest begünstigen kann und die Rechtsdurchsetzung erschwert, spielt auch die schnelle Verbreitung von Rechtsverletzungen im Internet eine Rolle. Damit geht häufig auch eine Perpetuierung der Inhalte einher:[202] Ist ein rechtsverletzender Inhalt einmal online verfügbar, kann er von zahlreichen Nutzern in kürzester Zeit geteilt und weiter verbreitet werden, sodass er sich kaum vollständig

---

[197] *Askani,* Private Rechtsdurchsetzung, S. 135; *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 103; *Kipshagen,* Haftung bei offenem WLAN, S. 51 f.; *Schmidt,* Äußerungsrechtlicher Schutz, S. 38.

[198] *Nietsch*, Anonymität und Durchsetzung, S. 113 ff.

[199] S. *OLG München*, Urt. v. 14.6.2018 – 29 U 732/18, GRUR 2018, 1050, 1054 – Kinox.to.

[200] *Lausen*, ZUM 2017, 278, 288.

[201] *Kühling,* NJW 2015, 447, 449 der deshalb von einer Anonymität-Asymmetrie spricht; S. auch *Kersten,* JuS 2017, 193, 193.

[202] S. auch *Beck,* MMR 20009, 736, 738 f.; *Glaser,* NVwZ 2012, 1432, 1432; *Greve/Schrädel*, MMR 2008, 644, 648; *Härting*, Internetrecht, Rn. 427 ff.; *Kreutzer*, MMR 2007, 732, 734; *Krischker,* JA 2013, 488, 489 ff.; *Kümmel*, Die Implementierung der Haftung, S. 13; *Reichenbacher,* JZ 2020, 558, 561; *Sahl/Bielzer*, ZRP 2020, 2, 4.

wieder entfernen lässt.[203] Auch wenn der ursprüngliche Inhalt bereits entfernt wurde, können zahlreiche Kopien auf den Rechnern anderer Nutzer erstellt worden sein.[204] Der Schnelligkeit der Verbreitung von rechtsverletzenden Inhalten steht die lange Dauer und Beschwerlichkeit gerichtlicher Verfahren gegenüber.[205]

Im Unterschied zur analogen Welt wirken sich die Rechtsverletzungen zudem in der Regel nicht nur auf einen lokalen oder begrenzten Bereich aus, sondern sind weltweit abrufbar.[206] Der Betroffene kann sich daher - zum Beispiel bei Persönlichkeitsrechtsverletzungen - dem Wirkungskreis der Rechtsverletzung nicht durch einen Ortswechsel entziehen, da zum Beispiel auch die neuen Nachbarn und Arbeitgeber Kenntnis von den entsprechenden Inhalten erlangen können.[207]

D. Zusammenfassung Kapitel 2

Rechtsverletzungen durch Nutzer von Internetdiensten sind ein häufiges Phänomen. Viele Internetnutzer treten dabei anonym auf. Die Anonymität im Sinne dieser Arbeit besteht in der Nicht-Identifizierbarkeit des Nutzers durch den Rechteinhaber. Diese kann Rechtsverletzungen begünstigen und erschwert die Rechtsdurchsetzung für die Rechteinhaber.

Rechtsverletzungen erfolgen im Internet auf vielfältige Weise. Besonders häufig sind Rechte des geistigen Eigentums, Persönlichkeitsrechte und das Recht am eingerichteten und ausgeübten Gewerbebetrieb betroffen. Die Besonderheiten von Rechtsverletzungen im Online-Bereich können die Intensität einer

---

[203] Das gilt vor allem, wenn ein Inhalt bei einer Suchmaschine abrufbar war, S. *Brunst,* Anonymität im Internet, S. 76.

[204] *Greve/Schrädel*, MMR 2008, 644, 648; *Kreutzer*, MMR 2007, 732, 734*, Schmidt*, Äußerungsrechtlicher Schutz, S. 39.

[205] *Askani,* Private Rechtsdurchsetzung, S. 139 f.

[206] S. dazu *Schmidt,* Äußerungsrechtlicher Schutz, S. 38.

[207] Zur Ubiquität von Persönlichkeitsrechtsverletzungen S. *EuGH*, Urt. v. 13.5.2014 – C-131/12, GRUR 2014, 895, 900 – Google Spain.

Rechtsverletzung erheblich verstärken.[208] Vor diesem Hintergrund können massenhaft auftretende Rechtsverletzungen im Internet nicht als hinzunehmendes gesellschaftliches Phänomen bagatellisiert werden. Vielmehr muss das Gewicht der Eingriffe in die Rechte der Betroffenen beachtet und bei der Ausgestaltung von Rechtsschutzmöglichkeiten berücksichtigt werden.

An einer Rechtsverletzung im Internet können neben den betroffenen Rechteinhabern verschiedene Diensteanbieter und deren Nutzer beteiligt sein. Welche Diensteanbieter involviert sind, unterscheidet sich im Einzelfall. Von der Frage der Beteiligung der Diensteanbieter ist insbesondere abhängig, an wen etwaige Auskunftsbegehren der Rechteinhaber gerichtet werden.

---

[208] S. zur Intensität von Persönlichkeitsrechtsverletzungen im Hinblick auf die Dauerhaftigkeit *LG Kiel*, Urt. v. 27.4.2006 - 4 O 251/05, NJW 2007, 1002, 1002.

Kapitel 3

Interessenskonflikt

Bei anonymen Rechtsverletzungen im Internet besteht ein Konflikt zwischen den Interessen der Rechteinhaber, Nutzer und Diensteanbieter. Dabei sind vor allem die Interessen der Rechteinhaber und der Nutzer gegenläufig. Die Rechteinhaber werden einen möglichst umfassenden Schutz ihrer Rechtsgüter und möglichst effektive und wirkungsvolle Rechtsschutzmöglichkeiten anstreben. Dies umfasst auch die Möglichkeit, Auskunft über die Identität des Rechtsverletzers zu erhalten. Die Nutzer dagegen berufen sich auf den Schutz ihrer Anonymität und die möglichst ungestörte Internetnutzung als Ausdruck individueller Freiheitsrechte. Diensteanbieter dagegen könnten anstreben, ihre Dienste unter möglichst geringer staatlicher Regulierung und Einflussnahme erbringen zu können.

Alle Beteiligten können sich dabei auf Rechtspositionen berufen, die ihre Grundlage im Grundgesetz beziehungsweise in den Grundrechten der Grundrechtecharta der europäischen Union finden. Sowohl die derzeit existierenden nationalen Auskunftsansprüche als auch ein möglicher Auskunftsanspruch de lege ferenda, müssen sich an den Wertungen des Grundgesetzes und der Grundrechtecharta messen lassen.

Der Ausgleich der verschiedenen Interessen der Beteiligten ist maßgeblich für die Bewertung der derzeitigen Rechtslage und stellt zugleich die Basis für Verbesserungsvorschläge de lege ferenda dar. Daher sind zunächst die Auswirkungen von Grundrechten des Grundgesetzes und der Grundrechtecharta der europäischen Union auf zivilrechtlichen Streitigkeiten zu untersuchen (A.), sowie die Interessen der Rechteinhaber (B.), der Nutzer (C.), und der Diensteanbieter (D.) zu beleuchten, um aus den gewonnenen Erkenntnissen Folgerungen für den Ausgleich des Interessenskonflikts zu treffen (E.).

A. Auswirkungen von Grundrechten auf zivilrechtliche Streitigkeiten

Die Grundrechte der Rechteinhaber, Nutzer und Diensteanbieter stellen in erster Linie Abwehrrechte gegen den Staat dar. Unter Privaten finden diese grundsätzlich keine unmittelbare Anwendung. Dennoch wirken sich die verfassungsrechtlichen Wertungen auch auf zivilrechtliche Streitigkeiten aus.

Hinsichtlich der nationalen Grundrechte unterliegen der Gesetzgeber sowie die (Zivil-)Gerichte der Grundrechtsbindung nach Art. 1 Abs. 3 GG. Zivilrechtliche Rechtsbeziehungen müssen daher so normiert werden, dass verschiedene Grundrechtspositionen zu einem verhältnismäßigen Ausgleich gebracht werden.[1] Die Zivilgerichte müssen die entsprechenden Regelungen dann ihrerseits verfassungskonform auslegen.[2] Dies beinhaltet etwa die Vornahme umfassender Interessensabwägungen, sowie die Auslegung unbestimmter Rechtsbegriffe im konkreten Einzelfall.

Neben dieser sogenannten „Ausstrahlwirkung der Grundrechte" können dem Staat Pflichten zukommen, bei Gefährdungen für die Grundrechtsträger auch im Zivilrecht ein Mindestmaß an Grundrechtsschutz sicherzustellen.[3] Dem Gesetzgeber kommt dabei aber ein weiter Beurteilungsspielraum zu.[4] Maßgeblich ist das sogenannte Untermaßverbot, nach dem zumindest ein Minimum an

---

[1] Vgl. *BVerfG*, Beschl. v. 24.2.1971 - 1 BvR 435/68, NJW 1971, 1645, 1648; *Starck* in: Mangoldt/Klein/Stark, Art. 1 GG Rn. 312 ff.

[2] *BVerfG*, Beschl. v. 6.11.2019 – 1 BvR 16/13, NJW 2020, 300 Rn. 76 ff. – Recht auf Vergessen I; *BVerfG*, Beschl. v. 11.4.2018 – 1 BvR 3080/09, NJW 2018, 1667 Rn. 34 – Stadionverbot m.w.N.

[3] Siehe zum Begriff der „Ausstrahlwirkung" beziehungsweise der „mittelbaren Drittwirkung" etwa *BVerfG,* Beschl. v. 6.11.2019 – 1 BvR 16/13, NJW 2020, 300 Rn. 75 ff. – Recht auf Vergessen I; *BVerfG,* Beschl. v. 11.4.2018 – 1 BvR 3080/09, NJW 2018, 1667 Rn. 33 ff. - Stadionverbot; *Jarass* in: Jarass/Pieroth, Art. 1 GG Rn. 48 ff.; *Rüfner* in: Isensee/Kirchhoff, Staatsrecht Handbuch V, § 117 Rn. 54 ff. Dagegen mehren sich aber die Literaturstimmen, die eine Ausstrahlwirkung der Grundrechte ablehnen und die Wirkungsweise von Grundrechten auch im Zivilrecht ausschließlich über Abwehr- und Schutzpflichten begründen, s. dazu etwa *Hillgruber* in: BeckOK Grundgesetz, Art. 1 Rn. 73.1 m.w.N., *Neuner*, NJW 2020, 1851, 1851 ff.

[4] S. etwa *BVerfG*, Beschl. v. 11.4.2018 – 1 BvR 3080/09, NJW 2018, 2542 Rn. 31 ff. – Stadionverbot m.w.N.

Schutz gewährleistet sein muss. Der Staat verletzt seine Schutzpflichten dementsprechend, wenn keine Maßnahmen zum Schutz gefährdeter Grundrechtspositionen getroffen werden oder die getroffenen Maßnahmen völlig unzureichend sind.[5] Durch diese staatlichen Schutzpflichten wird verhindert, dass der Grundrechtsschutz im zivilrechtlichen Bereich ausgehöhlt wird. Vielmehr ist auch im privatrechtlichen Bereich die objektive Werteordnung der Grundrechte sicherzustellen.[6]

Neben den nationalen Grundrechten spielt auch die Unionsgrundrechtecharta eine Rolle. Diese Arbeit befasst sich mit verschiedenen Rechtsgebieten, die stark durch das Unionsrecht geprägt sind. Die Grundrechtecharta findet ihre Anwendung gemäß Art. 51 Abs. 1 GRC in sämtlichen Bereichen, in denen das Recht der europäischen Union durchgeführt wird. Im nationalen Privatrecht sind die Unionsgrundrechte deshalb vor allem bei der Umsetzung von Richtlinien durch den deutschen Gesetzgeber von Bedeutung. Dazu zählt etwa die Umsetzung der Enforcement-Richtlinie im Bereich des geistigen Eigentums, Art. 17 DSM-Richtlinie im Hinblick auf die urheberrechtliche Haftung von Diensteanbietern für das Teilen von Online-Inhalten oder der Umsetzung der e-privacy-Richtlinie hinsichtlich des Datenschutzrechts im Telekommunikationsbereich. Der nationale Gesetzgeber ist bei der Umsetzung der Richtlinien zur grundrechtskonformen Gestaltung des Zivilrechts und die Gerichte zur grundrechtskonformen Auslegung verpflichtet. Dazu gehört auch der Ausgleich widerstreitender Interessen bei privatrechtlichen Streitigkeiten.[7] Besondere Relevanz weisen die Unionsgrundrechte außerdem bei den unmittelbar im nationalen Recht anwendbaren Vorschriften der europäischen Union wie der DSGVO oder dem DSA auf.

Das Verhältnis der Grundrechte des Grundgesetztes zu denen der Grundrechtecharta wird durch das *BVerfG* im Rahmen seiner Rechtsprechung zu

---

[5] *BVerfG*, Urt. v. 28.05.1993 - 2 BvF 2/90, 2 BvF 4/92, 2 BvF 5/92, NJW 1993, 1751, 1756; *Canaris*, Grundrechte und Privatrecht, S. 83 ff.

[6] Vgl. *Herdegen* in: Maunz/Dürig, Art. 1 Abs. 3 GG Rn. 17 ff.

[7] Vgl. *BVerfG*, Beschl. v. 06.11.2019 – 1 BvR 276/17, NJW 2020, 300 – Recht auf Vergessen II.

„Recht auf Vergessen I“ und „Recht auf Vergessen II“ näher bestimmt.[8] Demnach sind die Unionsgrundrechte bei unionsrechtlich vollständig vereinheitlichten Regelungen vorrangig anzuwenden. Bei nationalem Recht, das nicht vollständig unionsrechtlich determiniert ist, prüft das *BVerfG* primär am Maßstab der Grundrechte des Grundgesetzes.

B. Interessen der Rechteinhaber

Die Interessen der Rechteinhaber bestehen vordergründig in einem möglichst umfassenden Schutz ihrer Rechtsgüter. Diese Rechtsgüter, die durch die Verletzung durch Private berührt werden, sind im Grundgesetz bzw. in der Grundrechtecharta der europäischen Union verankert. Daraus resultiert ein Interesse an einem möglichst umfassenden Schutz und einer effektiven Rechtsdurchsetzung.

I. Verankerung der betroffenen Rechtsgüter

Die Rechtsgüter, die von den oben beschriebenen Verletzungen absolut geschützter Rechte im Internet betroffen sein können, sind in den Grundrechten des Grundgesetzes und der Grundrechtecharta der europäischen Union verankert. Die nachstehenden Ausführungen beschränken sich auf die am häufigsten von Rechtsverletzungen im Internet betroffenen Rechtsgüter: Persönlichkeitsrechte, Geistiges Eigentum und das Recht am eingerichteten und ausgeübten Gewerbebetrieb.

1. Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG

Besonders verfassungsrechtlich geprägt ist vor allem der zivilrechtliche Persönlichkeitsschutz. Der Begriff des allgemeinen Persönlichkeitsrechts wurde ursprünglich von den Zivilgerichten entwickelt und wurde neben besonderen Persönlichkeitsrechten – beispielsweise aus § 12 BGB und § 22 KUG - anerkannt und als absolut geschütztes Recht unter den Schutz der §§ 823 Abs. 1, 1004 BGB

[8] S. *BVerfG*, Beschl. v. 06.11.2019 – 1 BvR 16/13, NJW 2020, 300, 300 ff. – Recht auf Vergessen I; *BVerfG*, Beschl. v. 06.11.2019 – 1 BvR 276/17, NJW 2020, 314, 314 ff. – Recht auf Vergessen II.

gestellt.[9] Dieser Begriff wurde zwar im Verfassungsrecht übernommen, weist aber dennoch Unterschiede auf und muss sich an die strukturellen Eigenschaften des Verfassungsrechts anpassen.[10]

In Anlehnung an die zivilrechtliche Rechtsprechung des *BGH*[11] leitet das *BVerfG* das Allgemeine Persönlichkeitsrecht aus der allgemeinen Handlungsfreiheit aus Art. 2 Abs. 1 GG in Verbindung mit der Menschenwürdegarantie des Art. 1 Abs. 1 GG ab.[12] Der persönliche Schutzbereich erfasst jedenfalls alle natürlichen Personen. Da das Grundrecht an die personale Identität natürlicher Personen anknüpft, ist das allgemeine Persönlichkeitsrecht gemäß Art. 19 Abs. 3 GG dem Wesen nach nur schwer auf juristische Personen übertragbar.[13] Das *BVerfG* hat diese Frage bisher nicht abschließend beantwortet und die Anwendbarkeit anhand des konkreten Einzelfalls beurteilt.[14]

Das Grundrecht schützt in sachlicher Hinsicht verschiedene Aspekte der Persönlichkeit, die nicht durch andere Grundrechte erfasst werden, aber ebenfalls von herausragender Bedeutung für die Persönlichkeit sind.[15] Der entwicklungsoffene und weite Schutzbereich wird durch von der Rechtsprechung gebildete vielfältige Fallgruppen konturiert.[16] Dazu gehören etwa das Recht auf Selbstdarstellung, der Schutz der Ehre, das Recht am eigenen Namen, das Recht am eigenen Wort und am eigenen Bild, der Schutz der sozialen Identität und das Recht auf informationelle Selbstbestimmung.[17]

---

[9] *BGH,* Urt. v. 25.5.1954 - I ZR 211/53, NJW 1954, 1404, 1405; *BGH*, Urt. v. 14.2.1958 - I ZR 151/56, NJW 1958, 827, 827.

[10] *Lang* in: BeckOK GG, Art. 2 GG Rn. 33.

[11] *BGH,* Urt. v. 25.5.1954 - I ZR 211/53, NJW 1954, 1404, 1404.

[12] *BVerfG*, Urt. v. 5.6.1973 - 1 BvR 536/72, NJW 1973, 1266, 1266 – Lebach-Fall.

[13] *Stern*, Staatsrecht, Band III/1, 1127.

[14] So wurde eine Anwendbarkeit bei verschiedenen Aspekten des Persönlichkeitsschutzes abgelehnt, S. etwa *BVerfG*, Beschl. v. 26.2.1997 - 1 BvR 2172/96, NJW 1997, 1841, 1843. Dagegen wurde das „Recht am gesprochenen Wort" auch juristischen Personen zuerkannt *BVerfG*, Beschl. v. 9.10.2002 - 1 BvR 1611/96, NJW 2002, 3619, 3619.

[15] *BVerfG*, Urt. v. 27.2.2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 Rn. 168 – Online-Durchsuchung.

[16] Vgl. *BVerfG*, Beschl. v. 13.6.2007 - 1 BvR 1783/05, NJW 2008, 39 Rn. 71.

[17] Vgl. zu den verschiedenen Fallgruppen etwa *Di Fabio* in: Maunz/Dürig, Art. 2 GG Rn. 166 ff. Vgl. auch *Rixen* in: Sachs, Art. 2 GG Rn. 121 ff.

Zur Strukturierung des Schutzbereichs wird zudem teilweise auf die sogenannte Sphärentheorie zurückgegriffen.[18] Dabei wird unterschieden zwischen der Intimsphäre als Kernbereich der privaten Lebensgestaltung, der Privatsphäre und der Teilnahme am öffentlichen Leben im Rahmen der Sozialsphäre.[19] Diese Kategorisierung kann auch Anhaltspunkte für die Beurteilung der Schwere eines Eingriffs in das allgemeine Persönlichkeitsrecht bieten. Während sich Eingriffe in die Sozialsphäre leichter rechtfertigen lassen, ist die Intimsphäre eines Menschen wegen der Nähe zur Menschenwürde besonders stark geschützt. Nicht zu rechtfertigen sind Eingriffe in den Kernbereich der Menschenwürde.[20]

Sowohl zivilrechtliche Rechtsverletzungen besonderer Persönlichkeitsrechte – wie das Recht am eigenen Namen oder am eigenen Bild – , als auch des allgemeinen Persönlichkeitsrechts (im Sinne der BGH-Rechtsprechung zu § 823 Abs. 1 BGB) tangieren das Grundrecht des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG. Die Beurteilung einer (vermeintlichen) Rechtsverletzung beispielsweise im Sinne des § 823 Abs. 1 BGB erfordert häufig eine Abwägung mit anderen verfassungsrechtlich geschützten Interessen – wie etwa der Meinungs- oder Pressefreiheit. Bei einer Verletzung des § 22 KUG wird der Interessensausgleich über die Vorschrift des § 23 KUG vorgenommen. Im Rahmen des § 823 Abs. 1 BGB erfolgt eine umfassende Prüfung des Interessensausgleichs bei der Prüfung der Rechtswidrigkeit.

Die verfassungsrechtlichen Differenzierungen sind auch für die zivilrechtlichen Abwägungsentscheidungen maßgeblich. So sind Eingriffe in den intimen Bereichen der Persönlichkeit nur sehr schwer zu rechtfertigen, während in der Sozialsphäre der Persönlichkeitsschutz gegenüber gegenläufigen öffentlichen Interessen häufiger zurücktritt.

---

[18] BVerfG, Beschl. v. 16.7.1969 - 1 BvL 19/63, NJW 1969, 1707, 1707 f. – Mikrozensus.

[19] *BVerfG*, Beschl. v. 3.6.1980 - 1 BvR 185/77, NJW 1980, 2070, 2070; *BVerfG*, Beschl. v. 11.10.1978 - 1 BvR 16/72, NJW 1979, 595, 595; *BVerfG*, Beschl. v. 19.7.1972 - 2 BvL 7/71, NJW 1972, 2214, 2214; *BVerfG*, Beschl. v. 15.1.1970 - 1 BvR 13/68, NJW 1970, 555, 555; *BVerfG*, Beschl. v. 16.7.1969 - 1 BvL 19/63, NJW 1969, 1707, 1707 - Mikrozensus.

[20] *BVerfG*, Urt. v. 3.3.2004 - 1 BvR 2378/98 u. 1 BvR 1084/99, NJW 2004, 999, 1002 – Großer Lauschangriff; *BVerfG*, Beschl. v. 31.1.1973 - 2 BvR 454/71, NJW 1973, 891, 891.

2. Recht am eingerichteten und ausgeübten Gewerbebetrieb

Im Zivilrecht wird das Recht am eingerichteten und ausgeübtem Gewerbebetrieb als richterrechtlich ausgestaltetes sonstiges Recht im Sinne des § 823 Abs. 1 BGB angesehen.[21] Der Umfang des verfassungsrechtlichen Schutzes des Gewerbebetriebs ist aber umstritten.[22] So hat das *BVerfG* bislang nicht abschließend bewertet, ob der eingerichtete und ausgeübte Gewerbebetrieb die Anforderungen des Eigentumsbegriffs des Art. 14 GG nach verfassungsrechtlichem Verständnis erfüllt.[23] Jedenfalls werden Unternehmen aber als tatsächliche Zusammenfassung der zu ihrem Vermögen gehörenden Sachen und Rechte durch Art. 14 GG geschützt.[24]

Der Schutzgegenstand des Eigentums ist nämlich stark normativ geprägt. Der zivil-rechtliche Eigentumsbegriff des § 903 BGB dient als Leitbild und prägt den verfassungsrechtlichen Begriff. Nach bürgerlich-rechtlichem Verständnis besteht das Wesen des Eigentumsrechts in der Zuordnung von Gütern zu einer natürlichen oder juristischen Person, wodurch diesen zum privaten Nutzen umfassende Herrschafts- und Verfügungsbefugnisse zugewiesen werden.

Die Eigentumsgarantie des Art. 14 GG geht über das Sacheigentum hinaus, orientiert sich aber am Eigentumsverständnis des § 903 BGB. Demnach wer-den von Art. 14 GG alle vermögenswerten Rechte erfasst, „die dem Berechtigten von der Rechtsordnung in der Weise zugeordnet sind, dass dieser die damit verbundenen Befugnisse nach eigenverantwortlicher Entscheidung zu seinem privaten Nutzen ausüben darf." In persönlicher Hinsicht erstreckt sich der Schutzbereich auf natürliche Personen und nach Art. 19 Abs. 3 GG auch auf inländische juristische Personen sowie nichtrechtsfähige Personenvereinigungen.

---

[21] S. oben unter Kap. 2 § 3 B. III.

[22] S. etwa *Axer* in: BeckOK GG, Art. 14 GG Rn. 51 m.w.N.

[23] *BVerfG,* Urt. v. 6.12.2016 – 1 BvR 2821/11, NJW 2017, 217 Rn. 228 ff.; *BVerfG,* Beschl. v. 8.9.2010 - 1 BvR 1890/08, NJW 2010, 3501 Rn. 20 ff.; *BVerfG*, Beschl. v. 10.6.2009 - 1 BvR 198/08, NVwZ 2009, 1426, 1428; *BVerfG,* Beschl. v. 26.6.2002 - 1 BvR 558/91 u. a., NJW 2002, 2621, 2625 - Glykolwarnung; *BVerfG*, Beschl. v. 29.07.1991 - 1 BvR 868/90, NJW 1992, 36, 37 m.w.N.

[24] Vgl. *BVerfG*, Beschl. v. 29.07.1991 - 1 BvR 868/90, NJW 1992, 36, 37 m.w.N.

Das weite Verständnis vom verfassungsrechtlichen Eigentumsbegriff ist ein Argument dafür, den Gewerbebetrieb – entsprechend der durch § 823 Abs. 1 BGB geschützten Rechtsposition – darüber hinaus als Gesamtheit und wirtschaftliche Einheit anzusehen und als solche unter den Schutz des Art. 14 GG zu stellen.[25] Dadurch wird der verfassungsrechtlichen Schutz auf alles ausgeweitet, „was in seiner Gesamtheit den wirtschaftlichen Wert des konkreten Betriebes ausmacht".[26] Auch freiberuflich tätige Personen – wie etwa Ärzte oder Rechtsanwälte – können sich auf das Recht am eingerichteten und ausgeübtem Gewerbebetrieb berufen.[27]

Diese verfassungsrechtlich geschützte Rechtsposition kann beispielsweise von geschäftsschädigenden Bewertungen oder Äußerungen im Internet tangiert werden. Häufig ergeben sich dabei auch Überschneidungen mit dem Schutzbereich der Berufsfreiheit aus Art. 12 GG, in dem das Recht auf Außendarstellung eines Unternehmens verfassungsrechtlich verankert ist.[28] Die Berufsfreiheit schützt dabei den Erwerb beziehungsweise die berufliche Betätigung, die Eigentumsfreiheit das Erworbene und die Innehabung bestimmter Vermögensgüter.[29]

Bei Rechtsverletzungen des eingerichteten und ausgeübten Gewerbebetriebes durch Private haben Art. 14 Abs. 1 GG bzw. Art. 12 Abs. 1 GG Auswirkungen auf zivilrechtliche Sachverhalte über Schadensersatz- und Unterlassungsansprüche, die sich aus der Stellung als sonstiges Recht im Sinne von § 823 Abs. 1 BGB ergeben können. Ob eine rechtsverletzende Handlung vorliegt, hängt von der

---

[25] *Axer* in: BeckOK GG, Art. 14 GG Rn. 52; *Jarass* in: Jarass/Pieroth, GG, Art. 14 Rn. 9; *Leisner* in: Isensee/Kirchhoff VIII, § 173 Rn. 26; *Papier/Shirvani* in: Maunz/Dürig, Art. 14 GG Rn. 200; *Wendt* in: Sachs, Art. 14 GG Rn. 26.

[26] S. etwa *BGH*, Urt. v. 28.1.1957 - III ZR 141/55, NJW 1957, 630, 631; *BGH*, Urt. v. 31.1.1966 - III ZR 110/64, NJW 1966, 1120, 1120.

[27] *BGH,* Beschl. v. 03.03.1986 - AnwZ (B) 1/86*,* NJW 1986, 2499, 2500.

[28] *BVerfG*, Beschl. v. 26.6.2002 - 1 BvR 558/91 u. a., NJW 2002, 2621, 2622 – Glykolwarnung; *BVerfG*, Beschl. v. 29.10.2002 - 1 BvR 525/99, NJW 2003, 879, 879 – Facharztbezeichnung; *BVerfG*, Beschl. v. 8.3.2005 - 1 BvR 2561/03, NJW 2005, 1483, 1483 – Anwaltsnotare m.w.N. Zur Überschneidung von Art. 12 GG und Art. 14 GG s. *Papier/Shivani* in: Maunz/Dürig, Art. 14 GG Rn. 27.

[29] *BVerfG, Beschl. v. 8.6.2010 - 1 BvR 2011, 2959/07,* NVwZ 2010, 1212, 1214; *BVerfG*, Beschl. v. 16.3.1971 - 1 BvR 52, 665, NJW 1971, 1255, 1260.

Abwägung mit anderen verfassungsrechtlich ebenfalls geschützten Rechtsgütern des vermeintlichen Rechtsverletzers – wie zum Beispiel der Meinungsfreiheit aus Art. 5 Abs. 1 GG – ab.

3. Geistiges Eigentum

Die Rechte des geistigen Eigentums werden durch eine schöpferische Leistung begründet und ihren Schöpfern durch einfach-gesetzliche Regelungen Verfügungs- und Verwertungsrechte zugeordnet.[30] Auch solche Immaterialgüterrechte erfüllen daher die verfassungsrechtlichen Anforderungen des Eigentumsbegriffs aus Art. 14 GG und werden vom Schutzumfang des Art. 14 GG erfasst. Auch hier zeigt sich wieder die starke normative Prägung der Eigentumsgarantie aus Art. 14 GG. Deren Schutzbereich bezieht sich nämlich auf eine vermögenswerte Position der Rechteinhaber, die ihnen erst durch den Gesetzgeber zugewiesen wird.

Der Eigentumsschutz erstreckt sich damit auch auf die vermögensrechtlichen Aspekte des Urheberrechts, dessen Wesen gerade in der „Zuordnung des vermögenswerten Ergebnisses der schöpferischen Leistung an den Urheber" besteht.[31] Dies gilt auch für die mit dem Urheberrecht verwandten Schutzrechte wie jenes des Tonträgerherstellers nach § 85 Abs. 1 S. 1 UrhG.[32]

Eine vergleichbare Zuordnung besteht beim Patent-, Sortenschutz- und Designrecht.[33] Auch die Ausschlussfunktion des Markenrechts führt zu einem subjektiven Recht, das durch die Eigentumsgarantie des Art. 14 GG geschützt wird.[34]

Das Urheberpersönlichkeitsrecht dagegen hat weniger einen vermögensrelevanten als vielmehr einen ideellen Charakter und knüpft an die Persönlichkeit des Urhebers an. Dies spricht dafür, das Urheberpersönlichkeitsrecht nicht am

---

[30] Vgl. *Papier/Shivani* in: Maunz/Dürig, Art. 14 GG Rn. 314.

[31] *BVerfG,* Beschl. v. 7.7.1971 - 1 BvR 765/66, NJW 1971, 2163, 2163.

[32] BVerfG, Urt. v. 31.5.2016 – 1 BvR 1585/13, NJW 2016, 2247, 2248; BVerfG, Beschl. v. 03.10.1989 - 1 BvR 775/86, NJW 1990, 896, 896.

[33] S. dazu *Papier/Shivani* in: Maunz/Dürig, Art. 14 GG Rn. 318 ff. m.w.N.

[34] *BVerfG,* Beschl. v. 22.5.1979 - 1 BvL 9/75, NJW 1980, 383, 385; S. auch *Papier/Shivani* in: Maunz/Dürig, Art. 14 GG Rn. 320.

Schutz des Art. 14 GG zu messen, sondern dem Schutz des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG zu unterstellen.

Aufgrund des großen Einflusses des Unionsrechts im Bereich des geistigen Eigentums – etwa durch die Vorgaben der Enforcement-Richtlinie, spielt auch die Grundrechtecharta eine wichtige Rolle. Gemäß Art. 17 Abs. 2 GRC fällt das geistige Eigentum ausdrücklich unter den Eigentumsschutz des Art. 17 GRC.

Der Gesetzgeber und die Gerichte müssen daher den Schutz des geistigen Eigentums als Ausprägung der Eigentumsfreiheit beachten. Dies gilt auch im Hinblick auf Verletzungen von Immaterialgüterrechten durch Private. Wird beispielsweise urheberrechtlich geschütztes Material im Internet verbreitet, wird das Eigentumsrecht des Urhebers berührt. Bei derartigen Beeinträchtigungen von Immaterialgüterrechten durch Internetnutzer ist häufig eine Abwägung mit anderen verfassungsrechtlich geschützten Rechtsgütern – zum Beispiel mit der Kunst- oder Meinungsfreiheit – erforderlich. Dabei ist zu berücksichtigen, dass gem. Art. 17 Abs. 1 S. 3 GRC die Nutzung des Eigentumsrecht zum Zwecke des Wohles der Allgemeinheit geregelt werden kann. Gem. Art. 14 Abs. 2 GG gilt der Grundsatz der Sozialbindung des Eigentums. Das Eigentum soll folglich auch dem Wohl der Allgemeinheit dienen, sodass mit einer Eigentümerstellung auch Verpflichtungen einhergehen können. Die Rechte der Eigentümer können daher durch Gemeinwohlinteressen begrenzt werden, solange diese Einschränkung verhältnismäßig ist.[35]

Dies ist bei Internetsachverhalten vor allem im Bereich des Urheberrechts von Bedeutung. Der individuelle urheberrechtliche Schutz ist zugunsten des Gemeinwohls zu begrenzen. Zum Ausdruck kommen schutzwürdige Gemeinwohlinteressen derzeit insbesondere durch die Schrankenregelungen der §§ 44a ff. UrhG.[36] Die Sozialpflichtigkeit des Eigentums wird überdies bei Diskussionen um die freie Verfügbarkeit urheberrechtlich geschützter Werke im Internet aufgegriffen.[37] Je stärker aber der Eingriff in das Urheberrecht wiegt, desto gewichtiger müssen die Interessen des Gemeinwohls sein. Eine bloße

---

[35] Vgl. *BVerfG*, Urt. v. 1.3.1979 - 1 BvR 532 u.a., NJW 1979, 699, 703.

[36] *Stieper* in: Schricker/Loewenheim, Vor §§ 44a ff. Rn. 15.

[37] S. dazu etwa *Milkovic,* Das digitale Zeitalter, S. 152 ff.

Beschränkung des Verbotsrechts beeinträchtigt die Position des Urhebers weniger stark, als wenn die betreffende Nutzung auch ohne Vergütung ermöglicht wird.[38]

Für die oben beschriebenen zivilrechtlichen Verletzungen des Rechts auf Leben und körperlicher Unversehrtheit im Internet dient vor allem § 823 Abs. 1 BGB der Erfüllung der staatlichen Schutzpflicht.

II. Effektive Rechtsdurchsetzung

Das Interesse der Rechteinhaber am Schutz ihrer verfassungsrechtlich geschützten Rechtsgüter umfasst auch den Wunsch nach einer möglichst effektiven Rechtsdurchsetzung gegen private Eingriffe. Auf die Rechtsschutzgarantie des Art. 19 Abs. 4 GG können sich die Rechteinhaber diesbezüglich aber nicht stützen, da diese nur bei Rechtsverletzungen durch die öffentliche Gewalt greift.[39]

Im Anwendungsbereich der Grundrechtecharta der europäischen Union ergibt sich das Gebot des effektiven Rechtsschutzes für unionsrechtlich garantierte subjektive Rechte unmittelbar aus Art. 47 GRC. Art. 47 GRC kann bereits beeinträchtigt sein, wenn der zur Verfügung stehende Rechtsbehelf, den Schutz des fraglichen Rechts nicht ausreichend gewährleistet.

Im Übrigen lässt sich ein schutzwürdiges Interesse an einer möglichst effektiven Rechtsdurchsetzung bei Eingriffen durch Privatpersonen sowohl aus dem staatlichen Schutzauftrag hinsichtlich der beeinträchtigten Grundrechte als auch aus dem Rechtsstaatsprinzip ableiten.

Die staatliche Verpflichtung zum Schutz der Grundrechte der Rechteinhaber bewirkt, dass der Staat wenigstens ein Mindestmaß an Schutz auch vor Eingriffen privater Dritter gewährleisten muss. Der Gesetzgeber erfüllt seinen Schutzauftrag - neben strafrechtlichen Vorschriften - auch durch zivilrechtliche

---

[38] Vgl. *Stieper* in: Schricker/Loewenheim, Vor §§ 44a ff. Rn. 15 m.w.N.

[39] S. zum Verhältnis des Art. 19 Abs. 4 GG zum aus dem Rechtsstaatsprinzip abgeleiteten allgemeinen Justizgewährungsanspruchs etwa *Schmidt-Aßmann* in: Maunz/Dürig, Art. 19 Abs. 4 GG Rn. 16 f. m.w.N.

Unterlassungs- und Schadensersatzansprüche. Die Möglichkeit, diese zivilrechtlichen Ansprüche in der Praxis auch tatsächlich durchsetzen zu können, wird zumindest dann vom Gewährleistungsgehalt der Grundrechte erfasst, wenn andernfalls die Rechteinhaber ihrer verfassungsrechtlichen Positionen weitgehend beraubt wären.[40] In diesem Fall bestünde eine Verpflichtung des Gesetzgebers, die Durchsetzbarkeit der Ansprüche sicherzustellen.

Noch weiter geht der Schutz durch den allgemeinen Justizgewährungsanspruch, der aus dem Rechtsstaatsprinzip abgeleitet wird.[41] Der Rechtsstaat ordnet das Gewaltmonopol dem Staat zu und nimmt dem Bürger das Recht, seine (vermeintlichen) Ansprüche selbst durchzusetzen.[42] Daher ist der Staat verpflichtet, eine staatlich geordnete und wirksame Rechtsdurchsetzung zu ermöglichen.[43] Der Inhaber eines Anspruchs muss die notwendigen Instrumente erhalten, um seine Rechte Privatpersonen gegenüber geltend machen und einer gerichtlichen Überprüfung zuführen zu können.

Gerade im Internet sind die verfassungsrechtlichen Positionen der Rechteinhaber nicht unerheblichen Gefahren nichtstaatlicher Eingriffe ausgesetzt. Hinzu kommt häufig die Anonymität der Internetnutzer, wodurch die Rechtsdurchsetzung erheblich erschwert bis unmöglich werden kann. Die Ansprüche, die den verfassungsrechtlichen Interessen der Rechteinhaber Ausdruck verleihen, könnten ins Leere laufen.

Daher ließe sich jedenfalls erwägen, aus den Grundrechten der Rechteinhaber eine Verpflichtung des Gesetzgebers abzuleiten, die Rechtsdurchsetzung der Rechteinhaber - zum Beispiel durch die Einführung von Auskunftsansprüchen - zur Identifizierung rechtsverletzender Internetnutzer zu erleichtern.[44]

---

[40] Vgl. *Schmidt-Aßmann* in: Maunz/Dürig, Art. 19 Abs. 4 GG Rn. 16; S. im Hinblick auf Urheberrechtsverletzungen *Nietsch*, Anonymität und Durchsetzung, S. 116.

[41] Zur Ableitung des allgemeinen Justizgewährungsanspruchs s. etwa *Schmidt-Aßmann* in: Maunz/Dürig, Art. 19 Abs. 4 GG Rn. 16 m.w.N.

[42] *BVerfG*, Beschl. v. 13.03.1990 - 2 BvR 94/88 u. a., NJW 1991, 413, 413; *BVerfG*, Urt. v. 11.6.1980 - 1 PBvU 1/79, NJW 1981, 39, 41; *Sachs* in: Sachs Grundgesetz, Art. 20 Rn. 162.

[43] *BVerfG*, Beschl. v. 13.03.1990 - 2 BvR 94/88 u. a., NJW 1991, 413, 413; *BVerfG*, Urt. v. 11.6.1980 - 1 PBvU 1/79, NJW 1981, 39, 41; *Schmidt-Aßmann* in: Maunz/Dürig, Art. 19 Abs. 4 GG Rn. 17 m.W.N.

[44] Vgl. *Nietsch*, Anonymität und Durchsetzung, S. 117.

Ohne die Identifizierung des Anspruchsgegners scheitert die gerichtliche Anspruchsdurchsetzung gegen anonyme Rechtsverletzer im Internet. Damit der Weg zu den Gerichten in diesen Fällen tatsächlich offensteht, bedarf es bereits im Vorfeld des gerichtlichen Verfahrens Identifizierungsmöglichkeiten für die Rechteinhaber.[45] Der Gesetzgeber ist daher grundsätzlich dazu verpflichtet, den Rechteinhabern die entsprechenden Werkzeuge – beispielsweise durch die Schaffung von Auskunftsansprüchen - an die Hand zu geben.

Allerdings bedeutet dies nicht, dass der Rechtsdurchsetzung im Internet keine Grenzen gesetzt sein können. Schon auf Grund der vielen technischen Möglichkeiten zur Anonymisierung können und werden die Möglichkeiten der Rechtsdurchsetzung nie vollständig lückenlos sein. Vor allem müssen bei der Ausgestaltung von Rechtsdurchsetzungsmaßnahmen – wie der Schaffung von Auskunftsansprüchen - kollidierende Freiheitsrechte der Internetnutzer beachtet und mit dem Rechtsdurchsetzungsinteresse der Rechteinhaber abgewogen werden.[46] Die freie Nutzung von Internetdiensten und der Schutz von personenbezogenen Daten können die Rechtsdurchsetzungsmöglichkeiten begrenzen.

Dies ändert jedoch nichts daran, dass zumindest dem Grunde nach ein berechtigtes Interesse der Rechteinhaber an einer effektiven Rechtsdurchsetzung auch gegenüber Privaten besteht, das sich auf das Rechtsstaatsprinzip – ggf. in Verbindung mit den jeweils betroffenen Grundrechten – beziehungsweise auf Art. 47 GRC stützen lässt.

C. Interessen der Nutzer

Dem Interesse der Rechteinhaber an der Schadloshaltung ihrer Rechtsgüter und einer möglichst effektiven Rechtsdurchsetzung stehen die Interessen der Nutzer von Internetdiensten gegenüber. Vorrangig besteht vor allem der Wunsch auf Gewährleistung und Wahrung der Anonymität. Eng damit

---

[45] So auch *Nietsch,* Anonymität und Durchsetzung, S. 119.

[46] *BVerfG,* Beschl. v. 13.6.2006 - 1 BvR 1160/03, NJW 2006, 3701 Rn. 70: Der Gesetzgeber hat „grundrechtliche Schutzaussagen zu Gunsten des Rechtsuchenden, aber auch zu Gunsten Dritter, deren Belange durch den begehrten Rechtsschutz berührt werden, zu beachten und hierbei bereichsspezifischen Besonderheiten Rechnung zu tragen."

verbunden ist auch das Bedürfnis der Nutzer, Dienste zur Ausübung eigener Freiheitsrechte – zum Beispiel der Meinungs- oder Kunstfreiheit – möglichst ohne Beeinträchtigungen nutzen zu können.

I. Schutz der Anonymität der Internetnutzer

Zur Rechtsdurchsetzung der Rechteinhaber gegenüber den Nutzern von Internetdiensten ist deren Identifizierung und damit verbunden eine Aufhebung ihrer Anonymität notwendig. Dies erfordert in der Regel die Erhebung, Speicherung und Verarbeitung personenbezogener Daten der Nutzer. Dadurch werden jedoch grundrechtlich geschützte Rechte der Nutzer berührt.

Im Grundgesetz bewirken sowohl das Fernmeldegeheimnis, als auch verschiedene Ausprägungen des allgemeinen Persönlichkeitsrechts zumindest in einem gewissen Umfang einen Schutz vor der Zuordnung einer Handlung oder eines Sachverhalts zu Nutzern von Internetdiensten.[47]

Im Bereich des Datenschutzes sind wegen des starken Einflusses des Unionsrechts durch Datenschutzgrundverordnung und e-privacy-Richtlinie auch die Unionsgrundrechte von besonderer Bedeutung. Das Grundrecht auf Schutz personenbezogener Daten aus Art. 8 GRC sowie das das Recht auf Achtung des Privat- und Familienlebens wird auf der Ebene des Sekudärrechts vor allem durch die Datenschutzgrundverordnung und die e-privacy-Richtlinie konkretisiert.

Daher gilt es, den Umfang des Anonymitätsschutzes und die Folgen für die Rechtsdurchsetzung vor allem im Hinblick auf zivilrechtliche Auskunftsansprüche zur Identifizierung von Internetnutzern zu untersuchen.

1. Schutz von Verkehrsdaten

Besonderem grundrechtlichem Schutz unterfallen Verkehrsdaten. Dazu gehören auch die bei der Übertragung von Signalen im Internet anfallenden Telekommunikationsdaten. Diese werden sowohl durch Art. 8 GRC als auch durch das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG geschützt.

---

[47] S. auch *Brunst,* Anonymität im Internet, S. 280 f.

Die e-privacy-Richtlinie trifft diesbezüglich eine das Recht auf Schutz personenbezogener Daten aus Art. 8 GRC konkretisierende Sonderregel für den Bereich der Telekommunikation.[48] Insbesondere die während eines Telekommunikationsvorgangs anfallenden Verkehrsdaten werden durch die e-privacy-Richtlinie besonders geschützt.

Derartige Telekommunikationsdaten können zudem dem Schutz des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG unterfallen. Das Fernmeldegeheimnis schützt „die unkörperliche Vermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs".[49] Der Begriff der Telekommunikation ist dabei weit zu verstehen und erfasst auch neue Technologien der Fernmeldetechnik und damit grundsätzlich auch die Kommunikation bei der Nutzung von Internetdiensten.[50] Dadurch kommt dem Fernmeldegeheimnis im Hinblick auf die fortschreitende Digitalisierung eine große Relevanz zu.

Bezüglich der Identifizierung der Nutzer von Diensten der Informationsgesellschaft ist von Bedeutung, dass nicht nur der Inhalt der Kommunikation vom Schutzbereich erfasst wird, sondern auch deren näheren Umstände. Geschützt ist bereits die Tatsache, ob überhaupt eine Kommunikation stattgefunden hat.[51] Vor allem unterfallen auch Informationen über die Beteiligten und deren Anschlüsse, Nummern oder auch der Zeitpunkt des Kommunikationsvorgangs dem Schutzbereich des Art. 10 GG.[52] Die Aufhebung der Anonymität eines Teilnehmers der Kommunikation kann daher dessen Rechte aus Art. 10 GG berühren.

---

[48] S. etwa *EuGH,* Urt. v. 20.09.2022 - Az. C-793/19, NJW 2022, 3135, 3135 ff.

[49] *BVerfG*, Urt. v. 2.3.2010 - 1 BvR 256/08 u.a., NJW 2010, 833 Rn. 189 - Vorratsdatenspeicherung; *BVerfG*, Urt. v. 27.2.2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 Rn. 128– Online-Durchsuchung; *BVerfG*, Beschl. v. 9.10.2002 - 1 BvR 1611/96, NJW 2002, 3619, 3619.

[50] Ausdrücklich etwa *BVerfG*, Urt. v. 27.2.2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 Rn. 181 ff. – Online-Durchsuchung; *Kindt*, MMR 2009, 147, 150.

[51] *BVerfG*, Beschl. v. 27.5.2020 – 1 BvR 1873/13 u.a., NJW 2020, 2699 Rn. 98 – Bestandsdatenauskunft II.

[52] *BVerfG*, Beschl. v. 27.5.2020 – 1 BvR 1873/13 u.a., NJW 2020, 2699 Rn. 98 – Bestandsdatenauskunft II; *Bantlin*, JuS 2019, 669, 669 f.; *Hermes* in: Dreier/Schulze, Art. 10 GG Rn. 42; *Kugelmann*, NJW 2003, 1777, 1778; *Schoch*, JURA 2011, 194, 197.

Schwierigkeiten bereitet allerdings, dass der Schutzbereich des Fernmeldegeheimnisses auf Individualkommunikation beschränkt ist. Eine Kommunikation, die an die Allgemeinheit gerichtet ist, wird dagegen grundsätzlich nicht vom Schutzumfang erfasst.[53]

Die Unterscheidung zwischen individueller und an die Allgemeinheit gerichteter Kommunikation ist im Internet jedoch nicht immer trennscharf möglich.[54] Vor allem ergibt sich die Einstufung der Kommunikation nicht bereits durch die Wahl des Übertragungsmediums, da dasselbe Medium sowohl zur Individual-, als auch zur Massenkommunikation genutzt werden kann.[55] Auch aus der Art des Internetdienstes lässt sich häufig nicht zweifelsfrei ableiten, zu welcher Form der Kommunikation dieser genutzt wurde.[56]

Dennoch ist zu berücksichtigen, dass zur Beurteilung der Individualität der Kommunikation im Internet teilweise eine Auswertung deren Inhalts notwendig wäre, die dem Schutzzweck des Fernmeldegeheimnisses richtigerweise entgegenstehen würde.[57] Sofern dies der Fall ist, muss im Sinne eines möglichst umfassenden Schutzes der entsprechende Vorgang vom Schutzbereich des Fernmeldegeheimnis erfasst werden.[58] Dies gilt vor allem bei einer massenhaften undifferenzierten Erfassung von Kommunikationsdaten,[59] wie zum Beispiel bei

---

[53] *BVerfG*, Beschl. v. 24.1.2012 – 1 BvR 1299/05, NJW 2012, 1419 Rn. 111 - Vorratsdatenspeicherung; *Durner* in: Maunz/Dürig, Art. 10 GG Rn. 118; *Hermes* in: Dreier, Art. 10 GG Rn. 39; *Gusy*: in Mangoldt/Klein/Stark, Art. 10 GG, Rn. 62.

[54] Ausführlicher dazu *Brunst,* Anonymität im Internet, S. 266 f.; *Czychowski*, MMR 2004, 514, 518 f.; *Pirner*, ZUM 2010, 833, 840 jeweils m.w.N.

[55] *Brunst,* Anonymität im Internet, S. 266.

[56] So auch *Brunst,* Anonymität im Internet, S. 266, der als Beispiel auf einen Webbrowser verweist, der sowohl als Webfronted für E-Mail-Kommunikation, als auch für ein Webforum genutzt werden kann. S. auch *Sievers*, Schutz der Kommunikation, S. 129 f. A.A. *Czychowski,* MMR 2004, 514, 518 f., der von der Möglichkeit einer Differenzierung anhand der Portnummern ausgeht.

[57] *Brunst,* Anonymität im Internet, S. 267; *Germann*, Gefahrenabwehr und Strafverfolgung, S. 118; *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 85; *Sieber/Nolde*, Sperrverfügungen, S. 80.

[58] So auch *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 85.

[59] Vgl. *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 85.

der anlasslosen Speicherung dynamischer IP-Adressen im Rahmen der Vorratsdatenspeicherung.[60]

2. Schutz sonstiger personenbezogener Daten

Kommunikationsdaten, die nicht dem Schutzbereich des Fernmeldegeheimnisses oder der e-privacy-Richtlinie zuzuordnen sind, werden ebenfalls durch Art. 7, 8 GRC, sowie durch das Recht auf informationelle Selbstbestimmung erfasst.

Insgesamt führt die Tatsache, dass anders als im Offline-Alltag im Internet jede Handlung teilweise ungewollt oder unbewusst Spuren hinterlässt, zu einem gestärkten Bewusstsein für den Schutz personenbezogener Daten im Online-Bereich. Durch fortschreitende technische Entwicklungen können zudem immer mehr Daten massenhaft gespeichert und verarbeitet werden.[61]

Als Reaktion auf das besondere Gefährdungspotential für personenbezogene Daten durch modernere Datenverarbeitung hat das BVerfG bereits im Jahr 1983 das Recht auf Informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 1 Abs. 1 GG i.V.m. Art. 2 Abs. 1 GG abgeleitet, das heute noch umso aktueller ist.[62]

Im Bereich des Unionsrechts ergibt sich der Schutz personenbezogener Daten aus den Art. 7, 8 GRC, die durch die DSGVO konkretisiert werden. Als personenbezogene Daten geschützt sind dabei alle individualisierten oder individualisierbaren Informationen einer Person.[63]

---

[60] S. dazu *BVerfG*, Urt. v. 2.3.2010 - 1 BvR 256/08 u.a., NJW 2010, 833 Rn. 194 ff. – Vorratsdatenspeicherung; S. zum Eingriff in Art. 7, 8 GRC *EuGH,* Urt. v. 20.09.2022 - Az. C-793/19, NJW 2022, 3135, 3135 ff.; *EuGH*, Urt. v. 6.10.2020 – C-511/18 u.a., NJW 2021, 531, 531 ff. – La Quadrature du Net; S. auch *EuGH,* Urt. v. 21.12.2016 – C-203/15 u.a., NJW 2017, 717 – Tele2 Sverige.

[61] S. zu dieser Problematik *BVerfG*, Urt. v. 27.2.2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 Rn. 179 – Online-Durchsuchung; *Brunst,* Anonymität im Internet, S. 221 ff.

[62] *BVerfG*, Urt. v. 15.12.1983 - 1 BvR 209/83 u. a., NJW 1984, 419, 419 ff. - Volkszählungsurteil.

[63] Vgl. die Definition personenbezogener Daten in Art. 4 Nr. 1 DS-GVO.

Der zentrale Gewährleistungsgehalt dieser Grundrechte besteht in dem umfassenden Recht der Grundrechtsträger, selbst über die Preisgabe und Verwendung personenbezogener Daten bestimmen zu können.[64] Der weite Schutzbereich erstreckt sich auf sämtliche Formen der Datenverarbeitung – insbesondere auf die Erhebung, Speicherung, Verwendung und Weitergabe der Daten.[65]

Vor dem Hintergrund der massenhaften Speicherung und Verknüpfung personenbezogener Daten existieren auch keine „belanglosen" - und damit vermeintlich weniger schutzbedürftigen - persönlichen Daten.[66] Denn selbst Daten, die bei isolierter Betrachtung nur einen sehr geringen Aussagegehalt enthalten, können in Kombination weitreichende Rückschlüsse auf persönlichkeitsrelevante Tatsachen zulassen.[67]

Dem Grundrechtsträger soll es ermöglicht werden, seine Identität vor anderen zu bewahren. Er wird davor geschützt, dass seine personenbezogenen Daten ohne sein Einverständnis erhoben, gespeichert und verwendet werden. Gibt er personenbezogene Daten freiwillig weiter, kommt dies keinem Verzicht auf seine grundrechtlich geschützten Rechte gleich, sondern ist vielmehr ein Ausdruck seines Selbstbestimmungsrechts.[68] Auch Informationen, die durch den Grundrechtsträger selbst veröffentlicht wurden, werden daher vor einer Weiterverarbeitung geschützt, wenn beispielsweise durch das Zusammentragen mit anderen Daten ein neuer Aussagegehalt entstehen würde.[69]

---

[64] S. etwa *BVerfG*, Urt. v. 15.12.1983 - 1 BvR 209/83 u. a., NJW 1984, 419, 421 – Volkszählungsurteil. S. auch zu einer aktuellen Entscheidung *BVerfG*, Beschl. v. 6.11.2019 – 1 BvR 16/13, NJW 2020, 300, 307 – Recht auf Vergessen I; *BVerfG*, Beschl. v. 28.7.2016 – 1 BvR 335/14 u.a., NJW 2017, 466 Rn. 9.

[65] *BVerfG*, Urt. v. 15.12.1983 - 1 BvR 209/83 u. a., NJW 1984, 419, 422 – Volkszählungsurteil.

[66] *BVerfG*, Urt. v. 15.12.1983 - 1 BvR 209/83 u. a., NJW 1984, 419, 422 – Volkszählungsurteil.

[67] S. *Brunst,* Anonymität im Internet, S. 219 f.

[68] *Gersdorf* in: BeckOK Informations- und Medienrecht, Art. 2 GG Rn. 17.

[69] Hintergrund dieses Schutzes ist die Gefahr der Erstellung von Persönlichkeitsprofilen durch unbewusst und aus technischen Gründen anfallende Daten, S. dazu BVerfG, Beschl. v. 6.11.2019 – 1 BvR 16/13, NJW 2020, 300 Rn. 103 – Recht auf Vergessen I.

Dies spielt für die Anonymität im Internet, die gerade aus der fehlenden Zuordnung eines Sachverhalts zu einer Identität rührt, eine große Rolle.[70] Viele Internetnutzer geben eine Vielzahl an personenbezogenen Daten freiwillig an die Diensteanbieter preis. Hinzu kommen Daten, die bei der Internetnutzung aus technischen Gründen anfallen und häufig unbewusst übertragen werden. Die Verknüpfung und Kombination, sowie die Zuordnung solcher Daten zu bestimmten Verhaltensweisen oder Umständen führt zur Entstehung neuer persönlicher Daten und berührt das Recht auf informationelle Selbstbestimmung.

3. Konsequenzen für zivilrechtliche Auskunftsansprüche

Gerade im Internet besteht eine erhebliche Gefährdungslage für das Recht auf informationelle Selbstbestimmung durch private Unternehmen (Facebook, Google, etc.). Daher ist der Staat in der Pflicht, in angemessenem Umfang den Schutz des Rechts auf informationelle Selbstbestimmung auch Privaten gegenüber sicherzustellen. Der Schutz von personenbezogenen Daten der Nutzer durch die nationalen Grundrechte sowie durch die Art. 7, 8 GRC wirkt sich daher auch auf die Ausgestaltung von Auskunftsansprüchen und die Möglichkeiten der Identifizierung von Internetnutzern aus.

Sowohl die Erhebung und Speicherung personenbezogener Daten als auch deren Verwendung und Weitergabe zum Zwecke der Auskunftserteilung tangieren die Schutzbereiche verschiedener Grundrechte.

Eine wichtige Rolle spielt in diesem Zusammenhang vor allem der Schutz vor missbräuchlicher Anwendung von Auskunftsansprüchen zum Beispiel zur Ausforschung von Daten. Der Datenerhebung und Datenverarbeitung durch Private sind daher von staatlicher Seite Grenzen zu setzen. Zudem muss ein angemessener Ausgleich zwischen den Interessen der Rechteinhaber und der Internetnutzer hergestellt werden.

Zudem sind sowohl Art. 7, 8 GRC, als auch Art. 10 GG hinsichtlich der Verarbeitung von Verkehrsdaten von Bedeutung. Dies hat Auswirkungen für die Realisierung und Ausgestaltung zivilrechtlicher Auskunftsansprüche und damit

---

[70] So auch *Nietsch*, Anonymität und Durchsetzung, S. 39. Zum Begriff der Anonymität s. oben Kap. 2 § 1 A.

der Rechtsdurchsetzungsmöglichkeiten der Rechteinhaber. Ein besonderer Schutz ergibt sich, wenn Internetdienste zur individuellen Kommunikation genutzt werden oder wenn dies zweifelhaft ist und zur Klärung eine Auswertung des Kommunikationsinhalts notwendig wäre. Dabei wird vor allem die Möglichkeiten der Speicherung und die Weitergabe von Telekommunikationsdaten im Rahmen einer Auskunftserteilung an die Rechteinhaber beeinflusst.

Problematisch ist in diesem Zusammenhang vor allem die massenhafte und undifferenzierte Speicherung von Kommunikationsdaten, wie (dynamischer) IP-Adressen und Zugriffszeiten auf Internetdienste. Zudem wird die Erhebung und Speicherung von Telekommunikationsdaten zu staatlichen Zwecken – zum Beispiel zur Strafverfolgung – eingeschränkt. Dadurch verfügen die Dienstanbieter nur sehr eingeschränkt über Telekommunikationsdaten, die für eine Auskunftserteilung genutzt werden könnten.

Die Beschränkung der zulässigen Erfassung und Speicherung von Kommunikationsdaten beeinflusst dementsprechend auch die Möglichkeiten, Auskunft von den Diensteanbietern erhalten zu können. Zudem berührt die Weitergabe von Daten an die Rechteinhaber den Schutz der Verkehrsdaten, wenn die Auskunftserteilung nur unter Verwendung von Telekommunikationsdaten erfolgen kann. Daraus resultieren höhere Anforderungen an die Zulässigkeit der Auskunftserteilung – wie beispielsweise das Erfordernis einer richterlichen Anordnung.

Im zivilrechtlichen Auskunftsverfahren erfolgt der Zugriff auf die Kommunikationsdaten in der Regel durch private Anbieter von Telekommunikationsdiensten.[71] Der Gesetzgeber ist dennoch in der Pflicht, die Kommunikationsteilnehmer als Grundrechtsträger auch vor den damit verbundenen Eingriffen Privater in den Telekommunikationsvorgang zu schützen. Da die Telekommunikation im Internet weit überwiegend über private Diensteanbieter erfolgt, muss die Vertraulichkeit der Kommunikation und deren näherer Umstände auch vor Eingriffen Privater geschützt werden. Wäre der Schutz ausschließlich auf die Abwehr von staatlichen Eingriffen begrenzt, würden

[71] S. auch *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 87.

erhebliche Schutzlücken in diesem Bereich entstehen.[72] Dieser Schutzpflicht ist er zum Beispiel durch die Einführung der einfachgesetzlichen Regelungen der §§ 3, 9 TTDSG nachgekommen, wodurch auch private Diensteanbieter zur Wahrung des Fernmeldegeheimnisses verpflichtet werden.[73]

II. Freiheitsausübung der Nutzer

Sehr häufig werden die Internetdienste durch die Nutzer zur Ausübung wichtiger grundrechtlicher Freiheiten – wie der Meinungs-, Kunst-, Informations-, Wissenschafts- oder Pressefreiheit – genutzt. Dies wirkt sich auf die Abwägung bei der materiellen Rechtsverletzung und gegebenenfalls auch auf die Rechtsdurchsetzung durch die Rechteinhaber aus.

1. Relevanz der Freiheitsausübung für die Beurteilung der Rechtsverletzung

Bereits bei der Frage, ob das Verhalten eines Nutzers überhaupt eine Rechtsverletzung auf der Ebene der einfachen Gesetzte darstellt, spielt die Ausübung grundrechtlich geschützter Freiheiten durch die Nutzer häufig eine große Rolle. Diese Freiheiten kollidieren mit der Position der Rechteinhaber: Zum Beispiel kann eine Bewertung etwa eines Lehrers in einem Bewertungsportal das allgemeine Persönlichkeitsrecht des Rechteinhabers beeinträchtigen, aber auch Ausdruck der Meinungsfreiheit des bewertenden Nutzers sein. Der Gebrauch eines urheberrechtlich geschützten Materials kann das Eigentumsrecht des Urhebers beeinträchtigen, aber auch der Ausübung der Meinungs-, Informations- oder der Kunstfreiheit des Nutzers dienen.

Der Staat ist zum Schutz der grundrechtlichen Freiheitsrechte der Nutzer ebenso verpflichtet wie zum Schutz der verfassungsrechtlichen Rechte der Rechteinhaber. Die widerstreitenden Interessen sind bereits auf der Ebene des einfachen Rechts zu berücksichtigen und in einen angemessenen Ausgleich zu bringen: Bei Beeinträchtigungen des Persönlichkeitsrechts muss eine Abwägung mit der Meinungsfreiheit des sich Äußernden erfolgen.

---

[72] S. zur Schutzpflicht im Rahmen des Art. 10 GG im Hinblick auf die zunehmende Privatisierung von Telekommunikationsdiensten *BVerfG,* Beschl. v. 9.10.2002 - 1 BvR 1611/96, NJW 2002, 3619, 3619.

[73] Vgl. auch *Brunst,* Anonymität im Internet, S. 279.

2. Auswirkung auf die Rechtsdurchsetzung der Rechteinhaber

Die verfassungsrechtlich geschützten Freiheiten der Nutzer schlagen nicht nur auf der Ebene der Rechtsverletzung durch, sondern können sich auch auf die Rechtsdurchsetzung durch die Rechteinhaber auswirken.

Wenn die Diensteanbieter Maßnahmen gegen Rechtsverletzungen ergreifen beziehungsweise gegen rechtsverletzende Handlungen tätig werden, können Freiheitsrechte der Nutzer beeinträchtigt werden. Die Sperrung einer Internetseite oder das Löschen von möglicherweise rechtsverletzenden Inhalten berührt nicht nur die Meinungs-, Presse- oder Kunstfreiheit des handelnden Nutzers, sondern auch die Informationsfreiheit von Dritten, die als Internetnutzer an einer Informationsgewinnung gehindert werden.[74] Es besteht also ein allgemeines Informationsinteresse von Internetnutzern, das vor allem dann zu berücksichtigen ist, wenn der Zugang zu Informationen verhindert wird, deren rechtsverletzende Qualität unklar ist, oder wenn durch Sperrmaßnahmen auch legale Inhalte blockiert werden.

Sicherlich schützen die grundrechtlichen Freiheitsrechte die (möglicherweise rechtsverletzenden) Nutzer aber nicht davor, sich mit der Rechtsposition der Rechteinhaber juristisch auseinandersetzten und gegebenenfalls über die Auslegung von Gesetzten streiten zu müssen. Der Staat ist allerdings grundsätzlich in der Pflicht, die Ausübung grundrechtlicher Freiheiten der Nutzer im Internet auch vor Eingriffen Dritter zu schützen. Daher ist die Freiheitsausübung der Nutzer beispielsweise bei der Frage von Bedeutung, wer das Risiko der Rechtsdurchsetzung im Internet tragen sollte.

---

[74] *Askani,* Private Rechtsdurchsetzung, S. 199 f.; *Holznagel,* Notice and Take-Down-Verfahren, S. 232; *Thome,* Sperrverfügungen, S. 140 ff.; *Volkmann* in: Spindler/Schuster, § 59 RStV Rn. 18; *Hoffmann/Volkmann* in: Spindler/Schuster, § 7 TMG Rn. 57-60. S. auch zu Art. 11 EuGRCh *EuGH*, Urt. v. 26.04.2022 – C-401/19, NJW 2022, 1663, Rn. 45 ff. – Polen/Europäisches Parlament und Rat; *EuGH*, Urt. v. 27.3.2014 – C-314/12, GRUR 2014, 468, 468 f. – UPC Telekabel; *EuGH*, Urt. v. 24. 11. 2011 - C-70/10, GRUR 2012, 265, 268 –Scarlet/SABAM; *EuGH*, Urt. v. 16. 2. 2012 - C-360/10, GRUR 2012, 382, 384 – Netlog/ SABAM.

Dies lässt sich besonders gut am Beispiel der im Urheberrecht viel diskutierten Upload-Filter darstellen:[75] Der Einsatz von Upload-Filtern zum Schutz von Urheberrechten kann dazu führen, dass auch legale Inhalte entfernt werden, was zu einer Beeinträchtigung der Informations- und Meinungsfreiheit der Nutzer führen kann.[76] Es besteht die Gefahr, dass das Risiko der Rechtsdurchsetzung in diesem Fall auf die Nutzer verlagert wird, die aktiv gegen die Entfernung der Inhalte vorgehen müssen. Dadurch können sie in ihrer Freiheitsausübung stärker beeinträchtigt werden, als wenn die Rechteinhaber die Rechtsdurchsetzungslast träfe und diese die Entfernung der Inhalte erst erstreiten müssten. Dennoch können sog. Upload-Filter mit der Meinungs- und Informationsfreiheit der Nutzer vereinbar sein, wenn Maßnahmen getroffen werden, durch die die widerstreitenden Interessen in einen verhältnismäßigen Ausgleich gebracht werden.[77] Es erscheint dabei geboten, den Gefahren des Over-Blockings vorzubeugen und die Nachteile für die Nutzer durch die Umkehr der Aktionslast auszugleichen.[78]

Der Meinungsäußerungsfreiheit der Nutzer wird ein besonderer Stellenwert beigemessen, der sich auch auf die Rechtsdurchsetzung der Rechteinhaber auswirken kann. Die Anonymität im Internet kann wesentlich für die freie Meinungsäußerung sein, wenn mit der Offenlegung der Identität – zum Beispiel beim Whistleblowing – Repressalien verbunden wären.[79] Der *BGH* spricht auch davon, dass die Anonymität dem Internet „immanent" sei und anonyme Meinungsäußerungen denselben Schutz erfahren, wie Äußerungen unter

---

[75] Die Diskussion entbrennt auf Grund von Art. 17 Abs. 4 DSM-RL, der eine Verantwortlichkeit der Diensteanbieter vorsieht, falls diese nicht Vorkehrungen treffen, um das Hochladen künftiger rechtswidriger Inhalte zu verhindern.

[76] S. etwa *Raue/Steinebach*, ZUM 2020, 355, 357.

[77] So auch *EuGH*, Urt. v. 26.04.2022 – C-401/19, NJW 2022, 1663, Rn. 48 ff. – Polen/Europäisches Parlament und Rat; Vgl. auch *Raue/Steinebach*, ZUM 2020, 355, 364; *Schwartmann/Hentsch*, MMR 2020, 207, 207 ff.

[78] S. dazu auch *EuGH*, Urt. v. 26.04.2022 – C-401/19, NJW 2022, 1663, 48 ff. – Polen/Europäisches Parlament und Rat; *Schwartmann/Hentsch*, MMR 2020, 207, 207 ff.

[79] Vgl. *BGH*, Urt. v. 23.9.2014 – VI ZR 358/13, NJW 2015, 489, 493 – Ärztebewertungsprotal II; *BGH*, Urt. v. 23.6.2009 - VI ZR 196/08, NJW 2009, 2888 Rn. 38- Spickmich; *Härting*, NJW 2013, 2065, 2068; *Nietsch*, Anonymität, S. 47.

Namensnennung.[80] Anonyme Meinungsäußerungen sind also nicht per se weniger schutzwürdig.[81] Dennoch trifft es zu, dass die Gefährdung die durch anonyme Äußerungen zum Beispiel für Persönlichkeitsrechte anderer ausgeht, größer sein kann, als wenn die Identität eines Nutzers bekannt ist.[82]

Unabhängig davon, welche Schutzintensität man anonymen Meinungsäußerungen beimisst, ist mit Blick auf eine möglichst freie Meinungsäußerung, dem Äußernden das Recht zu gewähren, grundsätzlich selbst darüber zu entscheiden, ob er seine Meinung anonym kundgeben möchte.[83] Daraus ergibt sich auch eine staatliche Schutzpflicht, anonyme Meinungsäußerungen zu ermöglichen.[84] Im Ergebnis geht die Schutzwirkung im Zivilrecht aber nicht über den Gewährleistungsgehalt des Rechts auf informationelle Selbstbestimmung hinaus. Es bedarf aber eines Ausgleichs zwischen dem Rechtsdurchsetzungsinteresse der Rechteinhaber und dem Schutz der Anonymität der sich äußernden Nutzer.

D. Interessen der Diensteanbieter

Im Konflikt zwischen den Nutzern und den Rechteinhabern sind die Diensteanbieter zunächst einmal Dritte. Dennoch ist ihre Position keineswegs neutral. Durch die Bereitstellung ihres Dienstes schaffen sie eine Gefahrenquelle und tragen dadurch meist zumindest eine mittelbare Verantwortung für die Rechtsverletzung. Die Rechtsdurchsetzung im Internet ist zudem ohne Beteiligung der Diensteanbieter kaum möglich. Andernfalls lässt sich sehr häufig weder der Ursprung und Umfang der Rechtsverletzung noch die Identität des Rechtsverletzers ermitteln. Auch die Entfernung rechtsverletzender Inhalte oder Sperrung von Nutzerzugängen oder Internetseiten erfordert ein Tätigwerden der Diensteanbieter. Damit kommt ihnen eine zentrale Rolle bei der

---

[80] *BGH*, Urt. v. 23.6.2009 - VI ZR 196/08, NJW 2009, 2888 Rn. 38 – Spickmich. Vgl. auch *Kersten*, JuS 2017, 193, 196.

[81] *Ohly*, AfP 2011, 428, 436. A.A. aber *Berneuther,* AfP 2011, 218, 222 f.; *Greve/Schärdel,* MMR 2008, 644, 648; *Kühling,* NJW 2015, 447, 448; Wiese, JZ 2011, 608, 612 ff.

[82] S. etwa *Kühling*, NJW 2015, 447, 448; *Bernreuther*, AfP 2011, 218, 222 f.; *Greve/Schärdel*, MMR 2008, 644, 648.

[83] *Nietsch*, Anonymität und Durchsetzung, S. 48; *Kersten*, JuS 2017, 193, 196.

[84] *Kersten*, JuS 2017, 193, 196.

Rechtsdurchsetzung zu. Die grundrechtlich geschützten Interessen der Diensteanbieter können dabei allerdings im Widerspruch zu den Rechtsdurchsetzungsinteressen der Rechteinhaber stehen.

I. Unternehmerische Freiheit und Berufsfreiheit

Die Diensteanbieter können sich unter anderem auf ihre unternehmerische Freiheit aus Art. 16 GRC beziehungsweise auf das Recht auf freie Berufsausübung aus Art. 12 Abs. 1 GG berufen. Regelungen, die die Diensteanbieter verpflichten, Auskunft über Nutzer und deren Handlungen zu erteilen, Kontroll- und Überwachungsmaßnahmen durchzuführen oder in bestimmten Situationen gegen Rechtsverletzungen tätig zu werden, greifen in dieses Recht ein.[85]

Entsprechende Maßnahmen können außerdem mit hohen Kosten und großem Aufwand verbunden sein. Umfassende Prüf-, Kontroll-, und Überwachungspflichten haben einen erheblichen Mehraufwand zur Folge. Müssen die Diensteanbieter aktiv gegen Rechtsverletzungen vorgehen, können zudem Verluste entstehen, wenn sich die Beziehungen zu den Nutzern verschlechtern und die Nutzerzahlen sinken.[86] Ist von diesen Kosten auch bereits erworbenes Vermögen der Diensteanbieter betroffen, liegt gegebenenfalls auch eine Beeinträchtigung des Eigentumsrechts vor.[87] Jedenfalls darf der Gesetzgeber Diensteanbietern, deren Tätigkeiten von der Rechtsordnung gebilligt sind, keine Pflichten auferlegen, die ihr Geschäftsmodell wirtschaftlich gefährden und sie in ihrer Tätigkeit unverhältnismäßig stark einschränken.[88]

Die Diensteanbieter schaffen allerdings Gefahrenquellen für rechtswidrige Handlung im Zusammenhang mit der Nutzung ihrer Dienste. Daher erscheint es prinzipiell gerechtfertigt, die Diensteanbieter mit in die Verantwortung zu

---

[85] *Germann*, Gefahrenabwehr und Strafverfolgung, S. 405; S. in Bezug auf Art. 16 GRCh *EuGH*, Urt. v. 27.3.2014 – C-314/12, GRUR 2014, 468, 468 ff. – UPC Telekabel. S. auch *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 85.

[86] *Rohlfing*, Enforcement-Richtlinie, S. 167.

[87] *Volkmann* in: Spindler/Schuster, § 59 RStV Rn. 20.

[88] *Askani,* Private Rechtsdurchsetzung, S. 200. S. auch *EuGH,* Urt. v. 12.7.2011 - C-324/09, GRUR 2011, 1025, 1025 – L'Oréal/eBay; *EuGH,* Urt. v. 16. 2. 2012 - C-360/10, GRUR 2012, 382, 382 – Netlog/SABAM; *BGH,* Urt. v. 26.11.2015 – I ZR 174/14, GRUR 2016, 268 Rn. 26 f. – Störerhaftung des Access-Providers.

nehmen. Allerdings dürfen die Diensteanbieter nicht in unverhältnismäßiger Weise beeinträchtigt werden. Dafür können verschiedene Kriterien herangezogen werden:

Je weniger der Diensteanbieter für die Rechtsverletzung (mittelbar) verantwortlich ist, desto geringer ist der Aufwand, der ihm bei der Rechtsdurchsetzung zugemutet werden kann. Access-Provider vermitteln beispielsweise lediglich den Zugang zum Internet und erbringen damit eine gesellschaftlich gewünschte Dienstleistung. Der Bezug zur Rechtsverletzung ist bei der reinen Zugangsvermittlung deutlich geringer als zum Beispiel bei Host-Providern, die die rechtsverletzenden Inhalte speichern. Die Hürden für eine Inanspruchnahme sind daher bei Access-Providern grundsätzlich höher anzusetzen.[89]

Zudem greifen verschiedenen Maßnahmen in unterschiedlichem Maße in die Rechte der Diensteanbieter ein. Die bloße Auskunftserteilung in einem konkreten Fall nach einem richterlichen Beschluss ist wohl mit einem eher geringen Aufwand verbunden. Problematischer dürften dagegen umfassende Prüf- und Kontrollpflichten und insbesondere präventive Überwachungspflichten sein. Zumal solche Pflichten auch mit der Gefahr von Fehleinschätzungen bei der Beurteilung von Rechtsverletzungen einhergehen und die Diensteanbieter dadurch Unterlassungs- oder Schadensersatzansprüchen der Nutzer ausgesetzt werden könnten.

Dem Verhältnismäßigkeitsgrundsatz kann aber beispielsweise durch Ersatzansprüche der Diensteanbieter gegen die unmittelbaren Verletzer oder Entschädigungen genüge getan werden. Zudem können Regelungen für den Fall einer unabsichtlichen Fehlbeurteilung getroffen werden.

---

[89] Vgl. *BGH*, Urt. v. 26.11.2015 – I ZR 174/14, GRUR 2016, 268, Rn. 28 ff. – Störerhaftung des Access-Provider, der bei Sperrverfügungen gegen Access-Provider eine Abwägung unter Verhältnismäßigkeitsgesichtspunkten voraussetzt und eine subsidiäre Inanspruchnahme von Access-Providern vorsieht. S. auch *Volkmann* in: Spindler/Schuster, § 59 RStV Rn. 63 f.

II. Presse- und Rundfunkfreiheit

Die Diensteanbieter können sich darüber hinaus gegebenenfalls auch auf die Rundfunk- oder Pressefreiheit berufen.[90] Ob es sich bei Online-Diensten um Rundfunk oder Presse handelt, lässt sich nicht immer trennscharf beurteile.[91] Grundsätzlich wird nach der Art der Verbreitungsform unterschieden.[92] Während es sich bei der Presse um ein gegenständliches Medium handelt, handelt es sich beim Rundfunk um eine elektro-magnetische Verbreitungsform.[93] Allerdings können auch Inhalte auf Datenträgern, sowie die Online-Ausgaben von Tageszeitungen der Pressefreiheit zugeordnet werden, bei denen kein entsprechendes Trägermedium existiert.[94] Jedenfalls sind aber die Begriffe der Presse und des Rundfunks entwicklungsoffen, sodass grundsätzlich auch Online-Dienste darunterfallen können.[95]

Die Diensteanbieter können sich allerdings nur dann auf diese Kommunikationsfreiheiten berufen, wenn sie in irgendeiner Weise redaktionell tätig werden.[96] Zugangsanbieter erfüllen diese Voraussetzung nicht.[97] Content-Provider, deren Inhaltsangebot den redaktionellen Anforderungen entspricht, werden durch die Mediengrundrechte des Art. 5 Abs. 1 GG grundsätzlich geschützt.[98]

---

[90] Ausführlich zu den Medienfreiheiten von Diensteanbietern S. etwa *Tief,* Kommunikation, S. 93 ff.

[91] *Kühling* in: BeckOK Informations- und Medienrecht, Art. 5 GG Rn. 88.

[92] *BVerfG,* Urt. v. 5.2.1991 - 1 BvF 1/85 u.a., NJW 1991, 899, 899.

[93] Vgl. etwa *Schemmer* in: BeckOK GG, Art. 5 GG Rn. 43, 67 m.w.N.

[94] S. etwa *Schulze-Fielitz* in: Dreier, Art. 5 GG Rn. 90 m.w.N.

[95] S. etwa *Kühling* in: BeckOK Informations- und Medienrecht, Art. 5 GG Rn. 60, 88 m.w.N.

[96] Vgl. *Kühling* in: BeckOK Informations- und Medienrecht, Art. 5 GG Rn. 63; *Volkmann* in: Spindler/Schuster, § 59 RStV Rn. 14 ff.

[97] *Stumpf,* Das Recht auf Vergessenwerden, S. 200 f.; *Volkmann* in: Spindler/Schuster, § 59 RStV Rn. 16 f. A.A. vor allem im Hinblick auf die Bedeutung von Suchmaschinen für den Informationszugang der Nutzer *Arning/Moos/Schefzig,* CR 2014, 447, 453; *Lewinski,* AfP 2015, 1, 6; *Milstein,* K&R 2013, 446, 447.

[98] *Volkmann* in: Spindler/Schuster, § 59 RStV Rn. 14.

Schwieriger zu beurteilen ist die Rechtslage bei Host-Providern.[99] Besonders soziale Netzwerke tragen unzweifelhaft erheblich zur öffentlichen Meinungsbildung bei.[100] Das Speichern und die Verbreitung von Informationen und Inhalten ihrer Nutzer kann nur dann eine geschützte Tätigkeit darstellen, wenn der angebotene Dienst gezielt eine Plattform für meinungsbildende Inhalte bietet oder der Dienst darauf ausgerichtet ist, solche Inhalte vorzuhalten, zu moderieren und zu verbreiten.[101] Dienste, die zwar auch zur Meinungsverbreitung, Meinungsbildung, oder Informationsgewinnung genutzt werden, aber bei denen dies nicht den vordergründigen Zweck darstellt und keine redaktionelle Darbietung der Inhalte erfolgt, werden dagegen nicht von der Presse- und Rundfunkfreiheit erfasst.[102] Davon zu trennen ist jedoch die Meinungs- und Informationsfreiheit der Nutzer, die unabhängig von der Art des verwendeten Dienstes besteht.[103]

Maßnahmen zur Rechtsdurchsetzung – vor allem das Löschen von Inhalten oder zu weitreichende Prüfpflichten- können im Einzelfall also auch die Presse- und Rundfunkfreiheit der Diensteanbieter beeinträchtigen.[104] Bei der Regelung und Anordnung solcher Maßnahmen ist deshalb der Verhältnismäßigkeitsgrundsatz zu beachten.

III. Nemo-tenetur-Grundsatz

Eine weitere – wenngleich eher untergeordnete – Rolle spielt der nemo-tenetur-Grundsatz (nemo tenetur se ipsum accusare) im Zusammenhang mit einer Auskunftserteilung durch die Diensteanbieter. Werden die Diensteanbieter nämlich zu einer Auskunft an die Rechteinhaber über die Rechtsverletzung verpflichtet, kann im Einzelfall damit auch verbunden sein, dass sich die Diensteanbieter selbst einer Straftat oder Ordnungswidrigkeit bezichtigen müssten. Zudem kann der Diensteanbieter, wenn sich dadurch eine eigene

---

[99] S. zu den Anbietern sozialer Netzwerke *Gersdorf,* MMR 2017, 439, 443 f.; *Ladeur/Gostomzyk*, K&R 2017, 390, 392; *Müller-Tepitz,* ZUM 2020, 365, 369.

[100] *Friehe*, NJW 2020, 1697, 1700.

[101] *Volkmann* in: Spindler/Schuster, § 59 RStV Rn. 15. Vgl. auch *BVerfG*, Beschl. v. 13.1.1988 - 1 BvR 1548/82, NJW 1988, 1833, 1833 ff – Presse Grosso.

[102] A.A. aber *Gersdorf,* MMR 2017, 439, 443 ff.

[103] S. oben unter Kap. 3 § 3 B.

[104] Vgl. *Askani,* Private Rechtsdurchsetzung, S. 201.

Verantwortlichkeit für die Rechtsverletzung herausstellt, Folgeansprüchen der Rechteinhaber ausgesetzt sein.[105]

Der nemo-tenetur-Grundsatz wird aus dem Rechtsstaatsprinzip abgeleitet und ist in erster Linie ein Schutz davor, sich selbst oder einen Angehörigen im Rahmen eines Strafverfahrens belasten zu müssen.[106] Ob und inwieweit dieser Grundsatz im Zivilrecht anwendbar ist, ist aber strittig.[107] Zumindest darf er nicht durch zivilrechtliche Auskunftsansprüche unterlaufen werden.[108] Es würde dem Grundsatz zuwiderlaufen, wenn die Diensteanbieter durch die Auskunftserteilung sich selbst oder einen Angehörigen einer Straftat bezichtigen müssten und dies dann im Strafprozess gegen sie verwendet werden könnte. Dieses Problem lässt sich allerdings durch ein Beweisverwertungsverbot – beispielsweise in Anlehnung an die Regelung des § 101 Abs. 8 UrhG – beheben. Die alleinige Bereitstellung des Dienstes dürfte in vielen Fällen ohnehin keinen Straftatbestand erfüllen. Dies gilt vor allem für Access-Provider oder WLAN-Betreiber, die lediglich den Zugang zum Internet vermitteln.

Häufiger könnten sich die Diensteanbieter aber infolge der Auskunftserteilung zivilrechtlichen Ansprüchen – wie Unterlassungs- und Schadensersatzansprüchen – durch die Rechteinhaber ausgesetzt sehen.[109] Dies gilt vor allem dann, wenn neben der Auskunft über die Identität des rechtsverletzenden Nutzers auch über Details der Rechtsverletzung – wie Umfang und Verbreitung des verletzenden Inhalts – informiert wird. Dabei könnte sich beispielsweise Verletzungen von Prüfpflichten herausstellen, die Ansprüche gegen den Diensteanbieter selbst begründen können. Vor dieser Gefahr zivilrechtlicher Folgeansprüche schützt der nemo-tenetur-Grundsatz allerdings nicht.[110]

---

[105] Vgl. *Siebert*, Geheimnisschutz, S. 173.

[106] S. etwa *BVerfG*, Beschl. v. 13.1.1981 - 1 BvR 116/77, NJW 1981, 1431, 1431 ff.

[107] Ablehnend *BVerfG*, Beschl. v. 13.1.1981 - 1 BvR 116/77, NJW 1981, 1431, 1432 m.w.N.

[108] Vgl. zur Pflicht zur Selbstbelastung von Arbeitnehmern *Tödtmann/von Erdmann*, NZA 2020,1577, 1577 ff.

[109] S. auch *Siebert*, Geheimnisschutz, S. 172 f.

[110] *BVerfG*, Beschl. v. 13.1.1981 - 1 BvR 116/77, NJW 1981, 1431, 1432.

Auskunftsansprüche gegen Diensteanbieter dienen in erster Linie dem Zweck, die Rechtsdurchsetzung gegen den unmittelbaren Verletzer zu ermöglichen.[111] Der nemo-tenetur-Grundsatz steht einer solchen Auskunft daher in aller Regel nicht entgegen.

E. Folgerungen und Zusammenfassung Kapitel 3

Bei anonymen Rechtsverletzungen im Internet entsteht durch das Dreiecksverhältnis zwischen Rechteinhabern, Nutzern und Diensteanbietern eine sehr komplexe Interessenslage. Die zum Teil gegenläufigen Interessen müssen zu einem möglichst schonenden und angemessenen Ausgleich gebracht werden.

Die Rechteinhaber können sich dabei auf ihre grundrechtlich geschützten Rechtsgüter berufen. Ihr Schutz darf nicht durch die Anonymität von Internetnutzern ausgehöhlt werden. Sie haben ein berechtigtes Interesse an einer effektiven Rechtsdurchsetzung.

Dies steht vor allem im Konflikt mit den Interessen von Internetnutzern. Nutzer, die Rechte der Rechteinhaber verletzen, tragen die Hauptverantwortung für ihr Verhalten. Die Interessen der Rechteinhaber überwiegen daher in der Regel deren Interessen am Schutz Anonymität der Nutzer. Allerdings lässt sich nicht immer auf den ersten Blick zweifelsfrei feststellen, ob überhaupt eine Rechtsverletzung vorliegt. Zudem überwiegt die rechtmäßige und völlig legitime Nutzung von Internetdiensten. Zum Schutze aller Nutzer darf die Ausübung von Freiheitsrechten und damit verbunden die Anonymität aller Nutzer im Internet nicht zu stark beschränkt werden.

Wenn aber zugunsten der Interessen der Internetnutzer die Rechtsdurchsetzung erschwert wird, wird dies häufig durch Inpflichtnahme der Diensteanbieter kompensiert. Allerdings kann auch nicht die volle Verantwortung für die Rechtsverletzungen auf die Diensteanbieter übertragen werden. Sicherlich tragen die Diensteanbieter durch die Erbringung ihrer Internetdienste einen Teil zu den rechtsverletzenden Handlungen ihrer Nutzer bei, indem sie eine

---

[111] Vgl. *Siebert*, Geheimnisschutz, S. 173.

Gefahrenquelle schaffen. Zudem ziehen sie auch wirtschaftliche Vorteile aus der Nutzung rechtswidrige Inhalte. Allerdings leisten sie häufig auch einen gewünschten Beitrag zum gesellschaftlichen Leben. Problematisch ist vor allem, wenn eine Inanspruchnahme der Nutzer als unmittelbare Rechtsverletzer von vornherein ausgeschlossen bleibt und die Diensteanbieter die alleinige Verantwortung für sämtliche Rechtsverletzungen, die bei der Nutzung ihrer Dienste begangen werden, tragen müssen. Letztlich können damit Preiserhöhungen durch die Online-Dienste verbunden sein, die auch von den Nutzern getragen werden müssen, die sich gesetzeskonform verhalten.

Der anonymen Rechtsverletzungen im Internet zugrundeliegende Interessenskonflikt zwischen den beteiligten Diensteanbietern, Nutzern und Rechteinhabern ist so zu einem angemessenen Ausgleich zu bringen, dass nicht allein eine der Parteien übermäßig belastet wird. Vielmehr bedarf es einer Abwägung mit Blick auf eine angemessene Risiko- und Verantwortungsverteilung. Eine Identifizierung der Nutzer als unmittelbare Rechtsverletzer darf dabei nicht von vornherein ausgeschlossen sein.

Kapitel 4

Technische Möglichkeiten der Identifizierung von Internetnutzern

Bevor die rechtlichen Fragen um die Auskunftsersuche der Rechteinhaber und die damit verbundene Deanonymisierung von Internetnutzern geklärt werden können, müssen zunächst unabhängig hiervon die technischen Möglichkeiten einer Identifizierung von Internetnutzern betrachtet werden. Als Ausgangspunkt gilt es daher zu untersuchen, wie die Rechteinhaber überhaupt Kenntnis von einer Rechtsverletzung im Internet erlangen können (A.) und welche Rolle die verschiedenen Diensteanbieter bei der Identifizierung der Rechtsverletzer spielen können (B.). Die Ermittlung eines Teilnehmers an einem Kommunikationsvorgang im Internet kann dabei entweder anhand bei der Nutzung von Anwendungsdiensten anfallender Daten – wie Name, Wohnanschrift, Adresse, Kontodaten oder E-Mail-Adresse – (C.) oder unter Zuhilfenahme der IP-Adresse oder (D.) gelingen.

A. Kenntniserlangung von einer Rechtsverletzung

Die Identifizierung eines Internetnutzers setzt zunächst einmal voraus, dass der Rechteinhaber überhaupt Kenntnis von einer (möglichen) Rechtsverletzung erlangt. Wie dies erfolgt, unterscheidet sich von Fall zu Fall: Die Kenntnisnahme durch den Rechteinhaber kann vom Rechtsverletzer beabsichtigt oder in Kauf genommen sein, indem beispielsweise bewusst rechtsverletzende Inhalte über einen Internetdienst verbreitet werden, auf die auch der Rechteinhaber Zugriff hat oder die Inhalte an den Rechtinhaber adressiert werden. Häufig werden solche Inhalte oder rechtsverletzende Verhaltensweisen im Internet aber auch nur durch Zufall bemerkt.

Eine technische Dimension besteht in jenen Fällen, in denen die Rechte-inhaber gezielt nach Rechtsverstößen im Internet suchen können. Einen wichtigen

Anwendungsbereich stellt dabei das Durchsuchen von Filesharing-Netzwerken nach urheberrechtlich geschütztem Material dar. Die Rechteinhaber beauftragen dazu in der Regel spezialisierte Unternehmen, die unter Einsatz einer entsprechenden Software - zum Beispiel durch einen Testdownload – überprüfen, ob Werke des betreffenden Rechteinhabers auf entsprechenden Plattformen angeboten werden.[1] Die Rechteinhaber erhalten dadurch Kenntnis von der Rechtsverletzung und gleichzeitig über die IP-Adressen der Teilnehmer der Filesharing-Plattform.[2]

B. Die Rolle der Diensteanbieter

Die Diensteanbieter spielen für die Identifizierung von Internetnutzern eine entscheidende Rolle. Ohne ihre Mitwirkung können die Rechteinhaber die Identität anonymer Nutzer in der Regel nicht ermitteln. Der Beitrag, den die Diensteanbieter dabei leisten können, ist nach Art des Dienstes und der Rechtsverletzung verschieden, da sie unterschiedliche Beiträge zum rechtsverletzenden Verhalten ihrer Nutzer leisten und dadurch jeweils auch Zugriff auf andere Daten haben.

Zur besseren Unterscheidung kann das OSI-Schichtenmodell (Open Systems Interconnection Reference Model) herangezogen werden. Dabei wird der Datenübertragungsvorgang in sieben Schichten dargestellt.[3] Für diese Arbeit kommt es insbesondere auf die Differenzierung zwischen den transportorientierten Schichten (Schichten 1-4) und den überwiegend inhaltsbezogenen

---

[1] *Abdallah/Gercke,* ZUM 2005, 368, 368 ff.; *Brüggemann,* Drittauskunftsanspruch, S. 46 f.; *Brunst,* Anonymität im Internet, S. 96 f.; *Gercke,* CR 2006, 210, 211; *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 105; *Hoeren,* NJW 2008, 3099, 3099 f.; *Kindt,* MMR 2009, 147, 147; *Leicht,* VuR 2009, 346, 346; *Nietsch,* K&R 2011, 101, 102; *Welp,* Auskunftspflicht von Access-Providern, S. 26.

[2] Dies ist auf die Funktionsweise von Filesharing-Plattformen zurückzuführen, bei der die Daten anders als beim Client-Server-Modell unmittelbar zwischen den Teilnehmern an einem Filesharing-Netzwerk ausgetauscht werden. Durch den Download eines Werks erhält man so die IP-Adressen der anderen Teilnehmer.

[3] Ausführlichere Darstellung bei *Brunst,* Anonymität im Internet, S. 49; *Freiling/Heinson,* DuD 2009, 547, 547 ff; *Schütz* in: Beck'scher TKG-Kommentar, Rn. 35 ff.; *Tanenbaum*, Computernetzwerke, S. 54 ff.

Schichten (Schichten 5-7)[4] und vor allem der untersten Anwendungsschicht an. Dem Transport von Informationen sind diejenigen Diensteanbieter zuzuordnen, die für die Übertragung von Signalen sorgen. Dazu zählen vor allem die Zugangsanbieter. Bei der Anwendungsschicht geht es um den konkret angebotenen Dienst - wie einen World-Wide-Web-, Mail – oder Messenger-Dienst oder Peer-to-Peer-Dienst, aber auch Anbietern des Domain Name Systems.[5]

Deutlich werden die unterschiedlichen Rollen der Diensteanbieter auch bei den im ersten Teil herausgearbeiteten Fallgruppen:[6] Die erste Fallgruppe betrifft rechtswidrige Nutzerinhalte, die von Internetdiensten gespeichert und verbreitet werden. Dazu gehören World-Wide-Web-Dienste wie Plattformen, aber auch Messenger- oder E-Mail-Dienste. Diese Internetdienste sind der Anwendungsschicht zuzuordnen. Gegebenenfalls speichern sie Daten ihrer Nutzer wie Namen, Adressen, Geburtsdatum, Mail-Adressen, Kontodaten, Telefonnummern, etc. Darüber hinaus können sie die IP-Adressen, die zu einem bestimmten Zeitpunkt bei der Nutzung des Dienstes verwendet wurden, protokollieren.

Während die Dienste der Anwendungsschicht vor allem über Informationen verfügen, die im Zusammenhang mit der konkreten (rechtsverletzenden) Nutzung ihrer Dienste anfallen, können Zugangsanbieter dazu beitragen, den Weg der Datenübertragung zurückzuverfolgen. Denn ihre Dienstleistung besteht überwiegend in der Signalübertragung, wodurch die Nutzung der angewendeten Internetdienste erst ermöglicht wird. Dementsprechend ist es die Rolle der Zugangsanbieter bei der Identifizierung, die verwendete IP-Adresse einem Endnutzer zuzuordnen.

In der zweiten Fallgruppe, bei der es sich um sonstiges rechtswidriges Nutzerverhalten handelt, besteht eine ähnliche Rollenverteilung zwischen den verschiedenen Diensteanbietern. Die Diensteanbieter der Anwendungsschicht – sofern vorhanden – können eventuell Auskunft darüber gehen, welcher Nutzer, wann ihren Dienst genutzt hat.[7] Die Zugangsanbieter können unter Umständen

---

[4] *Schütz* in: Beck'scher TKG-Kommentar, Rn. 38.

[5] Vgl. *Brunst,* Anonymität im Internet, S. 49.

[6] S. dazu oben unter Kap. 2 §3 A.

[7] An einem solchen Diensteanbieter fehlt es zum Beispiel bei dezentralen P2P-Systemen, S. oben unter Kap. 2 § 2 B IV. 4.

eine Rückverfolgung des Kommunikationsvorgangs anhand der IP-Adresse vornehmen.

In den ersten beiden Fallgruppen existieren deshalb im Wesentlichen zwei verschiedene Möglichkeiten, die Identität der Nutzer zu ermitteln: Zum einen kann die Identifizierung direkt durch den angewendeten Dienst – z.B. durch den Host-Provider erfolgen, wenn dieser Auskunft über personenbezogene Daten des Nutzers – wie Name, Adresse, Kontodaten, etc. geben kann. Zum anderen kann der Nutzer über die zum Zeitpunkt der Rechtsverletzung verwendete IP-Adresse unter Zuhilfenahme der Zugangsanbieter zurückverfolgt werden.[8]

Anders verhält es sich bei Rechtsverletzungen durch Domaininhaber. Hier spielt die IP-basierte Identifizierung der Nutzer keine Rolle. Stattdessen steht die Auskunft der DENIC oder der zuständigen Domain-Registrare im Vordergrund.

C. Identifizierung über Anwendungsdienste

Für die Rechteinhaber ist es oft am einfachsten, wenn sie direkt bei den Diensten der Anwendungsschicht Auskunft über die Identität eines Nutzers erhalten können. Dafür müssten die Diensteanbieter aber über ausreichend Informationen verfügen, um den Nutzer identifizieren zu können.

Bei der Nutzung von Internetdiensten fallen sehr oft eine Vielzahl von Daten an, die Aufschluss über die Identität der Nutzer geben könnten. Die Anonymität eines Internetnutzers gegenüber den Rechteinhabern ist aber erst aufgehoben, wenn diese die rechtsverletzende Handlung eindeutig einer Person zuordnen können. Darüber hinaus bedarf es für die Rechtsdurchsetzung gegen den Nutzer aber grundsätzlich auch einer ladungsfähigen Anschrift des Nutzers, um den Anforderungen einer Klageschrift des § 253 Abs. 2 Nr. 1 ZPO zu genügen.[9] Primäres Ziel der Rechteinhaber wird es deshalb sein, Name und Adresse des Nutzers in Erfahrung zu bringen.

---

[8] Hierbei kann es aber auch zunächst erforderlich sein, dass zum Beispiel der Host-Provider vorab Auskunft über die verwendete IP-Adresse erteilt.

[9] S. dazu etwa *Bacher,* BeckOK ZPO, § 253 ZPO Rn. 46.

Dennoch kann es auch hilfreich sein, wenn die Diensteanbieter über andere personenbezogene Daten ihrer Nutzer verfügen. Je mehr Informationen sich über den Nutzer zusammentragen lassen, desto wahrscheinlicher ist es, dass die Identifizierung gelingt: Unter Umständen kann zum Beispiel aus der Mailadresse der Name eines Nutzers abgeleitet werden, wenn diese sich aus dem Vor- und Nachnamen zusammensetzt.[10] Aus hinterlegten Zahlungsinformationen lassen sich gegebenenfalls die Adresse des Zahlungsinstituts ableiten, bei der der Nutzer ein Konto besitzt. Dies kann im Einzelfall Rückschlüsse zum Beispiel über den Wohnort des Nutzers zulassen. Das Zahlungsinstitut kann dann gegebenenfalls auch Auskunft über den zugehörigen Kontoinhaber geben.[11] Auch die IP-Adresse kann manchmal lokalisiert werden.[12] Sind zumindest Wohnort und Name bekannt, lässt sich wiederum die genaue Anschrift durch eine Adressabfrage beim Einwohnermeldeamt ermitteln. Auch eine Telefonnummer lässt sich gegebenenfalls über den Telekommunikationsanbieter einem Anschlussinhaber zuordnen.[13]

Für die Rechteinhaber ist es deshalb oft sinnvoll, so viele personenbezogene Daten von den Anwendungsdiensten zu erfragen, wie möglich. Ob den Rechteinhabern die Identifizierung tatsächlich gelingen kann, hängt davon ab, welche Informationen bei der Nutzung übertragen werden und welche Daten von den Anwendungsdiensten verarbeitet werden.

I. Dienste des World Wide Web

Das World Wide Web ermöglicht unter der Verwendung des HTTP- (Hypertext Transfer Protocol) oder HTTPS-Protokolls (Hypertext Transfer

---

[10] S. dazu auch *OLG Bamberg*, Urt. v. 12.5.2005 - 1 U 143/04, CR 2006, 274, 276 mit der Feststellung, dass es sich in diesem Fall bei der E-Mail-Adresse um ein personenbezogenes Datum handelt.

[11] S. zur Auskunft gegen die Sparkasse Magdeburg nach § 19 Abs. 2 MarkenG *EuGH,* Urt. v. 16.7.2015 – C-580/13, GRUR 2015, 894, 894 ff. – Coty Germany. S. nachfolgend auch *BGH,* Urt. v. 21.10.2015 – I ZR 51/12, GRUR 2016, 497, 497 ff. – Davidoff Hot Water II.

[12] *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 62; *Schmidt/Pruß* in: Auer-Reinsdorff/Conrad, § 3 Rn. 136.

[13] Vgl. *Vonau,* GRUR-Prax 2021, 59 m. Anm. zu *EuGH,* Urt. v. 9.7.2020 – C-264/19, GRUR 2020, 841 – YouTube-Drittauskunft.

Protocol Secure) das Abrufen von Webseiten.[14] Dafür ist die Verwendung eines Browsers wie Firefox, Internet Explorer oder Google Chrome erforderlich.[15] Webseiten speichern in den Logfiles ihrer Webserver häufig eine große Bandbreite von Informationen über ihre Nutzer: So wird neben der IP-Adresse etwa der verwendete Browser, die Sprache, das Betriebssystem und die Bildschirmauflösung der Nutzer protokolliert.[16] Webserver können alle Zugriffe auf ihre Webseiten festhalten.[17] Eine Identifizierung des Nutzers ist aber nur möglich, wenn auch darüber hinaus Daten erhoben werden. Viele Dienste setzen eine Anmeldung oder Registrierung der Nutzer voraus.[18] Häufig müssen dafür Name und Mailadresse angegeben werden. Meist werden diese Daten aber nicht auf Echtheit geprüft. Zudem können zum Beispiel Wegwerf-E-Mail-Adressen zur Anmeldung verwendet werden. Anders verhält es sich aber, wenn die Daten für die konkrete Dienstleistung notwendig sind. Also wenn etwa die Postanschrift für eine Lieferung oder Bankdaten für einen Bezahlvorgang benötigt werden.[19] Eine Umgehung, zum Beispiel durch anonyme Zahlungsmittel, wird dabei nicht immer möglich beziehungsweise für viele Nutzer nicht üblich sein.[20]

Zudem gibt es viele Nutzer, die ihre persönlichen Daten recht bereitwillig preisgeben, selbst wenn es für die Nutzung des Dienstes nicht zwingend erforderlich wäre. Besonders in sozialen Netzwerken veröffentlichen Nutzer eine Vielzahl zum Teil sehr persönlicher Informationen über sich – wie Beziehungsstatuts, Ausbildung, besuchte Schulen, Familienangehörige etc. Teilweise fehlen erkennbare Hinweise bei der Registrierung, welche Daten tatsächlich angegeben werden müssen und welche optional sind oder die Diensteanbieter verlangen mehr Daten als eigentlich notwendig wäre.[21] Ob eine Identifizierung eines

---

[14] *Brunst,* Anonymität im Internet, S. 54; *Schmidt/Pruß* in: Auer-Reinsdorff/Conrad, § 3 Rn. 109.

[15] *Schmidt/Pruß* in: Auer-Reinsdorff/Conrad, § 3 Rn. 109.

[16] *Brunst,* Anonymität im Internet, S. 56 f.; *Köhntopp/Köhntopp,* CR 2000, 248, 250 ff.; *Schmidt/Pruß* in: Auer-Reinsdorff/Conrad, § 3 Rn. 136.

[17] *Nietsch,* Anonymität und Durchsetzung, S. 65.

[18] S. dazu *Siebert,* Geheimnisschutz, S. 376.

[19] *Brunst,* Anonymität im Internet, S. 75.

[20] S. zu anonymen Zahlungsmöglichkeiten ausführlich *Brunst,* Anonymität im Internet, S. 103 ff.

[21] Vgl. *Brunst,* Anonymität im Internet, S. 75.

Nutzers gelingen kann, hängt daher von der Art der Webseite, sowie vom Verhalten der Diensteanbieter und Nutzer ab.

II. Peer-to-Peer-Dienste

Bei der Nutzung von Peer-to-Peer-Diensten erfolgt der Informationsaustausch direkt unter den Teilnehmern.[22] Ein zentraler Diensteanbieter, der die Daten der Teilnehmer verarbeitet, existiert meist nicht. Die Rechteinhaber können aber eigenständig an Daten der Nutzer gelangen, wenn sie selbst am Netzwerk teilnehmen. In der Regel steht dabei die IP-basierte Identifizierung im Vordergrund.[23]

III. Usenet

Das Usenet verwendet NNTP (Network News Transfer Protocol) und besteht in einer dezentralen Verbindung von Servern, die von unterschiedlichen Diensteanbietern betrieben werden.[24] Beim Hochladen oder Abrufen von Inhalten wird lediglich die IP-Adresse der Nutzer übertragen. Usenet-Provider speichern darüber hinaus meist keine Daten ihrer Nutzer und protokollieren auch nicht, wer Zugang zu einer Newsgroup hat.[25] Auch bei der Nutzung des Usenets ist deshalb – wenn überhaupt – eine Identifizierung nur des Absenders einer Nachricht anhand der IP-Adresse möglich.[26]

IV. E-Mail-Dienste

E-Mail-Dienste basieren auf dem SMTP-Protokoll (Simple Mail Transfer Protocol). Beim Versand einer E-Mail wird die Nachricht an den SMTP-Server des Mail-Dienstes übertragen.[27] Dabei wird unter anderem die IP-Adresse des Absenders übermittelt. Dadurch kann dokumentiert werden, zwischen welchen Nutzern der Mailverkehr stattgefunden hat.[28] Das Abrufen einer Mail kann

---

[22] S. oben unter Kap. 2 § 2 B IV. 4.

[23] Vgl. auch *Brunst,* Anonymität im Internet, S. 97.

[24] S. oben unter Kap. 2 § 2 B IV. 4.

[25] *Schmidt/Pruß* in: Auer-Reinsdorff/Conrad, § 3 Rn. 164.

[26] S. dazu *Brunst,* Anonymität im Internet, S. 101 f.

[27] *Brunst,* Anonymität im Internet, S. 64; *Schmidt/Pruß* in: Auer-Reinsdorff/Conrad, § 3 Rn. 177.

[28] *Brunst,* Anonymität im Internet, S. 64.

über einen Webserver oder einen Mail-Client unter Verwendung des POP3- (Post Office Protocol) oder IMAP-Protokolls (Internet Message Access Protocol) erfolgen.[29] Der Empfänger der Mail kann im Header Informationen wie die IP-Adresse des Absenders einsehen. Diese IP-Adresse kann eventuell durch Zugangsanbieter zum Nutzer (Absender der Mail) zurückverfolgt werden.

Neben den Daten, die beim Versenden und Empfangen einer Mail anfallen, erheben Mail-Dienste zum Teil weitere Daten ihrer Nutzer: Die Nutzung eines E-Mail-Dienstes erfordert regelmäßig eine Anmeldung mit Mailadresse und einem Passwort.[30] Häufig wird zusätzlich der Name des Nutzers gespeichert. Vor allem bei kostenpflichtigen Maildiensten werden darüber hinaus gegebenenfalls noch Kontoinformationen und Zahlungsdaten, sowie gegebenenfalls die Wohnanschrift erhoben. Eine Verifikation dieser Daten erfolgt aber in der Regel nicht.

Dennoch können unter Umständen die Anbieter von E-Mail-Diensten einer Mailadresse, Daten wie Name, Kontoinformationen und Anschrift ihres Nutzers zuordnen. Dadurch könnte zum Beispiel der Absender einer Mail mit rechtsverletzendem Inhalt durch Auskunft des E-Mail-Dienstes identifiziert werden. Aber auch, wenn sich ein Nutzer bei einem anderen Internetdienst mit seiner Mailadresse registriert hat, kann der E-Mail-Anbieter zur Identifizierung dieses Nutzers beitragen, wenn die Rechteinhaber zuvor die Mailadresse ermitteln konnten.[31]

V. Internet Relay Chat, Instant Messenger, VoIP-Dienste

Internet Relay Chat, Instant Messenger oder VoIP-Dienste ermöglichen eine Kommunikation in Echtzeit per Text, Bildern, Video oder Sprache.[32] Entweder erfolgt die Kommunikation über einen zentralen Server oder unmittelbar unter den Teilnehmern selbst.[33] Wird ein zentraler Server verwendet, erhält der Betreiber Zugriff auf die IP-Adressen der Nutzer, Informationen darüber wie lange

---

[29] Ausführlicher *Brunst,* Anonymität im Internet, S. 64 f.; *Grünwald/Nüßing*, MMR 2016, 91, 92; *Schmidt/Pruß* in: Auer-Reinsdorff/Conrad, § 3 Rn. 177.

[30] Vgl. *Brunst,* Anonymität im Internet, S. 55.

[31] S. dazu auch *Siebert,* Geheimnisschutz, S. 369.

[32] Vgl. *Brunst,* Anonymität im Internet, S.65.

[33] *Brunst,* Anonymität im Internet, S.66. Ausführlich zur technischen Funktionsweise solcher Dienste *Grünwald/Nüßing*, MMR 2016, 91, 92 f.

und mit welchen anderen Teilnehmern ein Austausch stattgefunden hat und gegebenenfalls sogar über den Inhalt einer Nachricht, sofern dieser nicht verschlüsselt wird. Selbst wenn die Kommunikation unmittelbar unter den Teilnehmern stattfindet, wird die Verbindung zwischen den Nutzern meist über einen zentralen Server aufgebaut, sodass die Diensteanbieter Aufschluss über die IP-Adressen der Nutzer erhalten.[34]

Gemeinsam haben die genannten Dienste, dass in der Regel eine Kommunikation nur unter den Nutzern des jeweiligen Dienstes möglich ist.[35] Dies erfordert eine Anmeldung zum Beispiel mit einem Pseudonym oder einer Mailadresse. Zudem führen die Betreiber oft Teilnehmerverzeichnisse.[36] Das dient dem Zweck, dass die Nutzer eindeutig adressiert werden können. Messenger Dienste wie WhatsApp verwenden zum Beispiel die Telefonnummer zur eindeutigen Identifizierung. WhatsApp und ähnliche Dienste erhalten zudem Zugriff auf die Kontaktdaten und gegebenenfalls den Standort der Nutzer.

Darüber hinaus geben viele Nutzer noch weitere Informationen wie Namen, Profilbild, Status, Geburtsdatum, etc. über sich preis, die von den Diensteanbietern gespeichert werden. Durch die Kombination dieser Daten mit denen, die während eines Kommunikationsvorgangs anfallen, können die Diensteanbieter unter Umständen sehr umfassende Nutzerprofile erstellen.

Ebenso wie bei Webdiensten hängen die Identifizierungsmöglichkeiten der Rechteinhaber davon ab, über welche Daten die Diensteanbieter im konkreten Einzelfall verfügen. Da sowohl Mail-Dienste als auch IRC, Messenger- und VoIP-Dienste traditionelle Kommunikationsdienste ersetzen, die Kommunikation erheblich beschleunigen und so Einzug in den Alltag der Nutzer halten, können auch verstärkt personenbezogene Daten erhoben werden. Ähnliches gilt aber zum Beispiel auch für soziale Netzwerke.

---

[34] *Brunst,* Anonymität im Internet, S.67; *Grünwald/Nüßing*, MMR 2016, 91, 92; *Kühling/Schall*, CR 2015, 641, 644.

[35] *Grünwald/Nüßing*, MMR 2016, 91, 92.

[36] *Brunst,* Anonymität im Internet, S.66.

VI. Identifizierung von Domaininhabern und Webseiten-Betreibern

Einen Sonderfall stellt die Identifizierung von Domaininhabern dar. Domaininhaber nutzten die Dienste der Domain-Registrare und der Registrys (z.B. DENIC), um eine Domain anzumelden. Dabei müssen sie zwingend ihren Namen und ihre Anschrift, sowie weitere Informationen (Name, Anschrift, Telefonnummer und Mailadresse) des administrativen Ansprechpartners (Admin C) angeben.[37] Die Registrare speichern diese Daten in einer öffentlichen Whois-Datenbank.[38] Kommt es durch die Verwendung einer Domain zu einer Rechtsverletzung, können die Rechteinhaber den zuständigen Registrar auf Auskunft in Anspruch nehmen. Dasselbe gilt, wenn sich rechtsverletzende Inhalte auf der Webseite des Domaininhabers befinden. Hierbei ist ein Rückgriff auf die Registries oder den Domain-Registrar nur erforderlich, wenn keine Impressumspflicht aus § 5 TMG besteht oder der Domaininhaber diese nicht korrekt eingehalten hat.

Die Identifizierung durch die Domain Registrare kann aber scheitern, wenn Privacy Domains verwendet werden, bei denen die persönlichen Daten des Domaininhabers durch Proxy-Informationen ersetzt werden.[39] In diesem Fall müsste zusätzlich Auskunft bei dem Diensteanbieter eingeholt werden, der die Anonymisierung der Domain ermöglicht hat.

Wird die IP-Adresse einer Webseite durch einen CDN-Provider verdeckt und damit die Anonymität des Anbieters der Seite hergestellt, ist zur Aufdeckung der Identität die Mitwirkung des CDN-Providers erforderlich.[40]

D. Identifizierung von Internetnutzern mittels IP-Adresse

Ist eine Identifizierung nicht bereits durch die Anwendungsdienste möglich, besteht die Möglichkeit, den Nutzer anhand seiner IP-Adresse

---

[37] S. auch *Brunst,* Anonymität im Internet, S. 93.

[38] S. etwa zum Whois-Service der DENIC https://www.denic.de/service/whois-service/ (Stand: 24.05.2022).

[39] Ausführlicher *Brunst,* Anonymität im Internet, S. 93 f.

[40] S. dazu *OLG Köln,* Urt. v. 9.10.2020 – 6 U 32/20, GRUR 2021, 70, 71 – Herz Kraft Werke.

zurückzuverfolgen. IP-Adressen werden bei jedem Kommunikationsvorgang im Internet technisch zwingend übertragen. Daher sind sie bei der Identifizierung von Internetnutzern von zentraler Bedeutung.

I. Technische Grundlagen zur IP-Adresse

IP-Adressen setzen sich zurzeit mehrheitlich noch aus vier Byte-Werten zwischen 0 und 255 zusammen, die durch Punkte voneinander getrennt werden (Beispiel: 123.45.67.89). Daraus ergeben sich ungefähr 4,3 Milliarden verschiedene mögliche Kombinationen für IP-Adressen.[41] Bei der Einwahl ins Internet wird dem Rechner eine IP-Adresse zugeordnet, die zumindest in diesem Zeitpunkt nur einmalig vergeben ist.[42]

Die IP-Adresse ist also eine notwendige Adressierung, damit die Daten an die jeweils richtigen Empfänger gelangen können.[43] Ihre Funktion lässt sich daher mit der eines „Briefumschlags" vergleichen.[44] Bei jedem Vorgang im Internet werden IP-Adressen zur Datenübertragung ausgetauscht. Wird beispielsweise eine Website aufgerufen, so wird die IP-Adresse an den Server der Website übermittelt, der dann die entsprechenden Daten zurücksendet. Der Header der zu übertragenden Datenpakete enthält Informationen über die IP-Adresse des Quell- und Zielrechners.[45]

Die Einmaligkeit dieser IP-Adressen bildet die Grundlage für eine eindeutige Identifizierung von Internetnutzern.[46] Dabei bestehen aber Unterschiede zwischen statischen und dynamischen IP-Adressen.

---

[41] *Nietsch,* Anonymität und Durchsetzung, S. 61.

[42] *Meyerdierks,* MMR 2009, 8, 9; *Nietsch,* Anonymität und Durchsetzung, S. 61.

[43] Vgl. *Brüggemann,* Drittauskunftsanspruch, S. 44; *Freund/Schnabel,* MMR 2011, 495, 495; *Nietsch,* Anonymität und Durchsetzung, S. 61; *Tanenbaum,* Computernetzwerke, S. 69; *Welp,* Auskunftspflicht von Access-Providern, S. 10.

[44] *Freiling/Heinson,* DuD 2009, 547, 549; *Federrath,* ZUM 2006, 434, 435; *Sandor,* Datenspeicherung, Rn. 423.

[45] Ausführlicher dazu *Welp,* Auskunftspflicht von Access-Providern, S. 12.

[46] Vgl. *Welp,* Auskunftspflicht von Access-Providern, S. 10.

1. Statische IP-Adresse

Statische IP-Adressen werden fest vergeben. Das bedeutet, dass jede Einwahl ins Internet durch einen Rechner unter derselben IP-Adresse erfolgt. Während früher die statische Vergabe von IP-Adressen für alle Nutzer üblich war,[47] werden solche IP-Adressen heute vor allem von größeren Unternehmen verwendet.[48]

Dies liegt an den Vorteilen, die statische IP-Adressen gegenüber dynamischen IP-Adressen bieten: Statische IP-Adressen erleichtern unter anderem die Kommunikation verschiedener technischer Geräte – zum Beispiel PC, Drucker, etc. - untereinander in einem Netzwerk. Zudem werden sie für den Betrieb eines Web- oder Mail-Servers, der über gleichbleibende Internetadressen abrufbar sein soll, benötigt.[49]

2. Dynamische IP-Adresse

Durch den großen Anstieg an internetfähigen Geräten und die erheblich gestiegene Internetnutzung ist der Bedarf an IP-Adressen heutzutage aber sehr hoch.[50] Dieser Bedarf könnte bei einer statischen Vergabe aller IP-Adressen nicht gedeckt werden. Daher erfolgt die private Internetnutzung derzeit überwiegend unter der Verwendung von dynamischen IP-Adressen.[51] Diese werden bei jeder Einwahl ins Internet – und in der Regel spätestens nach 24 Stunden – neu vergeben. Der jeweilige Access-Provider, der den Zugang zum Internet anbietet, verfügt dazu über ein Kontingent an IP-Adressen, die den Nutzern immer wieder neu für den Zeitraum des Nutzungsvorgangs zugewiesen werden.[52]

---

[47] S. dazu etwa *Köhntopp/Köhntopp*, Datenspuren im Internet, S. 1.

[48] Vgl. *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 104; *Nietsch,* Anonymität und Durchsetzung, S. 62.

[49] Vgl. *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 38.

[50] S. auch *Brunst,* Anonymität im Internet, S. 51.

[51] S. auch *Brüggemann,* Drittauskunftsanspruch, S. 45; *Hoeren,* ZRP 2010, 251, 253; *Sandor,* Datenspeicherung, Rn. 421.

[52] *Brunst,* Anonymität im Internet, S. 51; *Germann,* Gefahrenabwehr und Strafverfolgung, S. 66; *Hoeren,* ZRP 2010, 251, 252 f.; *Nietsch,* Anonymität und Durchsetzung, S. 62; *Solmecke,* K&R 2007, 138, 140.

Dazu wird der MAC-Adresse des verwendeten Rechners die IP-Adresse zugeteilt.[53]

Dieser Vorgang erhöht – verglichen mit der Verwendung statischer IP-Adressen - die Anonymität der Internetnutzer erheblich, da die Zuordnung der IP-Adresse zu einem Anschluss nur in Verbindung mit dem konkreten Zeitraum der Nutzung erfolgen kann.[54]

3. iPv6-Adressen

Um dem zukünftig weiter steigenden Bedarf an IP-Adressen gerecht werden zu können, wurden die sogenannten iPv6-Adressen entwickelt. Im Unterschied zu den eben beschriebenen iPv4-Adressen bestehen diese aus 16 Bytes und setzen sich aus einem Netzwerk-Präfix (8 Bytes) und einem Interface Identifier (8 Bytes) zusammen. Das Netzwerk-Präfix wird – ebenso wie iPv4-Adressen – von den Access-Providern vergeben. Der Interface-Identifier wird meist durch den Rechner selbst an eine Netzwerkschnittstelle vergeben.[55]

Durch die Adressierung des iPv6 wird die Anzahl der Kombinationsmöglichkeiten gegenüber dem iPv4-System von etwa 4,3 Milliarden auf ca. 340 Sextillionen erheblich erweitert.[56] Dies würde es – anders als bei der Verwendung von iPv4-Adressen – ermöglichen, IP-Adressen – insbesondere das Netzwerk-Präfix – an alle Nutzer statisch zu vergeben.[57] Deshalb wird befürchtet, dass der verstärkte Einsatz von iPv6-Adressen zukünftig zu einer starken Aufweichung der Anonymität im Internet führen könnte.[58] Als positiver Effekt für die Rechteinhaber wäre damit eine erleichterte Rückverfolgung von Internetnutzern verbunden.

---

[53] *Nietsch,* Anonymität und Durchsetzung, S. 62.

[54] *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 104.

[55] *Nietsch,* Anonymität und Durchsetzung, S. 67.

[56] *Brunst,* Anonymität im Internet, S.45; *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 38; *Freund/Schnabel*, MMR 2011, 495, 495.

[57] *Hoeren,* ZRP 2010, 251, 252 f.; *Nietsch,* Anonymität und Durchsetzung, S. 70; *Sandor,* Datenspeicherung, Rn. 432.

[58] So etwa *Hoeren,* ZRP 2010, 251, 253; Positiv wertend dagegen *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 348.

Derzeit sind aber iPv4-Adressen noch etwas stärker verbreitet und werden nur langsam durch iPv6-Adressen verdrängt.[59] Außerdem ist auch bei iPv6-Adressen eine statische Vergabe durch die Access-Provider nicht zwingend.[60] Zumindest im Hinblick auf das Netzwerk-Präfix unterscheiden sich im Hinblick auf die Identifizierung von Internetnutzern iPv6-Adressen nicht wesentlich von einer iPv4-Adressierung.[61] Die nachstehenden Ausführungen, die sich weitgehend auf die derzeit noch vorherrschenden iPv4-Adressen konzentrieren, lassen sich daher weitgehend übertragen. Vor allem durch Heranziehung des Interface Identifiers können sich aber dennoch Abweichungen bei der Identifizierung von Internetnutzern ergeben. Im Hinblick darauf, dass die Ablösung durch iPv6 als Nachfolgemodell bereits feststeht, werden diese Besonderheiten daher an den relevanten Stellen dieser Arbeit aufgegriffen.

II. Ermittlung der bei der Rechtsverletzung verwendeten IP-Adresse

Als Ausgangspunkt für die Identifizierung eines Internetnutzers muss der Rechteinhaber die IP-Adresse, die bei der Rechtsverletzung im Internet verwendet wurde, herausfinden. In einigen Fällen können die Rechteinhaber diese eigenständig ermitteln, häufig sind sie dabei aber auf die Auskunft des Anbieters eines durch den Nutzer verwendeten Telemediendienstes angewiesen.

1. Eigenständige Ermittlung

Eine eigenständige Ermittlung der IP-Adresse kann immer dann gelingen, wenn eine Kommunikation beziehungsweise ein Austauschen von Daten unmittelbar zwischen dem Rechteinhaber und dem Nutzer stattgefunden hat, wodurch an den Rechteinhaber als Empfänger der Daten die IP-Adresse des Absenders mitübertragen wird. Das ist vor allem bei Peer-to-Peer-Netzwerken der Fall. Zum Beispiel können rechtsverletzende Handlungen in Filesharing-Netzwerken unter Zuhilfenahme einer entsprechenden Software aufgespürt werden, indem von Seiten der Rechteinhaber selbst eine Teilnahme im Filesharing-

---

[59] S. etwa zur iPv6-Konnektivität bei Google-Nutzern https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption (Stand: 24.05.2022).

[60] Ausführlicher zur Adressierung im iPv6-System etwa *Nietsch,* Anonymität und Durchsetzung, S. 66 ff.

[61] S. auch *Nietsch,* Anonymität und Durchsetzung, S. 68.

Netzwerk erfolgt.[62] IP-Adresse und Zugriffszeiten der Nutzer können so festgehalten werden.[63]

Aber auch, wenn ein E-Mail-Verkehr zwischen dem Nutzer und dem Rechteinhaber stattgefunden hat, lässt sich eine IP-Adresse ausmachen. Der Header der E-Mail enthält Informationen über den Absender der Mail einschließlich der IP-Adresse, die der Rechteinhaber im Quelltext einsehen kann. Allerdings können durch den Einsatz von Remailern die Header-Informationen ausgetauscht werden, sodass die eigentliche IP-Adresse nicht mehr erkennbar ist.[64]

2. Erfassung der IP-Adressen der Nutzer durch Anwendungsdienste

In vielen anderen Fällen lässt sich die IP-Adresse aber nur mit Hilfe der Anwendungsdienste herausfinden. Indem diese einen Dienst bereitstellen, der für die rechtsverletzende Handlung genutzt wurde oder bei dem rechtsverletzende Inhalte für die Nutzer gespeichert werden, werden Nutzerdaten an die Diensteanbieter übermittelt. Dabei wird insbesondere die IP-Adresse an den Anbieter des Dienstes übertragen, damit die angefragten Daten an den richtigen Empfänger gesendet werden können. Die auf diese Weise anfallenden Nutzerdaten können die Diensteanbieter in ihren Log-Files speichern.[65]

Neben der IP-Adresse können auch die Zugriffszeiten der Nutzer durch die Diensteanbieter protokolliert werden. Der Rechteinhaber benötigt diese Daten zur Identifizierung, wenn der Rechtsverletzer eine dynamische IP-Adresse verwendet hat. Denn der Access-Provider kann ohne dieses Wissen keine Angaben über einen Anschlussinhaber machen, der die IP-Adresse nur für einen bestimmten Zeitpunkt innehatte.

---

[62] Dies erfolgt häufig durch Unternehmen die unter Einsatz einer speziellen Software für die Rechteinhaber Filesharing-Netzwerke nach urheberrechtlich geschütztem Material durchsuchen, S. bereits oben unter Kap. 4 §1. S. auch *Abdallah/Gercke,* ZUM 2005, 368, 368 ff.; *Brüggemann,* Drittauskunftsanspruch, S. 46 f.; *Gercke,* CR 2006, 210, 211; *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 105; *Hoeren,* NJW 2008, 3099, 3099 f.; *Kindt,* MMR 2009, 147, 147; *Leicht,* VuR 2009, 346, 346; *Nietsch,* K&R 2011, 101, 102.

[63] *Brüggemann,* Drittauskunftsanspruch, S. 46 f.; *Hoeren,* NJW 2008, 3099, 3099.

[64] Vgl. *Brunst,* Anonymität im Internet, S. 88 ff.

[65] S. auch *Hage/Hitzfeld* in: Loewenheim/Koch, S. 17.

Sofern die Diensteanbieter entsprechende Nutzerdaten in ihren Log-Dateien speichern, könnten die Rechteinhaber also im Wege eines Auskunftsersuchens Kenntnis von der IP-Adresse und den Zugriffszeiten des Rechtsverletzers erlangen.

III. Identifizierung durch Verknüpfung weiterer Daten mit der IP-Adresse

Neben der IP-Adresse und den Zugriffszeiten können im Internet mit und ohne das Wissen der Nutzer noch viele weitere Daten anfallen, die die Anonymität der Nutzer einschränken. Wird zum Beispiel eine Webseite über einen Browser abgerufen, können auf dem Rechner der Nutzer sogenannte Cookies abgelegt werden, die unter Umständen bei einem erneuten Besuch der Seite ausgelesen werden.[66] Trotz einer wechselnden IP-Adresse kann der Webserver den Nutzer auf diese Weise wiedererkennen.[67]

In der Regel führen solche Daten aber nicht zu einer unmittelbaren Identifizierung der Nutzer. Zumindest ist es den Rechteinhabern nicht möglich, diese zur Identifizierung einzusetzen, da hierfür eine „zentrale Stellung innerhalb des Informationsflusses erforderlich wäre".[68]

Im Einzelfall können sich solche Daten dennoch als hilfreich erweisen, wenn der Anwendungsdienst diese mit der IP-Adresse derartig verknüpfen kann, dass er weitere identifizierende Daten erhält. Diese könnten dann wiederum an die Rechteinhaber weitergegeben werden. Das ist der Fall, wenn eine statische IP-Adresse mit Daten, die bei der Anmeldung zu einem Dienst eingegeben wurden, verknüpft werden kann.[69] In diesem Fall wäre eine Auskunft des Access-Providers überflüssig.[70]

---

[66] *Nietsch,* Anonymität und Durchsetzung, S. 65.

[67] *Nietsch,* Anonymität und Durchsetzung, S. 66.

[68] *Nietsch,* Anonymität und Durchsetzung, S. 74.

[69] S. zu Verknüfung statischer IP-Adressen mit Social-Plug-ins *Nietsch,* Anonymität und Durchsetzung, S. 74 f.

[70] *Nietsch,* Anonymität und Durchsetzung, S. 75.

IV. Ermittlung über den Access-Provider

In der Regel lässt sich der Inhaber einer IP-Adresse aber nur durch Auskunft des Access-Providers ermitteln. Die Rechteinhaber müssen dafür zunächst herausfinden, welcher Access-Provider die fragliche IP-Adresse vergeben hat, bevor die Access-Provider diese einem Anschlussinhaber zuordnen können.

1. Ermittlung des Access-Inhabers

Bei der Ermittlung des zuständigen Access-Providers kommt den Rechteinhabern zugute, dass die Provider über ein festes Kontingent an IP-Adressen verfügen, sodass sich anhand der IP-Adresse der jeweilige Provider zurückverfolgen lässt.

Zuständig für die Koordination der IP-Adressen ist die IANA (Internet Assigned Numbers Authority). Diese weist den Regional Internet Registries (RIR) Adress-Blöcke zu.[71] Es existieren insgesamt fünf solcher regionalen Vergabestellen. Für den europäischen Adressraum ist das RIPE NCC (Réseaux IP Européens Network Coordination Centre) zuständig.[72] Die RIRs wiederum verteilen die an sie vergebenen IP-Adressen an sogenannte Local Internet Registires (LIR).[73] Diese treten häufig selbst als Access-Provider auf und teilen ihren Endkunden IP-Adressen zu oder vergeben wiederum IP-Adressblöcke an andere Provider.[74]
Über sogenannte Whois-Datenbanken der RIRs lässt sich so ermitteln, welchem LIR eine IP-Adresse zugeordnet wurde.[75] So können die Rechteinhaber Kenntnis von den Kontaktdaten des Access-Providers erlangen.[76] Häufig lässt

---

[71] S. auch *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 41; *Brüggemann,* Drittauskunftsanspruch, S. 45; *Nietsch,* Anonymität und Durchsetzung, S. 62.

[72] S. auch *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 41.

[73] S. auch *Welp,* Auskunftspflicht von Access-Providern, S. 11.

[74] S. auch *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 41.

[75] Zunächst kann über eine Whois-Abfrage bei der IANA ermittelt werden, welcher RIR zuständig ist, s. dazu https://www.iana.org/whois; S. zur Whois-Abfrage der für Europa zuständigen RIPE NCC https://apps.db.ripe.net/db-web-ui/query.

[76] S. *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 62; *Brüggemann,* Drittauskunftsanspruch, S. 50; *Welp,* Auskunftspflicht von Access-Providern, S. 27.

sich die IP-Adresse auch grob lokalisieren.[77] Bei statischen IP-Adressen lässt sich hierdurch gegebenenfalls sogar bereits der Endkunde, dem die IP-Adresse zugeteilt wurde, zurückverfolgen.[78]

2. Ermittlung des Anschlussinhabers durch den Access-Provider

Sofern die Rechteinhaber Kenntnis über die IP-Adresse und den zuständigen Access-Provider erlangt haben, besteht die Möglichkeit durch diesen den Inhaber des Anschlusses zurückzuverfolgen, von dem aus die IP-Adresse im Internet verwendet wurde.

Den Inhaber einer statischen IP-Adresse kann der Access-Provider bereits unmittelbar aus den Kundenbestandsdaten ermitteln, da statische IP-Adressen stets demselben Nutzer zugewiesen werden.[79]

Bei dynamischen IP-Adressen muss der Access-Provider darüber hinaus prüfen, welcher Anschlusskennung die IP-Adresse zum Zeitpunkt der Rechtsverletzung zugeteilt war. Über die Anschlusskennung lassen sich dann Name und Adresse des Anschlussinhabers zurückverfolgen. Die Voraussetzung hierfür ist, dass die Diensteanbieter in Logfiles protokollieren, welche IP-Adressen zu welcher Zeit an welche Anschlusskennung zugeteilt wurden.[80] Diese Anschlusskennung kann dann den Bestandsdaten (vor allem Name und Anschrift) des Kunden zugeordnet werden.[81]

V. Ermittlung des tatsächlich handelnden Nutzers

Durch die Auskunft des Access-Providers lässt sich lediglich der Inhaber eines Internetanschlusses ermitteln. Dadurch lässt sich aber noch keine Aussage darüber treffen, wer den Anschluss beziehungsweise den Rechner zum

---

[77] *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 62; *Schmidt/Pruß* in: Auer-Reinsdorff/Conrad, § 3 Rn. 136.

[78] S. *Welp,* Auskunftspflicht von Access-Providern, S. 27.

[79] *Sandor,* Datenspeicherung, Rn. 429; *Welp,* Auskunftspflicht von Access-Providern, S. 27 f.

[80] Vgl. *Brunst,* Anonymität im Internet, S. 159; *Welp,* Auskunftspflicht von Access-Providern, S. 27. S. auch *Wimmers* in: Schricker/Loewenheim, § 101 UrhG Rn. 106.

[81] S. auch *Welp,* Auskunftspflicht von Access-Providern, S. 27.

entsprechenden Zeitpunkt verwendet hat und von wem die Rechtsverletzung tatsächlich ausgeht.

1. Auseinanderfallen von Anschlussinhaber und Nutzer

In vielen Fällen herrscht keine Personengleichheit zwischen dem Anschlussinhaber und dem tatsächlich handelnden Nutzer, da auf einen Internetzugang oft mehrere Nutzer über verschiedene Endgeräte zugreifen können.[82]

Ein Grund dafür ist, dass durch die Verwendung von „Adress-Übersetzungen" mehrere Rechner nach außen unter derselben IP-Adresse in Erscheinung treten können.[83] Dafür erhält jeder Rechner eine private IP-Adresse, die an einer zentralen Stelle in eine öffentliche IP-Adresse „übersetzt" wird.[84] Dies kann etwa über einen Router in lokalen Netzwerken erfolgen.[85] Die private IP-Adresse muss im Gegensatz zu öffentlichen nicht weltweit einmalig sein.[86] Sie ist aber erforderlich, damit innerhalb des privaten Netzwerks die Datenpakete an die richtigen Zugangsgeräte weitergeleitet werden können.[87] Über den Access-Provider lässt sich aber lediglich die öffentliche IP-Adresse zum Anschlussinhaber zurückverfolgen.

Vor allem die WLAN-Nutzung ermöglicht es, dass eine Vielzahl von Personen denselben Anschluss zur Internetnutzung verwenden können. So benutzen bei privaten WLAN-Netzwerken häufig Familienangehörige oder Mitglieder einer Wohngemeinschaft einen gemeinsamen WLAN-Anschluss.[88] Bei ungesicherten offenen Netzwerken ist sehr leicht auch Außenstehenden ein Zugriff möglich.[89] Doch selbst wenn Schutzmaßnahmen getroffen werden, besteht die Gefahr eines unbefugten Zugriffs etwa durch einen Hacker.[90] Daneben lassen sich

---

[82] Vgl. *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 35.

[83] S. dazu *Brunst,* Anonymität im Internet, S. 52; *Brüggemann,* Drittauskunftsanspruch, S. 45 f.

[84] *Brunst,* Anonymität im Internet, S. 52.

[85] *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 42.

[86] *Brunst,* Anonymität im Internet, S. 52; *Brüggemann,* Drittauskunftsanspruch, S. 46.

[87] *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 42.

[88] Vgl. *Brunst,* Anonymität im Internet, 167; *Röhl/Bosch,* NJW 2008, 1415, 1419.

[89] *Grosskopf,* CR 2007, 122, 123; *Nietsch,* Anonymität und Durchsetzung, S. 78.

[90] S. dazu *Brunst,* Anonymität im Internet, S. 165 f.

öffentliche WLAN-Netzwerke meist von einem völlig unbegrenzten Personenkreis nutzen.[91]

2. Ermittlung des verwendeten Endgerätes und des Nutzers

Gegebenenfalls können das konkret verwendete Endgerät und damit häufig auch der tatsächliche Nutzer über die MAC-Adresse ermittelt werden.[92] Die MAC-Adresse (Media Access Control) ist ein in jedem internetfähigen Gerät in der Netzwerkkarte integrierter Code, der 6 Bytes lang ist und in der Regel weltweit einzigartig ist.[93] Theoretisch könnte also über die MAC-Adresse das Endgerät eindeutig identifiziert werden.[94] Die MAC-Adresse könnten Rechteinhaber gegebenenfalls vom Anbieter des zur Rechtsverletzung genutzten anwendungsbezogenen Dienstes ermitteln, der neben der IP-Adresse auch die MAC-Adresse des verwendeten Geräts speichern kann.[95] Daneben kann gegebenenfalls auch über den Internetanschluss Aufschluss über die MAC-Adresse gewonnen werden, da die MAC-Adresse innerhalb eines Netzwerks der Zuordnung von Datenpaketen an die jeweiligen Zugangsgeräte dient.[96] Allerdings existiert kein öffentliches Register, über das die MAC-Adressen zugeordnet werden können, sodass der Rechteinhaber damit erstmal nichts anfangen kann.[97] Zudem sind MAC-Adressen auch manipulierbar.[98] Das heißt, dass gegebenenfalls eine von der in der Netzwerkkarte vorgegebenen abweichende MAC-Adresse angezeigt wird.

---

[91] S. *LG Frankenthal*, Beschl. v. 6.3.2009 - 6 O 60/09, MMR 2009, 487, 488; *LG Kiel*, Beschl. v. 2.9.2009 – 2 O 221/09, ZUM 2009, 978, 979

[92] S. dzau etwa *Mantz,* Rechtsfragen offener Netze, S. 35.

[93] *Tanenbaum*, Computernetzwerke, S. 43 ff. S. auch *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S.35; *Sandor,* Datenspeicherung, Rn. 437.

[94] *Freiling/Heinson,* DuD 2009, 547, 548; *Sorge,* CR 2011, 273, 274.

[95] *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 61.

[96] *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 36; *Freiling/Heinson,* DuD 2009, 547, 548; *Nietsch,* Anonymität und Durchsetzung, S. 64; *Sorge,* CR 2011, 273, 274.

[97] *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 61; *Brunst,* Anonymität im Internet, S. 165. Ggf. lässt sich aber der Hersteller der Netzwerkschnittstelle ermitteln, s. *Alsbish,* DuD 2011, 482, 483 f.

[98] *Albish*, DuD 2011, 482, 484; *Brunst,* Anonymität im Internet, S. 165; *Mantz,* Rechtsfragen offener Netze, S. 36.

Theoretisch wäre es auch denkbar, das Zugangsgerät anhand der innerhalb des Netzwerks zugeteilten privaten IP-Adresse zurückzuverfolgen. Dazu müsste der Anschlussinhaber aber die vergebenen privaten IP-Adressen, sowie die an diese Adressen versendeten Datenpakete aufzeichnen und diese einem Zugangsgerät oder Nutzer zuordnen können, was mit einem erheblichen Aufwand verbunden wäre.[99]

Selbst für den Fall, dass ein konkretes Endgerät identifiziert werden kann, kann es schwierig sein, den Nutzer zu ermitteln, der das Gerät zum relevanten Zeitpunkt verwendet hat. So teilen sich in Familien und Wohngemeinschaften manchmal mehrere Personen dieselben Geräte.[100] Darüber hinaus haben in Büros und Computerräumen, in Schulen und Universitäten oft eine Vielzahl an Personen Zugriff auf dieselben Zugangsgeräte.[101] In Internetcafés lässt sich meist der Personenkreis, der ein Gerät verwendet haben könnte, überhaupt nicht mehr eingrenzen.[102]

In diesen Fällen ist eine technische Identifizierung des Nutzers oft nur noch schwer darstellbar. Eventuell befinden sich auf dem identifizierten Endgerät noch Daten im Browser-Cache über das Verhalten des Nutzers, die Aufschluss über dessen Identität geben.[103] Das ist zum Beispiel möglich, wenn der Nutzer sich mit persönlichen Daten in einem sozialen Netzwerk angemeldet hat.[104] Es wäre aber auch möglich herauszufinden, welcher Nutzer sich über einen WLAN-Hotspot einwählt, wenn eine Registrierung erfolgt.[105]

Ansonsten lässt sich die Identität des Nutzers aber nur noch durch dessen Verhalten, zum Beispiel durch die Befragung anderer gegebenenfalls anwesender Personen bestimmen. Handelt es sich um einen begrenzten Personenkreis –

---

[99] *Brunst,* Anonymität im Internet, S. 52.

[100] *Brunst,* Anonymität im Internet, S. 58 ff., 167.

[101] *Brunst,* Anonymität im Internet, S. 167.

[102] *Nietsch,* Anonymität und Durchsetzung, S. 77.

[103] *Brunst,* Anonymität im Internet, S. 61 ff.

[104] *Brunst,* Anonymität im Internet, S.60 ff.; *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 65.

[105] Dies erfolgt vor allem bei kommerziellen Hotspots zu Abrechnungszwecken; S. etwa *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 34 f.

zum Beispiel von Angehörigen einer Familie oder Wohngemeinschaft - lässt sich eventuell per Ausschlussprinzip der tatsächliche Nutzer ermitteln.

3. Besonderheiten bei iPv6-Adressen

Die zunehmende Verbreitung von iPv6-Adressen könnte gegebenenfalls zumindest die Ermittlung des verwendeten Zugangsgeräts erleichtern.[106] Dies gilt vor allem dann, wenn als Interface Identifier die MAC-Adresse des Gerätes verwendet werden würde. Durch die Kombination aus Netzwerk-Präfix und Interface Identifier können Rechnern, die in einem Netzwerk verbunden sind, jeweils eigene IP-Adressen zugeordnet werden.[107] So erhalten zwar – ähnlich dem iPv4-System - alle Rechner, die denselben Anschluss verwenden, dasselbe Netzwerk-Präfix vom Provider zugeteilt, allerdings kann jedem Rechner ein anderer Interface Identifier zugeordnet werden.[108] Dadurch würden nur noch die Personen unter derselben IP-Adresse in Erscheinung treten, die sich auch dasselbe Gerät teilen, aber nicht mehr diejenigen, die nur den selben Anschluss verwenden.[109]

Die Verwendung der MAC-Adresse als Interface Identifier würde zwar nicht unmittelbar eine Identifizierung des Endgeräts ermöglichen, allerdings wäre die Anonymität des Nutzers dadurch erheblich stärker eingeschränkt. Selbst wenn der Nutzer unterschiedliche Internetanschlüsse verwendet, behält er nämlich denselben Interface Identifier und es würde sich nur das Netzwerk-Präfix verändern.[110] Gibt der Nutzer zum Beispiel bei der Verwendung eines Internetdienstes seinen Namen und seine Adresse an, dann können diese Daten mit dem Interface Identifier in Verbindung gebracht werden.[111] Auch bei der Nutzung

---

[106] S. zu den iPv6-Adressen bereits oben unter Kap. 4 §4 A. III.

[107] *Freund/Schnabel,* MMR 2011, 495, 495; *Nietsch,* Anonymität und Durchsetzung, S. 68; *Wegener/Heidrich,* CR 2011, 479, 480.

[108] *Freund/Schnabel,* MMR 2011, 495, 495; *Nietsch,* Anonymität und Durchsetzung, S. 68; *Wegener/Heidrich,* CR 2011, 479, 480.

[109] *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 68 f.; *Dix/Petri,* DuD 2009, 531, 532; *Freund/Schnabel,* MMR 2011, 495, 495; *Hoeren,* ZRP 2010, 251, 253; *Nietsch*, Anonymität und Durchsetzung, S. 86.

[110] *Freund/Schnabel,* MMR 2011, 495, 495; *Nietsch*, Anonymität und Durchsetzung, S. 86; *Wegener/Heidrich,* CR 2011, 479, 480.

[111] S. *Nietsch,* Anonymität und Durchsetzung, S. 87.

eines anderen Dienstes lässt sich so bei gleichbleibendem Interface Identifier der Nutzer leichter zurückverfolgen.

Noch gravierender wären die Folgen für die Anonymität, wenn aufgrund der Vielzahl neuer Kombinationsmöglichkeiten von IP-Adressen auch das Netzwerk-Präfix der iPv6-Adresse vermehrt statisch vergeben werden würde, sodass einem Anschluss stets ein festes Präfix zugeteilt wird. Anders als bei einer dynamischen IP-Adresse wäre die Rückverfolgung in diesem Fall erheblich erleichtert, da es nicht mehr auf den Zeitpunkt der Verwendung der IP-Adresse ankäme. Zudem lassen sich bei einer statischen Vergabe von IP-Adressen, personenbezogene Daten, die bei unterschiedlichen Kommunikationsvorgängen im Internet anfallen, stets mit der IP-Adresse verknüpfen, sodass sämtliche Aktivitäten im Internet nachverfolgt werden könnten.[112]

Durch die Möglichkeit der statischen Vergabe und die Verknüpfung der IPv6-Adresse mit der MAC-Adresse könnte die Anonymität von Nutzern deshalb weitgehend ausgehebelt werden.[113] Allerdings ist weder die statische Vergabe des Präfixes, noch die Verwendung der MAC-Adresse als Interface Identifier zwingend. Anstelle der MAC-Adresse kann das Zugangsgerät auch eine zufällige Zahl erstellen, die sich nach dem Kommunikationsvorgang ändern kann.[114] Auch kann der Access-Provider das Netzwerk-Präfix weiterhin dynamisch vergeben, was vor allem für Privatkunden vorteilhaft wäre.[115] Für die Identifizierung würden iPv6-Adressen gegenüber dem iPv4-System dann den Rechteinhabern keinen Vorteil mehr bringen.[116]

---

[112] Vgl. *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 70; Vgl. auch die allgemeinen Ausführungen zu statischen IP-Adressen bei *Nietsch,* Anonymität und Durchsetzung, S. 74, 87.

[113] *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 70; *Freund/Schnabel,* MMR 2011, 495, 496 ff.; *Hoeren,* ZRP 2010, 251, 252 f.

[114] S. auch *Freund/Schnabel,* MMR 2011, 495, 496; *Nietsch,* Anonymität und Durchsetzung, S. 67, 87.

[115] Vgl. *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 69.

[116] Vgl. *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 69.

VI. Anonymisierungsdienste

Bereits die Ausführungen zum Auseinanderfallen von Anschlussinhaber und Nutzer machen deutlich, dass die Identifizierung der Nutzer mittels IP-Adresse an Grenzen stoßen kann. Noch verstärkt wird die Problematik, wenn die Nutzer ihre Identität durch die Verwendung von Anonymisierungsdiensten zusätzlich verschleiern. Der Zweck solcher Dienste besteht in der Regel darin, eine Rückverfolgung der bei der Internetnutzung notwendigerweise übertragenden IP-Adressen zum Nutzer zu verhindern.

1. Proxy-Server

Proxy-Server dienen in erster Linie dem schnelleren Zugriff auf Informationen aus dem Internetrecht, indem sie Informationen zwischenspeichern und bei einer erneuten Anfrage, diese aus dem Cache an einen Nutzer vermitteln können.[117] Teilweise bieten Proxy-Provider darüber hinaus Anonymisierungsdienstleistungen an, indem sie die Anfragen der Nutzer nicht nur weiterleiten, sondern verschlüsseln.[118] Wird über einen Proxy eine Webseite aufgerufen, dann erfolgt dies unter der IP-Adresse des Proxys und nicht mehr der des anfragenden Nutzers.[119]

Dennoch ließe sich die IP-Adresse zum Nutzer zurückverfolgen, wenn der Proxy-Betreiber die weitergeleiteten Anfragen protokolliert.[120] Häufig ist für die Nutzung eines Proxy-Servers auch eine vorherige Anmeldung nötig.[121] Erheblich schwieriger stellt sich die Identifizierung eines Nutzers aber dar, wenn stattdessen „offene Proxy-Server" verwendet werden und diese in Form von Mix-Kaskaden hintereinandergeschaltet werden.[122] In diesem Fall müssten für eine Rückverfolgung verschiedene Diensteanbieter auf Auskunft in Anspruch genommen werden oder eine technische Analyse oder Überwachung des

---

[117] S. oben unter Kap. 2 § 2 B. III.

[118] *Brunst,* Anonymität im Internet, S. 132 ff.

[119] *Brunst,* Anonymität im Internet, S. 133; *Nietsch,* Anonymität und Durchsetzung, S. 71.

[120] *Brunst,* Anonymität im Internet, S. 53, 133; *Nietsch,* Anonymität und Durchsetzung, S. 72.

[121] *Brunst,* Anonymität im Internet, S. 133; *Nietsch,* Anonymität und Durchsetzung, S. 72.

[122] *Brunst,* Anonymität im Internet, S. 134; *Nietsch,* Anonymität und Durchsetzung, S. 72.

Datenverkehrs von außen erfolgen.[123] Im Rahmen der privaten Rechtsdurchsetzung wird sich dies aber in aller Regel nicht realisieren lassen.

2. Zentrale Anonymisierungsdienste

Zentrale Anonymisierungsdienste wie JonDonym und AN.ON basieren ebenfalls auf hintereinandergeschalteten Proxy-Servern. JonDonym und AN.ON beruhen auf dem lokalen Proxy JAP (Java Anon Proxy).[124] Dieser leitet die Daten verschlüsselt an einen ersten Proxy (Mix), der den Ausgangspunkt einer festen Mix-Kaskade darstellt.[125] Die Rückverfolgung wäre dadurch nur möglich, wenn die Betreiber aller Mixe zusammenwirken.[126] Eine Identifizierung des Nutzers durch den Rechteinhaber ist daher in aller Regel ausgeschlossen, wenn der Nutzer auf einen solchen Anonymisierungsdienst zurückgreift.

3. Dezentrale Anonymisierungsdienste

Dasselbe gilt auch bei dezentralen Anonymisierungsdiensten wie „The Onion Router" (TOR). Anders als bei zentralen Diensten wie AN.ON werden die Daten nicht über zentrale, feste Mix-Kaskaden, sondern unter den Nutzern des TOR-Netzwerkes übermittelt.[127] Die zu übermittelden Informationen werden so verschlüsselt, dass jeder Knotenpunkt nur einen Teil der Informationen entschlüsseln kann und lediglich erkennen kann, wohin die Daten weiterzuleiten sind.[128] Den ursprünglichen Absender kennt nur der erste Knoten, für die anderen ist nur der vorherige Knotenpunkt erkennbar.[129] Erst der letzte Knoten erhält die Information, wer der Empfänger ist und den unverschlüsselten

---

[123] S. ausführlicher zu den Möglichkeiten einer Rückverfolgung des Datenverkehrs *Brunst,* Anonymität im Internet, S. 134 f.

[124] *Brunst,* Anonymität im Internet, S. 144. Der Java Anon Proxy entstammt einem Forschungsprojekt der Universitäten Dresden und Regensburg, S. dazu *Brüggemann,* Drittauskunftsanspruch, S. 43.

[125] *Brunst,* Anonymität im Internet, S. 144; *Brüggemann,* Drittauskunftsanspruch, S. 44.

[126] *Brunst,* Anonymität im Internet, S. 145; *Nietsch,* Anonymität und Durchsetzung, S. 69 f.

[127] Ausführlich zur Funktionsweise von TOR, S. *Brunst,* Anonymität im Internet, S. 138 ff.; *Thiesen,* MMR 2014, 803, 803.

[128] *Brunst,* Anonymität im Internet, S. 138; *Federrath/Pfitzmann*, DuD 1998, 628, 629 ff.

[129] *Brunst,* Anonymität im Internet, S. 138; *Brüggemann,* Drittauskunftsanspruch, S. 43.

Nachrichteninhalt.[130] Durch diese Verschlüsselung und die meist internationalen Routen für den Datenverkehr ist eine Nachverfolgung des Nutzers im Wege privater Rechtsdurchsetzung praktisch ausgeschlossen.[131]

E. Zusammenfassung Kapitel 4

Insgesamt zeigt sich, dass die Identifizierung anonymer Rechtsverletzer bereits unabhängig von der rechtlichen Problematik die Rechteinhaber vor erhebliche praktische Probleme stellen kann.

Als Beispiel lässt sich die Identifizierung des Nutzers eines sozialen Netzwerks anführen, der einen rechtsverletzenden Inhalt über die Plattform verbreitet hat: Am einfachsten wäre es für den Rechteinhaber in diesem Fall, wenn das soziale Netzwerk selbst über ausreichend Daten verfügen würde, um die Identität des Nutzers offenzulegen. Ist dies nicht der Fall, bleibt nur noch die Möglichkeit, die IP-Adresse des Nutzers zurückzuverfolgen. Dafür muss das soziale Netzwerk – bei einer dynamischen IP-Adresse – in den Log-Dateien die IP-Adresse und die Zugriffszeiten des Nutzers speichern. Mit diesen Informationen kann der Rechteinhaber den zuständigen Access-Provider ausfindig machen. Dieser muss dann prüfen, welchem Anschluss die fragliche IP-Adresse zum Zugriffszeitpunkt zugeordnet war. Auf diese Weise kann dann der Anschlussinhaber ermittelt werden. Anschließend gilt es den tatsächlich handelnden Nutzer ausfindig zu machen.

Im Wesentlichen bestehen also zwei verschiedene Möglichkeiten, die Identität eines anonymen Internetnutzers aufzudecken:
Zum einen können sich die Rechteinhaber direkt an die Anbieter von Anwendungsdiensten – wie E-Mail-Dienste, Webseiten oder Domainregistrare – wenden. Ob die Diensteanbieter Auskunft über die Identität des Rechtsverletzers geben können, hängt davon ab, welche Daten bei der Nutzung der Dienste angefallen sind und welche gegebenenfalls darüber hinaus – zum Beispiel bei einer Anmeldung oder Registrierung – erhoben werden. Auch wenn im Einzelfall auf diese Weise Name und Anschrift nicht unmittelbar ermittelt werden können,

---

[130] *Brunst,* Anonymität im Internet, S. 138.
[131] Vgl. *Brunst,* Anonymität im Internet, S. 143.

kann es für die Rechtinhaber hilfreich sein, so viele Informationen wie möglich zu erhalten, um die Wahrscheinlichkeit zu erhöhen, zum Beispiel anhand von E-Mail-Adressen oder Kontodaten den Nutzer doch noch zu identifizieren.

Zum anderen besteht die Möglichkeit, die Identität des Rechtsverletzers mittels der IP-Adresse aufzudecken. Dabei müssen oft mehrere Diensteanbieter in Anspruch genommen werden. Kann die IP-Adresse nicht selbstständig ermittelt werden, muss erst der Anbieter des Anwendungsdienstes Auskunft über die bei der Rechtsverletzung verwendete IP-Adresse erteilen. Bei einer dynamischen IP-Adresse muss zudem die Uhrzeit des Zugriffs protokolliert werden. Anschließend gilt es, den zuständigen Access-Provider zu ermitteln, der diese Informationen abgleichen und prüfen muss, welchem Anschluss die fragliche IP-Adresse zum Zugriffszeitpunkt zugeordnet war. Kann auf diese Weise der Anschlussinhaber ermittelt werden, steht damit noch nicht automatisch auch der tatsächliche Nutzer fest. Je mehr Personen zur fraglichen Zeit Zugriff auf denselben Internetanschluss hatten, desto schwieriger gestaltet sich dessen Identifizierung[132] Praktisch nicht mehr realisierbar ist die Rückverfolgung der IP-Adresse zudem, wenn der Nutzer einen Anonymisierungsdienst verwendet und dadurch seine IP-Adresse verschleiert hat.

---

[132] *Brunst,* Anonymität im Internet, S.159 ff. spricht deshalb von „anonymen Einstiegspunkten", wenn Öffentliche Netzwerke, offene WLAN-Netzwerke oder illegale Einstiegsmöglichkeiten verwendet werden.

Kapitel 5

Auskunftsansprüche gegen Internetdiensteanbieter de lege lata

Neben den eben erläuterten praktischen und technischen Schwierigkeiten stellt die Identifizierung eines anonymen Rechtsverletzers die Rechteinhaber auch vor nicht unerhebliche rechtliche Hürden.

Zur Ermittlung der Identität eines anonymen Rechtsverletzers sind die Rechteinhaber auf die Mithilfe der Diensteanbieter angewiesen. Daher müssen sie die Möglichkeit haben, Auskunft von den Diensteanbietern verlangen zu können. Die Identitätsermittlung durch die Rechteinhaber setzt dementsprechend voraus, dass im Falle einer Verletzung ihrer Rechte ein Auskunftsanspruch gegen die Diensteanbieter besteht und die Auskunftserteilung im Hinblick auf die datenschutzrechtlichen Vorschriften möglich und zulässig ist. Auf Grund der bei Internet-Sachverhalten häufig angelegten Problematik der grenzüberschreitenden Sachverhaltskonstellationen gilt es aber zunächst kollisionsrechtliche Fragen zu klären (A.). Anschließend sind die de lege lata existierenden verschiedenen Anspruchsgrundlagen (B.) sowie der Konflikt mit den Regelungen des Datenschutzes (C.) und die prozessualen Rahmebedingungen der Auskunftsansprüche (D.) zu untersuchen und jeweils miteinander zu vergleichen (E.). Aus der Gesamtbetrachtung ergeben sich anschließend die de lege lata existierenden rechtlichen Möglichkeiten der Auskunftserteilung. (F.)

A. Kollisionsrecht

Rechtsverletzungen im Internet sind ein globales Phänomen. Inhalte im Internet sind grundsätzlich weltweit abrufbar. Rechteinhaber und Nutzer können aus verschiedenen Staaten stammen. Diensteanbieter haben ihren Sitz oft im Ausland und verletzende Handlungen können sich in unterschiedlichen Staaten auswirken. Deswegen stellt sich regelmäßig die Frage, ob die Diensteanbieter

nach deutschem materiellem Recht auf Auskunft in Anspruch genommen werden können und ob die nationalen Gerichte für ein solches Auskunftsbegehren zuständig sind.

I. Anwendbarkeit des deutschen Rechts

Die zu untersuchenden Auskunftsansprüche gegen Internetdiensteanbieter stützen sich auf die Verletzung absoluter Rechte durch deren Nutzer.[1] Maßgeblich für diese Arbeit sind daher in erster Linie die kollisionsrechtlichen Regelungen für Ansprüche aus unerlaubter Handlung.[2]

Das anwendbare materielle Recht ergibt sich dementsprechend grundsätzlich aus Art. 4 Rom II-VO. Art. 4 Abs. 1 Rom II-VO sieht vor, dass das Recht des Staates anzuwenden ist, in dem der Schaden eingetreten ist. Entscheidend ist demnach der Erfolgsort, an dem das geschützte Rechtsgut verletzt worden ist. Art. 4 Abs. 2 Rom II-VO normiert eine Ausnahme für den Fall, dass Schädiger und Geschädigter ihren gewöhnlichen Aufenthalt in demselben Staat haben. In diesem Fall ist das Recht dieses Staates anzuwenden. Zu einer Abweichung vom Grundsatz des Erfolgsortes kommt es nach Art. 4 Abs. 3 Rom II-VO außerdem, wenn sich aus den Umständen ergibt, dass eine unerlaubte Handlung eine engere Verbindung zu einem anderen Staat aufweist.[3] Zudem besteht gemäß Art. 14 Abs. 2 Rom II-VO für die Parteien die Möglichkeit der Rechtswahl.

Für einzelne Deliktstypen existieren aber Sonderregelungen, die von den Regelungen des Art. 4 Rom II-VO variieren.[4] So sind Persönlichkeitsrechtsverletzungen nach Art. 1 Abs. 2 lit. g) Rom II-VO vom Anwendungsbereich der Rom II-VO ausgenommen, sodass weiterhin die Vorschriften der Art. 40-42 EGBGB gelten.[5] Art. 40 Abs. 1 S. 1 EGBGB orientiert sich anders als Art. 4 Rom II-VO

---

[1] Vgl. *OLG Köln*, Urt. v. 25.3.2011 - 6 U 87/10, GRUR-RR 2011, 305, 305 – Schweizer Sharehoster.

[2] S. etwa *OLG Köln,* Urt. v. 25.3.2011 - 6 U 87/10, GRUR-RR 2011, 305, 305 – Schweizer Sharehoster; *OLG München,* Urt. v. 17.11.2011 – 29 U 3496/11, ZUM-RD 2012, 88, 91 jeweils zum Anspruch aus § 101 UrhG. S. zu § 19 MarkenG *BGH,* Urt. v. 12.1.2017 – I ZR 253/14, GRUR 2017, 397, 397 – World of Warcraft II.

[3] *Hoeren* in: Hoeren/Sieber/Holznagel, Teil 18.2 Rn. 152.

[4] Vgl. auch *Hoeren* in: Hoeren/Sieber/Holznagel, Teil 18.2 Rn. 153.

[5] *Bach* in: Spindler/Schuster, Art. 40 EGBGB Rn. 1.

grundsätzlich nicht am Erfolgs- sondern am Handlungsort.[6] Als Handlungsort ist der Ort zu verstehen, an dem der Ersteller die Informationen ins Internet hochgeladen hat. Dabei kann es sich etwa um den Wohnort eines Rechtsverletzers handeln.[7] Alternativ kann der Verletzte nach Art. 40 Abs. 1 S. 2 EGBGB aber auch auswählen, dass das Recht des Staates angewandt wird, in dem der Erfolgsort liegt.[8] Ähnlich wie bei Art. 4 Rom II-VO gibt es auch hier Ausnahmen in Art. 40 Abs. 2 und Art. 41 EGBGB, sowie die Möglichkeit einer Rechtswahl nach Art. 42 EGBGB.

Besonderheiten gelten auch bei Verletzungen des geistigen Eigentums. Hier greift gemäß Art. 8 Abs. 1 Rom II-VO das Schutzlandprinzip, nach dem das Recht des Staates anzuwenden ist, für den der Schutz begehrt wird.[9] Den Ausgangspunkt für das Schutzlandprinzip bildet das Territorialitätsprinzip.[10] Demnach ist der Schutz zum Beispiel des Urheber- oder Markenrechts auf das jeweilige Territorium eines Staates begrenzt.[11] Der Schutz des deutschen Rechts wirkt entsprechend nur in Bezug auf Handlungen, die in Deutschland begangen wurden.[12] Es bedarf also für die Anwendbarkeit des deutschen Rechts eines hinreichenden Inlandsbezugs der Handlung.[13]

---

[6] Vgl. etwa *Bach* in: Spindler/Schuster, Art. 40 EGBGB Rn. 4; *Hoeren* in: Hoeren/Sieber/Holznagel, Teil 18.2 Rn. 154.

[7] *Hoeren* in: Hoeren/Sieber/Holznagel, Teil 18.2 Rn. 155.

[8] S. zur Problematik der Ermittlung des Erfolgsortes bei Persönlichkeitsrechtsverletzungen im Internet etwa *Hoeren* in: Hoeren/Sieber/Holznagel, Teil 18.2 Rn. 155; *Spickhoff* in: BeckOK BGB, Art. 40 EGBGB Rn. 26, 39.

[9] S. etwa *OLG Frankfurt am Main*, Urt. v. 30.4.2019 – 11 U 27/18, ZUM-RD 2019, 532, 535; *LG München I,* Urt. v. 20.2.2019 – 37 O 5140/18, ZUM 2019, 602, 604; *Grünberger* in: NK-BGB VI, Art. 8 Rom II-VO Rn. 37.

[10] *McGuire* in: BeckOGK, Art. 8 Rom II-VO Rn. 29 f. S. auch *BGH,* Urt. v. 21.4.2016 – I ZR 43/14, GRUR 2016, 1048 Rn. 24 - An Evening with Marlene Dietrich.

[11] *OLG München*, Urt. v. 1.10.2009 - 29 U 2462/09, GRUR-RR 2010, 157, 157.

[12] *OLG Frankfurt am Main*, Urt. v. 30.4.2019 – 11 U 27/18, ZUM-RD 2019, 532, 535; *Grünberger* in: NK-BGB, Art. 8 Rom II-VO Rn. 40 ff.; *Hoeren* in: Hoeren/Sieber/Holznagel, Teil 18.2 Rn. 156.

[13] *Hoeren* in: Hoeren/Sieber/Holznagel, Teil 18.2 Rn. 157. S. etwa zur Problematik der Bestimmung des Handlungsortes bei Urheberrechtsverletzungen *EuGH*, Urt. v. 22.1.2015 – C-441/13, GRUR 2015, 296, 298 - Hejduk; *BGH,* Urt. v. 29.4.2010 - I ZR 69/08, GRUR 2010, 628, 628 – Vorschaubilder I. S. zur Bestimmung des Handlungsortes bei Markenrechtsverletzungen etwa *BGH,* Urt. v. 12.1.2017 – I ZR 253/14, GRUR 2017, 397, 397 – Worl of Warcraft

Die Anwendbarkeit des materiellen Datenschutzrechts ergibt sich aus Art. 3 DS-GVO beziehungsweise hinsichtlich der auch nach Einführung der DS-GVO noch geltenden nationalen Bestimmungen aus § 1 Abs. 2 TKG, § 1 Abs. 3 TTDSG oder § 1 Abs. 4 BDSG.[14]

Neben den Kollisionsregeln kann auch das in § 3 TMG geregelte Herkunftslandprinzip relevant werden. § 3 TMG dient der Umsetzung von Art. 3 ECRL. Das Ziel des europäischen Gesetzgebers bestand darin, für Diensteanbieter mit Sitz in einem EU-Mitgliedstaat einen möglichst sicheren Rechtsrahmen zu schaffen.[15] Das Herkunftslandprinzip sieht dementsprechend vor, dass für Telemediendiensteanbieter mit Sitz in einem Mitgliedstaat der Europäischen Union vorrangig das Recht dieses Staates zu beachten ist.[16] Hierbei handelt es sich aber nicht um eine echte Kollisionsnorm, sondern um ein sachrechtliches Beschränkungsverbot.[17] Außerdem findet das Herkunftslandprinzip nach § 3 Abs. 4 Nr. 6 TMG keine Anwendung im Urheberrecht, auf verwandte Schutzrechte, im Halbleiterschutzrecht und auf gewerbliche Schutzrechte. Jedenfalls kann die Anwendbarkeit des deutschen Rechts in vielen Fällen erreicht werden.

Auch wenn die Bestimmung des anzuwendenden Rechtsrahmens im Einzelfall schwierige Abgrenzungsfragen aufwerfen kann, setzt die vorliegende Arbeit die Anwendbarkeit des deutschen materiellen Rechts als gegeben voraus.

II; *BGH,* Urt. v. 13.10.2004 - I ZR 163/02, NJW 2005, 1435, 1436 – Hotel Maritime; *OLG Düsseldorf,* Beschl. v. 22.4.2008 - I-20 U 93/07, MMR 2008, 748, 748; *OLG München,* Urt. v. 16.6.2005 - 29 U 5456/04, CR 2006, 347, 348.

[14] S. ausführlich zum anwendbaren Recht im Datenschutz und insbesondere zu den Strukturprinzipien dessen IPR *Oster,* ZEuP 2021, 275, 275 ff. m.w.N. S. zu § 1 Abs. 1I TTDSG etwa *Ettig* in: Taeger/Gabel, § 1 TTDSG Rn. 16 ff.

[15] Vgl. Erwägungsgrund 22 der ECRL.

[16] Ausführlich zum Herkunftslandprinzip und der Umsetzungsnorm des § 3 TMG, S. etwa *Spindler* in: Spindler/Schmitz, § 3 TMG Rn. 1ff.

[17] S. etwa *BGH*, Urt. v. 14.1.2020 – VI ZR 496/18, NJW 2020, 1587, 1588; *BGH*, Urt. v. 14.1.2020 – VI ZR 496/18, GRUR 2020, 435 Rn. 25 – yelp.de; *BGH*, Urt. v. 27.2.2018 – VI ZR 489/16, NJW 2018, 2324 Rn. 23; *BGH*, Urt. v. 8.5.2012 – VI ZR 217/08, NJW 2012, 2197, 2197; *Spickhoff* in: BeckOK BGB, Art. 40 EGBGB Rn. 5; *Spindler* in: Spindler/Schmitz, § 3 TMG Rn. 18 ff. jeweils m.w.N.

II. Internationale Zuständigkeit deutscher Gerichte

Ebenso wird von der internationalen Zuständigkeit deutscher Gerichte ausgegangen. Sofern Diensteanbieter aus EU-Mitgliedstaaten auf Auskunft in Anspruch genommen werden sollen, richtet sich die internationale Zuständigkeit nach der EuGVVO. Diensteanbieter mit Sitz in einem anderen Mitgliedstaat können nach Art. 5 Abs. 1 EuGVVO grundsätzlich nur vor Gerichten dieses Staates verklagt werden.

Eine besondere Zuständigkeit für Ansprüche aus unerlaubter Handlung ergibt sich aber aus Art. 7 Nr. 2 EuGVVO. Demnach kann ein Diensteanbieter auch in dem Staat verklagt werden, an dem das schädigende Ereignis eingetreten ist.[18] Dabei reicht es aus, wenn eine unerlaubte Handlung den Gegenstand des Verfahrens bildet.[19] Art. 7 Nr. 2 EuGVVO umfasst deshalb nicht nur Schadensersatzansprüche, sondern auch Beseitigungs- und Unterlassungsansprüche.[20] Auch Auskunftsansprüche fallen unter diese Vorschrift, wenn sie an eine unerlaubte Handlung anknüpfen.[21] Dabei genügt es für die Gerichtszuständigkeit, wenn eine Verletzung behauptet wird, die nicht von vornherein ausgeschlossen werden kann.[22] Zudem fallen Auskunftsklagen gegen Diensteanbieter auch

---

[18] Der Kläger hat ein Wahlrecht zwischen dem Ort der Verwirklichung des Schadenserfolgs und dem Ort des für den Schadenseintritt ursächlichen Geschehens, S. *EuGH,* Urt. v. 5.6.2014 – C-360/12, GRUR 2014, 806 – Coty/First Note. S. zur Bestimmung des Erfolgsortes noch zu Art. 5 Nr. 3 EuGVVO a.F. *EuGH,* Urt. v. 25.10.2011 - C-509/09, GRUR 2012, 300 Rn. 48 – eDate Advertising; *EuGH,* Urt. v. 19.4.2012 - C-523/10, GRUR 2012, 654 Rn. 22 – Wintersteiger/Products 4U; *EuGH,* Urt. v. 22.1.2015 – C-441/13, GRUR 2015, 296 Rn. 24 ff. - Hejduk.

[19] S. noch zu Art. 5 Nr. 3 Brüssel-I-VO BGH, Urt. v. 27.11.2014 – I ZR 1/11, GRUR 2015, 689 Rn. 25 – Parfumflakon II.

[20] *BGH,* Urt. v. 18.7.2008 - V ZR 11/08, NJW 2008, 3502, 3503; *BGH,* Urt. v. 24.10.2005 - II ZR 329/03, NJW 2006, 689, 689; *BGH,* Urt. v. 13.10.2004 - I ZR 163/02, GRUR 2005, 431, 432 – Hotel Maritime; *Stadler* in: Musielak/Voit, Art. 7 EuGVVO Rn. 17.

[21] S. für akzessorische Auskunftsansprüche *BGH,* Urt. v. 27.11.2014 – I ZR 1/11, GRUR 2015, 689 Rn. 26 – Parfumflakon II; *BGH*, Urt. v. 24.9.2014 – I ZR 35/11, GRUR 2015, 264 Rn. 15 – Hi Hotel II. S. zu § 101 UrhG *LG Hamburg,* Urt. v. 7.7.2016 – 308 O 126/16, ZUM-RD 2017, 561, 563; S. auch *Stadler* in: Musielak/Voit, Art. 7 EuGVVO Rn. 17. S. auch zu Art. 5 Nr. 3 LugÜ *OLG Köln*, Urt. v. 25.3.2011 - 6 U 87/10, GRUR-RR 2011, 305 – Schweizer Sharehoster.

[22] *BGH,* Urt. v. 8.3.2012 - I ZR 75/10, GRUR 2012, 621 Rn. 18 – Oscar; *BGH,* Urt. v. 13.10.2004 - I ZR 163/02, GRUR 2005, 431, 432 – Hotel Maritime; *BGH,* 30.3.2006 - I ZR

dann unter Art. 7 Nr. 2 EuGVVO, wenn die rechtsverletzende Handlung nicht durch diese selbst, sondern durch deren Nutzer erfolgt.[23] Diensteanbieter können demnach vor nationalen Gerichten auf Auskunft über ihre rechtsverletzenden Nutzer in Anspruch genommen werden.

Die EuGVVO greift außerdem auch bei Verfahren, in denen im Vorfeld der Auskunftserteilung eine richterliche Gestattungsanordnung beantragt wird.[24] Da auch in Gestattungsverfahren die unerlaubte Handlung Gegenstand des Verfahrens ist, ist ebenfalls Art. 7 Nr. 2 anwendbar.[25] Jedenfalls kann aber eine rügelose Einlassung nach Art. 26 EuGVVO zur Zuständigkeit des nationalen Gerichts führen.[26]

Bei Diensteanbietern mit Sitz außerhalb der europäischen Union gelten die Regelungen des autonomen nationalen Zuständigkeitsrechts. Die Regelung zur örtlichen Zuständigkeit im autonomen deutschen Recht erfüllen eine Doppelfunktion, da aus ihr zusätzlich die internationale Zuständigkeit abgeleitet wird. Ähnlich wie bei Art. 7 Nr. 2 EuGVVO gilt für die Auskunftsansprüche gegen Internetdiensteanbieter der besondere Gerichtsstand für unerlaubte Handlungen nach § 32 ZPO.[27] Daneben existieren spezielle Sonderregelungen für

---

24/03, GRUR 2006, 513, 513 – Arzneimittelwerbung im Internet; *BGH,* Urt. v. 15.2.2007 - I ZR 114/04, GRUR 2007, 871, 871 – Wagenfeld-Leuchte; *BGH,* Urt. v. 12.12.2013 – I ZR 131/12, GRUR 2014, 601 Rn. 17 – Englischsprachige Pressemitteilung; S. auch *EuGH,* Urt. v. 19.4.2012 - C-523/10, GRUR 2012, 654, 654 – Wintersteiger; *EuGH*, Urt. v. 3.4.2014 – C-387/12, GRUR 2014, 599, 599 – Hi Hotel/Spoering.

[23] Anders aber bei Art. 97 Gemeinschaftsmarkenverordnung (Verordnung (EG) Nr. 207/2009 des Rates vom 26. Februar 2009 über die Gemeinschaftsmarke), die eine eigene Verletzungshandlung voraussetzt.

[24] So auch zu § 14 Abs. 3-5 TMG a.F. *BGH,* Beschl. v. 24.9.2019 – VI ZB 39/18, GRUR 2020, 101, Rn. 15 ff. – Facebook-Messenger. A.A. aber im Hinblick auf das Verfahren nach § 101 Abs. 9 UrhG *OLG München*, Beschl. v. 12.9.2011 - 29 W 1634/11, GRUR-RR 2012, 228, 229 – Englischer Provider; Kritisch zur Entscheidung des OLG München aber *Eifinger*, GRUR-Prax 2011, 474, 474 f.

[25] A.A. aber wohl *OLG München*, Beschl. v. 12.9.2011 - 29 W 1634/11, GRUR-RR 2012, 228, 229 – Englischer Provider.

[26] S. *BGH,* Beschl. v. 24.9.2019 – VI ZB 39/18, GRUR 2020, 101, Rn. 15 ff. – Facebook-Messenger.

[27] S. zur Anwendbarkeit von § 32 ZPO auf Auskunftsansprüche *OLG Düsseldorf*, Urt. v. 30.05.1958 - 2 U 166/57, GRUR 1959, 540, 541 – CAMAY-Seife; *Heinrich* in: Musielak/Voit,

bestimmte Auskunftsverfahren: Im Gestattungsverfahren nach § 14 Abs. 3-5 TMG ist nach § 14 Abs. 4 S. 4 TMG das Gericht zuständig, in dem der Verletzte seinen Sitz, Niederlassung oder Wohnsitz hat.[28] Eine Ausnahme gilt auch bei Verfahren über die Zulässigkeit der Verkehrsdatenauskunft etwa nach § 101 Abs. 9 UrhG oder § 19 Abs. 9 MarkenG. Nach Absatz 9 S. 2 der Auskunftsansprüche im Bereich des geistigen Eigentums ist das Gericht ausschließlich zuständig, in dem der auskunftspflichtige Diensteanbieter seinen Sitz, Wohnsitz oder eine Niederlassung hat.

B. Anspruchsgrundlagen

Die Rechteinhaber sind zur Identifizierung anonymer Rechtsverletzer sehr oft auf eine Auskunft durch die Diensteanbieter angewiesen. De lege lata können sich Rechteinhaber für ihre Auskunftsbegehren auf die speziellen Auskunftsansprüche im Bereich des geistigen Eigentums, auf § 21 Abs. 2 S. 2 TTDSG oder auf den allgemeinen aus § 242 BGB abgeleiteten Auskunftsanspruch stützen.

I. Auskunftsansprüche zur Durchsetzung der Rechte des geistigen Eigentums

Zu den wichtigsten Regelungen für Auskunftsansprüche gegen Internetdiensteanbieter gehören die im Zuge der Umsetzung der Enforcement-Richtlinie (RL 2004/48/EG) in § 101 UrhG, § 140b PatG, § 24b GebrMG, § 19 MarkenG, § 46 DesignG, § 37b SortG und § 9 Abs. 2 HalblSchG eingeführten Regelungen.[29] Es handelt sich hierbei um Parallelvorschriften, die in Wortlaut und

---

§ 32 ZPO Rn. 14; *Toussaint* in BeckOK ZPO, § 32 ZPO Rn. 5. S. auch zu Art. 5 Nr. 3 LuGÜ 1988 *BGH,* Urt. v. 28.6.2007 - I ZR 49/04, NJW-RR 2008, 57 Rn. 24 – Cambridge Institute. S. zu § 101 UrhG gegen lediglich als Störer haftende Diensteanbieter *OLG München*, Urt. v. 17.11.2011 – 29 U 3496/11, ZUM-RD 2012, 88, 91. S. zum notwendigen Inlandsbezug bei § 32 ZPO *BGH,* Beschl. v. 10.11.2009 - VI ZR 217/08, GRUR 2010, 261, 264 – Autocomplete-Funktion.

[28] Zur Anwendbarkeit der EuGVVO beim Gestattungsverfahren nach § 14 Abs. 3-5 TMG S. *BGH,* Beschl. v. 24.9.2019 – VI ZB 39/18, GRUR 2020, 101 Rn. 15 ff. – Facebook-Messenger.

[29] § 9 Abs. 2 HalblSchG verweist dabei lediglich auf die Regelung des § 24b GebrMG.

Aufbau weitgehend identisch sind, weswegen deren Voraussetzungen und Rechtsfolgen im Folgenden gemeinsam untersucht werden.

1. Drittauskunftsanspruch nach Absatz 2

Der erste Absatz dieser Normen enthält jeweils einen nicht akzessorischen Auskunftsanspruch gegen einen Verletzer auf Herkunft und Vertriebswege der rechtsverletzenden Erzeugnisse. Voraussetzung für diesen Anspruch ist eine Verletzung des Urheberrechts oder verwandter Schutzrechte in gewerblichem Ausmaß. Demgegenüber kann nach dem zweiten Absatz auch ein Dritter, der Nicht-Verletzer ist, auf die entsprechende Auskunft in Anspruch genommen werden. Ein Ziel des Gesetzgebers war es unter anderem, durch den zweiten Absatz einen Auskunftsanspruch gegen Internet-Diensteanbieter zu schaffen, durch den die betroffenen Rechteinhaber Auskunft über die Identität eines Rechtsverletzers im Internet erhalten können.[30]

Aus diesem Grund sollen im Folgenden zunächst die Voraussetzungen und Rechtsfolgen des Drittauskunftsanspruchs nach Absatz 2 untersucht werden. Die Ausführungen konzentrieren sich dabei darauf, inwieweit den Rechteinhabern ein Anspruch gegen Internet-Diensteanbieter zur Ermittlung der Identität eines Rechtsverletzers gewährt wird.

a) Aktiv- und Passivlegitimation

Aktivlegitimiert für den Auskunftsanspruch sind die Rechteinhaber. Passivlegitimiert sind die in Absatz 2 S. 1 Nr. 1-4 abschließend aufgezählten Personen. Für Internet-Diensteanbieter ist Absatz 2 S. 1 Nr. 3 maßgeblich. Zur Auskunft verpflichtet ist demnach, wer für rechtsverletzende Tätigkeiten genutzte Dienstleistungen erbringt. Der Begriff der Dienstleistung ist dabei weit und nicht im Sinne der §§ 611 ff. BGB zu verstehen.[31] Es werden alle Diensteanbieter der Informationsgesellschaft erfasst, sofern diese Tätigkeiten erbringen, die für rechtsverletzende Zwecke genutzt werden.[32]

---

[30] Ergibt sich etwa aus *Regierungsentwurf,* BT-Drs. 16/5048, 39, 49.

[31] Vgl. *Spindler* in: Spindler/Schuster, § 101 UrhG Rn. 7; *Spindler,* ZUM 2008, 640, 644.

[32] *Spindler,* ZUM 2008, 640, 644; S. zum Beispiel zu Sharehostern *BGH*, Beschl. v. 20.9.2018 – I ZR 53/17, GRUR 2018, 1239, 1239 – uploaded; *OLG Köln,* Urt. v. 25.3.2011 – 6 U 87/10, ZUM-RD 2011, 350, 350.

Genau in dieser Einschränkung liegt aber bereits das erste Problem des Drittauskunftsanspruchs: Gegebenenfalls ist es zur Identifizierung eines Nutzers erforderlich, auch eine Auskunft bei einem Diensteanbieter einzuholen, dessen Dienst nicht für die Rechtsverletzung, sondern lediglich anderweitig genutzt wird. Verbreitet ein Nutzer zum Beispiel urheberrechtlich geschütztes Material auf einer Plattform, dann nutzt er dafür jedenfalls den Dienst eines Host-Providers und eines Zugangsanbieters. Bei der Nutzung dieser Dienste besteht daher ein Zusammenhang der Nutzung mit der Rechtsverletzung. Kann der Betreiber der Plattform dem verletzten Rechteinhaber lediglich Auskunft über eine Mailadresse erteilen, könnte gegebenenfalls der E-Mail-Anbieter den Nutzer identifizieren. Dessen Dienst wurde allerdings nicht zur Rechtsverletzung genutzt, sodass kein Auskunftsanspruch besteht. Auch eine analoge Anwendung des Auskunftsanspruches scheidet in diesem Fall aus, da die Interessenslage nicht vergleichbar ist. Schließlich hat der Anbieter des E-Mail-Dienstes – anders als der Betreiber der Plattform und der Zugangsanbieter – die Rechtsverletzung durch die Erbringung seines Dienstes nicht ermöglicht.

Ein Vorteil für die Rechteinhaber könnte aber darin bestehen, dass der Auskunftsanspruch nicht auf Internetdienste beschränkt ist. So sind etwa auch Auskünfte von Zahlungsdienstleistern denkbar, wenn ein Nutzer zur finanziellen Abwicklung von Rechtsverletzungen Zahlungsinformationen angegeben hat.[33]

b) Offensichtlichkeit der Rechtsverletzung

Der Anspruch auf Drittauskunft besteht nach Absatz 2 nur bei Offensichtlichkeit der Rechtsverletzung oder wenn der Verletzte gegen den Verletzer Klage erhoben hat. Ist die Identität des Verletzers nicht bekannt, ist eine Klageerhebung nach deutschem Recht ausgeschlossen, da eine Bezeichnung der Parteien nach § 253 Abs. 2 Nr. 1 ZPO nicht möglich ist. Daher greift der Auskunftsanspruch aus § 101 Abs. 2 UrhG bei anonymen Rechtsverletzungen im Internet nur bei einer offensichtlichen Rechtsverletzung.

Absatz 2 soll einen Auskunftsanspruch also auch dann ermöglichen, wenn die Person, von der Auskunft begehrt wird, nicht selbst Rechtsverletzer ist und der

---

[33] *LG Hamburg,* Urt. v. 22.3.2017 – 308 O 480/16, MMR 2018, 114, 115; *LG Hamburg,* Urt. v. 7.7.2016 – 308 O 126/16, ZUM-RD 2017, 561, 563.

eigentliche Rechtsverletzer erst ermittelt werden soll.[34] Um das zu ermöglichen, ist der Anspruch aus Absatz 2 im Unterschied zu Absatz 1 auf offensichtliche Rechtsverletzungen beschränkt. Ursächlich dafür ist die Befürchtung, der Dritte – hier der Diensteanbieter – könnte bei unklarer Rechtslage zu Unrecht mit Auskunftsersuchen belastet werden.[35] Insbesondere soll der Diensteanbieter nicht das Risiko einer Fehlbeurteilung tragen müssen und daher nur bei offensichtlichen Rechtsverletzungen zur Auskunft verpflichtet sein.[36] Die Rechtsverletzung müsse deshalb so eindeutig sein, dass eine ungerechtfertigte Belastung des Dritten ausgeschlossen ist.[37]

aa) Auslegung des Merkmals

Zur Auslegung des Merkmals der Offensichtlichkeit wird meist auf die Regelungen in Absatz 7 verwiesen, die nicht nur auf den Drittauskunftsanspruch, sondern auch auf den Anspruch aus Absatz 1 anwendbar ist. Absatz 7 sieht für die Durchsetzung der Auskunftsansprüche im Wege des einstweiligen Rechtsschutzes ebenfalls das Kriterium der Offensichtlichkeit der Rechtsverletzung vor.[38]

Die Offensichtlichkeit der Rechtsverletzung wird unter Berücksichtigung der Interessen des Diensteanbieters beurteilt. Dementsprechend ist eine Rechtsverletzung offensichtlich, wenn für den Dritten ohne weitere Nachforschung in rechtlicher und tatsächlicher Hinsicht keine Zweifel an der Rechtswidrigkeit der Verletzungshandlung bestehen.[39] Die Verletzung muss so eindeutig sein, dass eine ungerechtfertigte Belastung des Dritten ausgeschlossen ist.[40] Zweifel in tatsächlicher oder rechtlicher Hinsicht schließen die Offensichtlichkeit daher aus.[41]

---

[34] Dies ergibt sich etwa aus *Regierungsentwurf,* BT-Drs. 16/5048, S.39.

[35] Hierzu etwa *LG Hamburg,* Urt. v. 11.3.2009 - 308 O 75/09, MMR 2009, 570, 571; *Meckel* in: Dreyer/Kotthoff/Meckel/Hentsch, § 101 UrhG Rn. 6. S. auch *Regierungsentwurf*, BT-Drs. 16/5048, 39.

[36] Vgl. *Welp*, Auskunftspflicht von Access-Providern, S. 156.

[37] *Regierungsentwurf*, BT-Drs. 16/5048, S.39.

[38] So etwa *Weidert/Molle* in: Ensthaler/Weidert, Kap. 7 Rn. 374.

[39] Vgl. *Welp*, Auskunftspflicht von Access-Providern, S. 162.

[40] *Regierungsentwurf,* BT-Drs. 16/5048, S.39; *OLG Karlsruhe,* Beschl. v. 1.9.2009 - 6 W 47/09, GRUR-RR 2009, 379, 382; *LG Köln,* Beschl. v. 17.12.2008 – 38 OH 8/08, ZUM 2009, 334, 334.

[41] *Regierungsentwurf,* BT-Drs. 16/5048, S.39.

bb) Kritik an der Beschränkung des Drittauskunftsanspruchs auf offensichtliche Rechtsverletzungen

Problematisch ist allerdings, dass die Offensichtlichkeit im Rahmen von Absatz 2 eine andere Funktion hat als in Absatz 7.[42] Die Einschränkung hinsichtlich der Offensichtlichkeit der Rechtsverletzung soll im Hinblick auf die einstweilige Verfügung unterschiedliche Ergebnisse im Eil- und im Hauptsacheverfahren vermeiden.[43] Dagegen besteht der Anspruch aus § 101 Abs. 2 UrhG überhaupt nur bei einer offensichtlichen Rechtsverletzung.

Die generelle Beschränkung des Drittauskunftsanspruchs auf offensichtliche Rechtsverletzungen kann den Rechteinhabern erhebliche Schwierigkeiten bereiten. Sofern die Rechtsverletzung nicht offensichtlich ist, wird die Identifizierung und damit auch die Rechtsdurchsetzung gegen den Verletzer auf dem Zivilrechtsweg in vielen Fällen unmöglich.

Der Rechteinhaber ist aber bei einer nicht offensichtlichen Rechtsverletzung nicht automatisch auch weniger schutzwürdig. So ergeben sich durch die Offensichtlichkeit einer Rechtsverletzung keine Anhaltspunkte zu deren Schwere. Beispielsweise kann einer Rechtsverletzung, die einen hohen wirtschaftlichen Schaden verursacht, ein sehr komplexer Sachverhalt zu Grunde liegen, der an den Anforderungen der Offensichtlichkeit scheitert. Es kann daher nicht überzeugen, die Möglichkeit der Identifizierung des Rechtsverletzers mittels Auskunftsanspruch an der Offensichtlichkeit der Rechtsverletzung festzumachen.

Das Ziel des Gesetzgebers war es, einen Drittauskunftsanspruch noch vor Klageerhebung und gerade auch zur Identifizierung des Verletzers zu schaffen.[44] Durch das Merkmal der Offensichtlichkeit der Rechtsverletzung besteht die Gefahr, bestimmte Fallkonstellationen von dieser Möglichkeit gänzlich auszuschließen.

Dazu kommt, dass die Auskunftserteilung bei Urheberrechtsverletzungen durch Zugangsanbieter häufig nur unter Verwendung von Verkehrsdaten

---

[42] So auch *Welp*, Auskunftspflicht von Access-Providern, S. 151 ff.

[43] Vgl. *Welp*, Auskunftspflicht von Access-Providern, S. 151.

[44] Ergibt sich unter anderem aus *Regierungsentwurf*, BT-Drs. 16/5048, 39.

möglich ist, sodass nach § 101 Abs. 9 UrhG ohnehin ein Richtervorbehalt besteht.[45] Dieser entschärft die Problematik einer ungerechtfertigten Belastung des Diensteanbieters, da der Diensteanbieter nicht mehr der Gefahr einer Fehlbeurteilung ausgesetzt ist. In diesem Fall kann zudem davon ausgegangen werden, dass durch die Notwendigkeit einer richterlichen Beurteilung die Missbrauchsgefahr hinsichtlich des Auskunftsanspruchs eher gering sein dürfte.

Die Beschränkung des Drittauskunftsanspruchs gegen Internetdiensteanbieter auf offensichtliche Rechtsverletzungen überzeugt daher nicht. Unabhängig davon, wie man den Begriff auslegt, liegt es auf der Hand, dass der Rechteinhaber dadurch bei der Durchsetzung seiner Rechte im Einzelfall vor erhebliche Hürden gestellt wird.

cc) Problematische Fallgruppen

Dass Zweifel in tatsächlicher und in rechtlicher Hinsicht die Offensichtlichkeit ausschließen können,[46] kann sich in verschiedenen Fallgruppen problematisch auswirken.

Umstritten war die Rechtslage lange Zeit vor allem beim Filesharing über Peer-to-Peer-Netzwerke: Schwierigkeiten ergaben sich dabei aus der Funktionsweise solcher Netzwerke, bei dem die Nutzer einer Tauschbörse gleichzeitig automatisch auch als Anbieter von Inhalten fungieren.[47] Dabei ist es möglich, dass Teile eines Film- oder Musikwerks von verschiedenen Anbietern heruntergeladen werden und erst beim Nutzer zur vollständigen Datei zusammengesetzt werden. Hat ein Nutzer eine Datei bisher erst anteilig heruntergeladen, bietet er wiederum automatisch diesen heruntergeladenen Teil den anderen Nutzern zum Download an. Würde anschließend der Download abgebrochen, hätte der jeweilige Nutzer bereits Dateifragmente angeboten, ohne überhaupt im Besitz der vollständigen Datei gewesen zu sein. Es war deshalb äußerst umstritten, ob

---

[45] S. dazu unten Kap. 5 §4 A.

[46] Hierzu etwa *LG Köln*, Beschl. v. 24.1.2014 - 209 O 188/13, MMR 2014, 193, 194; *Meckel* in: Dreyer/Kotthoff/Meckel/Hentsch, § 101 UrhG Rn. 6.

[47] Ausführlich zur Funktionsweise des Peer-to-Peer-Filesharings etwa *Solmecke/Bärenfänger*, MMR 2011, 567, 567 f.

bereits das Anbieten von Dateifragmenten eine Rechtsverletzung darstellt.[48] Der Rechteinhaber kann nämlich meist nur nachweisen, dass ein Teil des geschützten Werks beim Nutzer des Filesharing-Netzwerks vorhanden ist.[49] Es lässt sich daher nicht ausschließen, dass es sich bei diesen Teilen um Dateifragmente handeln, die lediglich „Datenmüll" darstellen und auch mit technischen Mitteln nicht wahrnehmbar gemacht werden können.[50] In diesen Fällen war eine offensichtliche Rechtsverletzung daher fraglich.

Inzwischen dürfte hier aber durch höchstrichterliche Entscheidungen weitgehend Klarheit eingetreten sein: So geht der *BGH* davon aus, dass regelmäßig zumindest eine in Mittäterschaft mit den anderen Nutzern der Internettauschbörse begangene Rechtsverletzung vorliegt.[51] Der *EuGH* geht sogar noch weiter und nimmt beim automatisierten Hochladen im Rahmen des Filesharings auch dann eine öffentliche Zugänglichmachung an, wenn lediglich Fragmente der Datei hochgeladen werden.[52]

Anhand dieses Beispiels zeigt sich dennoch die Schwäche des Merkmals der Offensichtlichkeit einer Rechtsverletzung in Fällen, in denen die Rechtslage noch unklar ist. Sind im Einzelfall Rechtsfragen umstritten, muss eine offensichtliche Rechtsverletzung ausscheiden.[53] In eine ähnliche Richtung weist eine Entscheidung des *LG Köln* im Jahr 2014 zum Streaming, bei dem eine Videodatei lediglich im Webbrowser des Nutzers abgespielt wurde. Das *LG Köln* hatte in diesem Fall eine offensichtliche Rechtsverletzung abgelehnt, da damals noch nicht höchstrichterlich geklärt war, ob eine derartige Handlung eine unerlaubte Vervielfältigung nach § 16 UrhG darstellt.[54]

---

[48] Ausführlicher etwa *Heckmann/Nordmeyer,* CR 2014, 41, 41 ff.; *Solmecke/Bärenfänger*, MMR 2011, 567.

[49] *Heckmann/Nordmeyer,* CR 2014, 41, 44.

[50] Hierzu etwa *LG Frankenthal,* Beschl. v. 15.6.2016 – 6 O 134/16, MMR 2016, 694;

[51] *BGH*, Urt. v. 6.12.2017 – I ZR 186/16, GRUR 2018, 303 Rn. 24 ff. – Konferenz der Tiere; *AG Frankenthal,* Urt. v. 5.7.2018 – 3a C 73/18, GRUR-RR 2018, 444 Rn. 36 – Saints Row IV.

[52] *EuGH,* Urt. v. 17.6.2021 – C-597/19, MMR 2022, 30, 30 – Mircom.

[53] Ähnlich *OLG München,* Urt. v. 24.3.2005 - 6 U 4696/04, MMR 2005, 616 616.

[54] *LG Köln*, Beschl. v. 24.1.2014 - 209 O 188/13, MMR 2014, 193, 194 – Redtube. S. zur Rechtmäßigkeit des Streamings mittlerweile *EuGH,* Urt. v. 26.4.2017 – C-527/15, ZUM 2017, 587 Rn. 70 – Stichting Brein/Wullems.

Eine offensichtliche Rechtsverletzung ist darüber hinaus in Fällen abzulehnen, in denen – zum Beispiel beim Setzen eines einfachen Links oder beim Framing - in der Regel kein Urheberrechtsverstoß vorliegt und sich dieser nur im konkreten Einzelfall – etwa wegen Kenntnis der Rechtswidrigkeit des Inhalts und des Handelns in Gewinnerzielungsabsicht - ergibt.[55]

Schwierigkeiten bereiten auch Inhalte, bei denen die Diensteinhaber nicht auf den ersten Blick erkennen können, ob eine Rechtsverletzung vorliegt. Ein Beispiel dafür stellen Inhalte im Internet dar, die sich des Mittels der Parodie, Karikatur oder Pastiches bedienen. Ob hierbei eine Schrankenregelung des Urheberrechts greift, kann nur im Einzelfall und unter Abwägung der widerstreitenden Interessen beurteilt werden.[56] Ein weiteres Beispiel sind bei der Kommunikation im Internet verwendete Memes, bei denen gegebenenfalls urheberrechtlich geschützte Inhalte genutzt werden. Für die Diensteanbieter ist hier nicht auf den ersten Blick erkennbar, ob es sich um eine Rechtsverletzung oder eine zulässige Nutzung handelt. Eine offensichtliche Rechtsverletzung ist in diesen Fällen daher abzulehnen.

Eine vergleichbare Problematik zeigt sich auch bei Markenrechtsverletzungen im Internet.[57] Beispielsweise ist zur Bewertung der Ähnlichkeit von Marken die Verwechslungsgefahr zu untersuchen.[58] Der Diensteanbieter kann eine entsprechende Beurteilung weder leicht selbst treffen, noch ist für ihn in einem solchen Fall auf den ersten Blick erkennbar, ob es sich um eine Rechtsverletzung handelt.

Alle exemplarisch aufgeführten Fälle verdeutlichen die Problematik des Merkmals der offensichtlichen Rechtsverletzung. Bei Ablehnung einer offensichtlichen Rechtsverletzung bleibt dem Rechteinhaber die Rechtsdurchsetzung gegen den anonymen Nutzer versperrt, sofern sich dessen Identität nicht

---

[55] S. ausführlicher zur Urheberrechtsverletzungen im Zusammenhang mit Links und Framing oben unter Kap. 2 §3 B. I. 1. a).

[56] S. zur Interessensabwägung auch *EuGH*, Urt. v. 3.9.2014 – C-201/13, GRUR 2014, 972, 972 ff. - Vrijheidsfonds/Vandersteen u.a.; *BGH*, Urt. v. 28.7.2016 – I ZR 9/15, GRUR 2016, 1157, 1157 ff. – Auf fett getrimmt.

[57] Ausführlicher *Welp*, Auskunftspflicht von Access-Providern, S. 166 f.

[58] *Welp*, Die Auskunftspflicht von Access-Providern, S. 166 f.

anderweitig als durch Auskunft der Diensteanbieter ermitteln lässt. Dadurch wird es dem Rechteinhaber aber gegebenenfalls auch erschwert, die umstrittene Rechts- oder Tatsachenlage einer gerichtlichen Entscheidung zuzuführen.

c) Gewerbsmäßigkeitserfordernis

Neben dem Merkmal der offensichtlichen Rechtsverletzung kann auch das Gewerbsmäßigkeitserfordernis den Rechteinhabern Schwierigkeiten bereiten.

aa) Gewerbsmäßigkeit der Diensteanbieter

Unstrittig ist zunächst, dass die Diensteanbieter ihre Tätigkeiten in gewerblichem Ausmaß erbringen müssen. Nach Absatz 1 S. 2 kann sich das gewerbliche Ausmaß aus der Anzahl oder der Schwere der Rechtsverletzung ergeben. Allerdings kann nicht ohne Weiteres auf diese Definition zurückgegriffen werden, da es sich im Rahmen des Absatzes 2 bei den Diensteanbietern um Nicht-Verletzer handelt.[59] Bei der Definition des gewerblichen Ausmaßes im Kontext der Drittauskunft kann es daher nicht auf die Schwere oder die Anzahl der Rechtsverletzungen ankommen. Vielmehr muss die Erbringung des Dienstes selbst in gewerblichem Umfang erfolgen. Hierbei kann auf die wirtschaftliche Zielsetzung und den Umfang der Dienstleistung abgestellt werden.[60] Diensteanbieter, die in geringem Ausmaß privat und ohne kommerzielles Interesse handeln, werden dadurch von der Auskunftspflicht ausgenommen. Dies kann zum Beispiel private WLAN-Betreiber ausschließen, wenn nur ein begrenzter Personenkreis Zugriff auf das Netzwerk hat. Auch bei öffentlichen Einrichtungen wie Schulen oder Universitäten, die Zugang zum Internet gewähren, ist eine Tätigkeit in gewerblichem Ausmaß fraglich.[61] Werbefinanzierte Dienste und kommerzielle Access-Provider, die Zugang zum Internet gegen Entgelt vermitteln, erfüllen diese Voraussetzung dagegen.[62]

---

[59] So auch *Welp,* Auskunftspflicht von Access-Providern, S. 142 f.

[60] Ähnlich *Welp,* Auskunftspflicht von Access-Providern, S. 145.

[61] Im Ergebnis für Universitäten bejahend *Welp*, Die Auskunftspflicht von Access-Providern, S. 146 f.

[62] Vgl. *Seichter,* WRP 2006, 391, 396; *Zombik,* ZUM 2006, 450, 455. Differenzierend *Welp*, Auskunftspflicht von Access-Providern, S. 141 ff.

bb) Doppeltes Gewerbsmäßigkeitserfordernis beim Anspruch aus § 101 Abs. 2 UrhG

Bei den gewerblichen Schutzrechten setzt zudem der Tatbestand der Rechtsverletzung ein Handeln im geschäftlichen Verkehr voraus, sodass Handlungen im privaten Bereich vom Schutzbereich der jeweiligen Gesetze ohnehin ausgenommen sind. Ein Auskunftsanspruch besteht hier nur, wenn auch die geschäftliche Zwecksetzung der Rechtsverletzung offensichtlich ist.

Beim urheberrechtlichen Auskunftsanspruch aus § 101 Abs. 2 UrhG ist es dagegen umstritten, ob neben der Tätigkeit der Diensteanbieter auch die Rechtsverletzung ein gewerbliches Ausmaß erreicht haben muss, wie es der Wortlaut des § 101 Abs. 1 UrhG voraussetzt.

Dies ist zum Teil auf eine in dieser Hinsicht unklare Gesetzgebungsgeschichte der Norm zurückzuführen.[63] Nach der Gesetzesbegründung des Bundestags sei eine Rechtsverletzung im geschäftlichen Verkehr auch Voraussetzung des Drittauskunftsanspruchs nach § 101 Abs. 2 UrhG.[64] Allerdings bezog sich diese Ausführung noch auf das Tatbestandsmerkmal des „geschäftlichen Verkehrs",[65] welches später durch den Rechtsausschuss in den Begriff „gewerbliches Ausmaß" geändert wurde.[66] Zudem forderte der Bundesrat den Bundestag dazu auf *„klarzustellen, dass der Auskunftsanspruch gemäß § 101 Abs. 2 UrhG-E nicht voraussetzt, dass die Rechtsverletzung im geschäftlichen Verkehr erfolgt ist."*[67] Dieser Aufforderung ist der Bundestag jedoch nicht nachgekommen. Zumindest wollte die damalige Bundesregierung jedoch im weiteren Gesetzgebungsverfahren *„die Auswirkungen des Merkmals des geschäftlichen Verkehrs auf den Auskunftsanspruch bei Urheberrechtsverletzungen prüfen."*[68] Ob eine solche Prüfung ausblieb oder ob der Gesetzgeber auch nach einer

---

[63] S. zur Gesetzgebungsgeschichte etwa *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 154; *Spindler* in: Spindler/Schuster, § 101 UrhG Rn. 8. Zur Kritik am Gesetzgebungsverfahren siehe *Rohlfing,* Enforcement-Richtlinie, S. 163 ff.

[64] Vgl. *Regierungsentwurf,* BT-Drs. 16/5048, 49.

[65] Daher eine Übertragung auf das Tatbestandsmerkmal „in gewerblichem Ausmaß" ablehnend *Bohne*, CR 2010, 104, 107 f.

[66] S. hierzu *RAusschuss,* BT-Drs. 16/8783, 50.

[67] *Regierungsentwurf,* BT-Drs. 16/5048, 59.

[68] *Regierungsentwurf*, BT-Drs. 16/5048, 65.

entsprechenden Prüfung noch daran festhalten wollte, dass auch beim Drittauskunftsanspruch eine Rechtsverletzung im geschäftlichen Verkehr bzw. in gewerblichem Ausmaß vorauszusetzen ist, lässt sich nicht eindeutig klären.

Auch durch Hinzuziehung der zugrundeliegenden Richtlinie kann die Frage nicht beantwortet werden. Erwägungsgrund 14 der Enforcement-Richtlinie stellt lediglich klar, dass für Rechtsverletzungen von gewerblichem Ausmaß ein Auskunftsanspruch zwingend umzusetzen ist.[69] Allerdings wird den Mitgliedstaaten freigestellt diese Maßnahmen auch bei anderen Rechtsverletzungen zu ergreifen.[70]

Einen ersten Anhaltspunkt für die Auslegung bietet aber der Wortlaut des § 101 Abs. 2 UrhG. Mit der Formulierung „besteht der Anspruch unbeschadet von Absatz 1" wird unstreitig auf § 101 Abs. 1 UrhG verwiesen. Fraglich ist jedoch, ob es sich dabei lediglich um eine Rechtsfolgenverweisung oder um eine Rechtsgrundverweisung handelt, die das Bestehen der Voraussetzungen des § 101 Abs. 1 UrhG auch für § 101 Abs. 2 UrhG erforderlich machen würde.

Teilweise wurde angenommen, § 101 Abs. 2 UrhG stelle keinen eigenen Auskunftsanspruch dar.[71] Dies wird unter anderem auf den Wortlaut gestützt, der besagt, dass nicht ein Anspruch, sondern „der Anspruch" unbeschadet von Absatz 1 besteht.[72] Es handele sich demnach bei § 101 UrhG um einen einheitlichen Auskunftsanspruch. § 101 Abs. 2 UrhG erweitere lediglich den Kreis der

---

[69] A.A. *Sandor,* Datenspeicherung, Rn. 147, der ohne doppeltes Gewerbsmäßigkeitserfordernis einen Widerspruch zur Richtlinie dahingehend sieht, dass gutgläubige Endnutzer nicht Gegenstand eines Auskunftsverfahrens sein sollen.

[70] A.A. *Heid*, Haftung bei Urheberrechtsverletzungen im Netz, S. 166 ff., die die Richtlinie dahingehend interpretiert, dass der Anspruch auch für Rechtsverletzungen unterhalb der Schwelle des gewerblichen Ausmaßes zwingend sei.

[71] S. etwa *OLG München,* Urt. v. 26.7.2011 – 29 W 1268/11, ZUM 2011, 760, 761 – Die Friseuse; *OLG Hamburg,* Urt. v. 17. 2.2010 – 5 U 60/09, ZUM 2010, 893, 897; *OLG Köln*, Beschl. v. 9.2.2009 - 6 W 182/08, MMR 2009, 334, 334; *OLG Oldenburg,* Beschl. v. 1.12.2008 - 1 W 76/08, MMR 2009, 188, 189; *OLG Zweibrücken*, Urt. v. 27.10.2008 – 3 W 184/08, ZUM-RD 2008, 605, 605; *Brüggemann,* Drittauskunftsanspruch, S. 220 ff.; *Hofmann,* MMR 2009, 655, 658; *Maaßen,* MMR 2009, 511, 511; *Welp*, Auskunftspflicht von Access-Providern, S. 96; *Wick,* Inhalt und Grenzen des Auskunftsanspruchs, S. 46; *Wilhelmi,* ZUM 2008, 942, 944.

[72] *Brüggemann,* Drittauskunftsanspruch, S. 221.

Auskunftspflichtigen, sodass die Anforderungen an die Rechtsverletzung aus § 101 Abs. 1 UrhG auch hinsichtlich des Anspruchs gegen die in Absatz 2 genannten Personen vorliegen müssen.[73]

Die besseren Gründe sprechen jedoch dafür, Absatz 2 als eigene Anspruchsgrundlage anzusehen. Auch der *BGH* geht inzwischen davon aus, dass § 101 Abs. 2 UrhG nicht an die Voraussetzungen des § 101 Abs. 1 UrhG geknüpft ist.[74] Dem Wortlaut nach kann der Anspruch aus § 101 Abs. 2 UrhG nämlich „unbeschadet von Absatz 1" geltend gemacht werden.[75] Neben dem Anspruch aus § 101 Abs. 2 UrhG muss also auch ein Anspruch aus § 101 Abs. 1 UrhG geltend gemacht werden können. Wenn es sich jedoch bei § 101 UrhG um einen einheitlichen Anspruch handeln würde, wäre diese Formulierung überflüssig. Vielmehr spricht der Wortlaut dafür, dass es sich in den beiden Absätzen um zwei verschiedene Ansprüche handelt, die verschiedenen Voraussetzungen unterliegen. Etwas Ähnliches lässt sich auch aus § 101 Abs. 4 UrhG ableiten, wonach „die Ansprüche nach den Absätzen 1 und 2" bei Unverhältnismäßigkeit ausgeschlossen sind. Der Verweis in § 101 Abs. 2 UrhG auf Absatz 1 umfasst demnach lediglich die Rechtsfolgenseite.[76]

In dieselbe Richtung weist eine Betrachtung unter Aspekten der Gesetzessystematik und des Zwecks der verschiedenen Regelungen des § 101 UrhG. Für eine

---

[73] *OLG Schleswig*, Beschl. v. 5.2.2010 - 6 W 26/09, GRUR-RR 2010, 239, 240; *OLG Hamburg,* ZUM 2010, 893, 897; *OLG Köln*, Urt. v. 17.2.2010 – 5 U 60/09, MMR 2009, 334, 334; *OLG Frankfurt a. M.,* Beschl. v. 12.5.2009 – 11 W 21/09, ZUM 2009, 639, 640; *OLG Oldenburg,* Beschl. v. 1.12.2008 - 1 W 76/08*,* MMR 2009, 188, 189; *OLG Karlsruhe,* Beschl. v. 1.9.2009 – 6 W 47/09, ZUM 2009, 957, 960; *OLG Zweibrücken*, Beschl. v. 27.10.2008 – 3 W 184/08, ZUM-RD 2008, 605, 605; *Welp,* Auskunftspflicht von Access-Providern, S. 96.

[74] *BGH*, Beschl. v. 19.4.2012 - I ZB 80/11, MMR 2012, 689 Rn. 10 ff. – Alles kann besser werden; *BGH,* Beschl. v. 25.10.2012 – I ZB 13/12, ZUM 2013, 38, 39 – Two Worlds II; *BGH,* Beschl. v. 5.12.2012 – I ZB 48/12, GRUR 2013, 536, 539 – Die Heiligtümer des Todes; S. auch *Bockslaff/Krause*, MMR 2012, 693, 693; *Bohne*, GRUR-Prax 2012, 405, 407; *Bohne*, CR 2010, 104, 108; *Czychowski/Nordemann*, GRUR 2013, 986, 994; *Czychowski/Nordemann*, NJW 2013, 756, 760; *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 156; *Heymann,* CR 2008, 568, 570; *Musiol,* GRUR-RR 2009, 1, 3.

[75] *BGH,* Beschl. v. 19.4.2012 - I ZB 80/11, MMR 2012, 689 Rn. 13; *Bäcker,* ZUM 2008, 391, 392; *Bohne,* CR 2010, 104, 106.

[76] Ähnlich *OLG Zweibrücken*, Beschl. v. 27.10.2008 - 3 W 184/08, MMR 2009, 43, 44; *Bohne*, CR 2010, 104, 106 f.

Rechtsgrundverweisung wird argumentiert, dass der Dritte ansonsten schlechter stünde als der Verletzer, da dieser nur bei Rechtsverletzungen in gewerblichem Ausmaß zur Auskunft verpflichtet wäre.[77]

Allerdings erfüllen die beiden Ansprüche aus § 101 Abs. 1 UrhG und § 101 Abs. 2 UrhG unterschiedliche Funktionen.[78] Der Anspruch gegen den Verletzer aus § 101 Abs. 1 UrhG verbessert die Durchsetzbarkeit etwaiger Schadensersatz- bzw. Unterlassungsansprüche, indem etwa Auskünfte zur Berechnung des Schadens erteilt werden können. Die Auskunft erleichtert es daher dem Verletzten vor allem, das Ausmaß der Rechtsverletzung bestimmen zu können.[79] § 101 Abs. 2 UrhG dagegen soll überhaupt erst die Rechtsdurchsetzung in den Fällen ermöglichen, in denen die Identität des Rechtsverletzers nicht bekannt ist.[80] Würde man eine Rechtsverletzung in gewerblichem Ausmaß auch beim Anspruch nach § 101 Abs. 2 UrhG voraussetzen, bestünde die Gefahr, dass der eigentliche Zweck der Regelung zumindest teilweise verfehlt würde.[81] Das Handeln in gewerblichem Ausmaß bestimmt sich nach § 101 Abs. 1 S. 2 UrhG anhand der Anzahl oder der Schwere der Rechtsverletzung. Teilweise ist es für die Rechteinhaber vor der Identifizierung des Rechtsverletzers aber gar nicht möglich, einen Überblick über den Umfang und die Anzahl von Rechtsverletzungen zu erhalten.[82] Dies widerspräche dem Zweck der Regelung des § 101 Abs. 2 UrhG, einen möglichst effektiven Auskunftsanspruch zur Ermittlung der Identität des Rechtsverletzers bei Verletzungen nach dem Urheberrechtsgesetz zu schaffen.[83]

---

[77] Vgl. *OLG Schleswig*, Beschl. v. 5.2.2010 - 6 W 26/09, GRUR-RR 2010, 239, 239; *OLG Oldenburg,* Beschl. v. 1.12.2008 - 1 W 76/08, MMR 2009, 188, 189; *LG Frankfurt a.M.,* Beschl. v. 18. 9. 2008 - 2/06 O 534/08, GRUR-RR 2009, 15, 15; *Welp,* Auskunftspflicht von Access-Providern, S. 96.

[78] *BGH*, Beschl. v. 19.4.2012 - I ZB 80/11, MMR 2012, 689 Rn. 21. – Alles kann besser werden; *LG Bielefeld,* Beschl. v. 20.03.2009 - 4 OH 49/09, BeckRS 2009, 26785.

[79] Vgl. *LG Bielefeld*, Beschl. v. 20.03.2009 - 4 OH 49/09, BeckRS 2009, 26785; *Bohne,* CR 2010, 104, 108.

[80] *Regierungsentwurf*, BT-Drs. 16/5048, S.39, 49.

[81] Darauf hinweisend der Bundesrat S. *Regierungsentwurf*, BT-Drs. 16/5048, 59. S. auch *BGH*, Beschl. v. 19.4.2012 - I ZB 80/11, MMR 2012, 689 Rn. 23 – Alles kann besser werden.

[82] Vgl. vor allem zum Filesharing *Regierungsentwurf*, BT-Drs. 16/5048, 59.

[83] *BGH*, Beschl. v. 19.4.2012 - I ZB 80/11, MMR 2012, 689 Rn. 23 – Alles kann besser werden.

§ 101 Abs. 2 UrhG stellt somit einen eigenständigen Anspruch dar. Beim Verweis auf § 101 Abs. 1 UrhG handelt es sich lediglich um eine Rechtsfolgenverweisung. Entsprechend besteht der Auskunftsanspruch gegen Internetprovider unabhängig vom Ausmaß der Rechtsverletzung.

d) Umfang der Auskunft

Welche Daten bei der Auskunftserteilung übermittelt werden können, ist abschließend in Absatz 3 geregelt. Relevant für die Identifikation von Rechtsverletzern im Internet ist Absatz 3 Nr. 1. Demnach umfasst der Auskunftsanspruch lediglich die Weitergabe von Namen und Anschrift des Nutzers der Dienstleistung. Sofern die Diensteanbieter über entsprechende Daten verfügen, können diese daher zumindest auf Auskunft über die Wohnanschrift und Namen der Rechtsverletzer in Anspruch genommen werden.

aa) IP-Adressen, Telefonnummern und E-Mail-Adressen

Es war längere Zeit lang umstritten, ob darüber hinaus auch IP-Adressen, Telefonnummern und E-Mail-Adressen vom Umfang des Auskunftsanspruchs erfasst werden.

Es vermag nicht zu überzeugen, allein wegen des Wortbestandteils der „Adresse", E-Mail-Adressen und IP-Adressen unter den Begriff der „Anschrift" zu subsumieren.[84] Als sinnvoll könnte sich allenfalls eine Auslegung erweisen, die sich an der Funktion der Anschrift orientiert. Die Weitergabe von Namen und Anschriften im Rahmen des Drittauskunftsanspruchs soll schließlich die Identifizierung eines Rechtsverletzers ermöglichen. Die „Anschrift" ermöglicht es den Rechteinhabern, den entsprechenden Nutzer „anschreiben" beziehungsweise kontaktieren zu können. In erster Linie erfüllt diese Funktion die ladungsfähige Anschrift des Rechtsverletzers. Bei einer erweiterten Auslegung des Begriffs könnte man allerdings erwägen, dass auch E-Mail-Adressen darunterfallen, da diese es dem Rechteinhaber ebenfalls ermöglichen könnten, schriftlich Kontakt mit dem Rechtsverletzer aufzunehmen.[85]

---

[84] Vgl. *Wimmers* in: Schricker/Loewenheim, § 101 UrhG Rn. 76.

[85] So im Ergebnis auch *OLG Frankfurt a.M.*, Urt. v. 22.8.2017 – 11 U 71/16, GRUR 2017, 1116, 1118; *OLG Köln,* Urt. v. 25.3.2011 - 6 U 87/10, GRUR-RR 2011, 305, 305 – Schweizer Sharehoster; *Spindler* in: Spindler/Schuster, § 101 UrhG Rn. 13; a.A. *LG Frankfurt a.M.*, Urt.

IP-Adressen erfüllen dagegen keine entsprechende Funktion. Sie ermöglichen es zwar gegebenenfalls, den Anschlussinhaber zu identifizieren, allerdings können die Rechteinhaber ohne nähere Informationen durch den Zugangsanbieter nichts mit der IP-Adresse anfangen. Insbesondere kann keine Kontaktaufnahme mit dem Inhaber einer IP-Adresse stattfinden. In diesem Punkt unterscheiden sich IP-Adressen von Anschriften nach Absatz 2 Nummer 1. Daher spricht viel dafür, dass IP-Adressen vom Umfang des Auskunftsanspruchs nicht erfasst werden.[86]

Inzwischen hat sich der *EuGH*[87] anlässlich eines Vorabentscheidungsersuchens des *BGH*[88] zu diesem Thema geäußert: Der Wortlaut des Absatz 3 der nationalen Auskunftsansprüche geht auf Art. 8 Abs. 2 a) der Enforcement-Richtlinie zurück. Der *BGH* legte dem *EuGH* die Frage vor, ob nach der Auslegung der Richtlinie vom Umfang der Auskunft auch E-Mail-Adressen, Telefonnummern und IP-Adressen erfasst werden. Der *EuGH* hat dazu entschieden, dass vom Wortlaut der „Adresse" lediglich die Wohnanschrift erfasst werde, nicht aber E-Mail-Adresse, Telefonnummer oder IP-Adresse.[89] Bei der „Adresse" handele es sich zudem um einen unionsrechtlichen Begriff, der in allen Mitgliedstaaten einheitlich ausgelegt werden muss.[90] Der *EuGH* hat aber klargestellt, dass es den Mitgliedstaaten freistünde, den Umfang des Auskunftsanspruchs zu erweitern.[91] In Deutschland ist dies aber nicht erfolgt. Deswegen werden E-Mail-Adressen, Telefonnummer und IP-Adresse von Absatz 3 der nationalen Auskunftsansprüche nicht erfasst.[92]

---

v. 3.5.2016 – 2-3 O 476/13, GRUR-RR 2017, 3, 3; *Wimmers* in: Schricker/Loewenheim, § 101 Rn. 76.

[86] So auch *OLG München*, Urt. v. 21.9.2006 - 29 U 2119/06, GRUR 2007, 419, 424 - Lateinlehrbuch; *LG Frankfurt a.M.*, Urt. v. 22.8.2017 – 11 U 71/16, GRUR-RR 2017, 3; *Wimmers* in: Schricker/Loewenheim, § 101 UrhG Rn. 76.

[87] *EuGH,* Urt. v. 9.7.2020 – C-264/19*,* GRUR 2020, 840, 840 – YouTube Drittauskunft.

[88] *BGH,* Beschl. v. 21.2.2019 – I ZR 153/17, ZD 2019, 270 – YouTube Drittauskunft.

[89] *EuGH,* Urt. v. 9.7.2020 – C-264/19*,* GRUR 2020, 840 Rn. 40 – YouTube Drittauskunft.

[90] *EuGH,* Urt. v. 9.7.2020 – C-264/19*,* GRUR 2020, 840 Rn. 28 – YouTube Drittauskunft.

[91] *EuGH,* Urt. v. 9.7.2020 – C-264/19*,* GRUR 2020, 840 Rn. 39 – YouTube Drittauskunft.

[92] S. auch *BGH,* Urt. v. 10.12.2020 – I ZR 153/17*,* ZUM 2021, 250, 250 – YouTube Drittauskunft II.

Darin liegt eine nicht unerhebliche Schwäche der Auskunftsansprüche im Bereich des geistigen Eigentums: Sowohl E-Mail-Adressen als auch Telefonnummern können im Einzelfall zu einer Identifizierung des Rechtsverletzers beitragen.[93] Besonders problematisch ist aber, dass auch kein Anspruch auf Auskunft über die IP-Adresse besteht. Da IP-Adressen technisch zwingend bei jedem Kommunikationsvorgang im Internet übertragen werden, besteht immer zumindest die theoretische Möglichkeit, den Rechtsverletzer anhand der IP-Adresse zurückverfolgen zu können.[94] Ist dem Rechteinhaber die IP-Adresse nicht bekannt und kann er sie auch nicht selbst – beispielsweise unter Verwendung einer entsprechenden Software – ermitteln, fällt diese wichtige Identifikationsmöglichkeit für die Rechteinhaber weg. In diesen Fällen müsste der Rechteinhaber in einem ersten Schritt Auskunft über die IP-Adresse erhalten, um daraufhin über den Access-Provider die Identität des Anschlussinhabers zu ermitteln.[95] Diese Möglichkeit wird den Rechteinhabern durch die Beschränkung des Anspruchsumfangs auf Namen und (Wohn-)Anschriften verwehrt.

bb) Sonstige zur Identifizierung nützliche Daten

Auch andere Daten, die sich als nützlich für die Identifizierung des Rechtsverletzer erweisen könnten, sind nach dem Urteil des *EuGH* nicht mehr vom Umfang des Auskunftsanspruchs erfasst. Auch mittels Bankdaten könnte beispielsweise über Umwege eine Identifizierung des Rechtsverletzers gelingen.[96] Diese Information wird allerdings ebenfalls nicht vom Drittauskunftsanspruch erfasst, der sich auf Namen und Adresse beschränkt.

cc) Auskunft über Inhaber von Internetanschlüssen und Nutzerkonten

Die überwiegende Ansicht geht wohl davon aus, dass es zumindest möglich ist, mittels der IP-Adresse über den Access-Provider Auskunft über Namen und Anschrift des Anschlussinhabers zu erhalten.[97]

---

[93] S. oben unter Kap. 4 § 3.

[94] S. oben unter Kap. 4 § 4 A.

[95] S. oben unter Kap. 4 § 4 B. II.

[96] S. oben unter Kap. 4 § 3.

[97] Dies voraussetzend etwa *OLG Köln*, Beschl. v. 20.4.2016 – 6 W 37/16, ZUM-RD 2016, 467, 467 - The Walking Dead; *OLG Frankfurt*, Beschl. v. 12.5.2009 – 11 W 21/09, ZUM 2009, 639, 640; *LG Köln*, Beschl. v. 17.12.2008 - 38 OH 8/08, MMR 2009, 489, 489; *LG Frankfurt*, Beschl. v. 18.9.2008 - 2-06 O 534/08, MMR 2008, 829, 829; *Dreier* in: Dreier/Schulze, § 101

Da der Anschlussinhaber jedoch nicht automatisch mit dem Rechtsverletzer gleichzusetzen ist, ist das nicht selbstverständlich. Beim Access-Providing besteht die Dienstleistung darin, einer anderen Person Zugang zum Internet zu verschaffen. Der Anschlussinhaber ist ein Nutzer dieser Dienstleistung. Es ist aber durchaus möglich, dass er den Anschluss zum Zeitpunkt der Rechtsverletzung nicht verwendet hat oder zumindest die Rechtsverletzung nicht selbst begangen hat. Beim rechtsverletzenden Nutzer und beim Anschlussinhaber kann es sich daher um verschiedene Personen handeln.[98] Ob der Anschlussinhaber tatsächlich selbst Rechtsverletzer ist, lässt sich allenfalls erst nach der Auskunftserteilung feststellen.

Teilweise wird die Diskussion um das Auseinanderfallen von Rechtsverletzer und Anschlussinhaber im Rahmen des Merkmals der Offensichtlichkeit geführt. Dabei ist umstritten, ob neben der Rechtsverletzung auch offensichtlich sein muss, dass der Anschlussinhaber selbst der Rechtsverletzer ist.[99] Die entscheidende Frage ist aber vielmehr, über welche Nutzer der Diensteanbieter zur Auskunft verpflichtet werden kann. Zur Rückverfolgung des tatsächlich handelnden Nutzers mittels IP-Adresse sind die Rechteinhaber darauf angewiesen, zunächst den Anschlussinhaber zu ermitteln. Auch wenn dieser die Rechtsverletzung nicht selbst begangen hat, besteht nur über ihn die Möglichkeit, den tatsächlich handelnden Nutzer noch zu identifizieren.[100] Es kommt deshalb darauf an, ob sich die Auskunftspflicht nur auf den rechtsverletzenden oder auch auf andere Nutzer erstreckt. Nimmt man an, dass der Diensteanbieter auch zur Auskunft über den Anschlussinhaber verpflichtet werden kann, wäre klar, dass sich

---

UrhG Rn. 10; *Reber* in: Möhring/Nicolini, § 101 UrhG Rn. 16 ff.; *Spindler* in: Spindler/Schuster, § 101 UrhG Rn. 21 ff.; *Wimmers* in Schricker/Loewenheim, § 101 UrhG Rn. 46 ff.

[98] S. bereits oben unter Kap. 4 § 4 E. I.

[99] Davon ausgehend, dass die Rechtsverletzung nicht offensichtlich auch vom Anschlussinhaber begangen worden sein muss etwa *OLG Köln,* Beschl. v. 7.20.2013 – 6 W 84/13, ZUM 2013, 951, 952 – Life of Pi; *OLG Köln,* Beschl. v. 20.1.2012 – 6 W 242/11, ZUM 2012, 582, 582; *OLG Zweibrücken,* Beschl. v. 21.9.2009 - 4 W 45/09, MMR 2010, 214, 215; *OLG Köln,* Beschl. v. 9.2.2009 – 6 W 182/08, ZUM 2009, 425, 427 – Die schöne Müllerin; *OLG Köln,* Beschl. v. 21.10.2008 - 6 Wx 2/08, MMR 2008, 820, 822 – Ganz anders; *Maaßen,* MMR 2009, 511, 512; *Musiol,* GRUR-RR 2009, 1, 4. Kritisch aber *LG Frankenthal,* Beschl. v. 6.3.2009 - 6 O 60/09, MMR 2009, 487, 488; *Sandor,* Datenspeicherung, Rn. 135; *Kitz,* ZUM 2006, 444, 447.

[100] Vgl. auch *Siebert,* Geheimnisschutz, S. 205.

die Offensichtlichkeit nur auf die Rechtsverletzung bezieht. Im umgekehrten Fall muss der Anspruch ausscheiden, wenn unklar ist, ob der Anschlussinhaber selbst Rechtsverletzer ist.

Es stellt sich daher die Frage nach der Auslegung des Auskunftsumfangs. Der Auskunftsanspruch aus Absatz 2 umfasst Auskünfte über Namen und Adresse „der Nutzer der Dienstleistungen". Sicherlich besteht aber kein Auskunftsanspruch über sämtliche Nutzer der Dienstleistung. Das ergibt sich nicht nur aus teleologischer Sicht, sondern zeigt sich auch in der Gesetzessystematik unter Hinzuziehung von Absatz 2 Nummer 3. Demnach sind Personen zur Auskunft verpflichtet, die „für rechtsverletzende Tätigkeiten genutzte" Dienstleistungen erbringen. Das heißt, dass der Nutzer in hinreichendem Bezug zur Rechtsverletzung stehen muss, bedeutet aber nicht zwingend, dass er selbst eine rechtsverletzende Handlung vorgenommen haben muss.

Daher kann auch die Auskunft über einen nicht-rechtverletzenden Anschlussinhaber vom Anspruchsumfang erfasst werden. Dafür spricht auch, dass die Nutzung des Internetanschlusses in der Risikosphäre des Anschlussinhabers liegt.[101] Damit besteht ausreichender Bezug des Anschlussinhabers zur Rechtsverletzung, der es rechtfertigt, den Anschlussinhaber - unabhängig von einer eigenen Verletzungshandlung - in den Umfang des Auskunftsanspruchs einzubeziehen. Das ist auch insofern schlüssig, als dass in einem späteren Verfahren gegen den Anschlussinhaber dieser im Rahmen seiner sekundären Darlegungslast angeben muss, wer als möglicher Nutzer seines Anschlusses in Betracht kommt.[102] Der BGH geht sogar noch weiter, indem er eine Haftung des Anschlussinhabers als Täter darauf stützt, dass dieser seiner sekundären Darlegungslast nicht nachgekommen ist.[103] Außerdem können sowohl der

---

[101] *OLG Köln,* Beschl. v. 21.10.2008 - 6 Wx 2/08, MMR 2008, 820, 822 – Ganz anders

[102] *BGH,* Urt. v. 12.5.2010 – I ZR 121/08, ZUM 2010, 696 Rn. 12 – Sommer unseres Lebens; *OLG Frankfurt*, Beschl. v. 20.12.2007 - 11 W 58/07, GRUR-RR 2008, 73, 74 – Filesharing durch Familienangehörige; *OLG Köln*, Urt. v. 23.12.2009 - 6 U 101/09, K&R 2010, 131, 131 f. Ausführlich zu sekundären Darlegungslast des Anschlussinhabers *Gotthardt,* ZUM 2021, 7, 7 ff; *Schaub,* NJW 2018, 17, 17 ff. S. zur Unionsrechtskonformität der Rechtsprechung des BGH *Paschold,* GRUR Int. 2018, 621, 621 ff.

[103] *BGH,* Urt. v. 17.12.2020 – I ZR 228/19, GRUR 2021, 714 Rn. 72, 80 – Saints Row; *BGH,* Urt. v. 12.5.2016 – I ZR 86/15, GRUR 2016, 1289 Rn. 28 – Silver Linings Playbook;

Rechteinhaber wie auch der Access-Provider ohne Identifizierung des Anschlussinhabers meistens überhaupt nicht feststellen, ob dieser selbst auch Rechtsverletzer ist.[104] Es entspricht daher dem Zweck eines möglichst effektiven Rechtsschutzes, wenn die Rechteinhaber auch einen Anspruch auf Auskunft über einen nicht-rechtsverletzenden Anschlussinhaber geltend machen können.[105]

Ein ähnliches Problem besteht im Übrigen auch, wenn eine andere Person als der Inhaber eines Nutzerkontos eine Rechtsverletzung unter Verwendung dieses Kontos begeht. Der Inhaber des Nutzerkontos ist in diesem Fall genauso zu behandeln wie der Anschlussinhaber und wird vom Umfang des Auskunftsanspruchs erfasst.

dd) Anspruchsumfang nach § 19 MarkenG, § 46 DesignG und § 37b SortenSchG

Schwierigkeiten bereitet auch die Formulierung zum Anspruchsumfang in § 19 MarkenG, § 46 DesignG und § 37b SortenSchG. Anders als bei den übrigen immaterialgüterrechtlichen Auskunftsansprüchen erstrecken sich zumindest nach deren Wortlaut die Ansprüche nicht auf die Auskunft über die Identität des Nutzers einer Dienstleistung. Es kann davon ausgegangen werden, dass es sich dabei um ein Versehen des Gesetzgebers handelt und die Möglichkeit der Auskunftserteilung über die Identität eines Nutzers für die Ansprüche in § 19 MarkenG, § 46 DesignG und § 37b SortenSchG nicht bewusst ausgeschlossen werden sollte.[106]

Dennoch ist der Wortlaut der § 19 MarkenG, § 46 DesignG und § 37b SortenSchG insoweit eindeutig und die Beschränkungen im Hinblick auf den Anspruchsumfang grundsätzlich als abschließend zu betrachten. Insofern müsste man sich im Rahmen einer analogen Anwendung mit der Planwidrigkeit der Regelungslücke auseinandersetzen.

Kritisch dagegen *Galetzka/Stamer*, K&R 2020, 486, 486; *Köhler,* ZUM 2018, 27, 27; *Ungern-Sternberg*, GRUR 2018, 225, 239.

[104] Vgl. *OLG Köln,* Beschl. v. 21.10.2008 - 6 Wx 2/08, MMR 2008, 820, 822 – Ganz anders.

[105] Vgl. *OLG Köln,* Beschl. v. 21.10.2008 - 6 Wx 2/08, MMR 2008, 820, 822 – Ganz anders.

[106] *Janal*, Europäisches Zivilverfahrensrecht, S. 262.

Besonders der markenrechtliche Auskunftsanspruch spielt bei anonymen Rechtsverletzungen im Internet in der Praxis eine Rolle, sodass im Hinblick auf den Anspruchsumfang eine Anpassung des § 19 MarkenG an die Regelungen aus § 101 UrhG, § 140b PatG, § 24b Abs. 3 GebrMG und § 9 Abs. 2 HalblSchG geboten ist.

e) Verhältnismäßigkeitserfordernis und Haftung

Darüber hinaus regelt Absatz 4, dass der Auskunftsanspruch nur besteht, wenn der Grundsatz der Verhältnismäßigkeit gewahrt wird. Die Auskunftserteilung muss demnach im Einzelfall geeignet, erforderlich und angemessen sein.[107] Dieser Verhältnismäßigkeitsgrundsatz, der auf Art. 8 Abs. 1 der Enforcement-Richtlinie zurückgeht, findet seine Berechtigung in der Kollision der verschiedenen Interessen der Rechteinhaber, Diensteanbieter und Nutzer. Insbesondere im Rahmen der Prüfung der Angemessenheit können Art und Schwere der Rechtsverletzung, sowie die Interessen des Auskunftspflichtigen, aber auch das Interesse der Nutzer am Schutz ihrer personenbezogenen Daten berücksichtigt werden.[108] Die Auskunftserteilung kann aber nur im Einzelfall unter besonderen Umständen unverhältnismäßig sein, da der Gesetzgeber bereits durch die Regelung des Auskunftsanspruchs den Interessen der Rechteinhaber grundsätzlich Vorrang eingeräumt hat.[109] Unverhältnismäßigkeit liegt etwa vor, wenn der Anspruchssteller offenkundig andere Ziele verfolgt als die Durchsetzung seiner Rechte.[110] Dazu zählt etwa die Ausforschung von Nutzerdaten ins Blaue oder das Ausspähen von Betriebsgeheimnissen.[111]

Allerding geht Art. 8 der Enforcement-Richtlinie davon aus, dass die zuständigen Gerichte über die Anordnung der Auskunftserteilung und damit auch über die Verhältnismäßigkeit des Auskunftsantrags des Verletzten entscheiden.[112] Dagegen bleibt die Verhältnismäßigkeitsprüfung nach der deutschen Umsetzung – sofern nicht der Richtervorbehalt nach § 101 Abs. 9 UrhG greift – dem

---

[107] S. etwa *Dreier* in: Dreier/Schulze, § 101 UrhG Rn.22; *Kramer*, Zivilrechtlicher Auskunftsanspruch, S. 171.

[108] *Siebert,* Geheimnisschutz, S. 159 f.

[109] S. etwa *Dreier* in: Dreier/Schulze, § 101 UrhG Rn 22 f.

[110] *Regierungsentwurf,* BT-Drs. 11/4792, S. 31.

[111] *Brüggemann,* MMR 2013, 278, 281.

[112] Vgl. *Regierungsentwurf,* BT-Drs. 16/5048, S. 63.

Diensteanbieter überlassen. Die Diensteanbieter sind aber keinesfalls in einer neutralen Position, da auch ihre eigenen Interessen durch ein Auskunftsbegehren berührt werden. Es kann deshalb in Frage gestellt werden, ob durch die Entscheidung der Diensteanbieter ein angemessener Interessensausgleich gewährleistet werden kann.

Ein weiteres Problem ist, dass die Diensteanbieter nach Absatz 6 gegenüber ihren Nutzern nicht haften, wenn sie gutgläubig wahrheitsgemäß Auskunft über deren Daten erteilt haben. Dies birgt die Gefahr, dass die Diensteanbieter im Zweifel eher dazu neigen werden, die Auskunft zu erteilen.

Die Beschränkung der Haftung bei einer wahrheitsgemäßen Auskunft auf Vorsatz oder grobe Fahrlässigkeit soll nach der Gesetzesbegründung dem Umstand Rechnung tragen, dass „in Fällen des Abs. 2 der Verpflichtete kaum beurteilen kann, ob überhaupt eine Rechtsverletzung vorliegt."[113] Sollte dies tatsächlich der Fall sein, stellt sich aber wiederum die Frage, wie die auskunftspflichtige Person dann in der Lage sein kann, die Verhältnismäßigkeit der Auskunftserteilung zu beurteilen. Dazu kommt, dass die Verpflichtung zur Auskunftserteilung nach Absatz 2 nur im Falle einer offensichtlichen Rechtsverletzung besteht, um den Dritten bei der Prüfung zu entlasten.[114] Eine zusätzliche Haftungsbeschränkung zugunsten des Auskunftspflichtigen wäre damit nicht mehr erforderlich. Insofern erweist sich das Regelungskonzept des Drittauskunftsanspruchs zum Teil als widersprüchlich.[115]

Sinnvoll erscheint dagegen, dass die Diensteanbieter bei einer vorsätzlich oder grob fahrlässigen falschen Auskunft den Rechteinhabern gegenüber nach Absatz 5 für den dadurch entstandenen Schaden haften. Die Diensteanbieter werden auf diese Weise dazu angehalten, eine korrekte Auskunft zu erteilen.[116] Erteilen die Diensteanbieter vorsätzlich oder grob fahrlässig eine fehlerhafte Auskunft bleibt dies nunmehr nicht folgenlos.[117] Der damit einhergehende Ausschluss einer Haftung bei leicht fahrlässigem Verhalten der Diensteanbieter

---

[113] *Regierungsentwurf,* BT-Drs. 16/5048, S. 39.
[114] *Regierungsentwurf,* BT-Drs. 16/5048, S. 39.
[115] *Peukert/Kur,* GRUR-Int 2006, 292, 297.
[116] *Regierungsentwurf,* BT-Drs. 16/5048, S. 39.
[117] *Regierungsentwurf,* BT-Drs. 16/5048, S. 39.

ist im Sinne der Verhältnismäßigkeit der Inanspruchnahme der Diensteanbieter für eine Verletzung ihrer Nutzer sinnvoll.

2. Auskunftsanspruch nach Absatz 1

Neben dem Drittauskunftsanspruch aus Absatz 2 kommt in einigen Fällen auch ein Anspruch gegen einen Diensteanbieter aus Absatz 1 in Betracht. Im Unterschied zu Absatz 2 richtet sich der Anspruch aus Absatz 1 nicht gegen Dritte, sondern gegen einen Verletzer. Die Voraussetzungen und Rechtsfolgen des Anspruchs entsprechen weitgehend denen des zweiten Absatzes. Anders als der Drittauskunftsanspruch nach Absatz 2 verlangt der Anspruch auf Auskunft gegen den Verletzer nach Absatz 1 allerdings nicht den Nachweis einer offensichtlichen Rechtsverletzung. Außerdem kann der Verletzer keinen Anspruch auf Kostenersatz für die Aufwendungen der Auskunftserteilung aus Absatz 2 Satz 3 gegen den Verletzten geltend machen. Eine Inanspruchnahme der Diensteanbieter nach Absatz 1 könnte daher für die Rechteinhaber in dieser Hinsicht vorteilhaft sein.

a) Anspruch auf Grundlage der Störerhaftung

Es ist umstritten, ob der Auskunftsanspruch nach Absatz 1 auch auf Störer anwendbar ist. Der Gesetzgeber hat diese Frage bei der Neufassung der immaterialgüterrechtlichen Auskunftsansprüche bewusst offengelassen.[118] Die besseren Argumente sprechen allerdings dafür, die Regelung des Absatz 2 im Hinblick auf den Auskunftsanspruch gegen Internet-Provider als abschließend zu betrachten.

Eine Inanspruchnahme von Störern über bloße Abwehransprüche hinaus lässt sich nur schwer konstruieren.[119] Auch die Enforcement-Richtlinie unterscheidet lediglich zwischen dem unmittelbaren Verletzer einerseits und dem Dritten andererseits.[120] Dementsprechend sollten in der nationalen Umsetzung Störer ausschließlich unter Absatz 2 subsumiert werden.[121]

---

[118] S. *Regierungsentwurf*, BT-Drs. 16/5048, 29 f.

[119] Hierzu ausführlicher etwa *Wimmers* in: Schrickers/Loewenheim, § 101 UrhG Rn. 27.

[120] *Wiebe* in: Büllesbach/Büchner, It doesn´t matter!?, 153, 167 ff.

[121] So auch *Janal*, Europäisches Zivilverfahrensrecht, S. 259 ff.

Mit der Neufassung des Drittauskunftsanspruchs in Absatz 2 besteht zudem eine ausdrückliche Regelung für einen Auskunftsanspruch gegen Internetdiensteanbieter, die die Identifizierung des Rechtsverletzers zumindest ermöglichen soll. Diese Regelung ist im Zusammenhang mit der Auskunftserteilung durch Internetdiensteanbieter gegenüber der Regelung aus Absatz 1 spezieller und als abschließend zu betrachten. Das Kriterium der offensichtlichen Rechtsverletzung dient im Rahmen des Drittauskunftsanspruchs unter anderem dem Schutz der personenbezogenen Daten der Nutzer vor einer unbegründeten Weitergabe und einem Ausspähen ihrer Daten. Durch die Anwendung des Auskunftsanspruchs aus Absatz 1 auf Internetdiensteanbieter würde dieses Schutzinstrument umgangen werden. Absatz 1 ist daher auf den bloßen Störer nicht anzuwenden.[122]

b) Anspruch aufgrund der Haftung des Diensteanbieters als Rechtsverletzer

Ein Anspruch aus Absatz 1 gegen einen Diensteanbieter kann aber dann bestehen, wenn nicht nur der Nutzer, sondern auch der Diensteanbieter selbst als Rechtsverletzer agiert. Sofern die Diensteanbieter lediglich als Vermittler von Inhalten auftreten, ist dies aber meist nicht der Fall.

Etwas anderes gilt aber vor allem im Urheberrecht. Hier wird von der Rechtsprechung inzwischen verstärkt eine täterschaftliche Haftung von Diensteanbietern in Bezug auf rechtsverletzendes Verhalten ihrer Nutzer angenommen.[123]

---

[122] So auch *Bohne* in: Wandtke/Bullinger, § 101 UrhG Rn. 6; *Kitz,* ZUM 2005, 298, 300; *Klett*, K&R 2005, 222, 224; *Knaack*, GRUR-Int 2004, 745, 749; *Schlegel*, CR 2005, 144, 144; *Wimmers* in: Schricker/Loewenheim, § 101 UrhG Rn. 28. A.A. *Reber* in: Möhring/Nicolini, § 101 UrhG Rn. 1; *Spindler* in: Spindler/Schuster, § 101 UrhG Rn. 3.

[123] S. zur Voraussetzung einer täterschaftlichen Haftung *EuGH,* Urt. v. 22.6.2021 – C-682/18 u.a., GRUR 2021, 1054 Rn. 102 – Youtube und Cyando; *EuGH,* Urt. v. 14.6.2017 – C-610/15, ZUM 2017, 746 Rn. 26 – Stichting Brein/Ziggo BV (The Pirate Bay); *EuGH,* Urt. v. 26.4.2017 – C-527/15, ZUM 2017, 587 Rn. 31 – Stichting Brein/Wullems; OLG Frankfurt a.M., Urt. v. 30.4.2019 – 11 U 27/18, GRUR-RR 2020, 57, 57. S. zur täterschaftlichen Haftung von Sharehostern OLG Hamburg, Beschl. v. 13.5.2013 – 5 W 41/13, GRUR-RR 2013, 382, 382 ff.; Zur Täterhaftung eines Usenet-Providers LG Hamburg, Urt. v. 22.6.2018 – 308 O 314/16, ZUM 2018, 814, 814 ff. S. auch Erfurth, GRUR-Prax 2021, 217, 217 ff.; Frey, MMR 2022, 97, 97 ff.; Holznagel, CR 2021, 603, 604; Jones, Urheberrechtliche Haftung, S. 76 ff.; Küster, Der Plattformbetreiber als Täter, S. 131 ff.; *Ohly,* ZUM 2017, 793, 802; Rauer/Bibi,

Im Rahmen des UrhDaG wurde darüber hinaus die täterschafltiche Haftung von Diensteanbietern für das Teilen von Online-Inhalten im Sinne von § 2 UrhDaG normiert. Diese können nach § 1 Abs. 1 UrhDaG selbst eine urheberrechtlich relevante Verwertungshandlung begehen, wenn sie der Öffentlichkeit Zugang zu Werken verschaffen, die von Nutzern ihrer Dienste hochgeladen wurden. Sie haften damit nunmehr selbst als Täter.[124] In diesen Fällen lässt sich deshalb – zumindest dem Wortlaut nach – ein Anspruch gegen die Diensteanbieter auch aus Absatz 1 ableiten. Durch die Ausweitung der täterschaftlichen Haftung im Urheberrecht, könnten daher die besonderen Voraussetzungen der Drittauskunft nach § 101 Abs. 2 UrhG teilweise obsolet werden.

Allerdings sollte Absatz 1 dahingehend teleologisch reduziert werden, dass Diensteanbieter vom Anwendungsbereich des ersten Absatzes ausgenommen werden, wenn deren Rechtsverletzung lediglich aus dem Verbreiten rechtsverletzender Inhalte ihrer Nutzer resultiert. Dies sollte zumindest für Auskünfte über die Identität des rechtsverletzenden Nutzers gelten. Die Interessenslage ist bei diesen Diensten nämlich vergleichbar mit anderen Host-Providern, die allenfalls als Störer für die Inhalte ihrer Nutzer haften. Das gilt zum Beispiel für den Betreiber eines Online-Marktplatzes, auf dem Nutzer markenrechtverletzende Produkte anbieten.[125] Dieser ist nur zur Auskunftserteilung verpflichtet, wenn die Rechtsverletzung offensichtlich ist. Es ist nicht ersichtlich, warum zum Beispiel Diensteanbieter im Anwendungsbereich des UrhDaG hinsichtlich der Auskunft über ihre Nutzer anders behandelt werden sollten. Weder sind die Diensteanbieter bei einer Urheberrechtsverletzung automatisch leichter in der Lage, eine Rechtsverletzung festzustellen, noch sind die Nutzer hinsichtlich einer missbräuchlichen Anwendung des Auskunftsanspruchs weniger schutzbedürftig.

ZUM 2021, 819, 819 ff.; *Spindler,* NJW 2021, 2554, 2554 ff.; *Stuve*, Haftung für Werbung, S. 126 ff.; *Ungern-Sternberg*, GRUR 2021, 1, 5.

[124] *Oster* in: BeckOK Urheberrecht, § 1 UrhDaG Rn. 19.

[125] Im Markenrecht wird eine vergleichbare Ausweitung der Täterhaftung anders als im Urheberrecht nicht vorgenommen, S. etwa *EuGH,* Urt. v. 2.4.2020 – C-567/18, GRUR 2020, 637 Rn. 37 ff. – Coty; *EuGH,* Urt. v. 12.7.2011 - C-324/09, GRUR 2011, 1025 Rn. 103 f. –L'Oreal; *EuGH*, Urt. v. 23.3.2010 - C-236/08 u.a., GRUR 2010, 445 Rn. 57 – Google France; S. auch *BGH*, Urt. v. 11.3.2004 - I ZR 304/01, GRUR 2004, 860, 863 – Internetversteigerung I; *BGH*, Urt. v. 19.4.2007 - I ZR 35/04, GRUR 2007, 708 Rn. 28 – Internetversteigerung II; *BGH*, Urt. v. 22.7.2010 - I ZR 139/08, GRUR 2011, 152 Rn. 31 – Kinderhochstühle im Internet.

Außerdem würde der Auskunftsanspruch nach Absatz 1 auch im Urheberrecht eine Rechtsverletzung in gewerblichem Ausmaß voraussetzen. Dabei müsste man auf die Handlung des Diensteanbieters – und nicht etwa auf die Rechtsverletzung des Nutzers – abstellen. Es ist aber schwierig, Anzahl und Schwere der Rechtsverletzung des Diensteanbieters zu bestimmen, da der gegenständliche rechtsverletzende Inhalt eigentlich vom Nutzer ausgeht. Es wäre widersprüchlich, wenn man allein aufgrund der Stellung als Dienstanbieter von einem gewerblichem Ausmaß ausgehen würde, obwohl dieses bei der rechtsverletzenden Handlung des privaten Nutzers gegebenenfalls abzulehnen wäre.[126] Auch dieser Aspekt spricht daher dafür, Absatz 1 für Dienstanbieter i.S.d. § 2 Abs. 1 UrhDaG bei einer Rechtsverletzung nach § 1 Abs. 1 UrhDaG nicht anzuwenden. Vielmehr existiert mit Absatz 2 eine spezielle Anspruchsgrundlage für einen Drittauskunftsanspruch, der auch auf diese Fälle ausschließlich Anwendung finden sollte.

Bei der Identifizierung eines anonymen Rechtsverletzers im Internet ist daher ausschließlich Absatz 2 anzuwenden, unabhängig davon, ob der Diensteanbieter für die Rechtsverletzung seiner Nutzer selbst als Störer oder Rechtsverletzer haftet.

3. Zwischenfazit zum Drittauskunftsanspruch im Bereich des geistigen Eigentums

Die gesetzgeberische Intention, durch den Anspruch aus Absatz 2 eine Grundlage für eine Auskunft gegen Internetdiensteanbieter zur Ermittlung der Identität des Rechtsverletzers zu schaffen, ist im Hinblick auf das Rechtsdurchsetzungsinteresse der Rechteinhaber grundsätzlich zu befürworten. Allerdings erreicht Absatz 2 dieses Ziel nur teilweise.

Bei der Ausgestaltung des Anspruchs wurde an einigen Stellen die spezielle Situation bei Rechtsverletzungen im Internet nicht ausreichend berücksichtigt. Nur

---

[126] Das gewerbliche Ausmaß wäre zumindest bei gutgläubigen privaten Endnutzern abzulehnen; S. dazu *Beschlussempfehlung des Bundestags,* BT-Drs. 16/8783, S. 50; S. auch Erwägungsgrund 40 der RL 2004/48/EG; Darüber hinausgehend aber etwa *OLG Köln,* 9.2.2009 – 6 W 182/08, ZUM 2009, 425, 427 f. – Die schöne Müllerin; S. allgemein zur Auslegung des Begriffs *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 142 ff.; *Weidert/Molle* in: Ensthaler/Weidert, Kap. 7 Rn. 366 ff.

ein in der Praxis oft zu großzügiger und mit dem Wortlaut der Normen nur schwer vereinbarer Umgang führt dazu, dass der Auskunftsanspruch bisher in vielen Fällen nicht ins Leere gelaufen ist.[127]

Große Schwierigkeiten kann den Rechteinhabern insbesondere der Nachweis einer offensichtlichen Rechtsverletzung bereiten. Bei einer unklaren Rechts- oder Tatsachenlage ist derzeit ein Auskunftsanspruch abzulehnen.

Problematisch ist auch, dass weder IP-Adressen noch Telefonnummern, E-Mail-Adressen oder Kontodaten vom Umfang des Auskunftsanspruchs erfasst werden. Zudem erstrecken sich – zumindest ihrem Wortlaut nach – die Ansprüche aus § 19 MarkenG, § 46 DesignG und § 37b SortenSchG nicht auf Auskünfte über die Identität des Nutzers einer Dienstleistung.

Zudem können lediglich Diensteanbieter in Anspruch genommen werden, deren Dienste auch tatsächlich für eine rechtsverletzende Handlung genutzt wurden.

Auch vermag es nicht zu überzeugen, den Diensteanbietern die komplexe Entscheidung über die Verhältnismäßigkeit einer Auskunftserteilung zu überlassen, obwohl deren eigene Interessen hiervon ebenfalls berührt werden. Außerdem sind das Verhältnismäßigkeitserfordernis, das Merkmal der offensichtlichen Rechtsverletzung und die Haftungsprivilegierung des Diensteanbieters bei wahrheitsgemäßer Auskunft nicht aufeinander abgestimmt.

Ein Teil der Unstimmigkeiten ist auf die Vermischung der verschiedenen Zielsetzungen der Ansprüche aus Absatz 1 und Absatz 2 zurückzuführen. Ein Anspruch gegen einen unmittelbaren Rechtsverletzer (Absatz 1) auf Auskunft über Herkunft und Vertriebswege der rechtsverletzenden Vervielfältigungsstücke oder sonstigen Erzeugnisse ist völlig anders zu beurteilen als ein Drittauskunftsanspruch zur Identifizierung anonymer Rechtsverletzer im Internet (Absatz 2). Daher ist eine strikte Trennung der verschiedenen Auskunftsansprüche

---

[127] S. hierzu teilweise, ohne auf die aufgezeigten Probleme überhaupt einzugehen *OLG Köln*, Beschl. v. 20.4.2016 – 6 W 37/16, ZUM-RD 2016, 467, 467 – The Walking Dead; *OLG Frankfurt*, Beschl. v. 12.5.2009 – 11 W 21/09, ZUM 2009, 639, 640; *LG Köln*, Beschl. v. 17.12.2008 - 38 OH 8/08, MMR 2009, 489.

geboten. Deshalb wäre eine Klarstellung wünschenswert, dass es sich bei dem Auskunftsanspruch nach Absatz 2 um einen eigenständigen Anspruch handeln muss. Zugleich sollte dieser Anspruch die besondere Situation der Rechteinhaber, Diensteanbieter und Nutzer im Online-Bereich noch stärker berücksichtigen.

II. Auskunftsanspruch nach § 21 Abs. 2 S. 2 TTDSG

Neben den Auskunftsansprüchen im Bereich des geistigen Eigentums existiert seit Kurzem eine weitere spezielle Anspruchsgrundlage für einen Drittauskunftsanspruch gegen Internet-Diensteanbieter. § 21 TTDSG wurde im Zuge des Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien eingeführt.[128] Dieses Gesetz dient dem Zweck, Rechtsklarheit zu schaffen, indem es die auch nach dem Inkrafttreten der DS-GVO weiterhin gültigen Datenschutzregelungen aus dem TMG und TKG im neuen TTDSG zusammenfasst.[129] § 21 TTDSG übernimmt weitgehend die vorherige Regelung aus § 14 TMG a.F.[130]

§ 21 Absatz 2 S. 1 TTDSG sieht vor, dass der Anbieter von Telemedien im Einzelfall Auskunft über bei ihm vorhandene Bestandsdaten erteilen darf, soweit dies zur Durchsetzung zivilrechtlicher Ansprüche wegen der Verletzung absolut geschützter Rechte aufgrund rechtswidriger Inhalte, die von § 10a Abs. 1 TMG oder § 1 III NetzDG erfasst werden, erforderlich ist. In § 21 Abs. 2 S. 2 TTDSG ist neuerdings zusätzlich geregelt, dass der Telemediendienst in diesem Umfang zur Auskunft verpflichtet ist.

1. § 21 Abs. 2 S. 2 TTDSG als Anspruchsgrundlage

Bei § 14 Abs. 3-5 TMG a.F. handelte es sich lediglich um eine datenschutzrechtliche Erlaubnisnorm, die ein Gestattungsverfahren für Auskunftsansprüche gegen Telemediendiensteanbieter bei der Verletzung absoluter Rechte vorsah. Diese datenschutzrechtliche Erlaubnis und die Regelung des Gestattungsverfahrens wurden in § 21 Abs. 2-4 TTDSG übernommen.

---

[128] S. BGBl. I 2021, 1982.
[129] Vgl. *Regierungsentwurf,* BT-Drs. 19/27441, S. 1.
[130] *Regierungsentwurf,* BT-Drs. 19/27441, S. 37.

§ 14 Abs. 3-5 TMG a.F. enthielt zunächst keine Anspruchsgrundlage für das Auskunftsbegehren des Verletzten.[131] Das ergab sich aus dem Wortlaut der Norm, die lediglich vorsah, dass der Diensteanbieter unter bestimmten Voraussetzungen eine Auskunft erteilen durfte, nicht aber, dass er dazu auch verpflichtet war.[132] Als Anspruchsgrundlage für einen Auskunftsanspruch kam daher früher nur ein aus § 242 BGB abgeleiteter allgemeiner Auskunftsanspruch in Betracht. Da dieser keine richterliche Anordnung erforderte, stellte sich die Frage des Verhältnisses zwischen § 14 Abs. 3-5 TMG a.F. und der dazugehörigen Anspruchsgrundlage.

Teilweise wurden deshalb im Rahmen des Gestattungsverfahrens durch die Rechtsprechung isoliert nur die Voraussetzungen aus § 14 Abs. 3-5 TMG a.F. geprüft, ohne auf den Auskunftsanspruch überhaupt einzugehen.[133] Dadurch bestand aber die Gefahr, dass im Rahmen des Verfahrens nach § 14 Abs. 3-5 TMG a.F. die Auskunftserteilung gestattet wird, obwohl die Voraussetzungen des § 242 BGB nicht erfüllt sind. Auch der *BGH* hatte diese Problematik erkannt und daher bereits vor der Änderung der Norm in einer Grundsatzentscheidung zu § 14 Abs. 3-5 TMG a.F. klargestellt, dass die Gerichte im Rahmen des Verfahrens nach § 14 Abs. 3-5 TMG a.F. auch zu prüfen haben, ob in materieller Hinsicht ein Auskunftsanspruch besteht.[134]

Dennoch verpflichtete die bloße Gestattungsanordnung die Diensteanbieter nicht zur Auskunft. War der Diensteanbieter trotz der Gestattung nicht zur Auskunftserteilung bereit, mussten die Rechteinhaber ihren Anspruch erst in einem zweiten Verfahren durchsetzen.[135] Aus der Perspektive der Diensteanbieter bestand bei einem solchen zweiten Prozess die Gefahr einer Kostentragung,

---

[131] Anders wohl *LG Berlin*, Beschl. v. 21.1.2020 - 27 AR 17/19, BeckRS 2020, 239 Rn. 9.

[132] S. dazu auch *Beschlussempfehlung und Bericht des Ausschusses für Recht und Verbraucherschutz*, BT-Drs. 18/13013, S.23.

[133] S. etwa *LG Frankfurt*, Beschl. v. 18.2.2019 - 2-03 O 174/18, BeckRS 2019, 3545 Rn. 30. Ähnlich *LG Berlin*, Beschl. v. 21.1.2020 - 27 AR 17/19, BeckRS 2020, 239 Rn. 9 wohl unter der Annahme, dass § 14 Abs. 3-5 TMG eine Anspruchsgrundlage für das Auskunftsbegehren darstellt.

[134] *BGH*, Beschl. v. 24.9.2019 – VI ZB 39/18, GRUR 2020, 101 Rn. 58 – Facebook-Messenger.

[135] *Bohlen,* NJW 2020, 1999, 2002.

sodass diese möglicherweise vorsichtshalber die Auskunft erteilt hätten, auch wenn sie im Einzelfall dazu gar nicht verpflichtet gewesen wären.

Inzwischen hat der Gesetzgeber reagiert und die Regelung des § 14 Abs. 3-5 TMG a.F., die durch § 21 Abs. 2-4 TTDSG übernommen wurde, angepasst. Nach § 21 Abs. 3 S. 2 TTDSG entscheidet das Gericht nunmehr auch über die Verpflichtung zur Auskunftserteilung. Dadurch bleibt den Beteiligten ein zweistufiges Verfahren erspart. Außerdem wurde die Regelung (§ 21 Abs. 2 S. 2 TTDSG) dahingehend ergänzt, dass unter den Voraussetzungen der Auskunftsgestattung der Diensteanbieter auch zur Erteilung der Auskunft verpflichtet ist.[136] Dabei verzichtete der Gesetzgeber aber ausdrücklich darauf, „den allgemeinen Auskunftsanspruch auf Grundlage von § 242 BGB zu kodifizieren".[137] Stattdessen wurde nur für den Bereich des § 21 Abs. 2-4 TTDSG eine Sonderregelung geschaffen.[138] Sofern die Voraussetzungen für die Gestattung der Auskunft vorliegen, besteht nun also nach § 21 Abs. 2 S. 2 TTDSG auch ein Anspruch auf Erteilung der Auskunft.[139]

2. Passivlegitimation

Zur Auskunft verpflichtet sind lediglich Anbieter von Telemediendiensten. Im Unterschied zu den Auskunftsansprüchen im Bereich des geistigen Eigentums werden andere Diensteanbieter – insbesondere Telekommunikationsdienste - nicht erfasst. Dafür ist es im Rahmen des § 21 Abs. 2 S. 2 TTDSG unerheblich, ob der Telemediendienst, von dem die Auskunft begehrt wird, zur Rechtsverletzung genutzt wurde. Anders als bei dem allgemeinen aus § 242 BGB abgeleiteten Auskunftsanspruch kommt es nicht auf ein – durch die Störerhaftung begründbares – Rechtsverhältnis zwischen Diensteanbieter und Rechteinhaber an.

Bei der Vorgängerregelung aus § 14 Abs. 3-5 TMG a.F. wurde auf Grund des Verweises auf das NetzDG teilweise davon ausgegangen, dass die Regelung nur

---

[136] S. *Regierungsentwurf,* BT-Drs. 19/18792, S. 55.

[137] S. *Regierungsentwurf,* BT-Drs. 19/18792, S. 55.

[138] S. *Regierungsentwurf,* BT-Drs. 19/18792, S. 55.

[139] S. *OLG Schleswig*, Beschl. v. 23.3.2022 – 9 Wx 23/21, GRUR-RS 2022, 5901 Rn. 34. S. auch *Freytag,* GRUR-Prax 2021, 716, 716.

auf soziale Netzwerke anwendbar sei.[140] Inzwischen verweist die Regelung des § 21 Abs. 2 TTDSG auch auf rechtswidrige Inhalte nach § 10a Abs. 1 TMG, sodass man diese Diskussion auch um die Anbieter von Videosharingdiensten erweitern könnte, sodass je nach Rechtsverletzung nur die Anbieter sozialer Netzwerke oder von Videosharingdiensten auskunftspflichtig wären.[141] Der *BGH* hatte jedoch schon bei der Diskussion im Rahmen von § 14 Abs. 3-5 TMG a.F. klargestellt, dass sich der Verweis auf das NetzDG nur auf die Strafvorschriften beziehe, bei deren Verwirklichung ein Auskunftsanspruch bestehe, nicht aber auf den persönlichen Anwendungsbereich des § 14 Abs. 3-5 TMG. a.F.[142] Dem ist im Hinblick auf den insoweit eindeutigen Wortlaut der Norm und die Gesetzgebungsmaterialien auch beizupflichten.[143] Entsprechend ist auch § 21 Abs. 2 S. 2 TTDSG auf alle Anbieter von Telemediendiensten anwendbar.

3. Anforderung an die Rechtsverletzung

Der Anwendungsbereich des § 21 Abs. 2 TTDSG erstreckt sich lediglich auf die Verletzung absolut geschützter Rechte durch rechtswidrige Inhalte im Sinne von § 10a TMG oder § 1 Abs. 3 NetzDG. Nach § 1 Abs. 3 NetzDG sind nur solche Inhalte rechtswidrig, die die abschließend aufgezählten Straftatbestände der §§ 86, 86a, 89a, 91, 100a, 111, 126, 129 bis 129b, 130, 131, 140, 166, 184b, 185 bis 187, 189, 201a, 241 oder 269 StGB erfüllen.[144] Daneben erfasst § 21 Abs. 2 TTDSG rechtswidrige Inhalte im Sinne des § 10a Abs. 1 TMG. Damit werden Inhalte beschrieben, deren Rechtswidrigkeit auf einer Regelung beruhen, die auf § 10a Abs. 1 TMG verweist. Derzeit betrifft dies rechtswidrige Inhalte im Sinne von § 5b JMStV, die entweder nach § 4 JMStV unzulässig sind oder entwicklungsbeeinträchtigende Angebote nach § 5 Abs. 1, 2, 6 JMStV, die der

---

[140] *OLG Nürnberg,* Beschl. v. 17.7.2019 – 3 W 1470/19, MMR 2020, 322 Rn. 13; *OLG Frankfurt*, Beschl. v. 6.9.2018 – 16 W 27/18, ZD 2019, 127, 127; *Pille,* NJW 2018, 3545, 3546; *Mafi-Gudarzi,* K&R 2018, 466, 467.

[141] S. zum Begriff des Videosharingplattform-Dienstes § 2 Nr. 10 TMG.

[142] *BGH*, Beschl. v. 24.9.2019 – VI ZB 39/18, GRUR 2020, 101 Rn. 49 ff. – Facebook-Messenger.

[143] S. dazu *Regierungsentwurf,* BT-Drs. 18/12727, 25. S. auch *OLG Köln,* Beschl. v. 11.3.2021 – 15 W 10/21, BeckRS 2021, 7395; *Bohlen,* NJW 2020, 69, 70; *Prinz,* K&R 2020, 69, 70.

[144] S. auch *Ettig* in: Taeger/Gabler, § 21 TTDSG Rn. 12 f. S. noch zu § 14 Abs. 3-5 TMG *Schmitz* in: Spindler/Schmitz, § 14 TMG Rn. 58 f.

Anbieter des Video-Sharing-Dienstes der Allgemeinheit bereitstellt, ohne seiner Verpflichtung aus § 5 Abs. 1, 3 bis 5 nachzukommen.[145]

Bei den in § 1 Abs. 3 NetzDG genannten Straftatbeständen handelt es sich um Delikte, die entsprechend dem Schutzzweck des NetzDG vor allem dem Zweck der Gewährleistung der öffentlichen Sicherheit der Kommunikation im Netz dienen.[146] Eine ähnliche Schutzrichtung verfolgt § 10a TMG i.V.m. §§ 4, 5 JMStV. § 10a TMG dient der Umsetzung von Art. 28b AVMD-Richtlinie[147] und damit „dem Schutz Minderjähriger vor entwicklungsbeeinträchtigenden Inhalten und der Allgemeinheit vor Hass und Gewaltaufrufen".[148] Als rechtsverletzende Inhalte sind etwa Verletzungen der Menschenwürde (§ 4 Abs. 1 S.1 Nr. 8 JMStV) oder Posendarstellungen Minderjähriger (§ 4 Abs. 1 S. 1 Nr. 9 JMStV) erfasst.[149]

Für die individuelle Rechtsdurchsetzung bei Rechtsverletzungen im Internet sind vor allem die in § 1 Abs. 3 NetzDG aufgezählten Delikte relevant, die auch im Wege der Privatklage nach § 374 Abs. 1 StPO verfolgt werden können. Das gilt insbesondere für die Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen nach § 201a StGB, die Bedrohung nach § 241 StGB oder für die Ehrverletzungsdelikte der §§ 185-187 StGB.

Theoretisch erfasst § 21 Abs. 2 S. 2 TTDSG alle absoluten Rechte. Der sachliche Anwendungsbereich deckt aber durch die Begrenzung auf ganz bestimmte rechtswidrige Inhalte insgesamt nur einen Teil der häufigen Rechtsverletzungen im Internet ab. Bei Namensrechtsverletzungen oder sonstigen Persönlichkeitsrechtsverletzungen, die die Schwelle zur Strafbarkeit nicht überschreiten,

---

[145] *Ettig* in: Taeger/Gabler, § 21 TTDSG Rn. 13.

[146] *Gersdorf,* MMR 2017, 439, 441; *Heckmann/Wimmers*, CR 2017, 310, 311; *Heidrich/Scheuch* in: Taeger, Recht 4.0, 305, 314; *Hoven/Gersdorf* in: BeckOK Informations- und Medienrecht, § 1 NetzDG Rn. 4.

[147] Richtlinie 2010/13/EU des europäischen Parlaments und des Rates vom 10. März 2010 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste), Abl. 2010 L95, 1.

[148] *Holznagel/Hartmann* in: Hoeren/Sieber/Holznagel, Teil 3 Rn. 62.

[149] Ausführlicher dazu, S. *Liesching* in: BeckOK JMStV, § 4 JMStV Rn. 7 ff.

besteht in der Regel kein Anspruch auf Auskunft nach § 21 Abs. 2 S. 2 TTDSG. Anders als von *Lampmann* angenommen, erstreckt sich der Anspruch auch nicht auf Urheberrechtsverletzungen.[150] § 10a TMG normiert zwar Pflichten für Videosharing-Dienste, allerdings trifft § 10a TMG selbst keine Regelung zu rechtswidrigen Inhalten, sondern wird erst durch einen Verweis auf diese Vorschrift aktiviert.[151] § 21 Abs. 2 S. 2 TTDSG erfasst deshalb lediglich rechtswidrige Inhalte im Sinne der §§ 4, 5 JMStV.

Dagegen kommt ein Auskunftsanspruch vor allem bei schwerwiegenden Persönlichkeitsrechtsverletzungen wie etwa Beleidigungen oder der Verbreitung intimer Fotos in Betracht.[152] Bei Verletzungen des Rechts am eingerichteten und ausgeübten Gewerbebetrieb kann es zudem zu einem Anspruch etwa wegen einer Verletzung nach § 1 Abs. 3 NetzDG iVm § 186 oder § 187 StGB kommen.[153]

Allerdings fehlen in der Aufzählung des § 1 Abs. 3 NetzDG die neu eingeführten Straftatbestände der gefährdenden Verbreitung personenbezogener Daten (§ 126a StGB), sowie die verhetzende Beleidigung (§ 192a StGB). Da diese Delikte vor allem im Online-Bereich relevant werden und sich gegen die Verbreitung von Hass und Hetze richten, wäre eine entsprechende Ergänzung sinnvoll.

Eine weitere Einschränkung resultiert aus der Beschränkung des Anspruchs auf „rechtswidrige Inhalte". Sonstige gegebenenfalls rechtsverletzende

---

[150] *Lampmann*, NJW 2021, 783, 783 f. m.Anm. zu *BGH*, Urt. v. 10.12.2020 – I ZR 153/17 - YouTube-Drittauskunft II; Ähnlich wohl auch *Bornemann* in: BeckOK Informations- und Medienrecht, § 10a TMG Rn. 13.

[151] S. auch *Regierungsentwurf,* BT-Drs. 19/18789, S. 38.

[152] Vgl. noch zum reinen Gestattungsverfahren nach § 14 Abs. 3-5 TMG a.F. *BGH*, Beschl. v. 24.9.2019 – VI ZB 39/18, GRUR 2020, 101, 101 ff. – Facebook-Messenger.

[153] Vgl. noch zum Auskunftsanspruch nach § 242 BGB i.V.m. § 14 Abs. 3-5 TMG a.F. *OLG Celle*, Beschl. v. 23.9.2021 – 5 W 39/21, GRUR-RS 2021, 31960 Rn. 17 – Ex-Angestellte; *OLG Köln,* Beschl. v. 11.3.2021 – 15 W 10/21, MMR 2021, 573 Rn. 43 ff. S. außerdem zur Beleidigungsfähigkeit und zur Verleumdung gegenüber juristischen Personen und Personenvereinigungen *Valerius* in: BeckOK StGB, § 185 Rn.8 ff., § 187 Rn 4.

Verhaltensweisen wie etwa das Erstellen eines Fake-Profils werden daher nicht vom Anspruch aus § 21 Abs. 2 S. 2 TTDSG erfasst.[154]

4. Erforderlichkeit zur Durchsetzung zivilrechtlicher Ansprüche

Die Verpflichtung zur Auskunftserteilung besteht nur soweit dies zur Durchsetzung zivilrechtlicher Ansprüche erforderlich ist. Der Gesetzgeber ging davon aus, dass diese Voraussetzung den Voraussetzungen des aus § 242 BGB abgeleiteten Auskunftsanspruchs ähnelt.[155] Dementsprechend muss der Rechteinhaber ein Informationsbedürfnis haben. Ein Auskunftsanspruch dürfte ausgeschlossen sein, soweit der Rechteinhaber die Möglichkeit hat, die begehrte Informationen anderweitig zu erhalten.

5. Umfang der Auskunftserteilung

Vom Umfang des Auskunftsanspruchs werden alle Bestandsdaten der Telemediendiensteanbieter erfasst. Dies betrifft etwa Namen, Anschriften, E-Mail-Adressen, Kontoinformationen, Telefonnummern und Pseudonyme der Nutzer. Auf die Vorgängerregelung des § 14 TMG a.F. wurde noch durch § 15 Abs. 5 S. 4 TMG a.F. verwiesen, sodass sich der Umfang von § 14 Abs. 3-5 TMG a.F. auch auf Nutzungsdaten erstreckte.[156] Dieser Verweis aus § 15 Abs. 5 S. 4 TMG a.F. ist aber inzwischen weggefallen. § 21 Abs. 2 S. 2 TTDSG betrifft deshalb ausschließlich Bestandsdaten. Daten, die während des Nutzungsvorgangs anfallen – wie zum Beispiel die IP-Adresse – werden von der Regelung nicht erfasst.

6. Zwischenfazit zum Anspruch aus § 21 Abs. 2 S. 2 TTDSG

Der Anwendungsbereich des § 21 Abs. 2 S. 2 TTDSG ist deshalb insgesamt in verschiedener Hinsicht begrenzt. Die Vorschrift regelt lediglich die Auskunftserteilung durch Telemediendienste. Außerdem besteht der Anspruch nur bei bestimmten Rechtsverletzungen. Zudem beschränkt sich der Anspruchsumfang auf Bestandsdaten.

---

[154] Etwas anderes gilt aber, wenn das Erstellen des Fake-Profis zum Beispiel in Verbindung zum Beispiel mit dem Verbreiten eine Beleidigung i.S.d. § 185 StGB darstellt, S. dazu *OLG Schleswig,* Beschl. v. 23.3.2022 – 9 Wx 23/21, GRUR-RS 2022, 5901 Rn. 26.

[155] *Regierungsentwurf,* BT-Drs. 19/18792, S. 55.

[156] *Ettig* in: Taeger/Gabler, § 21 TTDSG Rn. 10.

Das führt zum einen dazu, dass der Auskunftsanspruch in vielen Fällen unzureichend ist, um einen anonymen Rechtsverletzer zu identifizieren. Eine Identifizierung anhand der IP-Adresse etwa kann der Anspruch nicht ermöglichen. Zum anderen werden einige Fallkonstellationen trotz Verletzung absoluter Rechte überhaupt nicht erfasst.

Letzteres ist vermutlich darauf zurückzuführen, dass die Vorgängerregelung des § 14 Abs. 3-5 TMG a.F. im Zuge des Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG) eingeführt wurde. § 14 Abs. 3-5 TMG a.F. ergänzte lediglich die Regelungen des NetzDG. Das NetzDG sollte vor allem zu einer Lösung gesellschaftlich relevanter Probleme insbesondere im Hinblick auf eine Verschärfung des gesellschaftlichen Diskurses durch die „nicht selten hasserfüllte" Debattenkultur im Netz beitragen.[157] Der Schwerpunkt lag dabei insgesamt vor allem auf einer stärkeren Verantwortlichkeit der Betreiber sozialer Netzwerke, aber nicht vordergründig auf der Verbesserung der individuellen Rechtsdurchsetzung gegen anonyme Nutzer.

III. Analoge Anwendung sonstiger spezieller Ansprüche

Neben den bislang untersuchten Ansprüchen existieren in §§ 13, 13a UKlaG und § 810 BGB spezielle Anspruchsgrundlagen, die in analoger Anwendung den Rechteinhabern eine Identifizierung eines anonymen Rechtsverletzers ermöglichen könnten. Eine solche entsprechende Anwendung der genannten Vorschriften kommt allerdings bei Rechten des geistigen Eigentums nicht in Betracht, da auf Grund der spezialgesetzlichen Auskunftsansprüche offensichtlich keine Regelungslücke existiert.

Bei allen Verletzungen sonstiger absolut geschützter Rechte, die nicht von § 21 Abs. 2 S. 2 TTDSG erfasst werden, wäre eine analoge Anwendung von spezielleren Anspruchsgrundlagen, denen eine vergleichbare Interessenslage zugrunde liegt, dem allgemeinen aus § 242 BGB abgeleiteten Auskunftsanspruch vorzuziehen.

---

[157] S. *Regierungsentwurf,* BT-Drs. 18/12356, S. 1.

1. §§ 13, 13a UKlaG

§§ 13, 13a UKlaG gewährt zur Durchsetzung bestimmter Unterlassungsansprüche einen Auskunftsanspruch gegen Telekommunikations- und Telemedien-diensteanbieter. Nach § 13 UKlaG sind jedoch nur Industrie- und Handelskammern, rechtsfähige Verbände zur Förderung gewerblicher oder selbstständiger beruflicher Interessen und qualifizierte Einrichtungen im Sinne von § 13 Abs. 1 UKlaG auskunftsberechtigt. Zudem kann eine Auskunft nur zur Durchsetzung der Ansprüche aus § 1 bis 2a und § 4a UKlaG erteilt werden. Nach § 13a UKlaG können auch sonstige Inhaber von Unterlassungsansprüchen auskunftsberechtigt sein. Jedoch gilt dies nur für den engen Anwendungsbereich der Lieferung unbestellter Sachen, der Erbringung unbestellter sonstiger Leistungen oder der Zusendung oder sonstiger Übermittlung unverlangter Werbung. §§ 13, 13a UKlaG kann daher zumindest nicht direkt angewendet werden.

Mit der Einführung von §§ 13, 13a UKlaG wurde auf die Problematik reagiert, dass die Inhaber von Unterlassungsansprüchen zur Durchsetzung ihrer Ansprüche Kenntnis von Namen und ladungsfähiger Anschrift des Anspruchsverpflichteten benötigen.[158] Hat der Anspruchsgegner zum Beispiel nur eine Internetadresse angegeben, lässt sich der Unterlassungsanspruch nicht ohne weiteres durchsetzen. §§ 13, 13a UKlaG normieren also Auskunftsansprüche gegen Diensteanbieter zur Verbesserung der Durchsetzbarkeit von bestimmten Unterlassungsansprüchen.

Auf den ersten Blick erscheint daher zumindest die Interessenlage vergleichbar. In vielen Fällen, in denen im Internet Rechte verletzt werden, stehen dem Grunde nach dem Rechteinhaber Unterlassungsansprüche gegen den Rechtsverletzer zu. Oft steht der Durchsetzbarkeit dieser Ansprüche jedoch entgegen, dass die Identität des Verletzers nicht bekannt ist.

Dennoch ist eine analoge Anwendbarkeit im Hinblick auf den Zweck der Normen abzulehnen, da die §§ 13, 13a UKlaG als enge Ausnahmevorschriften

---

[158] Hierzu etwa statt vieler *Micklitz/Rott* in: MüKo ZPO, § 13 UKlaG Rn. 1 f.

lediglich die Durchsetzbarkeit verbraucherschützender Vorschriften und nicht die Durchsetzung von Individualinteressen gewährleisten sollen.[159]

Dem könnte man zwar entgegenhalten, dass in den Fällen von § 13a UKlaG zum Beispiel bei der Lieferung unbestellter Sachen auch Unterlassungsansprüchen von Mitbewerbern aus den §§ 3, 8 Abs. 1 UWG sowie den §§ 823 Abs. 1, 862, 1004 BGB analog wegen Verletzung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb erfasst sind,[160] sodass durchaus auch die Rechtsdurchsetzung bei einer Verletzung von Individualrechtsgütern verbessert wird. Allerdings handelt es sich dabei wohl nicht um den primären Zweck dieser Vorschrift.

Zudem stellen die §§ 13, 13a UKlaG im Hinblick auf den speziellen Anwendungsbereich im Zusammenhang mit einzelnen verbraucherschützenden Vorschriften Ausnahmevorschriften dar, die einer Analogie nicht zugänglich sind.[161] Darüber hinaus ist zu bemerken, dass eine Auskunft über Verkehrsdaten von der Rechtsfolge der §§ 13, 13a UKlaG ohnehin nicht gedeckt wäre.[162] Daher bestünde selbst bei einer analogen Anwendung lediglich die Möglichkeit, Auskunft über die beim Diensteanbieter vorhandenen Bestandsdaten zu erhalten.

2. § 810 BGB

Bei § 810 BGB handelt es sich zwar nicht um einen Auskunftsanspruch, allerdings regelt dieser ein Einsichtnahmerecht in Urkunden, durch das der Verletzte ebenfalls Informationen über die Identität des Rechtsverletzers erlangen könnte. Für die Rechteinhaber könnte vor allem eine Einsichtnahme in die gespeicherten Log-Dateien eines Diensteanbieters von Interesse sein, um an die IP-

---

[159] So zumindest im Hinblick auf eine Anwendung bei Urheberrechtsverletzungen vor Einführung von § 101 UrhG n.F. auch *Kohl,* Haftung der Betreiber von Kommunikationsforen, S. 155; *Kramer,* Zivilrechtlicher Auskunftsanspruch, S. 84.

[160] Vgl. *LG Bonn,* Urt. v. 19.7.2004 - 6 S 77/04, MMR 2004, 767; *Micklitz/Rott* in: MüKO ZPO, § 13 UKlaG Rn. 3.

[161] Hierzu etwa *BGH*, Urt. v. 2.5.2002 - I ZR 45/01, NJW-RR 2002, 1617, 1619 - Faxkarte.

[162] *Welp*, Auskunftspflicht von Access-Providern, S. 40.

Adresse und die Zugriffszeiten der Nutzer zu gelangen.[163] Solche technischen Aufzeichnungen stellen jedoch mangels verkörperter Gedankenerklärung keine Urkunden im zivilprozessualen Sinne dar.[164]

Daher kommt ebenfalls nur eine analoge Anwendung der Vorschrift im Hinblick auf technische Aufzeichnungen in Betracht. Allerdings gewährt § 810 BGB das Recht zur Einsichtnahme nur, wenn die technische Aufzeichnung im Interesse des Anspruchstellers errichtet wurden oder ein Rechtsverhältnis zwischen dem Anspruchsteller und einem Dritten beurkundet wird.

Hier liegen jedoch weder die weiteren Voraussetzungen des § 810 BGB vor, noch stellt sich die Interessenslage vergleichbar dar. In den Log-Dateien der Diensteanbieter wird lediglich die Internetnutzung und damit allenfalls ein Rechtsverhältnis zwischen dem Diensteanbieter und den Nutzern dokumentiert.[165] Auch werden diese Daten nicht gespeichert, um einem Dritten die Möglichkeit der Rechtsverfolgung zu schaffen.[166] Außerdem kann davon ausgegangen werden, dass sich auf einem entsprechenden Datenträger eine Vielzahl von Daten befinden würden, an deren Einsicht die Rechteinhaber kein berechtigtes Interesse haben. Auch eine analoge Anwendung des § 810 BGB ist daher abzulehnen.

3. Fazit zur analogen Anwendung bereits bestehender Vorschriften

Die Ausführungen zeigen, dass eine analoge Anwendung von Vorschriften, die in einem anderen Kontext erlassen wurden, auf die Situation anonymer Rechtsverletzungen im Internet äußerst problematisch ist.

Dies lässt sich auch darauf zurückführen, dass der Gesetzgeber abseits der IP-Rechte und von § 21 Abs. 2 S. 2 TTDSG bewusst auf eine Einführung von spezialgesetzlichen Auskunftsansprüchen gegen Internetdiensteanbieter verzichtet

---

[163] S. zu entsprechenden Überlegungen im Bereich des Urheberrechts *Kitz*, GRUR 2003, 1014, 1016; *Kramer*, Zivilrechtlicher Auskunftsanspruch, S. 89; *Welp*, Auskunftspflicht von Access-Providern, S. 41 f.

[164] S. etwa *Habersack* in: MüKo BGB, § 810 BGB Rn. 3.

[165] *Kitz*, GRUR 2003, 1014, 1016; *Welp*, Auskunftspflicht von Access-Providern, S. 41 f.

[166] *Kitz*, GRUR 2003, 1014, 1016; *Welp*, Auskunftspflicht von Access-Providern, S. 41 f.

hat, obwohl die Problematik durchaus bekannt war.[167] Daher lässt sich regelmäßig bereits an der Planwidrigkeit der Regelungslücke zweifeln. Entsprechend ist auch eine analoge Anwendung der immaterialgüterrechtlichen Drittauskunftsansprüche bei der Verletzung von sonstigen absolut geschützten Rechten abzulehnen.

Außerdem bedarf es im Hinblick auf die hochrangigen Rechtsgüter auf beiden Seiten einer ausdrücklichen Regelung, die die widerstreitenden Interessen zu einem angemessenen Ausgleich bringen kann. Der Rückgriff auf bereits bestehende Vorschriften, die in einem anderen Zusammenhang eingeführt wurden, erscheint daher unangebracht.

IV. Auskunftsanspruch aus § 242 BGB

Abgesehen von den bereits näher untersuchten Auskunftsansprüchen des geistigen Eigentums und aus § 21 Abs. 2 S. 2 TTDSG existieren bei Rechtsverletzungen im Internet keine speziellen gesetzlich geregelten Auskunftsansprüche gegen Internet-Provider. Außerhalb des Anwendungsbereichs dieser Vorschriften kommt daher nur ein Auskunftsanspruch gegen Internet-Diensteanbieter aus § 242 BGB in Betracht.

1. Herleitung des allgemeinen Auskunftsanspruchs aus § 242 BGB

Für einen solchen Auskunftsanspruch finden sich zunächst keine Anhaltspunkte im Gesetz. Allerdings wurde von der Rechtsprechung in verschiedenen Fallkonstellationen, in denen ein in der Praxis typisches Informationsbedürfnis besteht, ein Auskunftsanspruch in erweiterter Auslegung der §§ 259, 260 BGB auf der Grundlage des Grundsatzes von Treu und Glauben aus § 242 BGB hergeleitet.[168]

---

[167] S. zur Einführung des Anspruchs aus § 21 Abs. 2 S. 2 TTDSG, bei der der Gesetzgeber ausdrücklich davon abgesehen hat, den allgemeinen Auskunftsanspruch aus § 242 BGB zu kodifizieren *Regierungsentwurf,* BT-Drs. 19/18792; S. 55. Dass die Problematik auch davor bereits bekannt war, ergibt sich auch aus dem *Regierungsentwurf zum Netzwerkdurchsetzungsgesetz*, BT-Drs. 12356, S. 28.

[168] *BGH*, Urt. v. 28.10.1953 - II ZR 149/52, NJW 1954, 70, 70 f.

Die Anwendung dieses Auskunftsanspruchs erstreckt sich dabei auf eine große Bandbreite verschiedener Fallkonstellationen. So dient der Anspruch beispielsweise als wichtige Ergänzung einer Vielzahl von gesetzlichen Informationsansprüchen im Bereich des Familien- und Erbrechts.[169] Zudem wird § 242 BGB herangezogen, um dem Verletzten im Bereich des Lauterkeitsrechts Auskünfte zur Berechnung von Schadensersatzansprüchen zu gewähren.[170]

Allein der Umstand, dass eine Person Kenntnis über Tatsachen hat, die für eine andere Person relevant sind, verpflichtet aber natürlich nicht zur Auskunft.[171] Die Rechtsprechung hat daher eine Formel zur Konkretisierung des Auskunftsanspruchs aus § 242 BGB entwickelt: Eine Auskunftspflicht besteht demnach nur bei einem Rechtsverhältnis, dessen Wesen es mit sich bringt, dass der Berechtigte in entschuldbarer Weise über Bestehen oder Umfang seines Rechts im Ungewissen und der Verpflichtete in der Lage ist, unschwer die zur Beseitigung dieser Ungewissheit erforderlichen Auskünfte zu erteilen.[172]

2. Übertragung auf Auskunftsansprüche gegen Internetdiensteanbieter

Auch bei anonymen Rechtsverletzungen im Internet besteht ein Informationsbedürfnis des betroffenen Rechteinhabers. Dies ergibt sich daraus, dass erst die Identität des Rechtsverletzers ermittelt werden muss, bevor Ansprüche gegen den Rechtsverletzer geltend gemacht werden können.

---

[169] S. etwa *BGH*, Urt. v. 4.12.1980 - IVa ZR 46/80, NJW 1981, 2051, 2051 ff.; *BGH*, Urt. v. 2.6.1993 - IV ZR 259/92, NJW 1993, 2737, 2737 ff.; *BGH*, Urt. v. 9.12.1987 - IVb ZR 5/87, NJW 1988, 1906, 1906 ff.; *BGH*, Urt. v. 7.5.2003 - XII ZR 229/00, NJW 2003, 3624, 3624 ff.; *BGH*, Urt. v. 9.2.2005 - XII ZR 93/02, NJW 2005, 1492, 1492 ff.

[170] S. im Hinblick auf Immaterialgüterrechtsverletzungen etwa *BGH*, Urt. v. 5.6.1985 - I ZR 53/83 , NJW 1986, 1244, 1244 ff. – GEMA-Vermutung I. Hinsichtlich des Wettbewerbsrechts, S. etwa *BGH*, Urt. v. 27.11.1964 - Ib ZR 23/63, GRUR 1965, 313, 313 ff.; *BGH*, Urt. v. 16.2.1973 - I ZR 74/71, GRUR 1973, 375, 375 ff.; *BGH*, Urt. v. 11.03.1982 - I ZR 58/80, GRUR 1982, 420, 420 ff. – BBC/DDC; *BGH*, Urt. v. 2.2.1995 - I ZR 16/93, NJW 1995, 1420, 1420 ff.

[171] *BGH*, Urt. v. 22.1.1957 - VI ZR 334/55, NJW 1957, 669, 669 f.

[172] Ständige Rechtsprechung seit *BGH*, Urt. v. 28.10.1953 - II ZR 149/52, NJW 1954, 70, 70 f. S. auch *BGH*, Urt. v. 1.7.2014 - VI ZR 345/13, MMR 2014, 704 Rn. 6 m.w.N. Ausführlicher zu den Voraussetzungen des Auskunftsanspruchs aus § 242 BGB etwa *Beckhaus*, Die Bewältigung von Informationsdefiziten, S. 40 ff; *Haeffs*, Der Auskunftsanspruch, S. 127 ff.

Die Rechtsprechung gesteht den Rechteinhabern daher teilweise einen Auskunftsanspruch gegen Diensteanbieter der Informationsgesellschaft aus § 242 BGB zu. Anerkannt war dieser Anspruch vor allem bei Persönlichkeitsrechtsverletzungen im Internet.[173]

Besonderheiten ergeben sich dabei allerdings bei der Herleitung der erforderlichen rechtlichen Sonderverbindung zwischen Auskunftsschuldner und Auskunftsgläubiger. Zur Auskunft verpflichtet werden kann im Rahmen eines Anspruchs nach § 242 BGB nur derjenige, der in einem besonderen Rechtsverhältnis zum Anspruchsteller steht.

Der Auskunftsanspruch aus § 242 BGB wurde ursprünglich von der Rechtsprechung entwickelt, um im Zweipersonenverhältnis Informationsdefizite bezüglich des Inhalts oder Umfangs eines Anspruchs zu beseitigen.[174] Im Unterschied dazu geht es hier darum, einen bestehenden Anspruch gegen einen unbekannten Dritten durchsetzen zu können. Allerdings wird § 242 BGB teilweise auch bei Dreipersonenverhältnissen als Anspruchsgrundlage für einen Auskunftsanspruch herangezogen, sofern auch gegenüber dem Dritten eine rechtliche Sonderverbindung besteht. Als Beispiel ist insbesondere der lauterkeitsrechtliche Drittauskunftsanspruch aus § 242 BGB anzuführen.[175]

Das besondere Rechtsverhältnis kann sich dabei auch aus einem gesetzlichen Schuldverhältnis ergeben.[176] Zur Begründung eines Auskunftsanspruchs gegen Internet-Diensteanbieter wird daher auf einen Unterlassungsanspruch aus §§ 823, 1004 BGB abgestellt.[177]

Regelmäßig geht die Rechtsverletzung jedoch nicht vom Diensteanbieter aus, sodass gegen diese zunächst auch keine Unterlassungsansprüche bestehen.

---

[173] S. *BGH*, Urt. v. 1.7.2014 - VI ZR 345/13, MMR 2014, Rn. 6 f.; *BGH,* Beschl. v. 24.9.2019 – VI ZB 39/18, GRUR 2020, 101 Rn. 58 – Facebook Messenger; *Czychowski/Nordemann*, GRUR 2013, 986, 995; *Paschke/Halder*, MMR 2016, 723, 724.

[174] Vgl. *Kohl*, Die Haftung der Betreiber von Kommunikationsforen, S. 157.

[175] S. etwa *BGH*, Urt. v. 24.03.1994 - I ZR 42/93, NJW 1994, 1958, 1958 ff. – Cartier-Armreif; *BGH*, Urt. v. 23.2.1995 - I ZR 75/93, NJW 1995, 1965, 1965 ff. – Schwarze Liste.

[176] *BGH*, Urt. v. 1.7.2014 - VI ZR 345/13, MMR 2014, 704 Rn. 6 m.w.N.

[177] S. *BGH*, Urt. v. 1.7.2014 - VI ZR 345/13, MMR 2014, 704 Rn. 6; *Paschke/Halder*, MMR 2016, 723, 724; S. auch *Kohl,* Die Haftung der Betreiber von Kommunikationsforen, S. 157.

Anders verhält es sich nur, wenn der jeweilige Diensteanbieter - z.B. auf Grund der Verletzung von Prüfpflichten - als Störer für die Rechtsverletzung haftet.[178]

Dementsprechend lässt sich grundsätzlich ein Anspruch gegen Internet-Diensteanbieter unter die von der Rechtsprechung entwickelten Voraussetzungen für einen Auskunftsanspruch auf Grundlage des § 242 BGB subsumieren. Allerdings ist der Anwendungsbereich zumindest auf die Fälle begrenzt, in denen ein Unterlassungsanspruch gegen den Dienstanbieter auf Grundlage der Störerhaftung besteht.

3. Voraussetzungen des Auskunftsanspruchs gegen Internetdiensteanbieter

Die wichtigste Voraussetzung für den Auskunftsanspruch gegen Internetdiensteanbieter aus § 242 BGB stellt dementsprechend die Haftung des Diensteanbieters als Störer dar. Ein Rechtsverhältnis, das den Anforderungen des allgemeinen Auskunftsanspruchs gerecht wird, kann sich also aus einem gesetzlichen Schuldverhältnis nach Maßgabe der §§ 823, 1004 BGB ergeben.

Diese Voraussetzung kann den Rechteinhabern Schwierigkeiten bereiten, da der Unterlassungsanspruch gegen die Diensteanbieter an die Verletzung etwaiger Verhaltens- oder Prüfpflichten geknüpft ist.[179]

Das *OLG Celle* dagegen hat angenommen, dass der Auskunftsanspruch nicht voraussetze, dass der Diensteanbieter selbst nach den Grundsätzen der Störerhaftung noch in Anspruch genommen werden könne. Ausreichend sei das gesetzliche Schuldverhältnis, dass mit der Beanstandung des rechtsverletzenden

---

[178] S. ausführlicher zur Störerhaftung Kap. 7 § 2.

[179] *BGH*, Urt. v. 1.3.2016 – VI ZR 34/15, GRUR 2016, 855, 855 – www.jameda.de; *BGH,* Urt. v. 1.7.2014 – VI ZR 345/13, GRUR 2014, 902 Rn. 6 – Ärztetebewertung; *BGH*, Urt. v. 25.10.2011 - VI ZR 93/10, GRUR 2012, 311 Rn. 23 ff. – Blog-Eintrag; *BGH*, Urt. v. 30.6.2009 - VI ZR 210/08, GRUR 2009, 1093, 1093 – Focus Online; *BGH*, Urt. v. 21.9.2017 – I ZR 11/16, GRUR 2018, 178, 178 – Vorschaubilder III; *BGH*, Urt. v. 17.8.2011 - I ZR 57/09, GRUR 2011, 1038, 1038 – Stiftparfüm; *BGH*, Urt. v. 17.12.2010 - V ZR 44/10, GRUR 2011, 321, 321 – Preußische Gärten; *BGH*, Urt. v. 1.4.2004 - I ZR 317/01, GRUR 2004, 693, 693 – Schöner Wetten; *BGH*, Urt. v. 11.3.2004 - I ZR 304/01, GRUR 2004, 860, 860 – Internetversteigerung I; *BGH,* Urt. v. 30.4.2008 - I ZR 73/05, GRUR 2008, 702, 702 – Internetversteigerung III.

Beitrags beim Diensteanbieter entstehe und entsprechende Prüfpflichten für diesen begründe.[180] Diese Ansicht verkennt allerdings, dass das Rechtsverhältnis nach §§ 823, 1004 BGB erst durch die Verletzung etwaiger Pflichten entsteht. Andernfalls bestünde ein Widerspruch zu den Haftungsprivilegierungen der §§ 7 ff. TMG.[181] Das gesetzliche Schuldverhältnis wird deshalb erst durch die Verletzung von Verhaltens- oder Prüfpflichten begründet. Haftet der Diensteanbieter nicht zumindest als Störer für die Rechtsverletzung, besteht kein Rechtsverhältnis zwischen ihm und dem Rechteinhaber. Ein Anspruch gegen einen Dritten, der keine Verantwortung für die Rechtsverletzung trägt, lässt sich aus § 242 BGB nicht ableiten.

Wird also beispielsweise ein rechtsverletzender Inhalt durch einen Nutzer auf einer Internetseite veröffentlicht und der entsprechende Inhalt vom Betreiber der Seite nach der Beanstandung durch den Rechteinhaber wieder gelöscht, besteht in der Regel kein Unterlassungsanspruch gegen diesen.[182] Dementsprechend muss auch ein Auskunftsanspruch aus § 242 BGB in einem solchen Fall ausscheiden.[183] Dem *OLG Celle* ist daher dahingehend zuzustimmen, dass durch die Begrenzung auf die Haftung des Diensteanbieters als Störer der Anspruch in vielen Fällen ins Leere läuft.[184] In Kenntnis der bisherigen Rechtsprechung hat der Gesetzgeber aber dennoch ausdrücklich auf die Kodifizierung des Anspruchs aus § 242 BGB verzichtet und lediglich mit § 21 Abs. 2 S. 2 TTDSG eine Sonderregelung getroffen.[185]

---

[180] *OLG Celle,* Beschl. v. 23.9.2021 – 5 W 39/21, GRUR-RS 2021, 31960 Rn. 23 ff.

[181] S. dazu auch *EuGH*, Urt. v. 24. 11. 2011 - C-70/10, GRUR 2012, 265, Rn. 47 ff. – Scarlet/SABAM; *EuGH*, Urt. v. 16. 2. 2012 - C-360/10, GRUR 2012, 382 Rn. 33 – Netlog/SABAM; *BGH*, Urt. v. 16.5.2013 – I ZR 216/11, GRUR 2013, 1229 Rn. 36 – Kinderhochstühle im Internet II; *BGH*, Urt. v. 12.7.2012 – I ZR 18/11, GRUR 2013, 370, Rn. 28 – Alone in the Dark; *BGH*, Urt. v. 17.8.2011 - I ZR 57/09, GRUR 2011, 1038, Rn. 39 – Stiftparfüm.

[182] S. etwa *BGH*, Urt. v. 27.3.2012 - VI ZR 144/11, GRUR 2012, 751 Rn. 20 – RSS-Feeds.

[183] *BGH,* Urt. v. 1.7.2014 – VI ZR 345/13, GRUR 2014, 902 Rn. 6 – Ärztebewertung; *BGH*, Urt. v. 10.12.2020 – I ZR 153/17, ZUM 2021, 250 Rn. 33 f. – YouTube-Drittauskunft II; *OLG Köln,* Beschl. v. 11.3.2021 – 15 W 10/21, BeckRS 2021, 7395 Rn. 50.

[184] *OLG Celle,* Beschl. v. 23.9.2021 – 5 W 39/21, GRUR-RS 2021, 31960 Rn. 24; S. auch *OLG Köln,* Beschl. v. 11.3.2021 – 15 W 10/21, BeckRS 2021, 7395 Rn. 50.

[185] *Regierungsentwurf,* BT-Drs. 19/27441, S. 55. Vgl. auch *OLG Köln,* Beschl. v. 11.3.2021 – 15 W 10/21, BeckRS 2021, 7395 Rn. 50; *OLG Frankfurt a.M.,* Beschl. v. 6.9.2018 - 16 W 27/18, BeckRS 2018, 23780 Rn. 68; *Bohlen,* NJW 2020, 1999, 2003.

Hinzu kommt, dass mit dem dritten Änderungsgesetz zum TMG die Störerhaftung von Access-Providern abgeschafft wurde.[186] Nach § 8 Abs. 1 S. 2 TMG können diese sowie auch WLAN-Betreiber und andere Zugangsanbieter nunmehr nicht auf Schadensersatz, Beseitigung oder Unterlassung einer Rechtsverletzung in Anspruch genommen werden, sofern sie nicht für diese Rechtsverletzung verantwortlich sind. In der Regel kommt daher mangels rechtlicher Sonderbeziehung ein Anspruch aus § 242 BGB gegen Zugangsanbieter nicht in Betracht.

Die weiteren Voraussetzungen für die Auskunftserteilung sind dagegen weitgehend unproblematisch. Insbesondere lässt sich eine informationelle Notlage des Anspruchstellers bei anonymen Rechtsverletzungen im Internet gut begründen. Schließlich ist der Rechteinhaber darauf angewiesen, die Identität des Rechtsverletzers zu ermitteln, um Ansprüche gegen diesen geltend machen zu können. Zudem wird in der Regel davon auszugehen sein, dass eine Auskunftserteilung für den Diensteanbieter zumutbar ist, wenn dieser als Störer haftet, da er die erforderlichen Maßnahmen gegen die Rechtsverletzung nicht unternommen hat.

4. Kritik an der Anwendung des § 242 BGB auf Internetdiensteanbieter

Die Anwendung des § 242 BGB als Anspruchsgrundlage für Auskunftsansprüche gegen Internetdiensteanbieter überzeugt allerdings insgesamt nicht. Die Interessenslage bei anonymen Rechtsverletzungen im Internet stellt sich anders dar als bei den Fallkonstellationen, für die die Rechtsprechung den Auskunftsanspruch aus § 242 BGB ursprünglich entwickelt hat.

---

[186] Ausführlicher etwa *Grisse*, GRUR 2017, 1073, 1076; *Nicolai,* ZUM 2018, 33, 43; *Paal/Hennemann* in: BeckOK Informations- und Medienrecht, § 7 TMG Rn. 53a; *Spindler,* NJW 2017, 2305, 2305 ff.; *Volkmann* in: Spindler/Schuster, § 1004 BGB Rn. 33. Dennoch können im Bereich des geistigen Eigentums in unionsrechtskonformer Auslegungen Sperransprüchen nach § 7 Abs. 4 TMG analog gegen Access-Provider geltend gemacht werden, S. *BGH,* Urt. v. 26.7.2018 – I ZR 64/17, GRUR 2018, 1044 Rn. 49 – Dead Island; *Hennemann,* ZUM 2018, 754, 754 ff.; *Paal/Hennemann* in: BeckOK Informations- und Medienrecht, § 7 TMG Rn. 72 a ff.; *Spindler*, GRUR 2018, 1012, 1014 ff.; Anders aber *OLG München*, Urt. v. 14.6.2018 – 29 U 732/18, GRUR 2018, 1050, 1050 – Kinox.to, das weiterhin Sperransprüche auf die Störerhaftung nach § 1004 BGB analog stützt.

Die größten Überschneidungen bestehen mit der Fallgruppe des lauterkeitsrechtlichen Drittauskunftsanspruch, da auch hier ein Dritter auf Auskunft in Anspruch genommen wird. Allerdings zeigt sich bei näherer Betrachtung der gerichtlichen Entscheidungen ein deutlicher Unterschied der beiden Fallkonstellationen hinsichtlich der Interessenlage.

Im Rahmen des lauterkeitsrechtlichen Drittauskunftsanspruchs wurde beispielsweise ein Schmuckhändler dazu verpflichtet, Auskunft über die Bezugsquelle eines durch diesen angebotenen, den ergänzenden wettbewerbsrechtlichen Leistungsschutz verletzenden Armreif zu erteilen.[187] Auch ein Anbieter von Kosmetikartikeln mit entfernter Herstellernummer musste gegenüber dem Hersteller seine Bezugsquelle darlegen.[188] In beiden Fällen wurde ein lauterkeitsrechtlicher Verstoß des Anspruchsschuldners angenommen. Die rechtliche Sonderverbindung ergab sich also daraus, dass eine Person, die selbst rechtsverletzend agiert hat, Auskunft über den Ursprung beziehungsweise die Quelle dieser Rechtsverletzung geben muss.

Die Ausweitung des Anspruchs aus § 242 BGB auch auf Auskünfte über Dritte kann im Rahmen des Lauterkeitsrechts durchaus sinnvoll sein. Die untersuchten Fälle des lauterkeitsrechtlichen Drittauskunftsanspruchs unterscheiden sich allerdings sehr häufig von den Ansprüchen gegen Internetdiensteanbieter dahingehend, dass die zur Auskunft verpflichteten Diensteanbieter nicht selbst eine Rechtsverletzung begangen haben, sondern lediglich als Störer für die Rechtsverletzung eines Nutzers des angebotenen Dienstes haften. Die Internetdiensteanbieter müssen nicht über die Quelle einer durch sie selbst begangenen Rechtsverletzung Auskunft geben, sondern über die Rechtsverletzung eines Dritten, für die sie allenfalls als Störer haften.

Das nach der Formel der Rechtsprechung für den Auskunftsanspruch aus § 242 BGB erforderliche Rechtsverhältnis ergibt sich beim lauterkeitsrechtlichen Drittauskunftsanspruch gerade aus der rechtswidrigen Handlung des Auskunftspflichtigen. Die Störerhaftung von Internetdiensteanbietern dagegen stellt kein vergleichbares Rechtsverhältnis dar, aus dem sich ein

---

[187] *BGH*, Urt. v. 24.3.1994 - I ZR 42/93, NJW 1994, 1958, 1958 ff. – Cartier-Armreif.

[188] *BGH*, Urt. v. 17.5.2001 - I ZR 291/98 , GRUR 2001, 841, 841 ff. – Entfernung der Herstellungsnummer II.

Auskunftsanspruch ableiten lässt. Die Interessenslage ist nicht mit den Fallkonstellationen vergleichbar, die dem wettbewerbsrechtlichen Drittauskunftsanspruch zu Grunde liegen.

Zudem spricht auch die komplexe Interessenslage im Online-Bereich gegen eine Anwendung des Auskunftsanspruchs aus § 242 BGB. Bei anonymen Rechtsverletzungen im Internet stehen sich häufig verfassungsrechtlich geschützte Interessen der Beteiligten gegenüber. Die geschützten Rechte des betroffenen Rechteinhabers kollidieren mit dem Recht auf Anonymität der Nutzer. Zudem spielt wegen der Vielzahl sensibler Daten im Internet der Datenschutz eine wichtige Rolle. Daneben sind noch die Interessen der Internetdiensteanbieter zu berücksichtigen, die durch die Verpflichtung zur Auskunftserteilung ebenfalls beeinträchtigt werden.

Für die Regelung eines Auskunftsanspruchs gegen Internetdiensteanbieter ist deshalb ein deutlich höheres Maß an Transparenz erforderlich, als ein aus § 242 BGB abgeleiteter Auskunftsanspruch gewährleisten kann.[189] Im Hinblick darauf und auf Rechtsverletzungen im Internet erscheint der Rückgriff auf § 242 BGB problematisch. Vielmehr bedarf es eines ausdrücklich normierten Auskunftsanspruchs gegen Internetdiensteanbieter, der die spezielle Situation berücksichtigt und die kollidierenden Interessen zu einem angemessenen Ausgleich bringt

5. Verhältnis zu den spezialgesetzlichen Auskunftsansprüchen

Unabhängig davon stellt sich die Frage, in welchem Verhältnis der aus § 242 BGB abgeleitete Auskunftsanspruch zu den speziellen Anspruchsgrundlagen im Bereich des geistigen Eigentums und aus § 21 Abs. 2 S. 2 TTDSG steht. Spätestens seit Inkrafttreten der Auskunftsverpflichtung nach § 21 Abs. 2 S. 2 TTDSG muss deshalb geklärt werden, ob für den allgemeinen Auskunftsanspruch überhaupt noch ein Anwendungsbereich verbleibt.

a) Anwendbarkeit bei Rechtsverletzungen des geistigen Eigentums

Auch wenn der Auskunftsanspruch aus § 242 BGB nur gegen die Diensteanbieter besteht, die als Störer für die Rechtsverletzung haften, könnte eine

[189] Ähnlich *Kohl*, Die Haftung der Betreiber von Kommunikationsforen, S. 159.

Anwendung dieser Anspruchsgrundlage gegenüber den speziellen Anspruchsgrundlagen aus dem Bereich des geistigen Eigentums durchaus vorteilhaft für die Rechteinhaber sein.

Insbesondere ist der Anspruch aus § 242 BGB nicht auf offensichtliche Rechtsverletzungen beschränkt. Außerdem setzt der allgemeine Auskunftsanspruch kein Handeln in gewerblichem Ausmaß voraus, sodass auch private Diensteanbieter zur Auskunft verpflichtet werden könnten. Zudem erstreckt sich der Umfang des Anspruchs auf alle benötigten Informationen – also etwa auch auf die Herausgabe von IP- oder E-Mail-Adressen.[190]

Es stellt sich daher die Frage, ob bei einer Verletzung des geistigen Eigentums der Auskunftsanspruch aus § 242 BGB zusätzlich zu den spezialgesetzlichen Anspruchsgrundlagen angewendet werden kann.

Richtigerweise ist dies aber im Rahmen des Anwendungsbereichs der spezialgesetzlichen Auskunftsansprüche gegen Internetdiensteanbieter abzulehnen. Absatz 2 der Auskunftsansprüche enthält eine spezielle Vorschrift für einen Drittauskunftsanspruch gegen Internetdiensteanbieter, die gegenüber der allgemeinen Vorschrift des § 242 BGB vorrangig ist. Die Regelungen, die der Gesetzgeber im Rahmen der speziellen Auskunftsansprüche getroffen hat, dürfen nicht durch eine Anwendung des § 242 BGB umgangen werden. Dies gilt insbesondere für das Merkmal der offensichtlichen Rechtsverletzung, das die Diensteanbieter schützen soll, da diese die Rechtsverletzung nicht abschließend beurteilen können.

Eine Anwendung des § 242 BGB kommt daher nur in den Fällen in Betracht, in denen keine spezialgesetzliche Anspruchsgrundlage existiert. Etwas anderes gilt nur für akzessorische Ansprüche zum Beispiel auf Auskunft über Umfang und Dauer einer Rechtsverletzung zur Berechnung eines Anspruchs, nicht aber für Auskünfte über Dritte.[191]

---

[190] S. hierzu *BGH,* Urt. v. 10.12.2020 – I ZR 153/17, ZUM 2021, 250 Rn. 31 ff. – YouTube-Drittauskunft II.

[191] S. zum akzessorischen Auskunftsanspruch nach § 242 BGB bei Urheberrechtsverletzungen etwa *Weidert/Molle* in: Ensthaler/Weidert, Kap. 7 Rn. 358 ff.

b) Verhältnis zu § 21 Abs. 2 S. 2 TTDSG

Dasselbe Spezialitätsverhältnis gilt auch im Rahmen des Anwendungsbereichs des § 21 Abs. 2 S. 2 TTDSG. Auch hier darf die speziellere Regelung nicht durch die Anwendung des allgemeinen Auskunftsanspruchs umgangen werden. § 21 Abs. 2 S. 2 TTDSG ist deshalb allein anwendbar, soweit es sich um eine der dort aufgeführten Rechtsverletzungen handelt und die Auskunftserteilung durch einen Telemediendienst erfolgen soll.

Seit der Einführung des § 21 Abs. 2 S. 2 TTDSG ist deshalb fraglich, ob überhaupt noch Raum für eine Anwendung des allgemeinen Auskunftsanspruchs aus § 242 BGB auf die Drittauskunft durch Internetdiensteanbieter bei der Verletzung absoluter Rechte verbleibt. In Betracht kommt der allgemeine Auskunftsanspruch noch in zwei Konstellationen: Zum einen kann er herangezogen werden, wenn nicht die Auskunft eines Telemediendienstes begehrt wird, zum anderen, wenn keine Rechtsverletzung durch rechtswidrige Inhalte i.S.d. § 21 Abs. 2 S. 2 TTDSG vorliegt.

Der Gesetzgeber wollte lediglich für den Bereich der in § 14 Abs. 3 TMG a.F. geregelten Fälle eine Sonderregelung schaffen, den Anspruch aus § 242 BGB aber nicht kodifizieren.[192] Das spricht dafür, dass § 242 BGB außerhalb des Anwendungsbereichs des § 21 Abs. 2 S. 2 TTDSG grundsätzlich anwendbar bleiben sollte.

Dennoch dürfte seit Inkrafttreten des speziellen Auskunftsanspruchs aus § 21 Abs. 2 S. 2 TTDSG der allgemeine Auskunftsanspruch in der Praxis zu vernachlässigen sein. Die gegenüber dem speziellen Anspruch aus § 21 Abs. 2 S. 2 TTDSG erweitere Passivlegitimation des § 242 BGB, die sich etwa auch auf Telekommunikationsanbieter erstreckt, wird durch das Erfordernis der Störerhaftung stark begrenzt. Zudem ist § 21 Abs. 2 S. 2 TTDSG eng mit dem in § 21 Abs. 3-4 TTDSG vorgesehenen datenschutzrechtlichen Gestattungsverfahren verknüpft. Das sorgt dafür, dass nicht nur ein Anspruch auf Auskunftserteilung besteht, sondern auch die dazugehörige datenschutzrechtliche Erlaubnisnorm existiert. Ohne eine entsprechende Regelung ist die Auskunftserteilung trotz bestehender Anspruchsgrundlage nicht zulässig.

---

[192] *Regierungsentwurf,* BT-Drs. 19/27441, S. 55.

C. Der Konflikt mit dem Schutz personenbezogener Daten

Die Identifizierung eines Rechtsverletzers zur Rechtsdurchsetzung im Individualinteresse mittels Auskunftserteilung durch Internetdiensteanbieter steht im Konflikt mit dem Schutz der personenbezogenen Daten der Internetnutzer. Selbst bei Vorliegen eines Auskunftsanspruchs können die Rechteinhaber keine Auskünfte über die Person des Rechtsverletzers erhalten, wenn der Diensteanbieter nicht über die dafür erforderlichen Daten verfügt oder er hierüber keine Auskünfte an Dritte erteilen darf.

Die Auskunftsansprüche können demnach wegen Unmöglichkeit in tatsächlicher oder rechtlicher Hinsicht nach § 275 Abs. 1 BGB ausgeschlossen sein. Im Folgenden wird untersucht, ob die de lege lata geltenden datenschutzrechtlichen Bestimmungen dem Rechteinhaber die Identifizierung eines anonymen Rechtsverletzers im Internet ermöglichen.

I. Bestimmung des anzuwendenden Rechtsrahmens

Mit dem Inkrafttreten der DS-GVO am 25.05.2018 wurden viele der bis dahin noch gültigen nationalen Datenschutzregelungen durch die DS-GVO verdrängt. Daher ist zunächst festzustellen, welche datenschutzrechtlichen Vorschriften anzuwenden sind.

1. Anwendbare nationale Regelungen

Bis dahin galten für Internetdiensteanbieter vor allem die bereichsspezifischen datenschutzrechtlichen Vorschriften aus dem TMG a.F. oder TKG a.F. Diese nationalen Regelungen sind zu großen Teilen durch den Vorrang der DS-GVO als unmittelbar geltendes Unionsrecht unanwendbar geworden. Das hat den Gesetzgeber dazu veranlasst, die bereichsspezifischen Regelungen, die trotz der DS-GVO noch gültig sein sollen, im neuen TTDSG zusammenzufassen.[193]

Das TTDSG besteht dabei aus drei Teilen: Der erste Teil enthält allgemeine Regelungen. Im zweiten und dritten Teil befinden sich jeweils Regelungen zum Datenschutz in der Telekommunikation beziehungsweise zum Telemediendatenschutz. Die Anwendbarkeit der Datenschutzregelungen des TTDSG im

[193] *Regierungsentwurf,* BT-Drs., 19/27441, S. 1 f.

Bereich der Telekommunikation knüpft an die Verpflichtung zur Wahrung des Fernmeldegeheimnisses nach § 3 Abs. 2 TTDSG an. Daneben verbleiben einzelne Regelungen für Telekommunikationsdienste weitgehend unverändert im TKG. Außerdem bleiben auch weiterhin Regelungen des BDSG neben der DS-GVO anwendbar. Im Anwendungsbereich des TTDSG oder TKG werden diese aber durch die bereichsspezifischen Vorschriften verdrängt.[194]

Vor allem im Bereich des Telekommunikationsrechts lässt sich die Fortgeltung einzelner datenschutzrechtlicher Bestimmungen auf Art. 95 DS-GVO stützen. Dieser sieht vor, dass die DS-GVO den Diensteanbietern in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auferlegt, soweit sie besonderen in der e-privacy-Richtlinie festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.[195] Daraus ergibt sich, dass die e-Privacy-Richtlinie neben der DS-GVO anwendbar bleibt und im Rahmen ihres Anwendungsbereichs dieser als lex specialis vorgeht.[196] Nationale Vorschriften zum Schutz personenbezogener Daten bleiben ebenso bestehen, soweit sie der Ausführung der e-Privacy-Richtlinie dienen.[197]

Daher behalten einige Regelungen des Telekommunikationsgesetzes zum Fernmeldegeheimnis und zu Verkehrsdaten in Bezug auf öffentlich zugängliche Kommunikationsnetzwerke ihre Gültigkeit. Zu nennen sind hier beispielsweise

---

[194] S. etwa *Schmidt* in: Taeger/Gabel, § 1 BDSG Rn. 17. S. zu TMG a.F. und TKG a.F. *Kremer,* CR 2012, 438, 440.

[195] S. zur Problematik, dass die Vorschriften der e-privacy-Richtlinie dasselbe Ziel verfolgen müssen, *Kühling/Sauerborn*, CR 2021, 271, 272 f.

[196] S. *Regierungsentwurf,* BT-Drs. 19/27441, S. 34 f.; S. auch *Assion* in: Auer-Reinsdorff/Conrad, § 31 Rn. 211; *Karg* in: Simitis/Hornung/Spieker, Art. 95 DS-GVO Rn. 3; *Kühling/Raab* in: Kühling/Buchner, Art. 95 DS-GVO Rn. 1; *Pille* in: Gola, Art. 95 DS-GVO Rn. 11; *Sydow*, Europäische Datenschutzgrundverordnung, Art. 95 DS-GVO Rn, 1, 3. S noch zu §§ 88, 96, 97 TKG a.F. *Klabundel/Selmeyer* in: Ehmann/Selmeyer, Art. 95 DS-GVO Rn. 2.

[197] Ausführlich etwa *Eckhardt* in: Spindler/Schuster, § 91 TKG Rn. 6 ff.; *Piltz*, CR 2021, 555, 556; *Kiparski*, CR 2021, 482, 482 f.; *Kiparski/Sassenberg*, CR 2018, 324, 324 ff.; *Kühling/Sauerborn*, CR 2021, 271, 272 f.; *Schramm/Shvets*, MMR 2019, 228, 229.

die Vorschriften der §§ 3, 9 und 10 TTDSG, die in der e-Privacy-Richtlinie verankert sind.[198]

Nationale Datenschutzregelungen aus dem TTDSG, TKG oder dem BDSG bleiben außerdem anwendbar, wenn sie von einer Öffnungsklausel der DS-GVO gedeckt sind.[199] Von Bedeutung ist in diesem Zusammenhang vor allem Art. 6 Abs. 4 DS-GVO. Obwohl der Gesetzgeber von der Anwendbarkeit der Regelungen des TTDSG und des TKG neben der DS-GVO ausgeht, muss anhand jeder einzelnen Vorschrift deren Anwendbarkeit überprüft werden.

2. Abgrenzung Telemedien- und Telekommunikationsdatenschutzrecht

Die verschiedenen bereichsspezifischen Datenschutznormen des TTDSG beziehen sich entweder nur auf die Anbieter von Telekommunikations- oder von Telemediendiensten. Daher müssen auch nach Inkrafttreten der DS-GVO die verschiedenen Dienste voneinander abgegrenzt werden.

a) Telekommunikationsdienste

Der Begriff des Telekommunikationsdienstes ist in § 3 Nr. 61 des neuen TKG, das am 1. Dezember 2021 in Kraft getreten ist, definiert. Die Neuregelung dient der Umsetzung der EKEK-Richtlinie.[200]. Davor wurde nach der Rechtsprechung des *EuGH* zur ePrivacy-RL die Einordnung als Telekommunikationsdienst ausschließlich danach beurteilt, ob ein Dienst „Verantwortung für die Übertragung von Signalen" übernimmt.[201]

---

[198] S. ausführlich zu den einzelnen Vorschriften etwa *Eckhardt* in: Spindler/Schuster, § 88 TKG Rn. 36, § 96 TKG Rn.14, § 97 TKG Rn. 36. S ebenfalls noch zu §§ 88, 96, 97 TKG a.F. *Klabundel/Selmeyer* in: Ehmann/Selmeyer, Art. 95 DS-GVO Rn. 2.

[199] *Piltz*, CR 2021, 555, 556. Ausführlich zur Fortgeltung einzelner Regelungen der §§ 11 ff. TMG *Conrad/Hausen* in: Auer-Reinsdorff/Conrad, § 36 Rn. 19-23; *Sesing*, MMR 2019, 347, 347 ff.

[200] Richtlinie (EU) 2018/1972 des europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung), Abl. 2018 L 321, S. 36.

[201] *EuGH,* Urt. v. 13.6.2019 – C-193/18, MMR 2019, 514 Rn. 32 – Google LLC. S. zur Anwendung dieser Rechtsprechung im deutschen Recht *OVG Münster*, Urt. v. 5.2.2020 - 13 A 17/16, BeckRS 2020, 2401, Rn. 20 ff.

Nach der Neuregelung ist der Begriff des Telekommunikationsdiensteanbieters nicht mehr allein auf die technische Dimension der Signalübertragung begrenzt. Mit eingeschlossen sind neben Diensten, die „allein oder weit überwiegend in der Übertragung von Signalen in Telekommunikationsnetze bestehen" (§ 3 Nr. 61 lit. c) TKG) auch ausdrücklich Zugangsanbieter (§ 3 Nr. 61 lit. a) TKG) und sogenannte interpersonelle Kommunikationsdienste (§ 3 Nr. 61 lit- b) TKG).

Access-Provider zählen zu den Internetzugangsdiensten.[202] Zu den Diensten, die allein oder weit überwiegend in der Übertragung von Signalen in Telekommunikationsnetze bestehen, gehören WLAN-Betreiber und Anonymisierungsdienste wie TOR.[203] Um Telekommunikationsdienste i.S.d. § 3 Nr. 61 TKG handelt es sich aber nur, wenn der jeweilige Dienst auch öffentlich zugänglich ist.[204] Daneben ist eine einschränkende Voraussetzung für alle Telekommunikationsdienste, dass diese in der Regel gegen Entgelt erbracht werden müssen. Dabei reicht es aber auch aus, wenn sich die Dienste über personenbezogene Daten oder Werbung finanzieren.[205] Das Erfordernis der Entgeltlichkeit schließt dennoch häufig etwa private offene WLAN-Netzwerke, aber zum Beispiel auch Universitäten als Telekommunikationsdienste aus.[206] Bei lokalen Internetzugängen, die nur einem bestimmten Personenkreis zur Verfügung stehen, kann es an der öffentlichen Zugänglichkeit mangeln.[207]

Vor der Neuregelung des Telekommunikationsrechts war vor allem die rechtliche Einordnung sogenannter Over-the-top-Dienste umstritten.[208] Diese Dienste

---

[202] S. zur Einordnung von Access-Providern als TK-Diensteanbieter bereits vor Inkrafttreten des neuen TKG *Schmitz* in: Hoeren/Sieber/Holznagel, Teil 16.2 Rn. 129.

[203] S. zur Einordnung von Anonymisierungsdiensten als TK-Dienst *Schmitz* in: Hoeren/Sieber/Holznagel, Teil 16.2 Rn. 137 ff. S. speziell zu TOR *Rau/Behrens*, K&R 2009, 766, 767; *Thiesen*, MMR 2014, 803, 804.

[204] *Moench*, NVwZ 2021, 1652, 1653.

[205] S. Erwägungsgrund 16 der EKEK-Richtlinie. S. auch *Regierungsentwurf,* BT-Drs. 19/26108, S. 237; *Moench*, NVwZ 2021, 1652, 1656 f.

[206] Vgl. *Moench*, NVwZ 2021, 1652, 1653, 1656 f.

[207] *Moench*, NVwZ 2021, 1652, 1653.

[208] S. insbesondere die Rechtsprechung zu GMail und SkypeOut *EuGH*, Urt. v. 13.6.2019 – C-193/18, MMR 2019, 514, 514 ff. – Google LLC; *EuGH*, Urt. v. 5.6.2019 – C-142/18, MMR 2019, 517, 517 ff. – SkypeOut. S. ausführlich etwa *Bulowski,* Regulierung von Internetkommunikationsdiensten, S. 56 ff.; *Schneider*, ZD 2014, 231, 231 ff.

bieten basierend auf dem Internet eine Alternative zu traditionellen Telekommunikationsdiensten wie der Post und klassischer Telefonie.[209] Neben Mail-Diensten zählen dazu auch Messenger- und Internettelefonie-Dienste wie Skype, WhatsApp, der Facebook-Messenger, Telegram, etc.

Sie sorgen zwar dafür, dass Datenpakete an die Nutzer übertragen werden, allerdings liegt die eigentliche Verantwortung für die Signalübertragung meist bei Zugangsanbietern und Netzbetreibern, die solche Web-Dienste erst ermöglichen.[210] Over-the-top-Dienste, die sich lediglich der üblichen Signalübertragung im Internet bedienen, waren deshalb in der Regel nicht als Telekommunikationsanbieter zu klassifizieren.[211] Etwas anderes galt allenfalls dann, wenn die Diensteanbieter die Kommunikation ihrer Nutzer speziell verschlüsselten[212] oder weil besondere Vereinbarungen mit Anbietern von Telekommunikationsnetzen geschlossen wurden, sodass sie im Einzelfall ihren Nutzern gegenüber doch für die Signalübertragung verantwortlich waren.[213]

Die zunehmende Verdrängung traditioneller Telekommunikationsdienste durch Internetdienste machte es erforderlich, strengere Anforderungen an Over-the-top Dienste – vor allem im Hinblick auf den Schutz von Nutzerdaten – zu stellen. Durch die Einführung des Begriffs der interpersonellen Kommunikatonsdienste in § 3 Nr. 61 lit. b) des neuen TKG kommt es bei diesen Diensten nicht mehr auf die technische Signalübertragung an, sondern auf deren Funktion als Mittel zur Kommunikation unter zwei oder mehr Personen.[214] Damit

---

[209] Im Falle eines Mail-Dienstes werden beispielsweise den Mailadressen die IP-Adressen der Endgeräte zugeordnet, Vgl. *EuGH,* Urt. v. 13.6.2019 – C-193/18, MMR 2019, 514, 514 ff. – Google LLC; *OVG Münster*, Urt. v. 5.2.2020 - 13 A 17/16, BeckRS 2020, 2401 Rn. 30.

[210] *OVG Münster*, Urt. v. 5.2.2020 - 13 A 17/16, BeckRS, 2020, 2401, Rn. 30; *Martini,* BeckOK Informations- und Medienrecht, § 1 TMG Rn. 13g.

[211] *EuGH*, Urt. v. 13.6.2019 – C-193/18, MMR 2019, 514 Rn. 37 – Google LLC; *Ludwigs/Huller,* NVwZ 2019, 1099, 1099 f.

[212] Vgl. *Schmitz* in: Hoeren/Sieber/Holznagel, Teil 16.2 Rn. 147.

[213] S. dazu *EuGH,* Urt. v. 5.6.2019 – C-142/18, MMR 2019, 517, 517 ff. – SkypeOut, der den Dienst SkypeOut aufgrund von Vereinbarungen mit belgischen Netzbetreiben als elektronischen Kommunikationsdienst ansieht. Vgl. auch *Martini* in: BeckOK Informations- und Medienrecht, § 1 TMG Rn. 13g.

[214] Vgl. Erwägungsgrund 15 EKEK-Richtlinie.

handelt es sich bei Over-the-Top-Diensten nunmehr um Telekommunikationsdienste.[215]

Einige Regelungen des neuen Telekommunikationsrechts gelten nur für sogenannte nummerngebundene interpersonelle Kommunikationsdienste im Sinne von § 3 Nr. 37 TKG. Wird eine Nummer lediglich als Kennung und nicht zur Herstellung der Verbindung genutzt, gilt der Dienst als nummernunabhängig.[216] Die meisten internetbasierten Over-The-Top-Dienste wie Messenger- oder E-Mail-Diensten fallen deshalb nicht unter den Begriff des nummerngebundenen Telekommunikationsdienstes.[217]

Um interpersonelle Telekommunikationsdienste handelt es sich nur, wenn das „interaktive Element des Informationsaustauschs" im Vordergrund steht, sodass der Empfänger auf die erhaltene Information antworten kann.[218] So werden etwa soziale Netzwerke und Dienste, bei denen die interpersonelle Kommunikation nur einer reinen und untergeordneten Nebenfunktion dient, nicht erfasst.[219] Außerdem handelt es sich nur um interpersonelle Kommunikationsdienste, wenn lediglich ein begrenzter Personenkreis miteinander kommuniziert.

Wie schwierig die Abgrenzung zwischen einem interpersonellen Kommunikationsdienst und einem sozialen Netzwerk im Einzelfall sein kann, lässt sich gut am Beispiel des Messenger-Dienstes Telegram zeigen: Grundsätzlich handelt es sich bei Telegram um einen Messenger-Dienst wie WhatsApp, Signal, Threema, etc. Diese Dienste ersetzen klassische Telekommunikationsmittel wie zum Beispiel SMS oder Telefonie durch ein internetbasiertes Angebot. Sie ermöglichen also den Austausch von Text-, Sprach und Bildnachrichten zwischen einzelnen

---

[215] S. auch *Kühling/Sauerborn*, CR 2021, 271, 274.

[216] S. Erwägungsgrund 18 der EKEK-Richtlinie; *Regierungsentwurf,* BT-Drs. 19/26108, S. 233.

[217] S. ausdrücklich für die Messenger-Dienste *Regierungsentwurf,* BT-Drs. 19/26108, S. 233. Als Gegenbeispiel könnten Internetconnected VoIP-Dienste angeführt werden, die eine Verbindung zum bestehenden Telefonnetz aufbauen, S. dazu *Martini/von Zimmermann,* CR 2007, 427, 430; *Oster,* CR 2007, 769, 770.

[218] S. *Regierungsentwurf,* BT Drucksache 19/26108, S. 231.

[219] S. *Regierungsentwurf,* BT Drucksache 19/26108, S. 231.

Personen und Personengruppen. In dieser Funktion stellen Messenger-Dienste interpersonelle Kommunikationsdienste dar.

Telegram ermöglicht es seinen Nutzern darüber hinaus öffentliche Gruppen mit bis zu 200.000 Teilnehmern zu erstellen.[220] Zum Vergleich ist zum Beispiel bei WhatApp die maximale Gruppengröße auf lediglich 256 Nutzer begrenzt.[221] Außerdem besteht bei Telegram die Möglichkeit, einen Kanal zu eröffnen, dem eine unbegrenzte Zahl an Nutzern zwar folgen, dabei aber nicht selbst interagieren kann. In dieser Hinsicht fungiert Telegram daher eher als ein soziales Netzwerk.[222]

Umgekehrt ist die Individualkommunikation, die zum Beispiel über die Chatfunktion in sozialen Netzwerken stattfindet, problematisch. Sofern hier zwischen einem begrenzten Personenkreis Personen nicht öffentlich miteinander kommunizieren, ist die Chatfunktion eher mit einem Messenger- oder E-Mail-Dienst vergleichbar.[223]

Im Ergebnis sollte ein Dienst deshalb nicht pauschal als Ganzes in eine der beiden Kategorien einsortiert werden. Vielmehr muss danach unterschieden werden, ob die konkrete Funktion des Dienstes der Individualkommunikation dient und dadurch klassische Kommunikationsmittel ersetzt.[224]

b) Telemediendienste

Telemedien sind nach § 1 Abs. 1 S. 1 TMG alle elektronischen Informations- und Kommunikationsdienste, die keine Telekommunikationsdienste nach

---

[220] S. zu Gruppen und Kanälen auf Telegram https://www.telegram.org/faq?setln=de (Stand: 24.05.2022).

[221] S. https://www.whatsapp.com/features (Stand: 24.05.2022).

[222] Vgl. *Gielen/Uphues*, EuZW 2021, 627, 634; *Spindler,* GRUR 2021, 653, 653; Auch das BMJV geht wohl davon aus, dass es sich bei Telegram um ein soziales Netzwerk handelt, da es ein Bußgeldverfahren aufgrund von Verstößen gegen das NetzDG eingeleitet hat, s. dazu *Redaktion MMR Aktuell,* MMR-Aktuell 2021, 440252.

[223] *Bauer*, Soziale Netzwerke und strafprozessuale Ermittlungen, S. 291; *Karg/Fahl*, K&R 2011, 453, 456 f.

[224] So auch *Bauer*, Soziale Netzwerke und strafprozessuale Ermittlungen, S. 290; *Karg/Fahl*, K&R 2011, 453, 456; A.A. wohl *Eckel/Rottmeier,* NStZ 2021, 1, 10 f.

§ 3 Nr. 61 TKG, telekommunikationsgestützte Dienste nach § 3 Nr. 63 TKG oder Rundfunk nach § 2 RStV sind. Diese Definition wird durch § 2 Abs. 1 TTDSG auch für den bereichsspezifischen Datenschutz für Telemedien im Rahmen des TTDSG übernommen. Anbieter von Telemedien sind nach § 2 Nr. 1 TMG natürliche oder juristische Personen, die eigene oder fremde Telemedien zur Nutzung bereithalten oder Zugang zur Nutzung vermitteln. § 2 Abs. 2 Nr. 1 TTDSG erweitert den Personenkreis noch um Personen, die an der Erbringung von Telemedien mitwirken.[225]

Zu den Telemediendiensten gehören grundsätzlich alle Internetdienste, die eigene oder fremde Inhalte und Informationen anbieten oder Zugang zu Inhalten verschaffen. Das schließt etwa Anbieter von sozialen Netzwerken, Online-Marktplätzen, Sharehosterdiensten, Usenet-Servern, Streamingdiensten, Videoplattformen, Webseiten oder Blogbetreiber ein.

Telemediendienste werden zwar mittels Telekommunikation genutzt, betreiben aber selbst keinen Telekommunikationsdienst und unterfallen auch nicht dem Anwendungsbereich der speziellen Datenschutzregelungen für TK-Dienste. Allerdings konnte vor der Neuregelung des Begriffs der Telekommunikationsdienste ein Dienst zugleich unter den Begriff des Telemedien-, als auch des Telekommunikationsdienstes fallen.[226] Das betraf insbesondere interpersonelle Kommunikationsdienste wie Web-Mail- und Messenger-Dienste, aber gegebenenfalls auch bestimmte Anonymisierungsdienste wie Proxy-Server oder Access-Provider.[227]

Vor der Neuregelung des Begriffs des Telekommunikationsdienstes in § 3 Nr. 61 TKG unterschied § 1 Abs. 1 TMG a.F. danach, ob ein Dienst ganz oder nur teilweise in der Übertragung von Signalen bestand. Auf letztgenannte Dienste waren die Vorschriften des TMG grundsätzlich ebenfalls anwendbar. Von den

---

[225] *Ettig* in: Taeger/Gabel, § 2 TTDSG Rn. 16; *Piltz*, CR 2021, 555, 561.

[226] Ein Telekommunikationsdienst konnte gleichzeitig auch einen Telemedienst darstellen, wenn der erbrachte Dienst zwar überwiegend, aber nicht ausschließlich in der Übertragung von Signalen in Telekommunikationsnetze besteht; S. etwa *Martini* in: BeckOK Informations- und Medienrecht, § 1 TMG Rn. 11a; *Ricke* in: Spindler/Schuster, § 1 TMG Rn 7.

[227] S. etwa *Martini* in: BeckOK Informations- und Medienrecht, § 1 TMG Rn. 13 ff.; Ricke in: Spindler/Schuster, § 1 TMG Rn. 6 ff.; Spindler in: Spindler/Schmitz, § 1 TMG Rn. 26 ff.

bereichsspezifischen Datenschutzvorschriften waren jedoch Dienste, die überwiegend in der Übertragung von Signalen bestanden, nach § 11 Abs. 3 TMG a.F. weitgehend ausgenommen. Inzwischen nimmt § 1 Abs. 1 S. 1 TMG eine Legaldefinition des Begriffs der „Telemedien" vor, von der die Dienste aus § 3 Nr. 61 TKG ausdrücklich nicht mehr erfasst werden. Telemedien- und Telekommunikationsdienste schließen sich dadurch also gegenseitig aus. Durch die Erweiterung des Telekommunikationsbegriffs und die klare Abgrenzung zwischen Telemedien und Telekommunikation wird der Anwendungsbereich des Telemedienrechts, sowie im Speziellen des Telemediendatenschutzes reduziert.[228]

c) Sonstige Internetdienste

Daneben existieren noch einzelne Internetdienste, die weder Telemedien noch Telekommunikationsdienste darstellen. Dazu gehören vor allem Dienste, die lediglich administrative Aufgaben übernehmen, wie Domain-Registrare. Für diese Dienste gelten die bereichsspezifischen Datenschutzregelungen nicht. Stattdessen findet ausschließlich die DS-GVO und gegebenenfalls einzelne Regelungen des BDSG Anwendung.

II. Zulässigkeit der Bestandsdatenauskunft der Anwendungsdienste

Wie oben bereits ausgeführt, existieren im Wesentlichen zwei unterschiedliche Arten, die Identität eines Rechtsverletzers durch Auskünfte der Diensteanbieter zu ermitteln.[229] Insbesondere besteht die Möglichkeit, durch die bei den Anwendungsdiensten gespeicherten Nutzerdaten die Identität des Rechtsverletzers zu ermitteln.

Dabei muss zwischen Daten unterschieden werden, die während eines konkreten Nutzungsvorgangs anfallen und sogenannten Bestandsdaten, da für die Verarbeitung dieser Daten unterschiedliche gesetzliche Anforderungen bestehen.

---

[228] Die Haftungsprivilegierungen der §§ 8 ff. TMG müssen jedoch gegebenenfalls dennoch in unionsrechtskonformer Auslegung auch auf bestimmte Telekommunikationsdienste wie etwa Access-Provider angewendet werden; Vgl. noch zu § 1 TMG a.F. *Frey*, MMR 2014, 650, 653 f.; *Spindler* in: Spindler/Schmitz, § 1 TMG Rn. 32.

[229] S. ausführlicher oben unter Kap. 4 § 2.

Zur Identifizierung des Nutzers kann es in vielen Fällen bereits ausreichen, wenn die Diensteanbieter ihre Auskunft anhand von Bestandsdaten erteilen.

1. Begriff der Bestandsdaten

Die Unterscheidung von Bestandsdaten und anderen Daten, die bei der Nutzung von Internetdiensten anfallen, wirkt sich nur auf den bereichsspezifischen Datenschutz aus. Für den Bereich des Telemediendatenschutzes definiert § 2 Abs. 2 Nr. 2 TTDSG als personenbezogene Daten diejenigen „Daten, deren Verarbeitung zum Zweck der Begründung, inhaltlichen Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Anbieter von Telemedien und dem Nutzer über die Nutzung von Telemedien erforderlich" sind. Ähnlich verhält es sich im Telekommunikationsrecht, wonach gemäß § 3 Nr. 6 TKG als Bestandsdaten alle „Daten eines Endnutzers, die erforderlich sind für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste" gelten.[230]

Bestandsdaten werden häufig schon im Vorfeld der Nutzung von Anwendungsdiensten von den Nutzern – zum Beispiel im Wege einer Registrierung angegeben. Dabei handelt es sich vor allem um Daten wie Namen, Adressen, E-Mail-Adressen, Kontodaten, Telefonnummern, Pseudonyme etc.[231] Die Anwendungsdienste können gegebenenfalls allein anhand dieser Daten einen rechtsverletzenden Nutzer identifizieren. Veröffentlicht ein Nutzer zum Beispiel einen rechtswidrigen Inhalt unter einem Pseudonym auf einer Plattform, kann der Diensteanbieter das Pseudonym dem bürgerlichen Namen des Nutzers zuordnen. Dies setzt allerdings voraus, dass der jeweilige Diensteanbieter die notwendigen Daten vorhält und an die Rechteinhaber weitergeben darf.

---

[230] *Ettig* in: Taeger/Gabel, § 2 TTDSG Rn. 21. Kritisch zur unterschiedlichen Definition von Bestandsdaten im TKG und im TTDSG *Assion*, Stellungnahme, abrufbar unter: https://www.bundestag.de/resource/blob/835498/3fc24ea374301c2ba608c9509cc64ec1/19-9-1039_Stellungnahme_SV_Assion_oeA_TTDSG_21-04-2021-data.pdf, S. 14 (Stand: 24.05.2022).

[231] S. auch *Gabel,* ZUM 2002, 607, 611.

2. Speicherung von Bestandsdaten

Daten wie Namen und Adressen der Nutzer stellen personenbezogene Daten dar, bei denen es sich um Bestandsdaten handelt.

§ 172 Abs. 1 TKG enthält Pflichten bestimmter Telekommunikationsdienste zur Speicherung von Bestandsdaten zum Zwecke der Auskunftserteilung an Sicherheitsbehörden. Nummernunabhängige interpersonelle Kommunikationsdienste sind nach § 172 Abs. 3 TKG nur zur Speicherung von Bestandsdaten verpflichtet, wenn sie diese ohnehin selbstständig erheben, wozu sie aber nicht gezwungen sind.[232] Für die meisten Anwendungsdienste und insbesondere die sog. Over-the-top-Dienste greift die Pflicht zur Erhebung von Bestandsdaten aus § 172 Abs. 1 TKG nicht, weil es sich bei diesen Diensten um nummernunabhängige Telekommunikationsdienste handelt.[233] Nur wenn zum Beispiel ein E-Mail-Dienst Namen, Anschrift, E-Mail-Adresse und Kundenkennung seiner Nutzer erhebt, wird er nach § 172 Abs. 3 TKG verpflichtet, diese Daten auch zu speichern.[234]

Darüber hinaus existieren aber weder für Telekommunikations- noch für Telemediendienste Regelungen, unter welchen Umständen Bestandsdaten von Diensteanbietern erhoben und gespeichert werden dürfen.[235] Außerhalb des Anwendungsbereichs des § 172 Abs. 3 TKG sind daher für alle Anwendungsdienste gleichermaßen die Vorschriften der DS-GVO maßgeblich.

Die Diensteanbieter können demnach Bestandsdaten ihrer Nutzer erheben und speichern, sofern die allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 DS-GVO eingehalten wurden und die Verarbeitung nach Art. 6 Abs. 1 lit. a)-f) DS-GVO rechtmäßig ist. Zu erwähnen ist vor allem, dass die Erhebung der Daten zu einem festgelegten, eindeutigen und legitimen

---

[232] *Ferner* in: BeckOK StPO, § 172 TKG Rn. 9.

[233] S. ausführlicher dazu oben unter Kap. 5 § 3 A. II.

[234] Vgl. *Ferner* in: BeckOK StPO, § 172 TKG Rn. 10.

[235] Bis zur Neuregelung existierten noch Vorschriften etwa in § 14 Abs. 1 TMG a.F. oder § 95 TKG, die aber damals bereits keinen über die DS-GVO hinausgehenden Regelungsgehalt aufwiesen und deshalb durch diese verdrängt wurden, S. dazu etwa *Hunziker/Sassenberg*, CR 2019, 188, 189; *Kiparski,* CR 2021, 482, 488; *Kiparski/Sassenberg*, CR 2018, 324, 327; *Schramm/Shvets,* MMR 2019, 228, 230.

Zweck erfolgen muss. Zudem muss die Speicherung der Daten hinsichtlich des Ausmaßes und der Dauer auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Einige Diensteanbieter speichern in der Praxis in rechtmäßiger Weise solche personenbezogenen Daten ihrer Nutzer beispielsweise mit deren Einwilligung (Art. 6 Abs. 1 lit. a) DS-GVO) oder zur Erfüllung eines Vertrages (Art. 6 Abs. 1 lit. b) DS-GVO).

Telekommunikationsdienste können nach § 7 TTDSG im Zusammenhang mit der Begründung oder Änderung eines Vertragsverhältnisses zur Überprüfung der Bestandsdaten der Endnutzer einen Ausweis verlangen.[236] Damit können die angegebenen Daten sogar verifiziert werden.

Die vorsorgliche Speicherung von personenbezogenen Daten für den Fall eines möglichen Auskunftsersuchens durch private Dritte ist jedoch nicht zulässig. Die Speicherung von Bestandsdaten der Nutzer zum Zwecke einer späteren Auskunftserteilung lässt sich auch nicht etwa auf Art. 6 Abs. 1 lit. c) DS-GVO stützen, wonach eine Verarbeitung grundsätzlich zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, rechtmäßig sein kann. Die Tatsache, dass die Diensteanbieter auf der Grundlage eines Auskunftsanspruchs zur Herausgabe von Nutzerdaten verpflichtet sein könnten, reicht allein nicht aus um eine rechtliche Verpflichtung des Diensteanbieters im Sinne des Art. 6 Abs. 1 lit. c) DS-GVO zu begründen.[237] Vielmehr ist eine Datenverarbeitung nur zulässig, wenn der Diensteanbieter zur Datenverarbeitung als solches verpflichtet ist, nicht aber, wenn der Diensteanbieter zur Erfüllung anderweitiger Pflichten – also etwa zur Erfüllung einer Auskunftspflicht – Daten verarbeiten muss.[238]

Das Speichern von Bestandsdaten ist in der Regel auch nicht nach Art. 6 Abs. 4 lit. f) DS-GVO zur Wahrung der berechtigten Interessen eines Dritten zulässig. Das berechtigte Interesse muss nämlich bereits zum Zeitpunkt der Verarbeitung

---

[236] S. zur Vereinbarkeit dieser Regelung mit der DS-GVO *Kühling/Sauerborn*, CR 2021, 271, 275.

[237] S. *Albers/Veit* in: BeckOK Datenschutzrecht, Art. 6 DS-GVO Rn. 48. A.A. aber wohl *Schmitz* in: Hoeren/Sieber/Holznagel, Teil 16.2 Rn. 342.

[238] S. *Albers/Veit* in: BeckOK Datenschutzrecht, Art. 6 DS-GVO Rn. 48; *Taeger* in: Taeger/Gabel, Art. 6 DS-GVO Rn. 76.

tatsächlich bestanden haben und darf nicht lediglich hypothetisch sein.[239] Zum Zeitpunkt der Speicherung von Bestandsdaten liegt eine Rechtsverletzung meist nicht vor. Damit existiert auch kein berechtigtes Interesse eines Rechteinhabers an der Auskunftserteilung.

Deshalb kann für die Auskunftserteilung nur auf Daten zurückgegriffen werden, die zu einem anderen Zweck gespeichert wurden. Bestandsdaten dürfen also nur gespeichert werden, soweit dies zum Beispiel für das Vertragsverhältnis zwischen Diensteanbietern und Nutzern erforderlich ist. Die Diensteanbieter sind aber in der Regel nicht dazu verpflichtet, überhaupt Bestandsdaten ihrer Nutzer zu erheben. In vielen Fällen können die Anbieter von internetbezogenen Diensten den Rechteinhabern Namen und Adressen ihrer Nutzer daher nicht mitteilen. Selbst Online-Marktplätze oder soziale Netzwerke, bei denen die Nutzer zur Anmeldung häufig eine Vielzahl personenbezogener Daten angeben, verifizieren sehr oft die Daten ihrer Nutzer nicht.

3. Übermittlung von Bestandsdaten an die Rechteinhaber

Sofern die Diensteanbieter über Namen und Adressen ihrer Nutzer verfügen, könnten diese Daten zumindest theoretisch zur Identifizierung der Rechtsverletzer genutzt werden. Dies setzt jedoch voraus, dass die Diensteanbieter diese Informationen an die Rechteinhaber übermitteln dürfen. Dabei wird die Frage aufgeworfen, ob Namen und Adressen der Nutzer im Wege der Auskunftserteilung an Dritte zur Rechtsdurchsetzung weitergegeben werden dürfen, obwohl dies eine zweckändernde Weiterverarbeitung der personenbezogenen Daten voraussetzen würde.

a) § 21 TTDSG

Eine datenschutzrechtliche Erlaubnis für die zweckändernde Weiterverarbeitung kann sich aus § 21 TTDSG ergeben. Diese Vorschrift sieht vor, dass Diensteanbieter unter bestimmten Voraussetzungen Auskunft über Bestandsdaten an Dritte erteilen dürfen.

---

[239] S. *EuGH*, Urt. v. 11.12.2019 – C-708/18, ZWE 2020, 337 Rn. 44. S. auch *Albers/Veit* in: BeckOK Datenschutzrecht, Art. 6 DS-GVO Rn. 68.

aa) Begrenzung auf Telemediendienste

§ 21 TTDSG erstreckt sich aber lediglich auf Telemediendienste. Eine korrespondierende Regelung für Telekommunikationsdienste existiert nicht. Das ist spätestens seit der Neuregelung des Begriffs der Telekommunikationsdienste für die Rechteinhaber problematisch, da einige in der Praxis relevante Anwendungsbereiche von der Regelung nicht erfasst werden. Das betrifft zum Beispiel Persönlichkeitsrechtsverletzungen bei der Nutzung von interpersonellen Kommunikationsdiensten wie zum Beispiel Messenger- oder E-Mail-Diensten. Der *BGH* ging noch im Jahr 2020 in einer Entscheidung zu § 14 Abs. 3 TMG a.F. davon aus, dass eine Anwendung der Vorgängerregelung auf den Facebook-Messenger zumindest denkbar wäre.[240] Durch die eindeutige Zuordnung von interpersonellen Kommunikationsdiensten zu den Telekommunikationsdiensten wäre dies inzwischen nicht mehr möglich.

bb) Anwendbarkeit von § 21 TTDSG nach Inkrafttreten der DS-GVO

§ 21 TTDSG enthält Regelungen, die es dem Diensteabieter unter bestimmten Voraussetzungen erlauben, Daten zur Auskunftserteilung zum Zwecke der Durchsetzung zivilrechtlicher Ansprüche weiterzugeben. Diese Regelungen können somit eine Übermittlung von Bestandsdaten an Dritte und damit eine zweckändernde Weiterverarbeitung ermöglichen, sofern diese durch das Inkrafttreten der DS-GVO nicht verdrängt werden.

Nach Art. 6 Abs. 4 DS-GVO ist eine zweckändernde Weiterverarbeitung von Daten generell nur zulässig, wenn „die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist". Auf die Vereinbarkeit kommt es nach Art. 6 Abs. 4 DS-GVO allerdings nur an, wenn die Verarbeitung „nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten" beruht.

Es ist umstritten, ob sich aus dieser Formulierung eine Öffnungsklausel für Rechtsvorschriften der Mitgliedstaaten ableiten lässt, die von dem Grundsatz der Zweckvereinbarkeit abweichen. Während sich einige Stimmen in der

[240] *BGH*, Beschl. v. 24.9.2019 – VI ZB 39/18, GRUR 2020, 101 Rn. 24 ff., 57 – Facebook-Messenger.

Literatur[241] dagegen aussprechen, hielt der *BGH* in einer Entscheidung zum Gestattungsverfahren nach der Vorgängerregelung aus § 14 Abs. 3-5 TMG a.F. die Auslegung des Art. 6 Abs. 4 DS-GVO als Öffnungsklausel für so eindeutig, dass er auf ein Vorabentscheidungsersuchen verzichtete.[242] Dem *BGH*, der sich in besagter Entscheidung ausführlich mit Art. 6 Abs. 4 DS-GVO befasst hatte, ist dahingehend beizupflichten, dass sowohl Wortlaut, als auch Systematik und Zweck der Regelung für eine Auslegung als Öffnungsklausel sprechen.

Nach dem Wortlaut der Vorschrift muss der Zweck der Weiterverarbeitung mit dem ursprünglichen Zweck der Datenerhebung vereinbar sein, sofern die Verarbeitung „nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten" beruht. Daraus ergibt sich im Umkehrschluss, dass eine zweckändernde Verarbeitung, die sich auf eine mitgliedstaatliche Rechtsvorschrift stützen lässt, die den Anforderungen des Art. 6 Abs. 4 DS-GVO genügt, zulässig ist. Noch deutlicher wird dies im Erwägungsgrund 50 DS-GVO, wonach eine Weiterverarbeitung, die auf dem Recht der Mitgliedstaaten beruht, möglich sein soll.[243] Die Mitgliedstaaten werden damit ermächtigt, eine ausnahmsweise zulässige zweckverändernde Weiterverarbeitung zu gestatten.[244]

Auch aus der Systematik der Regelung ergibt sich nichts Gegenteiliges. Insbesondere kann Art. 6 Abs. 4 DS-GVO nicht lediglich als Ermächtigung des nationalen Gesetzgebers im Bereich einer Verarbeitung nach Art. 6 Abs. 1 lit. c), e)

---

[241] S. etwa *Buchner/Petri*, in: Kühling/Buchner, Art. 6 Rn. 180, 200; *Kühling/Sauerborn,* CR 2021, 271, 278; *Reimer* in: Sydow, Art. 6 DS-GVO Rn. 83; *Schmitz*, ZRP 2017, 172, 172; *Schulz* in: Gola, Art. 6 DS-GVO Rn. 32. S. auch *BVerwG*, Urt. v. 27.9.2018 – 7 C 5/17, NVwZ 2019, 473, 476.

[242] *BGH*, Beschl. v. 24.9.2019 – VI ZB 39/18, GRUR 2020, 101 Rn. 42 f. – Facebook-Messenger.

[243] Ähnlich auch *BGH*, Beschl. v. 24.9.2019 – VI ZB 39/18, GRUR 2020, 101 Rn. 39 – Facebook-Messenger.

[244] So auch *Albrecht/Jotzo*, Das neue Datenschutzrecht, S. 77; *Culik/Döpke*, ZD 2017, 226, 229; *Kramer* in: Auernhammer, Art. 6 DS-GVO Rn. 66; *Kühling/Martini*, EuZW 2016, 448, 451; *Roßnagel* in: Simitis/Hornung/Spieker, Art. 6 IV DS-GVO Rn. 18; *Schulz*, in: Gola, Art. 6 DS-GVO Rn. 190; *Taeger* in: Taeger/Gabel, Art. 6 DS-GVO Rn. 167.

DS-GVO verstanden werden.[245] Schließlich finden sich hierfür bereits entsprechenden Vorschriften in Art. 6 Abs. 2, 3 DS-GVO.[246] Art. 6 Abs. 4 DS-GVO dagegen regelt ausschließlich die zweckverändernde Weiterverarbeitung.

Sieht man Art. 6 Abs. 4 DS-GVO nicht als Öffnungsklausel an, wäre eine solche Weiterverarbeitung nur unter den engen Voraussetzungen der Zweckvereinbarkeit möglich. Es entspricht nicht dem Zweck von Art. 6 Abs. 4 DS-GVO, eine Weiterverarbeitung von rechtmäßig erhobenen Daten zur Durchsetzung zivilrechtlicher Ansprüche von vornherein auszuschließen.[247] Art. 6 Abs. 4 DS-GVO stellt daher eine Öffnungsklausel dar, die eine zweckverändernde Weiterverarbeitung auf Grund von Regelungen der Mitgliedstaaten ermöglicht. Davon scheint überdies auch der deutsche Gesetzgeber ausgegangen zu sein, der nach Inkrafttreten der DS-GVO mit der Einführung von § 24 BDSG von dieser Möglichkeit Gebrauch gemacht hat.[248]

Anders als noch von *Nink* im Hinblick auf die Vorgängerregelung des § 14 TMG a.F: angenommen, dient § 21 TTDSG auch der Wahrnehmung dieser Öffnungsklausel. *Nink* war der Ansicht, der Gesetzgeber habe im Zuge der Umsetzung und Anpassung der datenschutzrechtlichen Vorschriften anlässlich der Datenschutzgrundverordnung keine Anpassung der Vorschriften vorgenommen.[249] Dementsprechend würden die Regelungen des § 14 TMG a.F. nicht der Wahrnehmung der Öffnungsklausel dienen.[250] Ursprünglich sah der Gesetzgeber § 14 TMG zwar in der Tat lediglich als Übergangsregelung bis zum Inkrafttreten der DS-GVO an, allerdings hat er dennoch später die Regelung beibehalten.[251] Spätestens mit der Übernahme von § 14 TMG a.F. in § 21 TTDSG hat der Gesetzgeber deshalb von der Öffnungsklausel Gebrauch gemacht.

---

[245] Anders etwa *Buchner/Petri* in: Kühling/Buchner, Art. 6 DS-GVO Rn. 199 f.; *Heberlein* in: Ehmann/Selmayr, Art. 6 DS-GVO Rn. 51.

[246] S. *BGH*, Beschl. v. 24.9.2019 – VI ZB 39/18, GRUR 2020, 101 Rn. 37 – Facebook-Messenger.

[247] Ähnlich zu § 24 BDSG *Marsch* in: Sydow, § 24 BDSG Rn. 17.

[248] *Regierungsentwurf,* BT-Drs. 18/11325, 95 f. S. auch *BGH,* Beschl. v. 24.9.2019 – VI ZB 39/18, GRUR 2020, 101 Rn. 43 – Facebook-Messenger; *Schwartmann/Pieper* in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, 2018, Art. 6 DS-GVO Rn. 207

[249] S. noch zu § 14 TMG a.F. *Nink* in: Spindler/Schuster, §§ 11-15 TMG Rn. 4.

[250] *Nink* in: Spindler/Schuster, §§ 11-15 TMG Rn. 4.

[251] S. *Gesetzesentwurf,* BT-Drs. 18/12356, S. 28.

Zudem entspricht § 21 TDSG wie der *BGH* – zumindest für das Verfahren nach § 21 Abs. 2-4 TTDSG – ebenfalls zutreffend feststellt, den Anforderungen, die Art. 6 Abs. 4 DS-GVO an die mitgliedstaatliche Regelung stellt.[252] So muss die Regelung der Mitgliedstaaten „in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Art. 23 Abs. 1 DS-GVO genannten Ziele" darstellen. § 21 TTDSG dient der Durchsetzung zivilrechtlicher Ansprüche gemäß Art. 23 Abs. 1 lit. j) DS-GVO und ist notwendig, da anderenfalls eine Identifizierung eines Rechtsverletzers am Grundsatz der Zweckbindung aus Art. 5 Abs. 1 lit. b) DS-GVO scheitern könnte.[253] Darüber hinaus wird die Verhältnismäßigkeit durch Maßnahmen wie etwa das Erfordernis einer gerichtlichen Anordnung beim Gestattungsverfahren nach § 21 Abs. 3 TTDSG sichergestellt.

Art. 6 Abs. 4 DS-GVO stellt also eine Öffnungsklausel für mitgliedstaatliche Regelungen zur zweckändernden Weiterverarbeitung personenbezogener Daten dar. § 21 TTDSG entspricht den Anforderungen des Art. 6 Abs. 4 DS-GVO und kann daher weiterhin angewendet werden.

Offen gelassen hatte der *BGH* in seiner Entscheidung allerdings, ob die zweckändernde Weiterverarbeitung, die auf einer Vorschrift i.S.d. Art. 6 Abs. 4 DS-GVO beruht, wiederum rechtmäßig im Sinne des Art. 6 Abs. 1 lit. a)-f) DS-GVO sein muss.[254] Die Auskunftserteilung an Rechteinhaber ließe sich prinzipiell auf die Wahrung berechtigter Interessen eines Dritten im Sinne des Art. 6 Abs. 1 lit. f) DS-GVO stützen.

Allerdings greift Art. 6 Abs. 1 lit. f) DS-GVO nur, wenn nicht im Einzelfall die Interessen der von der Datenverarbeitung betroffenen Person die Interessen des Dritten überwiegen. Dementsprechend wäre es denkbar, § 21 TTDSG dahingehend unionsrechtskonform auszulegen, dass die Gestattung der

---

[252] So zumindest in Bezug auf das Gestattungsverfahren nach § 14 Abs. 3-5 TMG a.F. *BGH*, Beschl. v. 24.9.2019 – VI ZB 39/18, GRUR 2020, 101 Rn. 40 ff. – Facebook-Messenger.

[253] *BGH*, Beschl. v. 24.9.2019 – VI ZB 39/18, GRUR 2020, 101 Rn. 41 – Facebook-Messenger; *Hullen/Roggenkamp* in: Plath, § 14 TMG Rn. 22.

[254] *BGH*, Beschl. v. 24.9.2019 – VI ZB 39/18, GRUR 2020, 101 Rn. 44 – Facebook-Messenger. S. für die Erforderlichkeit der Erfüllung eines Rechtmäßigkeitstatbestandes aus Art. 6 Abs. 1 lit. a)-f) *Albers/Veit*, BeckOK Datenschutzrecht, Art. 6 DS-GVO Rn. 113.

Auskunftserteilung nur angeordnet werden darf, wenn nicht ausnahmsweise aufgrund besonderer Umstände die Interessen der Nutzer dem entgegenstehen.[255] Die Formulierung von § 21 Abs. 1, 2 TTDSG, dass die Anbieter von Telemedien „im Einzelfall" Auskunft über Bestandsdaten erteilen dürfen, „soweit" dies zur Durchsetzung zivilrechtlicher Ansprüche bzw. der Rechte am geistigen Eigentum erforderlich ist, ließe ausreichend Spielraum für eine solche Auslegung.

Selbst wenn man also davon ausgeht, dass die zweckändernde Weiterverarbeitung sich auf einen Rechtmäßigkeitstatbestand aus Art. 6 Abs. 1 lit. a)-f) stützen muss, lässt sich aus § 21 TTDSG grundsätzlich eine datenschutzrechtliche Erlaubnisnorm ableiten. Selbst eine gegebenenfalls erforderliche unionsrechtskonforme Auslegung würde nur in besonderen Ausnahmefällen zu einer Unzulässigkeit der Auskunftserteilung führen.

cc) Übermittlung an Rechteinhaber zur Durchsetzung der Rechte des geistigen Eigentums nach § 21 Abs. 1 TTDSG

§ 21 Abs. 1 TTDSG sieht vor, dass Telemediendiensteanbieter auf Anordnung der zuständigen Stelle zur Durchsetzung der Rechte am geistigen Eigentum Auskunft über Bestandsdaten erteilen dürfen. Leider ist dabei unklar, um wen es sich bei der zuständigen Stelle handelt und welche Anforderungen an die Anordnung zu stellen sind.

Zu einem besseren Verständnis der Norm trägt ein Rückblick auf die Vorgängerregelung aus § 14 Abs. 2 TMG a.F. bei. § 14 Abs. 2 TMG a.F. regelte in erster Linie die Auskunftserteilung an Bedarfsträger beispielsweise zum Zweck der Strafverfolgung oder zur Gefahrenabwehr.[256] Im Zuge der Umsetzung der Enforcement-Richtlinie wurde § 14 Abs. 2 TMG a.F. um einen Zusatz ergänzt, der die Auskunftserteilung auch zur Durchsetzung der Rechte am geistigen Eigentum gestattet. Im Zusammenhang mit den später eingeführten Auskunftsansprüchen in § 101 UrhG, § 140b PatG, § 24b GebrMG, § 19 MarkenG, § 46

---

[255] Vgl. *BGH*, Beschl. v. 24.9.2019 – VI ZB 39/18, GRUR 2020, 101 Rn. 45 – Facebook-Messenger.

[256] S. auch *Ettig* in: Taeger/Gabel, § 21 TTDSG Rn. 8; *Schmitz* in: Spindler/Schmitz, § 14 TMG Rn. 42.

DesignG, § 37b SortenSchuG und § 9 Abs. 2 HalblSchG sollte so eine Auskunft der Anbieter von Telemediendiensten an Private ermöglicht werden.[257]

Der Gesetzgeber ging bei der Neuregelung des § 14 Abs. 2 TMG a.F. damals wohl davon aus, dass die zukünftigen Auskunftsverfahren eine richterliche Anordnung voraussetzen würden.[258] Entsprechend gestattete die Norm eine Auskunftserteilung zur Durchsetzung der Rechte am geistigen Eigentum nur auf „Anordnung der zuständigen Stelle". Da die ebenfalls im Zuge der Umsetzung der Enforcement-Richtlinie eingeführten Anspruchsgrundlagen einen Richtervorbehalt aber nur für den Fall der Verwendung von Verkehrsdaten vorsehen, stellte sich von Anfang an die Frage, wie diese Formulierung des § 14 Abs. 2 TMG a.F. bei der Übermittlung von Bestandsdaten an Rechteinhaber zu verstehen ist.

Diese Problematik wurde inzwischen noch weiter verschärft, da der Gesetzgeber an der Formulierung „Auf Anordnung der zuständigen Stelle" mehrfach festgehalten hat. Insbesondere hat der Gesetzgeber die Auskunftserteilung an öffentliche Stellen aus § 14 Abs. 2 TMG a.F. ausgegliedert, sodass der Anwendungsbereich der Norm vollständig auf die Bestandsdatenauskunft an private Dritte reduziert wurde.[259] Zudem behielt § 21 Abs. 1 TTDSG auch nach der Übernahme des § 14 Abs. 2 TMG a.F. die umstrittene Formulierung bei.

Dennoch kommt es aber nicht in Betracht, auch für die Bestandsdatenauskunft nach dem Telemediengesetz eine richterliche Anordnung vorauszusetzen.[260] Dies stünde nämlich im Widerspruch zum Willen des Gesetzgebers, der die Auskunftsansprüche zur Durchsetzung der Rechte am geistigen Eigentum nur bei Verwendung von Verkehrsdaten unter Richtervorbehalt stellen wollte.[261] Damit scheidet eine analoge Anwendung zum in Absatz 9 der Auskunftsansprüche

---

[257] Ähnlich auch *Regierungsentwurf,* BT-Drs. 16/3078, S. 16.

[258] S. *Janal*, Europäisches Zivilverfahrensrecht, S. 268 unter Bezugnahme auf den *Regierungsentwurf*, BT-Drs. 16/3078, S. 16.

[259] Zuerst wurde die Regelung in § 15a TMG a.F. neu gefasst und später durch § 22 TTDSG übernommen, S. dazu auch *Ettig* in: Taeger/Gabel, § 21 TTDSG Rn. 8.

[260] *Ettig* in: Taeger/Gabel, § 21 TTDSG Rn. 8; *Hullen/Roggenkamp* in: Plath, § 14 TMG Rn. 24; *Schmitz* in: Spindler/Schmitz, § 14 TMG Rn. 42.

[261] S. *Regierungsentwurf*, BT-Drs. 16/5048, S. 38.

geregelten Richtervorbehalt ebenfalls aus.[262] Das zeigt sich auch unter systematischen Gesichtspunkten unter Hinzuziehung von § 21 Abs. 2-4 TTDSG, der anders als im Fall von § 21 Abs. 1 TTDSG ein richterliches Gestattungsverfahren ausdrücklich vorsieht.

Zu einer richterlichen Anordnung kann es im Rahmen von § 21 Abs. 1 TTDSG daher allenfalls kommen, wenn der Diensteanbieter die Auskunft mangels datenschutzrechtlicher Ermächtigung verweigert und der Rechteinhaber daraufhin eine gerichtliche Entscheidung herbeiführt.[263] Obwohl der Diensteanbieter unter Verweis auf die mangelnde datenschutzrechtliche Zulässigkeit die Auskunftserteilung ursprünglich zu Recht verweigern könnte, wäre er anschließend nach den allgemeinen Grundsätzen zur Kostentragung verpflichtet.[264] Dieses Ergebnis entspricht sicherlich nicht dem Zweck von § 21 Abs. 1 TTDSG.

Es erscheint deshalb unumgänglich bereits das Auskunftsbegehren des Rechteinhabers als Anordnung der zuständigen Stelle anzusehen.[265] Natürlich überzeugt es aber eigentlich nicht, dass der Rechteinhaber selbst die Auskunftserteilung durch den Diensteanbieter anordnen können soll.[266] Zudem müsste man wohl jede „Anordnung" des Rechteinhabers ausreichen lassen. Das hätte aber eine generelle Zulässigkeit der Bestandsdatenauskunft zur Durchsetzung der Rechte am geistigen Eigentum durch Telemediendiensteanbieter zur Folge, die sich so aus dem Wortlaut des § 21 Abs. 1 TTDSG nicht ergibt.

Um dem entgegenzuwirken, wird teilweise angenommen, der Anspruchsteller müsste dem Diensteanbieter seinen Anspruch glaubhaft und substantiiert darlegen, sodass er für den Diensteanbieter klar erkennbar ist.[267] Es ist allerdings zu bezweifeln, ob diese Lösung die Situation für Rechteinhaber und Diensteanbieter verbessern würde. Es ergibt sich außerdem aus dem Wortlaut der Norm, der eine „Anordnung" voraussetzt, nicht, dass nun der Diensteanbieter im Einzelfall

---

[262] S. *Janal*, Europäisches Zivilverfahrensrecht, S. 268 f.
[263] S. *Janal*, Europäisches Zivilverfahrensrecht, S. 268.
[264] Vgl. *Janal*, Europäisches Zivilverfahrensrecht, S. 268.
[265] So etwa *Schmitz* in: Spindler/Schmitz, § 14 TMG Rn. 42.
[266] Ähnlich auch *Janal*, Europäisches Zivilverfahrensrecht, S. 268.
[267] So etwa *Schmitz* in: Spindler/Schmitz, § 14 TMG Rn. 42.

prüfen muss, ob der Rechteinhaber seinen Anspruch hinreichend glaubhaft und substantiiert vorbringt.

Im Ergebnis bleibt es daher leider unklar, ob und unter welchen Voraussetzungen der Diensteanbieter den Rechteinhabern Auskunft über Bestandsdaten erteilen darf. In der derzeitigen Fassung stellt § 21 Abs. 1 TTDSG beide Parteien eines Auskunftsersuchens vor erhebliche Unsicherheiten.

dd) Übermittlung an Rechteinhaber nach § 21 Abs. 2-4 TTDSG

§ 21 Abs. 2-4 TTDSG enthält ebenfalls eine Regelung, die eine Verarbeitung von Bestandsdaten zur Auskunftserteilung an Dritte erlaubt. Diese Vorschrift ist aber anders ausgestaltet als die Erlaubnisnorm zur Durchsetzung der Rechte am geistigen Eigentum aus § 21 Abs. 1 TTDSG. § 21 Abs. 2-4 TTDSG greift lediglich bei bestimmten Verletzungen absoluter Rechte und unterliegt denselben Voraussetzungen wie der dazugehörige Auskunftsanspruch aus § 21 Abs. 2 S. 2 TTDSG.[268] Die Zulässigkeit der Auskunftserteilung setzt in diesen Fällen anders als nach § 21 Abs. 1 TTDSG eine gerichtliche Anordnung voraus. Auf Antrag der Rechteinhaber wird in einem einheitlichen Verfahren nach § 21 Abs. 3 TTDSG über die Zulässigkeit der Auskunftserteilung, aber zugleich auch über die Verpflichtung der Diensteanbieter entschieden.[269]

b) § 24 BDSG

Auch § 24 BDSG ermöglicht die zweckändernde Weiterverarbeitung von personenbezogenen Daten. Nach § 24 Abs. 1 Nr. 2 BDSG ist die Verarbeitung von Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche zulässig, sofern nicht die Interessen der betroffenen Person überwiegen. Zu den zivilrechtlichen Ansprüchen zählen auch Unterlassungs- oder Schadensersatzansprüche gegen Nutzer von Internetdiensten.[270] Ebenso wie § 21 TTDSG kann § 24 BDSG auf die Öffnungsklausel des Art. 6 Abs. 4 DS-GVO

---

[268] S. zu den Voraussetzungen des Auskunftsanspruchs oben unter Kap. 5 § 2 B.

[269] Ausführlicher zum Gestattungsverfahren unten unter Kap. 5 § 4 A.

[270] S. auch *Rose* in: Taeger/Gabel, § 24 BDSG Rn. 13.

gestützt werden.[271] Deshalb ist § 24 BDSG trotz Inkrafttreten der DS-GVO anwendbar. § 24 BDSG kann damit also grundsätzlich die Auskunftserteilung von Internetdiensteanbietern an die Rechteinhaber bei der Verletzung absoluter Rechte erlauben.

aa) Anwendbarkeit auf Telemediendienste

Im Hinblick auf die Anbieter von Telemedien stellt sich die Frage nach dem Verhältnis von § 24 BDSG zu § 21 TTDSG. Anders als § 21 TTDSG ist § 24 BDSG nicht begrenzt auf bestimmte Rechtsverletzungen. Außerdem erfordert § 24 BDSG im Unterschied zu § 21 Abs. 3 TTDSG auch keine richterliche Anordnung für die Zulässigkeit der Auskunftserteilung. Eine Anwendung von § 24 BDSG auf die Bestandsdatenauskunft durch Telemediendienste würde die Regelungen des § 21 TTDSG deshalb weitgehend unterlaufen.

Nach § 1 Abs. 2 S. 1 BDSG haben bereichsspezifische Regelungen über den Datenschutz auch nach dem Inkrafttreten der DS-GVO grundsätzlich Vorrang gegenüber den Vorschriften des BDSG. Das gilt aber nur für Regelungen wie § 21 TTDSG, die auch nach Inkrafttreten der DS-GVO noch anwendbar sind.

Zudem ist § 21 TTDSG als abschließende Regelung im Sinne von § 1 Abs. 2 S. 2 BDSG anzusehen. § 24 BDSG ist deshalb auf Telemediendienste auf Grund der spezielleren Vorschrift des § 21 TTDSG nicht anwendbar.[272] Das gilt auch dann, wenn etwa eine Rechtsverletzung nicht von § 21 Abs. 2-4 TTDSG erfasst wird.

Auch mit Blick auf die Gesetzgebungshistorie zeigt sich deutlich, dass für den Bereich der Telemedien eine Anwendung des § 24 BDSG vom Gesetzgeber nicht vorgesehen ist: Ursprünglich war es nämlich im Gesetzesentwurf zum Netzwerkdurchsetzungsgesetz vorgesehen, anstelle der Einführung der Absätze 3-5 in § 14 TMG a.F., § 14 Abs. 2 TMG a.F. auf alle absolut geschützten

---

[271] S. *Regierungsentwurf,* BT-Drs. 18/11325, S. 96. A.A. *Herbst* in: Kühling/Buchner, § 24 BDSG Rn. 13.

[272] So auch *BGH*, Beschl. v. 24.9.2019 – VI ZB 39/18, GRUR 2020, 101 Rn. 30 – Facebook-Messenger; *OLG Frankfurt a.M.,* Beschl. v. 6.9.2018 – 16 W 27/18, ZUM-RD 2019, 145, 147; *Hullen/Roggenkamp* in: Plath, § 14 TMG Rn. 22.

Rechte auszuweiten.[273] Dabei sollte es sich zunächst um eine Übergangsregelung bis zum Inkrafttreten der DS-GVO handeln, nach der der Gesetzgeber den bereichsspezifischen Telemediendatenschutz aufheben wollte, sodass nur noch die Regelungen des BDSG und der DS-GVO im Bereich der Telemedien gelten sollten.[274] Von diesen Plänen hat der Gesetzgeber allerdings Abstand genommen, indem er stattdessen § 14 Abs. 3-5 TMG a.F. eingeführt hat und im Jahr 2021 die Regelung des § 14 Abs. 2-5 TMG a.F. in § 21 TTDSG weitergeführt hat.[275] Daraus wird ersichtlich, dass die Auskunftserteilung durch Telemediendienste über Bestandsdaten der Nutzer nur noch in bestimmten abschließend geregelten Fällen und im Falle von § 21 Abs. 3 TTDSG nur mittels gerichtlicher Anordnung zulässig sein soll.

Der Gesetzgeber wollte die Bestandsdatenauskunft im Bereich der Telemedien daher nur in begrenzten Fällen und nur zur Durchsetzung bestimmter Ansprüche für zulässig erklären. Eine Anwendung des § 24 BDSG würde deshalb dem Willen des Gesetzgebers zuwiderlaufen und § 21 TTDSG konterkarieren. § 21 TTDSG regelt also abschließend für den Bereich der Telemedien, in welchen Fällen Bestandsdaten zur Auskunftserteilung verwendet und weitergegeben werden dürfen. Für eine Anwendung des § 24 BDSG bleibt daneben kein Raum.

bb) Anwendbarkeit auf Telekommunikationsdienste

Für Telekommunikationsdienste existiert keine mit § 21 TTDSG vergleichbare spezielle Regelung. § 1 Abs. 2 BDSG würde einer Anwendung von § 24 Abs. 1 Nr. 2 BDSG auf die Bestandsdatenauskunft an private Rechteinhaber durch Telekommunikationsdienste zumindest auf den ersten Blick nicht entgegenstehen.

Dennoch ist § 24 Abs. 1 Nr. 2 BDSG in dieser Hinsicht auf Grund zwei verschiedener Erwägungen jedenfalls teleologisch zu reduzieren. Zum einen stünde die Bestandsdatenauskunft durch Telekommunikationsdienste unter den

---

[273] S. *Gesetzesentwurf,* BT-Drs. 18/12356, S. 10. Dieses Vorhaben führte zu teilweiser massiver Kritik in der Literatur, S. etwa Spindler, ZUM 2017, 473, 486.

[274] S. *Gesetzesentwurf*, BT-Drs. 18/12356, S. 28.

[275] Vgl. auch *BGH*, Beschl. v. 24.9.2019 – VI ZB 39/18, GRUR 2020, 101 Rn. 30 – Facebook-Messenger.

Voraussetzungen des § 24 Abs. 1 Nr. 2 BDSG im Widerspruch zu § 21 TTDSG. Es überzeugt nicht, dass die Verarbeitung von Bestandsdaten zur Auskunftserteilung durch Telemediendienste unter engeren Voraussetzungen möglich ist, als es bei Anwendungsdiensten, die unter das Telekommunikationsgesetz fallen, bei Anwendung von § 24 BDSG der Fall wäre. Vor allem im Hinblick auf den Schutz von Nutzerdaten sind an Telekommunikationsdienste in der Regel strengere Anforderungen zu stellen.

Zum anderen widerspräche die Anwendung von § 24 Abs. 1 Nr.2 BDSG der Regelung des § 174 TKG. § 174 Abs. 1 S. 1 TKG erlaubt die Bestandsdatenauskunft an bestimmte Behörden oder öffentliche Stellen zum Beispiel zum Zwecke der Strafverfolgung oder der Gefahrenabwehr. Zumindest im Hinblick auf eine Auskunft gegenüber öffentlichen Stellen darf § 24 Abs. 1 Nr. 1 BDSG nicht angewendet werden, damit § 174 TKG nicht unterlaufen wird. Aber auch in Bezug auf die Auskunftserteilung an private Rechteinhaber wäre es unstimmig, wenn die Bestandsdatenauskunft an Behörden an strengere Voraussetzungen geknüpft würde als bei einer Auskunft gegenüber Privatpersonen. Vielmehr ist davon auszugehen, dass der Gesetzgeber anders als im Bereich der Telemedien bewusst auf die Einführung einer datenschutzrechtlichen Erlaubnis der Bestandsdatenauskunft durch Telekommunikationsdienste an Private verzichtet hat. § 174 TKG könnte insofern auch als abschließende Regelung i.S.d. § 1 Abs. 2 BDSG für die Bestandsdatenauskunft durch Telekommunikationsdienste gewertet werden.

Bei Telekommunikationsdiensten richtet sich die Zulässigkeit der zweckändernden Weiterverarbeitung zur Auskunftserteilung an Rechteinhaber deshalb ausschließlich nach Art. 6 Abs. 4 DS-GVO. Die Weiterverarbeitung ist nur erlaubt, wenn diese mit dem Zweck, zu dem die Daten ursprünglich erhoben wurden, vereinbar ist.[276] Die Bestandsdaten werden von den Diensteanbietern vor allem zu Vertragszwecken erhoben. Die strengen Kriterien der Vereinbarkeit werden bei der Weitergabe dieser Daten zum Zwecke der Rechtsdurchsetzung Dritter daher in der Regel nicht erfüllt sein.

---

[276] Ausführlich zu den Kriterien des Kompatibilitätstests, S. etwa *Albers/Veit* in: BeckOK Datenschutzrecht, Art. 6 DS-GVO Rn. 104; *Spindler/Dalby* in: Spindler/Schuster, Art. 6 DS-GVO Rn. 22 ff.

cc) Anwendbarkeit auf sonstige Dienste

Auf Anwendungsdienste, die weder Telekommunikationsdienste noch Telemediendienste anbieten, bleibt § 24 Abs. 1 Nr. 2 BDSG aber anwendbar. Der einzige relevante Anwendungsbereich dürfte hinsichtlich einer Auskunftserteilung der DENIC, der Domain-Registrare, der Anbieter von Privacy-Domains oder der administrativen Ansprechpartner einer Domain über die Inhaber einer Domain sein. Für diese Dienste gelten keine bereichsspezifischen Datenschutzvorschriften. Insofern unterscheiden sie sich von den anderen Anwendungsdiensten im Internet, da sie weder kommunikations- noch inhaltsbezogen agieren, sondern lediglich administrative Aufgaben erfüllen. Daher widerspricht eine Anwendung von § 24 Abs. 1 Nr. 2 BDSG auch nicht den bereichsspezifischen Regelungen aus dem TKG oder TTDSG.

Die Weiterverarbeitung von Bestandsdaten zur Auskunftserteilung an private Rechteinhaber ist zur Durchsetzung deren zivilrechtlicher Ansprüche daher datenschutzrechtlich nach § 24 Abs. 1 Nr. 2 BDSG zulässig, sofern nicht im Einzelfall die Interessen der betroffenen Person entgegenstehen.

4. Zwischenergebnis zu Bestandsdatenauskunft der Anwendungsdienste

Die Identifizierung eines anonymen Rechtsverletzers durch die Bestandsdatenauskunft der Anwendungsdienste ist im Ergebnis also nur denkbar, wenn der Diensteanbieter entsprechende Bestandsdaten seiner Nutzer vorhält. Auch wenn dies nach den allgemeinen Vorschriften der Art. 5, 6 DS-GVO insbesondere zu Vertragszwecken zulässig sein kann, besteht meistens keine Pflicht zur Speicherung solcher Nutzerdaten.

Zudem stellt die Auskunftserteilung über möglicherweise beim Anbieter gespeicherte Daten eine zweckändernde Weiterverarbeitung i.S.v. Art. 6 Abs. 4 DS-GVO dar. Ob eine solche im Einzelfall zulässig ist, unterscheidet sich nach der Art des Anwendungsdienstes: Bei Telemediendiensten ist die Auskunftserteilung nur nach den Maßstäben des § 21 TTDSG erlaubt. Im Bereich der Telekommunikationsdienste wird die zweckändernde Weiterverarbeitung zur Erteilung einer Auskunft an private Dritte in der Regel an den engen Kriterien der Vereinbarkeit mit dem ursprünglichen Zweck der Datenerhebung nach Art. 6 Abs. 4 DS-GVO scheitern. Die Auskunft der DENIC oder von Domain-

Registraren über Bestandsdaten ihrer Nutzer kann dagegen zumeist auf § 24 Abs. 1 Nr. 2 BDSG gestützt werden.

III. Nutzungs- und Verkehrsdatenauskunft der Anwendungsdienste

Neben den Bestandsdaten können auch Daten, die während der konkreten Nutzung eines Anwendungsdienstes anfallen, zur Identifizierung der Nutzer beitragen. Bei solchen Daten handelt es sich um Nutzungs- beziehungsweise um Verkehrsdaten.

Dabei ist zwischen zwei verschiedenen Konstellationen zu unterscheiden: Zum einen können solche Daten zur Bestandsdatenauskunft verwendet werden. Das ist zum Beispiel der Fall, wenn die Diensteanbieter eine IP-Adresse den passenden Bestandsdaten eines Nutzers zuordnen. In diesem Fall werden zwar lediglich die so ermittelten Bestandsdaten bei der Auskunft übermittelt, dennoch handelt es sich nicht um eine „reine" Bestandsdatenauskunft, da zur Auskunftserteilung Nutzungs- oder Verkehrsdaten verarbeitet werden.

Zum anderen besteht oft auch ein Interesse der Rechteinhaber daran, die Nutzungs- beziehungsweise Verkehrsdaten selbst in Erfahrung zu bringen. Vor allem, wenn sie die Nutzer anhand der IP-Adresse ermitteln wollen, werden sie versuchen herauszufinden, wann der anonyme Nutzer unter welcher IP-Adresse den fraglichen Anwendungsdienst genutzt hat.

1. Begriff der Nutzungs- und Verkehrsdaten

Der Begriff der Verkehrsdaten erstreckt sich ausschließlich auf Telekommunikationsdienste. § 3 Nr. 70 TKG definiert Verkehrsdaten als Daten, „deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind".[277] Nutzungsdaten sind nach § 2 Abs. 2 Nr. 3 TTDSG die personenbezogenen Daten eines Nutzers, „deren Verarbeitung erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen oder abzurechnen". Damit stellen sie eine Art Unterfall von Verkehrsdaten für das Telemedienrecht dar.[278] Personenbezogene Daten, die bei der Erbringung des

[277] S. zur Neuregelung des § 3 Nr. 70 TKG *Kiparski,* CR 2021, 482, 484.
[278] *Ettig* in: Taeger/Gabel, § 2 TTDSG Rn. 28.

Dienstes verarbeitet werden, sind deshalb je nach Art des Anwendungsdienstes Nutzungs- beziehungsweise Verkehrsdaten.

§ 2 Abs. 2 Nr. 3 TTDSG zählt als Beispiele für Nutzungsdaten Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie den Umfang der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien auf. Aber auch Informationen aus Cookies oder über den verwendeten Browser oder über das Betriebssystem stellen Nutzungsdaten beziehungsweise Verkehrsdaten dar.[279]

Von besonderer Bedeutung für die Rechteinhaber zur Identifizierung eines Nutzers sind vor allem IP-Adressen, sowie Informationen über Datum und Uhrzeit der Nutzung. Für die Anwendungsdienste kommt es zudem nicht darauf an, ob die Nutzer über statische oder dynamische IP-Adressen auf ihren Dienst zugreifen. Da die Anwendungsdienste die IP-Adressen nicht selbst zuweisen, stellen sowohl statische als auch dynamische IP-Adressen Nutzungs- beziehungsweise Verkehrsdaten dar.[280]

2. Personenbezug der IP-Adresse

Bevor beurteilt werden kann, ob die Anwendungsdienste Informationen über IP-Adressen zur Auskunftserteilung verwenden oder an die Rechteinhaber übermitteln dürfen, gilt es zu klären, ob es sich hierbei überhaupt um personenbezogene Daten handelt. Nach Art. 4 Nr. 1 DS-GVO sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person" beziehen.

Ein Personenbezug zur IP-Adresse besteht daher für die Diensteanbieter zumindest dann, wenn sie die IP-Adresse mit weiteren zur Identifizierung geeigneten Informationen verknüpfen können, sodass sie diese einer natürlichen Person zuordnen können.[281] Das ist zum Beispiel der Fall, wenn sie den Namen der Nutzer gespeichert haben und diesen mit der IP-Adresse in Verbindung bringen können. In Anbetracht der immer weitreichenderen Möglichkeiten, Daten von

---

[279] *Ettig* in: Taeger/Gabel, § 2 TTDSG Rn. 33.
[280] A.A. aber *Ettig* in: Taeger/Gabel, § 22 TTDSG Rn. 10.
[281] Vgl. Erwägungsgrund 30 der DS-GVO.

Internetnutzern massenweise zu erheben und miteinander zu kombinieren, werden in vielen Fällen bereits die Anwendungsdienste den Personenbezug zu einer IP-Adresse herstellen können.[282] Vor allem bei statischen IP-Adressen handelt es sich auch für die Anwendungsdienste meist um personenbezogene Daten, da diese immer demselben Anschluss zugewiesen werden und den Anschlussinhaber dadurch leichter identifizierbar machen.[283]

Die Zugangsanbieter können – anders als die Anwendungsdienste – den Nutzer zumindest bis zu einem Anschlussinhaber zurückverfolgen und damit gegebenenfalls die IP-Adresse in Bezug zu einer Person setzen.[284] Schwieriger zu beurteilen ist deshalb, ob es für die Bestimmbarkeit einer Person ausreichend ist, wenn nur der Zugangsanbieter als Dritter den Personenbezug herstellen kann. Entscheidend hierfür ist das Verständnis über den Begriff des Personenbezugs.[285] Ausgehend von einer absoluten Begriffsauslegung würde es genügen, wenn die hinter einer IP-Adresse stehende Person für irgendjemanden ermittelbar wäre.[286] Im Gegensatz dazu kommt es bei einem relativen Verständnis des Personenbezugs darauf an, ob dieser für den konkreten Diensteanbieter herstellbar ist. [287]

Der *EuGH* hat sich anlässlich einer entsprechende Vorlage durch den Bundesgerichtshof mit der Frage befasst, ob die IP-Adresse für den Anbieter einer

---

[282] S. dazu auch *Breyer*, ZD 2014, 400, 401.

[283] Vgl. auch *EuGH*, Urt. v. 19.10.2016 – C-582/14, NJW 2016, 3579 Rn. 36 – Breyer; *Bergt*, ZD 2015, 365, 370; *Breyer*, ZD 2014, 400, 401.

[284] S. zum Personenbezug von IP-Adressen bei Zugangsanbietern *EuGH*, Urt. v. 24. 11. 2011 - C-70/10, GRUR 2012, 265 Rn. 51 – Scarlet/SABAM. Zurecht darauf hinweisend, dass Anschlussinhaber und Nutzer nicht identisch sein müssen und auch juristische Personen Anschlussinhaber sein können *Härting,* CR 2008, 743, 755 f.; *Kartheuser/Gilsdorf*, MMR-Aktuell 2016, 382533.

[285] Ausführlicher hierzu bei den Ausführungen in der Vorlage des *BGH*, Beschl. v. 28.10.2014 – VI ZR 135/13, GRUR 2015, 192, 194 m.w.N. S. auch ausführlich zum damaligen Meinungsstreit *Bergt,* ZD 2015, 365, 365 ff. m.w.N.

[286] *Breyer,* ZD 2014, 400, 405; *Buchner,* DuD 2016, 155, 156; *Dregelies*, VuR 2017, 256, 257; *Herbst,* NVwZ 2016, 902, 904 f.

[287] *Eckhardt*, CR 2016, 786, 789; *Eßer* in: Auernhammer, Art. 4 DS-GVO Rn. 15; *Kartheuser/Gilsdorf*, MMR-Aktuell 2016, 382533; *Roßnagel/Kroschwald*, ZD 2014, 495, 496 f.; *Schatz*, NJW 2016, 1841, 1843; *Schreiber* in: Plath, Art. 4 DS-GVO Rn. 9 ff.

Webseite ein personenbezogenes Datum im Sinne der damals noch gültigen DSRL[288] darstellt, auch wenn der Diensteanbieter selbst die hinter der IP-Adresse stehende Person nicht ermitteln kann.[289] Der EuGH hat in seiner Entscheidung einen Mittelweg gewählt und entschieden, dass es sich auch für den Webseitenbetreiber grundsätzlich bei den IP-Adressen seiner Nutzer um personenbezogene Daten handeln kann.[290] Dies setzt jedoch voraus, dass der Diensteanbieter über rechtliche Mittel verfügt, die es ihm erlauben, ohne unverhältnismäßigen Aufwand die betreffende Person anhand der Zusatzinformationen des Zugangsanbieters bestimmen zu lassen.[291] Der EuGH legt bei seiner Entscheidung ein weites Verständnis vom Begriff des „rechtlichen Mittels" zu Grunde. Es kommt nicht darauf an, ob der Diensteanbieter im konkreten Fall etwa mittels eines Auskunftsanspruchs die Möglichkeit hätte die hinter der IP-Adresse stehende Person zu identifizieren, sondern lediglich, ob er abstrakt betrachtet über rechtliche Mittel verfügt, die betreffende Person zu ermitteln.[292]

Dieser Ansicht ist anschließend auch der *BGH* gefolgt, indem er den Personenbezug der IP-Adresse für den Webseiten-Betreiber bereits deshalb bejaht hat, weil dieser beispielsweise Strafanzeige bei den Strafverfolgungsbehörden erstatten oder gegebenenfalls die zur Gefahrenabwehr zuständigen Behörden einschalten könnte.[293] Die rein theoretische Möglichkeit einer Identifizierung würde demnach bereits ausreichen, um den Personenbezug der IP-Adresse zu begründen. Bei einer derart weiten Auslegung des relativen Personenbezugs werden für die Anbieter von Anwendungsdiensten IP-Adressen daher in aller Regel personenbezogene Daten darstellen.[294]

Die Entscheidung des *EuGH* ist auch nach dem Inkrafttreten der DS-GVO noch relevant, da sich die Begriffe Bestimmbarkeit aus Art. 2 lit. a) DSRL und

---

[288] Richtlinie 95/46/EG des europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Abl. 1995 L 281, 31.

[289] *EuGH*, Urt. v. 19.10.2016 – C-582/14, NJW 2016, 3579 - Breyer.

[290] *EuGH*, Urt. v. 19.10.2016 – C-582/14, NJW 2016, 3579 - Breyer.

[291] *EuGH*, Urt. v. 19.10.2016 – C-582/14, NJW 2016, 3579, 3580 f. - Breyer.

[292] S. *Mantz/Spittka*, NJW 2016, 3582, 3582.

[293] *BGH*, Urt. v. 16.5.2017 – VI ZR 135/13, NJW 2017, 2416, 2418.

[294] Ähnlich *Kühling/Klar*, ZD 2017, 24, 28.

der Identifizierbarkeit im Sinne von Art. 4 Nr. 1 DS-GVO gleichen.[295] Im Grundsatz legte der *EuGH* in seiner Entscheidung ein relatives Verständnis des Personenbezugs zu Grunde, bei dem es auf die Person ankommt, die die Daten verarbeitet.[296] Allerdings wurden insoweit auch Elemente der absoluten Theorie aufgenommen, als dass das Wissen Dritter berücksichtigt werden kann, wenn die verarbeitende Person über Mittel verfügt, mit diesem Wissen eine Identifizierung herbeizuführen.[297] Diese Bestandteile der Entscheidung bleiben auch für die Auslegung des Begriffs der personenbezogenen Daten in der DS-GVO maßgeblich.

Abweichungen von der bisherigen Rechtsprechung ergeben sich aber aus dem neuen Erwägungsgrund 26 der DS-GVO.[298] Demnach sollten, um festzustellen, ob eine natürliche Person identifizierbar ist, „alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren". Im Unterschied dazu kam es im Rahmen von Erwägungsgrund 26 der DSRL noch darauf an, ob Mittel „vernünftigerweise" – also im Rahmen der rechtlichen Möglichkeiten – eingesetzt werden können.[299] Daher kann davon ausgegangen werden, dass durch das Weglassen des Merkmals der „Vernunftgebundenheit" im Rahmen der DS-GVO jetzt auch illegale Möglichkeiten einer Identifizierung den Personenbezug herstellen können.[300] Entscheidend ist nunmehr dafür, ob die zur Verfügung stehenden Mittel auch

---

[295] S. dazu *Brauneck,* EuZW 2019, 680, 682.

[296] *Karg* in: Simitis/Hornung/Spieker in: Art. 4 Nr. 1 DS-GVO Rn. 60; *Karg,* DuD 2015, 520, 525; *Kartheuser/Gilsdorf*, MMR-Aktuell 2016, 382533; *Kipker/Kubis*, MMR 2017, 608, 609; *Klarg/Kühling* in: Kühling/Buchner, Art. 4 Nr. 1 DS-GVO Rn. 26; *Kring/Marosi*, K&R 2016, 773, 774; *Krügel*, ZD 2017, 455, 459; *Kühling/Klar,* ZD 2017, 24, 28; *Mantz/Spittka,* NJW 2016, 3579, 3582; *Marnau,* DuD 2016, 428, 429 f.; *Moos/Rothkegel*, MMR 2016, 845, 845; *Schantz,* NJW 2016, 1841, 1842 f.; *Ziegenhorn*, NVwZ 2017, 216, 217; A.A. wohl *Brink/Eckhardt*, ZD 2015, 205, 209; *Dregelies,* VuR 2017, 256, 257; *Gola* in: Gola, Art. 4 DS-GVO Rn. 16 ff.; *Hansen/Struwe*, GRUR-Prax 2016, 503, 503.

[297] *EuGH*, Urt. v. 19.10.2016 – C-582/14, NJW 2016, 3579 Rn. 43 ff. - Breyer.

[298] Vgl. *Brauneck,* EuZW 2019, 680, 683.

[299] S. dazu die *Generalanwalt Sanchez-Bordona*, Schlussantrag vom 12.05.2016 - EUGH Aktenzeichen C-582/14, BeckRS 2016, 81027 Rn. 72 – Breyer. S. auch *EuGH*, Urt. v. 19.10.2016 – C-582/14, NJW 2016, 3579 Rn. 45 f. – Breyer.

[300] *Brauneck,* EuZW 2019, 680, 684.

„wahrscheinlich" zur Identifizierung genutzt werden.[301] Völlig abstrakte, rein theoretische Möglichkeiten der Identifizierung reichen dadurch nicht mehr unbedingt aus, um den Personenbezug einer IP-Adresse zu begründen.[302]

Ob die IP-Adresse für einen Anwendungsdienst ein personenbezogenes Datum darstellt, kann daher nur anhand des konkreten Einzelfalls beurteilt werden. Je mehr Daten die Diensteanbieter über ihre Nutzer erheben und vorhalten, desto eher wird ein Personenbezug anzunehmen sein. Wenn die IP-Adresse zur Bestandsdatenauskunft verwendet werden soll, handelt es sich aber bei der IP-Adresse in jedem Fall um ein personenbezogenes Datum, da die Anwendungsdienste in diesem Fall den Personenbezug durch die Verknüpfung mit den Bestandsdaten herstellen.

Sofern lediglich Auskunft über die IP-Adresse und Zugriffszeiten der Nutzer erteilt werden soll, kann die IP-Adresse im Einzelfall für den Anwendungsdienst kein personenbezogenes Datum darstellen. In datenschutzrechtlicher Hinsicht wäre in diesem Fall die Verarbeitung der IP-Adresse weitgehend unproblematisch. Die nachfolgenden Ausführungen beschränken sich daher darauf, die Verarbeitung personenbezogener Daten zu untersuchen. Soweit Diensteanbieter Daten automatisiert speichern, wird sich häufig aber ohnehin nicht ohne weiteres feststellen lassen, ob sie einen Personenbezug zu einzelnen Daten herstellen können. Daher werden die Diensteanbieter diese Daten wie personenbezogene Daten behandeln müssen.

3. Speicherung der Daten

Damit die Anwendungsdienste Nutzungs- beziehungsweise Verkehrsdaten zur Auskunftserteilung verarbeiten können, müssen sie vorher die entsprechenden Daten ihrer Nutzer erheben und in ihren Log-Files speichern. Bei der Beurteilung der Zulässigkeit einer solchen Speicherung muss erneut zwischen Telekommunikations- und Telemediendiensten unterschieden werden.[303]

---

[301] *Brauneck,* EuZW 2019, 680, 684 ff.

[302] *Brauneck,* EuZW 2019, 680, 684 ff.; *Arning/Rothkegel* in: Taeger/Gabel, Art. 4 DS-GVO Rn. 31.

[303] Sonstige Anwendungsdienste, die weder Telekommunikations- noch Telemediendienste darstellen, spielen bei der Nutzungs- beziehungsweise Verkehrsdatenauskunft keine Rolle, da insbesondere bei den Domain-Registries die Bestandsdatenauskunft im Vordergrund steht.

a) Telemediendienste

Der Unterscheidung zwischen Nutzungs- und Bestandsdaten für Telemediendienste kommt nach dem Inkrafttreten der DS-GVO grundsätzlich keine besondere Rolle mehr zu. Inwieweit diese personenbezogenen Daten erhoben und gespeichert werden dürfen, richtet sich nach den allgemeinen Regeln der Art. 5, 6 DS-GVO. Die Regelung des § 15 Abs. 1 TMG a.F. zur Zulässigkeit der Speicherung von Nutzungsdaten ist spätestens seit dem Inkrafttreten der DS-GVO nicht mehr anwendbar und seit der Einführung des TTDSG auch vom Gesetzgeber aufgehoben worden.[304]

Ebenso wie auch bei der vorab untersuchten Speicherung von Bestandsdaten durch Telemediendiensteanbieter sind hier daher allein die allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten aus Art. 5, 6 Abs. 1 lit. a)-f) DS-GVO maßgeblich. Die Erhebung von Daten wie der IP-Adresse ist meist schon erforderlich, damit die angefragten Datenpakete an die richtigen Empfänger gelangen können. Darüber hinaus sind verschiedene Gründe denkbar, nach denen eine längerfristige Speicherung von Nutzungsdaten in den Log-Dateien der Anbieter zulässig sein könnte. So lässt sich unter Umständen die Speicherung von IP-Adressen zum Beispiel zum Schutz vor Cyberangriffen rechtfertigen.[305] Aber auch zu Abrechnungszwecken oder mit einer Einwilligung der Nutzer ist eine Speicherung von Nutzungsdaten denkbar.

Jedenfalls kann die Zulässigkeit der Speicherung nur anhand des konkreten Einzelfalls beurteilt werden. Eine Verpflichtung zur Speicherung von Nutzungsdaten wie IP-Adressen und Zugriffszeiten besteht nämlich auch hier ebenso wenig, wie die Möglichkeit, präventiv für etwaige spätere Auskunftsersuchen Dritter Nutzungsdaten vorzuhalten. Die Rechteinhaber sind daher für ihr Auskunftsbegehren stets auf Daten angewiesen, die die Diensteanbieter zu einem anderen Zweck erhoben und gespeichert haben.

---

[304] S. Artikel 3 des Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien *Beschlussempfehlung und Bericht des Ausschusses für Wirtschaft und Energie*, BT-Drs 19/29839 , S. 53 f. S. auch *Regierungsentwurf,* BT-Drs. 19/27441, S. 1 f. Die Regelung des § 15 Abs. 1 TMG a.F. wurde aber auch bereits vor Inkrafttreten der DS-GVO bereits für unionsrechtswidrig erklärt, S. *EuGH,* Urt. v. 19.10.2016 – C-582/14, NJW 2016, 3579 Rn. 59 ff. – Breyer.

[305] *Spindler* in: Spindler/Schmitz, § 15 TMG Rn. 54.

b) Telekommunikationsdienste

Für Anwendungsdienste, bei denen es sich um Telekommunikationsdienste handelt, stellen die während des Nutzungsvorgangs anfallenden Daten Verkehrsdaten dar. Verkehrsdaten unterliegen dem besonderen Schutz des Fernmeldegeheimnisses und dürfen nur in sehr engen Grenzen verarbeitet werden.

Seitdem Anwendungsdienste wie Over-the-top-Dienste (z.B. E-Mail-Dienste oder Messenger-Dienste) ausdrücklich den Telekommunikationsdiensten zugeordnet werden, unterliegen diese dem Fernmeldegeheimnis nach § 3 TTDSG. Insofern dürfen die Anbieter Verkehrsdaten wie die IP-Adresse und Datum und Uhrzeit der Nutzung nach § 9 Abs. 1 S. 1 TTDSG nur speichern, „soweit dies zum Aufbau und zur Aufrechterhaltung der Telekommunikation, zur Entgeltabrechnung oder zum Aufbau weiterer Verbindungen erforderlich ist". Darüber hinaus dürfen Verkehrsdaten nicht verarbeitet werden (§ 9 Abs. 1 S. 3 TDSG) und sind unverzüglich nach Beendigung der Verbindung zu löschen (§ 9 Abs. 1 S. 2 TTDSG). Die §§ 3 und 9 TTDSG dienen außerdem der Umsetzung der e-privacy-Richtlinie und sind daher auch nach Inkrafttreten der DSGVO vorrangig anwendbar.[306]

Zur Vorratsdatenspeicherung nach § 176 TKG sind – unabhängig von deren Verfassungs- und Unionsrechtskonformität[307] – die meisten Anwendungsdienste nicht verpflichtet, da nummernunabhängige interpersonelle Kommunikationsdienste hiervon ausgenommen sind.[308]

Die Anwendungsdienste dürfen Verkehrsdaten insgesamt also nur im sehr engen Rahmen des § 9 Abs. 1 TTDSG speichern. Es muss deshalb davon ausgegangen werden, dass in vielen Fällen die Auskunftserteilung bereits daran scheitern wird, dass die angefragten Daten überhaupt nicht (mehr) vorhanden sind.

---

[306] S. bereits oben unter Kap. 5 § 3 A. I.

[307] S. dazu Kap. 5 § 3 D. II. 1. c).

[308] S. zum Begriff der nummernunabhängigen interpersonellen Kommunikationsdienste oben unter Kap. 5 § 3 A. II. 1.

4. Übermittlung der Daten

Nutzungs- und Verkehrsdaten werden – wenn überhaupt – von den Diensteanbietern nicht zur späteren Auskunftserteilung an private Rechteinhaber gespeichert. Wenn diese Daten dennoch später zu diesem Zweck verwendet werden, handelt es sich um eine zweckändernde Weiterverarbeitung. Deren Zulässigkeit muss erneut getrennt anhand der Art des jeweiligen Anwendungsdienstes beurteilt werden.

a) Telemediendienste

Für Telemediendienste bestand in § 15 Abs. 5 S. 4 TMG a.F. ein Verweis auf § 14 Abs. 2-5 TMG a.F. (entspricht § 21 TTDSG), sodass unter denselben Voraussetzungen auch eine Auskunftserteilung über Nutzungsdaten zulässig war.[309] Mit dem Inkrafttreten des TTDSG ist diese Vorschrift jedoch weggefallen. Das TTDSG enthält keinen entsprechenden Verweis mehr auf § 21 TTDSG.[310]

Im Gegensatz dazu führt das TTDSG aber die Regelungen zur Auskunftserteilung an öffentliche Stellen aus §§ 15 a-c TMG a.F. in §§ 22 – 24 TTDSG fort. § 22 Abs. 1 S. 3 TTDSG erlaubt, dass die in eine Auskunft aufzunehmenden Bestandsdaten auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse bestimmt werden dürfen. Nach § 24 Abs. 1 TTDSG darf auch Auskunft über die Nutzungsdaten selbst erteilt werden. §§ 22-24 TTDSG sind aber begrenzt auf die Auskunft an bestimmte öffentliche Stellen, die nur unter besonderen Voraussetzungen – zum Beispiel zur Gefahrenabwehr – erteilt werden darf.

Da der Verweis aus § 15 Abs. 5 S. 4 TMG a.F. im Unterschied zu den Regelungen aus §§ 15 a-c TMG a.F. nicht in das TTDSG übernommen wurde, ist davon auszugehen, dass das TTDSG eine abschließende Regelung über die

---

[309] S. zu § 15 Abs. 5 S. 4 TMG a.F. *Schmitz* in: Spindler/Schmitz, § 14 TMG Rn. 44 ff., der davon ausging, dass § 15 Abs. 5 S. 4 TMG a.F. mit der e-privacy-Richtlinie nicht vereinbar war.

[310] S. auch *Ettig* in: Taeger/Gabel, § 21 TTDSG Rn. 10.

Verarbeitung von Nutzungsdaten zur Auskunftserteilung an Dritte trifft.[311] Für eine Anwendung von § 24 BDSG bleibt daneben kein Raum.

Die Auskunftserteilung an private Rechteinhaber durch Telemediendienste wäre deshalb nur zulässig, wenn die zweckändernde Weiterverarbeitung im Einklang mit Art. 6 Abs. 4 DS-GVO stünde. Die Anwendungsdienste speichern Nutzungsdaten meist im eigenen Interesse oder aus technischen Gründen. In der Regel ist deshalb der Zweck, zu dem die Daten ursprünglich erhoben wurden, nicht mit der Verarbeitung der Daten zur Auskunftserteilung an private Dritte vereinbar.

b) Telekommunikationsdienste

Ähnlich wie die §§ 22 und 24 TTDSG sehen die §§ 173, 174 und 177 TKG die Verarbeitung von Verkehrsdaten zur Auskunftserteilung an bestimmte staatliche Stellen vor. Eine Regelung für die Auskunftserteilung an Private existiert nicht. Vielmehr regelt § 9 Abs. 1 S. 3 TTDSG ausdrücklich, dass eine Verarbeitung von Verkehrsdaten, die über § 9 Abs. 1 S. 1 TTDSG – also über den Ausbau und die Aufrechterhaltung von Verbindungen, die Entgeltabrechnung oder den Aufbau weiterer Verbindungen – hinausgeht, unzulässig ist.

§ 9 TTDSG dient der Umsetzung der e-Privacy-Richtlinie und geht damit der DS-GVO vor.[312] Aufgrund der abschließenden bereichsspezifischen Regelung kommt auch eine Anwendung von § 24 BDSG nicht in Betracht. Damit dürfen Telekommunikationsdienste Verkehrsdaten nicht zur Auskunft an Private verarbeiten. Dadurch ist im Ergebnis die Auskunftserteilung über oder unter Verwendung von Verkehrsdaten bei Anwendungsdiensten, die Telekommunikationsdienste darstellen, nicht möglich.

5. Zwischenergebnis zur Verkehrs- und Nutzungsdatenauskunft

Die Möglichkeit der Auskunftserteilung über oder mittels Nutzungs- bzw. Verkehrsdaten unterscheidet sich – ähnlich wie bereits bei der Bestandsdatenauskunft – je nach Art des Anwendungsdienstes.

---

[311] Ähnlich *OLG Schleswig,* Beschl. v. 23.3.2022 – 9 Wx 23/21, GRUR-RS 2022, 5901 Rn. 31 f.

[312] S. bereits oben unter Kap. 5 § 3 A. I.

Öffentlich zugängliche Telekommunikationsdienste sind nach § 3 TTDSG zur Wahrung des Fernmeldegeheimnisses verpflichtet und dürfen Verkehrsdaten nur in sehr engen Grenzen erheben und speichern. Die Weitergabe oder Verwendung von Verkehrsdaten zur Auskunftserteilung an Private ist unzulässig.

Telemediendienste können Nutzungsdaten unter Wahrung der Vorgaben der Art. 5, 6 DS-GVO erheben und speichern. Die zweckändernde Weiterverarbeitung zur Erteilung der Auskunft an private Rechteinhaber wird aber regelmäßig nach Art. 6 Abs. 4 DS-GVO an der Inkompatibilität mit dem Zweck, zu dem die Daten ursprünglich erhoben wurden, scheitern.

IV. Identifizierung durch Zugangsanbieter anhand der IP-Adresse

Neben der Bestandsdatenauskunft der Anwendungsdienste stellt die Rückverfolgung der Nutzer anhand der IP-Adresse die wichtigste Möglichkeit der Identifizierung eines anonymen Internetnutzers dar. Dazu sind die Diensteanbieter auf die Auskünfte von Zugangsanbietern – wie Access-Providern, Betreiber von WLAN-Netzwerken und Anonymisierungsdiensten angewiesen. Sofern diese öffentlich zugängliche Dienste anbieten, handelt es sich bei den Zugangsanbietern um Telekommunikationsdienste im Sinne des § 3 Nr. 61 TKG.

Eine zentrale Rolle bei der Identifizierung eines Internetnutzers kommt den Access-Providern zu. Diese können die bei der Verletzungshandlung verwendete IP-Adresse einem bestimmten Anschlussinhaber zuordnen. Dafür ist es allerdings erforderlich, dass der jeweilige Access-Provider die notwendigen Verkehrs- und Bestandsdaten seiner Nutzer speichert und die Auskunftserteilung durch den Access-Provider mit den datenschutzrechtlichen Vorgaben in Einklang steht.

Sofern der rechtsverletzende Nutzer nicht mit dem Anschlussinhaber identisch ist oder zusätzliche Vorkehrungen zum Schutz seiner personenbezogenen Daten getroffen hat, kann darüber hinaus auch noch eine Auskunftserteilung durch den Anschlussinhaber oder durch Anonymisierungsdienste erforderlich werden.

1. Ermittlung der IP-Adresse

Um die IP-Adresse durch die Zugangsanbieter zurückverfolgen zu lassen, müssen die Rechteinhaber zunächst die bei der Rechtsverletzung verwendete IP-Adresse und die Zugriffszeiten des Nutzers ermitteln.

a) Ermittlung durch Auskunft der Anwendungsdienste

Eine Möglichkeit stellt dabei die Auskunftserteilung durch die Anbieter der genutzten Anwendungsdienste dar. Diese können gegebenenfalls Auskunft über die Nutzungs- oder Verkehrsdaten an die Rechteinhaber erteilen. Dies setzt jedoch voraus, dass der Diensteanbieter die IP-Adressen und Zugriffszeiten der Nutzer in den Log-Dateien speichert und diese an die Rechteinhaber weitergeben darf. Die Zulässigkeit einer solchen Datenverarbeitung durch die Anwendungsdienste wurde oben bereits untersucht.[313] Bei Telekommunikationsdiensten ist eine Auskunftserteilung über die Verkehrsdaten generell unzulässig, während es bei Telemediendiensten auf die Kompatibilität mit dem Zweck, zu dem die Daten ursprünglich erhoben wurden, ankommt.

b) Eigenständige Ermittlung der IP-Adresse durch die Rechteinhaber

Als Alternative zur Auskunftserteilung durch Telemediendiensteanbieter kann der Rechteinhaber unter bestimmten Voraussetzungen auch selbst die IP-Adresse des Rechtsverletzers ermitteln. Zum Beispiel kann die IP-Adresse des Absenders einer E-Mail dem Header der Mail entnommen werden.[314] In der Praxis besonders relevant ist der Einsatz einer Software durch Unternehmen, die im Auftrag von Urheberrechtsinhabern Filesharing-Netzwerke systematisch auf mögliche Rechtsverletzungen durchsuchen.[315] Wird eine rechtsverletzende Datei aufgespürt speichern diese Unternehmen die IP-Adressen der beteiligten Nutzer.[316]

Gegen ein solches Vorgehen bestehen allerdings ebenfalls datenschutzrechtliche Bedenken. Setzt man voraus, dass die Rechteinhaber über rechtliche

---

[313] S. oben unter Kap. 5 § 3 C.
[314] S. oben unter Kap. 4 § 3 D.
[315] *Welp*, Auskunftspflicht von Access-Providern, S. 19.
[316] *Welp*, Auskunftspflicht von Access-Providern, S. 19.

Möglichkeiten verfügen, durch Auskunftsansprüche gegen den Access-Provider oder zumindest im Rahmen eines Strafverfahrens die hinter einer IP-Adresse stehende Person identifizieren zu lassen, stellt die IP-Adresse für die Rechteinhaber ein personenbezogenes Datum dar.[317]

Die Erhebung der IP-Adresse und deren Weitergabe an die Access-Provider im Rahmen eines anschließenden Auskunftsersuchens ist daher an den Vorschriften der DS-GVO zu messen. Den Rechteinhabern kommt dabei zugute, dass die Durchsetzung ihrer zivilrechtlichen Ansprüche einen legitimen Zweck darstellt. Zudem weist die IP-Adresse für die Rechteinhaber selbst nur einen relativ geringen Personenbezug auf. Die Gefahr einer Identifizierung durch den Access-Provider besteht nämlich nur, sofern der Rechteinhaber eine Rechtsverletzung oder ein strafrechtlich relevantes Verhalten darlegen kann. Bei dynamischen IP-Adressen ist vorher wegen des Eingriffs ins Fernmeldegeheimnis zudem etwa nach § 101 Abs. 9 UrhG eine richterliche Anordnung erforderlich. Daher können die Rechteinhaber sich auf ein berechtigtes Interesse im Sinne des Art. 6 Abs. 1 S. 1 lit. f) DS-GVO berufen, sofern nicht im Einzelfall die Interessen der Nutzer überwiegen.[318]

Zu demselben Ergebnis kommt grundsätzlich auch der *EuGH*, der sich im Rahmen eines Vorabentscheidungsersuchens mit der Frage auseinandersetzte, ob die einer Auskunftserteilung durch den Access-Provider vorgelagerte Datenverarbeitung nach Art. 6 Abs. 1 S. 1 lit. f) DS-GVO zulässig ist.[319] In dem dieser Entscheidung zugrundeliegenden Sachverhalt sammelte das Unternehmen Media Protector im Auftrag der Rechteinhaberin Microm IP-Adressen von Nutzern eines Peer-to-Peer-Netzwerkes. Mircom erhob anschließend Klage gegen den Acess-Provider Telenet, der anhand der IP-Adressen Daten zur Identifizierung der Anschlussinhaber übermitteln sollte.

---

[317] Vgl. *EuGH,* Urt. v. 17.6.2021 – C-597/19, MMR 2022, 30 Rn. 104 – Mircom. S. zum Personenbezug bei Anbietern von Anwendungsdiensten oben unter Kap. 5 § 3 C. II.

[318] Vgl. *Generalanwalts Szpunar*, Schlussantrag vom 17.12.2020 – C-597/19, GRUR-RS 2020, 35419 Rn. 131 - Mircom; *EuGH,* Urt. v. 17.6.2021 – C-597/19, MMR 2022, 30 Rn. 111 – Mircom.

[319] *EuGH,* Urt. v. 17.6.2021 – C-597/19, MMR 2022, 30 Rn. 98 ff. – Mircom.

Bemerkenswert an der Entscheidung des *EuGH* ist aber vor allem, dass dieser neben der DS-GVO auch die e-privacy-Richtlinie herangezogen hat.[320] Interessant ist dies vor allem im Hinblick darauf, dass der *EuGH* die Rechtmäßigkeit der Speicherung von Nutzungsdaten wie IP-Adressen durch Webseiten-Betreiber in einer früheren Entscheidung ausschließlich anhand der damals geltenden Datenschutzrichtlinie bewertet hat.[321] Das ist auch insoweit nachvollziehbar, als vom persönlichen Anwendungsbereich der e-privacy-Richtlinie grundsätzlich lediglich elektronische Kommunikationsdienste erfasst sind. Bei dem Unternehmen Media Protector, das im Auftrag der Rechteinhaber die IP-Adressen der Nutzer gespeichert hat, handelt es sich aber ebenso wie bei einem Webseiten-Betreiber nicht um einen elektronischen Kommunikationsdienst.

Dennoch gelangt der *EuGH* bei seiner Entscheidung zur Datenverarbeitung durch Media Protector zu einer Anwendbarkeit der e-privacy-Richtlinie: Nach seiner Auffassung ergänzen und konkretisieren die Bestimmungen der e-Privacy-Richtlinie nach Art. 1 Abs. 2 e-privacy-Richtlinie i.V.m. Art. 94 Abs. 2 DS-GVO die DS-GVO zum Zwecke der Harmonisierung der Vorschriften der Mitgliedstaaten in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation.[322] Dadurch solle ein gleichwertiger Schutz der Grundrechte und Grundfreiheiten der Nutzer von elektronischen Kommunikationsdiensten in den Mitgliedstaaten sichergestellt werden.[323] Wenn die Zulässigkeit der Datenverarbeitung durch Media Protector anhand der DS-GVO beurteilt werden soll, sei deshalb vor allem zu untersuchen, ob die Verarbeitung im Einklang mit der e-privacy-Richtlinie steht.[324]

Unternehmen, die im Auftrag der Rechteinhaber IP-Adressen der Nutzer von P2P-Netzwerken verarbeiten, erlangen dadurch Zugriff auf Verkehrsdaten. Der EuGH stellt deshalb auf Art. 5 Abs. 1 e-privacy-Richtlinie ab. Demnach müssen die Mitgliedstaaten nach Art. 5 Abs. 1 e-privacy-Richtlinie das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von

---

[320] *EuGH,* Urt. v. 17.6.2021 – C-597/19, MMR 2022, 30 Rn. 113 ff. – Mircom.

[321] *EuGH*, Urt. v. 19.10.2016 – C-582/14, NJW 2016, 3579 - Breyer.

[322] *EuGH,* Urt. v. 17.6.2021 – C-597/19, MMR 2022, 30 Rn. 114 – Mircom. S. auch *EuGH*, NJW 2019, 655 Rn. 31.

[323] *EuGH,* Urt. v. 17.6.2021 – C-597/19, MMR 2022, 30 Rn. 114 – Mircom.

[324] *EuGH,* Urt. v. 17.6.2021 – C-597/19, MMR 2022, 30 Rn. 118 – Mircom.

Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer untersagen.[325]

Aus der Entscheidung des *EuGH* ist zu schließen, dass sich diese Verpflichtung nicht nur auf die Anbieter elektronischer Kommunikationsdienste bezieht, sondern auch auf Dritte – wie Media Protector -, die von außen auf Kommunikationsvorgänge einwirken. Das könnte auch die Unterschiede zur Entscheidung über die Speicherung von IP-Adressen durch Webseiten-Betreiber erklären. Anders als Media Protector ist der Webseiten-Betreiber Empfänger der Kommunikation mit dem Nutzer und erhält auf diese Weise die übermittelten Informationen über die Nutzungsdaten. Daher ist das „Abfangen" und Speichern von IP-Adressen durch von den Rechteinhabern beauftragte Unternehmen im Unterschied zu Anbietern von Webseiten nach Art. 5 Abs. 1 e-privay-Richtlinie zu messen.

Eine Ausnahme von der Verpflichtung des Art. 5 Abs. 1 e-privacy-Richtlinie leitet der *EuGH* aus Art. 15 Abs. 1 e-privacy-Richtlinie in Verbindung mit Art. 23 Abs. 1 DS-GVO, Art. 94 Abs. 2 DS-GVO ab.[326] Art. 23 Abs. 1 DS-GVO entspricht nach Ansicht des EuGH grundsätzlich Art. 13 Abs. 1 DSRL, auf den Art. 15 Abs. 1 e-privacy-Richtlinie verweist.[327] Art. 23 Abs. 1 lit. j) DS-GVO erlaubt es den Mitgliedstaaten dadurch, Rechtsvorschriften zu erlassen, die die Pflichten aus Art. 5 Abs. 1 e-privacy-Richtlinie zum Zwecke der Durchsetzung zivilrechtlicher Ansprüche beschränken. Die mitgliedstaatliche Regelung muss allerdings den Wesensgehalt der Grundrechte und Grundfreiheiten achten und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellen.[328]

Da die e-privacy-Richtlinie die DS-GVO konkretisiert, kann also nicht allein auf die Zulässigkeit der Datenverarbeitung nach Art. 5, 6 Abs. 1 lit. f) DS-GVO abgestellt werden. Vielmehr bedarf es einer Rechtsgrundlage im Sinne von Art. 15 Abs. 1 e-privacy-Richtlinie i.V.m. Art. 23 Abs. 1 lit. j) DS-GVO. Ob im nationalen Recht eine Rechtsgrundlage existiert, die den Anforderungen des Art. 23

---

[325] *EuGH,* Urt. v. 17.6.2021 – C-597/19, MMR 2022, 30 Rn. 115 – Mircom.
[326] *EuGH,* Urt. v. 17.6.2021 – C-597/19, MMR 2022, 30 Rn. 116 – Mircom.
[327] *EuGH,* Urt. v. 17.6.2021 – C-597/19, MMR 2022, 30 Rn. 116 – Mircom.
[328] *EuGH*, Urt. v. 17.6.2021 – C-597/19, MMR 2022, 30 Rn. 116 – Mircom.

DS-GVO genügt, konnte der *EuGH* in seiner Entscheidung nicht beurteilen, da das vorlegende belgische Gericht keine näheren Angaben zur Rechtsgrundlage gemacht hatte.[329] Der *EuGH* stellt aber klar, dass die Mitgliedstaaten die vorgelagerte Datenverarbeitung nach nationalem Recht im Lichte der e-privacy-Richtlinie zu überprüfen haben.[330]

Im deutschen Recht mangelt es an einer Vorschrift, die es dem Rechteinhaber oder einem beauftragten Unternehmen gestattet, im Vorfeld des Auskunftsersuchens Verkehrsdaten der Nutzer von P2P-Netzwerken zu verarbeiten. In Betracht kämen allenfalls die Auskunftsansprüche im Bereich des geistigen Eigentums, die zumindest dem Grunde nach einen Anspruch der Rechteinhaber gegen den Access-Provider auf Auskunft über Name und Adresse des Anschlussinhabers vorsehen. Diese Ansprüche dienen der Umsetzung der Enforcement-Richtlinie, die aber nach Art. 8 Abs. 3 lit. e) Enforcement-Richtlinie die Vorschriften zum Schutz personenbezogener Daten unberührt lässt.[331] Aus den nationalen Regelungen, die einen Anspruch auf Auskunft gegen Access-Provider vorsehen, ergibt sich deshalb nicht, dass auch die der Auskunftserteilung vorgelagerte Verarbeitung von Verkehrsdaten zulässig ist.

Werden dennoch im Auftrag der Rechteinhaber Verkehrsdaten gespeichert, um diese anschließend im Rahmen eines Auskunftsersuchens an den Access-Provider zu übermitteln, müsste eine solche Verarbeitung nach der Entscheidung des *EuGH* als unzulässig angesehen werden. In einem späteren Auskunfts- oder Gestattungsverfahren wäre deshalb die Verwertbarkeit der auf diese Weise ermittelten Daten fraglich.

Problematisch ist aber, dass der deutsche Gesetzgeber Art. 5 Abs. 1 e-privacy-Richtlinie nicht im Sinne der Auffassung des *EuGH* umgesetzt hat. Es existiert im nationalen Recht keine Vorschrift, die es Dritten verbietet, Verkehrsdaten von Nutzern elektronischer Kommunikationsmittel zu erheben und zu speichern. Die Regelungen zur Umsetzung der e-privacy-Richtlinie sehen lediglich Verpflichtungen oder Vorkehrungen der Anbieter von

---

[329] *EuGH,* Urt. v. 17.6.2021 – C-597/19, MMR 2022, 30 Rn. 119 – Mircom.

[330] *EuGH,* Urt. v. 17.6.2021 – C-597/19, MMR 2022, 30 Rn. 119 – Mircom.

[331] S. dazu auch *EuGH*, Urt. v. 29.1.2008 - C-275/06, GRUR 2008, 241 Rn. 57 – Promusicae.

Telekommunikationsdiensten vor oder verbieten das Abhören oder den Missbrauch von Funkanlagen. Diese Regelungen lassen auch keinen Spielraum für eine unionsrechtskonforme Auslegung im Sinne der Rechtsprechung des *EuGH* in der Sache Mircom. Daher muss von einer unzureichenden Umsetzung des Art. 5 Abs. 1 e-privacy-Richtlinie ausgegangen werden.

Durch die in dieser Hinsicht mangelnde Umsetzung von Art. 5 Abs. 1 e-privacy-Richtlinie gelangt man nach nationalem Recht aber überhaupt nicht zur Notwendigkeit einer Rechtsgrundlage im Sinne des Art. 15 Abs. 1 e-privacy-Richtlinie. Da anders als die Richtlinie die DS-GVO in den Mitgliedstaaten unmittelbar gilt, kann die der Auskunftserteilung durch den Access-Provider vorgelagerte Datenverarbeitung durch die Rechteinhaber (oder beauftragte Unternehmen) in Deutschland nur anhand der DS-GVO beurteilt werden.

Der deutsche Gesetzgeber sollte deshalb in zweierlei Hinsicht tätig werden: Zum einen gilt es, Art. 5 Abs. 1 e-privacy-Richtlinie entsprechend der Rechtsprechung des *EuGH* umzusetzen, beziehungsweise die nationalen Umsetzungsvorschriften anzupassen. Zum anderen sollte im Hinblick auf die Interessen der Rechteinhaber von der Möglichkeit Gebrauch gemacht werden, eine Rechtsgrundlage im Sinne des Art. 15 Abs. 1 e-privacy-Richtlinie für die vorgelagerte Verarbeitung von Verkehrsdaten durch die Rechteinhaber zu schaffen.

2. Auskunftserteilung durch den Access-Provider

Sofern die IP-Adresse vorab durch den Rechteinhaber ermittelt werden konnte, muss anschließend eine Auskunft beim Access-Provider über die Identität des hinter der IP-Adresse stehenden Anschlussinhabers eingeholt werden. Dieser kann die verwendete IP-Adresse gegebenenfalls einem seiner Nutzer zuordnen.

a) Speicherung der zur Identifizierung notwendigen Daten durch den Access-Provider

Dies setzt natürlich voraus, dass der Access-Provider die bei der jeweiligen Einwahl ins Internet vergebenen IP-Adressen, sowie Namen und Adressen der Nutzer speichert.

aa) Datenschutzrechtliche Einordnung der IP-Adresse

Um beurteilen zu können, ob und wie lange IP-Adressen durch den Access-Provider gespeichert werden dürfen, ist zunächst eine Einordnung der IP-Adresse unter Datenschutzgesichtspunkten erforderlich. Hierbei ist zwischen statischen und dynamischen IP-Adressen zu unterscheiden.

Eine statische IP-Adresse wird einem bestimmten Nutzer oder Rechner fest zugeordnet, sodass jede Einwahl ins Internet unter derselben IP-Adresse erfolgt. An private Nutzer werden dagegen in der Regel dynamische IP-Adressen vergeben. Das heißt, diesen Nutzern wird bei jeder Sitzung eine andere IP-Adresse zugewiesen.

Für den Access-Provider stellen sowohl statische als auch dynamische IP-Adressen personenbezogene Daten dar.[332] Bei der statischen IP-Adresse kann der Access-Provider durch die als Vertragsdaten gespeicherten Informationen den Nutzer ermitteln. Bei einer dynamischen IP-Adresse besteht der Personenbezug für den Access-Provider durch die Möglichkeit der Identifizierung eines Teilnehmers, an den die entsprechende IP-Adresse zum Zeitpunkt einer bestimmten Kommunikation vergeben wurde.

Dynamische IP-Adressen werden bei der Einwahl ins Internet erhoben. Es handelt sich dabei um Verkehrsdaten im Sinne von § 3 Nr. 70 TKG, die bei der Erbringung des Telekommunikationsdienstes erhoben werden.[333] Durch sie lassen sich Rückschlüsse auf nähere Umstände der Kommunikation ziehen.

Statische IP-Adressen dagegen werden bereits bei Vertragsschluss erhoben und haben als solche erstmal keinen Bezug zu einem konkreten Telekommunikationsvorgang. Sie stellen daher Bestandsdaten im Sinne von § 3 Nr. 6 TKG dar.

---

[332] S. *EuGH*, Urt. v. 24. 11. 2011 - C-70/10, GRUR 2012, 265, 268 – Scarlet/SABAM; *OLG Karlsruhe*, Urt. v. 4.12.2008 - 4 U 86/07, MMR 2009, 412, 412 ff.; *LG Frankenthal*, Beschl. v. 21.5.2008 - 6 O 156/08, MMR 2008, 687, 687 ff.; *Krüger/Maucher*, MMR 2011, 433, 436; *Sachs*, CR 2010, 547, 47; *Schmitz* in: Hoeren/Sieber/Holznagel, Teil 16.2 Rn 111.

[333] *EuGH,* Urt. v. 6.10.2020 – C-511/18 u.a., NJW 2021, 531 Rn. 152 – La Quadrature du Net; *BGH*, Beschl. v. 19.4.2012 - I ZB 80/11, MMR 2012, 689 Rn. 8 f. – Alles kann besser werden; *BGH,* Urt. v. 13.1.2011 - III ZR 146/10, MMR 2011, 341 Rn. 23.

bb) Zulässigkeit der Speicherung von Bestandsdaten

Nach dem Inkrafttreten der DS-GVO richtet sich die Zulässigkeit der Speicherung von Bestandsdaten durch Telekommunikationsanbieter nicht mehr nach § 95 TKG a.F., sondern – wie auch bei der Speicherung von Bestandsdaten im Bereich der Anwendungsdienste – in erster Linie nach den allgemeinen Regeln der Art. 5, 6 DS-GVO.[334] Bestandsdaten wie statischen IP-Adressen, Namen und Anschriften werden durch die Access-Provider insbesondere zur Erfüllung des Vertrages mit den Nutzern und zu Abrechnungszwecken gespeichert.

Außerdem sind die Access-Provider nach § 172 Abs. 1 TKG verpflichtet, für Auskunftsersuchen der Sicherheitsbehörden Bestandsdaten wie die vergebene Anschlusskennung (Nr. 2) und Name und Anschrift des Anschlussinhabers (Nr. 3) zu speichern.[335] Eine Verarbeitung im Sinne des § 172 TKG ist auf Grund der Öffnungsklausel in Art. 6 Abs. 2, 3 DS-GVO i.V.m. Art. 6 Abs. 1 S. 1 lit. c) DS-GVO auch zulässig.

cc) Zulässigkeit der Speicherung dynamischer IP-Adressen

Für die Auskunftserteilung mittels dynamischer IP-Adresse ist es erforderlich, dass der Access-Provider die IP-Adresse im Zusammenhang mit weiteren Verkehrsdaten wie des Datums oder der Uhrzeit der Verbindung speichert. Eine solche Speicherung der dynamischen IP-Adressen ist allerdings nur in sehr engen Grenzen zulässig. Insbesondere darf nach der Rechtsprechung zur Vorratsdatenspeicherung keine anlasslose Speicherung vorgenommen werden.[336] Im Übrigen richtet sich die Zulässigkeit der Speicherung von Verkehrsdaten im Unterschied zu den Bestandsdaten nach dem Telekommunikationsgesetz

---

[334] Zur Speicherung von Bestandsdaten im Bereich der Telemedien s. oben unter Kap. 5 § 3 B. II.

[335] S. zur Verfassungsmäßigkeit der Norm *Ferner* in: BeckOK StPO, § 172 TKG Rn. 4; S. zur Vorgängernorm des § 111 TKG a.F. *BVerfG*, Beschl. v. 24.1.2012 – 1 BvR 1299/05, NJW 2012, 1419 - Vorratsdatenspeicherung; *Löwenau/Ipsen* in: Scheuerle/Mayen, § 111 TKG Rn. 3 ff.; Eckhardt in: Beck´scher TKG-Kommentar, § 111 TKG Rn. 3 f.

[336] S. zur Vorratsdatenspeicherung *BVerfG*, Urt. v. 2.3.2010 - 1 BvR 256/08 u.a., NJW 2010, 833, 833 ff. – Vorratsdatenspeicherung.

beziehungsweise dem TTDSG, das in diesem Fall aufgrund von Art. 95 DS-GVO der DS-GVO vorgeht.[337]

Grundsätzlich ist die dynamische IP-Adresse nach § 9 Abs. 1 S. 2 TTDSG unverzüglich nach Beendigung der Verbindung zu löschen. Eine Speicherung über die Dauer des Kommunikationsvorgangs hinaus ist nach § 9 Abs. 1 S. 1 TTDSG nur zur Entgeltabrechnung oder zum Aufbau weiterer Verbindungen oder nach § 12 TTDSG zur Erkennung oder Beseitigung von Störungen zulässig.

Die Verarbeitung von Verkehrsdaten zur Entgeltabrechnung richtet sich nach § 10 TTDSG. Allerdings wird die Abrechnung der Verbindungen durch die Access-Provider häufig mittels Flatrates durchgeführt, sodass eine Speicherung der verwendeten Verkehrsdaten nicht erforderlich und daher in der Regel unzulässig ist.[338]

Access-Provider werden nach § 176 Abs. 3 TKG über die Vorschriften des TTDSG hinaus grundsätzlich verpflichtet, Verkehrsdaten wie IP-Adressen und Datum und Uhrzeit der Nutzer zum Zwecke der Auskunftserteilung an Behörden zur Strafverfolgung bei besonders schweren Straftaten oder zur Abwehr erheblicher Gefahren (S. § 177 TKG) auf Vorrat für zehn Wochen zu speichern. Die Regelung des § 176 Abs. 3 TKG geht auf § 113b TKG a.F. zurück, die der Gesetzgeber bei der Neuregelung des TKG weitgehend unverändert übernommen hat.[339] Sowohl der *EuGH*[340] als auch das *BVerfG*[341] haben in Entscheidungen zu Regelungen anderer Mitgliedstaaten beziehungsweise zur deutschen

---

[337] Ausführlicher oben unter Kap. 5 § 3 A. I.

[338] S. zur Löschungsverpflichtung bei Flatrate-Abrechnung *BGH*, Urt. v. 13.1.2011 - III ZR 146/10, MMR 2011, 343 Rn. 11 ff.; *LG Darmstadt*, Urt. v. 25.1.2006 - 25 S 118/05, GRUR-RR 2006, 173, 173 f.; *Breyer*, MMR 2011, 573, 574; *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 169 f.; *Spindler/Dorschel,* CR 2005, 38, 46; *Wehr/Ujica*, MMR 2010, 667, 668; *Welp*, Auskunftspflicht von Access-Providern, S. 293 ff.

[339] Unter Hinweis auf die damals laufenden Verfahren *Regierungsentwurf,* BT-Drs. 19/26108, S. 369 f.

[340] *EuGH*, Urt. v. 6.10.2020 – C-511/18 u.a., NJW 2021, 531, 531 ff. – La Quadrature du Net; S. auch *EuGH,* Urt. v. 21.12.2016 – C-203/15 u.a., NJW 2017, 717 – Tele2 Sverige.

[341] *BVerfG*, Urt. v. 2.3.2010 - 1 BvR 256/08 u.a., NJW 2010, 833, 833 ff. - Vorratsdatenspeicherung.

Vorgängerregelung strenge Anforderungen an die Vorratsdatenspeicherung gestellt.[342] Inzwischen hat der EuGH auf eine entsprechende Vorlage des BVerwG[343] auch die aktuelle deutsche Regelung zur Vorratsdatenspeicherung für unionsrechtswidrig erklärt.[344] Der Ausgang dieses Verfahrens ist aber ohnehin für diese Arbeit nicht von besonderer Bedeutung, da nach § 177 Abs. 2 TKG, die aufgrund von § 176 Abs. 3 TKG gespeicherten Daten nicht für andere als die in § 177 Abs. 1 TKG genannten Zwecke verwendet werden dürfen. Dementsprechend dürften die im Rahmen der Vorratsdatenspeicherung verarbeiteten Daten ohnehin nicht zur Auskunftserteilung an die Rechteinhaber genutzt werden.

Eine gesetzliche Regelung für die Speicherung von Verkehrsdaten zur Rechtsdurchsetzung im Individualinteresse existiert nicht. Für einen Auskunftsanspruch kann daher lediglich auf die Daten zurückgegriffen werden, die innerhalb der sehr engen Grenzen der §§ 9 ff. TTDSG gespeichert werden durften. In vielen Fällen werden Auskunftsansprüche daher bereits deshalb ins Leere laufen, weil die zur Identifizierung notwendigen Verkehrsdaten zum Zeitpunkt des Auskunftsbegehrens bereits nicht mehr vorhanden sind.

In der urheberrechtlichen Rechtsprechungspraxis wurde versucht dem entgegenzuwirken, indem aus § 101 Abs. 9 UrhG eine Pflicht des Access-Providers zur Speicherung der Daten „auf Zuruf" angenommen wurde.[345] Entsprechend

---

[342] Aus diesem Grund wurden die Regelung vorläufig außer Vollzug gesetzt, S. *OVG Münster*, Beschl. v. 22.6.2017 – 13 B 238/17, NVwZ-RR 2018, 43, 43 ff. S. zum derzeitigen Verzicht auf die Verhängung von Bußgeldern an Telekommunikationsdienste, die Verkehrsdaten nicht auf Vorrat speichern *Gola/Klug,* NJW 2017, 2593, 2594.

[343] *BVerwG,* Beschl. v. 25.9.2019 – 6 C 12/18, NVwZ 2020, 1108, 1108 ff. Zuvor hatte das VG Köln § 113b TKG a.F. für unionsrechtswidrig erklärt, S. *VG Köln*, Urt. v. 20.04.2018 - 9 K 7417/17, BeckRS 2018, 10123.

[344] *EuGH,* Urt. v. 20.09.2022 - Az. C-793/19, NJW 2022, 3135, 3135 ff.

[345] S. etwa *OLG Köln*, Beschl. v. 21.10.2008 - 6 Wx 2/08, MMR 2008, 820, 820; *OLG Hamburg*, Urt. v. 17.2.2010 - 5 U 60/09, MMR 2010, 338, 338; *OLG Karlsruhe*, Beschl. v. 1.9.2009 - 6 W 47/09, CR 2009, 806, 807; *OLG Frankfurt*, Beschl. v. 12.5.2009 - 11 W 21/09, MMR 2009, 542, 542; *LG Hamburg*, Urt. v. 11.3.2009 - 308 O 75/09, MMR 2009, 570, 571. Ablehnend aber *OLG Frankfurt a.M.*, Beschl. v. 17. 11. 2009 - 11 W 54/09, GRUR-RR 2010, 91 – Speicherung auf Zuruf; *OLG Frankfurt a.M.,* Beschl. v. 17. 11.2009 – 11 W 53/09 u.a., ZUM-RD 2010, 133, 134 f.; *OLG Frankfurt a.M.,* Beschl. v. 12.11.2009 - 11 W 41/09, MMR 2010, 62.

soll der Rechteinhaber den Access-Provider bei offensichtlichen Rechtsverletzungen dazu verpflichten können, die Löschung der zur Auskunftserteilung notwendigen Verkehrsdaten zu unterlassen.[346] Demnach würde sich aus dem Anspruch aus § 101 UrhG nicht nur eine Pflicht zur Auskunftserteilung ergeben, sondern auch eine Pflicht zur Unterlassung der Löschung der zur Erteilung der Auskunft erforderlichen Daten.

Die Herleitung eines solchen Anspruchs aus dem Auskunftsanspruch oder auch aus dem Grundsatz von Treu und Glauben ist zu kritisieren. Allein aus der Tatsache, dass ein Auskunftsanspruch besteht, lässt sich nicht ableiten, dass alle zur Auskunftserteilung notwendigen Daten vorgehalten werden dürfen. Vielmehr bedarf es hierfür einer datenschutzrechtlichen Erlaubnisnorm. Dies gilt insbesondere bei der Auskunftserteilung mittels dynamischer IP-Adresse, da hierbei Verkehrsdaten betroffen sind, bei deren Speicherung das Fernmeldegeheimnis aus Art. 10 GG berührt sein kann.[347]

Das Fehlen einer datenschutzrechtlichen Ermächtigungsnorm zur Speicherung der Verkehrsdaten zur Durchsetzung zivilrechtlicher Ansprüche, kann daher nicht umgangen werden. Für den urheberrechtlichen Auskunftsanspruch ergibt sich dies zudem auch aus § 101 Abs. 9 S. 8 UrhG, der die Vorschriften zum Schutz personenbezogener Daten ausdrücklich unberührt lässt. Vielmehr obliegt es dem Gesetzgeber, die widerstreitenden Interessen zu einem angemessenen Ausgleich zu bringen.[348]

Mit ähnlichen Bedenken muss daher auch der Rechtssprechungspraxis begegnet werden, die im Rahmen des Anordnungsverfahrens nach § 101 Abs. 9 UrhG eine Sicherung der für die Auskunftserteilung benötigten Verkehrsdaten mittels einer einstweiligen Anordnung nach § 49 FamFG ermöglicht.[349] Auch durch ein

---

[346] *LG Hamburg*, Urt. v. 11.3.2009 - 308 O 75/09, MMR 2009, 570, 571.

[347] *BVerfG,* Beschl. v. 13.11.2010 – 2 BvR 1124/10, ZUM-RD 2011, 396 Rn. 11 ff.- Verpflichtung zur Auskunft über IP-Adresse; *BVerfG,* MMR 2007, 308; *BGH,* Urt. v. 13.1.2011 - III ZR 146/10, MMR 2011, 344 Rn. 27.

[348] So auch *OLG Hamm*, Beschl. v. 2.11.2010 - I-4 W 119/10, MMR 2011, 193, 193 ff.; *Wimmers* in: Schricker/Loewenheim, § 101 Rn. 113.

[349] *OLG Köln,* Beschl. v. 21.1.2013 - 2 Wx 380/12, MMR 2013, 257, 257 ff.; OLG Nürnberg, Beschl. v. 3.6.2009 - 3 W 471/09, BeckRS 2009, 26651.

solches prozessuales Vorgehen darf nicht umgangen werden, dass in materiellrechtlicher Hinsicht keine Ermächtigungsgrundlage für die Speicherung von Verkehrsdaten zur Auskunftserteilung zum Zweck der individuellen Rechtsdurchsetzung besteht.[350]

Auch der *BGH* hat die Gefahr erkannt, dass die Auskunftsansprüche (im Bereich des geistigen Eigentums) ins Leere laufen könnten.[351] Darin sah er einen Widerspruch zum Zweck des Anspruchs aus § 101 Abs. 2, 9 UrhG.[352] Deswegen leitete er eine Pflicht der Access-Provider zur Speicherung der zur Auskunft erforderlichen Verkehrsdaten aus § 101 Abs. 2, 9 UrhG i.V.m. § 96 Abs. 1 S. 1 TKG a.F. ab.[353] Nach § 96 Abs. 1 S. 1 TKG a.F. durften die Diensteanbieter Verkehrsdaten für bestimmte im TKG geregelte Zwecke verarbeiten. Dieser Verweis erstreckte sich nach der Ansicht des *BGH* auch auf § 96 Abs. 2 TKG a.F.[354] § 96 Abs. 1 S. 2 TKG a.F. sah vor, dass die von den Diensteanbietern gespeicherten Daten nur für diese oder durch andere gesetzliche Vorschriften begründete Zwecke verwendet werden dürfen. Der *BGH* sah 101 Abs. 2, 9 UrhG als eine gesetzliche Vorschrift im Sinne des § 96 Abs. 1 S. 2 TKG a.F. an.[355] Entsprechend wären die Telekommunikationsdienste zur Speicherung von Verkehrsdaten zur Auskunftserteilung nach § 96 Abs. 1 S. 1 TKG a.F. verpflichtet.

Schon nach alter Rechtslage konnte zurecht bezweifelt werden, dass sich die weite Auslegung des § 96 Abs. 1 S. 1 TKG a.F. durch den *BGH* mit dem Telos dieser Norm in Einklang bringen lässt.[356] Nach der derzeitigen Rechtslage ist

---

[350] *Wimmers* in: Schricker/Loewenheim, § 101 Rn. 113.

[351] *BGH*, Urt. v. 21.9.2017 – I ZR 58/16, GRUR 2017, 1236 Rn. 30 – Sicherung der Drittauskunft.

[352] *BGH*, Urt. v. 21.9.2017 – I ZR 58/16, GRUR 2017, 1236 Rn. 58 ff. – Sicherung der Drittauskunft.

[353] *BGH*, Urt. v. 21.9.2017 – I ZR 58/16, GRUR 2017, 1236 Rn. 55 – Sicherung der Drittauskunft.

[354] *BGH*, Urt. v. 21.9.2017 – I ZR 58/16, GRUR 2017, 1236 Rn. 57, 62 – Sicherung der Drittauskunft.

[355] *BGH*, Urt. v. 21.9.2017 – I ZR 58/16, GRUR 2017, 1236 Rn. 57, 62 – Sicherung der Drittauskunft.

[356] Kritisch etwa *Grünberger,* ZUM 2018, 321, 332 f.; *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 165; *Hoffmann*, NJW 2009, 2649, 2653; *Kramer,* Zivilrechtlicher

diese Rechtsprechung aber ohnehin nicht mehr tragfähig, da die für die Entscheidung des *BGH* maßgebliche Vorschrift des § 96 TKG a.F. nicht mehr existiert. Mit § 9 TDSG besteht zwar eine Vorschrift, die in ihrem Regelungsgehalt im Wesentlichen dem § 96 TKG a.F. entspricht. Allerdings stellt § 9 TTDSG im Unterschied zu § 96 Abs. 1 S. 1 TKG a.F. ausdrücklich klar, dass die Diensteanbieter Verkehrsdaten nur verarbeiten dürfen, soweit dies zum Aufbau und zur Aufrechterhaltung der Telekommunikation, zur Entgeltabrechnung oder zum Aufbau weiterer Verbindungen erforderlich ist. Zudem ist die Vorschrift des § 96 Abs. 1 S. 2 TKG a.F. ersatzlos gestrichen worden. Die gesetzliche Grundlage für die Argumentation des *BGH* ist dadurch weggefallen.

Für die Beurteilung der Zulässigkeit der Speicherung von dynamischen IP-Adressen sind demnach allein die Vorschriften der §§ 9 ff. TTDSG maßgeblich. Für die Auskunftserteilung kann daher nur auf die Verkehrsdaten zurückgegriffen werden, die im Rahmen dieser Regelungen gespeichert werden dürfen.

Während sich die Speicherung statischer IP-Adressen im Verhältnis als relativ unproblematisch erweist, dürfen dynamische IP-Adressen durch die Access-Provider nur sehr begrenzt und insbesondere nicht zu dem Zweck einer Auskunftserteilung an Privatpersonen vorgehalten werden. Viele Auskunftsbegehren gegenüber Access-Providern werden daher bereits daran scheitern, dass die zur Identifizierung notwendigen Daten nicht mehr vorhanden sind. Dies kann dazu führen, dass selbst bei Bestehen einer Anspruchsgrundlage eine Auskunftserteilung aus tatsächlichen Gründen unmöglich und der Anspruch daher nicht durchsetzbar ist.

b) Zulässigkeit der Auskunftserteilung durch den Access-Provider

Zur Identifizierung der Rechtsverletzer muss der Access-Provider Name und Adresse des Anschlussinhabers ermitteln und an den Rechteinhaber weitergeben dürfen. Zur Beurteilung der Zulässigkeit einer solchen Auskunftserteilung ist erneut zwischen statischen und dynamischen IP-Adressen zu unterscheiden.

Auskunftsanspruch, S. 185 f.; *Spindler* in: Spindler/Schuster, § 101 UrhG Rn. 24; *Welp,* Auskunftspflicht von Access-Providern, S. 265 ff.

aa) Dynamische IP-Adressen

Um Name und Adresse eines Anschlussinhabers bei dynamischen IP-Adressen ermitteln zu können, muss der Access-Provider prüfen, welchem Anschluss die jeweilige IP-Adresse zum relevanten Zeitpunkt zugeordnet wurde. Die Auskunftserteilung kann daher nur unter Verwendung von Verkehrsdaten wie Datum und Uhrzeit der konkreten Verbindung erfolgen.[357] Die Verwendung von Verkehrsdaten durch Anbieter von Telekommunikationsdiensten unterfällt dem Anwendungsbereich der e-Privacy-Richtlinie und richtet sich daher nach den nationalen Vorschriften, die der Ausführung dieser Richtlinie dienen. Die DS-GVO kommt in diesem Bereich nicht zur Anwendung.[358]

Teilweise wurde vertreten, ein solches Vorgehen stehe generell im Widerspruch zur e-Privacy-Richtlinie, die eine Verwendung von Verkehrsdaten zur Auskunftserteilung an Dritte durch Diensteanbieter, die unter den Anwendungsbereich besagter Richtlinie fallen, nicht vorsehe.[359] Die Bestimmungen des Art. 6 e-privacy-Richtlinie zu den Verkehrsdaten seien als abschließend zu betrachten.[360] Die e-Privacy-Richtlinie stünde damit einer Identifizierung der Rechtsverletzer mittels IP-Adresse zum Zweck der Wahrnehmung berechtigter Interessen generell entgegen. Die einzelnen Mitgliedstaaten könnten dementsprechend keine Regelungen zur Identifikation eines Nutzers anhand seiner IP-Adresse treffen.[361]

---

[357] S. etwa *EuGH*, Urt. v. 17.6.2021 – C-597/19, MMR 2020, 30 Rn. 123 – Mircom; *BGH*, Beschl. v. 5.12.2012 – I ZB 48/12, GRUR 2013, 536 Rn. 37 – Die Heiligtümer des Todes; *BGH*, Beschl. v. 19.4.2012 - I ZB 80/11, MMR 2012, 689 Rn. 37 ff. - Alles kann besser werden; *OLG Hamburg*, Urt. v. 17.2.2010 - 5 U 60/09, BeckRS 2010, 8656 - Datenverwendung; *OLG Oldenburg*, Beschl. v. 1.12.2008 - 1 W 76/08, MMR 2009, 188, 189; *OLG Zweibrücken*, Beschl. v. 27.10.2008 – 3 W 184/08, ZUM-RD 2008, 605, 606; *OLG Köln*, Beschl. v. 21.10.2008 - 6 Wx 2/08, MMR 2008, 820, 820; *LG Frankfurt*, Beschl. v. 18.9.2008 - 2-06 O 534/08, MMR 2008, 829, 830; *Härting,* ITRB 2009, 35, 38; *Jüngel/Geißler*, MMR 2008, 787, 791 f.; *Kitz*, NJW 2008, 2374, 2375 f.; *Kitz*, ZUM 2006, 444, 448; *Kuper,* ITRB 2009, 12, 14; *Maaßen*, MMR 2009, 511, 513; *Spindler*, ZUM 2008, 640, 645; *Spindler/Dorschel,* CR 2006, 341, 435; *Welp*, Auskunftspflicht von Access-Providern, S. 237 ff.

[358] S. oben unter Kap. 5 § 3 A. I.

[359] *Spindler*, ZUM 2008, 640, 645; *Spindler/Dorschel*, CR 2006, 341, 345 f.

[360] *Spindler/Dorschel*, CR 2006, 341, 346.

[361] So ausdrücklich *Spindler/Dorschel*, CR 2006, 341, 346.

Der *EuGH* hat aber im Rahmen eines Vorabentscheidungsersuchens entschieden, dass die Regelungen der e-Privacy-Richtline die Möglichkeit der Mitgliedstaaten nicht ausschließen, eine Pflicht zur Weitergabe personenbezogener Daten im Rahmen eines zivilrechtlichen Verfahrens vorzusehen.[362] Dabei stützt er sich auf Art. 15 Abs. 1 e-Privacy-Richtlinie. Demnach können die Mitgliedstaaten die Pflicht zur Wahrung der Vertraulichkeit der Verkehrsdaten durch eigene Rechtsvorschriften beschränken, wenn diese gemäß Art. 13 Abs. 1 DSRL notwendig, angemessen und verhältnismäßig sind.[363] Der *EuGH* räumt damit den einzelnen Mitgliedstaaten einen relativ großen Spielraum für eigene Regelungen ein. Dies ist zu begrüßen, da hierdurch die Einführung vielschichtiger nationaler Vorschriften ermöglicht wird, die im Einzelfall die widerstreitenden Interessen besser zu einem verhältnismäßigen Ausgleich bringen können.

Diese Rechtsprechung ist auch auf die Situation nach dem Inkrafttreten der DS-GVO übertragbar und wurde inzwischen vom *EuGH* in einer weiteren Entscheidung bestätigt.[364] Die DSRL wurde nach Art. 94 Abs. 1 DS-GVO mittlerweile abgelöst. Der Verweis auf Art. 13 Abs. 1 DSRL gilt nach Art. 94 Abs. 2 DS-GVO als Verweis auf die DS-GVO. Art. 6 Abs. 4, 23 Abs. 1 DS-GVO entsprechen nach ihrem Regelungsgehalt der Vorschrift des Art. 13 Abs. 1 DSRL, indem sie den Mitgliedstaaten ähnliche Befugnisse zur Einführung abweichender nationaler Regelungen zugestehen.[365] Der Verweis auf Art. 13 Abs. 1 DSRL wirkt daher als Verweis auf Art. 6 Abs. 4, 23 Abs. 1 DS-GVO. Nach Art. 23 Abs. 1 lit. j) DS-GVO stellt die Durchsetzung zivilrechtlicher Ansprüche einen Zweck dar, auf den durch Art. Art. 15 Abs. 1 e-privacy-Richtlinie Bezug genommen wird.[366]

Die Mitgliedstaaten können daher entsprechend der Rechtsprechung des *EuGH* Regelungen treffen, die eine Verwendung von Verkehrsdaten zur Auskunftserteilung zum Zweck der Durchsetzung zivilrechtlicher Ansprüche

---

[362] *EuGH*, Urt. v. 29.1.2008 - C-275/06, GRUR 2008, 241 Rn. 54 – Promusicae; *EuGH,* Beschl. v. 19.2.2009 - Rs. C-557/07, MMR 2009, 242 Rn. 28; Dies kritisierend *Spindler*, GRUR 2008, 574, 575.

[363] *EuGH*, Urt. v. 29.1.2008 - C-275/06, GRUR 2008, 241 Rn. 49– Promusicae.

[364] *EuGH,* Urt. v. 17.6.2021 – C-597/19, MMR 2022, 30 Rn. 125, 132 – Mircom.

[365] *EuGH,* Urt. v. 17.6.2021 – C-597/19, MMR 2022, 30 Rn. 116 – Mircom.

[366] *EuGH,* Urt. v. 17.6.2021 – C-597/19, MMR 2022, 30 Rn. 117 – Mircom.

vorsehen. Die e-privacy-Richtlinie steht einer Identifizierung der Rechtsverletzer mittels IP-Adresse also nicht grundsätzlich entgegen.

Allerdings ergibt sich aus der Richtlinie auch keine Pflicht der Mitgliedstaaten zur Einführung einer solchen gesetzlichen Ermächtigung.[367] Es ist daher zu untersuchen, ob im deutschen Recht eine Regelung im Sinne des Art. 15 Abs. 1 e-privacy-Richtlinie existiert.[368]

Da bei der Verwendung von Verkehrsdaten zur Auskunftserteilung das Fernmeldegeheimnis berührt wird, müsste eine solche Vorschrift zum einen das Zitiergebot nach § 19 Abs. 1 S. 2 GG beachten. Zum anderen müsste sich die Norm nach § 3 Abs. 3 S. 3 TTDSG ausdrücklich auf Telekommunikationsvorgänge beziehen.[369]

Im Bereich des Urheberrechts geht der *BGH* wohl davon aus, dass sich aus dem Auskunftsanspruch gegen Internetdiensteanbieter aus § 101 Abs. 2, 9 UrhG eine solche Erlaubnis ergibt.[370] Hierfür spräche, dass nach der Gesetzesbegründung die Auskunftserteilung durch den Access-Provider bei Urheberrechtsverletzungen im Internet ein Ziel der Einführung von § 101 UrhG n.F. war.[371] Unter Bezugnahme hierauf könnte man erwägen, § 101 Abs. 9 UrhG als Vorschrift anzusehen, die sich ausdrücklich auf einen Telekommunikationsvorgang bezieht. Zudem wären durch § 101 Abs. 10 UrhG auch die Vorgaben des Zitiergebots gewahrt.

---

[367] *EuGH,* Urt. v. 17.6.2021 – C-597/19, MMR 2022, 30 Rn. 125 – Mircom; *EuGH*, Urt. v. 29.1.2008 - C-275/06, GRUR 2008, 241 Rn. 55 – Promusicae; *EuGH,* Urt. v. 19.4.2012 - C-461/10, MMR 2012, 471 Rn. 55 – Bonnier Audio.

[368] *EuGH,* Urt. v. 17.6.2021 – C-597/19*,* MMR 2022, 30 Rn. 127, 132 – Mircom.

[369] Da immer die Möglichkeit besteht, dass IP-Adressen bei der konkreten Einwahl ins Internet für Individualkommunikation genutzt wurden, ist das Fernmeldegeheimnis zu beachten.

[370] *BGH*, Urt. v. 21.9.2017 – I ZR 58/16, GRUR 2017, 1236 Rn. 62 – Sicherung der Drittauskunft; *BGH*, Beschl. v. 19.4.2012 - I ZB 80/11, MMR 2012, 689 Rn. 42 ff. - Alles kann besser werden; *OLG Frankfurt a.M.,* Beschl. v. 12.5.2009 - 11 W 21/09, MMR 2009, 542, 543; *OLG Karlsruhe*, Beschl. v. 1.9.2009 - 6 W 47/09, CR 2009, 806, 806; *OLG Köln*, Beschl. v. 21.10.2008 - 6 Wx 2/08, CR 2009, 107, 108 – Ganz anders; *Czychowski/Nordemann*, NJW 2008, 3095, 3097; *Heymann,* CR 2008, 568, 571; *Maaßen*, MMR 2009, 511, 513.

[371] S. *Regierungsentwurf*, BT-Drs. 16/5048, 39.

Dennoch eignet sich § 101 UrhG nicht als Ermächtigungsgrundlage für die Datenweitergabe.[372] Zum einen ist die Vorschrift zu unbestimmt, um eine gesetzliche Erlaubnis zur Verarbeitung von Verkehrsdaten darstellen zu können, da keine Regelung darüber getroffen wird, welche Daten zur Auskunftserteilung erhoben, verwendet und ausgewertet werden dürfen.[373] Zum anderen beinhaltet der materiell-rechtliche Auskunftsanspruch nicht automatisch auch eine Erlaubnisnorm zur Weitergabe von Verkehrsdaten. So führt *Kitz* zutreffenderweise aus, dass durch einen Anspruch auf Errichtung eines Werks aus § 631 Abs. 1 BGB auch nicht eine Baugenehmigung ersetzt werden kann.[374] Dementsprechend kann auch aus einem Auskunftsanspruch nicht automatisch auf das Vorliegen einer Erlaubnis zur Datenweitergabe geschlossen werden. Vielmehr bedarf es hierfür einer ausdrücklichen Regelung, die sich im Hinblick auf die festgestellte Unbestimmtheit nicht aus § 101 UrhG ergeben kann.

So wurde im Bereich der Telemedien für die Weitergabe von Bestandsdaten in § 21 TTDSG eine entsprechende ausdrückliche Erlaubnisnorm geschaffen.[375] Eine solche hätte erst recht für die Auskunftserteilung mittels Verkehrsdaten eingeführt werden müssen. Außerdem unterscheidet auch § 21 Abs. 2 TTDSG deutlich zwischen der datenschutzrechtlichen Erlaubnis (S. 1) und der Grundlage für den Auskunftsanspruch (S. 2). Eine solche Differenzierung nimmt § 101 UrhG nicht vor.

Zudem sprechen auch die wortgleichen Parallelvorschriften in § 140b PatG, § 24b GebrMG, § 19 MarkenG, § 46 DesignG, § 37b SortenSchuG und § 9 Abs. 2 HalblSchG dagegen, § 101 UrhG eine gesetzliche Ermächtigung für die Auskunftserteilung zu entnehmen. Mit Ausnahme von § 19 MarkenG existiert in der Praxis bei diesen Regelungen kein nennenswerter Anwendungsbereich im Zusammenanhang mit der Verfolgung von anonymen Rechtsverletzungen im

---

[372] So auch *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 164; *Kitz,* NJW 2008, 2374, 2375 f.; *Spindler/Dorschel*, CR 2006, 341, 343; *Spindler,* ZUM 2008, 640, 645; *Welp*, Auskunftspflicht von Access-Providern, S. 269 ff.

[373] *Welp*, Auskunftspflicht von Access-Providern, S. 269 ff.

[374] *Kitz,* ZUM 2006, 444, 448.

[375] *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 164; *Kitz,* NJW 2008, 2374, 2375 f.; *Mantz*, K&R 2009, 21, 22; *Moos*, K&R 2009, 154, 158; *Nägele/Nietsch*, WRP 2007, 1047, 1051; *Spindler*, ZUM 2008, 640, 645; *Spindler/Dorschel*, CR 2006, 341, 343; *Welp*, Auskunftspflicht von Access-Providern, S. 263 ff.

Internet. Daher handelt es sich hierbei nicht um Vorschriften, die sich ausdrücklich auf einen Telekommunikationsvorgang beziehen. Es würde zu weit gehen, aus diesen Vorschriften eine gesetzliche Erlaubnis zur Datenverarbeitung durch den Access-Provider abzuleiten. Es überzeugt nicht, diese Vorschriften bei identischem Wortlaut anders auszulegen als § 101 UrhG.

In der Rechtsprechung wurde zudem ergänzend zu § 101 UrhG mehrfach § 96 Abs. 1 S. 2 TKG a.F. als Erlaubnisnorm für die Auskunftserteilung durch den Access-Provider herangezogen.[376] Diese Vorschrift ist im Zuge der Neuregelung des TKG aber weggefallen, sodass sie nach der heutigen Rechtslage nicht mehr als Rechtsgrundlage für die Verarbeitung von Verkehrsdaten in Betracht kommt.[377]

Auch § 101 UrhG kann daher nicht als Erlaubnisnorm für die Auskunftserteilung herangezogen werden. Der Vollständigkeit halber bleibt zu erwähnen, dass Ansprüche aus § 242 BGB und § 21 Abs. 2 S. 2 TTDSG natürlich erst recht keine solche Erlaubnis enthalten, da sie ohnehin keine Auskunftserteilung durch den Access-Provider vorsehen.

Es fehlt daher für alle untersuchten Auskunftsansprüche an einer Norm, die es dem Access-Provider gestattet, bei dynamischen IP-Adressen Name und Adresse eines Anschlussinhabers zu ermitteln und an den Rechteinhaber weiterzugeben. Eine Auskunftserteilung an die Rechteinhaber mittels dynamischer IP-Adresse ist für den Access-Provider daher rechtlich nicht zulässig. Die entsprechenden Auskunftsbegehren der Rechteinhaber drohen an dieser Stelle zu scheitern.

Die bisherige abweichende Rechtsprechungspraxis insbesondere in den Filesharing-Fällen beruht auf einer zu weiten Auslegung des § 101 UrhG als Ermächtigungsgrundlage. Zudem wird einer Argumentation auf Basis des § 96 Abs. 1 S. 2 TKG a.F. nunmehr durch den Wegfall dieser Vorschrift die Grundlage entzogen. An dieser Stelle besteht daher trotz der bisher abweichenden

---

[376] *BGH*, Urt. v. 21.9.2017 – I ZR 58/16, GRUR 2017, 1236 Rn. 62 – Sicherung der Drittauskunft; *OLG Hamburg*, Urt. v. 17.2.2010 - 5 U 60/09, MMR 2010, 338, 338; S. auch *LG Hamburg*, Urt. v. 11.3.2009 - 308 O 75/09, MMR 2009, 570, 572.

[377] S. bereits oben unter Kap. 5 § 3 D. II. 1. c).

Rechtsprechung Handlungsbedarf für den Gesetzgeber, eine Grundlage für die Erlaubnis der Datenverarbeitung zur Auskunftserteilung zu schaffen.

bb) Statische IP-Adressen

Bei statischen IP-Adressen muss im Unterschied zu dynamischen IP-Adressen zur Auskunftserteilung lediglich ein Abgleich mit den bei Vertragsschluss gespeicherten Bestandsdaten vorgenommen werden. Die überwiegende Ansicht geht daher wohl davon aus, dass die Auskunftserteilung in diesem Fall lediglich unter Verwendung von Bestandsdaten erfolgt und somit das Fernmeldegeheimnis nicht berührt wird.[378]

Zum Teil wird dagegen angenommen, dass im Zusammenhang mit der Auskunftserteilung durch den Access-Provider statische IP-Adressen als Verkehrsdaten anzusehen seien.[379] Demnach handele es sich bei statischen IP-Adressen, die zur Ausgestaltung des Vertragsverhältnisses erhoben werden, zwar grundsätzlich um Bestandsdaten, allerdings komme diesen ein erweiterter Aussagegehalt zu, wenn sie bei der Einwahl ins Internet vergeben werden.[380] Im Zusammenhang mit einem speziellen Kommunikationsvorgang handele es sich daher bei statischen IP-Adressen um Verkehrsdaten.[381] Bei der Auskunftserteilung durch den Access-Provider bestehe ein Bezug zur konkreten Aktivität des Nutzers, bei der es zur Rechtsverletzung kam, sodass hierbei ein Eingriff in das Fernmeldegeheimnis vorliege.[382]

---

[378] *BVerfG*, Beschl. v. 24.1.2012 - 1 BvR 1299/05, MMR 2012, 410 Rn. 133 ff.; *LG München I*, Beschl. v. 24.5.2011 - 21 O 9065/11, GRUR-RR 2012, 71, 71; *LG Braunschweig*, Urt. v. 30.11.2016 – 9 S 393/15 (24), ZUM 2017, 434, 437; *Abdallah/Gercke*, ZUM 2005, 368, 374; *Dreier* in: Dreier/Schulze, § 101 UrhG Rn. 35; *Freund/Schnabel*, MMR 2011, 495, 499; *Gnirck/Lichtenberg*, DuD 2004, 598, 600; *Schramm*, DuD 2006, 785, 786; *Wehr/Ujica*, MMR 2010, 667, 668.

[379] *Brüggemann,* Drittauskunftsanspruch, S. 185 ff.; *Meyerdierks,* MMR 2013, 705; *Welp*, Auskunftspflicht von Access-Providern, S. 249 ff.

[380] *Welp*, Auskunftspflicht von Access-Providern, S. 250 f.

[381] *Brüggemann,* Drittauskunftsanspruch, S. 187; *Welp*, Auskunftspflicht von Access-Providern, S. 251.

[382] *Brüggemann,* Drittauskunftsanspruch, S. 187; *Welp*, Auskunftspflicht von Access-Providern, S. 250 ff. A.A. *BVerfG,* Beschl. v. 24.1.2012 - 1 BvR 1299/05, MMR 2012, 410 Rn. 133 ff.

Von der Lösung dieser Streitfrage hängt der Beurteilungsmaßstab für die Zulässigkeit der Auskunftserteilung ab. Geht man von einer Verwendung von Verkehrsdaten aus, würde die Auskunftserteilung auch bei einer statischen IP-Adresse unter den Anwendungsbereich der e-Privacy-Richtlinie fallen. Anderenfalls richtet sich die Zulässigkeit in erster Linie nach der DS-GVO. Zudem würde es bei einem Eingriff ins Fernmeldegeheimnis einer Norm bedürfen, die sich nach § 3 Abs. 3 S. 3 TTDSG speziell auf Telekommunikationsdienste bezieht und den Vorgaben des Zitiergebots aus Art. 19 Abs. 1 S. 2 GG genügt.

Richtigerweise ist allerdings bei der Auskunftserteilung durch den Access-Provider bei statischen IP-Adressen ein Eingriff ins Fernmeldegeheimnis abzulehnen. Dennoch erscheint zunächst die Differenzierung zur Einordnung der statischen IP-Adresse anhand des konkreten Funktionszusammenhangs durchaus plausibel.

In dieser Hinsicht lässt sich die statische IP-Adresse mit einer Festnetznummer vergleichen.[383] So vergibt beispielsweise ein Telefonanbieter für einen Anschluss eine bestimmte Telefonnummer, die natürlich bei jedem Anruf verwendet wird. Die in der Regel bei Vertragsabschuss vergebenen Anschlussnummern stellen grundsätzlich Bestandsdaten im Sinne von § 3 Nr. 6 TKG dar.[384] Werden unter diesen Nummern allerdings Telefonate geführt, handelt es sich in Bezug auf den konkreten Kommunikationsvorgang dagegen bei den verwendeten Telefonnummern um Verkehrsdaten nach § 3 Nr. 70 TKG.[385]

Ähnlich wie bei einer Festnetznummer werden die statischen IP-Adressen zunächst als Bestandsdaten für einen bestimmten Anschluss festgelegt. Bei der Einwahl ins Internet werden diese allerdings für einen konkreten Kommunikationsvorgang verwendet, sodass es sich hierbei um Verkehrsdaten handelt. Die Einordnung der statischen IP-Adresse muss daher im Einzelfall beurteilt werden. Um Verkehrsdaten handelt es sich nur, wenn ein Zusammenhang mit einem konkreten Kommunikationsvorgang besteht.

---

[383] *BVerfG,* Urt. v. 2.3.2010 - 1 BvR 256/08 u.a., NJW 2010, 833 Rn. 256 - Vorratsdatenspeicherung.

[384] S. *Büttgen* in: Beck´scher TKG-Kommentar, § 95 Rn. 2-4.

[385] S. *Büttgen* in: Beck´scher TKG-Kommentar, § 95 Rn. 2-4.

Bei statischen IP-Adressen im Kontext der Auskunftsansprüche gegen Access-Provider handelt es sich allerdings dennoch um Bestandsdaten. Es ginge zu weit, einen Bezug zu einem Telekommunikationsvorgang schon deshalb anzunehmen, weil die IP-Adresse, über die Auskunft begehrt wird, bei einem bestimmten Kommunikationsvorgang verwendet wurde. Vielmehr kommt es darauf an, ob bei der Auskunftserteilung durch den Access-Provider ein solcher Bezug hergestellt wird. Allerdings ist nur bei einer dynamischen IP-Adresse für die Ermittlung des Anschlussinhabers ein Rückgriff auf den genauen Zeitpunkt oder nähere Umstände des einzelnen Kommunikationsvorgangs erforderlich. Bei statischen IP-Adressen ist ein Rückgriff auf die als Vertragsdaten gespeicherten Bestandsdaten ausreichend.

Im Kontext der Auskunftserteilung durch den Access-Provider wird daher kein Bezug zu einem konkreten Telekommunikationsvorgang hergestellt, sodass bei statischen IP-Adressen zur Auskunftserteilung lediglich ein Zugriff auf Bestandsdaten erfolgt, wodurch weder der Schutzbereich des Fernmeldegeheimnisses noch der Anwendungsbereich der e-Privacy-Richtlinie berührt wird. Die Zulässigkeit der Auskunftserteilung richtet sich daher in erster Linie nach der DS-GVO.

Da die notwendigen Bestandsdaten nicht zum Zwecke der Auskunftserteilung an Dritte gespeichert wurden, hat die Auskunftserteilung eine zweckändernde Weiterverarbeitung der Daten zur Folge. Eine solche lässt sich grundsätzlich auf die Öffnungsklausel aus Art. 6 Abs. 4 DS-GVO stützen, sofern eine nationale Vorschrift existiert, die den Anforderungen des Art. 6 Abs. 4 DS-GVO genügt.

Auch hier könnte man zunächst wieder erwägen, die Erlaubnis für die Auskunftserteilung den ausdrücklich geregelten Auskunftsansprüchen aus § 101 UrhG, § 19 MarkenG, § 140b PatG, § 24b GebrMG, § 46 DesignG, § 37b SortenSchuG und § 9 Abs. 2 HalblSchG zu entnehmen. Allerdings wäre dem mit ähnlichen Bedenken zu begegnen wie bei der Auskunftserteilung mittels dynamischer IP-Adresse.[386]

[386] S. oben unter Kap. 5 § 3 D. II 2. a).

Auch wenn hier geringere Anforderungen an die Bestimmtheit zu stellen sind, ist problematisch, dass die untersuchten Auskunftsansprüche keinerlei Regelungen darüber enthalten, welche Daten zur Auskunftserteilung verwendet und ausgewertet werden dürfen. Auch für die Auskunft mittels Bestandsdaten gilt, dass sich nicht automatisch aus der Anspruchsgrundlage auch auf das Vorliegen einer datenschutzrechtlichen Erlaubnisnorm schließen lässt. Dies zeigt sich auch hier dadurch, dass für den Bereich der Telemedien in § 21 Abs. 1 TTDSG (bzw. in § 14 Abs. 2 TMG a.F.) eine Erlaubnisnorm für die Auskunftserteilung über Bestandsdaten zur Durchsetzung von Rechten am geistigen Eigentum eingeführt wurde. Für Access-Provider ist diese Norm allerdings nicht anwendbar. Für Telekommunikationsdienste fehlt eine entsprechende Norm. Daher kann aus den Anspruchsgrundlagen der § 101 UrhG, § 19 MarkenG, § 140b PatG, § 24b GebrMG, § 46 DesignG, § 37b SortenSchuG und § 9 Abs. 2 HalblSchG keine Erlaubnis für die Bestandsdatenauskunft abgleitet werden.

Auch eine Anwendung von § 24 Abs. 1 Nr. 2 BDSG kommt nicht in Betracht, da mit § 174 TKG eine abschließende Regelung für die Bestandsdatenauskunft durch Telekommunikationsdienste existiert, die nur eine Auskunft an staatliche Stellen vorsieht. Diese Vorschrift darf nicht durch eine Anwendung von § 24 Abs. 1 Nr. 2 BDSG zur Auskunftserteilung an private Rechteinhaber umgangen werden.

3. Identifizierung des Nutzers durch WLAN-Betreiber

Selbst wenn der zu einer IP-Adresse gehörige Anschluss mittels Auskunft des Access-Providers erfolgreich ermittelt werden konnte, ist der tatsächliche Rechtsverletzer damit noch nicht automatisch ermittelt. Die Rechteinhaber erhalten auf diese Weise nur Auskunft über die Person des Anschlussinhabers.

Gegebenenfalls ist es deshalb erforderlich, dass die Anschlussinhaber vorbeugende Maßnahmen treffen, um die Nutzer des Anschlusses identifizieren zu können. Besonders wichtig wäre dies bei öffentlichen WLAN-Hotspots, bei denen die Zahl der Nutzer unbegrenzt ist.[387] Aber selbst bei einem WLAN-Zugang

[387] *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 64. Ausführlich zu den verschiedenen Fallgruppen von Anonymität gegenüber dem Access-Provider *Brunst,* Anonymität im Internet, S. 159 ff.

in Hotels oder Cafés, in denen der Kreis der Nutzer begrenzt ist, kann der rechtsverletzende Nutzer in der Regel nur zurückverfolgt werden, wenn die Betreiber der Hotspots Daten ihrer Nutzer erheben.

WLAN-Betreiber unterfallen häufig nicht dem Telekommunikationsdatenschutz, da sie oft ihren Dienst nicht gegen Entgelt oder nicht öffentlich erbringen. Sofern die WLAN-Betreiber freiwillig Daten speichern, richtet sich die Zulässigkeit der Verarbeitung personenbezogener Daten zur Auskunftserteilung nach der DS-GVO und dem Telemediendatenschutz des TTDSG. Insofern kann auf die obigen Ausführungen zu den Telemediendiensten verwiesen werden.

Die meisten WLAN-Betreiber nehmen von sich aus aber keine Speicherung personenbezogener Daten ihrer Nutzer vor. Zudem können WLAN-Anbieter nach § 8 Abs. 4 Nr. 1 a) TMG nicht dazu verpflichtet werden, die Nutzer vor der Gewährung des Zugangs zu registrieren. Der Pflicht zur Speicherung von Bestandsdaten aus § 172 TKG unterfallen WLAN-Betreiber ebenfalls nicht.[388]

Wird ein drahtloses lokales Netzwerk von einer unbegrenzten oder nicht näher bestimmbaren Personenzahl genutzt, lässt sich der tatsächliche Rechtsverletzer deshalb in aller Regel nicht identifizieren. Gegebenenfalls wird zwar die MAC-Adresse des verwendeten Geräts übertragen, allerdings lässt sich von außen weder erkennen, welches Gerät hinter dieser MAC-Adresse steht, noch kann sie dem Besitzer des Geräts zugeordnet werden.[389]

Selbst wenn sich das verwendete Endgerät ermitteln ließe, müsste, wenn ein größerer Personenkreis – zum Beispiel in Computerräumen an Schulen oder Universitäten, in Internetcafés oder am Arbeitsplatz – Zugriff auf ein bestimmtes Gerät hat, protokolliert werden, welche Person zum relevanten Zeitpunkt den Rechner genutzt hat.[390] Auch die Ermittlung eines Rechtsverletzers, der sich auf

---

[388] S. dazu *Ferner* in: BeckOK StPO, § 172 TKG Rn. 12 ff.

[389] *Birkert,* Rechtsfragen bei der Öffnung lokaler Internetzugänge, S. 63 ff.; *Brunst,* Anonymität im Internet, S. 165.

[390] S. *Brunst,* Anonymität im Internet, S. 161 ff.

illegale Weise Zugang zu einem fremden, unzureichend gesicherten WLAN verschafft hat, dürfte meistens praktisch ausgeschlossen sein.[391]

4. Auskunftserteilung durch Anonymisierungsdienste

Ein weiteres Rechtsdurchsetzungshindernis für die Rechteinhaber stellt der Einsatz von Anonymisierungsdiensten dar. Die Nutzer können damit ihre IP-Adresse verschleiern. Um dennoch die Rechtsverletzer anhand der IP-Adresse zurückverfolgen zu können, müssten meist verschiedene Diensteanbieter auf Auskunft in Anspruch genommen werden.

Dafür müssten die Anonymisierungsdienste aber die erforderlichen Verkehrsdaten speichern und an die Rechteinhaber weitergeben. Wie auch bei Access-Providern ist im Ergebnis die dafür erforderliche Datenverarbeitung unzulässig, da entsprechende Rechtsgrundlagen fehlen.

Zudem widerspricht es in der Regel dem Geschäftsmodell der Anonymisierungsdienste, Daten ihrer Nutzer über das zwingend erforderliche hinaus zu speichern. Dem könnte zwar die Verpflichtung zur Vorratsdatenspeicherung nach §§ 175, 176 TKG entgegenstehen. Dennoch dürften nach derzeitiger Rechtslage Daten, die im Rahmen der Vorratsdatenspeicherung erhoben werden, nicht an private Rechteinhaber weitergegeben werden.

Zudem stellt der Einsatz von Anonymisierungsdiensten die Rechteinhaber häufig vor praktische Probleme, da die zu übermittelnden Informationen über Mix-Kaskaden und Routen im außereuropäischen Ausland geleitet werden. Dadurch sind die einzelnen Diensteanbieter für die Rechteinhaber meist überhaupt nicht greifbar.[392]

5. Zwischenergebnis zur Identifizierung von Nutzern durch Zugangsanbieter anhand der IP-Adresse

Die Identifizierung der Rechtsverletzer mittels IP-Adresse stellt die Rechteinhaber vor verschiedene datenschutzrechtliche Probleme:

---

[391] S. *Brunst,* Anonymität im Internet, S. 165 f.

[392] *Brunst,* Anonymität im Internet, S. 143; *Siebert,* Geheimnisschutz, S. 201.

Die Schwierigkeiten beginnen dabei schon im Vorfeld der Auskunftserteilung durch den Access-Provider bei der Ermittlung der IP-Adresse. In einigen Fällen ist es zwar möglich, dass die Rechteinhaber die IP-Adresse selbst - beispielsweise durch den Einsatz einer Software in Filesharing—Netzwerken erheben. Allerdings verarbeiten sie dabei personenbezogene Daten in Form von Verkehrsdaten. Das führt dazu, dass nach der Rechtsprechung des *EuGH* nicht nur die DS-GVO, sondern grundsätzlich auch die e-privacy-Richtlinie zu beachten ist.[393] In den meisten Fällen können die Rechteinhaber die IP-Adressen ohnehin nicht selbst ermitteln, sodass sie auf die Auskunft der Anwendungsdienste angewiesen sind.

Der Auskunftserteilung durch den Access-Provider stehen bei dynamischen IP-Adressen die sehr restriktiven Möglichkeiten der Speicherung von Verkehrsdaten entgegen. Im Ergebnis ist selbst für den Fall, dass die entsprechenden Daten vorhanden wären, die Weitergabe der dynamischen IP-Adresse mangels datenschutzrechtlicher Ermächtigungsgrundlage unzulässig.

Die Speicherung von statischen IP-Adressen untersteht deutlich niedrigeren Anforderungen, da es sich hierbei um Bestandsdaten handelt. Dennoch fehlt auch bei statischen IP-Adressen eine Rechtsgrundlage für die Bestandsdatenauskunft der Access-Provider an die Rechteinhaber.

Selbst wenn der Anschlussinhaber ermittelt werden könnte, kann die Identifizierung des Rechtsverletzers daran scheitern, dass die Betreiber von WLAN-Hotspots nicht zur Registrierung ihrer Nutzer und zur Speicherung von Nutzerdaten verpflichtet sind.

Außerdem dürfte beim Einsatz von Anonymisierungsdiensten die Rückverfolgung eines Nutzers anhand der IP-Adresse für die Rechteinhaber schon aus praktischen Gründen meist unmöglich sein. Jedenfalls wäre eine Auskunftserteilung der Anonymisierungsdienste an die Rechteinhaber aus Datenschutzgesichtspunkten nicht zulässig, da dies die Verarbeitung von Verkehrsdaten voraussetzen würde, wofür eine entsprechende Rechtsgrundlage fehlt.

---

[393] *EuGH,* Urt. v. 17.6.2021 – C-597/19, MMR 2022, 30 Rn. 113 ff. – Mircom.

Insgesamt steht das Datenschutzrecht de lege lata der Identifizierung eines anonymen Rechtsverletzers anhand der IP-Adresse durch die Rechteinhaber entgegen.

D. Prozessuale Rahmenbedingungen und Besonderheiten der Auskunftsansprüche

Die Drittauskunftsansprüche gegen Internetdiensteanbieter zur Identifizierung anonymer Rechtsverletzer bedürfen neben abgestimmten datenschutzrechtlichen Rahmenbedingungen auch einer sinnvollen prozessualen Einbindung. Prozessuale Instrumente können zu einem angemessenen Ausgleich der Interessen beitragen und einem etwaigen Missbrauch der Auskunftsansprüche vorbeugen. Das gilt insbesondere für Fragen nach einem Richtervorbehalt und dem Eilrechtsschutz.

Außerdem sind bei Auskunftsansprüchen zur Identifizierung anonymer Rechtsverletzer hinsichtlich der Beweisführung Besonderheiten zu beachten. Die de lege lata existierenden Auskunftsansprüche im Bereich des geistigen Eigentums, aus § 21 Abs. 2 S. 2 TTDSG, sowie der aus § 242 BGB abgeleitete Drittauskunftsanspruch unterscheiden sich nicht nur hinsichtlich ihrer materiell-rechtlichen Voraussetzungen und Rechtsfolgen, sondern auch teilweise hinsichtlich ihrer prozessualen Rahmenbedingungen.

I. Richtervorbehalt

Die parallelen Auskunftsansprüche im Bereich des geistigen Eigentums sehen in ihrem 9. Absatz einen Richtervorbehalt vor. Dementsprechend ist vor der Auskunftserteilung eine richterliche Anordnung erforderlich, wenn diese nur unter Verwendung von Verkehrsdaten erteilt werden kann.

Im Rahmen des Verfahrens nach Absatz 9 ordnet das Gericht die Zulässigkeit der Verwendung von Verkehrsdaten zur Auskunftserteilung an. In diesem Zusammenhang hat das Gericht auch die Voraussetzungen des Auskunftsanspruchs nach Absatz 2 zu prüfen.[394] Dennoch wird lediglich über die Gestattung

[394] *Dreier* in: Dreier/Schulze, § 101 UrhG Rn. 36.

der Auskunft, nicht aber auch über die Verpflichtung zur Auskunftserteilung entschieden.[395] Verweigert der Diensteanbieter trotz der Gestattung die Auskunft, müsste der Anspruch in einem weiteren Verfahren nach der ZPO tituliert werden.[396]

Anders verhält es sich bei dem Gestattungsverfahren nach § 21 Abs. 2-4 TTDSG. Bei der Ausgestaltung des § 21 Abs. 2-4 TTDSG hat sich der Gesetzgeber an der vorher bereits bestehenden Vorschrift aus § 101 Abs. 9 UrhG angelehnt.[397] Auch hier ist im Vorfeld der Auskunftserteilung eine richterliche Anordnung nach Abs. 3 erforderlich, in der das Gericht allerdings grundsätzlich auch über die Verpflichtung zur Auskunftserteilung mitentscheidet. Im Übrigen gelten in beiden Verfahren die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend.[398] Gegen die Entscheidung ist das Rechtsmittel der Beschwerde statthaft. Nach § 59 FamFG steht dies jedem zu, der durch den Beschluss in seinen Rechten beeinträchtigt wurde. Dadurch kann unter anderem ein identifizierter Anschlussinhaber unter Berufung auf das Fernmeldegeheimnis gegen den Beschluss vorgehen.[399] Auch nach der in diesem Fall meist schon eingetretenen Erledigung der Hauptsache kann das Beschwerdegericht nach § 62 Abs. 1 FamFG auf Antrag feststellen, dass der Beschluss den Beschwerdeführer in seinen Rechten verletzt hat.[400]

Ein weiterer entscheidender Unterschied besteht aber darin, dass im Rahmen des Gestattungsverfahrens nach § 21 Abs. 2-4 TTDSG auch schon bei der Verarbeitung von Bestandsdaten durch Telemediendiensteanbieter eine

---

[395] *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 160.

[396] *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 160; *Hoffmann,* MMR 2009, 655, 656.

[397] S. *Ettig* in: Taeger/Gabel, § 21 TTDSG Rn. 16 unter Bezugnahme auf *Beschlussempfehlung und Bericht des Ausschusses für Recht und Verbraucherschutz*, BT-Drs. 18/13013, S. 24.

[398] S. zum Gestattungsverfahren nach § 21 Abs. 2-4 TTDSG auch *Ettig* in: Taeger/Gabel, § 21 TTDSG Rn. 16 ff.

[399] *BGH*, Beschl. v. 5.12.2012 – I ZB 48/12, GRUR 2013, 536 Rn. 11 – Die Heiligtümer des Todes; *OLG Köln*, Beschl. v. 5.10.2010 - 6 W 82/10, MMR 2011, 108, 108 ff. Anders aber *OLG Köln*, Beschl. v. 5.5.2009 - 6 W 39/09, MMR 2009, 547, 547 ff. – John Bello Story 2. Ausführlicher dazu *Sandor,* Datenspeicherung, Rn. 272 ff.

[400] *Wimmers* in: Schricker/Loewenheim, § 101 UrhG Rn. 125.

richterliche Anordnung vorausgesetzt wird, während Absatz 9 der Auskunftsansprüche bei Verletzungen des geistigen Eigentums lediglich die Verkehrsdatenauskunft unter Richtervorbehalt steht. Das ist nicht nur widersprüchlich, sondern auch ein nicht unerheblicher Nachteil für die Rechteinhaber, wenn sie bereits für die Bestandsdatenauskunft stets vorab eine richterliche Anordnung erwirken müssen. Außerdem müssen die Rechteinhaber die Kosten für die richterliche Anordnung tragen, ohne vorher zu wissen, ob die spätere Auskunft überhaupt zur Identifizierung des anonymen Nutzers führt.

Der Richtervorbehalt schützt vor einem Missbrauch der Auskunftsansprüche und dem unberechtigten Ausspähen von Nutzerdaten.[401] Er kann daher ein sinnvolles Instrument zum Schutz der Interessen von Internetnutzern darstellen. Auf der anderen Seite ist die lange Dauer bis zur Erwirkung einer richterlichen Anordnung nachteilig für die Rechteinhaber. Zudem besteht die Gefahr einer hohen Belastung der Gerichte, wenn man bedenkt, dass Rechtsverletzungen im Internet ein Massenphänomen darstellen.[402] Außerdem wird der Diensteanbieter gezwungen, Teil eines gegebenenfalls kostenintensiveren Prozesses zu werden, auch wenn er das Auskunftsbegehren eigentlich für berechtigt hält.[403] Der Richtervorbehalt sollte daher auf die Fälle begrenzt werden, in denen er unbedingt zur Wahrung der Nutzerinteressen erforderlich ist.

II. Einstweiliger Rechtsschutz

Nutzerdaten, die bei der Kommunikation im Internet anfallen, werden häufig nur kurzfristig gespeichert. Verstreicht zu viel Zeit von der Rechtsverletzung bis zur Auskunftserteilung durch die Diensteanbieter, besteht die Gefahr, dass die zur Identifizierung benötigten Daten bereits nicht mehr vorhanden sind. Daher spielen Eilrechtsbehelfe bei der Auskunft über anonyme Rechtsverletzer im Internet eine große Rolle.

---

[401] S. zur besonderen Schutzbedürftigkeit bei der Verkehrsdatenauskunft *Regierungsentwurf,* BT-Drs. 16/5048, S. 40, 49.

[402] Ähnliche Bedenken äußerte auch der Bundesrat, S. *Regierungsentwurf,* BT-Drs. 16/5048, 56.

[403] *Regierungsentwurf,* BT-Drs. 16/5048, S. 38.

1. Einstweilige Verfügung nach §§ 935 ff. ZPO

Der 7. Absatz des § 101 UrhG sowie der Parallelvorschriften in § 19 MarkenG, § 140b PatG, § 24b GebrMG, § 46 DesignG und § 37b SortG ermöglichen es, die begehrte Auskunft im Wege der einstweiligen Verfügung nach den §§ 935-945 ZPO gegenüber den Diensteanbietern durchzusetzen. Im Wege dieses Verfahrens kann bereits die Verpflichtung zur Erteilung der Auskunft angeordnet werden.

Eine einmal erteilte Auskunft kann aber nicht wieder zurückgenommen werden, auch wenn sich in der Hauptsache herausstellen sollte, dass ein Anspruch tatsächlich nicht besteht.[404] Um Widersprüche zum Hauptsacheverfahren zu vermeiden, hat der Gesetzgeber eine offensichtliche Rechtsverletzung zur Voraussetzung einer einstweiligen Verfügung gemacht.[405]

Grundsätzlich ist die Option des einstweiligen Rechtsschutzes im Sinne des Rechtsschutzinteresses der Rechteinhaber begrüßenswert. Trotz der mangelnden Trennschärfe ist die Einschränkung der einstweiligen Verfügung auf offensichtliche Rechtsverletzungen im Hinblick auf die Vorwegnahme der Hauptsache nachvollziehbar. Allerdings zeigt sich hier erneut die Problematik des Merkmals der offensichtlichen Rechtsverletzung als Voraussetzung für den Auskunftsanspruch aus Absatz 2: Es vermag nicht zu überzeugen, dass bei Vorliegen der Voraussetzungen des Auskunftsanspruchs aus Absatz 2 immer auch eine einstweilige Verfügung möglich wäre.

Besonderheiten ergeben sich außerdem für das Verfahren bei einer Verkehrsdatenauskunft nach Absatz 9, bei denen im Vorfeld der Auskunftserteilung eine richterliche Anordnung über die Zulässigkeit der Auskunftserteilung erforderlich ist.[406] In diesen Fällen kann der Diensteanbieter im Rahmen des einstweiligen Rechtsschutzes allenfalls dazu verpflichtet werden, die notwendigen Daten

---

[404] *Dreier* in: Dreier/Schulze, § 101 UrhG Rn. 28.

[405] *Regierungsentwurf,* BT-Drs. 11/4792, S. 32.

[406] S. zur Verwendung von Verkehrsdaten bei dynamischen IP-Adressen etwa *BGH*, Beschl. v. 5.12.2012 – I ZB 48/12, GRUR 2013 Rn. 37 f. – Die Heiligtümer des Todes; *BGH*, Beschl. v. 19.4. 2012 – I ZB 80/11, GRUR 2012, 1026 Rn. 37 ff. – Alles kann besser werden; *Kitz*, NJW 2008, 2374, 2375; *Spindler/Nink* in: Spindler/Schuster, § 14 TMG Rn. 8; *Spindler*, ZUM 2008, 640, 645; *Spindler/Dorschel*, CR 2006, 341, 345;

im Rahmen des datenschutzrechtlich Zulässigen nicht zu löschen.[407] Könnten die Diensteanbieter bereits im Wege der einstweiligen Verfügung zur Auskunftserteilung verpflichtet werden, würde man den mit dem Richtervorbehalt bezweckten Schutz der Verkehrsdaten umgehen. Damit sich nicht zwei verschiedene Gerichte mit demselben Sachverhalt befassen müssen, ist es außerdem sachgerecht, im Rahmen des Verfahrens nach Absatz 9 ausschließlich auf eine einstweilige Anordnung nach § 49 FamFG abzustellen.[408]

2. § 49 FamFG

§ 49 FamFG findet in den Fällen Anwendung, in denen die Auskunftserteilung unter Richtervorbehalt steht. Das gilt sowohl für das Gestattungsverfahren nach § 21 Abs. 2-4 TTDSG, als auch für die eben genannten Verfahren nach Absatz 9 der Auskunftsansprüche im Bereich des geistigen Eigentums. Die in diesen Vorschriften geregelten Gestattungsverfahren verweisen jeweils nämlich auf das FamFG. Dies hat unter anderem den Vorteil, dass nach § 26 FamFG der Amtsermittlungsgrundsatz gilt.

Da eine richterliche Anordnung Zeit erfordert, besteht die Gefahr, dass bis dahin die Auskunftserteilung mangels der hierzu erforderlichen Daten bereits nicht mehr möglich ist. Das gilt vor allem bei der Auskunft mittels Verkehrsdaten, welche die Diensteanbieter nach § 9 Abs. 1 S. 2 TTDSG grundsätzlich unverzüglich nach Ende des Kommunikationsvorgangs löschen müssen.

Durch die einstweilige Anordnung kann es den Diensteanbietern untersagt werden, die zur Auskunft erforderlichen Daten bis zur richterlichen Entscheidung zu löschen, sodass die Nutzerdaten gesichert werden. Weder § 49 FamFG, noch die Vorschriften über das Gestattungsverfahren beinhalten aber eine datenschutzrechtliche Erlaubnisnorm. Die Diensteanbieter können deshalb auch im Wege der einstweiligen Verfügung nur insoweit verpflichtet werden, wie es

---

[407] *Dreier* in: Dreier/Schulze, § 101 UrhG Rn. 30.

[408] *Wimmers* in: Schricker/Loewenheim, § 101 UrhG Rn. 97; Ähnlich auch *OLG Hamburg,* Urt. v. 4.2.2016 - 5 U 10/12, BeckRS 2016, 127381 Rn. 33 ff. A.A. aber *BGH,* Urt. v. 21.9.2017 – I ZR 58/16, GRUR 2017, 1236 Rn. 28 – Sicherung der Drittauskunft, der § 101 Abs. 7 UrhG angewendet hat, obwohl auch eine richterliche Anordnung für die Auskunftserteilung nach § 101 Abs. 9 UrhG erforderlich war.

datenschutzrechtlich zulässig ist.[409] Ohne eine gesetzliche Regelung, die es den Diensteanbietern erlaubt, Nutzerdaten zur Auskunftserteilung an die Rechteinhaber zu speichern, besteht deshalb trotz Eilrechtsbehelf weiterhin die Gefahr, dass der Auskunftsanspruch ins Leere läuft.[410]

III. Beweisschwierigkeiten der Rechteinhaber

Sowohl die Auskunftsansprüche als auch die Gestattung der Auskunftserteilung setzen eine Rechtsverletzung durch einen Internetnutzer voraus. Der Nachweis einer solchen kann den Rechteinhabern im Einzelfall aber Schwierigkeiten bereiten.

1. Besonderheiten im Gestattungsverfahren

Dabei gelten im Verfahren der Auskunftserteilung bei den Ansprüchen im Bereich des geistigen Eigentums und nach § 242 BGB die Regelungen der ZPO. Die Beweisaufnahme in den Gestattungsverfahren richtet sich aber nach den Vorschriften für Verfahren der freiwilligen Gerichtsbarkeit. In diesen Verfahren gilt nach § 26 FamFG der Amtsermittlungsgrundsatz. Dies soll sicherstellen, dass es nicht vorschnell zur Herausgabe von Nutzerdaten kommt.[411] Das Gericht hat bei der Feststellung des Sachverhalts von Amts wegen die Wahrheit zu ermitteln und ist an die Beweisanträge der Beteiligten nicht gebunden.[412]

Außerdem gelten nach § 30 Abs. 1 FamFG die Regelungen für die Durchführung der förmlichen Beweisaufnahme entsprechend, sofern nicht der Amtsermittlungsgrundsatz entgegensteht.[413] Das Gericht entscheidet nach pflichtgemäßem Ermessen, ob es im Wege des Strengbeweises oder des Freibeweises vorgeht. Je intensiver durch eine Entscheidung in Grundrechte eingegriffen wird, desto eher wird aber eine förmliche Beweisaufnahme zu wählen sein.[414] Das ist

---

[409] So auch etwa *OLG Hamm*, Beschl. v. 2.11.2010 - I-4 W 119/10, MMR 2011, 193, 194.

[410] *OLG Hamm*, Beschl. v. 2.11.2010 - I-4 W 119/10, MMR 2011, 193, 193 f.

[411] Vgl. *BGH,* Beschl. v. 24.9.2019 – VI ZB 39/18, GRUR 2020, 101 Rn. 57 – Facebook-Messenger; *Beschlussempfehlung und Bericht des Ausschusses für Recht und Verbraucherschutz,* BT-Drs. 18/13013, 24.

[412] S. dazu *Burschel* in: BeckOK FamFG, § 26 FamFG Rn. 29; *Welp,* Auskunftspflicht von Access-Providern, S. 354.

[413] S. dazu *Burschel* in: BeckOK FamFG, § 30 FamFG Rn. 17.

[414] *Burschel* in: BeckOK FamFG, § 30 FamFG Rn. 7.

vor allem bei einem Eingriff ins Fernmeldegeheimnis – zum Beispiel bei einem Gestattungsverfahren nach § 101 Abs. 9 UrhG – der Fall.[415]

2. Nachweis der Rechtsverletzung

Die Rechteinhaber tragen zumindest die Darlegungslast für die Rechtsverletzung.[416] Für die parallelen Auskunftsansprüche im Bereich des geistigen Eigentums muss zudem der Nachweis über die Offensichtlichkeit der Rechtsverletzung erbracht werden, sodass eine andere Beurteilung als eine Rechtsverletzung kaum möglich erscheint.[417] Dafür müssen sich die Rechteinhaber des stärksten zur Verfügung stehenden Beweismittels bedienen.[418]

Bei Rechtsverletzungen im Internet können auch digitale Beweismittel eine Rolle spielen. Diese sind dem Beweis durch Ausgenschein nach § 371 ZPO (i.V.m. § 30 FamFG) zugänglich.[419] § 371 Abs. 1 ZPO ordnet elektronische Dokumente dem Beweis durch Augenschein zu und verlangt, dass diese vorgelegt oder übermittelt werden müssen. So können zum Beispiel Bild- oder Tondokumente auf einem Datenträger vorgelegt oder per Mail übermittelt werden.[420] Bei einer Seite im Internet kann als Beweis die URL angegeben werden.[421]

Weitgehend unproblematisch dürfte der Nachweis einer Rechtsverletzung sein, wenn die fraglichen Inhalte oder die zur Rechtsverletzung führenden Umstände für jedermann im Internet einsehbar sind. Problematischer ist es aber etwa, wenn die fraglichen Inhalte nur vorübergehend verfügbar oder bereits gelöscht sind oder lediglich einem begrenzten Personenkreis zugänglich sind. Da immer die Gefahr einer Löschung von Inhalten bestehen kann, ist es außerdem für die

---

[415] S. auch *Welp,* Auskunftspflicht von Access-Providern, S. 354. Weitergehend *Brüggemann,* Drittauskunftsanspruch, S.333, der für das Verfahren nach § 101 Abs. 9 UrhG eine Reduzierung des Ermessensspielraums auf null annimmt, sodass die Pflicht zur förmlichen Beweisaufnahme besteht.

[416] Vgl. *Czychowski,* GRUR-RR 2008, 265, 268.

[417] *OLG Frankfurt a.M.,* Urt. v. 14.3.2002 - 6 U 254/01, GRUR-RR 2003, 32, 32.

[418] *LG München I,* Urt. v. 6.6.2019 - 7 O 5358/19*,* BeckRS 2019, 10916.

[419] Ausführlich *Rupp,* Beweisführung mit privaten elektronischen Dokumenten, S. 75.

[420] *Huber* in: Musielak/Voit, § 371 ZPO Rn.13

[421] S. *Bach* in: BeckOK ZPO, § 371 ZPO Rn. 7a. S. zur Internetrecherche als Augenscheinsbeweis *Greger* in: FS Stürner, 289, 297.

Rechteinhaber wichtig, frühzeitig entsprechende Beweise möglichst umfassend zu sichern. Häufig wird dafür ein Screenshot als Nachweis einer Rechtsverletzung erstellt. Da dieser leicht fälschbar ist, hat er isoliert aber nur einen sehr geringen Beweiswert.[422] Es ist daher sinnvoll, diesen zumindest mit einem Zeitstempel zu versehen. Ein solcher bietet sich vor allem dann an, wenn es auf den genauen Zeitpunkt einer Rechtsverletzung ankommt. Das ist etwa der Fall, wenn der Nutzer anhand einer dynamische IP-Adresse identifiziert werden soll, da diese nur vorübergehend demselben Anschluss zugeordnet ist. Daneben können zur Beweisführung aber natürlich auch Zeugen der Rechtsverletzung angebracht werden. Zum Beispiel kann eine Person, die eine Rechtsverletzung manuell ermittelt hat, als Zeuge vernommen werden.[423]

Besonders schwierig ist der Nachweis einer Rechtsverletzung in Filesharing-Fällen.[424] Urheberrechtsverletzungen in P2P-Netzwerken werden in der Regel durch die Beauftragung spezialisierter Unternehmen aufgedeckt, die mittels einer Software die Netzwerke gezielt nach den urheberrechtlich geschützten Werken ihrer Auftraggeber durchsuchen[425]. Die Software erstellt meist einen Bildschirmausdruck des Filesharing-Netzwerks, aus dem auch der Hashwert der angeblich heruntergeladenen Datei hervorgehen kann.[426] Um nachzuweisen, dass es sich bei der Datei um eine Vervielfältigung seines Werkes handelt, muss der Rechteinhaber zusätzlich die Datei vorlegen und das Verfahren darlegen, mit dem der Hashwert berechnet wurde.[427] Zudem besteht die Möglichkeit, durch einen Testdownload nachzuweisen, dass es sich bei der fraglichen Datei um das gegenständliche geschützte Werk handelt.[428] Der BGH lässt es bereits

---

[422] So weisen *Gietl/Mantz,* CR 2008, 810, 815 etwa auf sog. „Abmahnbilder-Generatoren" hin, mit denen unter Angabe von Namen und IP-Adresse sich leicht ein Screenshot eines Filesharingprogramms fälschen lässt.

[423] Vgl. *Hohlweck,* GRUR 2014, 940, 941 f.

[424] Ausführlicher hierzu etwa *Gietl/Mantz,* CR 2008, 810, 815.

[425] *Brüggemann,* Drittauskunftsanspruch, S. 334.

[426] *Brüggemann,* Drittauskunftsanspruch, S. 334.

[427] S. auch *OLG Hamburg,* Beschl. v. 3.11.2010 - 5 W 126/10, DuD 2011, 213; *LG Frankenthal*, Beschl. v. 6.3.2009 - 6 O 60/09, MMR 2009, 487, 488; *LG Hamburg*, Urt. v. 14.3.2008 - 308 O 76/07, CR 2008, 401, 401; *Gietl/Mantz,* CR 2008, 810, 815; *Intveen*, ITRB 2008, 124, 125; *Lutz,* VuR 2010, 337, 340; *Nietsch,* K&R 2011, 101, 102; *Sandor,* Datenspeicherung, Rn. 449 ff.; *Sankol,* K&R 2008, 509, 512; *Welp,* Auskunftspflicht von Access-Providern, S. 356.

[428] *Brüggemann*, Drittauskunftsanspruch, S. 336; *Welp,* Auskunftspflicht, S. 357.

ausreichen, wenn die gewonnenen Ermittlungsergebnisse durch Screenshots der Software dokumentiert und durch Mitarbeiter des zuständigen beauftragten Unternehmens erklärt werden.[429]

3. Nachweis über zutreffende Ermittlung und Zuordnung einer IP-Adresse

Weitere Schwierigkeiten ergeben sich, wenn der Nutzer anhand der IP-Adresse identifiziert werden soll. De lege lata ist das nur für das Verfahren nach Absatz 9 der Auskunftsansprüche im Bereich des geistigen Eigentums relevant, da alle anderen Anspruchsgrundlagen eine Identifizierung des Anschlussinhabers durch den Access-Provider nicht vorsehen.

Die Herausforderung für die Rechteinhaber im Rahmen dieses Verfahrens besteht vor allem darin, den Nachweis darüber zu erbringen, dass die bei der Rechtsverletzung verwendete IP-Adresse zutreffend ermittelt wurde. Sofern die IP-Adresse über die Anwendungsdienste in Erfahrung gebracht wird, kommt es auf die Auskunft der entsprechenden Diensteanbieter und die Aufzeichnung der Daten in deren Log-Dateien an. Wird die IP-Adresse dem Header einer E-Mail entnommen, kann der Rechteinhaber diese selbst protokollieren.

Problematisch ist erneut der Einsatz einer Ermittlungssoftware bei Filesharing in P2P-Netzwerken.[430] Die Software zeigt neben der Datei und dem Hashwert die IP-Adresse, sowie die Uhrzeit an und erstellt darüber einen Screenshot des Filesharing-Netzwerks. Weder der Ablauf noch das Ergebnis der Ermittlungen durch die Software sind aber als solches von außen überprüfbar. Daher kommt es bei der Frage nach deren Beweiseignung maßgeblich auf die Zuverlässigkeit der Software an.[431] Der Nachweis hierüber kann durch ein Gutachten eines

---

[429] *BGH,* Urt. v. 11.6.2015 - I ZR 19/14, MMR 2016, 121 Rn. 34 – Tauschbörse I; *BGH,* Urt. v. 11.6.2015 - I ZR 75/14, MMR 2016, 131 Rn. 18 – Tauschbörse III.

[430] Siehe etwa *Morgenstern,* CR 2011, 203, 204 ff., der davon ausgeht, dass die beim Filesharing eingesetzte Software und die dokumentierten Beweismittel den Anforderungen der Computerforensik nicht genügen.

[431] S. dazu etwa AG Koblenz, Beschl. v. 2.1.2015 - 153 C 3184/14, ZD 2015, 237, 237, das die Zuverlässigkeit der Sofware „Observer" abgelehnt hat. S. auch *OLG Köln,* Beschl. v. 7.9.2011 - 6 W 82/11, MMR 2012, 41, 41 f.; *Karger,* GRUR-Prax 2010, 305.

Sachverständigen erbracht werden.[432] Neben der allgemeinen Eignung muss der Rechteinhaber nachweisen, dass die eingesetzte Software auch im konkreten Fall funktioniert hat.[433] Dabei ist etwa eine Zeugenvernehmung des zuständigen Mitarbeiters des durch die Rechteinhaber beauftragten Unternehmens denkbar.[434] Zweifel können auch durch Mehrfachermittlung einer IP-Adresse ausgeräumt werden.[435] Nach dem Grundsatz der freien richterlichen Beweiswürdigung nach § 37 Abs. 1 FamFG ist es aber ausreichend, wenn das Gericht zur Überzeugung kommt, dass die IP-Adresse im konkreten Fall zutreffend ermittelt wurde. Eine absolute Gewissheit, dass es nicht zu einer fehlerhaften Ermittlung gekommen sein könnte, ist nach Ansicht des *BGH* aber nicht erforderlich.[436]

Zudem stellt sich noch die Frage, ob die IP-Adresse durch den Access-Provider korrekt einem Anschlussinhaber zugeordnet werden kann. Insbesondere bei dynamischen IP-Adressen besteht die Problematik, dass bereits kleine Abweichungen der Zeitmessung zur Ermittlung des falschen Anschlusses führen können.[437] Daher ist es wichtig, dass sowohl die Zeitmessungen bei der Ermittlung der IP-Adresse als auch bei der Protokollierung durch den Access-Provider korrekt und übereinstimmend sind.[438] Meist wird diese Problematik erst in einem späteren Verfahren gegen den Anschlussinhaber relevant. Für die Frage, ob der Anschlussinhaber gleichzeitig auch die Rechtsverletzung begangen hat, wird der

---

[432] S. *OLG Köln,* Beschl. v. 7.20.2013 – 6 W 84/13, ZUM 2013, 951, 951 – Life of Pi; *OLG Köln,* Beschl. v. 3.7.2012 – 6 W 100/12, ZUM 2012, 985, 986 – Ermittlungssoftware. S. zu Einschränkungen bei der Beurteilung von Software zur Ermittlung von Rechtsverletzungen auch *OLG Köln,* Beschl. v. 20. 1. 2012 – 6 W 242/11, GRUR-RR 2012, 335, 335 – Beweisschwierigkeiten beim Filesharing.

[433] *Redeker,* IT-Recht, Rn. 1487.

[434] *Welp,* Auskunftspflicht von Access-Providern, S. 255 f. S. auch *BGH,* Urt. v. 11.6.2015 – I ZR 19/14, NJW 2016, 942 – Tauschbörse I. Vgl. auch *Brüggemann,* Drittauskunftsanspruch, S. 334.

[435] S. *LG Köln,* Urt. v. 14.12.2017 – 14 S 1/17, ZUM-RD 2018, 422, 422 f.

[436] *BGH,* Urt. v. 11.6.2015 – I ZR 19/14, MMR 2016, 121 Rn. 40 – Tauschbörse I*; BGH,* Beschl. v. 7.20.2013 – 6 W 84/13, ZUM 2013, 951, 951 f. – Life of Pi.

[437] *Bleich/Heidrich/Stadler*, c't 2010/19, 138, 139; *Brüggemann,* Drittauskunftsanspruch, S. 47; *Gietl/Mantz,* CR 2008, 810, 814 f.; *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 118; *Lutz*, VuR 2010, 337, 341; *Nietsch*, Anonymität und Durchsetzung, S. 81; *Röhl/Bosch*, NJW 2008, 1415, 1419.

[438] Vgl. *Nietsch,* Anonymität und Durchsetzung, S. 82 f.

Rechteinhaber insofern entlastet, als den Anschlussinhaber selbst die sekundäre Darlegungslast trifft.[439]

4. Beweisverwertungsverbote

Neben den Nachweisschwierigkeiten kann es auch zu Beweisverwertungsverboten kommen, wenn Beweismittel rechtswidrig erlangt wurden. Für den Zivilprozess existiert allerdings keine ausdrückliche Regelung über den Umgang mit derartigen Beweismitteln. Die rechtswidrige Erlangung eines Beweismittels führt nicht unmittelbar auch zu einem Verwertungsverbot.[440] Stattdessen ist die Verwertbarkeit anhand des konkreten Einzelfalls zu beurteilen.[441] Dabei ist maßgeblich auf den Schutzzweck der verletzen Norm abzustellen.[442] Demnach besteht ein Verwertungsverbot, wenn der Schutzzweck der verletzen Norm die Unverwertbarkeit des Beweises verlangt.[443]

Bei den Auskunfts- und Gestattungsverfahren zur Identifizierung eines anonymen Nutzers handelt es sich um selbstständige Verfahren.[444] Das Ziel des Auskunftsersuchens der Rechteinhaber besteht darin, den unmittelbaren Verletzer zu ermitteln, um Unterlassungs- oder Schadensersatzansprüche gegen diesen geltend machen zu können. Bei einem solchen Auskunfts- bzw. Gestattungsverfahren handelt es sich insofern um eine Art vorbereitendes Verfahren.[445] Beweisverwertungsverbote könnten sich daher sowohl im Auskunftsverfahren als aber auch im nachgelagerten Verfahren gegen den unmittelbaren Verletzer auswirken.

---

[439] S. oben unter Kap. 5 § 2 A. I. 4. c).

[440] *Bacher* in: BeckOK ZPO, Rn. 19.

[441] *Brand/Skowronek*, RDi 2021, 178, 184; *Kiethe*, MDR 2005, 965; *Nietsch,* K&R 2011, 101, 102.

[442] *Brüggemann,* Drittauskunftsanspruch, S. 316.

[443] *BGH,* Urt. v. 10.12.2002 - VI ZR 378/01, VersR 2003, 924, 925 f.; *OLG Köln,* Urt. v. 5.7.2005 - 24 U 12/05, NJW 2005, 2997, 2999. Kritisch *Muthorst*, Beweisverbot, S. 69 ff., 95 ff.

[444] Vgl. *Brüggemann,* Drittauskunftsanspruch, S. 331.

[445] Vgl. *Brüggemann,* Drittauskunftsanspruch, S. 331.

a) Auskunftserteilung ohne die erforderliche richterliche Anordnung

Zu einem Beweisverwertungsverbot kann es kommen, wenn die Auskunft ohne die entweder nach § 101 Abs. 9 UrhG[446] oder nach § 21 Abs. 3 S. 1 TTDSG erforderliche gerichtliche Anordnung erteilt wurde. Zumindest bei einer Auskunftserteilung im Sinne von § 101 Abs. 9 UrhG muss das Fehlen der richterlichen Anordnung zu einem Beweisverwertungsverbot führen.[447] Die Regelung dient dem Schutz des Fernmeldegeheimnisses der Nutzer und könnte andernfalls leicht umgangen werden. Im Rahmen einer Auskunftserteilung im Sinne des § 21 Abs. 3 S. 1 TTDSG wird das Fernmeldegeheimnis zwar nicht tangiert, allerdings wird durch die Auskunftserteilung das allgemeine Persönlichkeitsrecht der Nutzer tangiert, sodass auch hier eine Umgehung des Erfordernisses einer richterlichen Anordnung dem Schutzzweck der Norm widerspricht. Zumindest sollte die Auskunftserteilung jedenfalls dann zu einem Beweisverwertungsverbot führen, wenn die Rechteinhaber diese vorsätzlich ohne die notwendige gerichtliche Anordnung bei den Dienstanbietern erwirkt haben. Die durch eine solche Auskunftserteilung gewonnenen Beweise sind in einem späteren Verfahren gegen den unmittelbaren Rechtsverletzer unverwertbar.

Diskutiert wurde ein Beweisverwertungsverbot vor allem in den in der Praxis relevanten Reseller-Fällen, in denen Netzbetreiber und Endkundenanbieter auseinanderfallen. Soll ein Nutzer anhand der dynamischen IP-Adresse identifiziert werden, müssen in dieser Konstellation sowohl der Netzbetreiber als auch der Endkundenanbieter (Reseller) auf Auskunft in Anspruch genommen werden. Der Netzbetreiber kann lediglich Auskunft über die Anschlusskennung erteilen, der die IP-Adresse zum fraglichen Zeitpunkt zugeordnet war, während der Endkundenanbieter diese wiederum den Kundenbestandsdaten zuordnen kann. Es war deshalb umstritten, ob es auch für die Auskunftserteilung durch den Endkundenanbieter einer vorherigen gerichtlichen Anordnung nach § 101

---

[446] Dasselbe gilt auch für die Parallelvorschriften aus § 140b PatG, § 24b GebrMG, § 19 MarkenG, § 46 DesignG, § 37b SortG und § 9 Abs. 2 HalblShuG. Auf Grund deren geringen Anwendungsbereichs beschränken sich die Ausführungen hier zugunsten der Übersichtlichkeit aber auf § 101 Abs. 9 UrhG.

[447] Vgl. zu einem Beweisverwertungsverbot im Zivilprozess bei Fehlen eines richterlichen Beschlusses für eine Auskunft gegenüber Ermittlungsbehörden *OLG Karlsruhe,* Urt. v. 4.12.2008 - 4 U 86/07, MMR 2009, 412, 412.

Abs. 9 UrhG bedarf.[448] Teilweise wurde ein Beweisverwertungsverbot angenommen, falls die Auskunft des Endkundenanbieters ohne vorherige richterliche Anordnung erfolgte.[449] Inzwischen hat der *BGH* allerdings entschieden, dass die Auskunftserteilung durch den Endkundenanbieter keine gerichtliche Anordnung erfordert, da es sich um eine bloße Bestandsdatenauskunft handele.[450]

b) Datenschutzrechtlicher Verstoß

Daneben kommt ein Beweisverwertungsverbot in Betracht, wenn bei der Erlangung von Beweismitteln gegen Datenschutzregeln verstoßen wurde. Das kann zum Beispiel der Fall sein, wenn die Rechteinhaber selbst datenschutzwidrig Daten der Nutzer ermittelt haben oder wenn es im Rahmen der Auskunftserteilung durch die Diensteanbieter zu einem datenschutzrechtlichen Verstoß kommt.[451] Letzteres ist vor allem denkbar, wenn die zur Auskunft erforderlichen Daten nicht hätten erhoben oder gespeichert werden dürfen oder nicht zum Zwecke der Auskunftserteilung an die Rechteinhaber hätten übermittelt werden dürfen.[452]

---

[448] Gegen das Erfordernis einer gerichtlichen Anordnung S. *OLG Köln,* Beschl. v. 27.11.2012 – 6 W 181/12, GRUR-RR 2013, 137, 137 - Reseller; *AG Potsdam,* Urt. v. 12.11.2015 - 37 C 156/15, ZD 2016, 296, 296 - Uheilig; *Holznagel*, CR 2017, 193, 194 f.; *Issa,* ZUM 2017, 390, 396 f. A.A. *LG Frankenthal*, Urt. v. 11.8.2015 – 6 O 55/15, K&R 2015, 671, 671; *AG Augsburg*, Urt. v. 22.6.2015 - 16 C 3030/14, BeckRS 2015, 17406; *AG Rostock*, Urt. v. 25.8.2015 - 48 C 11/15, ZD 2016, 192, 192; *AG Koblenz*, Urt. v. 9.1.2015 - 411 C 250/14, ZD 2015, 235; *Zimmermann*, K&R 2015, 73, 74.

[449] *LG Frankenthal*, Urt. v. 11.8.2015 – 6 O 55/15, GRUR-RR 2016, 110 Rn. 15 – Reseller im Auskunftsverfahren; *AG Augsburg*, Urt. v. 22.6.2015 - 16 C 3030/14, GRUR-RS 2015, 17406 Rn. 24; *AG Koblenz*, Urt. v. 9.1.2015 - 411 C 250/14, NJOZ 2015, 2015, 655, 657; *AG Rostock*, Urt. v. 25.8.2015 - 48 C 11/15, ZD 2016, 192; *Zimmermann,* K & R 2015, 73, 75 f.

[450] *BGH,* Urt. v. 13.7.2017 – I ZR 193/16, NJW 2018, 781, 781 - Benutzerkennung; S. zur Entscheidung des BGH *Sesing,* NJW 2018, 754, 754 ff.; *Marly,* LMK 2018, 403212.

[451] S. zur Zulässigkeit der vorgelagerten Verarbeitung von Verkehrsdaten durch Rechteinhaber oben unter Kap. 5 § 3 D. I 2. Zum Beweisverwertungsverbot bei heimlicher Ermittlung möglicher Urheberrechtsverletzungen *OLG Hamburg,* Beschl. v. 3.11.2010 - 5 W 126/10, MMR 2011, 281, 281; *Nietsch,* K&R 2011, 101, 102; *Sandor,* Datenspeicherung, Rn 458 ff.

[452] S. zum Beweisverwertungsverbot bei Unzulässigkeit der Speicherung von Verkehrsdaten zum Zeitpunkt der Auskunftserteilung durch einen Access-Provider *OLG Karlsruhe,* Urt. v. 4.12.2008 - 4 U 86/07, MMR 2009, 412, 413.

Bei Datenschutzregelungen, die die Erhebung sensibler Daten nur unter besonderen Voraussetzungen erlauben, ist ein Beweisverwertungsverbot regelmäßig anzunehmen, damit nicht der Schutzzweck dieser Normen umgangen wird.[453] Das muss insbesondere gelten, wenn das Fernmeldegeheimnis oder das allgemeine Persönlichkeitsrecht des Internetnutzers dadurch beeinträchtigt wird.[454]

E. Vergleich der Auskunftsmöglichkeiten de lege lata

Die obigen Ausführungen weisen auf erhebliche Unterschiede der de lege lata existierenden Auskunftsmöglichkeiten je nach beeinträchtigtem Rechtsgut und Art der Rechtsverletzung hin. Diese ergeben sich in erster Linie aus den verschiedenen Anspruchsgrundlagen für einen Auskunftsanspruch gegen Internetdiensteanbieter. Zudem variieren auch die Regelungen zur Lösung des Konflikts mit dem Datenschutzrecht und die prozessualen Rahmenbedingungen. Dabei erscheint die unterschiedliche Behandlung größtenteils nicht gerechtfertigt.

I. Anspruchsgrundlage

Zunächst existierten nur im Bereich des geistigen Eigentums mit § 101 UrhG, § 19 MarkenG, § 140b PatG, § 24b GebrMG, § 46 DesignG, § 37b SortenSchuG und § 9 Abs. 2 HalblSchG speziell geregelte Anspruchsgrundlagen für einen Drittauskunftsanspruch gegen Internetdiensteanbieter. Mit § 21 Abs. 2 S. 2 TTDSG wurde inzwischen aber auch eine Anspruchsgrundlage bei der Verletzung sonstiger absoluter Rechte eingeführt. Allerdings ist diese Anspruchsgrundlage auf bestimmte rechtswidrige Inhalte beschränkt. Bei allen anderen Verletzungen absoluter Rechte kann weiterhin nur auf den allgemeinen Auskunftsanspruch aus § 242 BGB zurückgegriffen werden.

Im Bereich des geistigen Eigentums sind die Auskunftsansprüche dagegen nicht auf bestimmte Arten von Rechtsverletzungen beschränkt. Dabei ist im Bereich des geistigen Eigentums das Regelungsbedürfnis nicht grundsätzlich höher als bei anderen Rechtsverletzungen. Auch wenn man auf die hohen

---

[453] *Brüggemann,* Drittauskunftsanspruch, S. 317.

[454] *Bacher* in: BeckOK ZPO, Rn. 21.

wirtschaftlichen Schäden abstellt, die vor allem Urheberrechtsverletzungen im Internet für die Rechteinhaber bewirken, lässt sich nicht erklären, warum beispielsweise im Halbleiterschutzgesetz ein spezieller Auskunftsanspruch normiert ist. Während kein einziger Anwendungsfall von Verstößen gegen das HalblSchuG im Zusammenhang mit anonymen Rechtsverletzungen im Internet bekannt ist, gehören vor allem Persönlichkeitsrechtsverletzungen, aber auch Verletzungen des Rechts am eingerichteten und ausgeübten Gewerbebetrieb im Internet leider zum Alltag.

II. Passivlegitimation

Die Anspruchsgrundlagen unterscheiden sich zudem im Hinblick auf die Passivlegitimation. Je nach Anspruchsgrundlage können nur bestimmte Diensteanbieter zu einer Auskunft verpflichtet werden.

§ 21 Abs. 2 S. 2 TTDSG ist beschränkt auf die Anbieter von Telemediendiensten beschränkt. Leider werden daher weder Over-the-top-Anwendungsdienste noch Access-Provider vom Anwendungsbereich der Norm erfasst.

Anders verhält sich dies bei den Auskunftsansprüchen aus § 101 UrhG, § 19 MarkenG, § 140b PatG, § 24b GebrMG, § 46 DesignG, § 37b SortenSchuG und § 9 Abs. 2 HalblSchG. Hier kann im Einzelfall zwar das Gewerbsmäßigkeitserfordernis eine Hürde darstellen, ansonsten adressieren diese Ansprüche grundsätzlich alle Diensteanbieter, deren Dienstleistungen für rechtsverletzende Tätigkeiten genutzt werden – also insbesondere auch Telekommunikationsdienste wie Access-Provider. Dienste, die nicht zur konkreten Rechtsverletzung genutzt wurden, werden anders als bei § 21 Abs. 2 S. 2 TTDSG aber nicht erfasst.

§ 242 BGB knüpft wiederum an die Verantwortlichkeit der Diensteanbieter als Störer an, sodass etwa Access-Provider und WLAN-Betreiber von vorneherein nicht als Anspruchsgegner in Betracht kommen.

Ohne die Inanspruchnahme des Access-Providers ist eine Identifizierung des Rechtsverletzers mittels IP-Adresse in aller Regel nicht möglich. Diese Möglichkeit bei Rechtsverletzungen außerhalb des geistigen Eigentums von vornherein auszuschließen, überzeugt nicht. Die Identifizierung über die IP-Adresse kann bei allen Rechtsverletzungen im Internet relevant werden. Es lässt sich keine

pauschale Aussage darüber treffen, bei welchen Rechtsverletzungen eine Identifizierung mittels bei Telemediendiensteanbietern gespeicherten Bestandsdaten gelingen kann. Sicherlich hat sich vor allem bei den Filesharing-Fällen die Auskunftserteilung mittels IP-Adresse als essenziell für die Rechtsdurchsetzung erwiesen. Allerdings verfügen die Anbieter von Telemedien, deren Dienste etwa zur Verletzung von Persönlichkeitsrechten oder des Rechts am eingerichteten und ausgeübten Gewerbebetrieb genutzt werden, ebenso häufig nicht über Bestandsdaten, die die Aufdeckung der Identität der Nutzer ermöglichen würden. Auch in diesen Fällen könnte daher die IP-Adresse eine entscheidende Rolle bei der Identifizierung der Rechtsverletzer spielen.

III. Voraussetzungen der Ansprüche

Die Verschiedenheit der Auskunftsansprüche bewirkt darüber hinaus, dass die Möglichkeit, Auskunft durch die Diensteanbieter zu erlangen, an unterschiedliche Voraussetzungen geknüpft ist.

Die Auskunftsansprüche zur Identifizierung der Rechtsverletzer nach § 101 UrhG, § 19 MarkenG, § 140b PatG, § 24b GebrMG, § 46 DesignG, § 37b SortenSchuG und § 9 Abs. 2 HalblSchG greifen nur bei offensichtlichen Rechtsverletzungen, erfassen dabei aber grundsätzlich sämtliche Verletzungen des geistigen Eigentums.

Im Unterschied dazu ist § 21 Abs. 2 S. 2 TTDSG auf bestimmte – meist die Grenzen der Strafbarkeit überschreitende – rechtsverletzende Inhalte beschränkt. Anders als bei den Anspruchsgrundlagen im Bereich des geistigen Eigentums besteht ein Anspruch auch bei unklarer Rechtslage beziehungsweise, wenn die Rechtsverletzung nicht offensichtlich ist.

Die Voraussetzungen des allgemeinen Auskunftsanspruchs aus § 242 BGB dürften – abgesehen von der Notwendigkeit einer rechtlichen Sonderbeziehung – häufig wohl keine größere Hürde für die Rechteinhaber darstellen. Allerdings ist der Anwendungsbereich dieser Vorschrift durch die speziellen Ansprüche stark beschränkt.

Das Kriterium der Offensichtlichkeit kann eine nicht unerhebliche Hürde für die Rechteinhaber darstellen und überzeugt nicht für die Eingrenzung des

Auskunftsanspruchs. Darüber hinaus zeigt sich ein Widerspruch im Vergleich mit den Fallkonstellationen, für die sich der Auskunftsanspruch aus § 21 Abs. 2 S. 2 TTDSG oder § 242 BGB ergibt. Vor allem Persönlichkeitsrechtsverletzungen, aber auch Verletzungen des Rechts am eingerichteten und ausgeübten Gewerbebetrieb lassen sich ebenfalls nicht immer auf den ersten Blick beurteilen, da diese häufig eine Abwägung kollidierender Interessen im Einzelfall voraussetzen. Die Diensteanbieter sind hier verglichen mit Verletzungen von IP-Rechten im Internet ebenso mit dem Risiko der Fehlbeurteilung konfrontiert.

Dieselbe Problematik wird aber im Rahmen der Auskunftsansprüche unterschiedlich behandelt. Während die Auskunftsansprüche im Bereich des geistigen Eigentums eine Eingrenzung des Anspruchs auf offensichtliche Rechtsverletzungen vorsehen, wird im Rahmen des Auskunftsanspruchs aus § 21 Abs. 2 S. 2 TTDSG diesem Problem vor allem durch den generellen Richtervorbehalt Abhilfe geleistet.

IV. Umfang des Auskunftsanspruchs

Die Verschiedenheit der Anspruchsgrundlagen führt auch zu einer unterschiedlichen Reichweite der Auskunftsansprüche. Im Bereich des geistigen Eigentums erstreckt sich der Auskunftsanspruch gegen Internetdiensteanbieter nur auf Namen und Anschrift des Nutzers. Problematisch ist zudem, dass vom Wortlaut des § 19 MarkenG eine Auskunft über den Nutzer der Dienstleistungen nicht erfasst wird. Dass demgegenüber der in der Praxis deutlich weniger relevante Anspruch aus dem HalblSchuG die entsprechende Passage enthält, überzeugt daher nicht.

Der allgemeine Anspruch aus § 242 BGB ist in dieser Hinsicht nicht beschränkt und umfasst alle Informationen und Daten, die zur Identifizierung des Rechtsverletzers nützlich sein können. Einschränkungen ergeben sich hierbei erst unter Hinzuziehung der datenschutzrechtlichen Regelungen.

§ 21 Abs. 2 S. 2 TTDSG umfasst alle Bestandsdaten – also zum Beispiel auch Telefonnummern, Kontodaten und E-Mail-Adressen –, soweit sie zur Identifizierung des Nutzers erforderlich sind.

Demgegenüber überzeugt die Eingrenzung des Anspruchsumfangs im Bereich des geistigen Eigentums nicht. Vor allem Anwendungsdienste unterscheiden sich sehr ihrer Speicherpraxis. Häufig werden zum Beispiel nur die E-Mail-Adressen der Nutzer erhoben. Zudem existieren zumindest derzeit keine Registrierungs- oder Speicherpflichten, sodass die Auskunftsansprüche hinsichtlich der Bestandsdatenauskunft möglichst weit gefasst sein sollten.

Nutzungs- bzw. Verkehrsdaten wie die (dynamische) IP-Adresse oder Datum und Uhrzeit der Verbindung werden weder vom Umfang des Anspruchs § 21 Abs. 2 S. 2 TTDSG, noch von den Ansprüchen im Bereich des geistigen Eigentums erfasst.

V. Prozessuale Rahmenbedingungen

Der größte Unterschied hinsichtlich der prozessualen Rahmenbedingungen der Auskunftsansprüche besteht hinsichtlich des Richtervorbehalts. Im Bereich des geistigen Eigentums ist das richterliche Gestattungsverfahren nur bei der Verwendung von Verkehrsdaten erforderlich. Im Rahmen des Verfahrens nach § 21 Abs. 3-4 TTDSG wird dagegen bereits für die reine Bestandsdatenauskunft eine richterliche Anordnung vorausgesetzt.[455]

Sinnvollerweise wird im Rahmen des Verfahrens nach § 21 Abs. 3 TTDSG direkt über die Verpflichtung zur Auskunftserteilung mitentschieden (S. 2). Anders verhält sich dies aber beim Gestattungsverfahren nach § 101 Abs. 9 UrhG (und der Parallelvorschriften im Bereich des geistigen Eigentums).

In den Gestattungsverfahren besteht zudem die Möglichkeit einer einstweiligen Anordnung nach §§ 49 ff. FamFG. Darüber hinaus sehen die Auskunftsansprüche im Bereich des geistigen Eigentums in Absatz 7 die Möglichkeit der Auskunftserteilung im Wege der einstweiligen Verfügung vor.

Für die unterschiedlichen prozessualen Rahmenbedingungen der Auskunftsansprüche gibt es keinen sachlichen Grund. Im Hinblick auf die Interessenslage, insbesondere im Hinblick auf den Schutz von Nutzerdaten sowie auf die Missbrauchsgefahr, unterscheiden sich die Ansprüche nicht. Entsprechend wäre ein

---

[455] Vgl. *Bohlen*, NJW 2020, 1999, 2003.

einheitlicher prozessualer Rahmen für Auskunftsansprüche gegen Internetdiensteanbieter zur Identifizierung anonymer Rechtsverletzer sinnvoll.

VI. Regelung des Konflikts mit dem Datenschutzrecht

Ein Hauptproblem bei der Durchsetzung der Auskunftsansprüche gegen Internetdiensteanbieter stellt für die Rechteinhaber das Fehlen datenschutzrechtlicher Erlaubnisnormen dar. So ist etwa die Auskunftserteilung durch den Access-Provider anhand der IP-Adresse mangels datenschutzrechtlicher Erlaubnis unzulässig. Dasselbe gilt grundsätzlich für die Auskunftserteilung der Anwendungsdienste, soweit Verkehrs- oder Nutzungsdaten verarbeitet werden. Insgesamt fehlt es an Vorschriften, die eine Speicherung personenbezogener Daten zum Zwecke der Auskunftserteilung an private Rechteinhaber ermöglichen würden.

Dennoch existieren mit § 21 Abs. 2 S. 1 TTDSG und § 21 Abs. 1 TTDSG, aber auch § 24 Abs. 1 S. 1 Nr. 2 BDSG datenschutzrechtliche Normen, die die dazugehörigen Auskunftsansprüche ergänzen. Auch hier zeigt sich wieder der eben bereits kritisierte Unterschied bei der Bestandsdatenauskunft: Nach § 21 Abs. 3 S. 1 TTDSG bedarf es für die Zulässigkeit der Auskunftserteilung nach § 21 Abs. 2 TTDSG einer richterlichen Anordnung. Dagegen ist eine solche im Bereich des geistigen Eigentums nach der Vorschrift des § 21 Abs. 1 TTDSG – wenngleich diese in der Auslegung des Merkmals der „Anordnung der zuständigen Stelle“ nicht unproblematisch ist – nicht erforderlich.

F. Gesamtbetrachtung der Auskunftsmöglichkeiten

Die voranstehenden Untersuchungen zeigen, dass die Identifizierung von anonymen Rechtsverletzern im Internet mittels eines Auskunftsanspruchs die Rechteinhaber de lege lata vor erhebliche Schwierigkeiten stellen kann. Aus der Gesamtbetrachtung der verschiedenen Anspruchsvoraussetzungen in Kombination mit den datenschutzrechtlichen Regelungen ergibt sich, dass nur in wenigen Fällen eine Auskunftserteilung zur Identifizierung eines rechtsverletzenden Internetnutzers überhaupt rechtlich möglich ist.

Die Identifizierung eines Nutzers anhand der IP-Adresse ist generell unzulässig, da es jedenfalls an der erforderlichen Rechtsgrundlage für die Auskunftserteilung durch den Access-Provider mangelt. Das führt dazu, dass derzeit lediglich Auskunftsansprüche gegen Anwendungsdienste denkbar sind, da die Rückverfolgung eines Nutzers anhand der IP-Adresse bereits daran scheitert, dass der Anschlussinhaber nicht ermittelt werden kann.

Aber auch die Anwendungsdienste dürfen in der Regel Nutzungs- und Verkehrsdaten nicht zur Auskunftserteilung an die Rechteinhaber verarbeiten. Außerdem ist sogar die reine Bestandsdatenauskunft durch Telekommunikationsdienste de lege lata mangels datenschutzrechtlicher Erlaubnis für die zweckändernde Weiterverarbeitung unzulässig. Zielführend können deshalb lediglich die Auskunftsansprüche gegen Telemediendienste oder sonstige (Anwendungs-)Dienste sein.

Im Ergebnis verbleiben dadurch lediglich fünf in der Praxis denkbare Konstellationen, in denen das Auskunftsbegehren eines Rechteinhabers sowohl die Voraussetzungen einer Anspruchsgrundlage erfüllt als auch den datenschutzrechtlichen Anforderungen genügt:

– Im Falle einer Urheberrechtsverletzung können die Rechteinhaber die Anbieter von Telemediendiensten nach § 101 UrhG i.V.m § 21 Abs. 1 TTDSG auf Auskunft in Anspruch nehmen. Dieser Anspruch erstreckt sich allerdings lediglich auf Namen und Anschrift des anonymen Nutzers und setzt voraus, dass der Anwendungsdienst Kenntnis von den entsprechenden Bestandsdaten hat. Das kann etwa der Fall sein, wenn urheberrechtlich geschütztes Material über eine Plattform – zum Beispiel in Form von user generated content – verbreitet wird. Anspruchsgrundlage sollte aber in der Regel § 101 Abs. 2 UrhG sein. Deshalb muss die Rechtsverletzung offensichtlich sein und der Anwendungsdienst in gewerblichem Ausmaß erbracht werden.

– Ähnlichen Voraussetzungen unterliegt auch der Anspruch aus § 19 MarkenG i.V.m. § 21 Abs. 1 TTDSG. In der Praxis ist dieser Anspruch zum Beispiel bei Markenrechtsverletzungen auf Online-Marktplätzen relevant. Die Plattform ist in diesem Fall zur Auskunft über Namen und Adresse des

rechtsverletzenden Nutzers verpflichtet, sofern sie über diese Informationen verfügt.

– Sofern eine Kennzeichenrechtsverletzung im Zusammenhang mit der Domain-Vergabe erfolgt, können die Rechteinhaber nach § 19 MarkenG i.V.m. § 24 Abs. 1 S. 1 Nr. 2 BDSG Auskunft über Namen und Anschrift des Domaininhabers etwa durch die DENIC, den zuständigen Domain-Registrar, den Anbieter einer Privacy Domain oder den Admin C verlangen.

– Bei sonstigen Namensrechtsverletzung im Zusammenhang mit der Domain-Vergabe können dieselben Diensteanbieter nach § 242 BGB i.V.m. § 24 Abs. 1 S. 1 Nr. 2 BDSG auf Auskunft über den Domaininhaber in Anspruch genommen werden. Das gilt allerdings nur, wenn die Diensteanbieter als Störer für die Rechtsverletzung haften.[456]

– Bei Rechtsverletzungen aufgrund rechtswidriger Nutzerinhalte im Sinne des § 1 Abs. 3 NetzDG oder § 10a Abs: 1 TMG besteht ein Anspruch gegen Telemediendiensteanbieter auf Auskunft über sämtliche erforderliche Bestandsdaten aus § 21 Abs. 2 S. 2 TTDSG i.V.m. § 21 Abs. 2 S. 1 TTDSG. Nach § 21 Abs. 3-4 TTDSG ist dafür aber eine gerichtliche Anordnung erforderlich.

G. Zusammenfassung Kapitel 5

Die Untersuchung der de lege lata bestehenden Auskunftsmöglichkeiten zur Identifizierung eines anonymen Rechtsverletzers im Internet zeigt, dass das System der Auskunftsansprüche in vielerlei Hinsicht widersprüchlich und nicht aufeinander abgestimmt ist. Häufig reichen die bestehenden Auskunftsmöglichkeiten nicht aus oder es besteht überhaupt keine Möglichkeit, einen anonymen Rechtsverletzer zu identifizieren.

Die Auskunftsansprüche und die datenschutzrechtlichen Vorschriften sind nicht hinreichend an die besondere Situation anonymer Rechtsverletzungen im

[456] S. dazu etwa *BGH*, Urt. v. 27.10.2011 – I ZR 131/10, NJW 2012, 2279 – regierung-oberfranken.de.

Internet angepasst und dadurch nicht geeignet, die widerstreitenden Interessen zu einem angemessenen Ausgleich zu bringen.

Die aufgezeigten Defizite der Auskunftsansprüche gehen zu Lasten der Rechtsdurchsetzung der Rechteinhaber und führen dazu, dass ein Großteil der Verantwortung der Nutzer für ihre Inhalte auf die Diensteanbieter übertragen wird. Das Auskunftsrecht in diesem speziellen Bereich ist daher reformbedürftig, um die Möglichkeiten der Rechtsdurchsetzung im Online-Bereich zu verbessern und Widersprüche zu vermeiden. Dabei erscheint es notwendig, die Voraussetzungen und Rechtsfolgen der Auskunftsansprüche an die besondere Situation im Internet anzupassen, sowie die erforderlichen einheitlichen datenschutzrechtlichen und prozessualen Rahmenbedingungen für die Identifizierung anonymer Rechtsverletzer zu schaffen.

Kapitel 6

Untersuchung alternativer Möglichkeiten der Rechtsdurchsetzung

Die Notwendigkeit, de lege ferenda weitergehende Auskunftsansprüche zur Identifizierung anonymer Rechtsverletzer zu schaffen, besteht nur, wenn keine sinnvollen Alternativen existieren, die eine effektive Rechtsdurchsetzung ermöglichen und die widerstreitenden Interessen der Diensteanbieter, Nutzer und Rechteinhaber zu einem angemessenen Ausgleich bringen.

Im Folgenden wird deshalb die Identifizierung anonymer Rechtsverletzer über den Umweg der Akteneinsicht im Strafverfahren (A.) dargestellt. Außerdem wird untersucht, ob die Identifizierung der unmittelbaren Rechtsverletzer dadurch ersetzt werden kann, dass stattdessen die Diensteanbieter in die Verantwortung genommen werden (B.).

A. Identifizierung über den Umweg der Strafverfolgung

Wie die Analyse in Kapitel 5 gezeigt hat, können die Rechteinhaber anonyme Rechtsverletzer auf dem Zivilrechtsweg häufig nicht identifizieren. Selbst wenn dies im Einzelfall möglich wäre, ist die Identifizierung auf dem Zivilrechtsweg für die Rechteinhaber aufwändig und mit nicht unerheblichen Kosten verbunden.

Versuche der Rechteinhaber, die Identität eines rechtsverletzenden Internetnutzers anstelle durch Auskunftserteilung der Diensteanbieter auf der Grundlage zivilrechtlicher Auskunftsansprüche durch Akteneinsicht im Strafverfahren zu identifizieren, sind daher naheliegend.

I. Anfangsverdacht

Die Staatsanwaltschaft ist nach dem Legalitätsgrundsatz gemäß § 152 Abs. 2 StPO verpflichtet zu ermitteln, wenn der Anfangsverdacht einer Straftat besteht. Dafür muss die Staatsanwaltschaft aber überhaupt Kenntnis von einem möglicherweise strafbaren Verhalten erhalten.

Das kann zum Beispiel durch eine Meldung nach dem NetzDG erfolgen. Soziale Netzwerke sind nach § 3a NetzDG verpflichtet bestimmte rechtswidrige Inhalte an das Bundeskriminalamt als zentrale Stelle zu melden.[1] Dazu zählen insbesondere Straftaten, bei denen ein großes öffentliches Interesse an der Strafverfolgung besteht. Vor allem bei Straftaten wie der Volksverhetzung, der Gewaltdarstellung, der Belohnung oder Billigung von Straftaten, dem Verbreiten kinderpornographischer Inhalte oder der Bedrohung kann es gleichzeitig aber auch zu einer Verletzung absoluter Rechte eines Individuums kommen. Die Verpflichtung zur Meldung solcher strafbarer Inhalte besteht, wenn die Nutzer in Form einer Beschwerde die Inhalte nach § 3 NetzDG gemeldet haben und die Anbieter des sozialen Netzwerks die Inhalte entfernt oder gesperrt haben Eine Meldepflicht für Hosting-Dienste beim Verdacht auf Straftaten, die eine Gefahr für das Leben oder die Sicherheit einer Person darstellen, sieht Art. 18 DSA vor.

Häufig erfolgt die Kenntnisnahme der Strafverfolgungsbehörden aber auch mittels einer Strafanzeige gegen Unbekannt durch die betroffenen Rechteinhaber.[2] Bei einigen im Online-Bereich besonders relevanten Delikten handelt es sich ohnehin um relative oder absolute Antragsdelikte (s. zum Beispiel § 109 UrhG, § 143 Abs. 4 MarkenG, § 194 StGB, § 205 Abs. 1 StGB). Der erforderliche Strafantrag geht häufig mit der Anzeigeerstattung durch die Rechteinhaber einher.[3]

II. Identitätsfeststellung durch die Staatsanwaltschaft

Hat die Staatsanwaltschaft Kenntnis von einer möglichen Rechtsverletzung erhalten und besteht der Anfangsverdacht einer Straftat, obliegt es ihr, die

---

[1] § 3a NetzDG wird allerdings teilweise als mit dem Unionsrecht nicht vereinbar angesehen. S. dazu etwa *VG Köln*, Beschl. v. 01.03.2022 – 6 L 1277/21, MMR 2022, 330 Rn. 155 ff.

[2] S. dazu auch *Brüggemann*, Drittauskunftsanspruch, S. 389.

[3] S. auch *Welp*, Auskunftspflicht von Access-Providern, S. 323.

Identität des Täters im Rahmen der allgemeinen Sachverhaltsaufklärungspflicht nach § 160 StPO festzustellen.

Bei der Meldung an das Bundeskriminalamt nach § 3a NetzDG müssen die Anbieter sozialer Netzwerke neben dem Inhalt auch weitere Informationen wie Zugriffszeiten, Nutzername und IP-Adresse des Nutzers übermitteln (§ 3a Abs. 4 NetzDG). Diese Daten können die Grundlage für die Identifizierung des Täters durch die Strafverfolgungsbehörden bilden.

Die Staatsanwaltschaft kann im Unterschied zu den Rechteinhabern bei der Identifizierung eines Täters im Internet auf besondere Ermittlungsbefugnisse zurückgreifen. Zum Beispiel dürfen nach § 100g Abs. 1 S. 1 Nr. 2 StPO Verkehrsdaten erhoben werden, wenn eine Straftat mittels Telekommunikation begangen wurde. Dies erstreckt sich auf alle Straftaten, die im Wege der Kommunikation im Internet begangen werden, und zwar unabhängig von ihrer Schwere.[4] Werden Kommunikationsmittel wie das Internet zur Begehung von Straftaten eingesetzt, reduziert sich für die Nutzer der Schutz der Vertraulichkeit des „missbrauchten Mediums."[5] Zudem kann die Aufklärung von Straftaten, die mittels Telekommunikation begangen wurden, häufig nur durch einen Zugriff auf Verbindungsdaten gelingen.[6] Auf Daten, die im Rahmen der Vorratsdatenspeicherung nach § 176 TKG verarbeitet wurden, darf aber nur bei schweren Straftaten im Sinne des § 100g Abs. 2 StPO zurückgegriffen werden.[7]

III. Verweis auf Privatklageweg und Einstellung des Verfahrens

Eine Akteneinsicht durch die Rechteinhaber ist nur zielführend, wenn die Staatsanwaltschaft zuvor überhaupt Ermittlungen zur Identität des Nutzers angestellt hat.

Einige der Delikte, die im Online-Bereich besonders relevant sind, stellen aber Privatklagedelikte im Sinne des § 374 Abs. 1 StPO dar. Das betrifft insbesondere

---

[4] S. etwa *Bär* in: BeckOK StPO, § 100g StPO Rn. 9.

[5] *BVerfG*, Beschl. v. 17.6.2006 - 2 BvR 1085/05 u.a., NJW 2006, 3198 Rn. 17.

[6] *BVerfG*, Beschl. v. 17.6.2006 - 2 BvR 1085/05 u.a., NJW 2006, 3198 Rn. 17; S. auch *Wollweber*, NJW 2002, 1554.

[7] Die Verfassungs- und Unionsrechtskonformität der nationalen Regelungen zur Vorratsdatenspeicherung ist allerdings noch offen.

Ehrverletzungsdelikte (§§ 185-189 StGB), die Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen (§ 201a StGB), die Bedrohung (§ 241 Abs. 1-3 StGB), sowie Straftaten nach § 144 Abs. 1, 2 MarkenG oder §§ 106-108 UrhG und § 108b Abs. 1, 2 UrhG oder § 33 KunstUrhG. Liegen Hinweise auf ein solches Delikt vor, wird die Staatsanwaltschaft nach § 376 StPO - sofern das öffentliche Interesse nicht entgegensteht - den Rechtinhaber auf den Privatklageweg verweisen und das Verfahren nach § 170 Abs. 2 StPO einstellen.[8]

Grundsätzlich ist die Staatsanwaltschaft im Privatklageverfahren nach § 377 StPO nicht zur Mitwirkung verpflichtet. Allerdings sollen die Staatsanwaltschaften dennoch die erforderlichen Ermittlungen nach Abschnitt 87 Abs. 2 S. 1 RiStBV anstellen, wenn der Verletzte die Straftat nicht oder nur unter großen Schwierigkeiten aufklären könnte. In diesem Fall wäre es dem Verletzten nicht zuzumuten, Privatklage zu erheben. Die Staatsanwaltschaft soll deshalb erst nach den erforderlichen Ermittlungen auf den Privatklageweg verweisen.

Sofern den Rechteinhabern eigene Auskunftsansprüche gegen die Diensteanbieter zur Identifizierung eines Internetnutzers zur Verfügung stehen, kann von einer Zumutbarkeit der Privatklage ausgegangen werden.[9] Bestehen aber keine eigenen oder nur sehr unzureichende Identifizierungsmöglichkeiten, sollten zunächst Ermittlungen durch die Staatsanwaltschaft durchgeführt werden. Bei unbedeutenden Verfehlungen im Sinne des Abschnitt 87 Abs. 2 S. 2 RiStBV gilt dies allerdings nicht.[10]

Häufig kommt es bei geringfügigen Straftaten im Internet auch zur Einstellung des Verfahrens nach § 153 Abs. 1 StPO oder unter Zahlung einer Geldauflage nach § 153a StPO.[11] Für die Rechteinhaber ist die Einstellung nach § 153 Abs. 1

---

[8] S. auch *Beck/Kreißig*, NStZ 2007, 304, 308; *Sahl/Bielzer*, ZRP 2020, 2, 3 ff.; *Welp*, Auskunftspflicht von Access-Providern, S. 325.

[9] S. dazu auch *Welp*, Auskunftspflicht von Access-Providern, S. 326.

[10] S. dazu Brüggemann, Drittauskunftsanspruch, S. 395; Schmidt, GRUR 2010, 673, 675.

[11] S. insbesondere zur Verfahrenseinstellung beim Filesharing *Brüggemann*, Drittauskunftsanspruch, S. 394; *Kindt*, MMR 2009, 147, 147; *Solmecke*, K&R 2007, 138, 142. S. zur Verfahrenseinstellung bei Persönlichkeitsrechtsverletzungen *Bohlen*, NJW 2020, 1999, 1999; S.

StPO vor allem dann problematisch, wenn zuvor keine Ermittlungen zur Identität des Täters durchgeführt wurden. Dadurch wird ihnen die Möglichkeit versperrt, durch Akteneinsicht den Rechtsverletzer zu identifizieren.

IV. Akteneinsichtsrecht

Wenn die Staatsanwaltschaft Ermittlungen zur Identität des Täters im Internet angestellt hat, können die Rechteinhaber Einsicht in die Ermittlungsakten nehmen.

Ein Recht zur Akteneinsicht steht nach § 385 Abs. 3 StPO dem Privatkläger zu. Dafür müssten die Rechteinhaber aber auch tatsächlich Privatklage erheben, selbst wenn sie eigentlich kein Interesse an der Strafverfolgung des Nutzers haben.

Daher steht die Akteneinsicht in den Fällen im Vordergrund, in denen die Rechteinhaber im Anschluss an die Untersuchungen der Staatsanwaltschaft diese beantragen. Ein Rechtsanwalt kann gemäß § 406e Abs. 1 StPO für den Verletzten Einsicht in die Ermittlungsakten nehmen, sofern ein berechtigtes Interesse daran besteht. Die Durchsetzung zivilrechtlicher Ansprüche stellt ein solches berechtigtes Interesse dar.[12] Sofern der Verletzte nach § 395 StPO befugt ist, sich als Nebenkläger einer erhobenen öffentlichen Klage oder einem Antrag im Sicherungsverfahren anzuschließen, muss er kein berechtigtes Interesse darlegen (§ 406e Abs. 1 S. 2 StPO).

V. Akteneinsicht als Alternative zu zivilrechtlichen Auskunftsansprüchen?

Das Recht auf Akteneinsicht im Strafverfahren kann dazu beitragen, dass die Rechteinhaber auch ohne zivilrechtliche Auskunftsansprüche einen anonymen Rechtsverletzer identifizieren können. Nicht selten kann es bei Delikten im Internet aber zur Einstellung des Verfahrens beziehungsweise zu einem Verweis auf den Privatklageweg kommen, ohne dass zuvor die Staatsanwaltschaften die erforderlichen Ermittlungen durchgeführt haben. Der Weg einer

---

allgemein zur Interessensabwägung im Rahmen des § 406e StPO *BVerfG*, Beschl. v. 5.12.2006 - 2 BvR 2388/06, NJW 2007, 1052, 1053.

[12] *LG Saarbrücken*, Beschl. v. 2.7.2009 - 2 Qs 11/09, NStZ 2010, 111, 112; *LG Hildesheim*, Beschl. v. 6.2.2009 - 25 Qs 1/09, NJW 2009, 3799, 3800; *Schmidt,* GRUR 2010, 673, 675 f.

Identifizierung der Rechtsverletzer über die Akteneinsicht nach § 406e StPO führt die Rechteinhaber deshalb vor allem bei Rechtsverletzungen von geringerer Intensität nicht immer zum Ziel.[13] Schon allein deswegen stellt die Identifizierung anonymer Rechtsverletzer über die Akteneinsicht im Strafverfahren keine Alternative zu zivilrechtlichen Auskunftsansprüchen dar. Außerdem überschreiten viele Verletzungen absoluter Rechte im Internet die Schwelle zur Strafbarkeit nicht, sodass in diesen Fällen schon kein Anfangsverdacht besteht, der zu Ermittlungen der Strafverfolgungsbehörden führen würde.[14]

Die Identifizierung der Rechtsverletzer über den Umweg der Akteneinsicht im Strafverfahren ist aber auch rechtspolitisch oft nicht sinnvoll. Häufig steht bei den Rechteinhabern das Interesse an einer Strafverfolgung des Nutzers nicht im Vordergrund.[15] In vielen Fällen geht es vielmehr um die Identifizierung der Nutzer, um anschließend zivilrechtliche Ansprüche geltend machen zu können. Natürlich stellt die Akteneinsicht in die Ermittlungsakten grundsätzlich ein legitimes Instrument der Rechteinhaber dar. Allerdings tragen die Rechteinhaber zum Beispiel im zivilrechtlichen Gestattungsverfahren nach § 101 Abs. 9 UrhG oder § 21 Abs. 3 TTDSG – anders als bei einer Ermittlung durch die Staatsanwaltschaft – die Kosten für die Identifizierung der Rechtsverletzer.[16] Daher besteht die Gefahr, dass das Akteneinsichtsrecht missbraucht wird, um die kostenintensivere Identifizierung auf dem Zivilrechtsweg zu umgehen.[17] Das gilt aber natürlich nur insoweit, als überhaupt Möglichkeiten der Identifizierung auf dem Zivilrechtsweg bestehen.

---

[13] So auch *Kitz*, GRUR 2003, 1014, 1017 f.; *Kramer*, Zivilrechtlicher Auskunftsanspruch, S. 62.

[14] Vgl. *Pille*, NJW 2018, 3545, 3546.

[15] *Brüggemann*, Drittauskunftsanspruch, S. 389; *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 176; *Sankol*, K&R 2008, 509, 510; *Schmidt*, GRUR 2010, 673, 675.

[16] S. im Hinblick auf das Verfahren nach § 101 Abs. 9 UrhG *Brüggemann,* Drittauskunftsanspruch, S. 389; *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 176; *Sandor,* Datenspeicherung, Rn. 261.

[17] S. *Sandor*, Datenspeicherung, Rn. 261, der auf die Diskrepanz der Kostentragungsregel und der Akteneinsicht hinweist. S. zur Kritik an der „Instrumentalisierung der Strafverfolgungsbehörden" in Filesharing-Fällen *Kondziela*, MMR 2009, 295, 295. Ähnlich auch *Bär*, MMR 2007, 811, 813; *Hoeren*, NJW 2008, 3099, 3200; *Sankol*, MMR 2008, 482, 483; *Schwarz/Brauneck*, ZUM 2006, 701, 702 f.

Die massenhaften Rechtsverletzungen im Internet können aber nicht alle durch die Strafverfolgungsbehörden verfolgt werden.[18] Zudem steht der Aufwand der Strafverfolgung bei anonymen Tätern im Internet oft nicht in Relation zum eher geringen öffentlichen Interesse an der Strafverfolgung.[19] Das gilt zum Beispiel bei einigen Urheberrechtsverletzungen nach §§ 106-108, 108b UrhG, Markenrechtsverletzungen nach § 144 Abs. 1, 2 MarkenG oder bei einfachen Ehrverletzungsdelikten oder Taten im Sinne des § 201a StGB. Solche Delikte sind Massenphänomene im Internet. Da vor allem die Täterermittlung im Online-Bereich sehr umfassender Ermittlungsarbeit bedarf, wäre die Verfolgung aller Delikte im Internet nicht darstellbar.[20] Um die Strafverfolgungsbehörden mit der Verfolgung von weniger schweren Delikten im Internet nicht übermäßig zu belasten, wäre es daher zweckmäßige, den Rechteinhabern selbst die Mittel zu gewähren, die eine Rechtsdurchsetzung auf dem Zivilrechtsweg ermöglichen.

Um einem Missbrauch des Akteneinsichtsrechts vorzubeugen, könnte man bei solchen Delikten im Gegenzug § 406e Abs. 1 S. 1 StPO so auslegen, dass kein berechtigtes Interesse besteht, wenn den Rechteinhabern die Identifizierung des Nutzers über den Zivilrechtsweg möglich und zumutbar ist.[21] Ebenfalls können schutzwürdige Interessen des Beschuldigten (Fernmeldegeheimnis, Recht auf informationelle Selbstbestimmung)[22] dem Informationsinteresse nach § 406e Abs. 2 StPO überwiegen, wenn die Rechteinhaber offensichtlich kein Interesse an dessen Strafverfolgung haben, sondern lediglich die Identifizierungsmöglichkeiten der Staatsanwaltschaft für einen späteren Zivilprozess ausnutzen wollen.[23] Sofern die Rechteinhaber de lege ferenda über Mittel der Identifizierung

---

[18] So auch *Pfeifer*, CR 2017, 809, 811.

[19] Vgl. *Bohlen,* NJW 2020, 1999, 1999.

[20] Vgl. *Bohlen,* NJW 2020, 1999, 1999.

[21] Ähnlich *Sankol,* K&R 2008, 509, 512 f.; *Welp*, Auskunftspflicht von Access-Providern, S. 332 ff.

[22] S. dazu *BVerfG*, Beschl. v. 5.12.2006 - 2 BvR 2388/06, NJW 2007, 1052, 1052; S. auch *Brüggemann*, Drittauskunftsanspruch, S. 397.

[23] Vor allem bei Urheberrechtsverstößen im Zusammenhang mit dem P2P-Filesharing wurde unter anderem aus diesem Grund teilweise die Interessensabwägung zugunsten des Anschlussinhabers entschieden; S. *LG Hamburg*, Beschl. v. 21.4.2009 - 627 Qs 13/09, BeckRS 2009, 22518; *LG München*, Beschl. v. 12.3.2008 - 5 Qs 19/08, MMR 2008, 561, 561; *LG Saarbrücken*, Beschl. v. 28.1.2008 - 5 (3) Qs 349/07, MMR 2008, 562, 562. Teilweise wurde die Akteneinsicht auch bei Bagatellverletzungen verneint; S. *LG Saarbrücken*, Beschl. v. 26.8.2009 - 2

eines Nutzers verfügen, ist ihnen außerdem der Verweis auf den Privatklageweg auch ohne Mitwirkung der Staatsanwaltschaft zumutbar.

Natürlich ist die Strafverfolgung von anonymen Tätern im Internet dennoch von großer Bedeutung für die öffentliche Sicherheit und Ordnung sowie den Kampf gegen Hass und Hetze im Netz. Die Aufmerksamkeit der Strafverfolgungsbehörden sollte sich allerdings schwerpunktmäßig auf Delikte konzentrieren, bei denen ein großes öffentliches Interesse an der Strafverfolgung besteht wie etwa bei Straftaten gegen die öffentliche Ordnung oder gegen die sexuelle Selbstbestimmung. Daher kann eine Stärkung der Auskunftsmöglichkeiten der Rechteinhaber zu einer sinnvollen Entlastung der Staatsanwaltschaften beitragen.[24]

B. Haftung und Pflichten der Diensteanbieter

Zumindest de lege lata erschwert die Anonymität im Internet ein Vorgehen der Rechteinhaber gegen die Nutzer als unmittelbare Rechtsverletzer erheblich. Unter anderem deshalb zielen die Maßnahmen zur Rechtsdurchsetzung der Rechteinhaber verstärkt auf eine Inanspruchnahme der Diensteanbieter ab.[25] Auch Gesetzgebung und Rechtsprechung, sowohl auf nationaler als auch auf Unionsebene, versuchen zunehmend, einen regulatorischen Rahmen für die Pflichten und die Haftung von Internetdiensteanbietern zu schaffen. Dabei geht der Trend dahin, die Diensteanbieter stärker in die Verantwortung zu nehmen.[26]

Qs 33/09, BeckRS 2009, 27053; *LG Darmstadt*, Beschl. v. 20.4.2009 – 9 Qs 99/09, ZUM-RD 2009, 466, 467. S. auch *Sandor*, Datenspeicherung, Rn. 605.

[24] Ähnlich *Rechtsausschuss*, BT-Drs. 16/8783, S.44: „Die Stärke des Auskunftsanspruchs und die Belastung der Staatsanwaltschaften sei ein System kommunizierender Röhren.".

[25] Teilweise wird für die Inanspruchnahme der Diensteanbieter mit dem Gesichtspunkt des "cheapest cost avoider" argumentiert. Vgl. *Leistner*, ZUM 2012, 722, 723; *Ohly*, ZUM 2015, 308, 309. S. auch *Pille*, NJW 2018, 3545, 3546: „Verantwortungsverlagerung vom Täter zum Diensteanbieter". A.A. *Wagner,* GRUR 2020, 329, 336 f.

[26] Vgl. *Wagner*, GRUR 2020, 447, 451 f.

I. Grundlagen für eine Haftung der Diensteanbieter

Regelungen zur Haftung der Diensteanbieter sind insbesondere in den Vorschriften der §§ 7 ff. TMG, die die Umsetzung der Art. 12 ff. E-Commerce-Richtlinie enthalten. Diese Normen sehen in erster Linie Haftungsprivilegierungen für Zugangsanbieter (§ 8 TMG), Cache-Provider (§ 9 TMG) und Host-Provider (§ 10 TMG) vor. Jedenfalls in unionsrechtskonformer Auslegung erstrecken sich die Vorschriften der §§ 7 ff. TMG nicht nur auf Telemediendienste, sondern auch auf bestimmte Telekommunikationsdienste wie Access-Provider, die einen Dienst der Informationsgesellschaft im Sinne der E-Commerce-Richtlinie darstellen.[27] Die Harmonisierung durch die E-Commerce-Richtlinie bezieht sich aber lediglich auf die Privilegierung beziehungsweise Freistellung der Diensteanbieter von der Haftung. Können sich die Diensteanbieter nicht auf die Haftungsprivilegien der §§ 8-10 TMG berufen, richtet sich ihre Haftung grundsätzlich nach dem Recht der Mitgliedsstaaten.[28] Allerdings dürfen die Diensteanbieter nach § 7 Abs. 2 TMG, der auf Art. 15 E-Commerce-Richtlinie beruht, nicht zur allgemeinen Überwachung verpflichtet werden.[29]

Sowohl Gesetzgebung als auch Rechtsprechung tragen dazu bei, die Haftung und Verantwortlichkeit der Diensteanbieter näher auszugestalten. Diensteanbieter haften zunächst einmal nach allgemeinen Grundsätzen für eigene Inhalte oder Inhalte, die sie sich zu eigen gemacht haben (§ 7 Abs. 1 TMG). Ein Diensteanbieter macht sich einen Inhalt zu eigen, wenn nach außen ersichtlich ist, dass er inhaltlich Verantwortung für einen Inhalt übernommen hat oder sich mit dem Inhalt identifiziert hat.[30]

---

[27] *Frey*, MMR 2014, 650, 653 f.; *Spindler* in: Spindler/Schmitz, § 1 TMG Rn. 32;

[28] Ausnahmen gelten vor allem bei Verletzungen des geistigen Eigentums *Janal*, ZEuP 2021, 227, 236.

[29] S. zum Verbot allgemeiner Überwachungspflichten als Grenze der Haftung der Diensteanbieter *Schiff*, Informationsintermediäre, S. 97.

[30] S. zu Letzterem *BGH,* Urt. v. 1.3.2016 – VI ZR 34/15, NJW 2016, 2106 Rn. 17 f. – Ärztebewertungsportal III; *BGH,* Urt. v. 27.3.2012 - VI ZR 144/11, AfP 2012, 264 Rn. 11 – RSS-Feeds; *BGH,* Urt. v. 19.3.2015 – I ZR 94/13, NJW 2015, 3443 Rn. 25 – Hotelbewertungsportal; *BGH,* Urt. v. 12.11.2009 - I ZR 166/07, NJW-RR 2010, 1276 Rn. 24, 27 – marions-kochbuch.de; *Hofmann*, JuS 2017, 713, 717; *Wagner*, GRUR 2020, 447, 448.

Im Kontext dieser Arbeit ist aber vor allem auch die Haftung der Diensteanbieter für fremde Inhalte und Rechtsverletzungen ihrer Nutzer relevant. Die Basis für eine Haftung der Diensteanbieter für Rechtsverletzungen ihrer Nutzer nach nationalem Recht ist insbesondere die von der Rechtsprechung auf Grundlage der analogen Anwendung des § 1004 BGB entwickelte Störerhaftung.[31] Wer nicht selbst Täter oder Teilnehmer einer Verletzung absoluter Rechte ist, kann demnach als Störer haften, wenn er einen kausalen Mitwirkungsbeitrag zur Rechtsverletzung geleistet hat.[32]

Die wichtigste Voraussetzung für die Störerhaftung ist die Verletzung von Prüf- bzw. Verhaltenspflichten durch die Diensteanbieter.[33] Kommen die Diensteanbieter diesen Pflichten nicht nach, können die Rechteinhaber Unterlassungs- oder Beseitigungsansprüche gegen die Diensteanbieter geltend machen. Die Art und der Umfang solcher Pflichten wurden von der Rechtsprechung für verschiedene Arten von Online-Diensten unterschiedlich ausgearbeitet und bestimmen sich danach, inwieweit dem als Störer in Anspruch genommenen nach

---

[31] S. etwa *BGH*, Urt. v. 4.4.2017 – VI ZR 123/16, NJW 2017, 2029 Rn. 18; *BGH*, Beschl. v. 13.9.2018 – I ZR 140/15, GRUR 2018, 1132 Rn. 48 ff. – YouTube; *BGH,* Urt. v. 12.7.2012 – I ZR 18/11, GRUR 2013, 370, 370 – Alone in the dark; *BGH*, Urt. v. 9. 11. 2011 - I ZR 150/09, GRUR 2012, 304, 307 Rn. 50 – Basler Haar-Kosmetik; *BGH*, Urt. v. 25.10.2011 - VI ZR 93/10, GRUR 2012, 311 Rn. 20 ff. – Blog-Eintrag; *BGH*, Urt. v. 11.3.2004 - I ZR 304/01, MMR 2004, 668, 671 – Internet-Versteigerung I; *BGH*, Urt. v. 17.5.2001 - I ZR 251/99, GRUR 2001, 1038 - ambiente.de; *BGH*, Urt. v. 18.10.2001 - I ZR 22/99, GRUR 2002, 618, 619 - Meißner Dekor. S. zur Vereinbarkeit der Störerhaftung mit Art. 8 Abs. 3 InfoSoc-Richtlinie *EuGH*, Urt. v. 22.6.2021 – C-682/18 u.a., GRUR 2021, 1054 Rn. 119 ff. – YouTube und Cyando; *Spindler*, NJW 2021, 2554, 2556.

[32] *BGH,* Urt. v. 26.7.2018 – I ZR 64/17, GRUR 2018, 1044 Rn. 15 – Dead Island; *BGH,* Urt. v. 30.6.2009 – VI ZR 210/08, ZUM-RD 2009, 641, 641; *BGH,* Urt. v. 19.4.2007 - I ZR 35/04, GRUR 2007, 708 Rn. 40 – Internet-Versteigerung II; *BGH,* Urt. v. 12.7.2007 - I ZR 18/04, GRUR 2007, 890 Rn. 43 – Jugendgefährdende Medien bei ebay; *BGH,* Urt. v. 11.3.2004 - I ZR 304/01, GRUR 2004, 860 – Internet-Versteigerung I. S. auch *Pille*, NJW 2018, 3545, 3546.

[33] *BGH,* Urt. v. 26.7.2018 – I ZR 64/17, GRUR 2018, 1044 Rn. 15 – Dead Island; *BGH,* Urt. v. 16.5.2013 – I ZR 216/11, GRUR 2013, 1229 Rn. 34 – Kinderhochstühle im Internet II; *BGH,* Urt. v. 22.7.2010 - I ZR 139/08, GRUR 2011, 152 Rn. 45 – Kinderhochstühle im Internet; *BGH,* Urt. v. 19.4.2007 - I ZR 35/04, GRUR 2007, 708 Rn. 40 – Internet-Versteigerung II; *BGH,* Urt. v. 12.7.2007 - I ZR 18/04, GRUR 2007, 890 Rn. 43 – Jugendgefährdende Medien bei ebay; *BGH,* Urt. v. 17.5.2001 - I ZR 251/99, GRUR 2001, 1038, 1039.

den konkreten Umständen eine Prüfung zuzumuten ist.[34] Kriterien sind – neben der Art des Dienstes – zum Beispiel auch die Gefahrgeneigtheit eines Dienstes und die Erkennbarkeit der Rechtsverletzung.[35] Verhalten sich die Diensteanbieter nicht als neutrale Vermittler von Informationen, indem sie eine aktive Rolle einnehmen, unterliegen sie außerdem strengeren Prüfpflichten.[36] In diesen Fällen können sich die Diensteanbieter nach der Rechtsprechung des *EuGH* auch nicht auf die Haftungsprivilegierungen der E-Commerce-Richtlinie berufen.[37]

Im Urheberrecht hat sich der BGH inzwischen jedenfalls für Host-Provider von der Störerhaftung abgewandt.[38] Sofern die Diensteanbieter aber als Täter haften, bleibt zudem allgemein kein Raum mehr für die Anwendung der Störerhaftung. Insbesondere nach § 1 Abs. 2 UrhDaG und § 2 Abs. 1 UrhDaG können Diensteanbieter für das Teilen von Online-Inhalten selbst als Täter für urheberrechtsverletzende Inhalte ihrer Nutzer haften.[39] Nicht verantwortlich ist der Diensteanbieter nach § 1 Abs. 2 UrhDaG aber, wenn er seinen Pflichten der §§ 4, 7-11 UrhDaG nachgekommen ist. Im Rahmen des Anwendungsbereichs des UrhDaG treten die von der Rechtsprechung aufgestellten Grundsätze zur Störerhaftung zurück.[40] Diensteanbieter im Sinne des § 2 Abs. 1 UrhDaG können sich nach § 1 Abs. 2 UrhDaG auch nicht mehr auf die Haftungsprivilegierung nach § 10 Abs. 1 TMG berufen.

---

[34] Vgl. *BGH,* Urt. v. 12.5.2010 – I ZR 121/08, ZUM 2010, 696 Rn. 19 – Sommer unseres Lebens; *BGH,* Urt. v. 1.4.2004 - I ZR 317/01, MMR 2004, 529 – Schöner Wetten; *BGH*, Urt. v. 9.2.2006 - I ZR 124/03, GRUR 2006, 875 Rn. 32 – Rechtsanwalts-Ranglisten.

[35] S. auch *Schiff*, Informationsintermediäre, S. 203 ff.

[36] S. etwa *BGH*, Urt. v. 16.5.2013 – I ZR 216/11, GRUR 2013, 1229 Rn. 48 – Kinderhochstühle im Internet II.

[37] *EuGH,* Urt. v. 12.7.2011 - C-324/09, GRUR 2011, 1025 Rn. 116 – L'Oréal/eBay; *EuGH*, Urt. v. 23.3.2010 - C-236/08 u.a., GRUR 2010, 445 Rn. 114 –Google France.

[38] S. dazu *BGH*, Urt. v. 02.06.22 – I ZR 140/15, NJW 2022, 2980, 2980 ff.; *BGH*, Urt. 02.06.22, NJW 2022, 2994, 2994 ff. S. zur Frage, ob diese Rechtsprechungsänderung auch für andere Provider gilt *Ohly*, NJW 2022, 2961, 2961 ff.; *Hoffmann*, jurisPR-WettbR 9/2022 Anm. 1.

[39] Diese Norm dient der Umsetzung von Art. 17 DSM-RL; S. dazu etwa *Hofmann,* NJW 2021, 1905, 1905, 1906; *Metzger/Pravemann*, ZUM 2021, 288, 290; *Wandtke/Hauck*, ZUM 2021, 763, 767.

[40] *Hofmann,* GRUR 2018, 21, 28; *Leistner,* ZUM 2020, 897, 901 f.; *Metzger/Pravemann,* ZUM 2021, 288, 290.

Zukünftig wird der Bereich der Haftung und Verantwortung von Diensteanbietern, die Informationen vermitteln, auf europäischer Ebene durch den Digital Services Act, noch stärker harmonisiert wird.[41] Die Vorschriften der Art. 12-15 E-Commerce-Richtlinie werden durch Art. 89 Abs. 1 DSA gestrichen und durch die Art. 4 ff. DSA ersetzt. Diese führen die Haftungsprivilegierungen aus der E-Commerce-Richtlinie im Wesentlichen fort. Die nationalen Umsetzungsregelungen des TMG werden daher zukünftig durch den DSA verdrängt.

II. Pflichten der Diensteanbieter

Sowohl aus der von der Rechtsprechung entwickelten Störerhaftung als auch aus nationalen Regelungen aus dem TMG, dem UrhDaG oder dem NetzDG resultieren zum Teil umfassende Pflichten der Diensteanbieter in Bezug auf Rechtsverletzungen ihrer Nutzer, die hier lediglich überblicksartig dargestellt werden.

Der Verstoß gegen solche Pflichten kann zu einer Haftung der Diensteanbieter gegenüber den Rechteinhabern als Störer oder sogar Täter (§ 1 Abs. 1 UrhDaG) führen, aber auch bußgeldbewehrt sein.

1. Notice-andTake-Down

Diensteanbieter, die Inhalte ihrer Nutzer speichern (Host-Provider), sind verpflichtet, vermeintlich rechtswidrige Inhalte, die ihnen gemeldet werden, zu prüfen und gegebenenfalls unverzüglich zu entfernen oder zu sperren.[42] Angelegt ist dieses Notice-and-Take-Down-Verfahren bereits in § 10 Nr. 2 TMG.[43] Die Haftungsprivilegierung für Host-Provider greift nämlich nur, wenn sie, nachdem sie Kenntnis von einer Rechtsverletzung erhalten haben, unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr

---

[41] S. noch zum Entwurf des Digital Services Acts etwa *Gielen/Uphues*, EuZW 2021, 627, 627 ff.; *Janal,* ZEuP 2021, 227, 227 ff.; *Kühling*, ZUM 2021, 461, 461 ff.; *Spindler*, GRUR 2021, 545, 545 ff.; *Spindler,* GRUR 2021, 653, 653 ff.

[42] *BGH,* Beschl. v. 13.9.2018 – I ZR 140/15, GRUR 2018, 1132 Rn. 49 – YouTube; *BGH*, Beschl. v. 20.9.2018 – I ZR 53/17, GRUR 2018, 1239 Rn. 40 – uploaded; *BGH*, Urt. v. 11.3.2004 - I ZR 304/01, GRUR 2004, 860, 864 – Internet-Versteigerung I; *BGH*, Urt. v. 19.4.2007 - I ZR 35/04, GRUR 2007, 708 Rn. 45 – Internet-Versteigerung II; *BGH,* Urt. v. 12.7.2012 – I ZR 18/11, GRUR 2013, 370 Rn. 28 – Alone in the Dark.

[43] *Holznagel*, ZUM 2017, 615, 617.

zu sperren. Werden sie dennoch nicht tätig, können Beseitigungs- oder Unterlassungsansprüche auf Grundlage der Störerhaftung gegen sie geltend gemacht werden.[44] Die Rechteinhaber können in diesem Fall Beseitigungs- oder Unterlassungsansprüche gegen die Diensteanbieter geltend machen.

Daneben existieren aber auch gesetzliche Regelungen, die das Notice-and-Take-Down-Verfahren für bestimmte Dienste noch näher ausgestalten. Solche finden sich für soziale Netzwerke in § 3 NetzDG,[45] in §§ 10a, 10b TMG[46] für die Anbieter von Videosharing-Diensten und in den § 8 Abs. 1 UrhDaG[47] Zukünftig werden Art. 16, 17 DSA zu beachten sein.

2. Stay-down, kerngleiche Rechtsverletzungen und Uploadfilter

Das Notice-and-Take-Down-Verfahren dient lediglich dazu, rechtsverletzende Inhalte zu entfernen oder zu sperren. Es verhindert allerdings nicht, dass die Nutzer denselben Inhalt erneut hochladen.
Nach der Rechtsprechung des BGH können Host-Provider auch dann als Störer haften, wenn sie nicht Vorsorge treffen, dass künftig derartigen Verletzungen vermieden werden.[48] Die Diensteanbieter trifft die Pflicht zukünftige kerngleiche Verstöße zu verhindern.[49]

---

[44] *BGH*, Urt. v. 19.4.2007 - I ZR 35/04, GRUR 2007, 708 Rn. 45 – Internet-Versteigerung II; *BGH,* Urt. v. 12.7.2012 – I ZR 18/11, GRUR 2013, 370 Rn. 28 – Alone in the Dark.

[45] S. ausführlicher zu den Lösch- und Sperrpflichten nach § 3 NetzDG *Spindler*, GRUR 2018, 365, 369 ff.

[46] Die Vorschriften für die Anbieter von Videosharing-Diensten dienen der Umsetzung der AVMD-Richtlinie.

[47] Das UrhDaG dient dabei der Umsetzung von Art. 17 DSM-Richtlinie.

[48] *BGH*, Urt. v. 17.8.2011 - I ZR 57/09, GRUR 2011, 1038 Rn. 21 – Stiftparfüm; *BGH*, Urt. v. 11.3.2004 - I ZR 304/01, GRUR 2004, 860, 864 – Internet-Versteigerung I; *BGH*, Urt. v. 19.4.2007 - I ZR 35/04, GRUR 2007, 708 Rn. 45, 47 – Internet-Versteigerung II; *BGH*, Urt. v. 30. 4. 2008 - I ZR 73/05, GRUR 2008, 702 Rn. 51 – Internet-Versteigerung III; *BGH,* Urt. v. 12.7.2012 – I ZR 18/11, GRUR 2013, 370 Rn. 29 ff. – Alone in the Dark; *BGH,* Urt. v. 5.2.2015 – I ZR 240/12, GRUR 2015, 485 Rn. 52 – Kinderhochstühle im Internet III; S. auch *EuGH*, Urt. v. 12.7.2011 - C-324/09, GRUR 2011, 1025, Rn. 131 ff. - L'Orèal; *EuGH*, Urt. v. 3.10.2019 – C-18/18, MMR 2019, 798 Rn. 53 - Glawischnig-Piesczek. S. ausführlich auch *Paal/Hennemann* in: BeckOK Informations- und Medienrecht, § 7 TMG Rn. 62 ff. m.w.N.

[49] *BGH,* Beschl. v. 13.9.2018 – I ZR 140/15, GRUR 2018, 1132 Rn. 49 – YouTube; *BGH*, Beschl. v. 20.9.2018 – I ZR 53/17, GRUR 2018, 1239 Rn. 40 – uploaded; *BGH*, Urt. v. 11.3.2004 - I ZR 304/01, GRUR 2004, 860, 864 – Internet-Versteigerung I; *BGH*, Urt. v. 30.

Zur Verhinderung zukünftiger Rechtsverletzungen können die Diensteanbieter automatisierte Verfahren wie zum Beispiel Filtersysteme einsetzen.[50] Solche automatisierten Filter sieht § 7 Abs. 2 S. 2 UrhDaG für die Verhinderung des Uploads von urheberrechtswidrigen Inhalten ausdrücklich vor (Upload-Filter).[51]

Die Auferlegung präventiver Maßnahmen wie der Verwendung von Upload-Filtern steht allerdings im Konflikt zum Verbot der allgemeinen Überwachungspflicht.[52] Auch wenn die Inhalte auf einer Plattform nur im Hinblick auf bestimmte Rechtsverletzungen untersucht werden müssen, weicht das Erfordernis, alle Inhalte vorab zu untersuchen, dieses Verbot jedenfalls erheblich auf.[53]

3. Sperranordnungen

Rechteinhaber können außerdem subsidiär von WLAN-Betreibern i.S.d. § 8 Abs. 3 TMG nach § 7 Abs. 4 TMG Sperrung der Nutzung von Informationen im Hinblick auf eine Verletzung des geistigen Eigentums verlangen.[54] In unionsrechtskonformer[55] Auslegung ist § 7 Abs. 4 TMG analog auch auf andere Zugangsanbieter und insbesondere auf Access-Provider anzuwenden.[56] Dabei

---

4. 2008 - I ZR 73/05, GRUR 2008, 702 Rn. 51 – Internet-Versteigerung III; *BGH*, Urt. v. 17.8.2011 - I ZR 57/09, GRUR 2011, 1038 Rn. 21 – Stiftparfüm. S. auch *EuGH*, Urt. v. 3.10.2019 – C-18/18, MMR 2019, 798 Rn. 38 ff. - Glawischnig-Piesczek: „sinngleiche Informationen".

[50] S. *EuGH,* Urt. v. 3.10.2019 – C-18/18, GRUR 2019, 1208 Rn. 46 – Glawischnig-Piesczek; Besprechung bei *Geidel,* ZUM 2021, 16, 16 ff.; *Pfeifer*, GRUR-Prax 2019, 534, 534 ff.; *Spindler,* NJW 2019, 3274, 3274 ff. S. speziell zum Urheberrecht *Spindler,* GRUR 2020, 253, 257 ff.

[51] S. dazu etwa *Oster* in: BeckOK Urheberrecht, § 7 UrhDaG Rn. 20 f. m.w.N.

[52] *EuGH,* Urt. v. 3.10.2019 – C-18/18, MMR 2019, 798 Rn. 34 ff. – Glawischnig-Piesczek.

[53] Vgl. *Paal* in: BeckOK Informations- und Medienrecht, § 7 TMG Rn. 65; *Senftleben*, ZUM 2019, 369, 372.

[54] Ausführlicher dazu *Röß*, GRUR 2021, 823, 823 ff.

[55] S. Art. 8 Abs. 3 InfoSoc-RL und *EuGH*, Urt. v. 27.3.2014 – C-314/12, GRUR 2014, 468 Rn. 37 ff. – UPC Telekabel.

[56] S. *BGH,* Urt. v. 26.7.2018 – I ZR 64/17, GRUR 2018, 1044 Rn. 49 – Dead Island; *Hennemann,* ZUM 2018, 754, 754 ff.; *Spindler*, GRUR 2018, 1012, 1014 ff.; *Redeker* in: Redeker IT-Recht, D. Rn. 1433 ff. Anders aber *OLG München*, Urt. v. 14.6.2018 – 29 U 732/18, GRUR 2018, 1050, 1050 – Kinox.to, das weiterhin Sperransprüche auf die Störerhaftung nach § 1004 BGB analog stützt. Vor dem dritten Änderungsgesetz zum Telemediengesetz leitete der

können DNS-, URL-, IP- oder Port-Sperren eingesetzt werden.[57] DNS-Resolver, die Domainnamen in die dazugehörigen IP-Adressen auflösen, können nach der Rechtsprechung ebenfalls subsidiär auf Sperrung strukturell rechtsverletzender Webseiten in Anspruch genommen werden.[58]

4. Dekonnektierung oder Löschung einer Domain

Verletzt ein Domainname Rechtsverletzer in ihren Rechten oder sind strukturell rechtsverletzenden Internetseiten unter einer bestimmten Domain abrufbar, können die Rechteinhaber versuchen, die Dekonnektierung oder Löschung der Domain zu erwirken.[59] Geht es nicht um den Domainnamen, sondern um die Inhalte einer Webseite, kommt die Dekonnektierung oder Löschung einer Domain nur in Betracht, wenn die Inhalte „weit überwiegend illegal" sind.[60] Domain-Registries wie die DENIC und Domain-Registrare können auf der Grundlage der Störerhaftung zur Dekonnektierung einer Domain verpflichtet werden. Die DENIC haftet allerdings gegenüber dem Domaininhaber nur subsidiär.[61] Zudem treffen sie nur sehr eingeschränkt Prüfpflichten, da sie im öffentlichen Interesse agiert.[62] Ähnliches gilt auch für die Domain-Registrare.[63] Da diese allerdings anders als die Registries meist in Gewinnerzielungsabsicht

---

BGH Sperranordnungen gegen Access-Provider noch aus der Störerhaftung ab, S. *BGH*, Urt. v. 26.11.2015 – I ZR 174/14, GRUR 2016, 268 – Störerhaftung des Access-Providers.

[57] Ausführlicher etwa *Nicolai,* ZUM 2018, 33, 37 ff.; *Thome*, Sperrverfügungen, S. 40 ff. S. zu den Sperrungen durch Anbieter eines TOR-Servers *Thiesen,* MMR 2014, 803, 805 ff.

[58] Hierbei wird allerdings wieder auf die Störerhaftung zurückgegriffen; S. *OLG Köln*, Urt. v. 9.10.2020 – 6 U 32/20, GRUR 2021, 70 Rn. 88 ff. – Herz Kraft Werke. S. dazu auch *Nordemann,* GRUR 2021, 18, 18 ff.

[59] S. dazu *Volkmann* in: Spindler/Schuster, § 1004 BGB Rn. 42 ff.

[60] *BGH,* Urt. v. 15.10.2020 – I ZR 13/19, GRUR 2021, 63 Rn. 26 – Störerhaftung des Registrars; *BGH*, Urt. v. 26.11.2015 – I ZR 174/14, GRUR 2016, 268 Rn. 55 – Störerhaftung des Access-Providers.

[61] *BGH*, Urt. v. 17.5.2001 - I ZR 251/99, GRUR 2001, 1038, 1040 – ambiente.de; *BGH*, Urt. v. 27.10.2011 - I ZR 131/10, GRUR 2012, 651 Rn. 25 – regierung-oberfranken.de; *OLG Frankfurt a.M.,* Urt. v. 26.10.2010 - 11 U 30/10, MMR 2011, 176, 177 – sr.de.

[62] *BGH*, Urt. v. 17.5.2001 - I ZR 251/99, GRUR 2001, 1038, 1039 f. – ambiente.de; *BGH*, Urt. v. 27.10.2011 - I ZR 131/10, GRUR 2012, 651 Rn. 24 f. – regierung-oberfranken.de.

[63] *BGH*, Urt. v. 15.10.2020 – I ZR 13/19, GRUR 2021, 63 Rn. 30 ff. – Störerhaftung des Registrars. S. dazu auch *Hofmann,* NJW 2021, 274, 275 f.; *Nordemann,* GRUR 2021, 18, 18 ff.

handeln, müssen sie jedenfalls Hinweisen auf eine Rechtsverletzung nachgehen.[64]

Daneben ist auch eine Störerhaftung des Admin C denkbar.[65] Prüfpflichten des Admin C werden in der Regel allerdings erst durch einen entsprechenden Hinweis ausgelöst.[66] Im Falle der Verletzung von Prüfpflichten, kann der Admin C auf Löschung der Domain, für die er als administrativer Ansprechpartner eingetragen ist, in Anspruch genommen werden.

III. Inpflichtnahme der Diensteanbieter als Alternative zu Auskunftsansprüchen?

Angesichts der zum Teil sehr weitreichenden Pflichten der Diensteanbieter stellt sich die Frage, ob es daneben überhaupt einer Identifizierung der Nutzer als unmittelbare Rechtsverletzer bedarf. Schließlich haben die Rechteinhaber die Möglichkeit gegen Rechtsverletzungen vorzugehen, indem sie Löschung oder Sperrung verlangen. Zudem müssen die Diensteanbieter auch für die Zukunft kerngleiche Rechtsverletzungen verhindern und gegebenenfalls sogar präventive Maßnahmen gegen Rechtsverletzungen ergreifen.

Allerdings bringt die Verlagerung der Verantwortlichkeit auf die Diensteanbieter erhebliche Nachteile mit sich, die bei einer gegen die unmittelbaren Verletzer gerichteten Rechtsdurchsetzung nicht bestehen.

1. Gefahr des Overblockings

Die größte Gefahr besteht darin, dass die Diensteanbieter auf Grund der hohen Anforderungen, die an sie gestellt werden, dazu neigen könnten, vermeintlich rechtswidrige Inhalte im Zweifel vorsichtshalber zu löschen. Dadurch könnten rechtmäßige Inhalte fälschlicherweise entfernt werden. Das kann erhebliche

---

[64] *BGH*, Urt. v. 15.10.2020 – I ZR 13/19, GRUR 2021, 63 Rn. 30 ff. – Störerhaftung des Registrars.

[65] *BGH,* Urt. v. 9. 11. 2011 - I ZR 150/09, GRUR 2012, 304 Rn. 43 – Basler Haar-Kosmetik; *Spindler* in:Spindler/Schmitz, § 7 TMG Rn. 115.

[66] *BGH,* Urt. v. 9. 11. 2011 - I ZR 150/09, GRUR 2012, 304 Rn. 53 – Basler Haar-Kosmetik. Eine Ausnahme gilt bei gefahrerhöhendem Verhalten des Admin C; S. *BGH,* Urt. v. 9. 11. 2011 - I ZR 150/09, GRUR 2012, 304 Rn. 60 – Basler Haar-Kosmetik*; OLG Koblenz,* Urt. v. 23.4.2009 - 6 U 730/08, MMR 2009, 549, 550 f.

Auswirkungen auf den öffentlichen Meinungsaustausch haben,[67] sowie die Rechte aller redlichen Internetznutzer beeinträchtigen. Insbesondere kann dies dazu führen, dass die Nutzer von ihrer Meinungsfreiheit oder den Schrankenregelungen im Urheberrecht nicht mehr in vollem Umfang Gebrauch machen („Chilling Effects").[68]
Die Gefahr des Overblockings besteht insbesondere, wenn zu hohe Anforderungen an die Diensteanbieter gestellt werden. [69] Ein zu weit gehendes Löschen wurde deshalb unter anderem aufgrund der Pflichten des NetzDG befürchtet, da § 3 Abs. 2 NetzDG den Diensteanbietern nur kurze Zeit zur Prüfung eines beanstandeten Inhalts zugesteht, aber gleichzeitig § 4 NetzDG eine Bußgeldandrohung enthält.[70]

Außerdem ist bei der Einführung von Uploadfiltern beziehungsweise dem Einsatz sonstiger automatisierter Verfahren zur Erkennung von rechtswidrigen Inhalten zu befürchten, dass bereits der Upload rechtmäßiger Inhalte verhindert werden könnte.[71] Automatisierte Kontrollverfahren sind oft kaum in der Lage kerngleiche Verstöße zu erkennen.[72] Auch die umstrittenen Upload-Filter eignen sich nur eingeschränkt dazu, urheberrechtswidrige Inhalte von rechtmäßigen zu unterscheiden.[73] Vor allem in den vielen Fällen, in denen es zur Bewertung eines Inhalts auf eine Interessensabwägung oder den Kontext, in dem der fragliche Inhalt steht, ankommt, können automatisierte Verfahren keine zuverlässigen Entscheidungen treffen.[74] Zum Beispiel können Upload-Filter, die zur

---

[67] *Pille*, NJW 2018, 3545, 3548.

[68] *Becker,* ZUM 2019, 636, 648.

[69] *Löber/Roßnagel*, MMR 2019, 71, 73.

[70] *Gersdorf,* MMR 2017, 439, 446 f.; *Guggenberger*, ZRP 2017, 98, 99; *Holznagel*, ZUM 2017, 615, 623; *Nolte*, ZUM 2017, 552, 556. A.A. im Hinblick darauf, dass zutreffend das NetzDG Bußgelder nur bei systematischen Verstößen vorsieht *Eisenreich,* RDi 2021, 289, 291.

[71] S. dazu *Gielen/Tiessen*, EuZW 2019, 639, 645; *Kastl,* GRUR 2016, 671, 675; *Spindler,* CR 2019, 277, 289; *Suwelack,* MMR 2018, 582, 585.

[72] *Spindler,* MMR 2018, 48, 48. S. kritisch zum Einsatz von automatisierten Verfahren bei Persönlichkeitsrechtsverletzungen *Geidel*, ZUM 2021, 16, 24; *Keller*, GRUR Int 2020, 616, 619.

[73] S. zur Eignung von Upload-Filtern im Urheberrecht *Conrad,* ZUM 2017, 289, 298; *Gielen/Tiessen*, EuZW 2019, 639, 644 f.; *Kastl,* GRUR 2016, 671, 675; *Nolte,* ZUM 2017, 304, 310.

[74] Entschärft wird diese Problematik im UrhDaG dadurch, dass nach § 9 UrhDaG mutmaßlich erlaubte Nutzungen öffentlich wiederzugeben sind und der Diensteanbieter in diesem Fall nach § 12 Abs. 2 UrhDaG nur eingeschränkt haftet.

Vorbeugung von Urheberrechtsverletzungen eingesetzt werden, nicht erkennen, ob es sich auf Grund der Schrankenregelung für Parodien oder Karikaturen um eine zulässige Verwendung urheberrechtlich geschützten Materials handelt.[75]

Je höher die Anforderungen an die Diensteanbieter zur Verhinderung von Rechtsverletzungen sind, desto eher besteht also die Gefahr des Overblockings, vor allem, wenn die Folgen des Löschens rechtmäßiger Inhalte hinter denen bei unterbliebener Löschung rechtswidriger Inhalte zurückstehen.[76]

Diese Gefahr kann aber gemindert werden, wenn den Nutzern gleichzeitig wirksame Instrumente zum Schutz ihrer Interessen bereitgestellt werden. Dazu gehört insbesondere der „put-back"-Anspruch beziehungsweise der Anspruch auf Nichtlöschung der Inhalte.[77] Muss der Anspruch erst gerichtlich geltend gemacht werden, ist allerdings mit einer erheblichen Verzögerung zu rechnen, bis der rechtmäßige Inhalt wieder online verfügbar wäre. Selbst wenn den Nutzern in einem solchen Fall dem Grunde nach Schadensersatzansprüche zustehen würden, liegt oft kein materieller Schaden vor.[78]

Wichtig ist deshalb, dass die Nutzer auch außergerichtlich die Möglichkeit haben, gegen eine Löschung vorzugehen oder ihr sogar vorzubeugen. Das lässt sich zum Beispiel durch Pflichten der Diensteanbieter realisieren, vorab die

---

[75] *Spindler,* CR 2019, 277, 289; *Weiden,* GRUR 2019, 370, 371.

[76] S. dazu *OLG Karlsruhe*, Beschl. v. 28.2.2019 – 6 W 81/18, NJW-RR 2019, 1006; *Becker,* ZUM 2020, 681, 691; *Hofmann,* GRUR 2019, 1219, 1220; Nolte, ZUM 2017, 552, 558; Oster in: BeckOK Urheberrecht, § 7 UrhDaG Rn. 16 ff.; *Spindler*, GRUR 2018, 365, 369; *Wagner*, GRUR 2020, 447, 452: „Asymmetrische Anreize der Plattform".

[77] S. dazu *Hofmann*, ZUM 2017, 102, 105; *Pille,* NJW 2018, 3545, 3548; *Spindler,* GRUR 2018, 365, 371; S. zum Anspruch auf „put back" aus Nutzerverhältnis zum Anbieter *OLG Dresden,* Beschl. v. 19.1.2019 – 4 W 1074/18, GRUR-RR 2019, 408 – Account-Sperre; *Holznagel*, CR 2019, 518, 518 ff.; *Raue*, JZ 2018, 961, 961 ff.; *Spindler*, CR 2019, 238, 238 ff. Vgl. *BVerfG*, Beschl. v. 22.5.2019 – 1 BvQ 42/19, NJW 2019, 1935 – Der III. Weg.

[78] *Kaesling/Knapp*, MMR 2021, 11, 15; *Kaesling/Knapp*, MMR 2020, 816, 821; *Wagner*, GRUR 2020, 447, 452.

betroffenen Nutzer anzuhören[79] oder ein Gegenvorstellungsverfahren[80] vorzusehen. Auch durch sinnvolles Beschwerdemanagement[81] und außergerichtliche Streitbeilegung[82] lassen sich die Interessen der Nutzer besser wahren.

Dennoch lässt sich das Risiko, dass rechtmäßige Inhalte zeitweise online nicht abrufbar sind, nicht vollkommen ausschließen. Selbst kurzzeitige Verzögerungen, bis die Inhalte wieder abrufbar sind, können vor allem bei sehr aktuellen Themen oder Trends zu einem erheblichen Verlust von Reichweite führen.[83] Unliebsame legale Inhalte könnten deshalb absichtlich beanstandet werden in der Hoffnung, dass die Diensteanbieter diese zumindest vorübergehend löschen und dadurch weniger Menschen erreicht werden. Dem lässt sich allerdings entgegenwirken, indem man Nutzern und Diensteanbietern zumindest entsprechende Schadensersatzansprüche gewährt, obwohl in vielen Fällen der Nachweis eines materiellen Schadens schwierig sein wird.[84]

2. Legitimationsdefizit der Diensteanbieter

Ein weiteres Problem der Verantwortungsverlagerung auf die Diensteanbieter besteht darin, dass nunmehr nicht mehr Gerichte, sondern die Anbieter von Internetdiensten über die Rechtmäßigkeit von Inhalten entscheiden.[85] Rechtliche Bewertungen den Diensteanbietern zu überlassen, ist insbesondere dann problematisch, wenn gegensätzliche Interessen von Rechteinhabern und Nutzern abgewogen werden müssen.

---

[79] S. dazu *BGH,* Urt. v. 1.3.2016 – VI ZR 34/15, GRUR 2016, 855 Rn. 24, 40 ff. – jameda; *BGH*, Urt. v. 25.10.2011 - VI ZR 93/10, GRUR 2012, 311 Rn. 25 ff.

[80] S. etwa § 3b NetzDG.

[81] S. zum Beispiel § 14 UrhDaG und Art. Art. 20 DSA.

[82] S. zum Beispiel § 3c, 3f NetzDG, §§ 16, 17 UrhDaG und Art. 21 DSA.

[83] Ähnlich auch *Senftleben*, ZUM 2019, 369, 373; *Wagner,* GRUR 2020, 447, 452; *Weiden*, GRUR 2019, 370, 372.

[84] Ein solcher Schadensersatzanspruch ergibt sich etwa aus § 18 Abs. 2 UrhDaG. S. dazu *Raue* in: Dreier/Schulze, § 18 UrhDaG Rn. 12 ff. m.w.N. S. insbesondere zur Problematik des fehlenden materiellen Schadens der Nutzer *Spindler*, WRP 2021, 1245, 1246; *Wagner,* GRUR 2020, 447, 452.

[85] *Pille,* NJW 2018, 3545, 3548: „Legitimationsdefizit"; *Pille* in: Münchener Anwaltshandbuch IT-Recht, Teil 15.2 Rn. 43; *Pille,* Meinungsmacht sozialer Netzwerke, S.335 f., 360 ff.

Vor allem wenn den Diensteanbietern auferlegt wird, über die Rechtmäßigkeit beanstandeter Inhalte zu entscheiden oder Nutzern „rechtliches Gehör“[86] zu verschaffen, übernehmen sie Aufgaben, die grundsätzlich der staatlichen Rechtspflege vorbehalten sind. Insofern ist es konsequent, wenn eine „ausgeprägte Grundrechtsbindung“ privater Diensteanbieter im Hinblick auf die Freiheitsinteressen ihrer Nutzer vertreten wird.[87] Dennoch bleibt es bedenklich, dass die Abwägung verschiedener grundrechtlicher Interessen überwiegend in die Hände der Diensteanbieter gelegt wird. Vor allem verleiht es insbesondere großen Diensteanbietern noch mehr Macht und Einflussmöglichkeiten auf den öffentlichen Meinungsaustausch.[88]

Sicherlich ist es richtig, dass der Einfluss insbesondere großer Plattformen auf den öffentlichen Meinungsaustausch sehr groß ist. Gerade deshalb bedarf es aber eines regulatorischen Eingreifens des Gesetzgebers. Die Auslegung des Rechts, sowie die Bewertung von Einzelfällen sollte den Gerichten vorbehalten sein. Diese staatliche Aufgabe kann nicht einfach auf die Diensteanbieter verlagert werden, weil die Justiz droht, die große Anzahl der Fälle im Internet nicht bewältigen zu können und die Anonymität ein Vorgehen gegen die Nutzer als unmittelbare Rechtsverletzer erschwert. In jedem Fall müssen die Entscheidungen der Diensteanbieter gerichtlich überprüfbar sein.[89]

3. Diensteanbieter als Prozesspartei

Ein weiteres Problem ist, dass die Diensteanbieter durch ihre Verpflichtungen zur Prüfung oder zum Löschen von Inhalten Prozesspartei werden, obwohl die eigentliche Auseinandersetzung über die Rechtmäßigkeit eines Inhalts sich

---

[86] S. dazu *BGH,* Urt. v. 1.3.2016 – VI ZR 34/15, GRUR 2016, 855 Rn. 24, 40 ff. – jameda; *BGH*, Urt. v. 25.10.2011 - VI ZR 93/10, GRUR 2012, 311 Rn. 25 ff.; *Wagner*, GRUR 2020, 447, 453.

[87] S. *Friehe*, NJW 2020, 1697, 1699; *Jobst*, NJW 2020, 11, 12 ff.; *Kühling*, ZUM 2021, 461, 465 f.; *Tschorr,* MMR 2021, 204, 206 f. jeweils unter Bezugnahme auf *BVerfG*, Beschl. v. 6.11.2019 – 1 BvR 16/13, NJW 2020, 300 Rn. 77 – Recht auf Vergessen I; *BVerfG*, Beschl. v. 11.4.2018 – 1 BvR 3080/09, NJW 2018, 1667 Rn. 40 – Stadionverbot.

[88] Ähnlich *Wagner,* GRUR 2020, 447, 457.

[89] S. dazu auch *Pille,* NJW 2018, 3545, 3548.

in dem Verhältnis des verantwortlichen Nutzers zum Rechteinhaber abspielen müsste. Die Diensteanbieter sind insofern die „falsche Prozesspartei".[90]

Wenn die Rechteinhaber einen Inhalt beanstanden, hat das den Nachteil, dass die Diensteanbieter häufig nicht über die erforderlichen Informationen verfügen, um die Interessen der Nutzer wahrzunehmen.[91] Das ist vor allem der Fall, wenn ein Äußerungsdelikt im Raum steht. Der Diensteanbieter kann zum Beispiel nur schwer den Wahrheitsgehalt einer von einem Nutzer aufgestellten Tatsachenbehauptung überprüfen.[92] Zudem kennt der Diensteanbieter meist nicht den Hintergrund einer Aussage und kann nicht beurteilen, was sich eventuell im Vorfeld zwischen dem Nutzer und dem Rechteinhaber zugetragen hat.[93] Er kann daher nur schwerlich einen sinnvollen Vortrag etwa im Hinblick einer Interessensabwägung vornehmen.[94]

Zu einer echten Prozesspartei wird der Diensteanbieter, wenn entweder der Nutzer oder der Rechteinhaber gegen eine Entscheidung des Diensteanbieters über einen vermeintlich rechtswidrigen Inhalt gerichtlich vorgehen. Geht der Rechteinhaber gegen die Nichtlöschung eines Inhalts vor, sieht sich der Diensteanbieter in der Situation, den fremden Inhalt eines Nutzers verteidigen zu müssen.[95]
Aber auch für den betroffenen Rechtsinhaber und den Nutzer kann es nachteilig sein, den Prozess gegen den Diensteanbieter führen zu müssen: Der anonyme Nutzer kann seinen Inhalt im Verfahren zwischen Rechteinhaber und Diensteanbieter nicht verteidigen. Außerdem stellt sich die Frage, ob die Rechteinhaber überhaupt einen Anspruch auf der Grundlage der Störerhaftung gegen den Diensteanbieter auf Löschung des Inhalts haben, wenn dieser eine sorgfältige Prüfung durchgeführt, aber dennoch im Ergebnis eine andere Wertung

---

[90] *Wagner,* GRUR 2020, 329, 336.
[91] *Wagner*, GRUR 2020, 329, 336.
[92] *OLG Dresden*, Beschl. v. 7.1.2019 – 4 W 1149/18, NJW-RR 2019, 676 Rn. 15.
[93] Vgl. *Franz*, Der digitale Pranger, S. 21: „Stellvertreterprozess"; *Koreng*, GRUR-Prax 2017, 203, 204 f.
[94] *OLG Dresden*, Beschl. v. 7.1.2019 – 4 W 1149/18, NJW-RR 2019, 676 Rn. 15.
[95] *Pille*, NJW 2018, 3545, 3549.

vorgenommen hat. Einen Verstoß gegen Prüfpflichten wird man dem Diensteanbieter in diesem Fall kaum vorwerfen können.[96]

Ebenfalls problematisch ist, dass die Nutzer im Fall einer Löschung oder Sperrung durch Diensteanbieter, selbst gegen diesen vorgehen müssen. Das führt verglichen mit Rechtsverletzungen im Offline-Bereich zu einer Umkehr der Angriffs- und Prozesslast.[97] Außerhalb von Rechtsverletzungen im Internet müssten die Rechteinhaber gerichtlich gegen eine vermeintliche Rechtsverletzung vorgehen und tragen dadurch das Risiko des ungewissen Prozessausgangs und die Beweislast für die Rechtswidrigkeit des Inhalts.

Besonders bedenklich ist es, wenn bereits der Upload eines Inhalts etwa durch entsprechende Filter verhindert wird. Außerhalb des Internets würde zunächst eine Handlung erfolgen, die erst anschließend rechtlich bewertet wird.[98] Die Rechtsdurchsetzungslast würde die Rechteinhaber und nicht die Nutzer treffen. Dadurch, dass die Diensteanbieter verstärkt zur Verhinderung von Rechtsverletzungen im Internet in Anspruch genommen werden, werden diese Grundsätze aus dem Offline-Bereich zulasten der Nutzer umgekehrt.

4. Fazit zur Verlagerung der Verantwortlichkeit

Trotz all der aufgezeigten Probleme ist die Inpflichtnahme der Diensteanbieter nicht vollständig verzichtbar. Das liegt vor allem daran, dass eine lückenlose Identifizierung aller Internetnutzer nicht möglich oder jedenfalls wohl nicht verhältnismäßig wäre. Für den Fall, dass sich der unmittelbare Verletzer nicht ermitteln lässt, muss eine Rechtsdurchsetzung gegen die Diensteanbieter möglich sein. Vor allem die Anbieter großer Internetdienste müssen außerdem Verantwortung übernehmen für Gefahren, die von ihren Diensten ausgehen.[99]

Die Verlagerung der Verantwortung auf die Diensteanbieter kann und sollte aber eine Identifizierung der unmittelbaren Rechtsverletzer nicht ersetzen. Die vorherigen Ausführungen zeigen, dass grundsätzlich das Vorgehen gegen den

---

[96] *Pille*, NJW 2018, 3545, 3548.
[97] S. etwa *Becker,* ZUM 2019, 636, 640 ff.
[98] *Becker,* ZUM 2019, 636, 638 f.
[99] *Kühling*, ZUM 2021, 461, 462; *Wagner,* GRUR 2020, 329, 336 f.

unmittelbaren Rechtsverletzer gegenüber der Inanspruchnahme der Diensteanbieter vorzugswürdig ist.

Wird die Verantwortung für die Rechtsverletzungen der Nutzer fast vollständig auf die Diensteanbieter übertragen, würden die Diensteanbieter über Gebühr belastet werden. Dadurch können sie in ihrer Berufsfreiheit beeinträchtigt werden.[100]

Es ist deshalb wichtig, dass Identifizierungsmöglichkeiten der Rechteinhaber bestehen, damit ein Vorgehen gegen anonyme Nutzer nicht von vornherein ausgeschlossen wird. Die Inanspruchnahme des unmittelbaren Rechtsverletzers stellt ein Gegengewicht zur Haftung und Verantwortlichkeit der Diensteanbieter dar. Bei der Identifizierung anonymer Rechtsverletzer handelt es sich um ein wichtiges Instrument, das einen Ausgleich zum teilweise umfassenden Pflichtenprogramm der Diensteanbieter herstellen kann.

C. Zusammenfassung Kapitel 6

Weder die Identifizierung über den Umweg der Strafverfolgung noch die Verlagerung von Verantwortung auf die Diensteanbieter durch Haftung und die Übertragung von umfassenden Pflichten stellen Alternativen zur Identifizierung der Nutzer als unmittelbare Rechtsverletzer dar.

Der Identifizierung über den Umweg der Akteneinsicht im Strafverfahren, scheitert häufig daran, dass die Staatsanwaltschaften die Betroffenen auf den Privatklageweg verweisen oder das Verfahren nach § 153 StPO einstellen, ohne zuvor Ermittlungen anzustellen. Zudem überschreiten viele Rechtsverletzungen im Internet die Schwelle zur Strafbarkeit nicht. Bei weniger schweren Delikten, an deren Verfolgung kein besonderes öffentliches Interesse besteht, ist der Umweg der Identifizierung über die Akteneinsicht im Strafverfahren auch rechtspolitisch nicht sinnvoll.

---

[100] *Nolte*, ZUM 2017, 552, 560; *Pille*, NJW 2018, 3545, 3549.

Der erkennbare Trend in der Rechtsprechung und Gesetzgebung, anstelle einer Identifizierung der anonymen Nutzer, verstärkt die Diensteanbieter in die Verantwortung zu nehmen, ist zwar nachvollziehbar, aber nicht unbedenklich. Es besteht insbesondere die Gefahr, dass legale Inhalte fälschlicherweise gelöscht oder gesperrt werden. Zudem besteht ein Legitimationsdefizit der Diensteanbieter. Außerdem werden Rechtsstreitigkeiten als Konsequenz nicht zwischen den betroffenen Rechteinhabern und Nutzern, sondern zwischen lediglich einer der beiden Parteien und dem Diensteanbieter geführt, woraus verschiedene Folgeprobleme resultieren können.

Die Identifizierung der Nutzer über den Umweg des Strafverfahrens, über den Zivilrechtsweg sowie die Verpflichtung und Haftung der Diensteanbieter schließen sich nicht gegenseitig aus und können einander nicht vollständig ersetzen. Die beste Lösung besteht in einem sinnvollen Konzept für den Umgang mit anonymen Rechtsverletzungen im Internet, in dem alle denkbaren Instrumente Einzug finden und miteinander in Einklang gebracht werden.

Kapitel 7

Entwicklung eines allgemeinen Auskunftsanspruchs de lege ferenda

Die de lege lata existierenden Auskunftsansprüche sind in vielen Fällen nicht ausreichend, um anonyme Rechtsverletzer im Internet zu identifizieren. Daher soll im Folgenden ein allgemeiner Auskunftsanspruch gegen Internetdiensteanbieter de lege ferenda entwickelt werden, der die bestehenden Defizite möglichst weitgehend beheben soll.

Dabei gilt es zunächst zu betrachten, wie der Interessenkonflikt zwischen Diensteanbietern, Rechteinhabern und Nutzern de lege ferenda aufgelöst werden kann, um daraus Rückschlüsse für die Ausgestaltung eines Auskunftsanspruchs de lege ferenda zu ziehen. (A.)

Auf der Grundlage der bis dahin gewonnenen Erkenntnisse werden Überlegungen zu Inhalt und Umfang eines Auskunftsanspruchs gegen Internetdiensteanbieter de lege ferenda (B.), sowie zu den prozessualen (C.) und datenschutzrechtlichen (D.) Rahmenbedingungen eines solchen Anspruchs angestellt.

A. Überlegungen zur Lösung des Interessenskonflikts

Die oben dargestellten Interessen zwischen Diensteanbietern, Nutzern und Rechteinhabern müssen zu einem angemessenen Ausgleich gebracht werden. Dabei darf nicht eine der Parteien übermäßig belastet werden.

Für den Umgang mit anonymen Rechtsverletzungen im Internet bedarf es daher eines Gesamtkonzepts, das die Beteiligung der Diensteanbieter, die Inanspruchnahme anonymer Nutzer, sowie die Rechtsdurchsetzung der Rechteinhaber regelt. Maßgeblich für die Lösung des Interessenskonflikts sind die in Teil 2 dieser Arbeit untersuchten verfassungsrechtlichen Interessen der Parteien.

I. Bewertung des Interessensausgleichs de lege lata

Es ist sinnvoll, die derzeitige Rechtslage noch einmal im Hinblick auf die widerstreitenden Interessen zu betrachten, um daraus Schlüsse für die Lösung des Interessenskonflikts de lege ferenda zu ziehen.

Die Möglichkeiten der Rechteinhaber, anonyme Rechtsverletzer im Internet zu identifizieren, sind stark begrenzt. Selbst wenn in der Theorie ein Auskunftsanspruch gegen Diensteanbieter besteht, ist dieser häufig aus datenschutzrechtlichen Gründen nicht durchsetzbar, weil entweder die Diensteanbieter rechtlich nicht befugt sind, die Daten weiterzugeben oder bereits tatsächlich die Daten nicht (mehr) vorhanden sind.

Im Hinblick auf die Anonymität der unmittelbaren Rechtsverletzer werden häufig die Diensteanbieter zur Verantwortung gezogen. Sowohl die Rechtsprechung als auch der Gesetzgeber haben die Haftung von Diensteanbietern kontinuierlich weiterentwickelt und erlegen den Diensteanbietern zum Teil umfassende Pflichten auf.

Die Inanspruchnahme der Diensteanbieter anstelle der Nutzer bringt verschiedene Nachteile mit sich: Zu umfassende Pflichten der Diensteanbieter bergen die Gefahr des Overblockings und sogenannter „Chilling Effects".[1] Das gilt vor allem, wenn präventive Maßnahmen wie Upload-Filter ergriffen werden. Dadurch kann die Meinungs-, Kunst- oder Informationsfreiheit aller Nutzer beeinträchtigt werden. Zudem wäre die Identifizierung des Nutzers nachhaltiger, um zukünftigen Rechtsverletzungen vorzubeugen.[2] Wenn sich Rechtsverletzer im Internet sicher sein können, aufgrund ihrer Anonymität ohnehin nicht belangt werden zu können, werden Rechtsverletzungen im Internet weiter zunehmen. Außerdem ist es unter Berücksichtigung der Interessen aller Parteien sinnvoller, wenn sich Nutzer und Rechteinhaber als Streitparteien gegenüberstehen und wieder verstärkt Gerichte oder jedenfalls unabhängige Stellen im Streitfall über die Rechtmäßigkeit von Inhalten oder Handlungen im Internet entscheiden würden.

---

[1] S. bereits oben unter Kap. 6 § 2 C. I.

[2] *Pille* in: Münchener Anwaltshandbuch IT-Recht, Teil 15.2 Rn. 43: „disziplinierende Wirkung auf die Nutzer"; *Pille,* NJW 2018, 3545, 3549; *Löber/Roßnagel,* MMR 2019, 71, 76.

Die teilweise ausufernde Inpflichtnahme der Diensteanbieter bis hin zu einer eigenen Verletzerhaftung (§ 1 UrhDaG) für Rechtsverletzungen ihrer Nutzer beeinträchtigt deren unternehmerische Freiheit. Dies kann nur gerechtfertigt werden, wenn der Verhältnismäßigkeitsgrundsatz gewahrt ist. Wenn eine Identifizierung der Nutzer als unmittelbare Rechtsverletzer aber von vornherein ausscheidet, ist die alleinige Inanspruchnahme der Diensteanbieter meines Erachtens als nicht mehr angemessen zu werten.[3] Die alleinige Verantwortlichkeit spiegelt nicht den tatsächlichen Verursachungsbeitrag der Diensteanbieter wider und ist nur akzeptabel, wenn der Schutz der Anonymität der Internetnutzer das Interesse an deren Identifizierung überwiegt. Das kann etwa der Fall sein, wenn zugunsten von Identifizierungsmöglichkeiten die Rechte aller Internetnutzer übermäßig eingeschränkt werden müssten. Bei Nutzern, die rechtswidrig handeln, überwiegt das Interesse am Schutz ihrer Anonymität aber in der Regel nicht. Bestehen daher wie de lege lata in vielen Fällen von vornherein überhaupt keine oder nur äußerst unzureichende Möglichkeiten rechtsverletzende Nutzer zu identifizieren, ist die alleinige Inanspruchnahme der Diensteanbieter nicht zu rechtfertigen.

Dasselbe gilt auch im Hinblick auf den Schutz aller Internetnutzer vor den Gefahren durch Overblocking. Redliche Internetnutzer können im Einzelfall gegenüber den anonymen Rechtsverletzern bei einem Eingreifen der Diensteanbieter sogar schlechter gestellt sein: Die anonymen Nutzer, die tatsächlich die Rechte anderer verletzen, haben keinen Grund, sich über das Entfernen oder Sperren ihrer Informationen zu beschweren und haben gleichzeitig häufig kaum zu befürchten, selbst für ihre Rechtsverletzungen belangt zu werden. Wird aber ein rechtmäßiger Inhalt eines Nutzers entfernt oder blockiert, muss dieser selbst dagegen vorgehen. Kommt der Diensteanbieter dem Vortrag des Nutzers nicht nach, müsste dieser gerichtlich gegen die Entscheidung des Diensteanbieters vorgehen. Dafür müsste er aber seine Identität preisgeben. Zudem trifft ihn in diesem Fall die Beweis- und Prozesslast.

Während rechtsverletzende Nutzer also einfach an ihrer Anonymität festhalten können, werden die anderen Nutzer dazu gezwungen, entweder die Löschung

---

[3] Ähnlich auch *Nolte/Wimmers*, GRUR 2014, 16, 27: „Einseitig auf Inpflichtnahme der Diensteanbieter gerichtete Diskussion".

oder Blockierung eines rechtmäßigen Inhalts zu akzeptieren oder ihre Identität preiszugeben.

Aber auch für die Rechteinhaber kann es nachteilig sein, wenn sie nicht gegen die Nutzer selbst vorgehen können. Das gilt zum Beispiel, wenn von einem rechtsverletzenden Nutzer viele verschiedene Rechtsverletzungen ausgehen. Zudem besteht die Gefahr, dass derselbe Nutzer eine Rechtsverletzung bei einem anderen Dienst wiederholt, nachdem die Rechteanbieter bereits zuvor gegen einen Internetdiensteanbieter vorgegangen sind. Es entspricht dem Wunsch nach einem möglichst effektiven Rechtsschutz, die Ursache einer Rechtsverletzung zu bekämpfen, anstatt nur gegen ihre Folgen vorzugehen.

Die Identifizierung anonymer Rechtsverletzer ist daher ein wichtiges, ausgleichendes Element und ein Gegengewicht zu den umfassenden Pflichten und der Haftung der Diensteanbieter. Es dient dazu, die Rechte der Diensteanbieter und die der redlichen Internetnutzer mit jenen der Rechteinhaber in Ausgleich zu bringen. Dieses Instrument wird de lege lata aber zu wenig berücksichtigt.

II. Überlegungen zur Lösung des Interessenskonflikts de lege ferenda

Die unterschiedlichen Interessen der Diensteanbieter, Rechteinhaber und Nutzer müssen de lege ferenda so ausgeglichen werden, dass nicht eine der Parteien übermäßig belastet wird. Das gelingt unter Heranziehung der Grundsätze der praktischen Konkordanz und durch Überlegungen zu einer sinnvollen Verteilung von Lasten und Verantwortlichkeit.

1. Praktische Konkordanz

„Verfassungsrechtlich geschützte Rechtsgüter müssen in der Problemlösung einander so zugeordnet werden, daß jedes von ihnen Wirklichkeit gewinnt."[4]

Mit diesem Satz beschreibt *Hesse* den wesentlichen Aussagegehalt des Grundsatzes der praktischen Konkordanz: Bei einem Konflikt gegenläufiger Interessen soll allen Interessen möglichst weitgehend abgeholfen werden. Im Umkehrschluss heißt das aber auch, dass alle Beteiligten gleichermaßen

[4] *Hesse,* Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, Rn. 72.

Einschränkungen ihrer Rechte hinnehmen müssen.[5] Das Ziel der Lösung eines grundrechtlichen Konflikts ist damit ein möglichst schonender Ausgleich der verschiedenen Interessen.[6]

Greift man die obige Darstellung des Interessenskonflikts erneut auf, stehen für die verschiedenen Beteiligten im Wesentlichen die folgenden Interessen im Vordergrund: Die Rechteinhaber begehren Schutz ihrer Rechtsgüter wie zum Beispiel dem Recht auf Eigentum oder dem allgemeinen Persönlichkeitsrecht. Sie haben darüber hinaus ein Interesse an einem möglichst effektiven Rechtsschutz. Die Nutzer begehren Schutz ihrer Anonymität als Ausprägung ihres Rechts. Außerdem spielt häufig die Ausübung von Freiheitsrechten wie die Meinungs- oder Informationsfreiheit eine Rolle.Die Diensteanbieter können sich vor allem auf ihre unternehmerische Freiheit beziehungsweise ihre Berufsfreiheit stützen, die eine von Eingriffen Dritter geschützte und wirtschaftlich rentable Erbringung von Online-Diensten umfasst.

Wendet man die Grundsätze der praktischen Konkordanz an, müssen den Rechteinhabern möglichst wirksame Rechtsdurchsetzungsinstrumente zur Verfügung gestellt werden. Diese müssen allerdings – wie auch in der analogen Welt - nicht lückenlos sein. Begrenzt wird die Rechtsdurchsetzung durch die gegenläufigen Interessen der Nutzer und Diensteanbieter.

Anonyme Nutzer, die Rechte der Rechteinhaber verletzen, müssen deutliche Einschränkungen hinsichtlich ihrer Anonymität zugunsten der Rechtsdurchsetzung der Rechteinhaber hinnehmen. Grenzen bestehen vor allem, wenn unklar ist, ob überhaupt eine Rechtsverletzung vorliegt oder wenn anlasslos eine Vielzahl an Daten der Nutzer für die Aufhebung der Anonymität erhoben werden muss. Insbesondere gilt es die Interessen rechtmäßig agierender Nutzer zu schützen.

Die Diensteanbieter schaffen eine Gefahrenquelle und profitieren teilweise sogar von Rechtsverletzungen im Zusammenhang mit der Nutzung ihrer Dienste.[7] Daher müssen sie Einschränkungen im Hinblick auf ihre

---

[5] S. etwa *BVerfG,* Beschl. v. 16.5.1995 - 1 BvR 1087/91, NJW 1995, 2477, 2479 m.w.N.

[6] S. etwa *BVerfG,* Beschl. v. 16.5.1995 - 1 BvR 1087/91, NJW 1995, 2477, 2479 m.w.N.

[7] So mit Beispielen auch *Wagner,* GRUR 2021, 329, 337.

unternehmerische Freiheit und Berufsfreiheit hinnehmen. Diese Einschränkungen müssen allerdings dem Grad ihrer Verantwortlichkeit entsprechen. Zu ausufernde Verpflichtungen dürfen den Diensteanbietern ohne einen entsprechenden Ausgleich nicht aufgebürdet werden.

Die Auflösung des Interessenskonflikts de lege ferenda darf deshalb nicht ausschließlich zu Lasten einer der beteiligten Parteien gehen. Die Rechtsdurchsetzung darf bei anonymen Rechtsverletzungen im Internet nicht völlig unmöglich werden. Gleichzeitig kann aber das Recht auf Anonymität aller Internetnutzer nicht aufgehoben oder zu stark begrenzt werden. Zudem sollten die Diensteanbieter nicht die alleinige Verantwortung für Rechtsverletzungen ihrer Nutzer tragen müssen.

Dementsprechend müssen grundsätzlich Möglichkeiten für die Diensteanbieter bestehen, die Identität von Rechtsverletzern zu ermitteln. Diese müssen allerdings im Hinblick auf die Interessen der Internetnutzer verhältnismäßig sein. Die anonyme Nutzung von Internetdiensten muss allgemein weiterhin möglich sein. Die dadurch zwangsläufig entstehenden Rechtsdurchsetzungs-lücken sollten zumindest teilweise durch eine Inanspruchnahme der Diensteanbieter ausgeglichen werden können. Auch hierbei ist aber der Verhältnismäßigkeitsgrundsatz zu beachten. In die Abwägung können Kriterien wie der Umfang der Verantwortung und die Anzahl der Nutzer der Diensteanbieter einbezogen werden. Wenn dabei immer noch Lücken bei der Rechtsdurchsetzung verbleiben, müssen die Rechteinhaber dieses Risiko zugunsten eines angemessenen Interessensausgleichs in Kauf nehmen.

2.Verteilung von Lasten und Verantwortung

Bei der Frage, wie der Interessenskonflikt bei anonymen Rechtsverletzungen im Internet aufzulösen ist, spielt die gerechte Verteilung von Lasten und Verantwortung eine große Rolle. Dabei hilft es sich an allgemeinen, auch im analogen Bereich geltenden Grundsätzen zu orientieren. *Wagner* fasst diese Grundsätze sehr treffend zusammen:

„Eine undifferenzierte Verantwortlichkeit für das Tun und Lassen Dritter widerspricht aber auch dem elementaren deliktsrechtlichen Grundsatz, dass jeder für das eigene Verhalten verantwortlich ist und sich im Übrigen, außerhalb von Mitarbeiterverhältnissen nach dem Muster von

§ 831, darauf verlassen kann, dass die übrigen Akteure ihr eigenes Verhalten an den Geboten der Rechtsordnung ausrichten werden“[8]

Grundsätzlich ist also jeder für seine eigenen Handlungen und Unterlassungen selbst verantwortlich. Wer also zum Beispiel einen rechtsverletzenden Inhalt auf einer Plattform hochlädt, trägt die Verantwortung für diesen Inhalt. Dritte wie der Betreiber der Plattform dürfen grundsätzlich darauf vertrauen, dass sich ihre Nutzer rechtmäßig verhalten. Daher können sie für Inhalte ihrer Nutzer nicht ohne weiteres in die Pflicht genommen werden.

a) Anonyme Nutzer als Hauptverantwortliche

Die größte rechtliche Verantwortung sollte denjenigen treffen, der die Hauptverantwortung für eine Rechtsverletzung trägt und der der Rechtsverletzung am nächsten steht. Das ist in der Regel der Nutzer, von dem die Rechtsverletzung ursprünglich ausgeht.[9] Nur wenn man auch den Ursprung einer Rechtsverletzung bekämpft, kann man nachhaltig dazu beitragen, zukünftige Rechtsverletzungen zu verhindern und so der Verrohung der Online-Kommunikation entgegenzuwirken.[10]

b) Verhältnis zur Verantwortung der Diensteanbieter

Das kann aber im Umkehrschluss nicht bedeuten, dass die Diensteanbieter keinerlei Verantwortung für Handlungen ihrer Nutzer übernehmen müssen. Die Diensteanbieter schaffen durch Erbringung ihrer Dienste Gefahrenquellen sowohl für die Rechte anderer als auch für den öffentlichen Diskurs. Sie müssen sich deshalb an der Eindämmung dieser Gefahren beteiligen.[11]

---

[8] *Wagner* in: MüKo BGB, § 823 BGB Rn. 838

[9] Ebenfalls die Eigenverantwortlichkeit der Nutzer in den Vordergrund stellend *Pille,* NJW 2018, 3545, 3545 ff.

[10] *Janal,* ZEuP 2021, 227, 258 f.: „Eine dauerhafte Beendigung der Rechtsverletzung setzt zudem voraus, das Übel an der Wurzel anzupacken“; *Pille* in: Münchener Anwaltshandbuch IT-Recht, Teil 15.2 Rn. 43: „disziplinierende Wirkung auf die Nutzer“; *Pille,* NJW 2018, 3545, 3549; *Löber/Roßnagel,* MMR 2019, 71, 76.

[11] *Kühling,* ZUM 2021, 461, 462.

Allerdings kann nicht die Lösung sämtlicher Probleme, die moderne Kommunikationsmedien mit sich bringen, den Diensteanbietern überlassen werden. Es ist essenziell, dass die Nutzer lernen, verantwortungsvoll mit den Möglichkeiten umzugehen, die moderne Internetdienste bieten. Dafür ist es aber unerlässlich, dass sie auch selbst für ihre Rechtsverletzungen belangt werden können. Wie viel Verantwortung die Diensteanbieter darüber hinaus neben den Nutzern übernehmen müssen, lässt sich anhand verschiedener Kriterien bestimmen.

aa) Nähe zur Rechtsverletzung

Relevant ist dabei zunächst die Nähe des Diensteanbieters zur Rechtsverletzung. Je stärker der Diensteanbieter an der Rechtsverletzung beteiligt ist, desto mehr Verantwortung muss er auch übernehmen. Entscheidend ist dafür, welche Einwirkungsmöglichkeiten der Diensteanbieter überhaupt hat und inwieweit er davon Gebrauch gemacht hat.

Hierbei ist zunächst nach der Art des Dienstes zu unterscheiden. Zugangsanbieter beispielsweise ermöglichen lediglich die Nutzung von Internetdiensten, indem sie die erforderliche Internetverbindung herstellen. Sie haben unmittelbar keine Einwirkungsmöglichkeit auf Handlungen ihrer Nutzer. Damit können sie grundsätzlich als neutrale Dienste angesehen werden. Host-Provider dagegen speichern die Inhalte ihrer Nutzer. Damit haben sie stets die Kontrolle über die gespeicherten Inhalte. Die Erbringung ihres Dienstes steht daher in einem deutlich engeren Zusammenhang zur Rechtsverletzung.

Es ist daher sinnvoll, wenn Host-Provider aufgrund ihrer Nähe zur Rechtsverletzung erweiterte Pflichten übernehmen müssen. Insbesondere können sie dazu verpflichtet werden, Beschwerden über möglicherweise rechtsverletzende Inhalte entgegenzunehmen und die Funktion eines „Streitmittlers“ zu übernehmen, indem sie zum Beispiel den Kontakt zwischen dem Rechteinhaber und dem Nutzer herstellen.

Verlassen Host-Provider ihre neutrale Stellung als bloße Vermittler von Inhalten, indem sie sich Inhalte zu eigen machen, müssen sie auch darüber hinaus für die Inhalte haften.

bb) Gefahrgeneigtheit des Dienstes

Ein weiterer Faktor ist die Gefahr, die von einem Dienst ausgeht. Je größer diese Gefahr ist, desto mehr Verantwortung müssen die Diensteanbieter übernehmen.

Das gilt insbesondere für strukturelle Gefahren, die nicht auf die Verletzung individueller Rechte beschränkt sind. Dazu zählen etwa die Bekämpfung von Fake News, sowie die Gefahren für den öffentlichen Meinungsaustausch durch den Einsatz von Social Bots.[12] Diese Gefahren lassen sich ohne die Mitwirkung der Diensteanbieter nicht eindämmen. Vor allem große Diensteanbieter müssen hier als Gatekeeper verstärkt Verantwortung übernehmen.[13] Vereinfacht gilt, dass je mehr Nutzer etwa ein Hosting-Dienst hat, desto mehr Reichweite hat dieser Dienst und müsste deshalb auch mehr Verantwortung tragen. Aus diesem Grund sieht Abschnitt 5 des Digital Services Act besondere Verpflichtungen unter anderem für Anbieter sehr großer Plattformen.

Eine stärkere Verantwortung lässt sich auch begründen, wenn von einem Dienst aufgrund der Art des Dienstes besondere Gefährdungen für Rechte Dritter ausgehen. Das kann zum Beispiel der Fall sein, wenn ein Dienst seinen Nutzern das Verbreiten privater pornographischer Inhalte ermöglicht.

cc) Anonyme Nutzungsmöglichkeit

Des Weiteren müssen Host-Provider grundsätzlich stärker in die Verantwortung genommen werden, je mehr Anonymität sie ihren Nutzern ermöglichen. *Herwig* analysiert zutreffend, dass das Rechtsdurchsetzungsproblem der Rechteinhaber vor allem dann besteht, wenn die Host-Provider die Verantwortung für die Inhalte ihrer Nutzer ablehnen und gleichzeitig die Nutzer anonym auftreten.[14] Daraus leitet er ab, dass Host-Provider, die ihre Nutzer anonymisieren, selbst für die Rechtsverletzungen ihrer Nutzer haften müssten.[15]

---

[12] *Kühling*, ZUM 2021, 461, 470.

[13] *Wagner* in: MüKo BGB, § 823 BGB Rn. 839; *Wagner,* GRUR 2020, 329, 337.

[14] *Herwig*, ZD 2012, 558, 559.

[15] *Herwig*, ZD 2012, 558, 562.

Im Hinblick auf die Verteilung von Verantwortung ist diese Überlegung nachvollziehbar. Wenn ein Host-Provider die anonyme Nutzung seines Dienstes ermöglicht, dann ist es überzeugend, wenn er für die Inhalte seiner Nutzer auch mehr Verantwortung übernehmen muss. Das entspricht auch dem Grundgedanken, dass je größer die Gefahr ist, die von einem Dienst für die Rechte anderer ausgeht, desto mehr Verantwortung die Diensteanbieter tragen müssen. Schließlich kann auch die Anonymität der Nutzer die Gefahren erhöhen, die von einem Hosting-Dienst ausgehen. Ein ähnlicher Gedanke findet sich auch in der Rechtsprechung des *BGH*, der teilweise Host-Providern strengere Prüfpflichten auferlegt, wenn diese die Klarnamen ihrer Nutzer nicht erfragt beziehungsweise gespeichert hatten.[16]

Der Ansatz von *Herwig* ginge allerdings über eine bloße stärkere Verantwortlichkeit hinaus und würde konsequenterweise Hosting-Dienste, die anonym nutzbar sind, von den Haftungsprivilegierungen ausnehmen. Ein erheblicher Nachteil an dieser Lösung ist, dass sie falsche Anreize an die Diensteanbieter setzen würde. Wenn diese von der Haftungsprivilegierung profitieren wollten, dürften sie ihre Dienste überhaupt nicht mehr anonym anbieten. Täten sie das nicht, wäre es ihnen anderenfalls häufig auch gar nicht möglich, alle Inhalte vorab zu kontrollieren, um einer Haftung zu entgehen. Macht man die Haftungsprivilegierung davon abhängig, ob der Nutzer anonymisiert auftreten darf, würde man daher bestimmte Geschäftsmodelle praktisch abschaffen, beziehungsweise die Diensteanbieter dazu zwingen, alle Nutzer zu deanonymisieren.

Die Anonymität im Internet ist – trotz ihrer beschriebenen negativen Auswirkungen – für die Freiheitsausübung der Nutzer von großer Bedeutung. Vor allem in autokratischen Systemen ist die Kommunikation über das Internet häufig die einzige Möglichkeit der Menschen, von ihrem Recht auf freie Meinungsäußerung und ihrer Informationsfreiheit Gebrauch zu machen. Aber auch in demokratischen Staaten bestehen berechtigte Interessen daran, im Internet anonym auftreten zu können. Auch hier können kritische Fragen aufgeworfen und Meinungen geäußert werden, ohne dass die Menschen Repressionen

---

[16] *BGH*, Urt. v. 12.7.2007 - I ZR 18/04, GRUR 2007, 890 Rn. 25 ff. – Jugendgefährdende Medien bei eBay; *BGH,* Urt. v. 15. 8. 2013 – I ZR 80/12, GRUR 2013, 1030 Rn. 40 ff. – File-Hosting-Dienst; *OLG Hamburg*, Urt. v. 2.3.2017 – 29 U 1797/16, MMR 2017, 628, 631 – Gray's Anatomy.

befürchten müssen. Sowohl die Meinungsvielfalt als auch künstlerische Auseinandersetzungen können dadurch gefördert werden. Zudem ermöglicht es die Anonymität Whistleblowern, auf Missstände in der Gesellschaft oder in größeren Unternehmen hinzuweisen.

Dennoch ist aber zumindest der Grundgedanke richtig, dass Host-Provider, deren Dienste anonym genutzt werden, stärker in die Verantwortung genommen werden müssen. Das bedeutet aber lediglich, dass sie erhöhte Prüfpflichten treffen und sie bei einem Verstoß gegen diese Pflichten auch haftbar gemacht werden können. Dennoch verbleibende Lücken bei der Rechtsdurchsetzung müssen im Sinne eines möglichst schonenden Interessensausgleichs von den Rechteinhabern hingenommen werden. Das gilt insbesondere im Hinblick darauf, dass es eine vollständige Anonymität im Internet ohnehin praktisch kaum gibt. Auch wenn ein Nutzer gegenüber dem Rechteinhaber anonym ist, bedeutet das nicht, dass eine Identifizierung nicht möglich ist. Auskunftsansprüche gegen die Diensteanbieter können deshalb einen Ausgleich für die Haftungsprivilegierung der Diensteanbieter darstellen.

Im Umkehrschluss bedeutet das aber auch, dass Diensteanbieter, die ihre Nutzer selbst einfach identifizieren können, weil sie etwa die Klarnamen hinterlegt haben, weniger Pflichten treffen. In diesem Fall lässt sich eine subsidiäre Haftung erwägen.

c) Rechtsdurchsetzungslast der Rechteinhaber

Als weiterer Maßstab für die angestrebte Lösung des Interessenskonflikts dient neben der Verteilung von Verantwortung noch ein weiterer Grundsatz, der im Offline-Bereich selbstverständlich ist: Die Last für die Durchsetzung ihrer Rechte müssen die Rechteinhaber grundsätzlich selbst tragen. Die Rechteinhaber müssen also ihre Rechte gegebenenfalls auch gerichtlich durchsetzen und tragen dabei die Risiken des Prozesses und insbesondere die Gefahr der Kostentragung.

Dieser Grundsatz wird ins Gegenteil verkehrt, wenn die Nutzer auf die Entscheidung eines Diensteanbieters über einen von einem Rechteinhaber beanstandeten Inhalt reagieren müssen und gegebenenfalls gerichtlich gegen diese

Entscheidung vorgehen müssen.[17] Kritisch sind vor diesem Hintergrund proaktive Maßnahmen der Diensteanbieter wie die Verhinderung kerngleicher Rechtsverletzungen oder die Einführung von Upload-Filtern zu sehen, da diese die Umkehr der Angriffs- und Prozesslast noch verschärfen. Besser eingrenzen lässt sich die Gefahr zukünftiger Rechtsverletzungen, indem die verantwortlichen Nutzer identifiziert werden und selbst für ihre Rechtsverletzungen belangt werden können.[18]

Aufgrund der Anonymität vieler Internetnutzer ist es aber jedenfalls erforderlich, dass Host-Provider auf einen entsprechenden Hinweis hin Inhalte ihrer Nutzer prüfen müssen – wie es künftig Art. 16, 17 DSA vorsieht. Durch ein sinnvolles Beschwerdemanagement, in dem auch die Nutzerseite berücksichtigt wird, sowie durch außergerichtliche Streitbeilegung, können die daraus resultierenden Nachteile für die Nutzer minimiert werden. Auch hier enthalten Art. 20, 21 DSA bereits Anknüpfungspunkte für die Zukunft.

Daneben sollten aber die Identifizierungsmöglichkeiten der Rechteinhaber ausgeweitet werden, um eine Rechtsdurchsetzung gegen die Nutzer selbst zu ermöglichen, bei der die Rechteinhaber vergleichbar mit der analogen Welt die Rechtsdurchsetzungslast tragen.

d) Schutz der Freiheitsausübung der Nutzer

Damit einhergehend muss der Schutz der Freiheitsausübung von Internetnutzern berücksichtigt werden. Wenn sich die Rechtsdurchsetzung häufiger im Verhältnis zwischen Rechteinhabern und Nutzern abspielt, reduziert sich auch die Gefahr, dass die Diensteanbieter Inhalte fälschlicherweise löschen oder Informationen sperren.

Sicherlich ist es aber richtig, dass nicht nur die Gefahren des Overblockings zu den gefürchteten chilling effects der Nutzer führen können, sondern auch Auskunftsansprüche einen vergleichbaren Effekt haben könnten. Es ist zu

---

[17] S. etwa *Becker,* ZUM 2019, 636, 640 ff.

[18] Ähnlich *Pille* in: Münchener Anwaltshandbuch IT-Recht, Teil 15.2 Rn. 43: „disziplinierende Wirkung auf die Nutzer"; *Pille,* NJW 2018, 3545, 3549; *Löber/Roßnagel,* MMR 2019, 71, 76.

befürchten, dass Nutzer aus Angst vor Aufdeckung ihrer Anonymität und davor, mit einem gerichtlichen Verfahren belastet zu werden, sich selbst zensieren.[19] In gewisser Weise sind solche Effekte aber sogar beabsichtigt. Die Nutzer sollen sich schließlich damit auseinandersetzen, ob ihre Inhalte rechtmäßig sind und selbst für diese Verantwortung übernehmen. Lediglich die Gefahren durch unberechtigte Auskunftsersuchen der Rechteinhaber gilt es zu minimieren.

Zudem darf nicht übersehen werden, dass eine Selbstzensur der Nutzer auch durch die Verrohung der Kommunikation im Internet droht, die durch die Anonymität der Nutzer jedenfalls begünstigt wird. Vor allem bei kontroversen Themen könnten sich viele Menschen aus dem öffentlichen Diskurs zurückziehen, wenn sie sich andernfalls mit einer Welle von Hassnachrichten durch zum Teil anonyme Nutzer konfrontiert sähen.[20]

III. Lösungsansätze

Auf Grundlage der bislang gewonnenen Erkenntnisse sollen nachfolgend Ansätze für die Lösung des Interessensausgleichs de lege ferenda dargestellt werden. Das Ziel dabei ist es aber nicht, die zum Teil sehr ausdifferenzierte Gesetzgebung und Rechtsprechung zur Haftung und den Pflichten der Diensteanbieter auf nationaler sowie auf EU-Ebene völlig neu zu denken. Im Vordergrund steht dagegen vielmehr die Frage, auf welche Weise Auskunftsansprüche zur Identifizierung anonymer Internetnutzer sinnvoll in die bestehenden Konzepte eingebunden werden können und an welcher Stelle Anpassungen erforderlich sein könnten.

1. Schaffung eines möglichst wirksamen Auskunftsanspruchs

Der zentrale Bestandteil für die Lösung des Interessenskonflikt de lege ferenda ist die Schaffung eines möglichst effektiven Auskunftsanspruchs der Rechteinhaber gegen die Anbieter von Internetdiensten, um ihnen die Identifizierung anonymer Nutzer zu ermöglichen. Die Möglichkeiten der Inanspruchnahme der anonymen Nutzer zu verbessern, stellt ein entscheidendes

---

[19] *Koreng,* GRUR-Prax 2017, 203, 205.

[20] *Bohlen,* NJW 2020, 1999, 2004 unter Bezugnahme auf *Gesetzesentwurf,* BT-Drs. 19/17741, 1; Ähnlich auch *Kühling,* ZUM 2021, 461, 472.

Gegengewicht zur Verantwortung der Diensteanbieter dar, das zu einem schonenden Ausgleich der widerstreitenden Interessen beiträgt.

Der Auskunftsanspruch sollte möglichst viele Identifizierungsmöglichkeiten öffnen und daher alle unterschiedlichen Diensteanbieter und grundsätzlich auch alle Daten, die zur Identifizierung der Diensteanbieter beitragen können, umfassen.

Der weite Umfang des Auskunftsanspruchs ist erforderlich, da trotz der Einführung von Auskunftsansprüchen die Anonymität aller Internetnutzer möglichst wenig eingeschränkt werden soll. Wenn aber nicht zum Beispiel im Rahmen einer Registrierungspflicht systematisch bestimmte Daten aller Nutzer verpflichtend erhoben werden, ist es erforderlich, die Identifizierungsmöglichkeiten so weit wie möglich auszuweiten.

Klar ist, dass der Identifizierung von Nutzern über Auskunftsansprüche Grenzen gesetzt sein werden. Wenn kein Zwang für die Diensteanbieter bestehen soll, Nutzerdaten anlasslos zu erheben, wird sich die Identität vieler Nutzer trotz Auskunftsanspruch nicht feststellen lassen. Das gilt vor allem, wenn die Nutzer zusätzlich Anonymisierungsdienste verwenden.

Teilweise wird gegen die Ausweitung von Auskunftsansprüchen auf die Gefahr hingewiesen, dass mehr Nutzer Anonymisierungsdienste nutzen oder ins Darknet ausweichen könnten, was sich kontraproduktiv auf die Strafverfolgung auswirken könnte.[21] Diese Gefahr dürfte allerdings geringer sein als angenommen, da vielen Nutzern erkennbar die Sensibilität für den Schutz ihrer Daten fehlt und durch einen wirksamen Auskunftsanspruch de lege ferenda auch grundsätzlich nicht mehr Daten erhoben werden sollten als vorher. Außerdem sind viele Anonymisierungsdienste kostenpflichtig und für die alltägliche Nutzung von Internetdiensten zum Beispiel über das Smartphone für viele Nutzer unattraktiv. Zudem sind zivilrechtliche Auskunftsansprüche im Verhältnis zu den Ermittlungen durch Strafverfolgungsbehörden ein milderes Mittel und dürften daher auch weniger Abschreckungspotential haben.

---

[21] *Koreng*, GRUR-Prax 2017, 203, 205; Ähnlich auch *Kersten,* JuS 2017, 193, 203: „Vorratsdatenspeicherung als „überwachungsstaatliche Werbung für das Darknet".

Dass einzelne Nutzer insbesondere zur Vermeidung der Strafverfolgung auf Anonymisierungsdienste zurückgreifen, ist ein bekanntes Problem, das sich durch die Ausweitung der Auskunftsansprüche aber zumindest nicht wesentlich verstärken dürfte. Das sieht man auch daran, dass zum Beispiel sehr viele Filesharing-Nutzer trotz der Einführung des Auskunftsanspruchs aus § 101 Abs. 2 UrhG noch bis heute anhand ihrer IP-Adresse zurückverfolgt werden können.

2. Einschränkung der Anonymität der Nutzer

Auskunftsansprüche zur Identifizierung von Internetnutzern müssen von entsprechenden datenschutzrechtlichen Regelungen zur Speicherung und Verwendung von Daten zur Auskunftserteilung flankiert werden. Die Ausweitung der Auskunftsansprüche geht daher unweigerlich mit einer Einschränkung der Anonymität der Nutzer einher.

Diese Begrenzung der Anonymität rechtsverletzender Nutzer ist verfassungsrechtlich nicht nur gerechtfertigt, sondern im Hinblick auf einen möglichst schonenden Interessensausgleich sogar geboten. Das Recht eines Nutzers auf Anonymität überwiegt selbst bei weniger schweren Rechtsverletzungen nicht die Interessen der Rechteinhaber, Diensteanbieter und der rechtmäßig agierenden Nutzer.[22] Dem Umstand, dass vor einer Auskunftserteilung unklar ist, ob eine Rechtsverletzung tatsächlich vorliegt, kann durch ein Offensichtlichkeitserfordernis bzw. einen Richtervorbehalt ausgeglichen werden.

Es muss daher so weit wie möglich verhindert werden, dass Nutzerdaten unberechtigterweise herausgegeben werden. Außerdem sollten die Möglichkeiten der anlasslosen Speicherung von Nutzerdaten nicht zum Zwecke der Ergänzung von Auskunftsansprüchen ausgeweitet werden.

3. Vorbeugung von Missbrauch

Zum Schutz der Anonymität der Internetnutzer muss außerdem dem Missbrauch von Auskunftsansprüchen gegen Internetdiensteanbieter vorgebeugt werden.

---

[22] Vergleich mit Aufhebung der Pseudonymität eines Autofahrers durch Kennzeichen bei Parkverstoß *Herwig*, ZD 2012, 558, 560.

Die Verfolgung von Rechtsverstößen und die Durchsetzung absoluter Rechte ist aber nicht missbräuchlich. Das gilt grundsätzlich auch für Massenabmahnungen zum Beispiel in Filesharing-Fällen, selbst wenn dahinter finanzielle Interessen spezialisierter Unternehmen stehen.[23]

Vielmehr müssen die Nutzer vor einer rechtsmissbräuchlichen Verwendung von Auskunftsansprüchen zur Ausforschung von Nutzerdaten beziehungsweise davor, dass bewusst nicht bestehende Rechte geltend gemacht werden, geschützt werden.[24] Diese Missbrauchsgefahren lassen sich aber vor allem durch prozessuale Instrumente eindämmen.

4. Subsidiäre Haftung der Diensteanbieter

Auch wenn die Auskunftsmöglichkeiten de lege ferenda ausgeweitet werden, wird die Inanspruchnahme der Nutzer und damit der hauptverantwortlichen Rechtsverletzer nicht immer möglich beziehungsweise den Rechteinhabern nicht immer zumutbar sein. Im Sinne der Verhältnismäßigkeit kann kein Auskunftsanspruch die unbegrenzte Identifizierung aller Internetnutzer ermöglichen. Daher muss jedenfalls subsidiär zur Haftung der Nutzer auch die Inanspruchnahme der Diensteanbieter möglich sein.

Selbst wenn eine Identifizierung der Nutzer möglich ist, kann diese und insbesondere die anschließende Rechtsdurchsetzung gegen den Nutzer teuer und sehr zeitaufwändig sein.[25]

Die Intensität der Rechtsverletzung kann sich aber erheblich verstärken, je länger ein Inhalt online abrufbar ist.[26] Sicherlich ist es zum Beispiel dem Betroffenen von einer schweren Persönlichkeitsrechtsverletzung im Zusammenhang mit der Veröffentlichung intimer Bilder oder massivster Diffamierungen nur schwer zumutbar, zunächst Auskunft über die Identität des Nutzers einholen zu müssen und anschließend Ansprüche gegen den verantwortlichen Nutzer

---

[23] So auch *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 120 f. m.w.N. A.A. *Tyra,* ZUM 2009, 934, 942 ff.; *Solmecke/Dierking*, MMR 2009, 727, 727 ff.

[24] S. auch *Hennemann,* Urheberrechtsdurchsetzung und Internet, S. 121.

[25] S. etwa *Wagner* in: MüKo BGB, § 823 Rn. 836.

[26] *Wagner,* GRUR 2020, 239, 336 f.

gegebenenfalls gerichtlich durchsetzen zu müssen. In der Zwischenzeit blieben die Inhalte nämlich abrufbar und könnten weiterverbreitet werden.

Aus diesem Grund herrscht in der Rechtsprechung weitgehend Einigkeit darüber, dass die Haftung von Host-Providern für einen effektiven Grundrechtsschutz erforderlich und nicht subsidiär zur Inanspruchnahme der Nutzer sei.[27]

Im Zusammenhang mit der Ausweitung der Auskunftsansprüche sollte aber dennoch grundsätzlich die subsidiäre Haftung aller Diensteanbieter angestrebt werden.[28] Andernfalls bestünde die Gefahr, dass die Rechteinhaber von der häufig einfacheren Inanspruchnahme der Diensteanbieter Gebrauch machen, ohne die Identifizierung des Nutzers voranzutreiben. Die Ziele des Auskunftsanspruchs de lege ferenda sind es aber, den Ursprung der Rechtsverletzungen nachhaltiger zu bekämpfen[29] und einen Ausgleich zu der mit Folgeproblemen behafteten sehr umfassenden Inpflichtnahme der Diensteanbieter herzustellen. Dabei geht es neben den Interessen der Diensteanbieter auch um den Schutz der rechtmäßig agierenden Nutzer. Diese Ziele würden verfehlt, wenn die Rechteinhaber von den Auskunftsansprüchen überhaupt keinen Gebrauch machen würden. Die Subsidiarität der Haftung der Diensteanbieter ist damit auch Ausdruck des Verhältnismäßigkeitsgrundsatzes.[30]

---

[27] *BGH,* Urt. v. 10.1.2019 – I ZR 267/15, MMR 2019, 522 Rn. 94 – Cordoba II; *BGH*, Urt. v. 27.2.2018 – VI ZR 489/16, NJW 2018, 2324 Rn. 45 – Internetforum; *BGH,* Urt. v. 27 3 2007 - VI ZR 101/06, NJW 2007, 2558 Rn. 13. S. auch *EuGH,* Urt. v. 14.6. 2012 – C-618/10, NJW 2012, 2257 Rn. 82 ff. – Google Spain.

[28] Im Grundsatz ebenfalls befürwortend *Leistner/Grisse,* GRUR 2015, 105, 107 f.; *Nolte/Wimmers,* GRUR 2014, 16, 27; *Pfeifer,* AfP 2015, 193, 199; *Spindler*, MMR 2018, 48, 52. S. auch *Pille,* NJW 2018, 3545, 3550, der eine Inanspruchnahme der Diensteanbieter nur für zulässig erachtet, wenn diese ihren Pflichten zur Identitätserfassung oder -mitteilung nicht nachkommen.

[29] Ähnlich *Pille* in: Münchener Anwaltshandbuch IT-Recht, Teil 15.2 Rn. 43: „disziplinierende Wirkung auf die Nutzer"; *Pille,* NJW 2018, 3545, 3549; *Löber/Roßnagel,* MMR 2019, 71, 76.

[30] *Hindelang,* Freiheit und Kommunikation, S. 321 f.; *Nolte/Wimmers,* GRUR 2014, 16, 24. Anders aber wohl *BVerfG,* Beschl. v. 6.11.2019 – 1 BvR 276/17, NJW 2020, 314 Rn. 119 – Recht auf Vergessen II, das die Inanspruchnahme der Diensteanbieter unter Effizienzgesichtspunkten als gleich- oder sogar vorrangig ansieht.

Von dem Grundsatz der subsidiären Haftung muss es im Hinblick auf die Interessen der Rechteinhaber allerdings Ausnahmen geben. Dabei spielen unter anderem die oben angestellten Überlegungen zur Verantwortlichkeit der Diensteanbieter eine Rolle.

Dem *BGH* ist insofern zuzustimmen, dass Dienste wie Host-Provider, die aufgrund ihrer Nähe zur Rechtsverletzung stärkere Einwirkungsmöglichkeiten haben, auch mehr Verantwortung tragen müssen. Bei reinen Zugangsdiensten kommt dagegen ohnehin lediglich eine subsidiäre Haftung in Betracht.[31] So können nach § 7 Abs. 4 TMG bereits jetzt WLAN-Betreiber nur auf Sperrung von Informationen in Anspruch genommen werden, wenn die Rechteinhaber keine anderweitigen Möglichkeiten haben, der Verletzung ihrer Rechte abzuhelfen. Dasselbe gilt zum Beispiel auch für Domain Registries und Domain-Registrare.[32]

Aber auch Host-Provider sollten in bestimmten Grenzen lediglich subsidiär haften. Sofern diese aber selbst als unmittelbare Rechtsverletzer auftreten, kommt eine subsidiäre Haftung nicht in Betracht.

Im Anwendungsbereich von Art. 17 DSM-RL wäre eine subsidiäre Haftung der Diensteanbieter im nationalen Recht unter anderem aus diesem Grund ohnehin unionsrechtswidrig. In Umsetzung dieser Richtlinie sieht § 12 III UrhDaG sogar umgekehrt vor, dass die Nutzer bis zum Abschluss eines Beschwerdeverfahrens nicht selbst verantwortlich gemacht werden dürfen. In diesem Bereich wäre zunächst eine Anpassung auf Unionsebene erforderlich. Ohnehin wäre eine Gleichbehandlung der Inhaber verschiedener absoluter Rechte wünschenswert, die eine Auflösung der Unterschiede zwischen DSM-RL beziehungsweise UrhDaG und DSA voraussetzen würde.[33] Einer subsidiären Haftung von Host-

---

[31] *BGH,* Urt. v. 26.11.2015 – I ZR 174/14, GRUR 2016, 268 Rn. 81 ff. – Störerhaftung des Access-Providers.

[32] S. zu den Registries *BGH*, Urt. v. 17.5.2001 - I ZR 251/99, GRUR 2001, 1038, 1039 f. – ambiente.de; *BGH,* Urt. v. 27.10.2011 - I ZR 131/10, GRUR 2012, 651 Rn. 24 f. – regierung-oberfranken.de. S. zu den Registraren *BGH*, Urt. v. 15.10.2020 – I ZR 13/19, GRUR 2021, 63 Rn. 30 ff. – Störerhaftung des Registrars. S. dazu auch *Hofmann*, NJW 2021, 274, 275 f.; *Nordemann,* GRUR 2021, 18, 18 ff.

[33] S. zum Verhältnis zwischen Art. 17 DSM-RL beziehungsweise dem UrhDaG und dem DSA etwa *Janal,* GRUR 2022, 211, 211 ff.

Providern steht im Bereich des geistigen Eigentums außerdem entgegen, dass die Mitgliedstaaten nach der Rechtsprechung des *EuGH* zur InfoSoc-Richtlinie und zur Enforcement-Richtlinie eine präventive Inanspruchnahme von Host-Providern vorsehen müssen.[34] Entsprechende Anpassungen hinsichtlich einer subsidiären Haftung von Host-Providern müssten daher auf Unionsebene erfolgen.

Außerhalb des Geltungsbereichs der genannten Richtlinien wird zukünftig vor allem der Digital Services Act Vorgaben für Pflichten und der Haftung der Diensteanbieter in den Mitgliedstaaten machen. Der DSA regelt das Verhältnis zwischen der Haftung der Diensteanbieter und der Haftung der Nutzer nicht ausdrücklich. In erster Linie sieht der DSA Pflichten der für Host-Provider wie ein verpflichtendes Notice-and-Take-Down-Verfahren in Art. 16, 17 DSA vor. Besondere Pflichten - wie ein internes Beschwerdemanagement (Art. 20 DSA) und die Zusammenarbeit mit außergerichtlichen Streitbeilegungsstellen (Art. 21 DSA) – treffen zudem Online-Plattformen, die die gespeicherten Inhalte ihrer Nutzer öffentlich verbreiten.[35] Allerdings schließt der umfassende Pflichtenkatalog eine lediglich subsidiäre Haftung der Diensteanbieter auch nicht aus. Die Subsidiarität würde lediglich dazu führen, dass im Falle einer Pflichtverletzung des Diensteanbieters dieser nur haftet, wenn die Inanspruchnahme des für den fraglichen Inhalt verantwortlichen Nutzers ausscheidet. Ein Widerspruch zu den Pflichten aus dem DSA ergibt sich daher nicht. Dies lässt sich auch aus Erwägungsgrund 27 des DSA ableiten, der vorsieht, dass Dritte, die von im Internet übertragenen oder gespeicherten rechtswidrigen Inhalten betroffen sind, versuchen sollen, Konflikte – wenn möglich – , ohne die Beteiligung der Diensteanbieter zu lösen. Zudem sollen die Nutzer für ihre Inhalte nach den Vorschriften des Unionsrechts und des nationalen Rechts haften.

Dennoch wäre es sinnvoll, im Hinblick auf den grenzüberschreitenden Charakter des Internets und dem Ziel einer weitgehenden Harmonisierung, das

---

[34] EuGH, Urt. v. 16. 2. 2012 - C-360/10, GRUR 2012. 382 Rn. 29 – Netlog/SABAM; EuGH, Urt. v. 12.7.2011 - C-324/09, GRUR 2011, 1025 Rn. 131 – Lóreal/eBay. S. ausführlich dazu *Fischer,* Die Einbindung von Providern, S. 239 ff.

[35] Online-Plattformen sind in Art. 2 lit. i) DSA legaldefiniert und stellen eine Unterkategorie der Host-Provider dar, die die Inhalte der Nutzer nicht nur speichern, sondern auch öffentlich verbreiten und so einer unbegrenzten Zahl an Nutzern zugänglich machen.

Verhältnis der Haftung der Diensteanbieter zur Haftung des Nutzers auf Unionsebene zu klären.

Bei der Frage nach der Subsidiarität der Haftung der Diensteanbieter müssen die Gefahren für die Rechteinhaber durch einen möglicherweise rechtsverletzenden Inhalt beachtet werden. Die Subsidiarität bewirkt, dass die Rechtsverletzer unabhängig von einer Pflichtverletzung der Diensteanbieter immer zuerst versuchen müssten, zum Beispiel Unterlassungsansprüche im Hinblick auf einen rechtsverletzenden Inhalt gegen die Nutzer durchzusetzen. Bei einer gegebenenfalls sehr zeit- und kostenintensiven Inanspruchnahme der Nutzer müssten sie daher gegebenenfalls über einen längeren Zeitraum hinnehmen, dass der rechtsverletzende Inhalt weiterhin online verfügbar wäre. Das ist besonders problematisch, wenn es sich um eine schwerwiegende Rechtsverletzung handelt.

Der Grundsatz der subsidiären Haftung muss bei Host-Provider daher in mehrerlei Hinsicht eingeschränkt werden: Zum einen sollten Host-Provider nur dann subsidiär haften, wenn sie selbst den unmittelbar verantwortlichen Nutzer anhand von Bestandsdaten identifizieren können oder die Identität des Nutzers dem Rechteinhaber bereits bekannt ist. Nicht zuzumuten wäre es den Rechteinhabern, wenn sie erst sämtliche Identifizierungsmöglichkeiten ausschöpfen müssten. Dies wäre sehr aufwändig und es wäre im Vorfeld ungewiss, ob die Identifizierung überhaupt gelingen wird.

Zum anderen wird der Grundsatz der Subsidiarität dadurch abgeschwächt, dass die Pflichten, die insbesondere der DSA Host-Providern auferlegt, neben der Haftung der Nutzer bestehen könnten. Host-Provider können vor allem zur Durchführung eines Notice-and-Take-Down-Verfahrens verpflichtet werden. Allerdings sollte zur Vermeidung von Overblocking der Diensteanbieter nur offensichtlich rechtsverletzende Inhalte entfernen müssen. Art. 16 Abs. 3 DSA trifft diesbezüglich bereits eine sinnvolle Regelung: Eine Kenntnis, die zu einer Haftung des Diensteanbieters führt, liegt lediglich vor, wenn die Melung „es einem sorgfältig handelnden Anbieter von Hostingdiensten ermöglichen, ohne eingehende Prüfung festzustellen, dass die einschlägige Tätigkeit oder Information rechtswidrig ist." Ein Verstoß gegen die Pflicht zur Entfernung eines beanstandeten Inhalts sollte allerdings nur zu einer subsidiären Haftung führen.

Dieser Lösungsansatz hat den Vorteil, dass weniger Anreize für die Diensteanbieter bestehen würden, beanstandete Inhalte im Zweifel vorsichtshalber zu löschen, um einer möglichen Haftung zu entgehen. Gleichzeitig würden aber Anreize für die Rechteinhaber gesetzt, von der Möglichkeit der Inanspruchnahme der Nutzer auch tatsächlich Gebrauch zu machen.

5. Einbindung von Identifizierungsmöglichkeiten ins Notice-and-Take-Down-Verfahren

Anknüpfend an die Überlegungen zur Subsidiarität der Haftung von Host-Providern wäre es sinnvoll, wenn de lege ferenda die Identifizierung des Nutzers direkt in das Notice-and-Take-Down-Verfahren vor allem von Plattform-Betreibern integriert werden würde. Als Grundlage kann das in Art. 16, 17 DSA geregelte Notice-and-Take-Down-Verfahren dienen. Anders als zum Beispiel bei reinen Webhosting-Diensten sind Plattform-Betreiber nach Art. 20 DSAbeziehungsweise nach Art. 21 DSA darüber hinaus verpflichtet, ihren Nutzern Zugang zu einem internen Beschwerdemanagement und zu einer außergerichtlichen Streitbeilegung zu verschaffen. Diese Regelungen des DSA können herangezogen werden, um die Möglichkeiten der Identifizierung von Nutzern in die Pflichten von Plattformen sinnvoll einzubinden.

In der Literatur wird zum Teil erwogen, den Nutzern die Wahl zu lassen, ob sie an einem beanstandeten Inhalt festhalten wollen und zur Verteidigung dieses Inhalts ihre Anonymität preisgeben oder die Entfernung des Inhalts in Kauf nehmen.[36] Ein solches Wahlrecht der Nutzer ist grundsätzlich zu befürworten, allerdings sollte die Konsequenz einer Ablehnung der Aufdeckung der Anonymität durch die Nutzer nicht unmittelbar die Entfernung des Inhalts darstellen. Andernfalls würde der Schutz anonymer Äußerungen und Ausdrucksformen abgewertet und die Missbrauchsgefahr von Beanstandungen erhöht.

Dennoch kann das Wahlrecht des Nutzers in das Notice-and-Take-Down-Verfahren eingebunden und um die Identifizierungsmöglichkeiten durch Auskunftsansprüche ergänzt werden: Sobald ein möglicherweise rechtsverletzender Inhalt beanstandet wird, soll der Host-Provider den verantwortlichen Nutzer darüber informieren und dafür Sorge tragen, dass die bereits vorhandenen

[36] *Wagner,* GRUR 2020, 447, 456; Befürwortend auch *Janal*, ZEuP 2021, 227, 261.

Bestandsdaten des Nutzers nicht gelöscht werden. Der Nutzer erhält gleichzeitig eine kurze Frist, in der er seine Identität aufdecken kann. Gibt er seine Identität freiwillig preis, bleibt der Inhalt online verfügbar und Rechteinhaber und Nutzer können sich ebenso wie in der Offline-Welt über die Rechtmäßigkeit des Inhalts streiten. Den Host-Provider treffen in diesem Fall grundsätzlich keine weiteren Verpflichtungen. Zudem haftet er aufgrund der Subsidiarität gegenüber dem Rechteinhaber nicht für diesen Inhalt. Sofern es sich um eine Online-Plattform handelt, wäre es sinnvoll, wenn Nutzern und Rechteinhabern in diesem Fall die Möglichkeit der außergerichtlichen Streitbeilegung in Erweiterung des Art. 21 DSA zur Verfügung stünde.

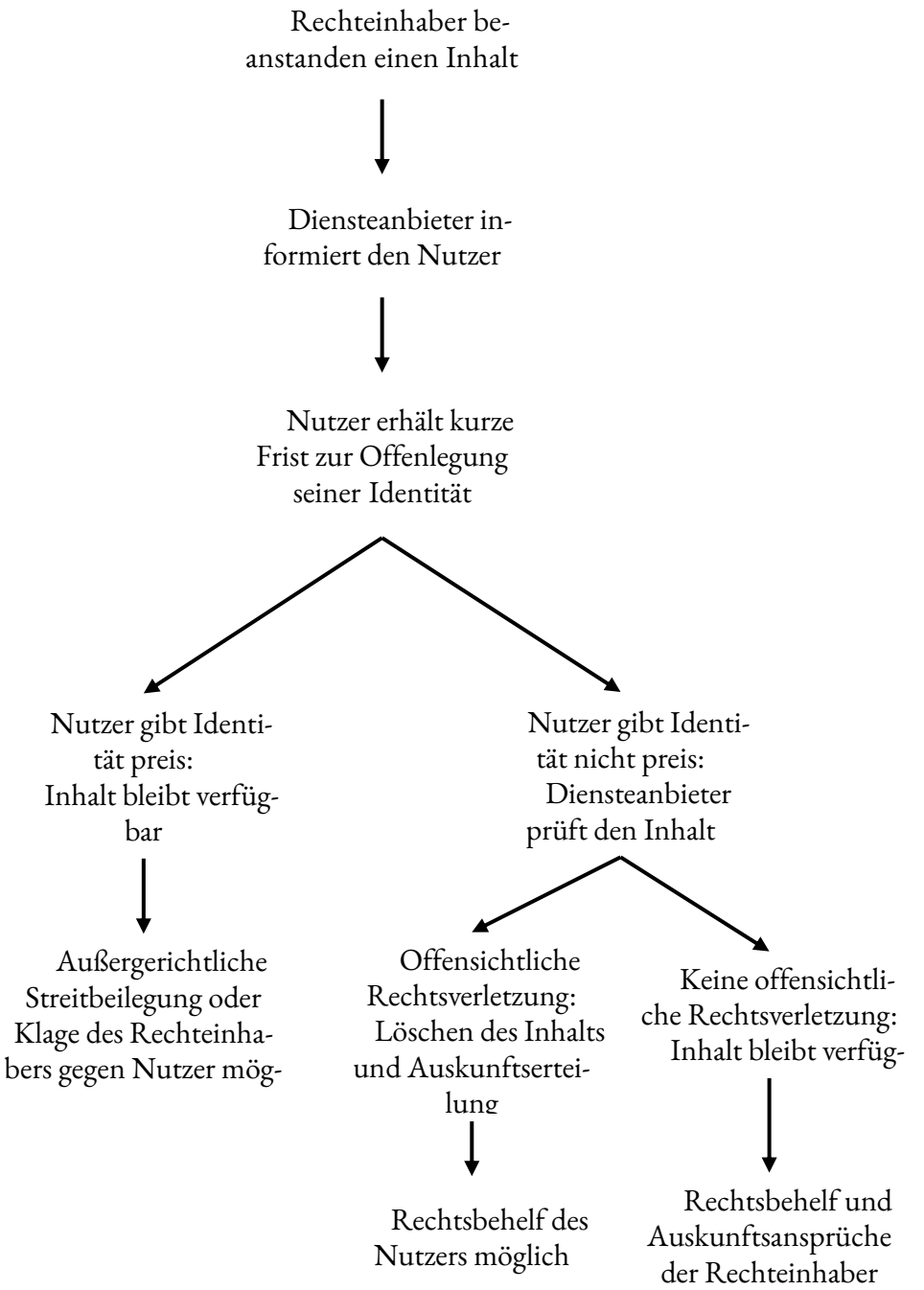
Hält der Nutzer dagegen an seiner Anonymität fest, muss der Dienstenbieter das eigentliche Notice-and-Take-Down-Verfahren durchführen und den beanstandeten Inhalt prüfen. Stellt er eine offensichtliche Rechtsverletzung fest, wird der Inhalt entfernt und der Diensteanbieter erteilt dem Rechteinhaber Auskunft über die Bestandsdaten des Nutzers. Andernfalls sollte der Inhalt abrufbar bleiben. Eine Ausnahme könnte gelten, wenn erkennbar ist, dass dem betroffenen Rechteinhaber schwere Nachteile drohen könnten, wenn der Inhalt bis zu einer gerichtlichen Entscheidung abrufbar bliebe. Der Rechteinhaber muss außerdem in jedem Fall die Möglichkeit haben, Auskunftsansprüche gegen den Diensteanbieter geltend zu machen. Gleichzeitig sollte man ihm Zugang zu einem internen Beschwerdemanagement in Anlehnung an Art. 20 DSA gewähren, sofern es sich um die Entscheidung einer Online-Plattform handelt.

Für das große Problemfeld der illegalen Nutzerinhalte auf Online-Plattformen könnte so eine verhältnismäßige Lösung geschaffen werden. Ein solches Vorgehen würde außerdem eine übermäßige Belastung der Justiz im Hinblick auf die große Zahl möglicher Rechtsverletzungen im Internet verhindern, ohne die Prüfungskompetenz des Diensteanbieters überzustrapazieren. Dem Plattform-Betreiber kommt damit weniger die Funktion eines Richters als die einer Art „Streitmittler" zwischen Rechteinhaber und Nutzer zu, die auch zu seinem ursprünglichen Verursachungsbeitrag passt.[37] Gegen jede Entscheidung des Diensteanbieters muss aber der Rechtsweg zu den staatlichen Gerichten für beide Parteien immer offenstehen.[38]

---

[37] *Wagner,* GRUR 2020, 447, 453 ff.

[38] Vgl. die Regelung in Art. 21 Abs. 1 UAbs. 2 DSA; *Wagner,* GRUR 2020, 447, 457.


Rechteinhaber beanstanden einen Inhalt
Diensteanbieter informiert den Nutzer
Nutzer erhält kurze Frist zur Offenlegung seiner Identität
Nutzer gibt Identität preis: Inhalt bleibt verfügbar
Nutzer gibt Identität nicht preis: Diensteanbieter prüft den Inhalt
Außergerichtliche Streitbeilegung oder Klage des Rechteinhabers gegen Nutzer mög-
Offensichtliche Rechtsverletzung: Löschen des Inhalts und Auskunftserteilung
Keine offensichtliche Rechtsverletzung: Inhalt bleibt verfüg-
Rechtsbehelf des Nutzers möglich
Rechtsbehelf und Auskunftsansprüche der Rechteinhaber

6. Begrenzung des Akteneinsichtsrechts im Strafverfahren

Parallel zur Ausweitung der Auskunftsmöglichkeiten de lege ferenda sollte das Recht der Rechteinhaber, Akteneinsicht im Strafverfahren zu nehmen, begrenzt werden, wenn kein öffentliches Interesse an einer Strafverfolgung besteht. Ansonsten bestünde die Gefahr, dass die Rechteinhaber von ihren zivilrechtlichen Auskunftsansprüchen keinen Gebrauch machen und aus Kostengründen stattdessen ausschließlich zum Zweck der späteren Akteneinsicht die Strafverfolgungsbehörden mit Ermittlungen belastet werden. Dieses Problem lässt sich durch eine entsprechende Auslegung des § 406e StPO lösen.

Sofern aber ein großes öffentliches Interesse an der Strafverfolgung besteht, zum Beispiel weil der Straftatbestand der Volksverhetzung erfüllt wurde, ist ein Meldeverfahren der Diensteanbieter wie nach dem NetzDG sinnvoll. Auch Art. 18 DSA sieht eine Meldepflicht bei Straftaten vor, die das Leben oder die Sicherheit einer Person gefährden. Sofern in diesen Fällen auch individuelle Rechte verletzt werden, spricht auch nichts gegen eine Akteneinsicht durch die Rechteinhaber.

B. Inhalt und Umfang eines allgemeinen Auskunftsanspruchs

De lege ferenda gilt es einen allgemeinen Auskunftsanspruch gegen Internetdiensteanbieter zu schaffen, der eine Identifizierung anonymer Nutzer durch die Rechteinhaber ermöglichen kann, aber gleichzeitig auch die Interessen der Diensteanbieter und der Nutzer berücksichtigt. Die lege lata bestehenden Unterschiede der verschiedenen einschlägigen Auskunftsansprüche sind – wie sich oben gezeigt hat – nicht zu rechtfertigen. Das System der bisher existierenden Auskunftsansprüche ist widersprüchlich und nicht aufeinander abgestimmt. Daher wird de lege ferenda eine einheitliche Lösung für die Inhaber aller absolut geschützten Rechte angestrebt.

I. Unionsrechtliche Vorgaben

Das Internetrecht ist sehr stark unionsrechtlich geprägt. Vor allem gilt das für Verletzungen des geistigen Eigentums und des Urheberrechts im Speziellen, sowie für die Haftung und Pflichten der Diensteanbieter und den Schutz personenbezogener Daten im Internet. Ein nationaler Auskunftsanspruch gegen

Internetdiensteanbieter muss daher im Einklang mit den einschlägigen, unionsrechtlichen Regelungen stehen.

Das Unionsrecht regelt selbst bislang keine Auskunftsansprüche gegen Internetdiensteanbieter und zwingt auch die Mitgliedstaaten grundsätzlich nicht zur Einführung solcher Auskunftsansprüche. Lediglich Art. 8 Abs. 1 c) Enforcement-Richtlinie enthält für den Bereich des geistigen Eigentums eine Verpflichtung der Mitgliedstaaten Auskunftsansprüche vorzusehen. Die Mitgliedstaaten müssen demnach dafür Sorge tragen,

„dass die zuständigen Gerichte im Zusammenhang mit einem Verfahren wegen Verletzung eines Rechts des geistigen Eigentums auf einen begründeten und die Verhältnismäßigkeit wahrenden Antrag des Klägers hin anordnen können, dass Auskünfte über den Ursprung und die Vertriebswege von Waren oder Dienstleistungen, die ein Recht des geistigen Eigentums verletzen, von dem Verletzer und/oder jeder anderen Person erteilt werden, die (...) nachweislich für rechtsverletzende Tätigkeiten genutzte Dienstleistungen in gewerblichem Ausmaß erbrachte, (...)"

Damit beinhaltet diese Vorschrift zumindest bei gewerblichen Verletzungen des geistigen Eigentums grundsätzlich auch einen Drittauskunftsanspruch gegen Internetdiensteanbieter.[39] Allerdings regelt Art. 8 Enforcement-Richtlinie nicht das Verhältnis zum Datenschutzrecht. Der *EuGH* hat aber in der Entscheidung Promusicae festgestellt, dass im Hinblick auf den Schutz personenbezogener Daten, die Mitgliedstatten durch Art. 8 Abs. 1 der Enforcement-Richtlinie nicht verpflichtet werden, Auskunftsansprüche gegen Access-Provider zur Identifizierung eines Anschlussinhabers zu schaffen.[40] Die Mitgliedstaaten müssen nicht zwingend die Pflicht zur Weitergabe personenbezogener Daten im Rahmen eines zivilrechtlichen Verfahrens vorsehen.[41] Dieses Urteil ist auch auf andere Internetdienste, die auf sensible Daten ihrer Nutzer zugreifen können, anwendbar, sodass der Enforcement-Richtlinie grundsätzlich keine Verpflichtung der Mitgliedstaaten zu entnehmen ist, zivilrechtliche Auskunftsansprüche gegen Internetdiensteanbieter zur Identifizierung von Internetnutzern zu

---

[39] *Fischer*, Die Einbindung von Providern, S. 308 f.

[40] *EuGH*, Urt. v. 29.1.2008 - C-275/06, GRUR 2008, 241 Rn. 57 f. – Promusicae; S. auch *Weber*, Enforcement-Richtlinie, S. 135 ff.

[41] *EuGH*, Urt. v. 29.1.2008 - C-275/06, GRUR 2008, 241 Rn. 60 – Promusicae.

regeln.[42] Die deutschen Umsetzungsvorschriften des § 101 UrhG und der Parallelvorschriften etwa in § 19 MarkenG gehen deshalb bereits über das zwingend Erforderliche hinaus.

In derselben Entscheidung hat sich der *EuGH* allerdings auch mit dem Verhältnis eines mitgliedstaatlichen Auskunftsanspruch zur e-privacy-Richtlinie befasst. Dabei hat er entschieden, dass die e-privacy-Richtlinie einem mitgliedstaatlichen Auskunftsanspruch gegen Access-Provider nicht entgegensteht, sofern dieser insbesondere den Grundsatz der Verhältnismäßigkeit wahrt.[43] Die Mitgliedstaaten haben daher sehr viel Spielraum, ob und in welchem Umfang die Auskunftsansprüche bei Verletzungen des geistigen Eigentums eine Identifizierung anonymer Nutzer durch Internetdiensteanbieter ermöglichen.

Nicht abschließend geklärt ist bislang das Verhältnis von Auskunftsansprüchen durch Internetdiensteanbieter zur Datenschutzgrundverordnung. Das betrifft vor allem die Konstellationen, die nicht vom Anwendungsbereich der e-privacy-Richtlinie erfasst werden.[44] Allerdings bietet die Datenschutzgrundverordnung durch Erlaubnistatbestände wie Art. 6 Abs. 1 lit. c) DS-GVO und Öffnungsklauseln wie Art. 6 Abs. 4 DS-GVO ausreichend Spielraum für die Mitgliedstaaten, sodass sie Auskunftsansprüchen gegen Internetdienste jedenfalls nicht generell entgegensteht.

Auch der Digital Services Act enthält keine Regelung für einen Auskunftsanspruch der Rechteinhaber zur Identifizierung eines anonymen Nutzers gegen Internetdiensteanbieter. Art. 10 DSA macht allerdings Vorgaben für gerichtliche und behördliche Auskunftsanordnungen.[45] Nach Art. 10 Abs. 2 DSA müssen die Mitgliedstaaten dafür sorgen, dass die Anordnungen folgende Bedingungen erfüllen:

---

[42] S. für Host-Provider *Fischer*, Einbindung von Providern, S. 309.

[43] *EuGH*, Urt. v. 29.1.2008 - C-275/06, GRUR 2008, 241 Rn. 49 ff., 68 ff. – Promusicae; Kritisch etwa *Brüggemann,* Drittauskunftsanspruch, S. 151 ff.; *Weber,* Enforcement-Richtlinie, S. 127 ff.

[44] Das ist grundsätzlich der Fall für die „reine" Bestandsdatenauskunft durch Telekommunikationsdienste, sowie der Auskunft durch Telemediendienste und sonstige Internetdienste.

[45] S. zum Verhältnis zwischen Art. 9 DSA-E und Art. 8 Enforcement-Richtlinie *Janal,* ZEuP 2021, 227, 260; *Spindler,* GRUR 2021, 545, 551.

„a) diese Anordnung enthält Folgendes:

> eine Angabe der Rechtsgrundlage nach Maßgabe des Unionsrechts oder des nationalen Rechts für die Anordnung;
>
> Informationen zur Identifizierung der erlassenden Behörde;
>
> klare Angaben, anhand deren der Anbieter von Vermittlungsdiensten den bzw. die bestimmten Empfänger ermitteln können, zu dem Informationen angefordert werden, etwa einen oder mehrere Kontonamen oder eindeutige Kennungen;
>
> eine Begründung, wozu die Informationen benötigt werden und warum die Auskunftsanordnung erforderlich und verhältnismäßig ist, um festzustellen, ob die Nutzer des Vermittlungsdienstes das geltende Unionsrecht oder nationale Recht im Einklang mit dem Unionsrecht einhalten, es sei denn, eine solche Begründung kann aus Gründen der Verhütung, Ermittlung, Erkennung und Verfolgung von Straftaten nicht gegeben werden;
>
> Angaben über Rechtsbehelfsmechanismen, die dem Diensteanbieter und den betreffenden Nutzern zur Verfügung stehen;
>
> unter Umständen Angaben dazu, welche Behörde über die Ausführung der Anordnung zu informieren ist;

b) Die Anordnung verpflichtet den Diensteanbieter nur zur Bereitstellung von Informationen, die er ohnehin bereits für die Zwecke der Erbringung des Dienstes erfasst hat und die seiner Verfügungsgewalt unterliegen.

c) Die Anordnung wird in einer der vom Anbieter von Vermittlungsdiensten gemäß Artikel 11 Absatz 3 angegebenen Sprache (...) übermittelt und an die vom Anbieter gemäß Artikel 11 benannte elektronische Kontaktstelle geschick (...)t."

Diesen Vorgaben müssen nationale Auskunftsansprüche von Rechteinhabern dann genügen, wenn die Auskunft aufgrund richterlicher Anordnung – etwa, weil die Auskunftserteilung unter Richtervorbehalt steht - ergeht. Insbesondere gilt es für die Ausgestaltung von Auskunftsansprüchen de lege ferenda zu berücksichtigen, dass die Diensteanbieter nicht dazu verpflichtet werden dürfen, andere Informationen zu übermitteln als diejenigen, die sie ohnehin bereits erfasst haben und die ihrer Verfügungsgewalt unterliegen.

Art. 10 DSA zeigt allerdings noch einmal, dass bisher das Gleichgewicht zwischen den Pflichten der Diensteanbieter und der Inanspruchnahme der Nutzer als unmittelbare Rechtsverletzer auch auf EU-Ebene nicht stimmt. Während

der Digital Services Act umfassende Pflichten vor allem für Plattformen normiert, macht Art. 10 DSA nur allgemeine Vorgaben für möglicherweise in den Mitgliedstaaten vorgesehene Auskunftsanordnungen. Dabei wird weder die Möglichkeit einer Identifizierung anonymer Nutzer vorgeschrieben noch das Verhältnis zwischen einer Inanspruchnahme der Nutzer und den Pflichten der Diensteanbieter geregelt. Auch das Verhältnis zum Datenschutzrecht bleibt ungeklärt. Entsprechend wäre hier ein Nachsteuern auf EU-Ebene sinnvoll. Dennoch sollte die konkrete Ausgestaltung von Auskunftsansprüchen den Mitgliedstaaten überlassen bleiben, die vor allem die prozessuale Ausgestaltung im Einklang mit ihrem nationalen Verfahrensrecht ausgestalten können.[46]

Jedenfalls verbleibt aber derzeit ausreichend Spielraum für die Mitgliedstaaten, Auskunftsansprüche der Rechteinhaber gegen Internetdiensteanbieter zur Identifizierung anonymer Nutzer im Einklang mit dem Unionsrecht zu regeln.

II. Ausgestaltung eines allgemeinen Auskunftsanspruchs

Im nationalen Recht sollte de lege ferenda ein allgemeiner Auskunftsanspruch gegen Internetdiensteanbieter zur Identifizierung anonymer Rechtsverletzer im Internet eingeführt werden. Ein solcher Anspruch würde den Auskunftsanspruch aus § 21 Abs. 2 S. 2 TTDSG vollständig ersetzen. Die Auskunftsansprüche im Bereich des geistigen Eigentums, sowie der aus § 242 BGB abgeleitete Auskunftsanspruch blieben grundsätzlich bestehen, würden allerdings in ihrem Anwendungsbereich durch den spezielleren Anspruch beschränkt.

Als Regelungsstandort für einen allgemeinen Auskunftsanspruch gegen Anbieter von Internetdiensten würde sich etwa das TTDSG eignen, da es bereits gemeinsame Regelungen für Telekommunikations- und Telemediendienste enthält und der Auskunftsanspruch mit dem Datenschutzrecht eng verbunden ist.

1. Aktiv- und Passivlegitimation

Aktivlegitimiert sollten de lege ferenda alle Personen sein, die geltend machen in ihren Rechten verletzt zu sein. Dies dient der angestrebten Gleichbehandlung der Inhaber aller absoluten Rechte. Der größte Anwendungsbereich dürfte für

---

[46] *Janal*, ZEuP 2021, 227, 261 f.

Rechte des Geistigen Eigentums und im Speziellen für das Urheber- und Markenrecht, sowie für Persönlichkeitsrechte und das Recht am eingerichteten und ausgeübten Gewerbebetrieb bestehen.

Die Passivlegitimation sollte alle Anbieter von Internetdiensten jeglicher Art umfassen und nicht etwa auf Anbieter von Telemedien- oder Telekommunikationsdiensten beschränkt sein. Zur Abgrenzung vom Begriff des Diensteanbieters aus § 2 Nr. 1 TMG und von internetunabhängigen Telekommunikationsdiensten empfiehlt es sich, den Begriff des „Internetdiensteanbieters" zu verwenden und neu zu definieren.

Der Kreis der möglichen Anspruchsgegner muss möglichst breit ausgestaltet werden. Ein gewerbsmäßiges Tätigwerden der Diensteanbieter sollte nicht vorausgesetzt werden. Dies ist auch aus Verhältnismäßigkeitsgesichtspunkten nicht erforderlich. Durch die Möglichkeit der anonymen Nutzung ihrer Dienste schaffen auch diejenigen Diensteanbieter eine nicht unerhebliche Gefahrenquelle, die nicht in gewerbsmäßigen Umfang agieren. Außerdem ist die Aufdeckung der Anonymität der Nutzer milder als eine eigene Haftung der Diensteanbieter.

Der Auskunftsanspruch sollte außerdem auch Diensteanbieter umfassen, deren Dienst nicht unmittelbar zur Rechtsverletzung genutzt wurde. So kann zum Beispiel ein E-Mail-Dienst Auskunft über den Inhaber einer E-Mail-Adresse erteilen, mit der sich ein Nutzer bei einem anderen Dienst, über den er die Rechtsverletzung begangen hat, angemeldet hat. Auch wenn für die Rechtsverletzung der E-Mail-Dienst selbst nicht genutzt wurde, besteht ein hinreichender Zusammenhang zwischen der Erbringung des Dienstes und der Rechtverletzung, der die Inanspruchnahme des Diensteanbieters rechtfertigt. Für die konkrete Ausgestaltung des Auskunftsanspruchs kann sich in dieser Hinsicht an der Formulierung des § 21 TTDSG orientiert werden. Dementsprechend wären die Diensteanbieter ohne weitere Einschränkungen zur Auskunftserteilung verpflichtet, „soweit dies zur Durchsetzung zivilrechtlicher Ansprüche wegen der Verletzung absolut geschützter Rechte (...) erforderlich ist."

Der in dieser Arbeit vorgeschlagene allgemeine Auskunftsanspruch beschränkt sich allerdings bewusst auf die Auskunft von Internetdiensteanbietern. Für die

Identifizierung anonymer Rechtsverletzer im Internet könnten zwar auch Auskünfte anderer Akteure – wie Banken oder Anbietern von Festnetz- und Mobilfunknummern hilfreich sein. Allerdings unterscheidet sich die Interessenslage in diesen Fällen stärker von der Inanspruchnahme von Internetdiensten. Rechtsprechung und Gesetzgebung legen Internetdiensten – wenngleich in sehr unterschiedlichem Umfang – hinsichtlich rechtswidriger Handlungen ihrer Nutzer teilweise umfangreiche Pflichten auf. Auskunftsansprüche gegen Internetdienste schaffen hierzu ein Gegengewicht, das bei Banken und Festnetz- und Mobilfunkanbietern nicht in derselben Art und Weise erforderlich ist. Außerdem unterscheiden sich die Interessen der Nutzer im Hinblick auf den Datenschutz bei Internetdiensten und in der Offline-Welt. Aufgrund der besseren Vergleichbarkeit beschränkt sich der hier vorgeschlagene Auskunftsanspruch deshalb auf Internetdiensteanbieter. Soweit Auskünfte gegen Banken und Festnetz- und Mobilfunkanbieter de lege lata noch nicht von Auskunftsansprüchen erfasst werden, könnte in diesem Bereich zukünftig dennoch eine Ergänzung unter Berücksichtigung der abweichenden Interessenslage sinnvoll sein.[47]

Zu beachten ist aber, dass Online-Zahlungsdienstleister wie paypal oder klarna vom Begriff des Internetdiensteanbieters erfasst werden und dadurch auch dem hier vorgeschlagenen Auskunftsanspruch de lege ferenda unterfallen. Dasselbe kann auch für klassische Zahlungsdienstleister wie Banken gelten, wenn diese im konkreten Einzelfall die Funktion eines Online-Zahlungsdienstleisters übernommen haben. Hat ein Nutzer aber lediglich seine Kontonummer bei der Registrierung in einem Online-Dienst angegeben, kann die Bank nicht als Internetdiensteanbieter auf Auskunft über den Kontoinhaber in Anspruch genommen werden.

---

[47] Die Drittauskunftsansprüche im Bereich des geistigen Eigentums greifen grundsätzlich auch gegenüber Banken; S. dazu auch *EuGH,* Urt. v. 16.7.2015 – C-580/13, GRUR 2015, 894 – Coty Germany; S. auch *BGH,* Beschl. v. 17.10.2013 – I ZR 51/12, GRUR 2013, 1237 – Davidoff Hot Water; *BGH,* Urt. v. 21.10.2015 – I ZR 51/12, GRUR 2016, 497 – Davidoff Hot Water II. S. zur Kollision des außergerichtlichen Auskunftsanspruchs gemäß § 101 Absatz 2 Satz 1 Nr. 3 UrhG und des luxemburgischen Bankgeheimnisses *Herrmann/Würdemann*, GRUR Int. 2017, 933, 933 ff.

2. Anforderung an die Rechtsverletzung

Um den Auskunftsanspruch möglichst breit aufzustellen, sollten außerdem keine besonderen Anforderungen an die Rechtsverletzung gestellt werden. Weder sollte es Bagatellgrenzen geben noch im Fall der Verletzung des Urheberrechts gewerbsmäßiges Handeln vorausgesetzt werden. Ohne die Identifizierung der Nutzer lässt sich häufig Ausmaß und Schwere einer Rechtsverletzung nicht sinnvoll beurteilen.

Aus diesem Grund darf der Auskunftsanspruch zur Identifizierung anonymer Internetnutzer auch nicht eine offensichtliche Rechtsverletzung voraussetzen. Das Kriterium der Offensichtlichkeit eignet sich nicht zur Begründung des Auskunftsanspruchs, da den Rechteinhabern auch im Falle nicht offensichtlicher Rechtsverletzungen ein Auskunftsanspruch zustehen muss. Allerdings kann auf prozessualer Ebene bei einer offensichtlichen Rechtsverletzung die Auskunftserteilung unter erleichterten Bedingungen erteilt werden.

Der Gefahr eines zu ausufernden und nicht mehr im Verhältnis zur Rechtsverletzung stehenden Gebrauchs der Auskunftsansprüche kann auch ohne Bagatellgrenzen oder andere Einschränkungen in Bezug auf die Rechtsverletzung entgegengewirkt werden. Sowohl durch ein Verhältnismäßigkeitserfordernis als auch durch prozessuale Instrumente wird verhindert, dass Rechteinhaber in unverhältnismäßiger Weise Auskunft verlangen.

3. Umfang des Auskunftsanspruchs

Auch im Hinblick auf den Umfang des Auskunftsanspruchs sollte dieser möglichst weit gefasst sein. Neben Bestandsdaten muss auch die Auskunft über beziehungsweise unter Zuhilfenahme von Nutzungs- und Verkehrsdaten möglich sein. Der damit einhergehende Eingriff in das Recht der Nutzer auf Anonymität kann durch prozessuale und datenschutzrechtliche Regelungen ausgeglichen werden.

Dabei ist zu beachten, dass die Auskunftserteilung auch nach Art. 10 Abs. 2 b) DSA nur mittels Daten erbracht werden darf, die der Diensteanbieter ohnehin bereits erhoben hat. Außerdem stellt eine punktuelle Auskunftserteilung einen deutlich geringeren Eingriff in das Recht auf Anonymität dar, als eine anlasslose

Datenspeicherungen oder das Sammeln von Daten, die die Erstellung von Persönlichkeitsprofilen ermöglicht.

Desweitern sollte sich die Auskunft auch auf Nutzer erstrecken, bei denen unklar ist, ob es sich bei diesen um die Rechtsverletzer handelt, weil etwa ein Nutzerkonto oder ein Internetanschluss auch von einer anderen Person genutzt worden sein könnte. Natürlich muss aber eine Verbindung zur Rechtsverletzung bestehen. Auch hier bietet es sich wieder an, sich an der Formulierung des § 21 Abs. 2 TTDSG zu orientieren und den Auskunftsanspruch davon abhängig zu machen, ob er „für die Durchsetzung zivilrechtlicher Ansprüche wegen der Verletzung absolut geschützter Rechte (...) erforderlich ist."

4.Verhältnismäßigkeitserfordernis

Der Auskunftsanspruch muss den Grundsatz der Verhältnismäßigkeit im Hinblick auf die Interessen der Nutzer und der Diensteanbieter wahren. Das ergibt sich bereits aus dem verfassungsrechtlich gebotenen Ausgleich der widerstreitenden Interessen.

Für Rechtsverletzungen des geistigen Eigentums verlangt Art. 8 Abs. 1 Enforcement-Richtlinie darüber hinaus, dass eine gerichtliche Auskunftsanordnung nur aufgrund eines die Verhältnismäßigkeit wahrenden Antrags des Klägers ergehen darf. Der deutsche Gesetzgeber ging bei dessen Umsetzung über Art. 8 Abs. 1 Enforcement-Richtlinie hinaus, in dem nach § 101 Abs. 2 UrhG und dessen Parallelvorschriften auch eine Auskunftserteilung ohne vorherige gerichtliche Anordnung möglich ist. Dies führte aber zu der oben bereits aufgegriffenen Problematik, dass die Diensteanbieter die Verhältnismäßigkeit der „Anordnung" der Rechteinhaber prüfen müssten.

Soll ein Auskunftsanspruch auch ohne Richtervorbehalt möglich sein, ist es die Aufgabe des Gesetzgebers, die Verhältnismäßigkeit sicherzustellen. Bei der Umsetzung der Enforcement-Richtlinie kam der Gesetzgeber seiner Aufgabe nach, indem er die Auskunftserteilung von einer offensichtlichen Rechtsverletzung abhängig gemacht hat. Bei einer offensichtlichen Rechtsverletzung kann davon ausgegangen werden, dass die Interessen der Rechteinhaber denen der Nutzer und der Diensteanbieter überwiegen und die Auskunftserteilung dadurch verhältnismäßig ist. Insofern wäre ein ausdrückliches

Verhältnismäßigkeitserfordernis jedenfalls für die reine Bestandsdatenauskunft nicht erforderlich gewesen.

Problematisch an der damaligen Lösung ist jedoch, dass der Auskunftsanspruch auf offensichtliche Rechtsverletzungen beschränkt ist. Eine sinnvolle Lösung könnte de lege ferenda daher wie folgt aussehen: Die Auskunft unter Verwendung besonders sensibler Daten könnte ebenso wie bei nicht offensichtlichen Rechtsverletzungen unter Richtervorbehalt gestellt werden. Dabei kann durch ein Verhältnismäßigkeitserfordernis im Sinne des § 101 Abs. 4 UrhG sichergestellt werden, dass die Gerichte im Einzelfall die Verhältnismäßigkeit der Auskunftserteilung sicherstellen. Bei offensichtlichen Rechtsverletzungen kann die Bestandsdatenauskunft auch ohne richterliche Anordnung erfolgen. Die Verhältnismäßigkeit wird dabei bereits durch das Merkmal der Offensichtlichkeit gewährleistet.

5. Schadensersatzansprüche

Diensteanbieter sollten gegenüber ihren Nutzern grundsätzlich haften können, wenn sie Auskünfte über Nutzerdaten erteilen, ohne dazu verpflichtet zu sein. Ein Haftungsausschluss wie in Absatz 6 der Auskunftsansprüche im Bereich des geistigen Eigentums setzt falsche Anreize für die Diensteanbieter, eine Auskunft vorsichtshalber zu erteilen. Durch das Merkmal der Offensichtlichkeit und den Richtervorbehalt wird das Haftungsrisiko der Diensteanbieter ohnehin stark reduziert.

Zu befürworten ist es, den Rechteinhabern einen Anspruch auf Schadensersatz einzuräumen für den Fall, dass die Diensteanbieter eine Auskunft grob fahrlässig oder vorsätzlich falsch erteilen. Dadurch werden die Diensteanbieter dazu angehalten, die Auskunft auch korrekt zu erteilen.

C. Prozessuale Rahmenbedingungen

In mehrerlei Hinsicht ist der eben vorgeschlagene allgemeine Auskunftsanspruch de lege ferenda weitergehend als die bisher existierenden Ansprüche. Das ist auch erforderlich, um die Möglichkeiten der Identifizierung von anonymen Internetnutzern möglichst breit aufzustellen und auf diese Weise eine

Verbesserung des status quo zu erzielen, ohne die Diensteanbieter zu einer weitergehenden Erhebung von Nutzerdaten zu verpflichten.

Im Gegenzug gilt es allerdings auch die Interessen der betroffenen Nutzer und der Diensteanbieter in den Blick zu nehmen. Daher ist ein prozessualer Rahmen für den allgemeinen Auskunftsanspruch herzustellen, der die Ansprüche gegen die Internetdiensteanbieter realisiert, aber gleichzeitig auch etwaigen Problemen – zum Beispiel der Gefahr von Missbrauch – vorbeugt. Geeignete prozessuale Rahmenbedingungen sind deshalb essenziell für die Wahrung des Verhältnismäßigkeitsprinzip und den Ausgleich der widerstreitenden Interessen unter den Gesichtspunkten der praktischen Konkordanz.

I. John-Doe-Verfahren?

Der Vorschlag eines allgemeinen Auskunftsanspruchs de lege ferenda beruht auf der Grundannahme, dass das Auskunftsverfahren zwischen dem Rechteinhaber und einem Diensteanbieter geführt wird. Ein solches Auskunftsverfahren ist allerdings nicht alternativlos. Stattdessen könnte die Identifizierung der Nutzer im Wege eines Schadensersatz- oder Unterlassungsprozesses aufgrund einer Klage der Rechteinhaber gegen den unbekannten Nutzer erfolgen. Ein Verfahren gegen Unbekannt kennt das deutsche Zivilprozessrecht nicht. Diskutiert wird ein solches Verfahren daher anhand des Vorbilds des US-amerikanischen John-Doe-Verfahrens, das eine Klage gegen unbekannte Internetnutzer ermöglichen würde.[48] Die Klage gegen den Nutzer kann im Rahmen des John-Doe-Verfahrens unter einem Pseudonym erfolgen.[49] Als solches könnten bei Rechtsverletzungen im Internet zum Beispiel Benutzernamen, Benutzerkonten oder die verwendete IP-Adresse in Kombination mit den Zugriffszeiten angeführt werden.

Bei einer Übertragung des John-Doe-Verfahrens ins deutsche Recht könnte daher zunächst in einer Art Vorverfahren – zum Beispiel im Rahmen eines In-

---

[48] *Verheijden,* Rechtsverletzungen auf YouTube und Facebook, S. 316 f. S. auch *Ladeur/Gostomzyk*, NJW 2012, 710, 715, die ein John-Doe-Verfahren vor sogenannten Cyber Courts vorschlagen, an dem sich auch die Nutzer unter einem Pseudonym beteiligen könnten. S. allgemein zum John-Doe-Verfahren etwa *Hilgard,* IWRZ 2018, 250, 250 ff.

[49] *Hilgard,* IWRZ 2018, 250, 250.

Camera-Verfahrens[50] - die Identität des Nutzers mithilfe der Diensteanbieter ermittelt werden beziehungsweise gegebenenfalls den Diensteanbietern aufgegeben werden, die zur Identifizierung notwendige Daten nicht zu löschen. Im Hauptverfahren entscheidet dann das Gericht darüber, ob eine Rechtsverletzung vorliegt und die Identität des Nutzers dem Rechteinhaber bekannt gegeben werden darf. Am Ende des Verfahrens gegen Unbekannt könnte der Nutzer dann gegenüber dem Rechteinhaber identifiziert werden.[51]

Der Vorteil eines solchen Verfahrens bei Rechtsverletzungen im Internet bestünde darin, dass das Gericht zunächst über die Rechtmäßigkeit des Inhalts entscheiden könnte und erst anschließend die Identität des Nutzers gegenüber dem Rechteinhaber preisgegeben werden würde. Dadurch würde die Anonymität der Internetnutzer vor der vorschnellen Weitergabe und der Ausforschung von Nutzerdaten, sowie vor einem Missbrauch der Auskunftsansprüche geschützt werden.

Auf der anderen Seite kann sich der Beklagte aber im Rahmen eines solchen Verfahrens nicht verteidigen und seine Sichtweise darstellen. Das ist vor allem problematisch, wenn sich die Wirkung des Urteils nicht nur auf die Rechtsmäßigkeit der Auskunftserteilung, sondern auch auf das Vorliegen einer Rechtsverletzung erstreckt. Vor allem bei Äußerungsdelikten kann auch das Gericht ohne Kenntnis der Hintergründe und näheren Umstände kaum die Rechtmäßigkeit eines Inhalts beurteilen. Wird in einem solchen Fall lediglich die Sicht der Rechteinhaber gehört, würden die Nutzer erheblich benachteiligt werden. Für die Rechteinhaber wäre es zwar effektiver, wenn gleichzeitig auch über die Rechtmäßigkeit des Handelns des Nutzers entschieden würde, da sie im Anschluss an die Auskunftserteilung nicht noch ein weiteres Verfahren gegen den Nutzer führen müssten. Der Nutzer würde allerdings erheblich in seinem Anspruch auf rechtliches Gehör nach Art. 103 GG beeinträchtig werden.

---

[50] S. auch *Janal,* ZEuP 2021, 227, 261.

[51] Einen anderen Vorschlag für die Übertragung des John-Doe-Verfahrens auf anonyme Rechtsverletzungen im Internet unterbreiten *Nolte/Wimmers*, GRUR 2014, 16, 27, die eine gerichtliche Sperranordnungen gegen anonyme Nutzer vorschlagen, auf Grund derer die Diensteanbieter zur Sperrung verpflichtet werden würden.

Dem könnte dadurch abgeholfen werden, indem man dem Nutzer die Möglichkeit gibt, sich unter dem Pseudonym als eine Art „Avatar" tatsächlich am Verfahren zu beteiligen.[52] Dies würde aber voraussetzen, dass nicht bereits die Beteiligung des Nutzers zu dessen Identifizierung führt. Daher könnte eine solche Beteiligung in der Praxis wohl nur schriftlich erfolgen, was vor allem die Frage aufwirft, wie sichergestellt werden kann, dass es sich bei dem Verfasser eines entsprechenden Schriftstückes tatsächlich um den fraglichen Nutzer handelt. Des Weiteren müssten Klageschriften, aber auch Gerichtsdokumente tatsächlich zugestellt werden können, ohne dass Name und Anschrift des Nutzers bekannt werden. Die Zuverlässigkeit einer Zustellung über die Diensteanbieter darf zurecht bezweifelt werden.[53]

Weniger problematisch wäre die fehlende Beteiligungsmöglichkeit der Nutzer, wenn im Rahmen des Verfahrens gegen Unbekannt lediglich über die Zulässigkeit der Auskunftserteilung entschieden werden würde. Allerdings käme ein solches Verfahren praktisch einem allgemeinem Richtervorbehalt für die Auskunftserteilung durch die Diensteanbieter gleich. Der Unterschied bestünde dann nur noch in den am Prozess beteiligten Parteien.

Insgesamt bringt ein dem US-amerikanischen John-Doe-Verfahren angelehntes Verfahren gegen Unbekannt gegenüber einem Auskunftsverfahren gegen die Diensteanbieter daher keine wesentlichen Vorteile mit sich. Der Missbrauchsgefahr durch Auskunftsansprüche lässt sich auch durch anderweitige prozessuale Mittel - wie zum Beispiel einem Richtervorbehalt - vorbeugen, die mit der deutschen Zivilprozessordnung leichter in Einklang zu bringen sind. Stattdessen ist ein solches Verfahren in Bezug auf den Anspruch der Nutzer auf rechtliches Gehör nachteilig. Zudem ist auch den Diensteanbietern die Beteiligung am Auskunftsverfahren grundsätzlich zumutbar, da sie durch die Erbringung ihrer Dienste die Gelegenheit für Rechtsverletzungen schaffen.

II. Richtervorbehalt

Anstelle eines Verfahrens gegen Unbekannt können die Nachteile der Nutzer, die durch die Ausweitung der Identifizierungsmöglichkeiten durch

---

[52] S. *Laudeur/Gostomzyk*, NJW 2012, 710, 715.

[53] *Verheijden,* Rechtsverletzungen auf YouTube und Facebook, S. 317 f.

Auskunftsansprüche drohen, durch einen Richtervorbehalt ausgeglichen werden. Der Vorteil daran ist, dass im deutschen Zivil- bzw. Zivilprozessrecht der Richtervorbehalt bereits etabliert ist. Sowohl bei der Verkehrsdatenauskunft im Bereich des geistigen Eigentums als auch im Rahmen des Anspruchs aus § 21 Abs. 2 S. 2 TTDSG hat der Gesetzgeber einen Richtervorbehalt vorgesehen. An diese Regelungen kann für den allgemeinen Auskunftsanspruch de lege ferenda angeknüpft werden. Entschieden werden muss vor allem, in welchen Konstellationen eine vorherige richterliche Anordnung für die Auskunftserteilung notwendig sein soll. Dabei gilt es, die Vor- und Nachteile eines Richtervorbehalts zu beachten.

Gegen einen Richtervorbehalt spricht die lange Verfahrensdauer, bis es zu einer richterlichen Anordnung und anschließend zur Auskunftserteilung kommt.[54] In der Zwischenzeit könnten notwendige Nutzerdaten aber bereits gelöscht worden sein. Zudem entstehen Verfahrenskosten, die nicht erforderlich wären, wenn die Diensteanbieter auch ohne richterliche Anordnung zur Auskunftserteilung bereit wären, weil sie ein Auskunftsersuchen für berechtigt halten.[55]

Auf der anderen Seite dient der Richtervorbehalt dem Schutz besonders sensibler Nutzerdaten vor einer unberechtigten Weitergabe durch die Diensteanbieter.[56] Damit verbunden verhindert der Richtervorbehalt den Missbrauch von Auskunftsansprüchen zum Beispiel zur Ausforschung von Nutzerdaten.[57]

---

[54] S. zur Kritik am Richtervorbehalt in § 101 Abs. 9 UrhG *Regierungsetwurf,* BT-Drs. 16/5048, S. 56; *Bäcker,* ZUM 2008, 391, 392; *Ernst/Seichter*, ZUM 2007, 513, 513; *Nägele/Nietsche*, WRP 2007, 1047, 1050; *Schwarz/Brauneck,* ZUM 2006, 701, 710; *Zombik*, ZUM 2006, 450, 453 f.

[55] S. *Regierungsentwurf,* BT-Drs. 16/5048, S. 56; *Bäcker,* ZUM 2008, 391, 392; *Ernst/Seichter*, ZUM 2007, 513, 513; *Nägele/Nietsche*, WRP 2007, 1047, 1050; *Schwarz/Brauneck,* ZUM 2006, 701, 710; *Zombik*, ZUM 2006, 450, 453 f.

[56] Aus verfassungsrechtlichen Gründen wurde deshalb im Zuge der Umsetzung der Enforcement-Richtlinie ein Richtervorbehalt bei der Verwendung von Verkehrsdaten eingeführt; S. dazu *Regierungsentwurf,* BT-Drs. 16/5048, S. 63. Ebenfalls befürwortend *Raabe*, ZUM 2006, 439, 442; *Langhoff,* ZUM 2006, 457, 458.

[57] Ähnlich *Bohlen,* NJW 2020, 1999, 2003; Peukert/Kur, GRUR-Int 2006, 292, 297; Splittgerber/Klytta, K&R 2007, 78, 84.

Verfassungsrechtlich ist der Richtervorbehalt deshalb immer dann geboten, wenn es um die Verarbeitung besonders sensibler Daten geht oder wenn unklar ist, ob überhaupt eine Rechtsverletzung vorliegt, sodass das Risiko einer unberechtigten Auskunftserteilung besteht.

Um solche besonders sensiblen Daten handelt es sich unter anderem bei Verkehrsdaten. Verkehrsdaten können in zweierlei Hinsicht für die Identifizierung eines Nutzers herangezogen werden: Zum einen könnten Rechteinhaber von Telekommunikationsdiensten, die gleichzeitig Anwendungsdienste sind (wie zum Beispiel interpersonelle Kommunikationsdienste) Auskunft über Verkehrsdaten wie die IP-Adresse eines Nutzers begehren. In diesem Fall besteht eine Zuordnung der IP-Adresse zu einem Individualkommunikationsvorgang. Die Auskunftserteilung beeinträchtigt daher das Fernmeldegeheimnis des betroffenen Nutzers. Zum anderen können Verkehrsdaten zum Beispiel von Zugangsanbietern verwendet werden, um eine Auskunft über Bestandsdaten zu erteilen. In der Regel wird dabei eine IP-Adresse unter Verwendung von Zugriffszeiten einer Anschlusskennung zugeordnet. Dabei wird ebenfalls eine Verbindung zu einem Telekommunikationsvorgang hergestellt. In den allermeisten Fällen lässt sich nicht ausschließen, dass innerhalb dieses Telekommunikationsvorgang nicht auch Individualkommunikation stattgefunden haben könnte, sodass auch in diesem Fall das Fernmeldegeheimnis berührt ist.

Differenzierter verhält es sich bei Nutzungsdaten. Anders als Telekommunikationsdienste dienen Telemediendienste in aller Regel nicht der Individualkommunikation. Insbesondere sind interpersonelle Telekommunikationsdienste nach § 1 Abs. 1 TMG in Verbindung mit § 3 Nr. 61 lit. b) TKG nicht mehr als Telemedien zu klassifizieren. Sofern Telemediendienste lediglich Nutzungsdaten wie die IP-Adresse zur Bestandsdatenauskunft verwenden, erhalten die Rechteinhaber weder zusätzliche Informationen über den Telekommunikationsvorgang, noch wird das Fernmeldegeheimnis berührt. Anders verhält es sich aber, wenn Auskunft über Nutzungsdaten selbst erteilt wird, also insbesondere, wenn die IP-Adresse eines Nutzers an einen Rechteinhaber übermittelt wird. Hier lässt sich nicht ausschließen, dass dem Nutzer dieselbe IP-Adresse auch zur Individualkommunikation, die vor, während oder nach der Nutzung des Telemediendienstes erfolgt sein könnte, zugewiesen war. An die Übermittlung von

Nutzungsdaten sind daher strengere Anforderungen zu stellen, als wenn diese lediglich zur Bestandsdatenauskunft verwendet werden.

Ebenfalls zu den sensiblen Daten sind Daten von Nutzern von Online-Zahlungsdienstleistern zu zählen. Solche Auskünfte von Online-Zahlungsdienstleistern fallen grundsätzlich unter das Bankgeheimnis. Für diese Auskünfte müsste das Zeugnisverweigerungsrecht aus § 383 Abs. 1 Nr. 6 ZPO modifiziert werden.[58] Im Gegenzug sollte die Auskunftserteilung von Online-Zahlungsdienstleistern ebenfalls unter Richtervorbehalt stehen.

Keinen Richtervorbehalt bedarf es bei der Auskunft über Bestandsdaten (auch unter Verwendung von Nutzungsdaten), sofern eine offensichtliche Rechtsverletzung vorliegt.[59] Das Merkmal der Offensichtlichkeit dient in diesem Fall nicht dem Schutz der Diensteanbieter vor Falschbeurteilung, sondern dem Schutz der Nutzer vor vorschneller Weitergabe ihrer Daten.

Das Verfahren der richterlichen Anordnung kann in Anlehnung an das Gestattungsverfahren zum Beispiel nach § 101 Abs. 9 UrhG oder § 21 Abs. 3 TTDSG gestaltet werden. Sinnvoll ist insbesondere die Zuordnung des Verfahrens an die Landgerichte, sowie die Anwendung der Vorschriften des FamFG. Um ein zusätzliches Verfahren zu vermeiden, sollte das Gericht außerdem entsprechend dem § 21 Abs. 3 S. 2 TTDSG im Zuge der Gestattungsanordnung zugleich über die Verpflichtung zur Auskunftserteilung entscheiden.

III. Berücksichtigung von Nutzerinteressen

Ein Nachteil des Auskunftsverfahrens, das zwischen Rechtinhabern und Diensteanbietern geführt wird, besteht darin, dass die Nutzer nicht Prozesspartei werden und aufgrund ihrer Anonymität zwangsläufig keine Möglichkeit haben, ihre Ansichten vorzutragen.

---

[58] Für die Auskunftsansprüche im Bereich des geistigen Eigentums muss bereits jetzt eine unionsrechtskonforme Auslegung erfolgen; S. *Scheuch* in: BeckOK ZPO, § 383 ZPO Rn. 23.2.

[59] Ähnlich im Hinblick auf offensichtliche Rechtsverletzungen *Janal*, ZEuP 2021, 227, 261.

Damit Nutzerinteressen bessere Berücksichtigung finden können, könnten aber in Ergänzung zum Richtervorbehalt *amicus-curiae*-Briefe für Auskunftsverfahren gegen Internetdiensteanbieter institutionalisiert werden.[60]

Als Vorbild dient das US-amerikanische Recht, nach dem der *amicus curiae* (lateinisch für Freund des Gerichts) als parteiischer Sachverständiger in einem Schriftsatz seine Ansichten zu Tatsachen, aber auch Rechtsfragen anbringen kann.[61] Als *amici curiae* könnten sich zukünftig vor allem Interessensverbände anbieten.

In jedem Fall sollten die Diensteanbieter aber ähnlich wie nach § 21 Abs. 4 S. 2 TTDSG den betroffenen Nutzer über die Einleitung des Verfahrens unterrichten.

IV. Eilrechtsschutz

Da Diensteanbieter Nutzerdaten häufig nur zeitlich begrenzt speichern (dürfen), besteht die Notwendigkeit schnellen Rechtsschutz zu erwirken. Sofern in Fällen offensichtlicher Rechtsverletzung die Auskunft von Bestandsdaten begehrt wird, ohne dass es einer richterlichen Anordnung bedarf, sollte die Auskunftserteilung in Anlehnung zum Beispiel an § 101 Abs. 7 UrhG auch im Wege der einstweiligen Verfügung nach den §§ 935-945 ZPO angeordnet werden können. Das Merkmal der Offensichtlichkeit würde an dieser Stelle dem Zweck dienen, eine abweichende Entscheidung in der Hauptsache zu vermeiden.

In allen anderen Fällen sollte die Auskunftserteilung nicht vorweggenommen werden können. Stattdessen kann – wie bisher – nach § 49 FamFG eine einstweilige Anordnung an die Diensteanbieter ergehen, die ihnen verbietet, die zur Auskunftserteilung erforderlichen Daten im Rahmen des datenschutzrechtlich Zulässigen bis zur Entscheidung durch das Gericht zu löschen. Damit diese Regelung nicht leerläuft, bedarf es de lege ferenda aber einer entsprechenden datenschutzrechtlichen Erlaubnisnorm.

---

[60] S. auch *Janal,* ZEuP 2021, 227, 261.

[61] S. ausführlich zum *amicus curiae* im US-amerikanischen Recht *Kühne,* Amicus Curiae, S. 58 ff.

V. Darlegungs- und Beweislast und Beweisverwertungsverbot

Spezielle Regelungen für die Darlegungs- und Beweislast sind nicht erforderlich. Grundsätzlich müssen die Rechteinhaber das Vorliegen der Voraussetzungen ihres Auskunftsanspruchs darlegen und beweisen.

Sofern eine vorherige richterliche Anordnung erforderlich ist, greift der Amtsermittlungsgrundsatz des FamFG. Dies bietet einen zusätzlichen Schutz der Nutzer und verhindert die vorschnelle Herausgabe ihrer Daten.[62]

Im Folgeprozess gegen einen Anschlussinhaber sollte die Rechtsprechung des *BGH* zur sekundären Darlegungslast auch auf die Verletzung anderer absoluter Rechte als des Urheberrechts übertragen werden.[63]

Zur Wahrung der Interessen der Diensteanbieter bedarf es außerdem eines Beweisverwertungsverbotes im Hinblick auf die Verwertung der durch die Auskunftserteilung gewonnen Erkenntnisse in einem Straf- oder Ordnungswidrigkeitenverfahren im Sinne etwa des § 101 Abs. 8 UrhG.

VI. Kostentragung

Ein Ziel der Ausweitung der Auskunftsansprüche de lege ferenda ist unter anderem, dass die Rechteinhaber wieder verstärkt selbst die Rechtsdurchsetzungslast tragen. Entsprechend sind sie auch verpflichtet die Kosten für eine etwaige erforderliche richterliche Anordnung zu tragen. Der Verletzte muss insofern in Vorkasse gehen, kann aber gegebenenfalls gegen den identifizierten Rechtsverletzer Schadensersatzansprüche geltend machen.

Klagt der Rechteinhaber einen Auskunftsanspruch ein, für den es eigentlich keiner richterlichen Anordnung bedürfte, weil etwa der Diensteanbieter die

---

[62] *Bohlen,* NJW 2020, 1999, 2003 unter Bezugnahme auf *Beschlussempfehlung und Bericht des Ausschusses für Recht und Verbraucherschutz,* BT-Drs. 18/13013, S. 24.

[63] S. zur Rechtsprechung des BGH bei Urheberrechtsverletzungen *BGH*, Urt. v. 12.5.2010 – I ZR 121/08, ZUM 2010, 696 Rn. 12 – Sommer unseres Lebens; *BGH*, Urt. v. 8.1.2014 – I ZR 169/12, NJW 2014, 2360, 2360 - BearShare; *BGH*, Urt. v. 11.6.2015 - I ZR 75/14, MMR 2016, 131 Rn. 37 – Tauschbörse III; *BGH,* Urt. v. 30.3.2017 – I ZR 19/16, NJW 2018, 65 Rn. 15 – Loud.

Auskunftserteilung zu Unrecht verweigert, trägt er auch in diesem Prozess das Kostenrisiko. Unterliegt der Diensteanbieter in diesem Prozess, trägt er nach § 91 ZPO grundsätzlich auch die Kosten des Rechtsstreits.

Die Kostentragung kann dennoch eine Hürde für die Rechteinhaber darstellen, die sie im Einzelfall an ihrer Rechtsdurchsetzung hindern kann.[64] Allerdings unterscheidet sich dieser Umstand nicht wesentlich von Rechtsverletzungen in der analogen Welt. Zudem trägt die Kostentragungsregel dazu bei, die Missbrauchsgefahr, die von Auskunftsansprüchen ausgehen kann, zu reduzieren, da die Rechteinhaber abwägen müssen, ob sie das Kostenrisiko eingehen wollen.

Aus demselben Grund und weil die Diensteanbieter als Dritte in Anspruch genommen werden, sollte de lege ferenda der Rechteinhaber dem Diensteanbieter zum Ersatz der für die Auskunftserteilung erforderlichen Aufwendungen entsprechend dem § 101 Abs. 2 S. 3 UrhG verpflichtet werden.

D. Anpassung des Datenschutzrechts de lege ferenda

Damit die Auskunftsansprüche de lege ferenda auch tatsächlich zur Identifizierung eines Nutzers führen können, müssen diese von verhältnismäßigen Datenschutzregeln flankiert werden. Dabei muss sowohl die Erhebung und Speicherung von Nutzerdaten als auch deren Verarbeitung zur Auskunftserteilung in den Blick genommen werden.

Dabei wird angestrebt, die Identifizierungsmöglichkeiten der Rechteinhaber zu erweitern, ohne die Anonymität aller Internetnutzer in unverhältnismäßiger Weise einzuschränken.

I. Erhebung und Speicherung der notwendigen Daten

Die Identifizierung anonymer Internetnutzer scheitert häufig schon daran, dass Nutzerdaten nicht erhoben werden, beziehungsweise zum Zeitpunkt der Auskunftserteilung nicht (mehr) vorhanden sind.

---

[64] *Sahl/Bielzer*, ZRP 2020, 2, 3.

Aus Sicht aller Internetnutzer ist es im Hinblick auf ihr Recht auf Anonymität problematisch, wenn die Diensteanbieter präventiv und anlasslos dazu verpflichtet werden, Nutzerdaten zu erheben und für Auskunftszwecke zu speichern. Deshalb müssen Regelungen, die de lege ferenda den Diensteanbietern erweiterte Pflichten hinsichtlich der Erhebung und Speicherung von Nutzerdaten auferlegen, verhältnismäßig sein. Vor allem sollte eine punktuelle und anlassbezogene Speicherung der allgemeinen Erhebung von Daten aller Internetnutzer vorgezogen werden.

1. Bestandsdaten

Die Bestandsdatenauskunft ist in der Regel der schnellste und einfachste Weg für die Rechteinhaber, einen anonymen Nutzer zu identifizieren. So soll auch nach dem in dieser Arbeit vorgeschlagenen allgemeinen Auskunftsanspruch de lege ferenda, die Auskunftserteilung über Bestandsdaten bei offensichtlichen Rechtsverletzungen ohne vorherige richterliche Anordnung möglich sein. Außerdem reicht häufig die Auskunft eines einzelnen Diensteanbieters, wenn direkt bei dem zur Rechtsverletzung genutzten Anwendungsdienst der Name und die Anschrift des Nutzers erfragt werden kann.

a) Anwendungsdienste

Aus diesem Grund würden Registrierungspflichten vor allem bei Anwendungsdiensten dazu beitragen, dass anonyme Internetnutzer deutlich leichter identifiziert werden könnten. Wenn alle Nutzer sich mit ihrem Klarnamen anmelden müssten und gegebenenfalls lediglich nach außen hin unter einem Pseudonym auftreten würden, könnten die Diensteanbieter auf eine Anfrage des Rechteinhabers hin sehr leicht einen rechtsverletzenden Nutzer anhand von Bestandsdaten identifizieren.

Unter anderem deshalb und vor dem Hintergrund einer zunehmend verrohenden Online-Kommunikation werden teilweise Registrierungs- beziehungsweise Klarnamenpflichten bei der Nutzung von Internetdiensten und insbesondere von Plattformen wie sozialen Netzwerken oder Bewertungspattformen erwogen.[65]

---

[65] Ablehnend *Caspar,* ZRP 2015, 233, 234 f.

Jedenfalls ist eine Klarnamenpflicht in der Gestalt abzulehnen, dass die Nutzer auch nach außen hin unter ihrem Klarnamen auftreten müssen. Bei einer solchen Pflicht würden Auskunftsansprüche weitgehend an Bedeutung verlieren, da die Rechteinhaber leichter erkennen könnten, wer der rechtsverletzende Nutzer ist.

Dies würde aber das Recht auf Anonymität der Nutzer verletzen und letztlich das Ende des freien Internets bedeuten. [66] Dabei stellt sich schon die praktische Frage, ob die Diensteanbieter dann auch dazu verpflichtet wären, die Angaben der Nutzer zu verifizieren.[67] Es erscheint realitätsfern, wenn sich in Zukunft alle Nutzer von Internetdiensten zuvor zum Beispiel per Post-Ident-Verfahren oder über Online-Ausweisfunktionen ausweisen müssten.

Ein ähnliches Problem besteht auch, wenn die Diensteanbieter lediglich dazu verpflichtet werden, ihre Nutzer zu registrieren, diese dann aber nach außen hin unter einem Pseudonym auftreten können. Eine solche Registrierungspflicht wäre aber dennoch grundsätzlich ausreichend, um im Nachhinein eine Identifizierung eines Nutzers zumindest zu fördern. Zudem wäre dies ein milderes Mittel im Verhältnis zu einer „echten" Klarnamenpflicht. Ähnlich hat auch der *BGH* zur Klarnamenpflicht des sozialen Netzwerks Facebook entschieden: Facebook darf nach dieser Entscheidung seine Nutzer dazu auffordern, sich mit ihrem Klarnamen anzumelden, aber nicht dazu zwingen, diesen auch nach außen hin und gegenüber den anderen Nutzern anzugeben.[68] Allerdings besteht ein Unterschied, ob ein Dienst die Daten seiner Nutzer selbstständig erfragt oder ob der Staat Nutzer und Internetdiensteanbieter zur Angabe beziehungsweise Erhebung von Nutzerdaten zwingt. Unter anderem aus diesem Grund ist das BGH-Urteil auch nicht auf die Frage übertragbar, ob eine gesetzliche Registrierungspflicht für Internetdienste mit dem Ziel, zukünftige mögliche Rechtsverletzer zu identifizieren, verhältnismäßig wäre.[69]

---

[66] Ähnlich *Glaser,* NVwZ 2012, 1432, 1438; *Ohly,* AfP 2011, 428, 436.

[67] S. dazu auch *Janal,* ZeuP 2021, 227, 295 f.

[68] *BGH,* Urt. v. 27.1.2022 – III ZR 3/21, ZD 2022, 276 Rn. 40 – Klarnamenpflicht bei Facebook.

[69] Zudem ist die Entscheidung nicht auf der Basis der derzeitigen Rechtslage unter Anwendung der DS-GVO ergangen; S. dazu *Schwartmann*, ZD 2022, 133, 133 f.

Stattdessen ist eine allgemeine Registrierungspflicht, die alle Internetdienste und Nutzer umfasst, abzulehnen, da sie zu stark in das Recht der Nutzer auf Anonymität eingreifen würde und die Nutzer in der Ausübung ihrer grundrechtlichen Freiheiten stark beeinträchtigen würde.[70] Es kann deshalb auch dahinstehen, ob sich eine solche Verpflichtung im Einklang mit der DS-GVO bringen ließe.[71]

Als Argument für eine Klarnamen- beziehungsweise Registrierungspflicht wird zum Teil ein Vergleich mit dem Vermummungsverbot oder der Pflicht zur Anmeldung von Demonstrationen angeführt.[72] Eine Demonstration ist aber mit der Freiheitsausübung im Internet tatsächlich nicht vergleichbar. Aus einem Vermummungsverbot auf Demonstrationen kann außerdem nicht darauf geschlossen werden, dass Internetnutzer ihre Daten zur Identifizierung hinterlegen müssen. Trotz Vermummungsverbot sind einzelne Teilnehmer auf einer Demonstration nicht derartig identifizierbar, dass eine Vielzahl personenbezogener Daten wie Name, Anschrift, E-Mail-Adresse etc. erkennbar wäre. Einer Registrierungspflicht würde es eher entsprechen, wenn jeder Teilnehmer an einer Demonstration vorher beim Anmelder der Demonstration seine Daten angeben müsste und der Anmelder diese festhalten müsste.

Außerdem sind Daten, die gegenüber einem Internetdienst angegeben werden, deutlich sensibler und gefährdeter. Algorithmen können im Internet viele Einzelinformationen zu einem Gesamtbild zusammenfügen.[73] Dies ermöglicht unter Umständen auch die Erstellung von Persönlichkeitsprofilen. Die Anonymität ist im Internet deshalb von größerer Bedeutung als in der analogen Welt.

Grundsätzlich sollte daher auch de lege ferenda nur auf Daten zurückgegriffen werden können, die die Diensteanbieter freiwillig und im Einklang mit dem Datenschutzrecht erheben durften. Es ist auch nicht zu erwarten, dass dies zu einem völligen Leerlaufen der Auskunftsansprüche führen würde. Die Diensteanbieter sind nämlich nicht verpflichtet, eine vollständig anonyme Nutzung

---

[70] A.A. etwa *Lorenz*, VuR 2014, 83, 89 f.; *Pille* in: Münchener Anwaltshandbuch IT-Recht, Teil 15.2 Rn. 43.

[71] *Bafteh/Hattem*, ZD 2022, 283, 283 ff.; *Bock,* GRUR-Prax 2021, 30, 30.

[72] *Bohlen,* NJW 2020, 1999, 2004. S. im Ergebnis ablehnend *Ohly,* AfP 2011, 428, 436.

[73] *Härting,* NJW 2013, 2065, 2069.

ihrer Dienste zu ermöglichen.[74] In der Praxis erheben Internet-Dienste eine Vielzahl von Daten ihrer Nutzer. Auch die Nutzer geben häufig freiwillig zahlreiche Informationen gegenüber den Diensteanbietern preis. Sehr viele Internetdienste setzen im Vorfeld der Nutzung die Angabe von personenbezogenen Daten voraus. So müssen sich die Nutzer von sozialen Netzwerken, Online-Marktplätzen, Chatforen, Bewertungsplattformen etc. häufig vorab registrieren. Bei einigen Diensten ist die Angabe personenbezogener Daten auch zu Zahlungs- oder Abrechnungszwecken erforderlich. Dabei hängt es bei Anwendungsdiensten unter anderem von der Art des jeweiligen Dienstes ab, ob und welche Nutzerdaten erhoben werden können.[75]

All diese freiwillig preisgegebenen Daten werden aber allein aufgrund der Masse an Nutzern in der Regel durch die Diensteanbieter nicht verifiziert. Allerdings können auch nicht alle Nutzer von Internetdiensten durch Registrierungs- und Verifikationspflichten unter Generalverdacht gestellt werden. Das Recht aller Internetnutzer auf Anonymität überwiegt insofern dem Interesse der Rechteinhaber an der Rechtsdurchsetzung gegen einzelne rechtswidrig agierende Internetnutzer.

Ausnahmen sollte es aber bei Nutzern geben, die im geschäftlichen Verkehr agieren. Bei solchen Nutzern kommt eine Registrierungspflicht verbunden mit der Pflicht der Diensteanbieter, die angegebenen Daten zu überprüfen, durchaus in Betracht.[76] Bereits jetzt können Nutzer, die geschäftsmäßig eigene Inhalte anbieten – wie zum Beispiel Influencer oder Anbieter auf Online-Marktplätzen -, unter die Impressumspflicht des § 5 TMG fallen.[77] De lege ferenda wäre es

---

[74] Die Erhebung von Nutzerdaten durch Telemediendienste etwa bei der Registrierung ist insbesondere vereinbar mit § 19 Abs. 2 TTDSG, der Anbieter von Telemedien aufgibt, dass sie die Nutzung ihrer Dienste den Nutzern anonym oder unter Pseudonym ermöglichen müssen. § 19 Abs. 2 TTDSG bezieht sich nämlich nicht auf das Innenverhältnis zwischen den Diensteanbietern und ihren Nutzern. S. noch zu § 13 Abs. 6 TMG a.F. *OLG Düsseldorf,* Urt. v. 7.6.2006 - I-15 U 21/06, MMR 2006, 618, 620; *OLG Hamburg*, Urt. v. 4.2.2009 – 5 U 180/07, ZUM 2009, 417, 420 – Long Island Ice Tea; *Lauber-Rönsberg*, MMR 2014, 10, 13; Zu § 19 Abs. 2 TTDSG *Schwartmann,* ZD 2022, 133, 133 f.

[75] S. zu den üblicherweise bei Anwendungsdiensten erhobenen Daten bereits oben unter Kap. 4 § 3.

[76] So auch *Janal,* ZeuP 2021, 227, 260.

[77] S. dazu etwa *Solmecke* in: Hoeren/Sieber/Holznagel, Teil 21.1 Rn. 2 ff.

dennoch sinnvoll klarzustellen, dass geschäftsmäßige Nutzer verpflichtet sind, jedenfalls Name und Anschrift anzugeben, um ein etwaiges rechtliches Vorgehen gegen diese zu ermöglichen. Zudem werden Dienste - wie Online-Marktplätze -, die Fernabsatzgeschäfte mit Verbrauchern vermitteln, gemäß Art. 30 DSA dazu verpflichtet, die Daten geschäftsmäßiger Nutzer zu überprüfen.[78]

b) Zugangsdienste

Auch bei Zugangsdiensten sollte es grundsätzlich keine zusätzlichen Registrierungspflichten geben. Ohnehin werden bei Zugangsdiensten zum Teil Bestandsdaten der Nutzer erhoben. Vor allem bei Access-Providern ist es üblich, personenbezogene Daten ihrer Kunden zur Begründung eines Vertragsverhältnisses und zu Abrechnungszwecken zu speichern. Inzwischen sind diese auch zum Zwecke der Auskunftserteilung an Behörden nach § 172 Abs. 1 TKG dazu verpflichtet.

Darüber hinaus erscheint es aber erforderlich, die Anbieter von WLAN-Netzwerken dazu zu verpflichten, entweder ihren Anschluss wenigstens durch ein Passwort zu sichern oder ihre Nutzer zu registrieren. Dies lässt sich damit rechtfertigen, dass WLAN-Anbieter eine nicht unerhebliche Gefahrenquelle für die Rechtsgüter anderer schaffen, für die sie Verkehrssicherungspflichten tragen. Dies stünde derzeit im Widerspruch zu § 8 Abs. 4 TMG. Allerdings machen ungesicherte WLAN-Netzwerke die Identifizierung ihrer Nutzer praktisch unmöglich. Die derzeit vorgesehene und grundsätzlich sinnvolle Haftungsbeschränkung zugunsten von WLAN-Anbieter in § 8 Abs. 1 S. 2 TMG kann nicht gleichzeitig zu einer Freistellung von jeglicher Verantwortung führen. Sinnvoller erscheint es eine Haftungsfreistellung von WLAN-Anbietern von der Einhaltung konkreter Pflichten – wie Sicherungs- oder Registrierungspflichten abhängig zu machen.[79]

---

[78] S. Janal, ZEuP 2021, 227, 260 zur Regelung des Art. 22 DSA-E. S. zu einer solche Verpflichtung auch *EuGH,* Urt. v. 12.7.2011 - C-324/09, GRUR 2011, 1025 Rn. 142 – L'Oréal/eBay.

[79] S. dazu *EuGH,* Urt. v. 15.9.2016 – C-484/14, GRUR 2016, 1146 Rn. 90 ff. – McFadden.

2. Nutzungs- und Verkehrsdaten

Bei Nutzungs- und Verkehrsdaten ist die Speicherung von Nutzerdaten insgesamt problematischer als bei Bestandsdaten, da deren Speicherung in der Regel für die Erbringung eines Dienstes nicht erforderlich ist und gegebenenfalls das Fernmeldegeheimnis berühren kann.

a) Verdachtsunabhängige Speicherung von IP-Adressen

Besonders problematisch ist es auch hier wieder, wenn Nutzungs- beziehungsweise Verkehrsdaten anlasslos beziehungsweise präventiv für den Fall einer späteren Rechtsverletzung erhoben werden, da dies zwangsläufig die Daten aller Internetnutzer betrifft. Immer dann, wenn die Anwendungsdienste ihre Nutzer nicht bereits anhand von Bestandsdaten identifizieren können, sind Nutzungs- und Verkehrsdaten für die IP-basierte Identifizierung zwingend erforderlich. Dabei kommen Anwendungs- und Zugangsdiensten unterschiedliche Rollen zu.

aa) Anwendungsdienste

Bei den Anwendungsdiensten ist für die Identifizierung von Internetnutzern vor allem die Speicherung von IP-Adressen und Zugriffszeiten der Nutzer von Bedeutung. Diese könnten im Falle einer Rechtsverletzung eines Nutzers an die Rechteinhaber weitergegeben werden, die anschließend vom Access-Provider Auskunft über den Anschlussinhaber erhalten könnten.

Für Telekommunikationsdienste wie E-Mail-Dienste oder interpersonelle Kommunikationsdienste handelt es sich hierbei um Verkehrsdaten, die grundsätzlich unmittelbar nach dem Ende einer Verbindung zu löschen sind. Eine darüber hinaus gehende Verpflichtung der Diensteanbieter zur Speicherung der Verkehrsdaten ohne konkreten Anlass würde einen unverhältnismäßigen Eingriff in das Fernmeldegeheimnis aller Internetnutzer darstellen.

Alle anderen Anwendungsdienste und insbesondere Telemediendienste können Nutzungsdaten unter Einhaltung der Vorgaben aus Art. 5, 6 DS-GVO auch nach dem Ende des Nutzungsvorgangs in ihren Log-Dateien speichern. Nach der DS-GVO kann dies aber auch nicht präventiv für den Fall eines späteren Auskunftsbegehren durch die Rechteinhaber erfolgen. Eine gesetzliche

Verpflichtung dieser Dienste, Daten vorsorglich für etwaige Rechtsverletzungen abzuspeichern, ist daher abzulehnen.

bb) Zugangsdienste

Bei Auskunftsbegehren gegen Zugangsdienste geht es in der Regel darum, eine IP-Adresse zu einem Internetanschluss zurückzuverfolgen. Access-Provider können zu diesem Zweck die von ihnen zugewiesenen IP-Adressen mit den Zugriffszeiten abgleichen, um zu ermitteln, welchem Anschluss eine IP-Adresse zum fraglichen Zeitpunkt zugeordnet war. Anschließend können sie Auskunft über die Bestandsdaten des auf diese Weise ermittelten Anschlussinhabers erteilen.

Auch die Zugangsanbieter müssen grundsätzlich Verkehrsdaten nach dem Ende der Verbindung löschen. Die nationalen Regelungen zur Vorratsdatenspeicherung nach §§ 175, 176 TKG wurden inzwischen vom *EuGH* für unionsrechtswidrig erklärt.[80] Ohnehin dürften Daten, die zum Zweck der Vorratsdatenspeicherung gespeichert wurden, nicht für die Auskunftserteilung an Rechteinhaber verwendet werden. Auch zukünftig sollte nichts anderes gelten. Die Pflicht zur anlasslosen Vorratsdatenspeicherung ist – wenn überhaupt – nur zur Verfolgung schwerer Straftaten zulässig. Die enge Zweckbindung der Daten ist eine Voraussetzung dafür, dass eine Vorratsdatenspeicherung überhaupt dem hohen datenschutzrechtlichen Standard der Bundesrepublik Deutschland und der europäischen Union genügen kann.

b) Einzelfallbezogene Speicherung

Anstelle einer anlasslosen Speicherung von Nutzungs- und Verkehrsdaten sollte eine Lösung angestrebt werden, die im Einzelfall eine Identifizierung von rechtsverletzenden Nutzern anhand ihrer IP-Adresse ermöglicht, ohne dabei die Interessen aller Internetnutzer zu verletzen. Sofern dabei der Anwendungsbereich der e-privacy-Richtlinie betroffen ist, ergibt sich aus Art. 15 Abs. 1 e-privacy-Richtlinie i.V.m. Art. 23 Abs. 1 lit. j) DS-GVO ein ausreichender Regelungsspielraum für eine verhältnismäßige nationale Regelung.[81]

---

[80] *EuGH*, Urt. v. 20.09.2022 - Az. C-793/19, NJW 2022, 3135, 3135 ff.

[81] Vgl. *EuGH*, Urt. v. 29.1.2008 - C-275/06, GRUR 2008, 241 Rn. 53 ff. – Promusicae.

aa) Login-Falle

Bei Anwendungsdiensten bietet sich als Lösung die Einrichtung einer sogenannten Log-in-Falle an. Die Login-Falle ist ein Vorschlag des Vereins D64 zur Bekämpfung von Hate Speech im Internet.[82] Das Ziel dieses Vorschlags ist es eine Rechtsverfolgung zu ermöglichen, ohne zuvor eine Masse an Nutzerdaten anlasslos erheben zu müssen. Der Gedanke entspricht der Rechtsverfolgung in der analogen Welt: Zuerst wird eine Tat begangen und erst anschließend verfolgt.

Der Vorschlag lautet wie folgt:[83] Zunächst wird ein möglicherweise rechtsverletzender Inhalt angezeigt und von geschulten Polizisten überprüft. Stellen diese einen Anfangsverdacht fest, wird dem entsprechenden Nutzer die Login-Falle gestellt. Wenn dieser das nächste Mal den Dienst nutzt, erhebt der Dienst die IP-Adresse und gibt diese an die Ermittlungsbehörde weiter. Die Ermittlungsbehörde kann anschließend vom Access-Provider Auskunft über die zugehörigen Bestandsdaten erhalten.

Dieser Vorschlag ist zwar nicht so effektiv wie eine anlasslose Speicherung aller Nutzerdaten, stellt aber dafür ein verhältnismäßiges Mittel dar. Er ist daher auch auf die private, zivilrechtliche Rechtsdurchsetzung übertragbar: Anstelle der Behörden sollten die Rechteinhaber de lege ferenda mit einer entsprechenden richterlichen Anordnung eine Login-Falle erwirken können. Die Rechteinhaber müssten dafür gegenüber dem Gericht eine Rechtsverletzung nachweisen. Das Gericht könnte anschließend gegenüber dem Diensteanbieter die Einrichtung einer Login-Falle anordnen. Wenn der Nutzer den Dienst erneut aufruft, werden die Daten direkt an den Rechteinhaber übermittelt. Das Verfahren für die richterliche Anordnung könnte genauso wie das Verfahren bei einem für die Auskunftserteilung erforderlichen Richtervorbehalt ausgestaltet werden.

bb) Vorübergehende Speicherung

Darüber hinaus ist es erforderlich, dass die Rechteinhaber eine Löschung von Daten, die für die Auskunftserteilung erforderlich wären, durch die

---

[82] S. https://d-64.org/login-falle/ (Stand: 24.05.2022). S. dazu auch *Caspar*, ZRP 2021, 193, 193.

[83] S. https://d-64.org/login-falle/ (Stand: 24.05.2022).

Diensteanbieter verhindern können. Die Auskunftserteilung über oder unter Verwendung von Verkehrsdaten an Rechteinhaber erfordert nach dem in dieser Arbeit vorgeschlagenen allgemeinen Auskunftsanspruch de lege ferenda eine vorherige richterlicher Anordnung. Aufgrund der sehr kurzen Speicherfristen dieser sensiblen Daten kann es aber passieren, dass diese bis zur richterlichen Entscheidung bereits nicht mehr vorhanden sind.

Die Gerichte können die Diensteanbieter durch eine einstweilige Anordnung nach §§ 49 ff. FamFG in diesem Fall dazu verpflichten, die Daten nicht zu löschen. Dafür muss de lege ferenda eine entsprechende datenschutzrechtlichen Erlaubnisnorm geschaffen werden, die es den Diensteanbietern gestattet, aufgrund einer Anordnung nach §§ 49 ff. FamFG die zur Auskunftserteilung erforderlichen Daten nicht zu löschen. Eine entsprechende Regelung einer anlassbezogenen vorübergehenden Datenspeicherung schafft einen verhältnismäßigen Ausgleich zwischen den Interessen der Rechteinhaber mit dem Schutz der Anonymität der Nutzer.[84]

II. Verarbeitung der Daten zur Auskunftserteilung

Einer Anpassung des Datenschutzrechts bedarf es daneben auch im Hinblick auf die Weitergabe und Verwendung von Nutzerdaten zum Zwecke der Auskunftserteilung. Es bedarf datenschutzrechtlicher Vorschriften, die den allgemeinen Auskunftsanspruch de lege ferenda ergänzen. Diese Regelungen müssen es den Diensteanbietern erlauben, die zur Identifizierung notwendigen Auskünfte zu erteilen. Genau wie der Auskunftsanspruch selbst müssen auch die datenschutzrechtlichen Erlaubnisnormen weit gefasst sein. Die Erlaubnis muss alle Anbieter von Internetdiensten erfassen. Dabei muss sowohl die Herausgabe von Bestands-, als auch von Nutzungs- und Verkehrsdaten gestattet werden. Ebenso müssen die Diensteanbieter Nutzungs- und Verkehrsdaten zur Auskunftserteilung über Bestandsdaten verwenden dürfen.

Die Erlaubnis sollte - ebenso wie der Auskunftsanspruch selbst - unter der Bedingung stehen, dass die Daten für die Durchsetzung der zivilrechtlichen Ansprüche erforderlich sind.

---

[84] Ähnlich *Sandor,* Datenspeicherung, Rn. 800 ff.

Die Verhältnismäßigkeit dieser recht weitgehenden Befugnisse wird unter anderem durch das Erfordernis einer richterlichen Anordnung bei nicht-offensichtlichen Rechtsverletzungen sowie bei besonders sensiblen Nutzerdaten sichergestellt. Zudem ist das Eingriffsgewicht einer solchen punktuellen Auskunftserteilung als eher gering zu werten. Es können lediglich gezielt die Nutzerdaten in Erfahrung gebracht werden, die zur Verfolgung einer konkreten Rechtsverletzung erforderlich sind. Insbesondere eröffnet die Gestattung des Auskunftsanspruchs an die Rechteinhaber diesen nicht die Möglichkeit, anlasslos Nutzerdaten auszuforschen oder Persönlichkeitsprofile zu erstellen.[85] Sofern durch die Erlaubnisnormen eine zweckändernde Weitervergabe von Nutzerdaten gestattet wird, ist eine solche auch aufgrund der Öffnungsklausel aus Art. 6 Abs. 4 DS-GVO mit der Datenschutzgrundverordnung vereinbar. Im Anwendungsbereich der e-privacy-Richtlinie ergibt sich die Zulässigkeit einer nationalen Regelung aus Art. 15 Abs. 1 e-privacy-Richtlinie i.V.m. Art. 23 Abs. 1 lit. j) DS-GVO.[86]

E. Zusammenfassung Kapitel 7

De lege ferenda sollte ein allgemeiner Auskunftsanspruch geschaffen werden, der die bestehenden Auskunftsansprüche ablöst und die Inhaber aller absoluten Rechte gleichstellt. Das Ziel eines solchen Anspruchs ist es, einen Teil zu einem verhältnismäßigen Ausgleich der widerstreitenden Interessen der Rechteinhaber, Diensteanbieter und Nutzer anhand der Grundsätze der praktischen Konkordanz beizutragen.

Der Auskunftsanspruch muss sich in ein Gesamtkonzept für den Umgang mit rechtswidrigen Inhalten und Handlungen im Internet einfügen lassen. Dabei spielen insbesondere auch Erwägungen über die Verteilung von Lasten und Verantwortung eine Rolle. Der Auskunftsanspruch soll sicherstellen, dass Nutzer, die die Rechte anderer verletzen, selbst Verantwortung für ihre Handlungen übernehmen müssen. Umgekehrt sollten die Lasten und das Risiken der

---

[85] Vgl. *BVerfG,* Urt. v. 2.3.2010 - 1 BvR 256/08 u.a., NJW 2010, 833 Rn. 356- Vorratsdatenspeicherung.

[86] Vgl. *EuGH*, Urt. v. 29.1.2008 - C-275/06, GRUR 2008, 241 Rn. 53 ff. – Promusicae.

Rechtsdurchsetzung – so wie auch außerhalb der digitalen Welt – die Rechteinhaber tragen.

Mit der Ausweitung der Identifizierungsmöglichkeiten sollte aus diesem Grund einhergehen, dass die Diensteanbieter im Verhältnis zu ihren Nutzern grundsätzlich lediglich subsidiär haften. Dabei gilt es aber zu beachten, dass schon aus Verhältnismäßigkeitsgründen die Identifizierung der Nutzer nicht grenzenlos möglich sein wird und jedenfalls sehr zeitintensiv sein kann. Um zu verhindern, dass selbst Inhalte, die die Rechte anderer sehr stark beeinträchtigen, bis zur Identifizierung der Nutzer online abrufbar sind, sollten Host-Provider nur dann subsidiär haften, wenn sie selbst anhand von Bestandsdaten den verantwortlichen Nutzer identifizieren können. Daneben sollten Host-Provider außerdem die Pflicht treffen, offensichtlich rechtswidrige Inhalte zu entfernen.

Host-Provider und insbesondere Plattform-Betreiber könnten zukünftig noch stärker eine Vermittlerrolle zwischen Rechteinhabern und Nutzern einnehmen, wenn Möglichkeiten der Identifizierung eines rechtsverletzenden Nutzers in das Notice-and-Take-Down-Verfahren integriert werden. Eine Grundlage dafür bietet der DSA, der in Art. 16, 17 DSA ein Notice-and-Take-Down-Verfahren vorsieht. Dies lässt sich auch mit weiteren Pflichten von Plattform-Betreibern aus dem DSA-E, wie der Institutionalisierung eines internen Beschwerdemanagements (Art. 20 DSA) und der Verpflichtung, Zugang zur außergerichtlichen Streitbeilegung (Art. 21 DSA) zu gewähren, verbinden.

Der allgemeine Auskunftsanspruch de lege ferenda stellt daher eine wichtige Ergänzung zur Haftung und Inpflichtnahme der Diensteanbieter dar. Für die Ausgestaltung des Auskunftsanspruchs de lege ferenda kann zum Teil auf die bereits bestehenden Vorschriften zur Auskunftserteilung zurückgegriffen werden. Diese könnten zum Beispiel im TTDSG zusammengeführt und wie folgt modifiziert werden:

Um die Möglichkeiten der Identifizierung auszuweiten, sollte der Auskunftsanspruch de lege ferenda alle Diensteanbieter erfassen und den Inhabern aller Arten von absolut geschützten Rechten zustehen. Außerdem sollten keine besonderen Anforderungen an die Rechtsverletzung gestellt werden. Der Auskunftsanspruch sollte zudem sowohl die Auskunft über Bestandsdaten als auch über

Nutzungs- und Verkehrsdaten, sowie die Verwendung von Nutzungs- und Verkehrsdaten ermöglichen. Des Weiteren kann auch eine Auskunft über Nutzer ermöglicht werden, bei denen unklar ist, ob diese selbst die Rechtsverletzung begangen haben, weil etwa ihr Nutzerkonto oder ihr Internetanschluss von einer anderen Person verwendet worden sein könnte. Dabei kann sich an der Formulierung des § 21 Abs. 2 TTDSG orientiert werden. Die Auskunft ist demnach zu erteilen, „soweit dies zur Durchsetzung zivilrechtlicher Ansprüche wegen der Verletzung absolut geschützter Rechte (...) erforderlich ist." Das nach Art. 8 Abs. 1 Enforcement-Richtlinie geforderte Verhältnismäßigkeitserfordernis greift lediglich bei richterlicher Anordnung der Auskunftserteilung. Für den Fall, dass die Auskunftserteilung unter Richtervorbehalt steht, prüfen die Gerichte die Verhältnismäßigkeit im Einzelfall. Im Übrigen hat der Gesetzgeber die Verhältnismäßigkeit sicherzustellen, indem etwa nur bei offensichtlicher Rechtsverletzung eine Auskunftserteilung ohne Richtervorbehalt ermöglicht wird. Eines gesonderten Verhältnismäßigkeitserfordernisses, das die Diensteanbieter zu prüfen hätten, bedarf es nicht. Um sicherzustellen, dass die Diensteanbieter eine korrekte Auskunft erteilen, sollten diese für den Fall einer grob fahrlässig oder vorsätzlich falsch erteilten Auskunft, gegenüber den Rechteinhabern auf Ersatz der dadurch entstandenen Schäden haften.

Damit der sehr weit gefasste Auskunftsanspruch de lege ferenda die Verhältnismäßigkeit wahrt und um etwaigen Missbrauch vorzubeugen, bedarf es eines geeigneten prozessualen Rahmens. Im Vordergrund steht dabei der Richtervorbehalt. Dieser ist immer dann erforderlich, wenn zur Auskunftserteilung sensible Daten verarbeitet werden oder wenn unklar ist, ob überhaupt eine Rechtsverletzung vorliegt. Das Verfahren kann ähnlich ausgestaltet werden wie zum Beispiel in § 101 Abs. 9 UrhG oder § 21 Abs. 3 TTDSG. Zudem könnten amicus-curiae-Briefe zur Berücksichtigung von Nutzerinteressen im Auskunftsverfahren zugelassen werden. In Fällen offensichtlicher Rechtsverletzung, in denen keine richterliche Anordnung erforderlich ist, sollte die Auskunftserteilung außerdem im Wege der einstweiligen Verfügung angeordnet werden können. Bei einem Verfahren bei Richtervorbehalt kann eine einstweilige Anordnung nach §§ 49 ff. FamFG ergehen, die es dem Diensteanbieter verbietet, die zur Auskunftserteilung erforderlichen Daten bis zum Abschluss des Verfahrens zu löschen.

Zur Realisierung des Auskunftsanspruchs sind de lege ferenda außerdem Anpassungen des Datenschutzrechts erforderlich. Eine Verpflichtung der Diensteanbieter, anlasslos Nutzerdaten zu erheben und zu verifizieren ist nur bei Bestandsdaten von geschäftsmäßigen Nutzern möglich. Im Übrigen ist zur Wahrung des Rechts auf Anonymität der Internetnutzer eine einzelfallbezogene Speicherpflicht der Diensteanbieter vorzuziehen. Zu diesem Zweck sollten die Rechteinhaber de lege ferenda nach richterlicher Anordnung die Einrichtung einer Login-Falle erwirken können. Außerdem gilt es, eine Rechtsgrundlage dafür zu schaffen, dass die Diensteanbieter bis zu der Entscheidung in der Hauptsache auf eine einstweilige Anordnung nach §§ 49 ff. FamFG hin Nutzerdaten weiterhin speichern dürfen. Zudem müssen Erlaubnisnormen für die Verarbeitung von Daten zum Zwecke der Auskunftserteilung geschaffen werden, die mit dem Auskunftsanspruch de lege ferenda abgestimmt sind.

Kapitel 8

Ergebnisse der Arbeit und Ausblick

Rechtsverletzungen durch anonyme Nutzer im Internet sind Massenphänomene, die sowohl die Gesetzgebung als auch die Judikative vor Herausforderungen stellen.

Die Anonymität der Nutzer kann die Rechteinhaber daran hindern, ihre Rechte gegenüber einem Nutzer durchsetzen zu können. Dafür reicht es aus, wenn sie selbst den Nutzer nicht unmittelbar identifizieren können. Da jede Internetnutzung Spuren hinterlässt, kann aber eine Identifizierung häufig durch eine Auskunft von Internetdiensteanbietern erfolgen.

Für die Rechteinhaber bedeutet die Anonymität vieler Nutzer außerdem eine erhöhte Gefährdung ihrer Rechtsgüter. Wenn Nutzer nicht selbst für von ihnen begangene Rechtsverletzungen belangt werden können, ist es naheliegend, dass Rechtsverletzungen im Internet jedenfalls begünstigt werden. Neben der Anonymität der Nutzer beinhaltet aber auch die schnelle, weltweite Verbreitung von Inhalten via Internet und die damit verbundene Perpetuierung von Rechtsverletzungen ein nicht unerhebliches Gefährdungspotential für die Rechteinhaber.

Zwischen Rechteinhabern, Nutzern von Internetdiensten und den Diensteanbietern besteht bei anonymen Rechtsverletzungen ein Interessenskonflikt, der zu einem angemessenen und möglichst schonenden Ausgleich gebracht werden muss. Aus der Untersuchung der widerstreitenden Interessen hat sich ergeben, dass der Schutz der Anonymität rechtsverletzender Nutzer in der Regel nicht die Interessen der Rechteinhaber an der Durchsetzung ihrer Rechte überwiegt. Allerdings dürfen auch nicht alle Internetnutzer unter Generalverdacht gestellt werden. Die Anonymität und die Freiheitsausübung derjenigen Nutzer, die im Einklang mit der Rechtsordnung agieren, gilt es aus diesem Grund vorrangig zu schützen. Die Interessen dieser Nutzer überwiegen insoweit die Interessen der

Rechteinhaber. Die Lücken und Nachteile, die sich aus der Anonymität der Nutzer ergeben, können aber auch nicht vollumfänglich durch die Inpflichtnahme der Diensteanbieter kompensiert werden. Die Diensteanbieter tragen zwar eine Mitverantwortung für Rechtsverletzungen ihrer Nutzer, können sich aber gleichzeitig auf ihre unternehmerische Freiheit und ihre Berufsfreiheit berufen. Sie dürfen sich grundsätzlich darauf verlassen, dass die Nutzer ihr Verhalten an der Rechtsordnung ausrichten. Den Diensteanbietern dürfen deshalb gemessen an ihrem tatsächlichen Verursachungsbeitrag keine zu ausufernde Pflichten auferlegt werden. Insbesondere muss auch eine Identifizierung der anonymen Nutzer als unmittelbare Rechtsverletzer grundsätzlich möglich sein, um die Inpflichtnahme der Diensteanbieter auszugleichen und reduzieren zu können.

Die Grundlage für die Untersuchung der de lege lata existierenden Identifizierungsmöglichkeiten durch Auskunftsansprüche der Diensteanbieter bilden die Ergebnisse der Betrachtung der technischen Möglichkeiten einer Identifizierung. Dabei hat sich gezeigt, dass im Wesentlichen zwei verschiedene Möglichkeiten bestehen, die Identität eines anonymen Nutzers zu ermitteln. Am einfachsten ist es in der Regel, wenn der Nutzer direkt bei einem Anwendungsdienst anhand von Bestandsdaten identifiziert werden kann. Alternativ können Internetnutzer auch anhand ihrer IP-Adresse zurückverfolgt werden. Dies erfordert häufig aber die Beteiligung mehrerer Diensteanbieter.

Basierend auf diesen Ergebnissen hat sich gezeigt, dass die de lege lata bestehenden Auskunftsmöglichkeiten in vielen Fällen unzureichend sind, um eine Identifizierung anonymer Nutzer zu gewährleisten. Die Hauptprobleme sind, dass bereits die Auskunftsansprüche selbst nicht ausreichend umfassend sind oder Erlaubnisnormen für die Verarbeitung der erforderlichen Nutzerdaten fehlen. Zudem ist das System der Auskunftsansprüche zum Teil widersprüchlich und führt zu einer Ungleichbehandlung der Inhaber unterschiedlicher absoluter Rechte.

Diese Lücken bei der Rechtsdurchsetzung können auch nicht durch alternative Rechtsdurchsetzungsmöglichkeiten ausgeglichen werden. Weder die Möglichkeit der Identifizierung eines Nutzers anhand einer Akteneinsicht im Strafverfahren noch die Verlagerung von Pflichten auf die Diensteanbieter stellen

Alternativen für einen wirksamen Auskunftsanspruch gegen Internetdiensteanbieter dar. Vielmehr müssen in einem sinnvollen Konzept alle denkbaren Instrumente Einzug finden und miteinander in Einklang gebracht werden.

Daran anknüpfend ist de lege ferenda ein allgemeiner Auskunftsanspruch gegen Internetdiensteanbieter zur Identifizierung anonymer Nutzer zu schaffen, der in die bestehenden Haftungskonzepte integriert werden muss. Dabei kann der Auskunftsanspruch dazu beitragen, dass Diensteanbieter weniger stark in die Pflicht genommen werden müssen. Nicht nur auf nationaler, sondern insbesondere auf Unionsebene erscheint es deshalb möglich und erforderlich, den erkennbaren Trend, den Diensteanbietern immer ausufernde Pflichten aufzuerlegen, umzukehren. Vor allem sollten die Diensteanbieter grundsätzlich gegenüber ihren Nutzern lediglich subsidiär haften. Dies dient unter anderem dem Schutz rechtmäßig agierender Nutzer und trägt außerdem zu einer angemessenen Verteilung von Verantwortung und Lasten bei.

Der allgemeine Auskunftsanspruch muss die aufgezeigten Defizite der Auskunftsansprüche de lege lata ausgleichen, soweit dies mit dem Verhältnismäßigkeitsgrundsatz zu vereinbaren ist. Dafür ist der Anspruch möglichst weit zu fassen und sollte alle Inhaber absoluter Rechte gleichermaßen erfassen. Auf prozessualer Ebene trägt als Ausgleich dafür vor allem ein Richtervorbehalt bei der Verarbeitung sensibler Daten oder bei nicht offensichtlichen Rechtsverletzungen zur angemessenen Berücksichtigung der Nutzerinteressen bei.
Außerdem sind datenschutzrechtlichen Rahmenbedingungen herzustellen, die die Erfüllung des Auskunftsanspruchs erst ermöglichen. Anstelle einer weitergehenden anlasslosen Speicherung von Nutzerdaten sollte es den Rechteinhaber ermöglicht werden, eine Anordnung zur Einrichtung einer Login-Falle zu erwirken. Außerdem bedarf es einer datenschutzrechtlichen Vorschrift, die es den Diensteanbietern gestattet, im Rahmen einer einstweiligen Anordnung nach §§ 49 ff. FamFG Nutzerdaten bis zur Entscheidung in der Hauptsache zu speichern. Im Übrigen ist durch die Einführung entsprechender Erlaubnisnormen sicherzustellen, dass die Diensteanbieter die erforderlichen Daten zum Zwecke der Auskunftserteilung an die Rechteinhaber verarbeiten dürfen.

Das Ziel des allgemeinen Auskunftsanspruchs de lege ferenda kann es aber nicht sein, eine lückenlose Identifizierung aller Internetnutzer zu ermöglichen. Dies

wäre weder verhältnismäßig noch realisierbar, da Anonymisierungsdienste eine Rückverfolgung anonymer Nutzer in einigen Fällen unmöglich machen. Vielmehr soll der Auskunftsanspruch dazu beitragen, die recht einseitige Verlagerung der Verantwortung auf die Diensteanbieter auszugleichen.

Der Umgang mit rechtswidrigen Inhalten im Internet wird auch zukünftig die Rechtswissenschaft weiter beschäftigen. In naher Zukunft werden vor allem die Neuerungen auf EU-Ebene durch den Digital Services Act zum Gegenstand weiterer Diskussionen werden. Unklar ist außerdem, wie sich die schon seit längerem erwartete e-privacy-Verordnung auf den hier vorgeschlagenen Auskunftsanspruch auswirken könnte.

Literaturverzeichnis

Abdallah, Tarek/Gercke, Björn: Strafrechtliche und strafprozessuale Probleme der Ermittlung nutzerbezogener Daten im Internet, ZUM 2005, 368-376.

Albrecht, Jan/Jotzo, Florian: Das neue Datenschutzrecht der EU, Synopse, Baden-Baden 2017.

Alsbih, Amir: Der reale Wert einer IP-Adresse, DuD 2011, 482-488.

Arning, Marian/Moos, Flemming/Schefzig, Jens: Vergiss (,) Europa! Ein Kommentar zu EuGH, Urt. V. 13.5.2014 – Rs. C-131/12 – Google/Mario Costeja Gonzalez, CR 2014, 460, CR 2014, 447-456.

Askani, Helena: Private Rechtsdurchsetzung bei Urheberrechtsverletzungen im Internet, Baden-Baden 2021.

Assion, Simon: Stellungnahme als Sachverständiger zum Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG), BT-Druchsache 19/27441, abrufbar unter: https://www.bundestag.de/resource/blob/835498/3fc24ea374301c2ba608c9509cc64ec1/19-9-1039_Stellungnahme_SV_Assion_oeA_TTDSG_21-04-2021-data.pdf (Stand: 24.05.2022).

Auernhammer: Eßer, Martin/Kramer, Philipp/Lewinski, Kai von (Hrsg.), DSGVO/BDSG-Kommentar, 7. Auflage, Köln 2020 (zit.: *Bearbeiter* in: Auernhammer).

Auer-Reinsdorff, Astrid/Conrad, Isabell (Hrsg.): Handbuch IT- und Datenschutzrecht, 3. Auflage, München 2019 (zit.: *Bearbeiter* in: Auer-Reinsdorff/Conrad).

Bafteh, Philip/Hattem, Marek van: Anmerkung zu BGH, Urteil vom 27.01.2022 – III ZR 3/21 – Klarnamenpflicht bei Facebook, ZD 2022, 283-285.

Bange, Andreas: Von SOPA zum Copyright Alert System: Ein privatrechtlicher Ansatz zum Schutz gegen urheberrechtsverletzendes Streaming im Internet, Stuttgart 2016.

Bantlin, Franziska: Grundrechtsschutz bei Telekommunikationsüberwachung und Online-Durchsuchung, JuS 2019, 669-673.

Bauer, Sebastian: Soziale Netzwerke und strafprozessuale Ermittlungen, Berlin 2018.

Bäcker, Kerstin: Starkes Recht und schwache Durchsetzung, ZUM 2008, 391-396.

Bär, Wolfgang: Anmerkung zu AG Offenburg, Beschluss vom 20.7.2007 – 4 Gs 442/07, MMR 2007, 811-813.

Bäumler, Helmut/Mutius, Albert von (Hrsg.): Anonymität im Internet. Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts, Wiesbaden 2003 (zit.: *Bearbeiter* in: Bäumler/Mutius).

Beck, Simon/Kreißig, Wolfgang: Tauschbörsen-Nutzer im Fadenkreuz der Strafverfolgungsbehörden, NStZ 2007, 304-310.

Beck, Susanne: Internetbeleidigung de lege lata und de lege ferenda. Strafrechtliche Aspekte des „spickmich"-Urteils, MMR 2009, 736-740.

Becker, Maximilian: Automatisierte Rechtsdurchsetzung im Umsetzungsentwurf zu Art. 17 DSM-RL, ZUM 2020, 681-691.

Becker, Maximilian: Von der Freiheit, rechtswidrig handeln zu können. „Upload-Filter" und technische Rechtsdurchsetzung, ZUM 2019, 636-648.

Becker, Maximilian: Positive und negative Zeichenberechtigung im Internet, WRP 2010, 467-474.

Beckhaus, Gerrit: Die Bewältigung von Informationsdefiziten bei der Sachverhaltsaufklärung, Tübingen 2010.

Beck-Online Großkommentar Zivilrecht: Gsell, Beate/Krüger, Wolfgang/Lorenz, Stephan/Reymann, Christoph (Hrsg.), München (zit.: *Bearbeiter* in: BeckOGK).

Beck'scher Online-Kommentar BGB: Hau, Wolfgang/Poseck, Roman (Hrsg.), 61. Edition, München 2022 (zit.: *Bearbeiter* in: BeckOK BGB).

Beck'scher Online-Kommentar Datenschutzrecht: Brink, Stefan/Wolff, Amadeus (Hrsg.), 39. Edition, München 2022 (zit.: *Bearbeiter* in: BeckOK Datenschutzrecht).

Beck'scher Online-Kommentar FamFG: Hahne, Mea-Micaela/Schlögel, Jürgen/Schlünder, Rolf (Hrsg.), 42. Edition, München 2022 (zit.: *Bearbeiter* in: FamFG).

Beck'scher Online-Kommentar Grundgesetz: Epping, Volker/Hillgruber, Christian (Hrsg.), 50. Edition, München 2022 (zit.: *Bearbeiter* in: BeckOK GG).

Beck'scher Online-Kommentar Informations- und Medienrecht: Gersdorf, Hubertus/Paal, Boris (Hrsg.), 35. Edition, München 2022 (zit.: *Bearbeiter* in: BeckOK Informations- und Medienrecht).

Beck'scher Online-Kommentar JMStV: Liesching, Marc (Hrsg.), 20. Edition, München 2021 (zit.: *Bearbeiter* in: BeckOK JMStV).

Beck'scher Online-Kommentar Markenrecht: Kur, Annette/Bomhard, Verena/Albrecht, Friedrich (Hrsg.), 29. Edition, München 2022 (zit.: *Bearbeiter* in: BeckOK Markenrecht).

Beck'scher Online-Kommentar StGB: Heintschel-Heinegg, Bernd von (Hrsg.), 52. Edition, München 2022 (zit.: *Bearbeiter* in: BeckOK StGB).

Beck'scher Online-Kommentar StPO: Graf, Jürgen (Hrsg.), 43. Edition, München 2022 (zit.: *Bearbeiter* in: BeckOK StPO).

Beck'scher TKG-Kommentar: Geppert, Martin/Schütz, Raimund (Hrsg.), 4. Auflage, München 2013 (zit.: Bearbeiter in Beck´scher TKG-Kommentar).

Beck'scher Online-Kommentar Urheberrecht: Ahlberg, Hartwig/Götting, Horst-Peter/Lauber-Rönsberg, Anne (Hrsg.), 33. Edition, München 2022 (zit.: *Bearbeiter* in: BeckOK Urheberrecht).

Beck'scher Online-Kommentar ZPO: Vorwerk, Volkert/Wolf, Christian (Hrsg.), 44. Edition, München 2022 (zit.: *Bearbeiter* in: BeckOK ZPO).

Bergt, Matthias: Die Bestimmbarkeit als Grundproblem des Datenschutzrechts, ZD 2015, 365-371.

Bernreuther, Friedrich: Zur Interessensabwägung bei anonymen Meinungsäußerungen im Internet, AfP 2011, 218-223.

Bertermann, Nikolaus: Anmerkung zu LG Köln, Urteil vom 13.05.2015 – 28 O 11/15, MMR 2015, 524-526.

Betinger, Torsten/Freytag, Stefan: Verantwortlichkeit der DENIC e.G. für rechtswidrige Domains, CR 1999, 28-38.

Beukelmann, Stephan: Die Strafbarkeit von Feindeslisten, NJW-Spezial 2021, 248.

Bieszk, Dorothea/Stadtler, Susanne: Mobbing und Stalking: Phänomene der modernen (Arbeits-)Welt und ihre Gegenüberstellung, NJW 2007, 3382-3387.

Billmeier, Eva: Die Düsseldorfer Sperrungsverfügung: Ein Beispiel für verfassungs- und gefahrenabwehrrechtliche Probleme der Inhaltsregulierung in der Informationsgesellschaft, Münster 2007.

Bleich, Holger/Heidrich, Joerg/Stadler, Thomas: Schwierige Gegenwehr. Was tun bei unberechtigten Filesharing-Abmahnungen?, c´t 2020/19, S. 138-141.

Bock, Michael: Zulässigkeit der Klarnamenpflicht auf Facebook, GRUR-Prax 2021, 30.

Bockslaff, Frederik/Krause, Ringo: Anmerkung zu BGH, Beschluss vom 19.04.2012 – I ZB 80/11 – Alles kann besser werden, MMR 2012, 693-694.

Bohlen, Marc: Der zivilrechtliche Auskunftsanspruch bei der Bekämpfung von Hass im Internet, NJW 2020, 1999-2004.

Bohne, Daniel: Zum Erfordernis eines gewerblichen Ausmaßes der Rechtsverletzung in § 101 Abs. 2 UrhG, CR 2010, 104-109.

Bohne, Daniel: BGH: Drittauskunftsanspruch auch ohne gewerbliches Ausmaß der Rechtsverletzung, GRUR-Prax 2012, 405-407.

Bosbach, Jens/Wiege, Stephanie: Die strafrechtliche Verantwortlichkeit des Usenet-Providers nach dem Urheberrechtsgesetz, ZUM 2012, 293-299.

Böckenförde, Thomas: Die Ermittlung im Netz. Möglichkeiten und Grenzen neuer Erscheinungsformen strafprozessualer Ermittlungstätigkeit, Tübingen 2003.

Böckenförde, Thomas: Auf dem Weg zur elektronischen Privatsphäre. Zugleich Besprechung von BVerfG, Urteil v. 27.2.2008 – „Online-Durchsuchung", JZ 2008, 925-939.

Brand, Thimo/Skowronek, Yannick: Die Herausforderungen der Digitalisierung für das zivilprozessuale Beweisverfahren, RDi 2021, 178-186.

Brauneck, Jens: DSGVO: Neue Anwendbarkeit durch neue Definition personenbezogener Daten?, EuZW 2019, 680-688.

Breyer, Patrick: (Un-)Zulässigkeit einer anlasslosen, siebentägigen Vorratsdatenspeicherung, MMR 2011, 573-578.

Breyer, Patrick: Personenbezug von IP-Adressen. Internetnutzung und Datenschutz, ZD 2014, 400-405.

Britz, Gabriele: Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, 411-415.

Brink, Stefan/Eckhardt, Jens: Wann ist ein Datum ein personenbezogenes Datum?, ZD 2015, 205-212.

Brunst, Phillip: Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, Berlin 2009.

Brüggemann, Sebastian: Der Drittauskunftsanspruch gegen Internetprovider, Baden-Baden 2012.

Brüggemann, Sebastian: Urheberrechtsdurchsetzung im Internet. Ausgewählte Probleme des Drittauskunftsanspruchs nach § 101 UrhG, MMR 2013, 278-282.

Brüning, Christoph/Helios, Marcus: Die verfassungsprozessuale Durchsetzung grundrechtlicher Schutzpflichten am Beispiel des Internets, Jura 2001, 155-162.

Buchner, Benedikt: Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, 155-161.

Bulowski, Stefan: Regulierung von Internetkommunikationsdiensten, Baden-Baden 2019.

Burkert, Clemens: Rechtsfragen bei der Öffnung lokaler Internetzugänge, Baden-Baden 2015.

Burschel, Hans-Otto: Einstellen von Bildern in Whatsapp ist keine Kontaktaufnahme, NZFam 2018, 1056.

Canaris, Claus-Wilhelm: Grundrecht und Privatrecht. Eine Zwischenbilanz, Berlin 1999.

Caspar, Johannes: Login-Falle oder locked in Überwachung?, ZRP 2021, 193.

Caspar, Johannes: Klarnamenpflicht versus Recht auf pseudonyme Nutzung, ZRP 2015, 233-236.

Conrad, Albrecht: Zum Modell der Rechteklärung und Rechteverwaltung auf Hosting-Plattformen, ZUM 2017, 289-301.

Cornils, Matthias: Präzisierung, Vervollständigung und Erweiterung: Die Änderungen des Netzwerkdurchsetzungsgesetzes 2021, NJW 2021, 2465-2471.

Culik, Nicolai/Döpke, Christian: Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen, ZD 2017, 226-230.

Czychowski, Christian: Das Gesetz zur Verbesserung der Durchsetzung von Rechten des Geistigen Eigentums Teil II: Änderungen im Urheberrecht, GRUR-RR 2008, 265-268.

Czychowski, Christian: Auskunftsansprüche gegenüber Internetzugangsprovidern „vor" dem 2. Korb und „nach" der Enforcement-Richtlinie der EU, MMR 2004, 514-519.

Czychowski, Christian/Nordemann, Jan Bernd: Grenzenloses Internet – entgrenzte Haftung?. Leitlinien für ein Haftungsmodell der Vermittler, GRUR 2013, 986-996.

Czychowski, Christian/Nordemann, Jan Bernd: Höchstrichterliche Rechtsprechung und Gesetzgebung im Urheberrecht 2012, NJW 2013, 756-761.

Czychowski, Christian/Nordemann, Jan Bernd: Vorratsdaten und Urheberrecht – Zulässige Nutzung gespeicherter Daten, NJW 2008, 3095-3099.

Determann, Lothar: Kommunikationsfreiheit im Internet. Freiheitsrechte und gesetzliche Beschränkungen, Baden-Baden 1999.

Dix, Alexander/Petri, Thomas: Das Fernmeldegeheimnis und die deutsche Verfassungsidentität, DuD 2009, 531-535.

Dregelis, Max: Wohin laufen meine Daten?. Datenschutz bei Sportuhren und Fitnesstrackern, VuR 2017, 256-262.

Dreier, Horst (Hrsg.): Grundgesetz Kommentar, Band I: Präambel, Artikel 1-19, 3. Auflage, Tübingen 2013 (zit.: *Bearbeiter* in: Dreier).

Dreier, Thomas/Schulze, Gernot (Hrsg.): Urheberrechtsgesetz Kommentar, 7. Auflage, München 2022 (zit.: *Bearbeiter* in: Dreier/Schulze).

Dreier, Thomas: Die Schlacht ist geschlagen – ein Überblick. Zum Ergebnis des Copyright Package der EU-Kommission, GRUR 2019, 771-779.

Dreyer, Gunda/Kotthoff, Jost/Meckel, Jost/Hentsch, Christian-Henner (Hrsg.): Urheberrecht, 4. Auflage, Heidelberg 2018 (zit.: *Bearbeiter* in: Dreyer/Kotthoff/Meckel/Hentsch).

Durner, Wolfgang: Fernmeldegeheimnis und informationelle Selbstbestimmung als Schranken urheberrechtlicher Sperrverfügungen im Internet?, ZUM 2010, 833-846.

Dustmann, Andreas: Die privilegierten Provider. Haftungseinschränkungen im Internet aus urheberrechtlicher Sicht, Baden-Baden 2001.

Ebner, Markus/Kulhanek, Tobias: Verhetzende Beleidigung (§ 192a StGB), ZStW 133 (2021), 984-1000.

Eckel, Philipp/Rottmeier, Christian: „Liken als Haten": Strafverfolgung von Hatespeech in Sozialen Netzwerken, NStZ 2021, 1-11.

Eckhardt, Jens: Anwendungsbereich des Datenschutzrechts – Geklärt durch den EuGH?, CR 2016, 786-790.

Ehmann, Eugen/Selmayr, Martin: Datenschutz-Grundverordnung, DS-GVO, Kommentar, 2. Auflage, München 2018 (zit.: *Bearbeiter* in: Ehmann/Selmayr).

Eifinger, Maxim: Deutsche Gerichte unzuständig für Anordnung nach § 101 IX UrhG bei Sitz des Internet-Service-Providers in Großbrittanien, GRUR-Prax 2011, 474-475.

Eisenreich, Georg: Digital Services Act – ein wirksames Instrument gegen Hass und Hetze im Netz?, RDi 2021, 289-293.

Ensthaler, Jürgen/Weidert, Stefan (Hrsg.): Handbuch Urheberrecht und Internet, 3. Auflage, Frankfurt am Main 2017 (zit.: *Bearbeiter* in: Ensthaler/Weidert).

Erfurth, Julian: Vom Störer zum Täter – Neue Ansätze zur Plattformhaftung nach EuGH Coty ./. Amazon und BGH YouTube, GRUR-Prax 2021, 217-219.

Ernst, Stefan/Seichter, Dirk: Die Störerhaftung des Inhabers eines Internetzugangs, ZUM 2007, 513-519.

Federrath, Hannes: Technische Grundlagen von Auskunftsansprüchen, ZUM 2006, 434-439.

Federrath, Hannes/Pfitzmann, Andreas: „Neue" Anonymitätstechniken. Eine vergleichende Übersicht, DuD 1998, 628-632.

Feldmann, Thorsten: Die Unterlassungsverpflichtung des Access-Providers als Störer, K&R 2011, 225-228.

Fischer, Linn-Karen: Die Einbindung von Providern in die Durchsetzung von Urheberrechten, Tübingen 2020.

Franz, Ulrich: Der digitale Pranger. Bewertungsportale im Internet, Berlin 2018.

Freiling, Felix/Heinson, Dennis: Probleme des Verkehrsdatenbegriffs im Rahmen der Vorratsdatenspeicherung, DuD 2009, 547-552.

Freiwald, Sven: Die private Vervielfältigung im digitalen Kontext am Beispiel des Filesharing, Baden-Baden 2004.

Freund, Bernhard/Schnabel, Christoph: Bedeutet IPv6 das Ende der Anonymität?, MMR 2011, 495-499.

Frey, Dieter/Rudolph, Carl: Das Urheberrechts-Diensteanbieter-Gesetz – ein Überblick, MMR 2021, 671-677.

Frey, Harald: Haftungsprivilegierung des Access-Providers nach § 8 TMG?, MMR 2014, 650-654.

Freytag, Stefan: Voraussetzungen des Auskunftsanspruchs im Gestattungsverfahren, GRUR-Prax 2021, 716.

Friehe, Matthias: Löschen und Sperren in sozialen Netzwerken, NJW 2020, 1697-1702.

Fromm, Karl/Nordemann, Jan (Hrsg.): Urheberrecht, Kommentar, 12. Auflage, Stuttgart 2018 (zit.: *Bearbeiter* in: Fromm/Nordemann).

Gabel, Detlev: Neue Rahmenbedingungen für den Datenschutz im Internet, ZUM 2002, 607-613.

Galetzka, Christian/Stamer, Erik: Streaming – aktuelle Entwicklungen in Recht und Praxis. Redtube, kinox.to & Co., MMR 2014, 292-298.

Geidel, Doreen: Pflicht zur Löschung ehrverletzender Kommentare durch Hosting-Anbieter, ZUM 2021, 16-26.

Gercke, Marco: Zugangsprovider im Fadenkreuz der Urheberrechtsinhaber, CR 2006, 210-216.

Germann, Michael: Gefahrenabwehr und Strafverfolgung im Internet, Berlin 2019.

Gersdorf, Hubertus: Hate Speech in sozialen Netzwerken. Verfassungswidrigkeit des NetzDG-Entwurfs und grundrechtliche Einordnung der Anbieter sozialer Netzwerke, MMR 2017, 439-447.

Gielen, Nico/Tiessen, Marten: Die neue Plattformhaftung nach der Richtlinie über das Urheberrecht im digitalen Binnenmarkt, EuZW 2019, 639-646.

Gielen, Nico/Uphues, Steffen: Digital Markets Act und Digital Services Act. Regulierung von Markt- und Meinungsmacht durch die Europäische Union, EuZW 2021, 627-637.

Gietl, Andreas/Mantz, Reto: Die IP-Adresse als Beweismittel im Zivilprozess, CR 2008, 810-816.

Glaser, Andreas: Grundrechtlicher Schutz der Ehre im Internetzeitalter, NVwZ 2012, 1432-1438.

Gnirck, Karen/Lichtenberg, Jan: Internetprovider im Spannungsfeld staatlicher Auskunftsersuchen, DuD 2004, 598-602.

Greger, Reinhard: Der surfende Richter: Sachverhaltsaufklärung per Internet, in: Festschrift für Rolf Stürner zum 70. Geburtstag, Tübingen 2013, S. 289-300.

Greve, Holger/Schärdel, Florian: Der digitale Pranger – Bewertungsportale im Internet, MMR 2008, 644.

Grisse, Karina: Was bleibt von der Störerhaftung?. Bedeutung der 3. Änderung des TMG für die zivilrechtliche Systematik und Umsetzung der Vermittlerhaftung in Deutschland, GRUR 2017, 1073-1081.

Grosskopf, Lambert: Anmerkung zu LG Hamburg, Beschl. v. 21.4.2006 – 308 O 139/06, CR 2007, 122-124.

Großmann, Sven: Der Beleidigungstatbestand: Partielle Reform oder grundlegende Revision?, GA 2020, 546-563.

Gröpl, Christoph/Windthorst, Kay/Coelln, Christian von (Hrsg.): Studienkommentar Grundgesetz, 3. Auflage, München 2017 (zit.: *Bearbeiter* in: Gröpl/Windthorst/Coelln).

Grözinger, Andreas: Die Überwachung von Cloud-Storage, Baden-Baden 2018.

Grünberger, Michael: Die Entwicklung des Urheberrechts im Jahr 2017 – Teil I, ZUM 2018, 271-285.

Grünberger, Michael: Die Entwicklung des Urheberrechts im Jahr 2017 – Teil II, ZUM 2018, 321-340.

Grünwald, Andreas/Nüßing, Christoph: Kommunikation over the Top. Regulierung für Skype, WhatsApp oder Gmail?, MMR 2016, 91-97.

Gola, Peter (Hrsg.): Datenschutz-Grundverordnung: DS-GVO, Kommentar, 2. Auflage 2018, München 2018 (zit.: *Bearbeiter* in: Gola).

Gola, Peter/Klug, Christoph: Die Entwicklung des Datenschutzrechts im ersten Halbjahr 2017, NJW 2017, 2593-2596.

Gotthardt, Lukas: Zivilprozessuale Rechtsdurchsetzung in Filesharing-Fällen mit Familienbezug – Nachforschungspflichten im Rahmen des sekundären Darlegungslast unter Berücksichtigung aktueller Rechtsprechung, ZUM 2021, 7-16.

Gounalakis, Georgios/Rhode, Lars: Persönlichkeitsschutz im Internet, München 2002.

Guggenberger, Nikolaus: Das Netzwerkdurchsetzungsgesetz – schön gedacht, schlecht gemacht, ZRP 2017, 98-101.

Habermann, Heiko: Die zivilrechtliche Störerhaftung bei einer Verletzung von Immaterialrechtsgütern im Internet, Hamburg 2016.

Haeffs, Julia: Der Auskunftsanspruch im Zivilrecht. Zur Kodifikation des allgemeinen Auskunftsanspruchs aus Treu und Glauben (§ 242 BGB), Baden-Baden 2010.

Hansen, Hauke/Struwe, Dario: Speicherung von IP-Adressen zur Abwehr von Cyberattacken zulässig. Anmerkung zu EuGH, Urteil vom 19.10.2016 – C-582/14 – Breyer, GRUR-Prax 2016, 503.

Hartmann, Alexander: Unterlassungsansprüche im Internet. Störerhaftung für nutzergenerierte Inhalte, München 2009.

Härting, Niko: Internetrecht, 6. Auflage, Köln 2017.

Härting, Niko: Anonymität und Pseudonymität im Datenschutzrecht, NJW 2013, 2065-2071.

Härting, Niko: Schutz von IP-Adressen. Praxisfolgen der BVerfG-Rechtsprechung zu Onlinedurchsuchung und Vorratsdatenspeicherung, ITRB 2009, 35-39.

Härting, Niko: Datenschutz im Internet. Wo bleibt der Personenbezug?, CR 2008, 743-748.

Härting, Niko/Schätzle, Daniel: Rechtsverletzungen in Social Networks, ITRB 2010, 39-42.

Heckmann, Jörn/Nordmeyer, Arne: Pars pro toto: Verletzung des Urheberrechtsgesetzes durch das öffentliche Zugänglichmachen von Dateifragmenten („Chunks“) in Peer-to-Peer-Tauschbörsen?, CR 2014, 41-45.

Heckmann, Dirk/Wimmers, Jörg: Stellungnahme der DGRI zum Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG), CR 2017, 310-316.

Heid, Veronika: Die Haftung bei Urheberrechtsverletzungen im Netz. Zur Reichweite des § 97 UrhG, Baden-Baden 2013.

Heidrich, Joerg/Scheuch, Brian: Das Netzwerkdurchsetzungsgesetz: Anatomie eines gefährlichen Gesetzes, in: Taeger, Jürgen (Hrsg.), Recht 4.0 – Innovationen aus den rechtswissenschaftlichen Laboren, Edewecht 2017, S. 305-320.

Hennemann, Moritz: Die Inanspruchnahme von Zugangsvermittlern: Von der Störerhaftung zum Sperranspruch, ZUM 2018, 754-762.

Hennemann, Moritz: Urheberrechtsdurchsetzung und Internet, Baden-Baden 2011.

Herbst, Tobias: Was sind personenbezogene Daten?, NVwZ 2016, 902-906.

Herrmann, Christoph/Würdemann, Aike: Herkunftslandprinzip oder Marktortprinzip? Zur Kollision des außergerichtlichen Auskunftsanspruchs gemäß § 101 Abs. 2 Satz 1 Nr. 3 UrhG und des luxemburgischen Bankgeheimnisses, GRUR Int. 2017, 933-943.

Herwig, Stefan: Austarierung von Anonymität und Verantwortung im Netz, ZD 2012, 558-563.

Hesse, Konrad: Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, Neudr. der 20. Auflage, Heidelberg 1999.

Heymann, Thomas: Das Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums, CR 2008, 568-575.

Hilgard, Mark: Pseudonymisierte Zivilklagen aus den USA. Unwägbarkeiten für ausländische Beklagte bei John Doe-Verfahren, IWRZ 2018, 250-253.

Hindelang, Steffen: Freiheit und Kommunikation. Zur verfassungsrechtlichen Sicherung kommunikativer Selbstbestimmung in einer vernetzten Gesellschaft, Berlin 2019.

Hinderks, Tobias: Die Kennzeichnungspflicht von Deepfakes, ZUM 2022, 110-119.

Hoeren, Thomas: Internetrecht, 3. Auflage, Berlin 2018.

Hoeren, Thomas: Was ist das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme?, MMR 2008, 365-366.

Hoeren, Thomas: Vorratsdaten und Urheberrecht – Keine Nutzung gespeicherter Daten, NJW 2008, 3099-3102.

Hoeren, Thomas: Anonymität im Web – Grundfragen und aktuelle Entwicklungen, ZRP 2010, 251-253.

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.): Handbuch Multimedia-Recht, 57. Ergänzungslieferung, München 2021 (zit.: *Bearbeiter* in: Hoeren/Sieber/Holznagel).

Hoffmann, Helmut: Das Auskunftsverfahren nach § 101 Abs. 9 UrhG n.F., MMR 2009, 655-661.

Hoffmann, Helmut: Die Entwicklung des Internet-Rechts bis Mitte 2009, NJW 2009, 2649-2655.

Hoffmann-Riem, Wolfgang: Kommunikationsfreiheiten. Kommentierungen zu Art. 5 Abs. 1 und 2 sowie Art. 8 GG, Baden-Baden 2002.

Hofmann, Franz: Schadensersatzpflicht von Upload-Plattformen, jurisPR-WettbR 9/2022 Anm. 1.

Hofmann, Franz: Störerhaftung des Domain-Registrars im Urheberrecht, NJW 2021, 274-277.

Hofmann, Franz: Das neue Urheberrechts-Diensteanbieter-Gesetz, NJW 2021, 1905-1910.

Hofmann, Franz: Fünfzehn Thesen zur Plattformhaftung nach Art. 17 DSM-RL, GRUR 2019, 1219-1229.

Hofmann, Franz: Kontrolle oder nachlaufender Rechtsschutz – wohin bewegt sich das Urheberrecht?, GRUR 2018, 21-29.

Hofmann, Franz: Prozedualisierung der Haftungsvoraussetzungen im Medienrecht – Vorbild für die Intermediärshaftung im Allgemeinen?, ZUM 2017, 102-109.

Hofmann, Franz: Mittelbare Verantwortlichkeit im Internet. Eine Einführung in die Intermediärshaftung, JuS 2017, 713-719.

Hofmann, Franz: Die Verletzung der Vertraulichkeit informationstechnischer Systeme durch Google Street View, CR 2010, 514-518.

Hohlweck, Martin: „Even Heaven Cries" – Eine rechtliche Zwischenbilanz von Filesharing-Verfahren, GRUR 2014, 940-947.

Holznagel, Bernd: Phänomen „Fake News" – Was ist zu tun?. Ausmaß und Durchschlagskraft von Desinformationskampagnen, MMR 2018, 18-22.

Holznagel, Bernd: Das Compliance-System des Entwurfs des Netzwerkdurchsetzungsgesetzes, ZUM 2017, 615-624.

Holznagel, Bernd: Domainnamen- und IP-Nummern-Vergabe – eine Aufgabe der Regulierungsbehörde?, MMR 2003, 219-222.

Holznagel, Daniel: Nach dem EUGH-Urteil in Sachen YouTube/Cyando: Fast alles geklärt zur Host-Provider-Haftung?, CR 2021, 603-608.

Holznagel, Daniel: Put-back-Ansprüche gegen soziale Netzwerke: Quo Vadis?, CR 2019, 518-526.

Holznagel, Daniel: Auskunft des Resellers über den Namen seiner Endnutzer (in Filesharingfällen) – kein Richtervorbehalt nach § 101 Abs. 9 UrhG, CR 2017, 193-197.

Holznagel, Daniel: Notice and Take-Down-Verfahren als Teil der Providerhaftung, Tübingen 2013.

Hornung, Gerrit: Ein neues Grundrecht. Der verfassungsrechtliche Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme, CR 2008, 299-306.

Hoven, Elisa/Wittig, Alexandra: Das Beleidigungsunrecht im digitalen Zeitalter, NJW 2021, 2397-2401.

Hunziker, Sven/Sassenberg, Thomas: Notwendigkeit einer Vereinbarung zur Auftragsverarbeitung bei Telekommunikationsdiensten?, CR 2019, 188-195.

Intveen, Carsten: Beweis für Rechtsverletzungen in Filesharingsystem, ITRB 2008, 124-125.

Isensee, Josef/Kirchhof, Paul: Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band V: Rechtsquellen, Organisation, Finanzen, 3. Auflage, Heidelberg 2007 (zit.: *Bearbeiter* in: Isensee/Kirchhoff V).

Isensee, Josef/Kirchhof, Paul: Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band VIII: Grundrechte, Wirtschaft, Verfahren, Gleichheit, 3. Auflage, Heidelberg 2010 (zit.: *Bearbeiter* in: Isensee/Kirchhoff VIII).

Issa, Tarek: Das „1-und-1-Prinzip": Zum Verfahren nach § 101 Abs. 9 UrhG und der zivilprozessualen Verwertbarkeit von Auskünften nach § 101 Abs. 2 Satz 1 Nr. 3 UrhG in sogenannten „Reseller"-Fällen, ZUM 2017, 390-398.

Janal, Ruth: Friendly Fire? Das Urheberrechts-Diensteanbieter-Gesetz und sein Verhältnis zum künftigen Digital Services Act, GRUR 2022, 211-221.

Janal, Ruth: Haftung und Verantwortung im Entwurf des Digital Services Acts, ZEuP 2021, 227-274.

Janal, Ruth: Europäisches Zivilverfahrensrecht und gewerblicher Rechtsschutz, Tübingen 2015.

Jansen, Frank/Hartmann, Sebastian: Straining und Mobbing im Lichte des Persönlichkeitsschutzes, NJW 2012, 1540-1545.

Jarass, Hans/Pieroth, Bodo (Hrsg.): Grundgesetz für die Bundesrepublik Deutschland: GG, 17. Auflage, München 2022 (zit.: *Bearbeiter* in: Jarass/Pieroth).

Jobst, Simon: Konsequenzen einer unmittelbaren Grundrechtsbindung Privater, NJW 2020, 11-16.

Jones, Laura: Die urheberrechtliche Haftung von Intermediären im Rechtsvergleich, Tübingen 2020.

Jüngel, Marc/Geißler, Tim: Der neue Auskunftsanspruch aus § 101 UrhG unter Berücksichtigung der bisherigen Rechtsprechung, MMR 2008, 787-792.

Kaesling, Katharina/Knapp, Jakob: Umsetzung der urheberrechtlichen Verantwortlichkeit von Upload-Plattformen, MMR 2021, 11-15.

Kaesling, Katharina/Knapp, Jakob: „Massenkreativität" in sozialen Netzwerken. Überlegungen zur Plattformverantwortlichkeit nach der DSM-RL, MMR 2020, 816-821.

Karg, Moritz: Anonymität, Pseudonyme und Personenbezug revisited?, DuD 2015, 520-526.

Karg, Moritz/Fahl, Constantin: Rechtsgrundlagen für den Datenschutz in sozialen Netzwerken, K&R 2011, 453-458.

Karger, Michael: Praktische Hinweise zum Parteivortrag nach der BGH-Entscheidung zur Störerhaftung des WLAN-Betreibers, GRUR-Prax 2010, 305-308.

Kartheuser, Ingemar/Gilsdorf, Friedrich: EuGH: Dynamische IP-Adressen können personenbezogene Daten sein, MMR-Aktuell 2016, 382533.

Kastl, Graziana: Filter – Fluch oder Segen?. Möglichkeiten und Grenzen von Filtertechnologien zur Verhinderung von Rechtsverletzungen, GRUR 2016, 671-678.

Kaufmann, Noogie: Metatagging – Markenrecht oder reformiertes UWG?, MMR 2005, 348-352.

Keiser, Thorsten: Schadensersatz und Schmerzensgeld bei Stalking?, NJW 2007, 3387-3391.

Keller, Daphne: Facebook Filters, Fundamental Rights, and the CJEU's Glawischnig-Piesczek Ruling, GRUR-Int. 2020, 616-623.

Kiethe, Kurt: Verwertung rechtswidrig erlangter Beweismittel im Zivilprozess, MDR 2005, 965-970.

Kindt, Anne: Grundrechtsschutz für Raubkopierer und Musikpiraten?, MMR 2009, 147-153.

Kiper, Dennis-Kenji/Kubis, Marcel: Anmerkung zu BGH, Urteil vom 16.5.2017 – VI ZR 135/13, MMR 2017, 608-610.

Kersten, Jens: Anonymität in der liberalen Demokratie, JuS 2017, 193-203.

Kiparski, Gerd: Die Telekommunikations-Datenschutzregelungen im neuen TTDSG. Überblick, Auslegung, Kritik, CR 2021, 482-491.

Kiparski, Gerd/Sassenberg, Thomas: DSGVO und TK-Datenschutz – Ein komplexes europarechtliches Geflecht, CR 2018, 324-330.

Kipshagen, Alexander: Haftung bei offenem WLAN. Ein Vergleich mit anderen Intermediären sowie zur Rechtslage in Großbritannien und den USA, Baden-Baden 2017.

Kitz, Volker: Rechtsdurchsetzung im geistigen Eigentum – die neuen Regeln, NJW 2008, 2374-2377.

Kitz, Volker: Zur Verantwortlichkeit für die Spiegelung von Inhalten eines Usenet-Servers, CR 2007, 603-605.

Kitz, Volker: Urheberschutz im Internet und seine Einfügung in den Gesamtrechtsrahmen, ZUM 2006, 444-450.

Kitz, Volker: § 101 a UrhG: Für eine Rückkehr zur Dogmatik. Zugleich Anmerkung zu LG Hamburg 308 O 264/04 und LG Köln 28O 301/04, ZUM 2005, 298-303.

Kitz, Volker: Die Auskunftspflicht des Zugangsvermittlers bei Urheberrechtsverletzungen durch seine Nutzer, GRUR 2003, 1014-1019.

Klett, Alexander: Zum Auskunftsanspruch nach § 101a UrhG, K&R 2005, 222-224.

Knaack, Roland: Die EG-Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums und ihr Umsetzungsbedarf im deutschen Recht, GRUR-Int 2004, 745-750.

Klöhn, Lars/Schmolke, Klaus: Unternehmensreputation (Corporate Reputation). Ökonomische Erkenntnisse und ihre Bedeutung im Gesellschafts- und Kapitalmarktrecht, NZG 2015, 689-697.

Koch, Robert: Haftung für die Weiterverbreitung von Viren durch E-Mails, NJW 2004, 801-807.

Kohl, Kathrin: Die Haftung der Betreiber von Kommunikationsforen im Internet und virtuelles Hausrecht, Münster 2007.

Kondziela, Andreas: Staatsanwälte als Erfüllungsgehilfen der Musik- und Pornoindustrie?. Akteneinsicht in Filesharing-Verfahren, MMR 2009, 295-300.

Koreng, Ansgar: Entwurf eines Netzwerkdurchsetzungsgesetzes: Neue Wege im Kampf gegen „Hate Speech"?, GRUR-Prax 2017, 203-205.

Koreng, Ansgar: Das „Unternehmenspersönlichkeitsrecht" als Element des gewerblichen Reputationsschutzes, GRUR 2010, 1065-1070.

Köhler, Sebastian: Die Haftung des privaten Internetanschlussinhabers zwischen Haftungsprivilegien und effektiver Rechtsverfolgung, ZUM 2018, 27-33.

Kramer, Andreas: Zivilrechtlicher Auskunftsanspruch gegenüber Access-Providern, Hamburg 2007.

Kremer, Sascha: Datenschutz bei Entwicklung und Nutzung von Apps für Smart Devices, CR 2012, 438-446.

Kreutzer, Till: Anmerkung zu LG Köln, Urteil vom 11.7.2007 – 23 O 263/07 – spickmich, MMR 2007, 732-734.

Kreutzer, Till: Napster, Gnutella & Co.: Rechtsfragen zu Filesharing-Netzen aus der Sicht des deutschen Urheberrechts de lege lata und de lege ferenda – Teil 1, GRUR 2001, 193-204.

Kreutzer, Till: Napster, Gnutella & Co.: Rechtsfragen zu Filesharing-Netzen aus der Sicht des deutschen Urheberrechts de lege lata und de lege ferenda – Teil 2, GRUR 2001, 307-312.

Kring, Markus/Marosi, Johannes: Ein Elefant im Porzellanladen – Der EuGH zu Personenbezug und berechtigtem Interesse, K&R 2016, 773-776.

Krischker, Sven: „Gefällt mir", „Geteilt", „Beleidigt"? – Die Internetbeleidigung in sozialen Netzwerken, JA 2013, 488-493.

Krügel, Tina: Das personenbezogene Datum nach der DS-GVO. Mehr Klarheit und Rechtssicherheit?, ZD 2017, 455-460.

Krüger, Stefan/Macher, Svenja-Ariane: Ist die IP-Adresse wirklich ein personenbezogenes Datum?, MMR 2011, 433-439.

Köhntopp, Marit/Köhntopp, Kristian: Datenspuren im Internet, CR 2000, 248-257.

Kubiciel, Michael/Großmann, Sven: Doxing als Testfall für das Datenschutzstrafrecht, NJW 2019, 1050-1055.

Kugelmann, Dieter: Die Vertraulichkeit journalistischer Kommunikation und das BVerfG, NJW 2003, 1777-1780.

Kuper, Ernst-Stefan: § 101 UrhG: Glücksfall oder Reinfall für Rechteinhaber, ITRB 2009, 12-15.

Kühling, Jürgen: „Fake-News" und „Hate-Speech" – Die Verantwortung der Medienintermediäre zwischen neuen NetzDG, MStV und Digital Services Act, ZUM 2021, 461-472.

Kühling, Jürgen: Im Dauerlicht der Öffentlichkeit – Freifahrt für personenbezogene Bewertungsportale?, NJW 2015, 447-450.

Kühling, Jürgen/Buchner, Benedikt (Hrsg.): Datenschutz-Grundverordnung, Bundesdatenschutzgesetz Kommentar, 3. Auflage, München 2020 (zit.: *Bearbeiter* in: Kühling/Buchner).

Kühling, Jürgen/Klar, Manuel: Anmerkung zu EuGH, Urteil vom 19.10.2016 – C-582/14 – Breyer, ZD 2017, 27-29.

Kühling, Jürgen/Martini, Mario: Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, 448-454.

Kühling, Jürgen/Sauerborn, Cornelius: TTDSG-Kabinettsentwurf und Art. 95 DSGVO. Klärende Neuordnung von Telekommunikations- und Telemediendatenschutz, CR 2021, 271-280.

Kühling, Jürgen/Schall, Tobias: WhatsApp, Skype & Co. – OTT-Kommunikationsdienste im Spiegel des geltenden Telekommunikationsrechts, CR 2015, 641-655.

Kühne, Ulrich: Amicus Curiae. Richterliche Informationsbeschaffung durch Beteiligung Dritter, Tübingen 2015.

Kümmel, Michael: Die Implementierung der Haftung von Host-Providern für Immaterialgüterrechtsverletzungen, Hamburg 2017.

Küster, Christoph: Der Plattformbetreiber als Täter in der urheberrechtlichen Verantwortlichkeit für nutzergesetzte Frames, Berlin 2019.

Lackner, Karl/Kühl, Kristian (Hrsg.): Strafgesetzbuch, Kommentar, 29. Auflage, München 2018 (zit.: *Bearbeiter* in: Lackner/Kühl).

Ladeur, Karl-Heinz/Gostomzyk, Tobias: Das Netzwerkdurchsetzungsgesetz und die Logik der Meinungsfreiheit, K&R 2017, 390-394.

Ladeur, Karl-Heinz/Gostomzyk, Tobias: Der Schutz von Persönlichkeitsrechten gegen Meinungsäußerungen in Blogs, NJW 2012, 710-715.

Lagasnerie, Geoffrey de: Die Kunst der Revolte: Snowden, Assange, Manning, Berlin 2016.

Lampmann, Arno: Anmerkung zur Entscheidung des BGH, Urteil vom 10.12.2020 – I ZR 153/17 – YouTube Drittauskunft II, NJW 2021, 783-784.

Langhoff, Helge: Auskunftsanspruch gegen Internetprovider, ZUM 2006, 457-461.

Lauber-Rönsberg, Anne: Rechtsdurchsetzung bei Persönlichkeitsrechten im Internet – Verantwortlichkeit von Intermediären und Nutzern in Meinungsforen und Personenbewertungsportalen, MMR 2014, 10-14.

Lausen, Matthias: Unmittelbare Verantwortlichkeit des Plattformbetreibers, ZUM 2021, 278-289.

Leicht, Armin: Beweisprobleme bei Urheberrechtsverletzungen von Tauschbörsennutzern in P2P-Netzwerken, VuR 2009, 346-351.

Leistner, Matthias: Der Referentenentwurf zur Umsetzung der DSM-RL und die Theorie vom Sui-generis-Charakter des Art. 17 DSM-RL, ZUM 2020, 897-912.

Leistner, Matthias: Grundlagen und Perspektiven der Haftung für Urheberrechtsverletzungen im Internet, ZUM 2012, 722-740.

Leistner, Matthias/Grisse, Karina: Sperrverfügungen gegen Access-Provider im Rahmen der Störerhaftung (Teil 2), GRUR 2015, 105-115.

Leupold, Andreas/Wiebe, Andreas/Glossner, Silke (Hrsg.): IT-Recht. Recht, Wirtschaft und Technik der digitalen Transformation, 4. Auflage, München 2021 (zit.: *Bearbeiter* in: Handbuch IT-Recht).

Lewinski, Kai von: Staat als Zensurhelfer – Staatliche Flankierung der Löschpflichten Privater nach dem Google-Urteil des EuGH, AfP 2015, 1-6.

Liesching, Marc/Knupfer, Jörg: Verantwortlichkeit von Internetcafe-Betreibern für die Zugangsgewährung zu jugendgefährdenden Inhalten, MMR 2003, 562-570.

Loewenheim, Ulrich/Koch, Frank (Hrsg.): Praxis des Online-Rechts, München 2000 (zit.: *Bearbeiter* in: Loewenheim/Koch)

Lorenz, Bernd: Anonymität im Internet? – Zur Abgrenzung von Diensteanbietern und Nutzern, VuR 2014, 83-90.

Löber, Lena/Roßnagel, Alexander: Das Netzwerkdurchsetzungsgesetz in der Umsetzung. Bilanz nach den ersten Transparenzberichten, MMR 2019, 71-76.

Ludwigs, Markus/Huller, Felix: OTT-Kommunikation: (Noch) Keine TK-Regulierung für Gmail & Co., NVwZ 2019, 1099-1101.

Lutz, Stefan: Verteidigungsstrategien bei Filesharing-Abmahnungen, VuR 2010, 337-346.

Maaßen, Stefan: Urheberrechtlicher Auskunftsanspruch und Vorratsdatenspeicherung, MMR 2009, 511-515.

Mafi-Gudarzi, Nima: Kein Auskunftsrecht über Bestandsdaten bei Beleidigung über Messenger-Dienst. Zugleich Kommentar zu LG Frankfurt a.M., Beschluss vom 30.04.2018 – 2-03 O 430/17, K&R 20018, 420 ff., K&R 2018, 466-467.

Martini, Mario/Zimmermann, Georg von: E-Mail und integrierte VoIP-Services: Telekommunikationsdienste i.S.d. § 3 Nr. 24 TKG?, CR 2007, 427-431.

Maier, Henrike: Meme und Urheberrecht, GRUR-Prax 2016, 397-398.

Mangoldt, Hermann von/Klein, Friedrich/Starck, Christian (Hrsg.): Kommentar zum Grundgesetz: GG, 7. Auflage, München 2018 (zit.: *Bearbeiter* in: Mangoldt/Klein/Starck).

Mantz, Reto: Rechtsfragen offener Netze. Rechtliche Gestaltung und Haftung des Access Providers in zugangsoffenen (Funk-)Netzen, Karlsruhe 2008.

Mantz, Reto: Die Rechtsprechung zum neuen Auskunftsanspruch nach § 101 UrhG, K&R 2009, 21-22.

Mantz, Reto/Spittka, Jan: Anmerkung zu EuGH, Urteil vom 19.10.2016 – C-582/14 – Breyer, NJW 2016, 3582-3583.

Marly, Jochen: Auskunft bei Filesharing – Benutzerkennung, LMK 2018, 403212.

Marnau, Ninja: Anonymisierung, Pseudonymisierung und Transparenz für Big Data, DuD 2016, 428-433.

Maunz, Theodor/Dürig, Günter (Hrsg.): Grundgesetz Kommentar, 95. Auflage, München 2021.

Meckel/Stanoevska-Slabeva (Hrsg.): Web 2.0, Die nächste Generation Internet, Baden-Baden 2008 (zit.: *Bearbeiter* in: Meckel/Stanoevska-Slabeva).

Metzger, Axel/Pravemann, Timm: Der Entwurf des UrhDaG als Umsetzung von Art. 17 DSM-RL – Ein gesetzgebungstechnischer Drahtseilakt, ZUM 2021, 288-299.

Meyer, Julia: Identität und virtuelle Identität natürlicher Personen im Internet, Baden-Baden 2011.

Meyerdierks, Per: Sind IP-Adressen personenbezogene Daten?, MMR 2009, 8-13.

Milkovic, Lilian: Das digitale Zeitalter – Segen oder Fluch für die wissenschaftliche Informationsversorgung?, Berlin 2008.

Milstein, Alexander: Weder Verantwortlichkeit noch „Pflicht zu Vergessen" von Suchmaschinenbetreibern nach EU-Datenschutzrecht, K&R 2013, 446-448.

Moench, Oliver: Neue Begriffsbestimmung für regulierte Telekommunikationsdienste, NVwZ 2021, 1652-1657.

Moos, Flemming: Die Entwicklung des Datenschutzrechts im Jahr 2008, K&R 2009, 154-161.

Moos, Flemming/Rothkegel, Tobias: Anmerkung zu EuGH, Urteil vom 19.10.2016 – C-582/14 – Breyer, MMR 2016, 845-847.

Morgenstern, Holger: Zuverlässigkeit von IP-Adressen-Ermittlungssoftware, CR 2011, 203-208.

Möhring, Philipp/Nicolini, Käte (Hrsg.): Urheberrecht, 4. Auflage, München 2018 (zit.: *Bearbeiter* in: Möhring/Nicolini).

Musielak, Hans-Joachim/Voit, Wolfgang (Hrsg.): Zivilprozessordnung mit Gerichtsverfassungsgesetz, Kommentar, 19. Auflage, München 2022 (zit.: *Bearbeiter* in: Musielak/Voit).

Musiol, Christian: Erste Erfahrungen mit der Anwendung des § 101 IX UrhG – wann erreicht die Verletzung ein „gewerbliches Ausmaß"?, GRUR-RR 2009, 1-4.

Muthorst, Olaf: Das Beweisverbot. Grundlegung und Konkretisierung rechtlicher Grenzen der Beweiserhebung und der Beweisverwertung im Zivil-, Straf- und Verwaltungsverfahren, Tübingen 2009.

Müller-Terpitz, Ralf: Filter als Gefahr für die Meinungspluralität? – Verfassungsrechtliche Erwägungen zum Einsatz von Filtertechnologien, ZUM 2020, 365-374.

Münchener Anwaltshandbuch IT-Recht: Leupold, Andreas/Braun, Jens-Daniel (Hrsg.), 3. Auflage, München 2013 (zit.: *Bearbeiter* in: Münchener Anwaltshandbuch IT-Recht).

Münchener Kommentar zum Bürgerlichen Gesetzbuch: Habersack, Mathias (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 3, 6. Auflage, München 2022 (zit.: *Bearbeiter* in: MüKo BGB).

Münchener Kommentar zum Bürgerlichen Gesetzbuch: Habersack, Mathias (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, Schuldrecht – Besonderer Teil IV, Band 7, 8. Auflage, München 2020 (zit.: *Bearbeiter* in: MüKo BGB).

Münchener Kommentar zur Zivilprozessordnung: Krüger, Wolfgang/Rauscher, Thomas (Hrsg.), Münchener Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz und Nebengesetzen, Band 7, 8. Auflage, München 2020 (zit.: *Bearbeiter* in: MüKo ZPO).

Nägele, Thomas/Nitsche, Christina: Gesetzesentwurf der Bundesregierung zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums, WRP 2007, 1047-1058.

Neuner, Jörg: Das BVerfG im Labyrinth der Drittwirkung, NJW 2020, 1851-1855.

Nicolai, Michael: Rechtssicherheit für WLAN-Anbieter: Neuer Versuch im 3. TMGÄndG, ZUM 2018, 33-43.

Nietsch, Thomas: Anonymität und die Durchsetzung urheberrechtlicher Ansprüche im Internet. Grundrechtliche Positionen im Spannungsfeld, Tübingen 2014.

Nietsch, Thomas: Zur Ermittlung dynamischer IP-Adressen durch Drittunternehmen. Zugleich Kommentar zu OLG Hamburg, Beschluss vom 3.11.2010 – 5 W 126/10, K&R 2010, 54, K&R 2011, 101-103.

Nolte, Georg: Hate-Speech, Fake-News, das „Netzwerkdurchsetzungsgesetz" und Vielfaltsicherung durch Suchmaschinen, ZUM 2017, 552-565.

Nolte, Georg: Drei Thesen zur aktuellen Debatte über Haftung und Verteilungsgerechtigkeit bei Hosting-Diensten mit nutzergenerierten Inhalten (sog. „Value-Gap"-Debatte), ZUM 2021, 304-312.

Nolte, Georg/Wimmers, Jörg: Wer stört? Gedanken zur Haftung von Intermediären im Internet – von praktischer Konkordanz, richtigen Anreizen und offenen Fragen, GRUR 2014, 16-27.

Nomos Kommentar BGB: Hüßtege, Rainer/Mansel, Heinz-Peter (Hrsg.), Band 6: Rom-Verordnungen, 3. Auflage, Bade-Baden 2019 (zit.: *Bearbeiter* in: NK-BGB VI).

Nordemann, Jan: Neues zur Providerhaftung im Urheberrecht. Registrare, CDN- und DNS-Provider und ihre strukturell rechtsverletzenden Kunden, GRUR 2021, 18-23.

Ohly, Ansgar: Von der Störerhaftung zur Haftung für die Verletzung urheberrechtlicher Verkehrspflichten, NJW 2022, 2961-2963.

Ohly, Ansgar: Der weite Täterbegriff des EuGH in den Urteilen „GS Media", „Filmspeler" und „The Pirate Bay": Abenddämmerung für die Störerhaftung?, ZUM 2017, 793-802.

Ohly, Ansgar: Die Verantwortlichkeit von Intermediären, ZUM 2015, 308-318.

Ohly, Ansgar: Verändert das Internet unsere Vorstellung von Persönlichkeit und Persönlichkeitsrecht?, AfP 2011, 428-438.

Oster, Jan: Internationale Zuständigkeit und anwendbares Recht im Datenschutz, ZEuP 2021, 275-306.

Oster, Jan: Voice over IP: Erscheinungsformen und ihre regulierungsrechtliche Behandlung, CR 2007, 769-773.

Paschke, Anne/Halder, Christoph: Auskunftsansprüche bei digitalen Persönlichkeitsrechtsverletzungen, MMR 2016, 723-727.

Paschold, Florian: Unionsrechtskonformität der Rechtsprechung des BGH zur sekundären Darlegungslast des Anschlussinhabers im Rahmen von Filesharing-Fällen mit Familienbezug nach der Entscheidung Afterlife, GRUR Int. 2018, 621-636.

Peukert, Alexander/Kur, Annette: Stellungnahme des Max-Planck-Instituts für Geistiges Eigentum, Wettbewerbs- und Steuerrecht zur Umsetzung der Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums in deutsches Recht, GRUR Int. 2006, 292-303.

Pfeifer, Karl-Nikolaus: Verpflichtung zur Löschung wort-/sinngleicher Äußerungen ist keine durch Art. 15 E-Commerce-Richtlinie verbotene allgemeine Überwachung, GRUR-Prax 2019, 534.

Pfeifer, Karl-Nikolaus: Urheberrechtliche Zulässigkeit der Weiterverwertung von im Internet abrufbaren Fotos. Einmal im Netz – für immer frei?, NJW 2018, 3490-3493.

Pfeifer, Karl-Nikolaus: Fake News und Providerhaftung. Warum das NetzDG zur Abwehr von Fake News die falschen Instrumente liefert, CR 2017, 809-813.

Pfeifer, Karl-Nikolaus: Die zivilrechtliche Verteidigung gegen Äußerungen im Internet, AfP 2015, 193-201.

Pfitzmann, Andreas/Köpsell, Stefan/Kriegelstein, Thomas: Sperrverfügungen gegen Access-Provider, Technisches Gutachten vom 22.12.2006, Online abrufbar und zitiert nach https://gluecksspiel.uni-hohenheim.de/fileadmin/einrichtungen/glueckspiel/Regulierung/20080428_technisches_Gutachten_SperrvervSperrver.pdf (Stand: 24.05.2022).

Pfitzmann, Birgit/Waidner, Michael/Pfitzmann, Andreas: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen, Teil 1, DuD 1990, 243-253.

Pille, Jens-Ulrich: Der Grundsatz der Eigenverantwortlichkeit im Internet, NJW 2018, 3545-3550.

Piltz, Carlo: Das neue TTDSG aus Sicht der Telemedien. Anwendungsbereich, Tracking und Aufsichtsbehörden, CR 2021, 555-565.

Plath, Kai-Uwe (Hrsg.): BDSG/DSGVO. Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen des TMG und TKG, 3. Auflage 2018, Köln 2018 (zit.: *Bearbeiter* in: Plath).

Prinz, Matthias: Anmerkung zur Entscheidung des BGH, Beschluss vom 24.9.2019 (VI ZB 39/18) – Zum Auskunftsanspruch gegen ein soziales Netzwerk zu Nutzerkonten mit beleidigendem Inhalt, K&R 2020, 69-71.

Raabe, Franziska: Der Auskunftsanspruch nach dem Referentenentwurf zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums, ZUM 2006, 439-444.

Rau, Marco/Behrens, Martin: Catch me if you can ... Anonymisierungsdienste und die Haftung für mittelbare Rechtsverletzungen, K&R 2009, 766-771.

Raue, Benjamin: Meinungsfreiheit in sozialen Netzwerken. Ansprüche von Nutzern sozialer Netzwerke gegen die Löschung ihrer Beiträge, JZ 2018, 961-970.

Raue, Benjamin/Steinebach, Martin: Uploadfilter – Funktionsweisen, Einsatzmöglichkeiten und Parametrisierung, ZUM 2020, 355-364.

Rauer, Nils/Bibi, Alexander: Das neue Urheberrechts-Diensteanbietergesetz, BB 2021, 1475-1480.

Rauer, Nils/Bibi, Alexander: Die fortentwickelte Intermediärshaftung im Urheberrecht, ZUM 2021, 819-828.

Redaktion MMR-Aktuell: BMJV Bußgeldverfahren gegen den Messenger-Dienst Telegram wegen Verstoß gegen NetzDG eingeleitet, MMR-Aktuell 2021, 440252.

Redeker, Helmut: IT-Recht, 7. Auflage, München 2020.

Reinbacher, Tobias: Die „Weiterverbreitung" von Hate Speech in sozialen Medien – Fragen der Beteiligung an einer gemäß § 185 StGB strafbaren Beleidigung, JZ 2020, 558-563.

Richter, Christoph/Geschke, Daniel/Klaßen, Anja: Hass im Internet. Wie Hate Speech die Meinungsbildung junger Menschen bedroht, ZJJ 2020, 148-157.

Rohlfing, Stephanie: Die Umsetzung der Enforcement-Richtlinie ins deutsche Recht, Hamburg 2009.

Roßnagel, Alexander/Kroschwald, Steffen: Was wird aus der Datenschutzgrundverordnung?, ZD 2014, 495-500.

Roßnagel, Alexander/Schnabel, Christoph: Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, 3534-3538.

Roßnagel, Alexander/ Scholz, Philip: Datenschutz durch Anonymität und Pseudonymität. Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721-731.

Röhl, Christoph/Bosch, Andreas: Musiktauschbörsen im Internet, NJW 2008, 1415-1420.

Röß, Simon: Die Haftung der WLAN-Betreiber bei illegalem Filesharing, GRUR 2021, 823-828.

Rupp, Susanne: Die Beweisführung mit privaten elektronischen Dokumenten, Baden-Baden 2018.

Sachs, Michael (Hrsg.): Grundgesetz Kommentar, 9. Auflage, München 2021 (zit.: *Bearbeiter* in: Sachs).

Sachs, Michael/Krings, Thomas: Das neue Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, JuS 2008, 481-486.

Sachs, Ulrich: Datenschutzrechtliche Bestimmbarkeit von IP-Adressen, CR 2010, 547-552.

Sahl, Christian/Bielzer, Nils: NetzDG 2.0 – Ein Update für weniger Hass im Netz, ZRP 2020, 2-5.

Sandor, Rene: Datenspeicherung und urheberrechtliche Durchsetzungsansprüche, Köln 2012.

Sankol, Barry: Akteneinsichtsgesuche nach § 406e StPO in Filesharing-Verfahren, K&R 2008, 509-513.

Schaar, Peter: Datenschutz im Internet, München 2002.

Schantz, Peter: Die Datenschutzgrundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841-1847.

Schaub, Renate: Sekundäre Darlegungslast und Interessensabwägung beim Filesharing über den Familienanschluss, NJW 2018, 17-19.

Scheuerle, Klaus-Dieter/Mayen, Thomas (Hrsg.): TKG: Telekommunikationsgesetz, Kommentar, 3. Auflage, München 2018 (zit.: *Bearbeiter* in: Scheuerle/Mayen).

Schiff, Alexander: Informationsintermediäre. Verantwortung und Haftung, Tübingen 2021.

Schmidt, Heiner: Anmerkungen zur Diskussion um die Beschränkung des Akteneinsichtsrechts in den Filesharingverfahren, GRUR 2010, 673-677.

Schmitz, Peter: E-Privacy-VO – unzureichende Regeln für klassische Dienste, ZRP 2017, 172-175.

Schmidt, Ramona: Äußerungsrechtlicher Schutz gegenüber Bewertungsportalen im Internet, Baden-Baden 2015.

Schneider, Mathias: WhatsApp & Co. – Dilemma um anwendbare Datenschutzregeln. Problemstellung und Regelungsbedarf bei Smartphone-Messengern, ZD 2014, 231-237.

Schlegel, Ralf: Auskunftspflichten von Internet-Service-Providern, CR 2005, 144-145.

Schoch, Friedrich: Der verfassungsrechtliche Schutz des Fernmeldegeheimnisses (Art. 10 GG), Jura 2011, 194-204.

Schramm, Marc/Shvets, Iryna: Umgang mit TK-Kundendaten nach Inkrafttreten der DS-GVO. Der TK-Kunde als besonderer Vertragspartner i.S.d. Datenschutzrechts?, MMR 2019, 228-233.

Schricker, Gerhard/Loewenheim, Ulrich (Hrsg.): Urheberrecht Kommentar, 6. Auflage, München 2020 (zit.: *Bearbeiter* in: Schricker/Loewenheim).

Schwartmann, Rolf: Die BGH-Entscheidung zur Facebook-Klarnamenpflicht läuft leer, ZD 2022, 133-134.

Schwartmann, Rolf/Hentsch, Christian-Henner: Stufenkonzept gegen Overblocking durch Upload-Filter, MMR 2020, 207-213.

Schwartmann, Rolf/Jaspers, Andreas/Thüsing, Gregor/Kugelmann, Dieter (Hrsg.): DS-GVO/BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Auflage, Heidelberg 2020 (zit.: *Bearbeiter* in: Schwartmann/Jaspers/Thüsing/Kugelmann).

Schwarz, Mathias/Brauneck, Anja: Verbesserung des Rechtsschutzes gegen Raubkopierer auf der Grundlage der EU-Enforcemennt-Richtlinie und deren Umsetzung in deutsches Recht, ZUM 2006, 701-713.

Seichter, Dirk: Die Umsetzung der Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums, WRP 2006, 391-400.

Senftleben, Martin: Filterverpflichtungen nach der Reform des europäischen Urheberrechts – Das Ende der freien Netzkultur?, ZUM 2019, 369-374.

Sesing, Andreas: Eine Bestandsaufnahme zum bereichsspezifischen Datenschutz für Telemedien, MMR 2019, 347-350.

Sesing, Andreas: Die Reichweite des Richtervorbehalts für urheberrechtliche Auskunftsansprüche gegen Access-Provider, NJW 2018, 754-756.

Sieber, Ulrich/Nolde, Malaika: Sperrverfügungen im Internet. Nationale Rechtsdurchsetzung im globalen Cyberspace?, Berlin 2008.

Siebert, Melanie: Geheimnisschutz und Auskunftsansprüche im Recht des Geistigen Eigentums, Tübingen 2011.

Sievers, Malte: Der Schutz der Kommunikation im Internet durch Art. 10 des Grundgesetzes, Baden-Baden 2003.

Simitis, Spiros/Hornung, Gerrit/Spiecker, Indra (Hrsg.): Datenschutzrecht Kommentar, DSGVO mit BDSG, Baden-Baden 2019 (zit.: *Bearbeiter* in: Simitis/Hornung/Spiecker).

Solmecke, Christian: Rechtliche Beurteilung der Nutzung von Musiktauschbörsen, K&R 2007, 138-143.

Solmecke, Christian/Bärenfänger, Jan: Urheberrechtliche Schutzfähigkeit von Dateifragmenten - Nutzlos = Schutzlos?, MMR 2011, 567-573.

Solmecke, Christian/Dam, Annika: Anmerkung zu EuGH, Urteil vom 05.06.2014 – C-360/13 – Public Relations Consultants Association, MMR 2014, 544-545.

Solmecke, Christian/Dierking, Laura: Die Rechtsmissbräuchlichkeit von Abmahnungen, MMR 2009, 727-730.

Sorge, Christoph: Zum Stand der Technik in der WLAN-Sicherheit, CR 2011, 273-276.

Spindler, Gerald: Haftung für Urheberrechtsverstöße auf Online-Plattformen – YouTube Reloaded, NJW 2021, 2554-2556.

Spindler, Gerald: Die Umsetzung von Art. 17 DSM-Richtlinie in deutsches Recht – Das UrhDaG (Teil 2), WRP 2021, 1245-1251.

Spindler, Gerald: Der Vorschlag für ein neues Haftungsregime für Internetprovider – der EU Digital Services Act (Teil 1), GRUR 2021, 545-553.

Spindler, Gerald: Der Vorschlag für ein neues Haftungsregime für Internetprovider – der EU Digital Services Act, Teil 2: Große und besonders große Plattformen, GRUR 2021, 653-662.

Spindler, Gerald: Art. 17 DSM-RL und dessen Vereinbarkeit mit primärem Europarecht. Zugleich ein Beitrag zu Umsetzungsmöglichkeiten, GRUR 2020, 253-261.

Spindler, Gerald: Neues zu (internationalen) Bewertungsportalen – Zugleich Anmerkung zu BGH, Urteile vom 14.1.2020 – VI ZR 459/18 (ZUM 2020, 331), VI ZR 496/18 (ZUM-RD 2020, 181) und VI ZR 497/18 (ZUM-RD 2020, 186), ZUM 2020, 433-440.

Spindler, Gerald: Weltweite Löschungspflichten bei Persönlichkeitsrechtsverletzungen im Internet, NJW 2019, 3274-3277.

Spindler, Gerald: Löschung und Sperrung von Inhalten aufgrund von Teilnahmebedingungen sozialer Netzwerke. Eine Untersuchung der zivil- und verfassungsrechtlichen Grundlagen, CR 2019, 238-247.

Spindler, Gerald: Die neue Urheberrechts-Richtlinie der EU, insbesondere „Upload-Filter" – Bittersweet?, CR 2019, 277-291.

Spindler, Gerald: Haftung ohne Ende?. Über Stand und Zukunft der Haftung von Providern, MMR 2018, 48-52.

Spindler, Gerald: Störerhaftung für Access-Provider reloaded, GRUR 2018,1012-1016.

Spindler, Gerald: Rechtsdurchsetzung von Persönlichkeitsrechten. Bußgelder gegen Provider als Enforcement?, GRUR 2018, 365-373.

Spindler, Gerald: Das neue Telemediengesetz – WLAN-Störerhaftung endgültig ade?, NJW 2017, 2305-2309.

Spindler, Gerald: Der Regierungsentwurf zum Netzwerkdurchsetzungsgesetz – europarechtswidrig?, ZUM 2017, 473-487.

Spindler, Gerald: Sperrverfügungen gegen Access-Provider – Klarheit aus Karlsruhe?, GRUR 2016, 451-460.

Spindler, Gerald: Der Auskunftsanspruch gegen Verletzer und Dritte im Urheberrecht nach neuem Recht, ZUM 2008, 640-648.

Spindler, Gerald: „Die Tür ist auf" – Europarechtliche Zulässigkeit von Auskunftsansprüchen gegenüber Providern. Urteilsanmerkung zu EuGH „Promusicae/Telefonica", GRUR 2008, 574-577.

Spindler, Gerald/Dorschel, Joachim: Vereinbarkeit der geplanten Auskunftsansprüche gegen Internet- Provider mit EU-Recht, CR 2006, 341-347.

Spindler, Gerald/Dorschel, Joachim: Auskunftsansprüche gegen Internet-Service-Provider. Zivilrechtliche Grundlagen und datenschutzrechtliche Grenzen, CR 2005, 38-47.

Spindler, Gerald/Klöhn, Lars: Neue Qualifikationsprobleme im E-Commerce. Verträge über die Verschaffung digitalisierter Informationen als Kaufvertrag, Wervertrag, Verbrauchsgüterkauf?, CR 2003, 81-86.

Spindler, Gerald/Schmitz, Peter (Hrsg.): Telemediengesetz mit Netzwerkdurchsetzungsgesetz Kommentar, 2. Auflage, München 2018 (zit.: *Bearbeiter* in: Spindler/Schmitz).

Spindler, Gerald/Schuster, Fabian (Hrsg.): Recht der elektronischen Medien, Kommentar, 4. Auflage, München 2019 (zit.: *Bearbeiter* in: Spindler/Schuster).

Splittgerber, Andreas/Klytta, Johanna: Auskunftsansprüche gegen Internetprovider, K&R 2007, 78-85.

Steinbrecher, Judith: Die EU-Urheberrechtsrichtlinie aus Sicht der Digitalwirtschaft. Zeit für Augenmaß und faktenbasierte Gesetzgebung, MMR 2019, 639-643.

Stieper, Malte: Die Umsetzung von Art. 17 VII DSM-RL in deutsches Recht (Teil 2). Entwurf einer Schranke für Karrikaturen, Parodien und Pastiches, GRUR 2020, 792-797.

Stern, Klaus: Das Staatsrecht der Bundesrepublik Deutschland, Band III/1, München 1988.

Stern, Klaus/Becker, Florian (Hrsg.): Grundrechte-Kommentar, 3. Auflage, Köln 2018 (zit.: *Bearbeiter* in: Stern/Becker).

Stumpf, Felix: Das Recht auf Vergessenwerden. Das Google-Urteil des EuGH – Vorbote der zweiten Chance im digitalen Zeitalter oder Ende der freien Kommunikation im Internet?, Baden-Baden 2017.

Stuve, Johannes: Haftung für Werbung auf urheberrechtsverletzenden Websites, Berlin 2021.

Suwelack, Felix: Leistungsschutzrecht und Upload-Filter aus ökonomischer Perspektive. Werden die Reform-Vorschläge der EU-Kommission ihrem eigenen Legitimationsmodell gerecht?, MMR 2018, 582-586.

Sydow, Gernot (Hrsg.): Europäische Datenschutzgrundverordnung, 2. Auflage, Baden-Baden 2018 (zit.: *Bearbeiter* in: Sydow).

Taeger, Jürgen/Gabel, Detlev (Hrsg.): DSGVO – BDSG – TTDSG, Kommentar, 4. Auflage, Frankfurt am Main 2022 (zit.: *Bearbeiter* in: Taeger/Gabel).

Tanenbaum, Andrew: Computernetzwerke, 4. Auflage, München 2004.

Thiel, Thorsten: Anonymität und Strukturwandel der Öffentlichkeit, zfmr 1/2016, S. 9-24.

Thiesen, Michael: Wie hoch ist der Preis der Anonymität. Haftungsrisiken beim Betrieb eines TOR-Servers, MMR 2014, 803-809.

Thome, Philipp: Sperrverfügungen gegen Internet Service Provider, Baden-Baden 2021.

Tief, Samira: Kommunikation aus Facebook, Twitter & YouTube, Berlin 2020.

Tödtmann, Ulrich/Erdmann, Charlotte von: Keine Pflicht zur Selbstbelastung für den Arbeitnehmer?, NZA 2020, 1577-1583.

Tschorr, Sophie: Soziale Netzwerke als Akteure für ein „besseres" Internet?, MMR 2021, 204-208.

Tyra, Frank: Ausgewählte Probleme aus der Abmahnpraxis bei Privatnutzungen in Musiktauschsystemen, ZUM 2019, 934-944.

Ungern-Sternberg, Joachim von: Die Rechtsprechung des EuGH und BGH zum Urheberrecht und zu den verwandten Schutzrechten im Jahr 2020, GRUR 2021, 1-18.

Ungern-Sternberg, Joachim von: Die Rechtsprechung des EuGH und BGH zum Urheberrecht und zu den verwandten Schutzrechten im Jahr 2017, GRUR 2018, 225-241.

Vassilaki, Irini: Bestrafung der Verbreitung von Feindeslisten im Internet – (k)ein Schutz personenbezogener Daten?, K&R 2021, 763-766.

Valerius, Brian: Hasskriminalität – Vergleichende Analyse unter Einschluss der deutschen Rechtslage, ZStW 132 (2020), 666-689.

Verheijden, Josina: Rechtsverletzungen auf YouTube und Facebook, Hamburg 2015.

Vonau, Eva: E-Mail-Adresse, IP-Adresse und Telefonnummer sind keine „Adresse", GRUR-Prax 2021, 59.

Wagner, Gerhard: Haftung von Plattformen für Rechtsverletzungen (Teil 1), GRUR 2020, 329-338.

Wagner, Gerhard: Haftung von Plattformen für Rechtsverletzungen (Teil 2), GRUR 2020, 447-457.

Waiblinger, Julian/Pukas, Jonathan: Die urheberrechtliche Haftung von Online-Plattformen nach dem Urheberrechts-Diensteanbieter-Gesetz (UrhDaG), MDR 2021, 1489-1496.

Wandtke, Axel-Artur: Persönlichkeitsschutz versus Internet. Politiker und Prominente im Fadenkreuz der Persönlichkeitsrechte, MMR 2019, 142-147.

Wandtke, Axel-Artur/Bullinger, Winfried (Hrsg.): Praxiskommentar Urheberrecht, 5. Auflage, München 2019 (zit.: *Bearbeiter* in: Wandtke/Bullinger).

Wandtke, Axel-Artur/Hauck, Ronny: Verantwortlichkeit und Haftung – Das Urheberrechts-Diensteanbieter-Gesetz im Kontext des allgemeinen Urheberrechts, ZUM 2021, 763-775.

Wandtke, Axel-Artur/Hauck, Ronny: Ein neues Haftungssystem im Urheberrecht – Zur Umsetzung von Art. 17 DSM-RL in einem „Urheberrechts-Diensteanbieter-Gesetz, ZUM 2020, 671-681.

Wandtke, Axel-Artur/Hauck, Ronny: Art. 17 DSM-RL - Ein neues Haftungssystem im Urheberrecht, ZUM 2019, 627-636.

Wandtke, Artur/Ostendorff, Saskia: Grenzen der Meinungsfreiheit bei Hassreden aus straf- und persönlichkeitsrechtlicher Sicht, ZUM 2021, 26-35.

Weber, Marc: Die Umsetzung der Enforcement-Richtlinie ins deutsche Recht. Unter besonderer Berücksichtigung der Umsetzung des Art. 7 RL, Frankfurt am Main 2010.

Wegener, Christoph/Heidrich, Joerg: Neuer Standard – Neue Herausforderungen: IPv6 und Datenschutz, CR 2011, 479-484.

Wehr, Christina/Ujica, Matei: „Alles muss raus" – Datenspeicherungs- und Auskunftspflichten der Access-Provider nach dem Urteil des BVerfG zur Vorratsdatenspeicherung, MMR 2010, 667-671.

Weiden, Henrike: Aktuelle Berichte – April 2019, GRUR 2019, 370-372.

Weidert, Stefan/Uhlenhut, Theresa/Lintig, Johannes: Kampf gegen Upload-Filter – Teil 2: Die neue Urheberrechtsrichtlinie, GRUR-Prax 2019, 295-297.

Welp, Kai: Die Auskunftspflicht von Access-Providern nach dem Urheberrechtsgesetz, München 2009.

Welser, Marcus von: Plattformhaftung nach dem Urheberrechts-Diensteanbieter-Gesetz (UrhDaG), GRUR-Prax 2021, 463-466.

Wiebe, Andreas: Enforcement-RL – Rechtsdurchsetzung nach der Richtlinie 2004/48/EG, in: Büllesbach, Alfred/Büchner, Wolfgang (Hrsg.), It doesn´t matter!?. Aktuelle Herausforderungen des Technikrechts, Köln 2006, S. 153-178.

Wiese, Günther: Bewertungsportale und allgemeines Persönlichkeitsrecht, JZ 2011, 608-617.

Wick, Gottlieb Rafael: Inhalt und Grenzen des Auskunftsanspruchs gegen Zugangsanbieter, Bonn 2010.

Wilhelmi, Rüdiger: Das gewerbliche Ausmaß als Voraussetzung der Auskunftsansprüche nach dem Durchsetzungsgesetz, ZUM 2008, 942-950.

Wollweber, Harald: Verbindungsdaten der Telekommunikation im Visier der Strafverfolgungsbehörden, NJW 2002, 1554-1556.

Ziegenhorn, Gero: Anmerkung zu EuGH, Urteil vom 19.10.2016 – C-582/14 – Breyer, NVwZ 2017, 216-218.

Ziegler, Katharina: Urheberrechtsverletzungen durch Social Sharing, Tübingen 2016.

Zimmermann, Johannes: Die unbeachtete Zweistufigkeit von Providerauskünften in Filesharingfällen, K&R 2015, 73-76.

Zombik, Peter: Der Kampf gegen Musikdiebstahl im Internet, ZUM 2006, 450.

digital | recht

Schriften zum Immaterialgüter-, IT-,
Medien-, Daten- und Wettbewerbsrecht

Martina Kasch

Auskunftsansprüche gegen Diensteanbieter der Informationsgesellschaft

Nutzer, die im Internet die Rechte anderer verletzen, sind ein verbreitetes Phänomen. Oft können Rechteinhaber wegen der Anonymität der Nutzer keine Ansprüche gegen diese durchsetzen. Die Arbeit beschäftigt sich mit den Möglichkeiten einer Identifizierung durch Auskunft von Internetdiensteanbietern.