Eingriffe in den Internet-Datenverkehr zur Durchsetzung des Urheberrechts. Zur Vereinbarkeit von Netzsperren und Deep Packet Inspection mit europäischen und deutschen Grundrechten

DISSERTATION

zur Erlangung des akademischen Grades Doctor iuris

(Dr. iur.)

Eingereicht am 23.10.2020

an der Juristischen Fakultät der Humboldt-Universität zu Berlin

von

Martin Fokken

Präsidentin: der Humboldt-Universität zu Berlin

Prof. Dr.-Ing. Dr. Sabine Kunst

Dekanin/Dekan der Juristischen Fakultät der Humboldt-Universität zu Berlin:

Prof. Dr. Dr. Stefan Grundmann, LL.M. (Berkeley)

Gutachter/innen:

1. Prof. Dr. Eva Inés Obergfell

2. Prof. Dr. Ronny Hauck

Tag der Disputation: 29.04.2021

Zusammenfassung

Die auf mitgliedstaatlicher und EU-Ebene grundrechtlich verbürgte Freiheit des Eigentums verlangt, das Urheberrecht effektiv zu schützen. Staatlich durchgeführte oder angeordnete technische Maßnahmen wie Netzsperren (IP- oder DNS-Sperren) und Deep Packet Inspection ermöglichen es u.a., gezielt die Übertragung von Daten zu blockieren, deren unlizenzierter Austausch über das Internet – etwa über Streaming-Portale – das Urheberrecht verletzt. Im Internet besteht ohne derartige technische Maßnahmen ein Durchsetzungsdefizit, da die unmittelbaren („Content Provider“) und mittelbaren Anbieter („Host-Provider“) der Inhalte oft nicht effektiv in Haftung genommen werden können; die technischen Betreiber der Infrastruktur des Internets („Internet Service Provider“) hingegen können dem staatlichen Zugriff nicht ausweichen. Die angesprochenen technischen Maßnahmen greifen jedoch in verschiedene Grundrechte des Grundgesetzes und der Charta der Grundrechte der Europäischen Union ein. Betroffen sind insbesondere die unternehmerische Freiheit (Art. 16 Charta) der Internet Service Provider, die Informationsfreiheit (Art. 11 Abs. 1 Charta), das Recht auf Achtung der Kommunikation (Art. 7 Charta), das Recht auf Schutz personenbezogener Daten (Art. 8 Abs. 1 Charta) der Internet-Nutzer sowie die jeweiligen mitgliedstaatlichen Entsprechungen dieser Grundrechte. Der Gegenstand dieser Arbeit ist die Untersuchung der Vereinbarkeit der Anwendung technischer Maßnahmen zur Durchsetzung des Urheberrechts mit europäischem Primärrecht und dem Grundgesetz.

Abstract

The Fundamental Right to Property, which is guaranteed at Member State and EU level, requires that copyright be effectively protected. Technical measures implemented by or required by states, such as IP/DNS blocking or Deep Packet Inspection, enable, inter alia, the targeted blocking of transmissions of data whose unlicensed exchange over the internet – e.g. via streaming portals – infringes copyrights. Without such technical measures, there is an enforcement deficit in the internet, as the direct ("content providers") and indirect providers ("host providers") of the content often cannot be effectively held liable; the technical operators of internet infrastructure ("internet service providers"), on the other hand, cannot evade governmental intervention. The technical measures mentioned, however, affect various fundamental rights of the German Constitution (the “Grundgesetz”) and the Charter of Fundamental Rights of the European Union. The rights affected are, in particular, the Freedom to Conduct a Business (Article 16 of the Charter) of internet service providers, the Freedom of Information (Article 11(1) of the Charter), the Right to Respect for Communications (Article 7 of the Charter) and the Right to Protection of Personal Data (Article 8 (1) of the Charter) of internet users, and the respective Member State equivalents of these fundamental rights. Subject matter of this thesis is to examine whether the use of technological measures to enforce copyrights is in compliance with European primary law and the German Grundgesetz.

Inhaltsverzeichnis

Abkürzungsverzeichnis

a.A.	andere Ansicht
aaO	am angegebenen Ort
ABl.	Amtsblatt
Abs.	Absatz
Abschn.	Abschnitt
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AfP	Zeitschrift für das gesamte Medienrecht
AG	Amtsgericht
Alt.	Alternative
Art.	Artikel
Aufl.	Auflage
BB	Betriebs-Berater
Bd.	Band
BDSG	Bundesdatenschutzgesetz
BeckOK	Beck'scher Onlinekommentar
BEREC	Body of European Regulators for Electronic Communications
Beschl.	Beschluss
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BND	Bundesnachrichtendienst
BRD	Bundesrepublik Deutschland
BT-Drs.	Bundestag-Drucksache
BVerfG	Bundesfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts (Zeitschrift)
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts (Zeitschrift)
Charta	Charta der Grundrechte der Europäischen Union
CLSR	Computer Law & Security Review
Comput. Commun. Rev.	Computer Communication Review
CR	Computer und Recht
DuD	Zeitschrift Datenschutz und Datensicherheit
ders.	derselbe
d.h.	das heißt
DENIC	Deutsches Network Information Center
Diss.	Dissertation
DNS	Domain Name System
DoS	Denial-of-Service
DPI	Deep Packet Inspection
DSGVO	Datenschutz-Grundverordnung
DVR	Datenverkehrsregulierung
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
Erg.-Lfg.	Ergänzungslieferung
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
EuR	Zeitschrift Europarecht
EUR	Euro
EURATOM	Europäische Atomgemeinschaft

EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EWHC	High Court of England and Wales
EWiR	Entscheidungen zum Wirtschaftsrecht
EWR	Europäischer Wirtschaftraum
Ext.	Extended
f.	„auf der folgenden Seite“
FCC	Federal Communications Commission
ff.	„auf den folgenden Seiten“
Fn.	Fußnote
fortgef.	fortgeführt
FTP	File Transfer Protocol
FU Berlin	Freie Universität Berlin
GA	Generalanwalt / Generalanwältin
GG	Grundgesetz
ggf.	gegebenenfalls
GlStV	Glücksspielstaatsvertrag
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GRUR-Beil.	Gewerblicher Rechtsschutz und Urheberrecht Beilage
GRUR Int.	Gewerblicher Rechtsschutz und Urheberrecht International
GRUR-Prax	Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter- und Wettbewerbsrecht
Habil.	Habilitation
h.M.	herrschende Meinung
Hrsg.	Herausgeber
HS.	Halbsatz
HStR	Handbuch des Staatsrechts
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HU Berlin	Humboldt-Universität zu Berlin
HUDOC	„Human Rights Documentation“ – Datenbank aller Entscheidungen des EGMR
i.E.	im Ergebnis
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
IANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical and Electronics Engineers
IEEE Globecom	IEEE Global Communications Conference
IEEE Network	IEEE Network: The Magazine of Global Internetworking
IEEP	International Economics and Economic Policy
IETF	Internet Engineering Task Force
IJCLP	International Journal of Communications Law and Policy
IJIO	International Journal of Industrial Organization
IJLIT	International Journal of Law and Information Technology
IMAP	Internet Message Access Protocol (urprünglich: Interactive Mail Access Protocol)
InfoSoc-Richtlinie	Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft
IP	Internet Protocol
IP-TV	Internet Protocol Television
IPv4	Internet Protocol version 4

ISP	Internet Service Provider
IT	Informationstechnik
JASA	Journal of the American Statistical Association
J. Comput. Graph. Stat.	Journal of Computational and Graphical Statistics
J. Netw. Syst. Manag.	Journal of Network and Systems Management
JTHTL	Journal on Telecommunications & High Technology Law
JURA	Juristische Ausbildung
jurisPR-ITR	juris PraxisReport IT-Recht
JuS	Juristische Schulung
JZ	JuristenZeitung
K&R	Kommunikation & Recht
Kap.	Kapitel
KFZ	Kraftfahrzeug
KJM	Kommission für Jugendmedienschutz
LAN	Local Area Network
LG	Landgericht
lit.	Buchstabe
m.w.N.	mit weiteren Nachweisen
MByte	Megabyte
Mio.	Million(en)
MMR	MultiMedia und Recht
MMR-Beil.	MultiMedia und Recht Beilage
MPI	Medium Packet Inspection
Mrd.	Milliarde(n)
n.F.	neue Fassung
NAS	Network Attached Storage
NGO	Non-governmental organization
Nichtannahmebeschl.	Nichtannahmebeschluss
NJW	Neue Juristische Wochenschrift
NSA	National Security Agency
NVwZ	Neue Zeitschrift für Verwaltungsrecht
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OEEC	Organisation für europäische wirtschaftliche Zusammenarbeit
OLG	Oberlandesgericht
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
P2P	Peer-to-Peer
POP3	Post Office Protocol Version 3
Rep.	„Reports of Judgments and Decisions“ des EGMR
RL	Richtlinie
Rn.	Randnummer
Rs.	Rechtssache
RSS	Rich Site Summary
RTSP	Real-time Streaming Protocol
S.	Seite
SABAM	Société belge des auteurs, compositeurs et éditeurs SCRL
SächsVBl	Sächsische Verwaltungsblätter
SIGCOMM Comput. Commun. Rev.	SIGCOMM Computer Communication Review
Slg.	Sammlung der Rechtsprechung des Gerichtshofes und des Gerichts Erster Instanz

SPI	Shallow Packet Inspection
SIGCOMM	Special Interest Group on Data Communications
SMTP	Simple Mail Transfer Protocol
SPID	Statistical Protocol IDentification
StPO	Strafprozessordnung
TCP	Transmission Control Protocol
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TMG	Telemediengesetz
TOS/DS	Type of Service/Differentiated Service
u.a.	und andere
U.S.	United States
UAbs.	Unterabsatz
UDP	User Datagram Protocol
UrhG	Urhebergesetz
URL	Uniform Resource Locator
Urt.	Urteil
UWG	Gesetz gegen den unlauteren Wettbewerb
v.	vom
Vbm.	Vorbemerkung
VG	Verwaltungsgericht
vgl.	vergleiche
VO	Verordnung
VoIP	Voice over IP
VPN	Virtual Private Network
VwGO	Verwaltungsgerichtsordnung
WEU	Westeuropäische Union
WLAN	Wireless Local Area Network
WRP	Wettbewerb in Recht und Praxis
WWW	World Wide Web
z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZGE	Zeitschrift für Geistiges Eigentum
ZRP	Zeitschrift für Rechtspolitik
ZugErschwG	Zugangserschwerungsgesetz
ZUM	Zeitschrift für Urheber- und Medienrecht

Einleitung

Das Phänomen der Digitalisierung führt dazu, dass unser Leben mehr und mehr „online" stattfindet – die Kommunikation mit anderen Menschen, wie wir Güter konsumieren und vertreiben, wie wir uns über unsere Umwelt informieren. Ermöglicht wird dieser Wandel durch eine umfassende Vernetzung – u.a. – unserer Häuser und Wohnungen, unserer Büros, Arbeitsgeräte und Mobiltelefone über das Internet, über das mit der Zeit immer größere Datenmengen übertragen werden können:

Die Verteilung großer Mengen an Information durch das Internet ist beinahe kosten- und verlustfrei, mit geringem zeitlichen Aufwand und ohne Qualitätsverlust möglich. Das hat offensichtliche Vorteile, die hier kaum der näheren Beschreibung bedürfen. Hervorzuheben ist hier vor dem Hintergrund dieser Arbeit beispielhaft die Möglichkeit der Internet-Nutzer, sich Medieninhalte – z.B. Bücher, Filme, Musik, auch solche, die urheberrechtlich geschützt sind – jederzeit und an jedem Ort auf Abruf in Echtzeit zu beschaffen. Insbesondere für die Inhaber der Rechte an diesen Medieninhalten kann dies vorteilhaft sein, da sie auf diese Weise ihre Inhalte direkt und mit geringeren Vertriebskosten als früher (vor dem Internet) vertreiben können.

Diese durch die technologische Entwicklung neu gewonnene Leichtigkeit der Informationsverteilung und -beschaffung hat allerdings ihre Schattenseiten. Denn die Frage, wie die unbeschränkte Verteilung und Beschaffung von Informationen, die berechtigterweise rechtlich geschützt sind, verhindert werden kann, ist aktueller denn je. Durch das Internet fallen viele Probleme der Übermittlung und Vervielfältigung, die bei analogen Medien immer noch bestehen, weg. Insbesondere sind Qualitätsverlust, Kosten und Zeit keine Faktoren mehr, die einer unbeschränkten Verbreitung von Informationen entgegenstehen – und die in der „analogen Welt" das geltende Recht bei seiner Durchsetzung wirksam unterstützten.

Der Schutz urheberrechtlich geschützter Werke ist von dieser Entwicklung in besonderem Maße nachteilig betroffen. Die digitale rechtswidrige Kopie steht dem Original oft in ihrer Qualität nicht nach, und die Verbreitung über das Internet kann schnell, einfach und mit geringen Kosten erfolgen.

Das Recht steht daher vor der Herausforderung, alte Durchsetzungmechanismen, die an Wirksamkeit verloren haben, durch neue zu ersetzen. Zu diesen neuen Mechanismen könnten auch Eingriffe in den Datenverkehr selbst gehören, z.B. IP-Sperren, DNS-Sperren und die sogenannte Deep Packet Inspection (DPI).

Das Sperren, Filtern und Untersuchen von Daten als Mittel zur Durchsetzung des Rechts sind andererseits nicht nur gesellschaftlich umstritten, wie die öffentliche Diskussion im Rahmen des Gesetzgebungsprozesses der EU-Richtlinie 2019/790 – in einem etwas anderen technischen Kontext – gezeigt hat. Auch ist die die Vereinbarkeit solcher Maßnahmen mit Grundrechten bislang nicht höchstrichterlich entschieden.

Fragestellung

In dieser Arbeit soll daher die folgende Frage untersucht werden:

> Sind hoheitliche Eingriffe in den Datenverkehr zur Durchsetzung des Urheberrechts verfassungs- und europarechtlich zulässig?

Kapitel 1 – Grundlagen

Zunächst sollen an dieser Stelle aus Gründen der Übersichtlichkeit vorab einige sachliche und technische Grundlagen geklärt werden. Dies bietet sich zunächst für die zur rechtlichen Einordnung hoheitlicher Eingriffe in den Datenverkehr (Datenverkehrsregulierung, DVR) wichtigen technischen Grundlagen an (unter Einschluss der beteiligten Akteure bzw. Provider). Zudem wird ein an die Datenverkehrsregulierung zur Urheberrechtsdurchsetzung in der grundrechtlichen Würdigung anzulegender Effektivitätsmaßstab herausgearbeitet sowie die tatsächliche Effektivität datenverkehrsregulierender Maßnahmen dargestellt.

I. Technische Grundlagen des Internets

Von Bedeutung für die rechtliche Einordung der Datenverkehrsregulierung sind die technischen Grundlagen des Internets selbst. Ihnen widmet sich der folgende Abschnitt. Die Ausführungen behandeln die Protokolle, Anwendungen und das physische Netz, auf denen das Internet aufbaut, also das technische Fundament des Internets. Die Ausführungen werden nur insoweit in die Tiefe gehen, wie es für das Verständnis der weiteren Untersuchung notwendig ist.

Um die Kommunikation von einem Rechner zu einem anderen über das Internet zu ermöglichen, bedarf es einheitlicher Konventionen und Regeln, die sicherstellen, dass die zu übermittelnden Daten an den richtigen Empfänger transportiert und von diesem auch verstanden werden. Diese Regeln oder Protokolle, die dafür sorgen, dass Hard- und Software unterschiedlicher Herkunft und Bauart sich dennoch verstehen, werden im Falle des Internets im TCP/IP-Referenzmodell zusammengefasst.[1]

Ein prägendes Merkmal des TCP/IP-Protokolls ist sein Aufbau in vier Schichten (L_1, L_2, L_3, L_4). Die Schichten des Protokolls sind dabei hierarchisch geordnet. Jede Schicht ist für die Lösung eines bestimmten Problems der Netzwerkkommunikation zuständig und eröffnet eine neue Abstraktionsebene.[2] Festgelegt werden insbesondere Aufgaben, Abstraktionsgrad, Komplexität und Funktionsumfang der jeweiligen Schicht.[3] Der Abstraktionsgrad ist umso höher, je höher die Schicht liegt.

---

[1] Das TCP/IP-Referenzmodell ist ein Bündel von Protokollen, das unter der Leitung von *Cerf* und *Kahn* in den frühen 1980er Jahren entwickelt wurde. Protokolle legen fest, in welcher Sprache und nach welchen sonstigen Regeln zwei Stellen miteinander kommunizieren.

[2] Je tiefer die Schicht, desto weniger abstrakt die betreffende Kommunikation.

[3] *Meinel/Sack*, Internetworking, 2.1 (S. 31 f.).

Es werden durchgehend ein paar wichtige Grundprinzipien eingehalten. Die Schichten werden *unabhängig* voneinander definiert, die Architektur des Schichtensystems ist streng modular. Das bedeutet, dass der innere Aufbau einer Schicht für die anderen Schichten keine Rolle spielt. Bei Bedarf kann also eine Protokollschicht verändert werden, etwa weil sich ein anderer Aufbau als effizienter erwiesen hat, ohne dass dies Auswirkungen auf die übrigen Schichten hat. Zudem sind die einzelnen Schichten voneinander abgeschirmt. Eine Schicht kann nur mit ihren jeweiligen Nachbarschichten kommunizieren also etwa Schicht L_3 mit Schicht L_2 und Schicht L_4, nicht jedoch mit Schicht L_1. Fest definiert sind hingegen die jeweiligen Schnittstellen, über die die Kommunikation mit den anderen Schichten stattfindet. Diese bleiben gleich, auch wenn die umgebenden Protokollschichten abgeändert werden.[4] Mit anderen Worten: Es ist für das Gesamtsystem der Internet-Kommunikation nicht ausschlaggebend, wie genau die Daten innerhalb einer spezifischen Schicht verarbeitet werden. Entscheidend ist nur, dass das Ergebnis an die nächste Ebene auf eine Weise übergeben wird, die diese verstehen und die sie weiterverarbeiten kann.

Werden Daten von einem Rechner zum nächsten übertragen, durchlaufen sie dabei der Reihe nach die diversen Schichten, indem sie von der einen Schicht an die jeweils nächsttiefere Schicht übertragen werden (und umgekehrt). Gleichgültig ist, um welche Art von Daten es sich handelt. Es kann der Text einer E-Mail sein, ein Steuerungsbefehl für eine Windkraftanlage, aber auch eine Filmdatei, die einen urheberrechtlich geschützten Kinofilm enthält.

Das Durchlaufen der verschiedenen Schichten verdient nähere Betrachtung: Zunächst befinden sich die eigentlichen Nutzdaten auf der Ebene der Anwendungsschicht. Diese Schicht wird hier als L_4 bezeichnet. Wenn man einen Vergleich mit der Briefpost ziehen möchte, handelt es sich bei den Nutzdaten um das Schreiben selbst, ohne Umschlag oder Adressierung. Diese Daten verarbeitet die tiefste Schicht (bzw. die dort verorteten Protokolle) nun im Rahmen ihres Aufgabenbereichs. Zudem fügt sie vor den Nutzdaten einen sogenannten Dateikopf (geläufiger: Datei-Header) H_4 an mit denjenigen Daten, die die Protokollschicht L_4 ihrem Gegenüber am empfangenden Rechner mitteilen möchte (also der dortigen L_4).

Die zu sendenden Daten, die sich immer noch auf dem Rechner des Absenders befinden, liegen nun in der Form | H_4 + Nutzdaten | vor. Dieses Datenpaket wird sodann an die nächsthöhere Protokollschicht H_3 über die dafür bestimmte Schnittstelle weitergereicht. Die Schnittstellen zur Kommunikation mit der nächsthöheren Ebene werden als Dienst-Interface bezeichnet.

In der Transportschicht L_3 werden die Daten wiederum entsprechend den Aufgaben dieser Schicht verarbeitet und das Ergebnis in einem weiteren Header H_3 ausgegeben. Dieser Header wird erneut dem bisherigen Datenpaket vorangestellt, so dass die aktuelle Schicht über die entsprechende Schnittstelle das Paket | H_3 + H_4 + Nutzdaten | an die nächste

[4] *Meinel/Sack*, Internetworking, 2.1.2 (S. 36).

Ebene übergeben kann. Dieser Vorgang wiederholt sich, bis das Datenpaket schließlich in der obersten Protokollschicht, der Netzzugangsschicht L_1, ankommt. Dabei ist zu beachten, dass die Protokolle jeder Ebene in Hinblick auf die Daten, die in den Schichten darunter liegen, blind sind. Für die Protokolle der Internet-Schicht L_2 stellt sich das Datenpaket als | H_2 + Nutzdaten | dar. Diese Nutzdaten enthalten dann die weiteren Dateiheader.

Nachdem die Protokolle der Netzzugangsschicht die Daten verarbeitet haben, wird das Paket an die physikalische Netzebene übergeben. Die Daten verlassen den Rechner und das lokale Netzwerk und reisen über das Internet zum Empfängerrechner. Das Paket hat nun die Form | H_1 + H_2 + H_3 + H_4 + Nutzdaten |.

Am Empfängerrechner angekommen, wird das Datenpaket in umgekehrter Richtung wieder entkapselt. Der Vorgang durchläuft erneut alle Schichten der Protokollsuite, startet nun aber zunächst in der oberste Schicht L_1. Diese Schicht liest dabei über die sogenannte Partner-Schnittstelle bzw. das Partner-Interface ausschließlich die Informationen aus Header H_1 aus und entfernt am Ende der Datenverarbeitung den Header aus dem Datenpaket (dieses hat dann also die Form | H_2 + H_3 + H_4 + Nutzdaten |. Anschließend reicht Schicht L_1 das Paket an die nächsttiefere Ebene L_2 weiter. Wird das Ergebnis der Datenverarbeitung aus L_1 noch benötigt, kann es nicht in H_1 aufbewahrt werden, da dieser Header entfernt wurde. In solchen Fällen werden die zu speichernden Daten vielmehr über die entsprechende Schnittstelle an L_2 übergeben. Dieser Vorgang wiederholt sich, bis das Datenpaket | H_4 + Nutzdaten | in der Anwendungsschicht ankommt und dieses die Nutzdaten an das Anwendungsprogramm ausgibt, zum Beispiel den Internet-Browser.

Der strikt hierarchische Aufbau und das Auslesen der Pakete nach dem festgelegten Schema ermöglicht nicht nur eine Kommunikation der einen Schicht mit ihren jeweiligen Nachbarschichten, sondern auch eine virtuelle, indirekte Kommunikation der Schichten auf den beteiligten Rechnern über das Partner-Interface, obwohl beispielsweise die Protokolle der Transportschicht auf den verschiedenen Computern keinen direkten Kontakt mit ihrer Partnerschicht aufnehmen.

Die vier Schichten eines IP-Pakets werden als Netzzugangsschicht (eng. Link Layer, L_1), Internet-Schicht (eng. Internet Layer, L_2), Transportschicht (eng. Transportation Layer, L_3) und Anwendungsschicht (eng. Application Layer, L_4) bezeichnet. Diesen Schichten vorgeschaltet ist die physikalische Schicht, die nach strenger Definition nicht Bestandteil des TCP/IP-Referenzmodells ist, aus Gründen der Vollständigkeit und Verständlichkeit aber dennoch kurz mit vorgestellt werden soll.

1. Physikalische Schicht

Das Internet ist eine weltweite, mit Hilfe von sogenannten Routern realisierte Kopplung physikalischer Netze, in denen das Internet Protocol eingesetzt wird.[5] Auf diese Weise ermöglicht es die Kommunikation zwischen räumlich voneinander entfernten lokalen

[5] *Badach/Hoffmann*, Technik der IP-Netze, 1.4.3 (S. 33).

Netzwerken und Endgeräten. Unabhängig von der Form und Aufbereitung der Daten müssen die Daten dabei über ein Trägermedium übermittelt werden. Dies geschieht über physische Medien wie Kupfer- und Glasfaserkabel oder aber über unkörperliche wie Richt- oder Rundfunk. Damit der Transport funktioniert, muss der zu übertragende Datenstrom in eine Form gebracht werden, die sich für das jeweilige Medium eignet, und auf der anderen Seite wieder umgewandelt werden, damit der Empfänger die Signale wieder als maschinenverständliche Daten erhält. Diesen Vorgang nennt man Modulation bzw. Demodulation und wird auf der Ebene der physikalischen Schicht (Physical Layer) nach entsprechenden Protokollen von spezieller Hardware (**Mo**dulator-**Dem**odulator, Modem) bewerkstelligt.

Die Protokolle legen die Regeln fest, nach denen die Netzwerk-Hardware und das Übertragungsmedium miteinander kommunizieren. Da die physikalische Schicht sehr hardware-nah ist, behandeln auch die Protokolle entsprechende (Hardware-)Probleme und weniger solche, die die Daten selbst betreffen. Die Protokolle der physikalischen Schicht regeln beispielsweise die Belegung von Steckverbindungen mitsamt Kabelspezifikationen, Verstärkerelementen und Netzwerkadaptern.[6]

2. Netzzugangsschicht

Die Aufgaben der Netzzugangsschicht liegen vornehmlich darin, Datenpakete zwischen zwei benachbarten Endsystemen sicher zu übertragen. Die kommunizierenden Rechner müssen direkt oder über sogenannte Diffusionsnetzwerke miteinander verbunden sein, ohne dass ein Zwischensystem zwischengeschaltet ist. Betrachtet man die einzelnen Phasen des Datenaustausches zwischen zwei Endsystemen stark vereinfacht als eine Datenübermittlung von einem Endsystem über ein lokales Netz, von dort über das Internet zu einem anderen lokalen Netz, in dem die Daten dann schließlich zu einem bestimmten Rechner geleitet werden, bewegen wir uns hier im Bereich der Kommunikation innerhalb der lokalen Netzwerke. Die Daten befinden sich also – je nach Architektur des lokalen Netzes – etwa zwischen Rechner und lokalem Netzwerk-Router. Hier stellen die Protokolle der Netzzugangsschicht sicher, dass die Kommunikation zwischen zwei Anwenderrechnern im selben Heimnetzwerk funktioniert, dass die Daten verschiedener Endgeräte, die an denselben Switch angeschlossen sind, nicht kollidieren, oder Fehler in der Datenübertragung entdeckt und nach Möglichkeit korrigiert werden. Zu diesen Zwecken spalten die entsprechenden Protokolle den Datenstrom („Bitstream“) in Pakete fester Größe auf und fügen einfach strukturierte Daten hinzu, die dafür Sorge tragen, dass Datenfehler entdeckt werden. Dies wird beispielsweise mit Prüfsummen bewerkstelligt. Außerdem wird auf dieser Ebene sichergestellt, dass mehrere in einem (W)LAN zusammengefasste Rechner nur die für sie bestimmten Daten aus dem Internet empfangen, obwohl dem ex-

[6] *Meinel/Sack*, Internetworking, 2.2.1 (S. 46 f.).

ternen Rechner lediglich die IP-Adresse des Routers bekannt ist. Verschiedene Technologien wie Ethernet und WLAN bauen auf den Protokollen der Netzzugangsschicht des TCP/IP-Referenzmodells auf.[7]

3. Internet-Schicht

Die Internet-Schicht (L_2) der TCP/IP-Protokoll-Suite soll die Kommunikation zweier Endsysteme, die an das Internet angeschlossen sind, über (womöglich auch) unterschiedliche Netzwerkarchitekturen hinweg ermöglichen.[8]

Die in der Internet-Schicht arbeitenden Protokolle beschreiben, wie das Routing der Datenpakete funktioniert, die über das Internet ausgetauscht werden. Dies ist notwendig, damit die Datenpakete ihren Bestimmungsort erreichen können. Das wichtigste Protokoll der Internet-Schicht ist das Internet Protocol (IP).[9] Das Internet-Protokoll trägt ein Datenpaket, dass in der Regel entweder nach dem TCP- oder dem UDP-Transportprotokoll übermittelt werden soll. IP fügt jedem Paket einen Header hinzu, dessen wichtigster Informationsgehalt die IP-Adressen von Sender und Empfänger sind.

IP stellt ein Adressierungsschema bereit, das es den Routern ermöglicht, die mit IP-Adressen versehenen Datenpakete über die verschiedenen Subnetze an den Empfangsrechner zuzustellen. Im Router des Netzbetreibers wird dazu der Header der Internet-Schicht H_2 ausgelesen. Das IP wählt dort nach definierten Kriterien den nächsten Vermittlungsknoten aus, an den das Paket weitergeleitet wird, bis dieses seinen Bestimmungsort erreicht hat.

Für das Routing werden grundsätzlich keine Manipulationen im H_2 vorgenommen. Die zur Durchführung des Routings notwendigen Steuerinformationen werden vielmehr von

---

[7] Vgl. *Meinel/Sack*, Internetworking, 2.3.2 (S. 53 ff.) für eine vertiefte Darstellung der Netzzugangsschicht.

[8] *Meinel/Sack*, Internetworking, 2.3.3 (S. 57).

[9] IP wird sowohl in der Version IPv4 als auch der Version IPv6 verwendet, *Badach/Hoffmann*, Technik der IP-Netze, 3 (S. 111). Hintergrund ist, dass der mögliche Adressraum, den IPv4 bereitstellen kann, sich dem Ende zuneigt und immer knapper bemessen ist. IPv6 hingegen bietet ausreichend Adressraum, um für die exponentiell steigende Nachfrage nach IP-Adressen für die absehbare Zukunft gerüstet zu sein. Nebeneffekt ist, dass ISPs ihren Kunden vermehrt statische, also dauerhafte IP-Adressen zuweisen können, anstatt diese – wie bislang üblich – dynamisch in kurzen Abständen neu zu vergeben. Dieser Aspekt ist aus rechtlicher Perspektive nicht zu vernachlässigen, da er die Zuordnung eines bestimmten Datenverkehrs zu einer konkreten Person vereinfacht. Der Auswertung der Daten bereits der Internet-Schicht könnte daher größere grundrechtliche Relevanz zukommen. Diese mit IPv6 verknüpfte Problematik könnte zukünftig relevant werden, auch wenn als Grundlage dieser Untersuchung wegen der noch vorherrschenden Verbreitung angenommen wird, dass bei der von einer Maßnahme der Datenverkehrsregulierung betroffenen Kommunikation noch der Standard IPv4 verwendet wird.

der Internet-Schicht über die entsprechenden Kommunikationsschnittstellen an die Netzzugangsschicht übergeben.[10] Dies betrifft insbesondere die MAC-Adresse (also die Hardwareadresse des Netzwerkadapters) des nächsten Routers auf dem Weg zum Empfangscomputer.

Eine Ausnahme von diesem Grundsatz besteht im Fall der Fragmentierung von Datenpaketen. Da die unterschiedlichen Netze, über die die Datenpakete übertragen werden, unterschiedliche Regeln für die maximale Paketgröße besitzen, müssen in H_2 gegebenenfalls auch Informationen transportiert werden, die beinhalten, wie Datenpakete, die während des Transports fragmentiert wurden, wieder zusammenzusetzen sind. Fragmentierung ist bisweilen ein notwendiger Schritt, um die Kommunikation zwischen unterschiedlich leistungsfähigen Netzwerken zu gewährleisten. Ist ein Datenpaket zu groß für ein Netzwerk, über das das weitere Routing abgewickelt werden soll, spaltet der Router das Paket in passende kleinere Pakete auf, die das Netzwerk verarbeiten kann. Jedes durch die Fragmentierung neu geschaffene Paket behält den Original-Header mitsamt der Header-ID.[11] Jedoch wird im Header H_2 durch den Router ein Datum hinzugefügt, das die Position des Fragments im Originalpaket kennzeichnet. So kann das Datenpaket später am Zielrechner wieder zusammengesetzt werden.[12]

Eine weitere Ausnahme vom Grundsatz, dass Router nicht den H_2 manipulieren, betrifft das dortige Datenfeld TOS/DS (Type of Service / Differentiated Service). Dort findet sich u.a. eine Option, die die Steuerung der Übertragungsgeschwindigkeit der Daten ermöglicht. Durch bestimmte Eintragungen an dieser Stelle wird das Datenpaket – abweichend vom Best-Effort-Grundsatz, dazu sogleich – mit einer höheren oder niedrigeren Priorität zu übertragen.[13]

In der Internet-Schicht findet sich auch eine Angabe zur Länge des Pakets in Bytes wieder.[14] Eigentlicher Zweck ist es, die Notwendigkeit einer Fragmentierung beim weiteren Routing zu bestimmen. Diese Information lässt sich jedoch auch für eine heuristische Datenverkehrsanalyse heranziehen, die helfen kann, den Inhalt der Nutzdaten des Bitstreams zu ermitteln oder abzuschätzen.

Die Internet-Schicht L_2 bietet lediglich eine *verbindungslose* Kommunikation an. Das bedeutet, dass auf dieser Ebene keine durchgehende Verbindung zwischen Absender und Empfänger aufgebaut wird, die den Austausch über die Regeln beim Ablauf der Kommunikation erlauben würde. Die Verbindung ist zudem auch *nicht zuverlässig*. Die Zustellung der Pakete wird nicht quittiert. Für die Fehlerkontrolle sind, abhängig davon, ob es sich um TCP- oder UDP-Kommunikation handelt, später die Transportschicht oder die

---

[10] *Meinel/Sack*, Internetworking, 2.3.3 (S. 58).
[11] *Meinel/Sack*, Internetworking, 2.3.3 (S. 57 f.).
[12] *Badach/Hoffmann*, Technik der IP-Netze, 3.2.2 (S. 118 f.)
[13] *Badach/Hoffmann*, Technik der IP-Netze, 3.2.1 (S. 115 ff.). Auf diese Weise wäre es beispielsweise denkbar, dass Datenverkehr, dessen Übertragung ein Regulierer nicht vollständig unterbinden, aber dennoch weniger attraktiv machen möchte, zu verlangsamen.
[14] *Badach/Hoffmann*, Technik der IP-Netze, 3.2 (S. 114).

Anwendungsschicht verantwortlich. Die Protokolle der Internet-Schicht stellen hingegen lediglich die Integrität der Header über eine Prüfsumme sicher. Ansonsten übernehmen die Protokolle nur dafür die Garantie, dass die Datenpakete so gut es geht übermittelt werden (Best-Effort-Grundsatz). Um dem Best-Effort-Grundsatz zu genügen, werden die Datenpakete unabhängig voneinander versendet und durchlaufen nicht selten unterschiedliche physikalische oder logische Trägernetze.[15]

4. Die Transportschicht

Die Transportschicht L_3 ist die zweittiefste Schicht im TCP/IP-Protokollstapel. Sie regelt den Verlauf der Datenübermittlung zwischen zwei Anwendungen auf verschiedenen Rechnern. Die Transportschicht nimmt die Daten einer Anwendung an deren Port am versendenden Rechner auf und übergibt die Daten am Empfangsrechner wieder an den Port der Empfängeranwendung. Die Protokolle der Transportschicht gewährleisten erster Linie die Integrität der gesendeten Daten. Das bedeutet, dass sie dafür sorgen, dass die Daten unbeschädigt beim Empfangsrechner ankommen.[16]

Im weiteren Verlauf dieser Arbeit wird von Bedeutung sein, wie zwei Programme auf verschiedenen Rechnern miteinander kommunizieren und wie sie sich gegenseitig identifizieren. Um ein Programm auf einem fremden Rechner im Internet eindeutig zu identifizieren, reicht die IP-Adresse des anderen Rechners nicht aus. Auf einem Computer warten in der Regel zeitgleich mehrere Anwendungen darauf, dass mit ihnen Kontakt aufgenommen wird, z.B. der Internet-Browser und der E-Mail-Client. All diese Programme haben einen Kanal zur Netzwerk-Schnittstelle des Computers geöffnet, über den sie auf eingehende Nachrichten warten. Diese Kanäle sind die sogenannten Ports. Damit auch die richtige Anwendung auf dem Endgerät angesprochen werden kann, also nicht etwa der Web-Browser die E-Mail bekommt, muss der Port angesprochen werden, also die Adresse der korrekten Anwendung auf dem Endgerät.

Verschiedene Ports sind quasi-standardisiert bestimmten Typen von Anwendungen zugeschrieben, so dass man auch als beobachtender Dritter mit einem Blick auf den Port des Empfangsrechners mit einiger Gewissheit eine Aussage über die Aufgabe der Empfangs-Anwendung treffen kann. Die Verwendung der standardisierten Ports ist allerdings weder technisch noch rechtlich zwingend.

Die IP-Adresse und der Port bilden zusammen den sogenannten Socket, die eindeutig identifizierbare Adresse einer Anwendung im Internet.[17] Innerhalb der Transportschicht arbeiten die beiden Protokolle TCP (Transmission Control Protocol) und UDP (User Datagram Protocol) und helfen, die Integrität der zwischen zwei Sockets ausgetauschten Daten sicherzustellen. Je nach den Bedürfnissen der empfangenden Anwendung an die Integrität der Daten wird dazu das jeweils passende Protokoll gewählt.

---

[15] *Badach/Hoffmann*, Technik der IP-Netze, 3.1 (S. 112).
[16] *Badach/Hoffmann*, Technik der IP-Netze, 1.4.4 (S. 34 f.).
[17] *Badach/Hoffmann*, Technik der IP-Netze, 1.4.4 (S. 36.).

TCP ist dabei das strengere Protokoll. Es handelt sich um eine sogenannte *verbindungsorientierte Kommunikation*. Zwischen den Sockets auf den kommunizierenden Rechnern wird zunächst eine logische Verknüpfung (TCP-Verbindung) hergestellt. Diese TCP-Verbindung lässt sich als virtuelle Direktleitung zwischen zwei Rechnern (in beiden Richtungen) verstehen. Die Anwendungen legen dann verschiedene Regeln für die Kommunikation auf dieser Verbindung fest. Diese beinhalten Regeln über die Nummerierung der Datenpakete, wie die Datenpakete beim Empfänger wieder zusammenzusetzen sind, welchen Weg die Daten durch das Netz nehmen sollen, wie die Fehlerkontrolle (wurden Daten beschädigt?) und die Flusskontrolle (sind die Daten in der richtigen Reihenfolge angekommen?) ablaufen sollen. Der Empfang der Daten wird jeweils entsprechend bestätigt, so dass die Verbindung zuverlässig ist.[18]

Bei Anwendungen, die keine Fehlertoleranz bei den übermittelten Daten erlauben, ist TCP das Protokoll der Wahl. Die umfangreichen Maßnahmen zur Sicherstellung der Datenintegrität sind deshalb notwendig, weil die zu übermittelnden Nutzdaten in der Regel zu groß für ein einzelnes IP-Paket sind und daher auf eine Vielzahl von Paketen aufgeteilt werden müssen.[19] TCP sorgt dafür, dass alle Pakete nacheinander in der richtigen Reihenfolge über denselben Weg über das Netz übertragen werden. Geht dennoch einmal ein Paket verloren, wird dies dem sendenden Rechner mitgeteilt, so dass dieser das Paket erneut anfordern kann. Kann TCP hingegen eine fehlerfreie Übertragung nicht sicherstellen, bricht nach einer Weile die Verbindung ab; ein Phänomen, das den meisten Internet-Nutzern vertraut sein dürfte.[20]

Dieses Sicherheitsnetz, das TCP aufbaut, ist allerdings mit einem Nachteil verbunden. Insbesondere, wenn die Datenintegrität während des Transports beschädigt wird, verlangsamt dies den Datenverkehr. Denn schließlich findet eine weitere Kommunikation statt, die zusätzliche Rechen- und Transportzeit beansprucht.

Ist eine vollständige Datenintegrität nicht notwendig, kommt daher oft UDP zum Einsatz. Eine gewisse Fehlertoleranz ist beispielsweise bei Anwendungen wie Voice over IP (VoIP) gegeben: Sprachübertragungen sind oft auch dann noch verständlich, wenn sie nicht perfekt sind. Dies äußert sich dann lediglich in Rauschen oder sonstigen Qualitätseinbußen. In diesen Fällen ist es wichtiger, dass überhaupt eine Datenverbindung besteht, weniger, dass sie fehlerfrei ist.

UDP verzichtet auf einen Großteil der Integritätskontrolle und ist damit bedeutend weniger komplex als TCP. Bei der Verwendung des TCP hingegen liefert die Transportschicht der Anwendungsschicht einen zusammenhängenden Strom an Daten. Die Anwendungsschicht „sieht“ also gar nicht, dass die Kommunikation in Form einzelner Pakete stattgefunden hat, da die Transportschicht diese bereits wieder zusammengesetzt hat.

---

[18] *Badach/Hoffmann*, Technik der IP-Netze, 1.4.4 (S. 34 ff.).
[19] *Meinel/Sack*, Internetworking, 2.3.4 (S. 60).
[20] *Badach/Hoffmann*, Technik der IP-Netze, 1.4.4 (S. 34 ff.).

UDP baut keine virtuelle Verbindung auf und spricht sich auch nicht über die Bedingungen des Transports ab. Es handelt sich wie bereits die Kommunikation auf der Ebene der IP-Schicht um eine *verbindungslose* Kommunikation. Einzelne Datenpakete, sogenannte Datagramme, werden unabhängig voneinander an den Empfangs-Socket gesendet. Die IP-Pakete werden getrennt voneinander an die Anwendungsschicht übergeben. Die Anwendung muss selbst dafür sorgen, dass die Datagramme zu einem sinnvoll zu verarbeitenden Datenstrom zusammengefügt werden.

Da die Datagramme unabhängig voneinander über das Internet übertragen werden, werden sie oft über verschiedene physische Pfade geroutet und kommen deshalb zu unterschiedlichen Zeiten an. Auch findet auf der Ebene der Transportschicht keine Fehlerkontrolle statt. Sind Daten fehlerhaft oder fehlen sie komplett, werden sie vom UDP einfach verworfen, es erfolgt keine Rückmeldung an den Absender.

Das Resultat des weitgehenden Verzichts auf Fehlerkontrolle beim UDP ist ein unter Umständen höherer Datenumsatz. Nicht alle Anwendungen sind jedoch fehlertolerant, so dass die Kenntnis des verwendeten Transportprotokolls durchaus in eingeschränktem Rahmen Rückschlüsse auf die Art der kommunizierenden Anwendung erlaubt.

5. Anwendungsschicht

Die Anwendungsschicht beinhaltet alle Prozesse, die Protokolle der Transportschicht dazu nutzen, Daten über das Internet zu versenden.[21] Grundsätzlich ist es für das Verständnis der Anwendungsschicht wichtig, sich den Unterschied zwischen den Netzwerkanwendungen und den darunterliegenden Protokollen der L_4 klar zu machen. Zur beispielhaften Erläuterung dient hier das E-Mail-System.

Das E-Mail-System als Netzanwendung ermöglicht es, dass über das Internet E-Mails ausgetauscht werden. Dem E-Mail-System liegen jedoch mehrere Anwendungen und Protokolle zu Grunde. Als Anwendungen seien E-Mail-Clients wie Microsoft Outlook oder Mozilla Thunderbird genannt, mit deren Hilfe die Nutzer E-Mails verfassen, adressieren und versenden können. Ebenso gehören zu diesem System E-Mail-Server, die die Postfächer der Nutzer bereitstellen. Davon wiederum zu unterscheiden sind die E-Mail-Protokolle wie SMTP, POP3 oder IMAP, die die Regeln des Datenaustauschs per E-Mail festlegen und die zu übermittelnden Daten an die Protokolle der Transportschicht übergeben.[22]

Neben dem E-Mail-System existieren allerdings eine Vielzahl an weiteren Netzwerkanwendungen, die ihrerseits auf andere Protokolle aufsetzen. Die wichtigste ist das World Wide Web (WWW), das Webserver- und Internet-Browser-Programme verwendet und zu einem großen Teil auf dem Protokoll HTTP aufsetzt.

Die Kommunikation der Anwendungsschicht des Senderechners mit derjenigen des Empfangsrechners erfolgt nach dem sogenannten Client/Server-Prinzip. Die Anwendung, die

---

[21] *Meinel/Sack*, Internetworking, 9.1.2 (S. 722).
[22] *Meinel/Sack*, Internetworking, 9.1.2 (S. 722).

aktiv wird und die Kommunikation aufnehmen möchte, ist dabei der Client, der andere Rechner wird Server genannt.[23]

Ein eingängiges Beispiel, anhand dessen hier die Kommunikation der Anwendungsschichten dargestellt werden soll, bietet das World Wide Web (WWW). Die Client-Software ist hier der Internet-Browser, die Server-Software ist der Web-Server. Die Kommunikation läuft dabei über das Protokoll HTTP ab. Dieses Protokoll muss daher sowohl die Funktionen bereitstellen, die der Client benötigt, als auch diejenigen des Servers.

Der Webbrowser sendet dem Webserver eine Nachricht, dass ihm der Server den Inhalt einer bestimmten Web-Seite liefern soll. Dazu übergibt der Internet-Browser mit Hilfe des HTTP diese Nachricht an die Transportschicht über eine Schnittstelle, den Port. Die Rolle des Ports wurde bereits bei der Darstellung der Transportschicht angesprochen.[24] Jedem Client wird von der Netzwerktransportsoftware ein verfügbarer Port zugeteilt, der am Rechner noch nicht anderweitig vergeben ist. Die diesen Port eindeutig identifizierende Portnummer wird im H_3 der Anfrage an den Server mitgesendet. Im Zusammenspiel mit der IP-Adresse des sendenden Computers ergibt die Portnummer den Socket des Clients. Kennt der Server den Socket des Clients, so weiß der Server, wie er den Client erreichen bzw. ihm antworten kann.

Um den Server über dessen Socket ansprechen zu können, muss der Client dessen Portnummer bereits kennen. Üblicherweise wird dieses Problem durch bestimmte Konventionen gelöst. Verbreitete Internetanwendungen benutzen oft Standard-Ports, die sogenannten Well-known Ports und die Registered Ports. Diese werden von der Internet Assigned Numbers Authority (IANA) einzelnen Netzwerkdiensten zugeteilt. HTTP benutzt serverseitig etwa sowohl bei der Verwendung von TCP als auch von UDP für gewöhnlich den Port 80.

Die Verwendung des Standard-Ports ist jedoch keineswegs zwingend. Theoretisch eignet sich technisch jeder Port für jede Aufgabe. Entscheidend ist nur, dass der Client die Port-Nummer des Servers kennt. Außer über die Verwendung von Standard-Ports kann dies etwa durch eine werksseitig für die Verwendung eines spezifischen Servers vorkonfigurierte Client-Software geschehen. Dann ist dem Client die Port-Nummer dadurch bekannt, dass ihm diese vom Programmierer der Internet-Anwendung mitgeteilt wurde. Eine andere Möglichkeit besteht darin, dass der Nutzer die Port-Nummer anderweitig kennt und sie manuell der Client-Software kommuniziert. Dies ist häufig bei E-Mail-Diensten der Fall, die ihre von den Standard-Nummern abweichenden Ports auf ihrer Web-Seite veröffentlichen. Die Nutzer müssen ihre E-Mail-Clients dann händisch für den Abruf bzw. den Versand von E-Mails konfigurieren.

Der Webserver (oder ein Server einer anderen Internet-Anwendung) hört den ihm eingerichteten Port des Transportprotokolls ab, er befindet sich im Abhörmodus. Meist beginnt

---

[23] *Meinel/Sack*, Internetworking, 9.1.2 (S. 722).
[24] Vgl. oben Kap. 1 I 4 (S. 8).

er mit dem Öffnen dieses Kanals bereits mit dem Start der Anwendung. Erreicht nun ein Datenpaket, das an den abgehörten Socket gerichtet ist, die Transportschicht des Servers, wird dieses an das abhörende Programm geleitet, das die Anfrage beantworten kann. In der Regel wird bei der Verwendung von HTTP nun zwischen Server und Client ein neuer Server-Port ausgehandelt (also einer, der sich vom „Handshake"-Port 80 unterscheidet).

Bekannte Protokolle der Anwendungsschicht sind etwa

HTTP (Hypertext Transfer Protocol, liefert Seiten des WWW über das Internet aus),

FTP (File Transfer Protocol, ein Protokoll zum Austausch von Dateien zwischen entfernten Computern),

SMTP (Simple Mail Transfer Protocol, das zum Versand von E-Mails verwendet wird)

DNS (Domain Name System, ein Protokoll, das Domain-Namen den zugehörigen IP-Adressen zuordnet)

oder BitTorrent (kollaboratives Filesharing-Protokoll).

Diese Aufzählung ist bei weitem nicht abschließend und zeigt nur einige der meistverwendeten Protokolle auf. Auch kommen mit der Entwicklung neuer Anwendungen und Netzwerktechniken ständig weitere Protokolle hinzu.

Jedes Protokoll hat einen individuellen Header. Die meisten davon sind standardisiert, der Aufbau von HTTP etwa wird durch die Internet Engineering Task Force (IETF) festgelegt.[25] Aus den Headern der Anwendungsschicht geht zunächst hervor, um welches Protokoll es sich handelt. Die Aufgabe der einzelnen Protokolle der Anwendungsschicht und die Anwendungsmöglichkeiten, die sie bieten, sind bekannt, so dass die Kenntnis des Protokolls Rückschlüsse auf die dahinterstehende Nutzer-Anwendung und deren Benutzungszweck erlaubt.

Im Kontext der Datenverkehrsregulierung zur Urheberrechtsdurchsetzung sollte man dabei beachten, dass viele Protokolle der Anwendungsschicht sich mehr oder weniger gut für die Übertragung urheberrechtlich geschützter Inhalte verwenden lassen. Bei Kommunikationsvorgängen über das Internet werden zwangsläufig Daten ausgetauscht. Bietet eine Anwendung die Möglichkeit, eine große Menge an Daten auszutauschen, eignet sie sich häufig auch für Filesharing[26]. Das betrifft auch solche Anwendungen wie E-Mail, obwohl

---

[25] *Leach u.a.*, HTTP/1.1, abrufbar unter https://tools.ietf.org/html/rfc2616 (zuletzt besucht am 09.10.2021); *Mogul/Nottingham*, HTTP Header Field Registrations, 2005, abrufbar unter https://tools.ietf.org/html/rfc4229 (zuletzt besucht am 09.10.2021).

[26] Unter dem Begriff „Filesharing" versteht man gemeinhin den Austausch digitaler Dateien über das Internet unter Einschluss rechtlich zulässigen Austauschs. Davon zu unterscheiden ist im Rahmen dieser Arbeit das „illegale Filesharing". Dieses ist im Rahmen dieser Arbeit definiert als als die Weitergabe von Dateien zwischen Benutzern des Internets, durch welche das Urheberrecht oder Leistungsschutzrechte i.S.d. Urheberrechtsgesetzes (UrhG) verletzt werden. „Filesharing" umfasst folglich „illegales Filesharing", erschöpft sich darin aber nicht.

SMTP in erster Linie für den Austausch von Text als Form elektronischer Post entwickelt wurde (und auch genutzt wird). Die Möglichkeit, einer E-Mail Dateien anzufügen, die auch urheberrechtlich relevant sein können, wird meist nur durch Restriktionen hinsichtlich der Größe der Dateien durch die E-Mail-Dienst-Anbieter begrenzt. FTP hingegen trägt die Datenübertragung bereits im Namen.

Dennoch stehen diese Protokolle nicht im Zentrum der Bemühungen, illegales Filesharing zu unterbinden. Vorherrschend bei Filesharing und Streaming sind andere Protokolle. BitTorrent (für Peer-to-Peer-Übertragungen) oder RTSP (Real-time Streaming Protocol, für Streaming-Dienste) lassen sich hier anführen. Nicht zuletzt aber eignet sich HTTP hervorragend nicht nur für den Transport von Hypertext, sondern selbst größter Datenmengen, so dass es auch bei Filesharing verbreitete Anwendung findet. Über die Art des verwendeten Protokolls lassen sich folglich gewisse Aussagen darüber treffen, mit welcher Wahrscheinlichkeit es sich um einen urheberrechtlich relevanten Vorgang handelt.

Abgesehen davon, dass der Header der Anwendungsschicht das verwendete Protokoll preisgibt, darf nicht unerwähnt bleiben, dass H_4 auch eine Vielzahl an weiteren, teilweise grundrechtssensiblen Daten transportiert. Bei dem Versand einer E-Mail enthält der Header des SMTP beispielsweise nicht nur den Adressaten, den Absender und die Empfänger in „CC“, sondern auch den Betreff, der oft den Nachrichteninhalt der E-Mail bereits zusammenfasst.[27]

Schließlich beinhaltet die Anwendungsschicht – auch und nicht zuletzt – die eigentlichen Nutzdaten (engl. Payload) der Nachricht. Diese bestehen bei einer E-Mail aus dem Nachrichtentext oder angehängten Dateien, beim Surfen im World Wide Web etwa aus der übertragenen Datei (in der Regel eine Web-Seite bzw. eine HTML-Datei), beim Video-Streaming aus dem Datenstrom, der die Videoinformationen enthält und bei VoIP aus den Audiodaten.

Die Kenntnis der Beschaffenheit des Payloads gibt die meisten Informationen zum Inhalt der Kommunikation preis. Ob ein urheberrechtlich relevanter Vorgang stattfindet, lässt sich daher durch eine Analyse der Nutzdaten am ehesten herausfinden. Diese Analyse ist andererseits aber auch potentiell mit den größten Grundrechtseingriffen verbunden.

II. Internet-Provider

Damit die Nutzer des Internets Zugang zu diesem Netzwerk und dessen vielfältigen Informationen und Angeboten haben, existieren verschiedene Dienstleister, die die dafür erforderliche Infrastruktur bereitstellen und notwendige Leistungen erbringen. Dies sind die sogenannten Internet-Provider. Diese Provider lassen sich entsprechend der großen Anzahl an unterschiedlichen Dienstleistungen, die den Betrieb des Internets ausmachen, in beinahe beliebig viele Unterkategorien aufteilen.

---

[27] *Meinel/Sack*, Internetworking, 9.3.2 (S. 768).

Für die Zwecke dieser Arbeit bietet sich aus inhaltlichen Gründen eine Unterscheidung zwischen Internet Service Providern (ISP), Host-Providern und Content Providern an, die sich im Wesentlichen, aber insbesondere im Hinblick auf die ISPs nicht ausschließlich an den §§ 7 ff. TMG orientiert. Gemäß der §§ 7 ff. TMG entscheidet sich an der dort vorgenommenen Kategorisierung in Access Provider, Host-Provider und Content Provider (dort nicht so benannt) die Reichweite der Haftung des jeweiligen Providers für das Verhalten Dritter. Die §§ 7 ff. TMG unterscheiden dabei zwischen der Vermittlung des Zugangs zur Nutzung von Telemedien (Access Provider), dem Bereithalten fremder Telemedien zur Nutzung (Host-Provider) und dem Bereithalten eigener Telemedien zur Nutzung (Content Provider), ohne dass es auf Zweck, Art oder Organisation der Tätigkeit des Providers ankäme.[28]

Gemäß § 2 Nr. 1 TMG sind Diensteanbieter (= Provider) alle natürlichen oder juristischen Personen, die eigene oder fremde Telemedien zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln.

Als Content Provider werden diejenigen Diensteanbieter bezeichnet, die als Telemediendienste eigene Inhalte im Internet zum Abruf auf einem Server bereitstellen. Unerheblich ist dabei, ob der Content Provider selbst die notwendige technische Infrastruktur bereitstellt oder dafür auf andere Dienstleister zurückgreift.[29] Dabei handelt es sich beispielsweise um den Betreiber einer Website mit eigenen Inhalten. Auch derjenige, der eine Datei bei einem Filehoster oder in einem Peer-to-Peer-Netzwerk öffentlich zugänglich macht, ist ein Content Provider.[30] Um eigene Inhalte eines Anbieters handelt es sich auch dann, wenn dieser die Inhalte nicht selbst geschaffen hat. Entscheidend ist, dass der Provider sie selbst eingestellt hat und bereithält.[31] Ebenso ist Content Provider, wer sich *fremde* Inhalte zu eigen macht.[32]

Host-Provider stellen demgegenüber die Inhalte dritter Anbieter über ihre technischen oder virtuellen inhaltlichen Plattformen den Nutzern des Internets zur Verfügung. Dabei

---

[28] Vgl. *Roggenkamp/Stadler* in: Heckmann/Paschke, Internetrecht, Kap. 1.4 Rn. 61 ff.; *Taeger/Kremer*, Recht im E-Commerce und Internet, S. 265.
[29] *Heckmann* in: Heckmann/Paschke, Internetrecht, 6. Aufl. 2019, Kap. 1 § 2 TMG Rn. 117 ff. mit umfangreichen Beispielen zur Erläuterung. Ähnlich *Hoeren* in: Hoeren u.a., Handbuch Multimedia-Recht, Teil 18.2 Rn. 12; *Sieber*, Verantwortlichkeit, S. 429, 434; *Stadler*, Haftung für Informationen, S. 32; *Waldenberger*, MMR 1998, 124 (124, 128).
[30] BGH, Urt. v. 12.07.2012, I ZR 18/11, Alone in the Dark, BGHZ 194, 339, Rn. 19; *Frey/Rudolph*, Haftungsregime, Rn. 65.
[31] *Roggenkamp/Stadler* in: Heckmann/Paschke, Internetrecht, Kap. 1.4 Rn. 90.
[32] Zur Frage, wann ein Anbieter sich eine Information zu eigen macht: BGH, Urt. v. 18.10.2007, I ZR 102/05, ueber18.de, GRUR 2008, 534, Rn. 20; BGH, Urt. v. 11. 12. 2012, VI ZR 314/10, IM „Christoph", GRUR 2013, 312, Rn. 14; BGH, Urt. V. 09.07.2015, I ZR 46/12, Die Realität II, MMR 2016, 190, Rn. 27; vgl. auch Bundesregierung, Entwurf eines Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr, BT-Drs. 14/6098, S. 23.

kann es sich um Betreiber von Internet-Servern handeln, aber auch z.B. um die Anbieter von Internet-Foren, Verkaufsplattformen, sozialen Netzwerken oder Filehostern.[33]

Internet Service Provider sind im Rahmen dieser Arbeit solche Diensteanbieter, die fremde Informationen lediglich innerhalb eines Kommunikationsnetzes wie dem Internet übermitteln oder für Endsysteme den Zugang zum Netz vermitteln. Bei ISPs handelt es sich um einen Oberbegriff, der zum einen die Access Provider, die den Netzzugang anbieten, und zum anderen die Network Provider, die ausschließlich Informationen übermitteln, umfasst. Ein Internet Service Provider stellt also im Wesentlichen die technische Infrastruktur des Internets und den Anschluss an diese sicher, in der Regel ohne Einfluss auf den Inhalt der übertragenen Informationen zu nehmen.[34] Die ISPs sind in dieser Arbeit schwerpunktmäßig von Interesse, da sie die Infrastruktur des Internets beherrschen und lediglich sie Maßnahmen der Datenverkehrsregulierung unmittelbar umsetzen können. Nicht zuletzt sind Internet Service Provider aber auch selbst Träger von Grundrechten und möglicherweise durch staatliche Anordnung von DVR-Maßnahmen betroffen.

III. Grundlagen der Datenverkehrsregulierung

„Datenverkehrsregulierung" (DVR) bezeichnet im Rahmen dieser Arbeit hoheitliche Eingriffe in den Datenverkehr des Internets. Mangels eigener Infrastruktur und technischer Möglichkeiten des Staates werden Maßnahmen der Datenverkehrsregulierung in der Praxis umgesetzt, indem der Staat (durch gesetzgeberisches, gerichtliches und/oder behördliches Handeln) diejenigen Internet Service Provider zu entsprechenden Handlungen verpflichten, über die sie rechtliche Gewalt ausüben (also diejenigen ISPs, die auf dem jeweiligen Hoheitsgebiet agieren).[35]

Zu den für eine Datenverkehrsregulierung in Frage kommenden Maßnahmen gehört in erster Linie, den Datenverkehr zu analysieren, zu blocken, umzuleiten und inhaltlich zu manipulieren – wobei der Analyse und dem Blockieren des Datenverkehrs die größte praktische Relevanz zukommt. Technisch durchgesetzt haben sich als Optionen für datenverkehrsregulierende Maßnahmen die IP-Sperre, die DNS-Sperre sowie Filtersysteme, die den Datenverkehr umfassend unter Verwendung von Deep Packet Inspection durchleuchten. Dabei sind auch Hybrid-Systeme im Sinne kombinierter Verfahren denkbar.Um in den Internet-Datenverkehr regulierend einzugreifen, bieten sich dem Staat gleich mehrere technische Optionen. Die unterschiedlichen möglichen Maßnahmen setzen an unterschiedlichen Stellen in der Netzinfrastruktur und dem TCP/IP-Protokollstapel an, sind unterschiedlich flexibel und effektiv und unterscheiden sich nicht zuletzt deshalb in ihren tatsächlichen und rechtlichen Implikationen.

---

[33] *Brinkel*, Filesharing, S. 310 f. m.w.N.; *Engels u.a.*, K&R 2007, 57 (59); *Härting*, Internetrecht, Rn. 2559; *Hopf*, ZUM 2008, 207 (216); *Koch*, BB 1996, 2049 (2050); *Volkmann*, CR 2008, 232 (233).
[34] *Sieber/Nolde*, Sperrverfügungen, S. 40; *Hoffmann* in: Spindler/Schuster, Recht der elektronischen Medien, Elfter Teil, § 8 TMG Rn. 16 f.; *Ricke* in: Spindler/Schuster, Recht der elektronischen Medien, § 1 TMG Rn. 6 f.
[35] Vgl. dazu *Schilling*, Präventive staatliche Kontrollmaßnahmen im Internet und ihre Vereinbarkeit mit dem Europarecht, S. 47.

1. DNS-Sperren

DNS-Sperren sind als Maßnahmen der Datenverkehrsregulierung lediglich im Bereich des World Wide Web relevant, also dem Teil des Internets, den man in der Regel mit einem Internet-Browser nutzt. Der Hauptanwendungsfall ist der, dass ein Nutzer eine bestimmte Website aufrufen will, ihm der Zugriff auf diese jedoch so schwer wie möglich gemacht werden soll. Ohne wirkliche Bedeutung ist die DNS-Sperre hingegen für andere Dienste des Internets. Auch auf Filesharing über Peer-to-Peer-Netzwerke haben DNS-Sperren keinen Einfluss, da diese auf einem anderen Protokoll basieren und von einer DNS-Sperre nicht betroffen werden.

Das DNS-System ist ein unterstützendes System, das technisch gesehen für die Funktionsweise nicht zwingend notwendig ist, aber die Nutzung des World Wide Web erheblich erleichtert. Gibt man in seinem Internet-Browser den Domain-Namen eines Internet-Auftritts ein, also etwa „www.hu-berlin.de“ für die Website der Humboldt Universität zu Berlin, ist dies für den Menschen eine eingängige und mehr oder weniger leicht zu merkende Adressierung. Für ein Maschinennetzwerk – wie das Internet eines darstellt – ist dies jedoch keine effiziente Art der Adressierung. Das Internet benötigt für das Routing der Daten von Computer zu Computer IP-Adressen.[36]

Diese Adressierung ist für Menschen schwierig zu merken. Zudem ist die Zahl an IP-Adressen begrenzt. Daher wird eine spezifische IP-Adresse vom zuständigen ISP nicht immer fest einem Computer(-Netzwerk) zugewiesen (statische IP-Adresse). Oft wird so verfahren, dass die Adresse ständig neu vergeben wird (dynamische IP-Adresse). Damit es den Nutzern erspart bleibt, sich eine Vielzahl an Zahlencodes zu merken, diese nachzuschlagen und ständig zu aktualisieren, wenn eine IP-Adresse einem neuen Rechner zugewiesen wurde, übernimmt diese Aufgabe das Domain Name System (DNS).[37] DNS ist ein Hintergrund-Dienst des Internets, der über ein hierarchisches System über das Netz verteilter DNS-Server realisiert wird.[38]

DNS-Server werden in erster Linie – aber nicht nur – von den ISPs betrieben und erfüllen eine Funktion die mit der eines Telefonbuchs vergleichbar ist. Der Nutzer muss sich nur den Domain-Namen merken und in seinen Web-Browser eingeben. Der Browser nutzt einen auf dem lokalen Computer im Hintergrund arbeitenden sogenannten Stub Resolver, um einen DNS-Server zu fragen, welche IP-Adresse momentan zu dieser Domain gehört. Der Stub Resolver übernimmt dabei die Rolle des Clients. Er kennt die IP-Adresse des nächstgelegenen DNS-Servers entweder dadurch, dass der Nutzer diese manuell eingegeben hat, oder aber die Adresse wurde automatisch in den Einstellungen des Netzwerks konfiguriert. Nachdem der Server mit der zum Domain-Namen zugehörigen IP-Adresse geantwortet hat, leitet der Stub Resolver diese (ungeprüft!) an den Browser weiter, der

---

[36] Ein Beispiel für eine IP-Adresse ist etwa 192.168.1.100; mehr zur Funktion von IP-Adressen unten Kap. 1 III 2 (S. 18).
[37] *Jung-Weiser* in: Fezer u.a., Lauterkeitsrecht, Bd. 1, S 11 Rn. 3.
[38] *Badach/Hoffmann*, Technik der IP-Netze, 5 (S. 231 f.); Jung-Weiser in: Fezer u.a., Lauterkeitsrecht, Bd. 1, S 11 Rn. 4.

nun den entsprechenden Web-Server über die mitgeteilte IP-Adresse anspricht.[39] Beim Nutzer wird so die angeforderte Seite im Browser aufgerufen, in aller Regel ohne dass er etwas von diesem technischen Vorgang mitbekommt.

Bei dem Schritt der Übermittlung der IP-Adresse vom DNS-Server an den Nutzer setzt die DNS-Sperre an. Bei der DNS-Sperre ändert der ISP bei seinem DNS-Server die dem Domain-Namen des zu sperrenden Angebots zugeordnete IP-Adresse. Dies kann – wie im soeben dargestellten Fall – die IP-Adresse einer beliebigen Internet-Seite sein; dann handelt es sich um eine Umleitung. Oder aber es wird gar keine IP-Adresse gesendet; in dem Fall handelt es sich um eine Sperre. Das Resultat ist in beiden Fällen, dass der Nutzer über den DNS-Server des ISP keinen Zugriff mehr auf die gesperrte Website hat. Gibt er den Domain-Namen ein, wird er entweder umgeleitet oder bekommt eine Fehlermeldung.[40]

Wie die Deep Packet Inspection nutzt die DNS-Sperre Daten aus der Anwendungsschicht im TCP/IP-System. Der Unterschied ist weniger ein rein technischer als ein inhaltlicher. Domain-Namen werden seit der Existenz des World Wide Web an den ISP gesendet und dort verarbeitet. Es ist also nicht neu, dass der Provider Daten seiner Nutzer verarbeitet, die dieser in der Anwendungsschicht seiner Datenpakete versendet. Entscheidend für die hier vertretene Abgrenzung ist, dass der Nutzer, wenn er eine IP-Adresse vom DNS-Server des Providers abfragt, weiß und möchte, dass der ISP den Inhalt seiner Anwendungsschicht zur Kenntnis nimmt. Er schickt die Nutz-Daten – also den Domain-Namen – explizit an den DNS-Server als Empfangsrechner. Der Empfangsrechner ist aber in den meisten denkbaren Fällen als die Stelle bestimmt, die die Daten der Anwendungsschicht auslesen und verarbeiten soll. Die Kenntnisnahme selbst und die Verarbeitung im Rahmen dessen, was der Nutzer vom Server explizit erfragt, sind insoweit rechtlich unproblematisch. Komplizierter wird es erst, wenn der Provider in Daten hineinschaut, ohne dass der Nutzer diese an den ISP als Empfänger gesendet hat (dies wäre dann eine Deep Packet Inspection) und/oder der Provider die Daten anders verarbeitet, als der Nutzer (wenn auch nur implizit) erbeten hat. Der letztere Fall liegt auch bei einer DNS-Sperre vor. Anstatt der IP-Adresse, die er erbeten hat, bekommt der Nutzer eine andere oder gar keine Adresse geliefert.

Die Anwendung von DNS-Sperren war in Deutschland bereits einmal geltendes Recht in Form des Zugangserschwerungsgesetzes (ZugErschwG) von 2010. [41] Dieses wurde jedoch bereits 2011 wieder aufgehoben. Das ZugErschwG sollte dafür Sorge tragen, dass Internet-Nutzern der Besuch von Webseiten mit kinderpornographischem Material verwehrt wird.[42] Gemäß § 1 Abs. 1 Satz 1 ZugErschwG sollte das Bundeskriminalamt eine Liste

---

[39] Vgl. weitergehend *Badach/Hoffmann*, Technik der IP-Netze, 5.1 (S. 232 ff.).
[40] *Pfitzmann u.a.*, Sperrverfügungen, S. 52.
[41] Gesetz zur Aufhebung von Sperrregelungen bei der Bekämpfung von Kinderpornographie in Kommunikationsnetzen.
[42] Intensiv mit den grundrechtlichen und technischen Implikationen des Zugangserschwerungsgesetzes setzt sich *Heliosch*, Sperrmaßnahmen im Internet auseinander.

mit ihm bekannten Internet-Seiten mit kinderpornographischem Material führen. Diese Liste sollte die Domain, die IP-Adresse und die URL des Telemedienangebots enthalten. § 2 Abs. 2 ZugErschwerG bestimmte, dass die größeren Internet Service Provider den Zugang zu dem Angebot für ihre Nutzer sperren mussten, nachdem diese Liste ihnen übermittelt wurde.[43] Sie durften dazu die drei genannten Daten verwenden,[44] sollten aber auf jeden Fall verhindern, dass die Eingabe der Domain-Namen in die zugehörige IP-Adresse aufgelöst wird. Stattdessen sollte der Nutzer auf eine dritte Seite umgeleitet werden, die einen Hinweis auf die eingerichtete Netzsperre enthält.

DNS-Sperren wurden aber bereits vor dem Inkrafttreten des ZugErschwG mehrfach in Deutschland auf öffentliche Anordnung von Providern installiert. So erließ die Bezirksregierung Düsseldorf bereits 2002 eine Anordnung an die ISPs in Nordrhein-Westfalen, den Zugang zu bestimmten rechtsextremen Internet-Angeboten in den USA mittels DNS-Sperre zu unterbinden. Diese Sperrverfügung wurde durch das VG Düsseldorf als rechtmäßig bestätigt.[45]

Des Weiteren wurde dem ISP Arcor vom LG Frankfurt a.M. 2007 in Form einer einstweiligen Verfügung aufgetragen, gegen den Internet-Pornographie-Anbieter „YouPorn" eine DNS-Sperre einzurichten.[46] Die Verfügung wurde allerdings im folgenden Hauptsacheverfahren wieder aufgehoben.[47]

2. IP-Sperren

Unter einer IP-Sperre (eigentlich: IP-Adress-Sperre) wird im Rahmen dieser Arbeit verstanden, dass der Internet Service Provider nicht zulässt, dass eine Datenverbindung zwischen einem Nutzer und einem Server hergestellt wird, der ein Angebot beherbergt, welches gesperrt werden soll. Dies gewährleistet der ISP, indem er die Weiterleitung von Datenverkehr mit der IP-Adresse des Servers verweigert.

Die IP-Adresse ist die technische Adresse eines Internet-Angebots. Sie enthält die Routing-Informationen, um das Angebot auf dem entfernten Rechner ansprechen zu können. Jedes Datenpaket im Internet enthält eine solche Adresse, damit die Betreiber der Netzinfrastruktur wissen, an welchen Rechner das Datenpaket zuzustellen ist. Die IP-Adressen von Sender und Empfänger liegen in der Internet-Schicht. Der ISP schaut also jedes Mal, wenn ein Datenpaket durch einen seiner Router transportiert wird, in dieses Paket hinein. Dies ist denklogisch unumgänglich, da ansonsten das Paket nicht zugestellt werden könnte.

Bei einer IP-Sperre registriert der ISP über eine zusätzliche Software an seinen Routern, wenn ein Datenpaket an den oder von dem Server gesendet wird, auf dem Inhalte liegen,

---

[43] *Hoffmann*, Die digitale Dimension der Grundrechte, S. 159.
[44] Die Domain, die IP-Adresse und die *URL*.
[45] VG Düsseldorf, Urt. v. 10.05.2005, 27 K 5968/02, CR 2005, 885 (885).
[46] LG Frankfurt, Beschl. v. 17.10.2007, 2/6 O 477/07, Rn. 27 (jurion).
[47] LG Frankfurt, Urt. v. 08.12.2008, 3-12 O 171/07, CR 2008, 536 (536).

die gesperrt werden sollen. Inhalt dieses Datenpakets kann z.B. eine Anfrage an den Server sein, die Daten einer Website für deren Anzeige im Internet-Browser zu senden. Statt der Webseite soll der Nutzer bei einer IP-Sperre jedoch nur eine Fehlermeldung erhalten, da der ISP bereits die Anfrage nicht an den Server gesendet hat.

Die IP-Sperre eignet sich in erster Linie dazu, Datenverkehr im World Wide Web zu unterbinden und weniger bzw. überhaupt nicht für andere Anwendungen wie beispielsweise Peer-to-Peer-Netzwerke. Ähnlich wie bei den DNS-Sperren und anders als bei einer Löschungsanordnung des Angebots gegen den Host-Provider ist die IP-Sperre dabei allerdings unabhängig vom Standort des Servers, auf dem die zu sperrenden Inhalte gespeichert sind, wirksam.

Aus rechtlicher Sicht ist bei der IP-Sperre allerdings zu beachten, dass hinter einer IP-Adresse bisweilen nicht nur ein einziges Angebot steckt. Oftmals werden von einem Host-Provider, also einem Anbieter von Server-Infrastruktur zum Betrieb eines Internet-Angebots wie einer Webseite, auf ein und demselben Server mehrere Angebote bereitgestellt, die ansonsten weder bezüglich ihres Inhalts noch bezüglich des Content Providers miteinander zu tun haben. Dies liegt daran, dass es wirtschaftlich sinnvoll ist, die vorhandenen Serverkapazitäten voll auszulasten. Wird eine IP-Adresse geblockt, unter der mehrere Angebote zu erreichen sind, hat das zur Folge, dass auch diejenigen Angebote geblockt werden, auf die es dem Regulierer gar nicht ankam.

Bei der IP-Sperre schaut der ISP in das Datenpaket hinein. Es handelt sich dennoch nicht um einen Fall der Deep Packet Inspection. Die IP-Adresse, die für eine IP-Sperre ausgelesen werden muss, befindet sich in der Internet-Schicht des Datenpakets, also keiner tiefen Schicht.[48] Das hat zur Folge, dass der technische Aufwand, um die Internet-Schicht auszulesen, geringer ist, als wenn der ISP in tiefere Schicht vordringen müsste. Zudem berührt das Auslesen der IP-Adresse im Gegensatz zu einer Deep Packet Inspection in der Regel weniger sensible Daten.

3. Deep Packet Inspection

Die Erläuterung der Deep Packet Inspection erfordert eine ausführlichere Darstellung als die von DNS- oder IP-Sperren. Wie bereits oben im Kap. 1 I erklärt, besteht der Datenverkehr im Internet aus vielen einzelnen Paketen, und die eigentlichen Nutzdaten werden in vier Schichten verpackt, die sich wiederum nach dem TCP/IP-Referenzmodell richten.[49] Bei den Schichten handelt es sich um die Netzzugangs-, die Internet-, die Transport- und die Anwendungsschicht. Da es zwischen den beiden Endpunkten der Internet-Kommunikation keine direkte physische Leitung gibt, durchlaufen die Datenpakete auf ihrem Weg zum Bestimmungsort auch spezialisierte Rechner der ISPs, die sogenannten Router, die die Informationen der IP-Header in der Internet-Schicht auswerten und die Pakete dann entsprechend weiterleiten. An diesen Netzwerkknoten können aber auch Hard- und Softwarelösungen der ISPs ansetzen, die Deep Packet Inspection möglich machen. Anstatt

---

[48] Vgl. *Greiner*, CR 2002, 620 (623).
[49] Siehe oben Kap. 1 I (S. 2 ff.).

lediglich den IP-Header auszulesen, nutzen diese Lösungen auch andere, tiefer liegende Daten des Pakets.

a. „Deep“

Um die Nutzdaten transportieren zu können, muss der Router des ISP nicht tiefer schauen als bis in die zweite Schicht, die Internet-Schicht. Hier befinden sich die Routing-Informationen. Sie sind – vereinfacht gesagt – Empfänger und Adressat der Daten (in Form von IP-Adressen). Zwei Schichten tiefer liegen die Protokolle, die den Kommunikationsablauf zwischen den Programmen auf Nutzer- und Server-Seite regeln, und der *Payload*. Dazwischen liegt die Transportschicht, in der u.a. die Ports festgelegt werden, über die sich die Programme auf Sender- und Empfängerseite austauschen.[50] Die beteiligten Programme verwenden dabei oft Standard-Ports (jedoch nicht immer). Da sich die Standard-Ports mit einiger Wahrscheinlichkeit bestimmten Anwendungen zuordnen lassen, kann man aus dieser Information gegebenenfalls Rückschlüsse auf die Art der Nutzdaten schließen, ohne diese selbst untersucht haben zu müssen.

Ob bereits das Hineinschauen in die Transportschicht als Deep Packet Inspection anzusehen ist, ist daher umstritten. Teilweise wird die DPI als die Aktivität einer Netzwerk-Hardware definiert, die keinen Endpunkt eines Kommunikationsvorgangs darstellt und andere Daten als die Empfänger-IP-Adresse der Internet-Schicht verwendet, unabhängig vom damit verfolgten Zweck.[51] Damit stellt er in den Vordergrund, dass der ISP für seine klassische Aufgabe des Routings nicht unbedingt mehr Informationen sammeln müsse als die Zieladresse des Pakets. Alles was darüber hinausgehe, müsse daher als *deep* bezeichnet werden.

Parsons hingegen differenziert zwischen Shallow, Medium und Deep Packet Inspection.[52] Shallow Packet Inspection dringt lediglich bis zur Internet-Schicht des Datenpakets vor und ist auf Header-Informationen beschränkt. Damit ist allerdings keine Einschränkung dahingehend verbunden, dass die bei der Shallow Packet Inspection (SPI) gesammelten Daten nur für Routing-Zwecke verwendet werden dürften. Der ISP kann beispielsweise die IP-Adressdaten sowie die Anzahl an Paketen der von dieser IP-Adresse gesendeten Nachricht dazu verwenden, über eine nachträgliche statistische Auswertung eine IP-

---

[50] Siehe oben Kap. 1 I 4 (S. 8).

[51] *Bowman*, Presentation to the Canadian Radio-television and Telecommunications Commission, 2009, S. 5, abrufbar unter http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1241688.doc (zuletzt besucht am 09.10.2021); so auch *Reed*, What Your Broadband Provider Knows About Your Webuse: Deep Packet Inspection and Communications Laws and Policies, 2008, S. 61 ff., abrufbar unter https://www.govinfo.gov/content/pkg/CHRG-110hhrg58071/html/CHRG-110hhrg58071.htm (zuletzt besucht am 09.10.2021).

[52] *Parsons*, Deep Packet Inspection in Perspective: Tracing its lineage and surveillance potentials, 2008, S. 5 ff., abrufbar unter https://qspace.library.queensu.ca/bitstream/handle/1974/1939/WP_Deep_Packet_Inspection_Parsons_Jan_2008.pdf (zuletzt besucht am 09.10.2021).

Blacklist zu erstellen, um eine IP-Sperre einzurichten.[53] Medium Packet Inspection (MPI) soll sich hingegen auf eine Paketuntersuchung bis weit hinein in die Anwendungsschicht beziehen und damit auch die Transportschicht umfassen. Die MPI nach der Definition Parsons wirft einen Blick auf alle Daten des Pakets – lediglich der Payload ist für die MPI tabu.[54] Deep Packet Inspection schließlich umfasse alle Schichten des Pakets inklusive der Nutzdaten.[55]

Einen kontextabhängigen Ansatz wählt hingegen *Cooper*. Sie definiert die DPI als die Sammlung, Beobachtung, Analyse und/oder die Speicherung von Daten, die sich oberhalb der Internet-Schicht befinden und in Beziehung zu einer Anwendung stehen.[56] Nach dieser Definition ist also die Beobachtung und Verarbeitung von Daten der Internet-Schicht nie, die der Anwendungsschicht und der Transportschicht stets dann Deep Packet Inspection, wenn aus den entsprechenden Daten der Transportschicht Rückschlüsse auf den materiellen Inhalt oder die Verwendung der Nutzdaten gezogen werden können.

Dieser Streit ist für die in dieser Arbeit behandelten Fragen nicht ohne Relevanz. Das Wort *deep* (= tief) hat hier doppelte Bewandtnis, nämlich eine technische und eine rechtliche. Technisch gesehen ist die Packet Inspection tiefer, je weiter man im TCP/IP-Referenzmodell nach unten vordringt. Es lässt sich dabei vom Wortlaut her sowohl mit *Bowman* und *Reed* argumentieren, dass man von *tief* sprechen kann, sobald man den Datenverkehr *tiefer* als für den klassischen Zweck der Paketweiterleitung notwendig betrachtet.[57] Ebenso gut lässt sich aus technischer Perspektive vertreten, dass *tief* erst dann erreicht ist, wenn man in der untersten Schicht, der Anwendungsschicht, angelangt ist.

Parsons sieht schließlich erst dann eine DPI verwirklicht, wenn die Nutzdaten selbst betroffen sind. Dies schließt die Möglichkeit ein, dass die Informationen des *Headers* der

---

[53] *Parsons*, Deep Packet Inspection in Perspective: Tracing its lineage and surveillance potentials, 2008, S. 6, abrufbar unter https://qspace.library.queensu.ca/bitstream/handle/1974/1939/WP_Deep_Packet_Inspection_Parsons_Jan_2008.pdf (zuletzt besucht am 09.10.2021).

[54] *Parsons*, Deep Packet Inspection in Perspective: Tracing its lineage and surveillance potentials, 2008, S. 7, abrufbar unter https://qspace.library.queensu.ca/bitstream/handle/1974/1939/WP_Deep_Packet_Inspection_Parsons_Jan_2008.pdf (zuletzt besucht am 09.10.2021).

[55] *Parsons*, Deep Packet Inspection in Perspective: Tracing its lineage and surveillance potentials, 2008, S. 8, abrufbar unter https://qspace.library.queensu.ca/bitstream/handle/1974/1939/WP_Deep_Packet_Inspection_Parsons_Jan_2008.pdf (zuletzt besucht am 09.10.2021).

[56] *Cooper*, DPI Dance, in: *Aspray/Doti*, Privacy in America, S. 139 (145).

[57] *Bowman*, Presentation to the Canadian Radio-television and Telecommunications Commission, 2009, S. 5, abrufbar unter http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1241688.doc; *Reed*, What Your Broadband Provider Knows About Your Webuse: Deep Packet Inspection and Communications Laws and Policies, 2008, S. 61 ff., abrufbar unter https://www.govinfo.gov/content/pkg/CHRG-110hhrg58071/html/CHRG-110hhrg58071.htm (zuletzt besucht am 09.10.2021).

Anwendungsschicht untersucht werden, ohne dass es sich um eine Deep Packet Inspection handeln würde.[58]

Cooper hingegen wählt eine eher rechtliche Perspektive, indem sie das Kriterium der Anwendungsbezogenheit in ihre Definition der DPI aufnimmt. Dahinter steht die Überlegung, dass Deep Packet Inspection am ehesten dann eine persönlichkeitsrechtliche Relevanz entwickelt, wenn Informationen über den materiellen Gehalt der Kommunikation werden. Die Untersuchung persönlichkeitsrechtlich irrelevanter Daten solle unabhängig von der technischen Tiefe nicht als *deep* bezeichnet werden.[59] *Cooper* stellt somit nicht die technische Tiefe, sondern die Sensibilität der verarbeiteten Informationen in den Vordergrund.

Die Bezeichnung *deep* besitzt in diesem Kontext also nicht nur einen technischen Aspekt, nämlich die Tiefe des Eindringens der Untersuchung im TCP/IP-Schichtenmodell, sondern auch einen materiellen Aspekt, nämlich den Umfang und die Sensibilität der potentiell zu erlangenden Informationen.

Durch eine Analyse des Payloads, der sich ebenfalls in der Anwendungsschicht befinden, kann derjenige, der die Untersuchung durchführt, den vollständigen Inhalt der Kommunikation beobachten und auswerten. Es ist offensichtlich, dass dadurch sensible Daten der Netznutzer Gegenstand der Datenverarbeitung werden können, die Untersuchung also materiell *tief* wäre. Wie sensibel diese Informationen im Einzelfall sind, hängt maßgeblich vom Inhalt der Kommunikation ab. Der materielle Inhalt der Kommunikation kann im Extremfall intimer Natur sein, oder aber keinen Informationsgehalt besitzen, der über die aus einer Analyse der Internet- und Transportschicht hinausginge. Betrachtet der Provider die Daten des Headers der Anwendungsschicht, kann er anhand der verwendeten Protokolle (z.B. HTTP für das World Wide Web, POP3/SMTP/IMAP für E-Mail) die Art des Datenverkehrs sicher identifizieren, welche er auf Grundlage der Informationen aus Internet- und Transportschicht nur vermuten konnte.

Auch die Daten in der Transportschicht können über die Art des Datenverkehrs viel aussagen, etwa welches Programm oder welchen Dienst der Nutzer verwendet, sei es E-Mail, Internet-Telefonie oder Filesharing. In Bezug auf Filesharing-Netze war beispielsweise bekannt, dass die Programme Morpheus und Kazaa standardmäßig den TCP-Port 1214 nutzten, eDonkey hingegen 4661 und 4662. Insbesondere in Verbindung mit den Daten, die der Provider ohnehin schon aus der Internet-Schicht kennt, also der IP-Adresse des Senders und des Adressaten, sowie dem Übertragungsprotokoll (TCP oder UDP) aus der Transport-Schicht, formt sich ein Paket an Meta-Daten, aus denen der Provider einige Informationen über den Kommunikationsvorgang und die daran Beteiligten erfahren

---

[58] *Parsons*, Deep Packet Inspection in Perspective: Tracing its lineage and surveillance potentials, 2008, S. 8, abrufbar unter https://qspace.library.queensu.ca/bitstream/handle/1974/1939/WP_Deep_Packet_Inspection_Parsons_Jan_2008.pdf (zuletzt besucht am 09.10.2021).

[59] *Cooper*, DPI Dance, in: *Aspray/Doti*, Privacy in America, S. 139 (143).

kann.[60] Die potentiell zu erlangenden Informationen aus der Untersuchung sind also rückgekoppelt an die Tiefe der Schichten. Dies gilt jedoch nur unter Einschränkungen. So ist die Zuverlässigkeit einer Datenverkehrsanalyse unter Einbeziehung von Port-Nummern Einschränkungen unterworfen. Denn Ports können manuell oder automatisch geändert werden, so dass sie nicht mehr den Standard-Port-Nummern entsprechen. Manche Ports sind zudem doppelt belegt. Den verwendeten Ports kommt für den ISP, der die Datenpakete untersucht, also eher die Bedeutung von Indizien zu.[61] Wird dieser Fakt ignoriert und werden auf Grundlage von Port-Nummern datenverkehrsregulierende Maßnahmen ergriffen, besteht stets eine große Gefahr von Overblocking durch „false positives", also der unbeabsichtigten Sperrung von Daten und Kommunikationsvorgängen.[62]

Bereits die Erfassung und Verarbeitung von Verkehrsdaten[63] aus der Internet-Schicht kann sensible Informationen zum Gegenstand haben, insbesondere wenn diese Daten mit anderen Daten verknüpft werden. Aus Verkehrsdaten, die über einige Zeit gesammelt wurden und sich einer konkreten Person zuordnen lassen, können beispielsweise sehr exakte Soziogramme gebildet werden.[64]

Daraus folgt, dass die Sensibilität der Informationen, die eine Untersuchung von Datenpaketen durch den ISP aufwirft, nicht nur von der technischen Tiefe der Untersuchung, sondern auch nicht unerheblich vom tatsächlichen materiellen Inhalt der Datenpakete und dem Kontext der Kommunikation abhängt. Die technische Tiefe der Untersuchung über die Internet-Schicht hinaus kann danach sowohl einen qualitativen, einen bloß quantitativen oder überhaupt keinen Unterschied hinsichtlich der Sensibilität ausmachen.

Allerdings lässt sich ein abstrakter Unterschied ausmachen zwischen einer Datenverkehrsuntersuchung der Internet-Schicht auf der einen Seite und der Untersuchung der Transport- und der Anwendungsschicht auf der anderen Seite. Die Auswertung der Routing-Informationen der Internet-Schicht ist denknotwendige Voraussetzung für die Vermittlung der Kommunikation über das Internet und wird bei jedem Datenübertragungsvorgang durchgeführt. Sie sollte daher nicht als *tief* bezeichnet werden. Auch wenn diese Auswertung nicht per se frei davon ist, potentiell sensible Informationen zu verarbeiten, so ergibt sich dennoch aus der Tatsache, dass die Auswertung der Informationen der In-

---

[60] *Stalla-Bourdillon u.a.*, CLSR 2014, 670 (670).
[61] Port-basierte Klassifizierung von Datenverkehr erreicht laut diversen Studien nur eine geringe Genauigkeit: *Aceto u.a.*, PortLoad: Taking the Best of Two Worlds in Traffic Classification, in: 2010 INFOCOM – IEEE Conference on Computer Communications Workshops, S. 3: 24 Prozent; *Moore/Papagiannaki*, Toward the Accurate Identification of Network Applications, in: *Dovrolis*, Passive and Active Network Measurement, S. 41 (49): 30 Prozent.
[62] Zur rechtlichen Problematik von Overblocking mehr im weiteren Verlauf dieser Arbeit.
[63] Verkehrsdaten sind gemäß der Legaldefinition des § 3 Nr. 30 TKG „Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden".
[64] Vgl. BVerfG, Urt. v. 02.03.2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Vorratsdatenspeicherung, BVerfGE 125, 260 (318 f.).

ternet-Schicht die Kommunikation erst ermöglicht, ein qualitativer Unterschied zur Untersuchung der tieferen Schichten. Letztere ist, selbst wenn gute Gründe für eine solche vorliegen sollten, ist keine Grundvoraussetzung der Kommunikation.

Eine Untersuchung der Transport- und der Anwendungsschicht hingegen ist technisch zur Datenübermittlung nicht zwingend, und erlaubt in beiden Fällen jedoch potentiell – wenn auch oft mit Abstufungen – die Verarbeitung sensibler Informationen. Daher ist es wenig sinnvoll, im vorliegenden Kontext begrifflich zu unterscheiden, ob die Paketuntersuchung lediglich die Anwendungsschicht oder auch die Transportschicht miteinschließt. Auf der Basis der technischen Tiefe ist insoweit keine abschließende Aussage über die Sensibilität der verarbeiteten Informationen zu erwarten.

Tief bedeutet daher im Kontext dieser Arbeit, dass sie technisch tiefer als zum Aufbau und zur Aufrechterhaltung einer Telekommunikationsverbindung notwendig vordringt und potentiell sensible Informationen zum Gegenstand haben kann. Um eine Deep Packet Inspection handelt es sich folglich immer dann, wenn eine Untersuchung der Header und/oder des Payloads der Transport- oder der Anwendungsschicht stattfindet.[65] Diese Definition ähnelt daher den technisch begründeten Definitionen von *Bowman* oder *Reed*.[66]

Die Definition von *Cooper* überzeugt aus dieser Perspektive hingegen nicht. Die Definition der Deep Packet Inspection nach *Cooper* ist dazu geeignet, eine konkrete Paketuntersuchung im Nachhinein rechtlich einzuordnen und dabei den Unterschied zwischen einer persönlichkeitsrechtlich relevanten und einer in dieser Hinsicht weniger problematischen Untersuchung zu bezeichnen. Will man den Begriff der Deep Packet Inspection jedoch für eine abstrakte Bewertung der Zulässigkeit einer Maßnahme der Datenverkehrsregulierung verwenden, ist er in dieser Form nicht hilfreich. Die Anwendungsbezogenheit bestimmter untersuchter Daten wird schließlich erst offenkundig, nachdem diese Daten bereits untersucht wurden. Für die Entscheidung, ob und wie tief ein ISP ein Paket untersuchen darf, dass nicht bereits untersucht wurde, ist eine Prognoseentscheidung erforderlich, die von einer potentiellen, nicht von einer tatsächlichen Betroffenheit von Persönlichkeitsrechten ausgeht. Die *potentielle* persönlichkeitsrechtliche Relevanz lässt sich hingegen durchaus *ex ante* anhand der technischen Tiefe ablesen.

Schließlich ist noch auf die Bedeutung des Ortes des Auslesens der Information hinzuweisen. *Bowman* berücksichtigt dies in seiner Definition, wenn er davon spricht, dass DPI

---

[65] Erhellend zu diesem Argument ist ein Blick auf die einfachgesetzlich Regelung des § 96 TKG, insbesondere dessen ersten beiden Absätze: Abs. 1 erlaubt die Verarbeitung von Daten, die zum "*Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung*" notwendig sind, um Telekommunikationsverbindungen aufzubauen. Abs. 2 hingegen verbietet deren Verarbeitung zu anderen Zwecken.

[66] *Bowman*, Presentation to the Canadian Radio-television and Telecommunications Commission, 2009, S. 5, abrufbar unter http://www.crtc.gc.ca/public/part-vii/2008/8646/c12_200815400/1241688.doc (zuletzt besucht am 09.10.2021); *Reed*, What Your Broadband Provider Knows About Your Webuse: Deep Packet Inspection and Communications Laws and Policies, 2008, S. 61 ff., abrufbar unter https://www.govinfo.gov/content/pkg/CHRG-110hhrg58071/html/CHRG-110hhrg58071.htm (zuletzt besucht am 09.10.2021).

nur dort in Erscheinung tritt, wo es sich nicht um einen „Endpunkt eines Kommunikationsvorgangs“ handelt.[67] Er meint damit, dass der Rechner, an den ein Datenpaket adressiert ist, dieses vollständig auslesen muss, um seinen Inhalt nutzen zu können. Es ergibt nämlich wenig Sinn, beispielsweise einer anderen Person eine E-Mail zu schicken, und das Speichern und die Anzeige des Textes beim Empfänger als DPI zu bezeichnen.

Um eine *tiefe* Untersuchung handelt es sich daher im Rahmen dieser Arbeit nur, wenn diese nicht bei der Kommunikationsgegenseite, sondern auf dem Übermittlungsweg – im Internet – erfolgt.

b. „Packet Inspection“

Auch wenn der Begriff der „Inspection“ (dt. in etwa „Untersuchung“ oder „Besichtigung“) nahelegt, dass es bei der DPI nur darum geht, den Inhalt der Datenpakete zu erkunden, beschränkt sich die Bedeutung des Begriffs nicht nur auf den Vorgang des Auslesens bzw. der Erhebung der Daten. Dies liegt in erster Linie daran, dass die Erlangung von Informationen bei Echtzeit-Anwendungen wie der DPI solange keinen Mehrwert darstellt, wie man die Informationen nicht verwendet. Dementsprechend werden DPI-Technologien von ihren Anbietern oft als Komplettlösungen verkauft, die dem Kunden neben der reinen Untersuchung des Datenstroms eine breite Palette an weitergehender Datenverarbeitung liefern. Diese Dienste beinhalten etwa die Sammlung, Speicherung, Auswertung, Modifikation und veränderte Weiterleitung der Daten.[68] Letztlich bestehen für die weitere Verarbeitung der einmal gewonnenen Daten keine absoluten technischen Hürden. Die theoretischen Möglichkeiten sind insoweit nicht beschränkter als die der Datenverarbeitung allgemein.[69] Deshalb bietet es sich nicht an, die Definition bezüglich der weiteren Verwendung der Daten einzuschränken. Der Begriff der DPI soll daher im Rahmen dieser Arbeit sowohl die Erhebung als auch jedwede weitere Verarbeitung der Paketdaten beschreiben.

Die Untersuchung und Klassifizierung erfolgt mit unterschiedlichen Verfahren. Welches Verfahren im Einzelfall zur Anwendung kommt, hängt davon ab, welche Daten die konkrete DPI-Anwendung benötigt, wie der zu untersuchende Datenverkehr strukturiert ist und welchem Zweck die DPI dienen soll.

Beim sogenannten 5-Tupel-Verfahren analysiert der ISP Daten aus den Internet- und Transportschichten, die Anwendungsschicht bleibt hingegen unangetastet. Konkret handelt es sich bei den analysierten Daten um die IP-Adresse und den Port des Absenders,

---

[67] *Bowman*, Presentation to the Canadian Radio-television and Telecommunications Commission, 2009, S. 5, abrufbar unter http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1241688.doc (zuletzt besucht am 09.10.2021).

[68] ipoque, Product portfolio, abrufbar unter https://www.ipoque.com/products, (zuletzt besucht am 09.10.2021).

[69] *Reed*, What Your Broadband Provider Knows About Your Webuse: Deep Packet Inspection and Communications Laws and Policies, 2008, S. 61 ff., https://www.govinfo.gov/content/pkg/CHRG-110hhrg58071/html/CHRG-110hhrg58071.htm (zuletzt besucht am 09.10.2021).

die IP-Adresse und den Port des Empfängers sowie das verwendete Transportprotokoll (TCP oder UDP).[70]

Ein anderes Verfahren zur Datenanalyse wirft einen Blick auf den Header der Anwendungsschicht, um die dort verwendeten Protokolle auszuwerten und bestimmten Anwendungen zuzuordnen. Diese Form der Analyse ist in gewisser Weise die Verfeinerung der Analyse mittels des 5-Tupels. Der ISP kann die Daten des Headers der Anwendungsschicht nutzen, um die konkrete Web-Anwendung, zu der der Datenverkehr gehört, genau zu identifizieren.

Für genauere Erkenntnisse über die verwendete Anwendung kann der ISP zudem die Daten des Headers der Anwendungsschicht auslesen.

Auch bei der Untersuchung der Nutzdaten kann der ISP aus verschiedenen Verfahren wählen. Diese lassen sich grob in zwei verschiedene Klassen einteilen. Bei der „klassischen" Variante liest das Filtersystem die Anwendungsschicht eines Datenpakets (bzw. einen Datenstrom) vollständig oder teilweise aus, analysiert die Daten, klassifiziert sie und ergreift entsprechend des Ergebnisses die programmierte Maßnahme. [71] Diese Vorgehensweise erlaubt die genaue Identifizierung und Klassifizierung der durchgeleiteten Daten, wenn diese gegen in der Datenbank der ISPs abgelegte Datenmuster abgeglichen werden. Dazu werden jedoch eine Menge Datenverarbeitungs-Ressourcen benötigt, und der Aufwand, die Datenmuster aktuell zu halten, erfordert großen Aufwand. [72]

Die Alternative zum Abgleich der Nutzdaten mit einer Datenbank besteht darin, den Datenstrom auf statistische Muster hin zu untersuchen, die genaue Rückschlüsse auf die Art der untersuchten Daten zulassen. Die Nutzdaten und der Aufbau der Pakete der Flows verschiedener Web-Anwendungen haben eine charakteristische Signatur, die präzise Rückschlüsse auf die Art des Datenverkehrs zulässt (heuristische Analyse).[73]

c. Zusammenfassende Definition

Führt man die soeben gewonnen Einsichten zusammen, lässt sich die Deep Packet Inspection aus der Perspektive, die dieser Arbeit zugrunde liegt, definieren als

---

[70] *Köhnen u.a.*, Enhancements to Statistical Protocol IDentification (SPID) for Self-Organised QoS in LANs, in: 2010 Proceedings of 19th ICCCN, S. 1 (2).

[71] *Królikowski*, Packet Inspection, in: Telemedicus Soko 2014, S. 141, 145; *Dreger u.a.*, Network Intrusion Detection, in: Proceedings of the 15th Conference on USENIX Security Symposium, 2006, S. 257 (259).

[72] *Hjelmvik/John*, Breaking and Improving Protocol Obfuscation, 2010, S. 4, abrufbar unter https://www.iis.se/docs/hjelmvik_breaking.pdf (zuletzt besucht am 09.10.2021).

[73] *Hjelmvik/John*, Breaking and Improving Protocol Obfuscation, 2010, S. 5, abrufbar unter https://www.iis.se/docs/hjelmvik_breaking.pdf (zuletzt besucht am 09.10.2021). Zu den charakteristischen Eigenschaften der Datenpakete, die sich zur Analyse heranziehen lassen, zählen etwa die Paketlänge, die zeitlichen Abstände der Pakete oder die ersten Bits der Nutzdaten; *Crotti u.a.*, SIGCOMM Comput. Commun. Rev. 2007, 5 (9); *Sen u.a.*, Accurate, Scalable In-network Identification of P2P Traffic Using Application Signatures, in: Proceedings of the 13th International Conference on World Wide Web 2004, 2004, S. 512 (513 f.).

das Auslesen und/oder die anderweitige elektronische Verarbeitung über das Internet gesendeter Daten, die innerhalb der Transport- und der Anwendungsschicht des TCP/IP-Referenzsystems liegen, wobei die Untersuchung auf dem Übertragungsweg über das Internet stattfindet.

d. Etablierte Anwendungsformen der DPI

Um die beinahe universelle Einsetzbarkeit und herausragende Flexibilität der DPI zu belegen, soll im Folgenden eine Übersicht über die bereits etablierten Anwendungsformen der DPI gegeben werden, ohne dass diese Anspruch auf Vollständigkeit erheben könnte.

Zwar bewegt sich die DPI in Anbetracht ihrer Einsatzmöglichkeiten und ihres Wirkungspotential weiterhin weitgehend außerhalb des Blickfelds des öffentlichen Diskurses.[74] Das bedeutet jedoch nicht, dass sich Datenverkehrsüberwachung und -diskriminierung erst in jüngster Zeit entwickelt hätten. Deren Anfänge reichen zurück bis zu den ersten Firewalls.[75] Mittlerweile haben sich die Anwendungsfelder jedoch bedeutend vermehrt. Damit einhergehend beginnen Politik[76] und Forschung[77] sich nunmehr vermehrt für die Thematik der Datenverkehrsklassifizierung zu interessieren, was dazu führt, dass ein gewisses Maß an Transparenz bezüglich der DPI-Praktiken der ISPs erreicht wurde.

Es liegt in der technischen Beschaffenheit der Deep Packet Inspection begründet, dass diese weitgehend ohne Kenntnis des Nutzers von statten geht, da sie im Herrschaftsbereich der ISPs durchgeführt und der Nutzer nicht von der Durchführung benachrichtigt wird.[78] Um an Informationen über dieses Verhalten der ISPs zu gelangen, sind dritte Stellen weitgehend auf – teilweise freiwillige – Angaben der Provider angewiesen.[79] Weitere

---

[74] Die öffentliche Debatte findet in erster Linie im Zusammenhang mit den Enthüllungen *Edward Snowdens* oder der ordnungsrechtlichen Diskussion zur Netzneutralität statt, ohne dass dabei in der Regel der Begriff der Deep Packet Inspection fällt.

[75] *Ingham / Forrest*, A history and survey of network firewalls,
A history and survey of network firewalls, in: The University of New Mexico Computer Science Department Technical Report 2002–37, 2002, S. 1 (4), abrufbar unter http://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf (zuletzt besucht am 09.10.2021).

[76] Exemplarisch für die Vereinigten Staaten; *Reed*, What Your Broadband Provider Knows About Your Webuse: Deep Packet Inspection and Communications Laws and Policies, 2008, abrufbar unter https://www.govinfo.gov/content/pkg/CHRG-110hhrg58071/html/CHRG-110hhrg58071.htm (zuletzt besucht am 09.10.2021); für die Europäische Union: BEREC, BEREC findings on traffic management practices in Europe, BoR (12) 30, 2012, abrufbar unter https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/45-berec-findings-on-traffic-management-pra_0.pdf (zuletzt besucht am 09.10.2021).

[77] Eine Erhebung über die Entwicklung der jährlich veröffentlichten Arbeiten (in englischer Sprache) von 1991 – 2009 findet sich bei *Dainotti u.a.*, IEEE Network 2012, 35 (36).

[78] *Cooper*, DPI Dance, in: *Aspray / Doti*, Privacy in America, S. 139 (149).

[79] Vgl. etwa BEREC, BEREC findings on traffic management practices in Europe, S. 4 f, BoR (12) 30, 2012, abrufbar unter http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/45-berec-findings-on-traffic-management-practices-in-europe (zuletzt besucht am 09.10.2021).

mehr oder weniger allgemein zugängliche Informationsquellen stellen die Produktbeschreibungen der Hersteller von DPI-Lösungen dar, wobei eine systematische wissenschaftliche Auswertung dieser Quellen bislang fehlt.

(1) Netzwerksicherheit

DPI-Lösungen wurden ursprünglich entwickelt, um die Netzwerksicherheit zu erhöhen. Mit dem Aufkommen der ersten über das Internet übertragenen Schad-Software entstand eine Nachfrage nach Lösungen, die vor Schad-Software schützen kann. Solche Vorsichtsmaßnahmen waren bereits Ende der 1980er Jahre notwendig, wie der Morris-Virus bewies.[80] Eine Lösung des Problems war, Firewalls zu entwickeln.[81] Firewalls sind im IT-Kontext virtuelleSchutzwände, die verhindern sollen, dass Schadsoftware in das lokale Netzwerk eindringt oder Daten stiehlt.

Eine Firewall untersucht beispielsweise eingehende Datenpakete auf Anzeichen, dass diese Viren oder ähnliches enthalten könnten. Sie lässt die Daten nur dann in das lokale Netzwerk oder den Rechner des Endnutzers, wenn dies nach seinen vorprogrammierten Regeln sinnvoll erscheint. Firewalls können auch ausgehenden Datenverkehr des Nutzers blocken, wenn etwa lokal installierte Programme unbefugt Daten nach außen senden.

Damit Firewalls diese Aufgaben bewältigen können, untersuchen sie die Datenpakete auf Informationen, ob es sich um zulässigen oder unzulässigen Datenverkehr handelt.[82] Diese Untersuchung kann je nach Konfiguration und Produkt sehr simpel auf der Ebene der Internet-Schicht geschehen, jedoch auch sehr aufwendig in der Anwendungsschicht bis hin zu einer Inspektion der Nutzdaten.[83] Klassischerweise sind Firewalls hingegen nicht beim ISP, sondern beim Nutzer eingerichtet.[84] Damit fallen sie nicht unter die hier verwendete Definition von Deep Packet Inspection.

Heutzutage wird jedoch ein bedeutender Teil der Netzwerksicherheitsfunktionen, die früher allein lokalen Firewalls vorbehalten war, auf der Ebene der Internet Service Provider geleistet. Europäische ISPs etwa gaben 2012 an, dass sie E-Mail-Spam blocken, indem sie Datenpakete aus bestimmten Quellen aussortieren, wenn dieser die Port-Nummer 25 (SMTP) enthält.[85] Auch in anderen Fällen von Netzwerkattacken, zum Beispiel Denial-of-

---

[80] Eine Chronologie findet sich bei *Spafford*, The internet worm incident, in: *Ghezzi/McDermid*, ESEC '89, S. 446 (446 f.).

[81] *Eichin/Rochlis*, With microscope and tweezers, in: IEEE Symposium on Security and Privacy 1989 Proceedings, 1989, S. 331 f.

[82] Für eine technisch präzisere Einführung in die Funktionsweise einer Firewall vgl. Ingham/Forrest, A history and survey of network firewalls, in: The University of New Mexico Computer Science Department Technical Report 2002-37, 2002, S. 1 (2 ff.), abrufbar unter http://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf (zuletzt besucht am 09.10.2021).

[83] *Stalla-Bourdillon u.a.*, CLSR 2014, 670 (673 ff.).

[84] *Eichin/Rochlis*, With microscope and tweezers, in: IEEE Symposium on Security and Privacy 1989 Proceedings, 1989, S. 331.

[85] BEREC, BEREC findings on traffic management practices in Europe, S. 9, BoR (12) 30, 2012, abrufbar unter http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/45-berec-findings-on-traffic-management-practices-in-europe (zuletzt besucht am 09.10.2021).

Service-Angriffen (DoS-Attacken) oder dem heimlichen Unterschieben von Viren, wird der Datenverkehr aus verdächtigen Quellen per DPI untersucht und gegebenenfalls unterbunden.[86]

(2) Traffic Management

Internet-Bandbreite ist eine begrenzte Ressource. Über eine spezifische Leitung kann zeitgleich nur eine bestimmte Menge an Daten übertragen werden. Der Datenverkehr steigt jedoch, und der Ausbau der Netzinfrastruktur ist teuer. Es kommt daher vor, dass die Nachfrage nach Übertragungskapazität das Angebot an manchen Orten übersteigt. In diesen Fällen staut sich der Datenverkehr. Läuft sinnbildlich der Zwischenspeicher der Router der Internet Service Provider über, kommt es zu Datenverlusten.

In früheren Zeiten wurden bei Aufkommen eines Datenstaus alle Datenpakete von den ISPs grundsätzlich gleichbehandelt. Eine Priorisierung bestimmten Datenverkehrs fand nicht statt (striktes Best-Effort-Prinzip). Das Netz war insoweit *neutral*.[87] Dies war letztlich eine technische Konsequenz aus dem sogenannten End-to-end-Grundsatz, nach dem die Aufgabe des Netzes lediglich das Routing des Datenverkehrs sein sollte. Um Datenverluste und Verzögerungen der Übertragung möglichst zu vermeiden, greifen eine Vielzahl an Protokollen in der Netzzugangs-, der Internet- und der Transportschicht ein.[88] Gegenüber der Art der transportierten Daten sollte das Netz hingegen „dumm" bleiben.[89]

Seit dem Aufkommen der DPI sind die Funktionen des Netzes allerdings nicht mehr auf das Routing beschränkt. Das Internet kann Datenverkehr nun nach seiner Art und Herkunft diskriminieren. Bei Datenstau können die ISPs den Datenverkehr klassifizieren und entsprechend der Anwendung oder der Art der übertragenen Daten priorisieren. Dies bringt gewisse Vorteile mit sich. Es gibt Datenverkehr, der auf konstant hohe Datenraten mehr angewiesen ist als anderer. So drosseln die Internet Service Provider z.B. durch DPI als Peer-to-Peer-Verkehr identifizierte Daten, da bei Peer-to-Peer-Kommunikation große

---

[86] BEREC, BEREC Report on differentiation practices and related competition issues in the scope of net neutrality, BoR (12) 132, 2012, S. 28, abrufbar unter http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/1094-berec-report-on-differentiation-practices-and-related-competition-issues-in-the-scope-of-net-neutrality (zuletzt besucht am 09.10.2021); *Bedner*, Rechtmäßigkeit der „Deep Packet Inspection", 2009, S. 9, abrufbar unter https://kobra.bibliothek.uni-kassel.de/bitstream/urn:nbn:de:hebis:34-2009113031192/5/BednerDeepPacketInspection.pdf (zuletzt besucht am 09.10.2021).

[87] Der Begriff „network neutrality" wurde von Tim Wu und Lawrence Lessig gemeinsam geprägt und in einer wissenschaftliche Publikation wohl erstmalig in *Wu*, JTHTL 2003, 141 (145) definiert als das Internet, das eine Anwendung nicht gegenüber der anderen bevorzugt (dort auch mit weiteren Hinweisen auf die Entwicklung des Begriffs). Die exakte Definition des Begriffs ist nicht unumstritten. Ausreichend ist hier die Definition von Wu, da der Themenkreis der Netzneutralität von dieser Arbeit zwar berührt wird, aber an dieser Stelle nicht die (auch sehr interessanten) wettbewerblichen Fragen der Netzneutralität aufgeworfen werden, die eine exakte Definition erfordern würden. Einen Überblick über den Streitstand zur Definition bietet *Read*, IJLIT 2012, 48 (52 f.).

[88] Eine Übersicht der zur diversen Verfahren zur Behebung von Überlastproblemen findet sich bei *Meinel/Sack*, Internetworking, 7.2.5 (S. 506 ff.).

[89] *Daly*, IJCLP 14 (2011), S. 1 (3); *Saltzer u.a.*, End-to-End Arguments in System Design, in: *Partridge*, Innovations in Internetworking, 1988, S. 195 (202).

Datenmengen mit tendenziell geringerer Dringlichkeit übertragen werden.[90] Davon können dann andere Dienste wie Internet-Telefonie (VoIP) profitieren, die nur einen geringen Datenhunger aufweisen, dafür aber sehr zeitkritisch sind.[91]

Es ist von einigen europäischen ISPs bekannt, dass sie entsprechende „intelligente" Maßnahmen gegen Datenstaus ergreifen, bei einer unbekannten Dunkelziffer.[92] Die technische Infrastruktur, um Datenverkehr anwendungsspezifisch zu priorisieren, ist folglich auch hierzulande bereits verbreitet.

(3) Spezial-Dienste

Eine weitere Anwendung der DPI ist die Bevorzugung von spezifischen Diensten, denen gegen Entgelt abweichend vom Best-Effort-Grundsatz eine höhere Priorität eingeräumt wird als anderen Diensten. Bereits vor der Etablierung der DPI konnte eine Anwendung einem Datenpaket im TOS/DS-Feld des Internet-Headers eine Anforderung an eine bestimmte Dienstequalität mitgeben. Stimmt der Netzbetreiber der Anforderung zu, wird das Paket entsprechend mit garantierter oder erhöhter Qualität übertragen.[93]

Die Möglichkeit, das TOS/DS-Feld mit Daten zu versehen, haben die Host-Anwendungen nicht exklusiv. Auch die Netzbetreiber können das TOS/DS-Feld verändern und somit die Priorität des Dienstes manipulieren. Die Deep Packet Inspection erlaubt es den ISPs, den Datenverkehr nicht nur nach seiner Herkunft, sondern auch seinem Inhalt nach zu überwachen, spezifische Dienste zu identifizieren und in der Folge zu bevorzugen oder zu benachteiligen.[94] Dieses Verhalten ist insbesondere aus wettbewerbspolitischen Gründen

---

[90] BEREC, BEREC Report on differentiation practices and related competition issues in the scope of net neutrality, BoR (12) 132, 2012, S. 29, abrufbar unter http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/1094-berec-report-on-differentiation-practices-and-related-competition-issues-in-the-scope-of-net-neutrality (zuletzt besucht am 09.10.2021).

[91] *Cooper*, DPI Dance, in: *Aspray/Doti*, Privacy in America, S. 139 (150); *Bedner*, Rechtmäßigkeit der „Deep Packet Inspection", 2009, S. 10, abrufbar unter https://kobra.bibliothek.uni-kassel.de/bitstream/urn:nbn:de:hebis:34-2009113031192/5/BednerDeepPacketInspection.pdf (zuletzt besucht am 09.10.2021).

[92] BEREC, BEREC findings on traffic management practices in Europe, BoR (12) 30, 2012, S. 9, abrufbar unter http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/45-berec-findings-on-traffic-management-practices-in-europe (zuletzt besucht am 09.10.2021).

[93] *Meinel/Sack*, Internetworking, 7.2.6 (S. 512 ff.).

[94] BEREC, BEREC findings on traffic management practices in Europe, BoR (12) 30, 2012, S. 11, abrufbar unter http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/45-berec-findings-on-traffic-management-practices-in-europe (zuletzt besucht am 09.10.2021).

hoch umstritten.[95] Die Netzneutralität zu durchbrechen ist dennoch auch in Europa verbreitet.[96] Mittlerweile wurden auf europäischer (und auf US-amerikanischer) Seite daher mehr oder weniger restriktive Verbote solcher Diskriminierungen verabschiedet.[97]

(4) Blocken und Drosseln von Diensten

Ebenfalls aus wettbewerbspolitischen, aber auch aus informationspolitischen Gründen umstritten sind Praktiken der ISPs, gewisse Dienste per DPI zu identifizieren und dann aus betriebswirtschaftlichen Gründen zu drosseln oder ganz zu blocken. Technisch ist der Vorgang mit der soeben beschriebenen Praxis bei den Spezial-Diensten zu vergleichen. Anwendung findet diese etwa bei Peer-to-Peer-Datenverkehr, um die Datenlast des Netzes zu reduzieren und so Investitionen in den Netzausbau vermeiden zu können. So sperrte der US-amerikanische ISP Comcast mittels Deep Packet Inspection für seine Nutzer Peer-to-Peer-Datenverkehr, ehe ihm dies von der amerikanischen Telekommunikationsaufsichtsbehörde FCC (Federal Communications Commission) mit der Begründung untersagt wurde, der Provider würde seine Nutzer von der Ausübung ihres Rechts abhalten, auf legale Inhalte des Internets zuzugreifen.[98] VoIP-Dienste wurden allerdings auch in Europa regelmäßig im mobilen Datennetz gesperrt, um die Geschäfte der ISPs mit der mobilen Telefonie zu schützen.[99]

(5) Effektivere Werbemaßnahmen

DPI kann genutzt werden, um den Datenverkehr der Nutzer zu analysieren, Nutzerprofile zu erstellen und diese Informationen dann werbetreibenden Dritten zur Verfügung zu stellen. Die DPI erfüllt dann eine ähnliche Funktion wie Cookies, nur ungleich effektiver.[100] Der Unterschied besteht allerdings darin, dass Nutzer über Cookies, die lokal gespeichert werden, Kontrolle ausüben können, wenn sie möchten. Auf DPI haben sie deutlich weniger Einwirkungsmöglichkeiten. Diese DPI-Anwendung wurde beispielsweise im Vereinigten Königreich ausprobiert.[101]

---

[95] Für eine Einführung in die Problematik s. etwa *Görisch*, EuZW 2012, 494; *Hahn/Wallsten*, The Economics of Net Neutrality, 2006, abrufbar unter https://doi.org/10.2202/1553-3832.1194 (zuletzt besucht am 09.10.2021); *Hogendorn*, IEEP 2007, 185; *Wu*, Network Neutrality: Competition, Innovation, and Nondiscriminatory Access, 2006, abrufbar unter https://dx.doi.org/10.2139/ssrn.903118 (zuletzt besucht am 09.10.2021).

[96] BEREC, BEREC findings on traffic management practices in Europe, BoR (12) 30, 2012, S. 11 ff., abrufbar unter https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/45-berec-findings-on-traffic-management-pra_0.pdf (zuletzt besucht am 09.10.2021).

[97] manager magazine Redaktion, Obama votiert gegen Überholspur im Netz, in: manager magazin online, 11.11.2014, abrufbar unter https://www.manager-magazin.de/politik/artikel/obama-votiert-gegen-ueberholspur-im-netz-a-1002167.html (zuletzt besucht am 09.10.2021).

[98] FCC, Pressemitteilung vom 04. August 2008, 2008, abrufbar unter https://transition.fcc.gov/Daily_Releases/Daily_Digest/2008/dd080804.html (zuletzt besucht am 09.10.2021).

[99] *BEREC*, BEREC findings on traffic management practices in Europe, BoR (12) 30, 2012, Abb. 5, abrufbar unter https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/45-berec-findings-on-traffic-management-practices-in-europe (zuletzt besucht am 09.10.2021).

[100] *Cooper*, DPI Dance, in: *Aspray/Doti*, Privacy in America, S. (139) 151.

[101] *Clayton*, The Phorm "Webwise" System, 2008, abrufbar unter https://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf (zuletzt besucht am 09.10.2021).

(6) Repressive Maßnahmen

Wenn ein Provider mittels DPI ermittelt hat, dass ein bestimmter Telekommunikationsvorgang eine unerlaubte Handlung darstellt, kann er diese Informationen verwenden, um repressive Maßnahmen gegen den Sender oder den Empfänger der Daten einzuleiten. Er kann die Ergebnisse seiner Datenverkehrsanalyse beispielsweise an Ermittlungsbehörden weiterleiten. Diese könnten dann rechtliche Schritte gegen den Betreiber des Angebots, etwa einen Filehoster, oder aber gegen den Empfänger der Daten einleiten. Denkbar wäre auch, dass es zu staatsanwaltlichen Ermittlungsverfahren gegen die Kommunikationsteilnehmer kommt, zu behördlichen Warnhinweisen wie in Frankreich zwischen 2009 und 2013 unter dem Hadopi-Gesetz[102] oder zu zivilrechtlicher Verfolgung durch die Inhaber verletzter Rechte.

(7) Inhaltsfilterung

Schließlich kann es zur Filterung und Manipulation unerwünschten Datenverkehrs auf Veranlassung durch dritte Stellen kommen. Am Beispiel des Urheberrechts bedeutet dies, dass Datenverkehr, der eine Urheberrechtsverletzung beinhaltet, durch Untersuchung des Datenstroms zunächst identifiziert wird, um den Datenverkehr in der Folge zu blocken. In Belgien beispielsweise wurde bereits versucht, ein solches Filtersystem per gerichtlicher Anordnung durchzusetzen.[103]

IV. Effektivität von Datenverkehrseingriffen in der Durchsetzung des Urheberrechts

Wie soeben dargestellt, eignen sich datenverkehrsregulierende Maßnahmen grundsätzlich dazu, Datenübertragungen über das Internet zu manipulieren oder zu verhindern. Würden diese bei Filesharing-Vorgängen angewandt, sei es bereits im Vorfeld durch Verhinderung des öffentlichen Zugänglichmachens oder direkt während des Übermittlungsvorgangs, könnten so gegebenenfalls Verletzungen des Urheberrechts verhindert oder unterbunden werden.[104] Da datenverkehrsregulierende Maßnahmen in erster Linie deshalb diskutiert werden, um eine effektivere Rechtsdurchsetzung zu ermöglichen, ist es geboten, sich mit der Effektivität dieser Maßnahmen gesondert auseinanderzusetzen. Nach einem Blick auf bestehende Durchsetzungsdefizite im Internet wird der Begriff der „Effektivität" im Kontext der Urheberrechtsdurchsetzung im Internet konkretisiert. Schließlich werden die oben[105] dargestellten Methoden der Datenverkehrsregulierung auf ihre Effektivität hin untersucht. .

---

[102] Vgl. das französische Gesetz LOI n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet.

[103] Vgl. EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 15 ff.

[104] Dies ist zumindest die Hoffnung des europäischen Gesetzgebers, die in Erwägungsgrund 59 der Richtlinie 2001/29/EG (InfoSoc-Richtlinie) zum Ausdruck kommt: Die Intermediäre sollen in Anbetracht der Durchsetzungsschwierigkeiten des Urheberrechts im digitalen Raum stärker in die Verantwortung genommen werden.

[105] Siehe oben Kap. 1 III 1–3 (S. 16 ff.).

1. Durchsetzungsdefizite

Je nach technischer Erscheinungsform illegalen Filesharings können aus unterschiedlichen Gründen Durchsetzungsdefizite auftreten. Unterschiedliche Dateitypen werden über diverse informationstechnische Protokolle ausgetauscht. Geschützte Werke werden zudem von zentralen wie dezentralen Speichern aus illegal verteilt.[106]

a. Filehoster

Eine beliebte Möglichkeit des Filesharings ist der Austausch über sogenannte „Filehoster".[107] Eine belastbare Aussage über das Ausmaß des illegalen Filesharings über Filehoster ist schwierig zu treffen. Die dazu veröffentlichten Informationen unterscheiden sich erheblich voneinander und sind potentiell von Interessen beeinflusst. Doch selbst bei den vorsichtigeren Schätzungen wird deutlich, dass Filesharing über Filehoster keine Randerscheinung ist. In einem gegen ihn geführten Rechtsstreit gab der damalige Marktführer Rapidshare den bei ihm gespeicherten Anteil rechtswidriger Dateien mit 5–6% an.[108]

Filehoster bieten geringe Zugangsschranken, eine hohe Skalierbarkeit der Größe der gespeicherten Daten und der durch die Anonymität von Up- und Downloadern resultierenden Probleme bei der Verfolgung von Urheberrechtsverletzungen.

Eine prägende Eigenschaft der Filehoster ist die Anonymität desjenigen, der die Filehoster-Plattform nutzt, um die fragliche Datei zum Abruf anzubieten. Beim Filesharing unter Benutzung von Filehostern findet keine direkte Datenübertragung zwischen Up- und Downloader statt.[109] Für die Vertreter der Rechteverwerter ist dies misslich, da sie die Identität der Uploader oft ermitteln, indem sie auf das Angebot zum Abruf des Uploaders eingehen, eine Datenverbindung etablieren und so die IP-Adresse des Rechteverletzers ermitteln. Da beim Filehosting allerdings der Filehoster als Instanz zwischengeschaltet ist, ist es daher nur für den Filehoster möglich, die IP-Adresse des Uploaders einzusehen. Der Filehoster hat aber kein Interesse daran, diese Information mit anderen zu teilen, so dass der Uploader letztlich anonym bleibt.[110]

b. Peer-to Peer-Netzwerke

Beim Filesharing über Peer-to-Peer-Netzwerke, bei dem eine Datenverbindung direkt zwischen Up- und Downloader etabliert wird und der Uploader sich sowohl gegenüber seinem Austauschpartner als auch gegenüber Dritten im Rahmen einer Dateisuche als Uploader der bestimmten Datei über seine IP-Adresse ausweist, ist der potentielle Rechteverletzer hingegen häufig identifizierbar, so dass eine Rechtsverfolgung grundsätzlich

---

[106] Bei den illegal geteilten geschützten Werken handelt es sich in erster Linie um Dateien, die Musik, Filme oder ausführbare Programme beinhalten, die über Filehoster oder aus dezentralen Peer-to-Peer-Netzwerken heruntergeladen werden.

[107] Filehoster (auch als „Sharehoster" bekannt) sind Anbieter großer Onlinefestplatten. Sie ermöglichen das anonyme Speichern und Abrufen großer Datenmengen von beliebigen Standorten.

[108] OLG Hamburg, v. 02.07.2008, 5 U 73/07, Rn. 165 (juris).

[109] *Gabriel/Albrecht*, ZUM 2010, 392 (392 f.).

[110] Vgl. dazu *Nietsch*, Anonymität und die Durchsetzung urheberrechtlicher Ansprüche im Internet, S. 239 ff.; *Röhl/Bosch*, NJW 2008, 1415 (1418).

möglich ist.[111] Seit Aussetzung der Vorratsdatenspeicherung in Deutschland durch das Bundesverfassungsgericht ist die Rechtsverfolgung in diesem Bereich allerdings erheblich erschwert, da die erforderlichen Daten, um eine IP-Adresse einem Anschlussinhaber zuzuordnen, von den Internet Service Providern in der Regel nicht mehr ausreichend lang vorgehalten werden. Die Anonymität des Datenverkehrs ist folglich zuletzt gestiegen. Daran hat sich *de facto* auch durch die ersatzweise von der Bundesregierung eingeführte „Höchstspeicherfrist" nichts geändert.[112]

c. Streaming

Rund um das Thema Filesharing werden auch illegale Streaming-Portale diskutiert, über die der Nutzer Filme abrufen und unmittelbar konsumieren kann, ohne dass er die dahinterstehenden Daten auf seinem Endgerät dauerhaft speichern muss. Zwar wurden bereits illegale Streaming-Seiten aufgrund staatlichen Eingreifens geschlossen, von einem flächendeckenden Vorgehen kann jedoch keine Rede sein. Die Lücke, die die Schließung der Portale hinterlassen hat, wurde schnell gefüllt.[113] Die Konsumenten der illegal gestreamten Werke bleiben zudem gegenüber Dritten – ähnlich wie beim technisch verwandten Filehosting – meist anonym, sieht man einmal von Ausnahmefällen ab.[114]

2. Definition der Effektivität

Es stellt sich die Frage, was „Effektivität der Durchsetzung des Urheberrechts" in diesem Kontext überhaupt bedeutet. Es bietet sich an, sich einer Antwort zunächst vom allgemeinen Verständnis des Wortes zu nähern. „Effektivität" wird von der Redaktion des Dudens mit „Wirksamkeit", „Durchschlagskraft" oder „Leistungsfähigkeit" umschrieben.[115] „Effektivität" beschreibt demnach also, wie erfolgreich eine bestimmte Maßnahme die mit ihr beabsichtigten Ziele zu erreichen in der Lage ist. Wie man dies allerdings bei Maßnahmen zur Durchsetzung des Urheberrechts bemisst, hängt entscheidend von der Perspektive ab, aus der man das Urheberrecht und die damit verfolgten Zwecke betrachtet.

Das Urheberrecht besitzt zwei Aspekte: einen persönlichkeitsrechtlichen und einen materiellen Aspekt. Fraglich ist daher, ob die Effektivität einer Datenverkehrsregulierung eher anhand der Wirksamkeit beim Schutz der ideellen oder beim Schutz der wirtschaftlichen Seite des Urheberrechts bewertet werden sollte. Denn dies kann zu unterschiedlichen Ergebnissen führen.

---

[111] *Röhl/Bosch*, NJW 2008, 1415 (1427).

[112] Es ist bislang ungeklärt, ob die Höchstspeicherfrist mit den Vorgaben des Europäischen Gerichtshofs (vgl. EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C-594/12, Digital Rights Ireland, EU:C:2014:238) oder des Bundesverfassungsgerichts (vgl. BVerfG, Urt. v. 02.03.2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Vorratsdatenspeicherung, BVerfGE 125, 260) vereinbar ist.

[113] Vgl. *Luis Aguiar u.a.*, Online Copyright Enforcement, Consumer Behavior, and Market Structure, 2015, S. 15, abrufbar unter https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/online-copyright-enforcement-consumer-behavior-and-market-structure (zuletzt besucht am 09.10.2021).

[114] heise online, Porno-Abmahnungen: Indizienkette zur IP-Adressen-Ermittlung verdichtet sich, 2013, abrufbar unter https://heise.de/-2065879 (zuletzt besucht am 09.10.2021).

[115] Dudenredaktion, Duden – Das Fremdwörterbuch, Suchwort „Effektivität", S. 287.

Sieht man den Schwerpunkt des Urheberrechts bei seinen persönlichkeitsrechtlichen Aspekten, so müsste es konsequenterweise darum gehen, die einzelne, konkret identifizierte urheberrechtsverletzende Handlung zu verhindern, selbst wenn dies keinen positiven wirtschaftlichen Effekt für den Rechteinhaber haben sollte. Denn dann ginge es nicht darum, einen ökonomischen Schaden abzuwenden, sondern vielmehr einen Schaden ideeller Natur. Die Abwendung eines wirtschaftlichen Schadens ist nicht immer deckungsgleich mit der Verhinderung einer Rechtsverletzung. Der ökonomische Effekt einer Datenverkehrsregulierung kann z.B. deshalb ausbleiben, weil die Maßnahme selbst mit nur geringem Aufwand umgangen werden kann. Oder, weil ein Filesharer die Möglichkeit haben könnte, ohne Weiteres auf andere, gleichwertige Angebote auszuweichen, die nicht von der Maßnahme betroffen sind. Die Abwendung eines wirtschaftlichen Schadens wäre aus dieser Perspektive nicht entscheidend. Wichtiger wäre es, dass eine bestimmte urheberrechtsverletzende Handlung abgestellt würde. Diese Abwendung einer Rechtsverletzung genügt sich selbst.[116]

Betrachtet man das Urheberrecht eher als ein ökonomisch-persönlichkeitsrechtsbezogenes Mischrecht und damit auch aus wirtschaftlicher Perspektive, müsste die Effektivität einer datenverkehrsregulierenden Maßnahme sich hauptsächlich daran messen lassen, wie erfolgreich sie Verletzungen des Urheberrechts an einem konkreten Schutzgegenstand insgesamt verringern würde. Eine Datenverkehrsregulierung zur Urheberrechtsdurchsetzung wäre danach also umso effektiver, je mehr Rechtsverletzungen sie insgesamt verhindern würde. Diese Perspektive lenkt den Blick im Schwerpunkt auf die wirtschaftlichen Aspekte. Der Fokus würde von der einzelnen Verletzungshandlung hin zum wirtschaftlich bedeutenden massenhaften illegalen Filesharings gelenkt. Berücksichtigt würden allerdings auch die persönlichkeitsrechtlichen Aspekte des Urheberrechts, da auf die Verringerung der rechtsverletzenden Handlungen abgestellt wird – und nicht lediglich auf den aus dem Recht am Schutzgegenstand zu erzielenden Erlös.

Ein rein wirtschaftlicher Blick auf das Urheberrecht würde die Effektivität hingegen nicht danach bewerten, ob und inwieweit Rechtsverletzungen verhindert werden, sondern allein unter dem Aspekt, wie stark der positive Effekt auf die wirtschaftliche Verwertbarkeit ist. Der Unterschied zu der soeben beschriebenen Perspektive käme dann zum Vorschein, wenn etwa Verletzungshandlungen durch die Datenverkehrsregulierung verhindert würden, dies jedoch der Verwertbarkeit des geschützten wirtschaftlichen Guts nicht helfen würde. Dies wäre beispielsweise der Fall, wenn die Rechtsverletzungen nur in solchen Fällen verhindert würden, in denen es ohnehin nicht zu einer wirtschaftlichen Verwertung durch den Urheber gekommen wäre.[117] Aus wohlfahrtsökonomischer Sicht hätte eine solche Datenverkehrsregulierung in diesem Fall nur nachteilige Folgen, da die Verbreitung eines öffentlichen Guts zu hohen Kosten (Infrastruktur und eingeschränkte Frei-

[116] In diesem Sinne: BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 47; *Finger/Conrath*, MMR 2016, 186 (187).
[117] Z.B. weil ein Werk in einem bestimmten regionalen Markt nicht verwertet wird.

heitsrechte) eingeschränkt würde, ohne dass dem Wohlfahrtsgewinne der Urheber (Einnahmen aus Verwertungsrechten) oder der Gesellschaft (etwa größeres Angebot an kulturellen Gütern durch Produktionsanreize beim Urheber) gegenüberstünden. Eine Datenverkehrsregulierung, die sich derart auswirken würde, könnte aus dieser streng ökonomischen Perspektive nicht als effektiv bezeichnet werden.[118]

Die beiden Aspekte des Urheberrechts werden in verschiedenen im Kontext dieser Arbeit relevanten Rechtsordnungen unterschiedlich gewichtet.

In der Rechtsprechung des EuGH wird das Urheberrecht primärrechtlich vorrangig als Teil des durch Art. 17 Satz 2 Charta geschützten geistigen Eigentums verstanden. Dies gilt insbesondere in Sachverhalten, in denen es um den effektiven Schutz des Urheberrechts gegen Filesharing geht.[119]

Im deutschen Verfassungsrecht werden die vermögensrechtlichen Aspekte des Urheberrechts durch Art. 14 Abs. 1 GG geschützt,[120] die urheberpersönlichkeitsrechtlichen Aspekte hingegen von Art. 2 Abs. 1, 1 Abs. 1 GG.[121] Das Bundesverfassungsgericht betont allerdings in der Regel den Schutz des Urheberrechts durch Art. 14 Abs. 1 GG, insbesondere auch in Filesharing-Sachverhalten.[122]

Das deutsche (einfachgesetzliche) Urheberrecht im Sinne des Urheberrechtsgesetzes ist ein einheitliches Recht, das sowohl die persönlichkeitsrechtlichen als auch die materiellen Interessen des Urhebers schützt (monistische Theorie). Dies ergibt sich bereits unmittelbar aus § 11 Satz 1 UrhG, ist aber auch im Schrifttum ganz herrschende Meinung. Beide Aspekte sind danach untrennbar miteinander verbunden.[123]

Einer rein wirtschaftlichen Betrachtung des Urheberrechts ist zugute zu halten, dass das Problem des massenhaften Filesharings, gegen das sich die datenverkehrsregulierenden Maßnahmen richten würden, im Schwerpunkt verwertungsrechtlicher Natur ist. Das Urheberrecht ist allerdings nach (kontinental-)europäischem Verständnis gerade keine rein verwertungsrechtliche Konstruktion, die sich aus ausschließlich wirtschaftlicher Perspek-

---

[118] Umgekehrt müsste eine DVR, die dazu führt, dass Rechtsverletzungen nicht – zumindest nicht repressiv, womöglich aber präventiv – verhindert werden, aber nichtsdestotrotz eine Steigerung der wirtschaftlichen Verwertbarkeit des Schutzguts bewirken, aus dieser Perspektive als effektiv bezeichnet werden.

[119] EuGH, Urt. v. 29.01.2008, Rs. C-275/06, Promusicae, Slg. 2008, I-00271, Rn. 61 ff.

[120] BVerfG, Nichtannahmebeschl. v. 17.11.2011, 1 BvR 1145/11, NJW 2012, 754 (756 f.); *Papier/Shirvani* in: Maunz/Dürig, Art. 14 GG Rn. 315 (Stand: 83. Erg.-Lfg, April 2018).

[121] BGH, Urt. .v. 26.11 1954, I ZR 266/52, Cosima Wagner, BGHZ 15, 249 (258); *Kreutzer*, Urheberrecht und Regelungsalternativen, Kap. 2 II B 1 (S. 166 f.), dort m.w.N.

[122] Vgl. BVerfG, Nichtannahmebeschl. v. 18.02.2019, 1 BvR 2556/17, NJW 2019, 1510 (1511); BVerfG, Nichtannahmebeschl. v. 17.11.2011, 1 BvR 1145/11, NJW 2012, 754 (756 f.).

[123] Vgl. nur *Loewenheim/Peifer* in: Loewenheim u.a., UrhG, § 11 Rn. 3; *Wiebe* in: Spindler/Schuster, Recht der elektronischen Medien, § 11 UrhG Rn. 1 f.; *Bullinger* in Wandtke/Bullinger, UrhG, § 11 Rn. 1 f., jeweils m.w.N.

tive bewerten ließe. Schon aus Gründen dogmatischer Kohärenz des Regulierungsgegenstands mit seinem Durchsetzungssystem ist eine rein wirtschaftliche Perspektive abzulehnen.

Eine rein persönlichkeitsrechtliche Perspektive ist ebenfalls bereits deshalb abzulehnen, weil sie ein zweiseitiges Problem nur einseitig betrachtet. Zudem verkennt sie, dass Filesharing in der Tat ein Problem mit verwertungsrechtlichem Schwerpunkt ist

Daher soll hier die „gemischte" Perspektive eingenommen werden, nach der sich die Effektivität daran messen lassen muss, inwieweit sie Verletzungen des Urheberrechts an einem konkreten Schutzgegenstand *insgesamt* verringert. Diese gemischte Perspektive besitzt zudem den Vorteil, dass sie im Einklang mit der dem deutschen Urheberrecht zugrunde liegenden monistischen Theorie steht und sich auch mit dem durch EuGH und Bundesverfassungsgericht gesetzten Schwerpunkt der vermögensrechtlichen Aspekte, insbesondere im Filesharing-Kontext, verträgt.

3. Effektivität der IP-Sperre

Bei der IP-Sperre lassen sich Umgehungsmöglichkeiten der Content Provider und solche der Nutzer unterscheiden. Beide betroffene Gruppen können ein Interesse an der Unwirksamkeit datenverkehrsregulierender Maßnahmen haben. Die Nutzer könnten auf die von ihnen gewünschten Inhalte zugreifen können wollen, die Content Provider ihre Inhalte an den Mann bringen. Zudem stellen sich unabhängig von aktiven Umgehungsbemühungen einige technische Probleme, die die Wirksamkeit von IP-Sperren herabsetzen können.

Ein solches technisches Problem besteht etwa beim überwiegend zum Filesharing verwendeten TCP-Protokoll. TCP-Verbindungen sind so konstruiert, dass unter diesem Protokoll versendete Daten den blockierten Pfaden bestmöglich auszuweichen versuchen. Werden Daten in einem Router aufgrund einer IP-Sperre nicht weitergeleitet, suchen diese daher einen alternativen Weg über andere Router.[124] Um zu funktionieren, müssten die IP-Sperren daher den Host- oder den Serverrechner „umzingeln", so dass für den Datenaustausch kein freier Weg zur Verfügung steht.

Eine mögliche Gegenmaßnahme der Content Provider macht es sich zunutze, dass Internet-Angebote unter mehreren IP-Adressen zu erreichen sein können („mirroring").[125] Ein solches Vorgehen ist in der Regel weniger durch staatliche Sperrmaßnahmen motiviert als durch Performanzgründe. Ist die Herkunft der Nutzerzugriffe auf einen Server weit über den Erdball verstreut, kann dies zu langsamen Verbindungen führen, je nachdem, wie weit der Nutzer sich vom Server entfernt befindet. Umgekehrt kann es die durchschnittlichen Zugriffszeiten für den Nutzer erheblich verkürzen, wenn der Server in dessen räumlichen Nähe ist. Um ein Angebot global schnell ausliefern zu können, halten manche Anbieter ihre Angebote daher auf mehreren Servern weltweit gespiegelt vor.

---

[124] *Heliosch*, Sperrmaßnahmen im Internet, S. 87; *Janssen*, Abweichendes Verhalten, S. 27.
[125] Zu den näheren technischen Hintergründen des „mirrorings" vgl. *Tanenbaum / Wetherall*, Computer Networks, 7.5.3 (S. 744 ff.).

Ein anderer häufiger Grund für das Betreiben dieser Spiegel-Server ist, dass das Angebot so häufig nachgefragt wird, dass ein einziger Server die Nachfrage nicht bedienen könnte. Ist ein Angebot unter mehreren IP-Adressen zu erreichen, ist es für eine effektive Sperre notwendig, alle IP-Adressen des Angebots zu sperren, was einen enormen administrativen Aufwand des ISP, der die Sperrung durchzuführen hätte, mit sich bringen würde. Eine Möglichkeit des Content Providers, dessen Angebote von einer Sperrmaßnahme betroffen sind, aus dieser unübersichtlichen Situation einen Vorteil zu ziehen, ist es, den Aufwand für den Internet Service Provider, der die IP-Sperre durchführt, zu erhöhen: Zieht der Content Provider mit seinem Angebot in kurzen Abständen von Server zu Server um, muss der ISP jedes Mal die IP-Adresse des Servers in seinem System anpassen, was zumindest zu Verzögerungen und Lücken in der Sperrmaßnahme führt.

Auch Nutzer können IP-Sperren umgehen, indem sie zunächst einem Virtual Private Network (VPN) beitreten, dessen Internet-Zugang von einem ISP vermittelt wird, der die fragliche IP-Sperre nicht implementiert hat. Greift der Nutzer nun per VPN auf den geblockten Server zu, bekommt dies der ISP des Nutzers auf herkömmlichem Wege nicht mit. Die IP-Adresse des geblockten Servers bleibt auf dem Weg innerhalb des VPN im Datenstrom des VPN verborgen. Sie wird nur auf dem Kommunikationsweg zwischen VPN und dem gesperrten Angebot nach außen sichtbar.

Für einen technisch nicht vorgebildeten Nutzer ist also durchaus ein wenig Aufwand nötig, eine IP-Sperre zu umgehen. Die Anforderungen sind allerdings nicht so hoch, dass der Nutzer manuell ein VPN konfigurieren können müsste. Im Netz gibt es leicht auffindbar kommerzielle Anbieter, die gegen geringes Entgelt Zugang zu einem VPN mit Internet-Zugang in verschiedenen Staaten bieten.

Eine Umgehungsmaßnahme, die mit der soeben geschilderten VPN-Methode verwandt ist, ist das sogenannte Tunneln über einen Proxy-Server. Dabei wird über eine auf dem Rechner des Nutzers installierte Client-Anwendung eine Verbindung mit einem entsprechenden Server im Internet aufgebaut. Der Trick besteht darin, dass die Tunnel-Software das vom ISP überwachte Protokoll – hier das IP-Protokoll – in einem anderen Protokoll versteckt, etwa dem HTTP in der Anwendungsschicht. In der vom ISP überwachten Internet-Schicht taucht die gesperrte IP-Adresse daher nicht auf, sondern nur die des Proxy-Servers. Die Kommunikation, die normalerweise zwischen Nutzer und gesperrtem Angebot stattfinden sollte, findet zwischen dem Proxy-Server und dem Angebot statt und wird dann über die getunnelte Verbindung an den Nutzer weitergeleitet.[126]

Unabhängig von etwaigen Umgehungsmaßnahmen leidet die Effektivität einer DVR mittels einer IP-Sperre ganz erheblich darunter, dass sie sich gegen den Anbieter der Inhalte richtet anstatt gegen die rechtswidrigen Inhalte selbst. Um ein neues Angebot zu sperren, muss dieses stets identifiziert und müssen entsprechende Maßnahmen ergriffen werden. Dies kann den Zugriff der Nutzer auf ebenjenes Angebot erschweren, hindert sie aber in

---

[126] *Pfitzmann u.a.*, Sperrverfügungen, S. 50 ff.

keiner Weise, auf andere Angebote mit den gleichen oder vergleichbaren Inhalten auszuweichen. Da die Kosten und die benötigte Zeit, um ein spezifisches Angebot neu online zu stellen, relativ gering sind, wird es in der Praxis kaum zu schaffen zu sein, gegen einen bedeutenden Teil der illegalen Angebote eine IP-Sperre einzurichten; viel weniger noch, diese Sperren aktuell zu halten.

Die Wirkungsweise von IP-Sperren ist zudem ihrer Natur nach auf einen bestimmten Teilbereich des Filesharings beschränkt. Sie richten sich nur gegen die Anbieter von statisch gehosteten Angeboten, die über das World Wide Web erreichbar sind. Gegen Filesharing-Angebote, die eine horizontalere und dezentralere Architektur verwenden (z.B. Peer-to-Peer-Netzwerke), sind IP-Sperren wirkungslos. Das hat mehrere Gründe. Dezentrale Tausch-Netzwerke sind nur dann durch IP-Sperren zu erreichen, wenn man die IP-Adressen zumindest eines großen Teils der Teilnehmer blocken würde. Zum einen wäre es unverhältnismäßig, wenn der Staat einen großen Anteil seiner Bürger dauerhaft von der Nutzung des Internets aussperren würde, nur um die Durchsetzung des Urheberrechts zu verbessern. Rein praktisch entstünde ein riesiger administrativer Aufwand aufgrund der schieren Masse an IP-Sperren, die nötig wäre, alle Nutzer zu sperren, die illegales Filesharing über Tauschbörsen betreiben.

Nicht zuletzt ist eine so global ansetzende IP-Sperre aber auch technisch nur schwer zu realisieren. Die IP-Adressen der meisten privaten Internet-Anschlüsse sind nicht statisch, sondern dynamisch.[127] Eine über den Tag hinaus wirksame IP-Sperre eines Nutzers müsste also ebenfalls dynamisch sein und mit der Vergabe der IP-Adresse an den zu sperrenden Nutzer synchronisiert sein. Bevor ein solcher Aufwand getrieben würde, wäre es allerdings einfacher, dem Nutzer gleich den Internet-Anschluss zu kündigen bzw. einen Anschluss zu verwehren, anstatt eine IP-Sperre zu einzurichten.

Wegen der leichten Umgehbarkeit und insbesondere der großen Lücken, die diese Form der Datenverkehrsregulierung dem illegalen Filesharing lässt, ist deren Effektivität gering. Zwar wird die konkrete Rechtsverletzung durch den gesperrten Anbieter erschwert und in manchen Fällen daher wohl auch verhindert, wenn der Nutzer sich nicht die Mühe machen möchte, die Sperre zu umgehen. Wie oben festgestellt wurde, kann dies jedoch nicht der hier angelegte Effektivitätsmaßstab sein.[128] Denn auch wenn die konkrete Rechtsverletzung des Anbieters im Einzelfall verhindert wird, werden die Rechtsverletzungen insgesamt am Schutzgut kaum verhindert, sondern im besten Fall zu einem anderen Anbieter hin verlagert.

4. Effektivität der DNS-Sperre

DNS-Sperren besitzen gegenüber anderen Ansätzen wie IP-Sperren oder dem Löschen des Angebots vom Server einige erhebliche Vorteile. Im Gegensatz zu einer Löschungsanordnung bezüglich des Angebots, auf dem dieses gehostet wird, kann sie auch dann einen

---

[127] Die IP-Adressen werden dem Anschluss in kurzen Abständen vom Internet Service Provider neu zugeordnet, so dass ein Anschluss-Inhaber keine „eigene" IP-Adresse besitzt. Vgl. oben S. 16.
[128] Vgl. oben Kap. 1 IV 2 (S. 37).

Zugriff auf das illegale Angebot verhindern, wenn der Server außerhalb des rechtlichen Einflussgebiets des Regulierers liegt.[129] Zudem ist einer DNS-Sperre wie die IP-Sperre durch einen einfachen Server-Umzug zu sabotieren.

Andererseits lassen sich DNS-Sperren mit geringem technischen Aufwand umgehen. Dazu bestehen mehrere Möglichkeiten, die sowohl auf Seite der Nutzer als auch auf Seite der Content Provider liegen.

Die offensichtlichste Umgehungsvariante besteht darin, die technische Dienstleistung eines DNS-Servers gar nicht erst in Anspruch zu nehmen. Diese Umgehungsmöglichkeit setzt bei der Tatsache an, dass nicht das Angebot gelöscht oder der Datenverkehr zum Angebot als solcher gesperrt, sondern lediglich die Übersetzung des Domain-Namens in die IP-Adresse manipuliert wird. Das Angebot bleibt also für den Nutzer erreichbar, solange diesem die IP-Adresse des Angebots bekannt ist. Er gelangt dann ohne Umwege über den DNS-Server direkt auf das gewünschte Internet-Angebot, und die Sperre, die für ihre Wirksamkeit darauf angewiesen ist, dass der Nutzer ein manipuliertes Datenverarbeitungsergebnis des DNS-Servers ausgegeben bekommt, läuft ins Leere.[130]

Ein Hindernis ist es jedoch, dass man sehr genau wissen muss, nach welchem Angebot man sucht, um die entsprechende IP-Adresse einer Domain herauszufinden. Herkömmliche Suchmaschinen (wie Google, Bing etc.) schaffen hier jedoch einfach Abhilfe. Handelt es sich um ein populäres Angebot, wird die IP-Adresse des Angebots schnell auf dritten Seiten bekannt gemacht oder das Angebot direkt verlinkt. Die dritte Seite wird dann von Suchmaschinen indiziert, so dass der Nutzer den Domain-Namen des Angebots anstatt in das Adressfeld seines Browsers lediglich in die Suchmaske seiner bevorzugten Suchmaschine eingeben muss. Mit wenigen Mausklicks ist er dann wieder auf der Seite des gesperrten Angebots. Auch können nachträglich neue Domain-Namen registriert werden, die dann mit der IP-Adresse des zu sperrenden Angebots verknüpft werden. Im letzteren Fall ist die Seite einfach unter mehreren Domainnamen erreichbar.

Bei weniger bekannten Angeboten helfen dem Nutzer hingegen darauf spezialisierte Web-Angebote, die ebenfalls leicht über Suchmaschinen zu finden sind. Diese teilen dem Nutzer die zu einem bestimmten Domain-Namen zugehörige IP-Adresse mit, wenn man diesen in eine Eingabe-Maske innerhalb des Web-Angebots eingibt.[131]

Wollen Nutzer DNS-Sperren nachhaltig umgehen, können sie auf einen alternativen DNS-Server ausweichen, dessen Betreiber nicht zu Sperrmaßnahmen verpflichtet wurde. Access Provider betreiben in der Regel einen eigenen DNS-Server, so dass diese verpflichtet werden können, die DNS-Sperre auf diesen Servern zu implementieren und somit den Zugriff ihrer Kunden auf das zu sperrende Angebot zu unterbinden. Beschränkt sich der

---

[129] Vgl. zum Problem der Rechtsdurchsetzung in der globalisierten Welt des Internets *Schliesky u.a.*, Drittwirkung im Internet, S. 127 f.
[130] *Billmeier*, Düsseldorfer Sperrungsverfügung, S. 205; *Heliosch*, Sperrmaßnahmen im Internet, S. 84; *Stadler*, Haftung für Informationen, S. 183.
[131] Zum Beispiel XIP Tech UG, abrufbar unter https://IP-info.org (zuletzt besucht am 09.10.2021).

Nutzer auf den standardmäßig eingestellten DNS-Server seines Access Providers, kann dies zu einer relativ effektiven Sperre führen. Nicht alle DNS-Server werden jedoch von den ISP betrieben. Und durch die globale Struktur des Internets liegen auch nicht alle DNS-Server im rechtlichen Zugriffsbereich deutscher oder europäischer Behörden und Gerichte.[132] Es fehlt für die staatlichen Organisationen daher die rechtliche Handhabe, wirklich alle Betreiber von DNS-Servern zu DNS-Sperren zu verpflichten.

Ein ausreichend motivierter Nutzer kann daher die Netzsperre umgehen, indem er in den Netzwerkeinstellungen seines Betriebssystems oder seines Browsers den standardmäßig anzurufenden DNS-Server ändert.[133] Für Nutzer, denen dafür die technischen Kenntnisse noch fehlen, existieren im Internet eine Vielzahl an Schritt-für-Schritt-Anleitungen.[134] Diese Lösung zur Umgehung von DNS-Sperren ist lediglich mit einem geringen einmaligen Aufwand von allenfalls ein paar Minuten verbunden und nachhaltig.

Auch der Content Provider, dessen Angebot mit einer DNS-Sperre gesperrt werden soll, kann effektive Umgehungsmaßnahmen der Sperre ergreifen. So kann er beispielsweise die Domain einfach wechseln und sein Angebot unter einem anderen Domain-Namen veröffentlichen. Über einschlägige Portale Dritter oder Suchmaschinen wird der neue Domain-Name des Angebots in der Folge schnell bekannt.

Zudem besteht auch hier das gleiche Problem wie bei der IP-Sperre, nämlich, dass sich die Sperre gegen den Anbieter bzw. eine bestimmte Website und nicht gegen den zu sperrenden Inhalt richtet. Die Folge ist, dass der geneigte Nutzer problemlos auf andere, bislang nicht gesperrte Angebote ausweichen kann.[135]

Die DNS-Sperre ist in der Summe im Vergleich zur IP-Sperre noch etwas einfacher zu umgehen, erfordert dafür seitens des Internet Service Providers jedoch auch einen geringeren Aufwand. Die IP-Sperre muss regelmäßig angepasst werden, während die DNS-

---

[132] Diese öffentlichen, von Providern unabhängigen DNS-Server werden nicht etwa lediglich von Unternehmen betrieben, die in exotischen Staaten und rechtlichen Grauzonen operieren. Betreiber sind auch Unternehmen wie Google, Universitäten, NGOs etc. Der DNS-Server von Google ist etwa unter der Adresse 8.8.8.8 erreichbar, vgl. Google, Public DNS, abrufbar unter https://developers.google.com/speed/public-dns/ (zuletzt besucht am 09.10.2021). Die DNS-Server der Humboldt Universität zu Berlin sind unter den IP-Adressen 141.20.1.3, 141.20.1.31 und 141.20.2.3 zu finden, vgl. Humboldt Universität zu Berlin, Merkblatt HU-Account, abrufbar unter https://www.cms.hu-berlin.de/de/dl/beratung/antrag/merkblatt.html (zuletzt besucht am 09.10.2021). Selbst der Betrieb eines DNS-Servers in der eigenen Wohnung ist technisch und hinsichtlich der Kosten kein großer Aufwand, z.B. DNS-Server-Lösung von Synology, vgl. Synology, How to set up your domain with Synology DNS Server, abrufbar unter https://www.synology.com/en-global/knowledgebase/tutorials/584 (zuletzt besucht am 09.10.2021).

[133] *Koreng*, Zensur im Internet, S. 135.

[134] Nur die ersten beiden Ergebnisse der Google-Suche mit den Suchbegriffen „anleitung dns server ändern“: Microsoft Corporation, Ändern der TCP/IP-Einstellungen – Windows-Hilfe, 2017, abrufbar unter https://support.microsoft.com/de-de/help/15089/windows-change-tcp-ip-settings (zuletzt besucht am 09.10.2021); *Brack*, Internet beschleunigen: So konfiguriert ihr einen alternativen DNS-Server, in: netzwelt.de, 2019, abrufbar unter https://www.netzwelt.de/news/125241-internet-beschleunigen-so-konfiguriert-alternativen-dns-server.html (zuletzt besucht am 09.10.2021).

[135] Vgl. oben Kap. 1 IV 3 (S. 37 ff.).

Sperre oft nur einen einmaligen Aufwand vom ISP erfordert. Ein weiterer Unterschied besteht darin, dass die DNS-Sperre zielgenauer ist und nur die entsprechende Website sperrt. Dies ist bei der IP-Sperre nicht zwangsläufig der Fall. Hier können auch unbeabsichtigter Weise die Angebote Dritter als Kollateralschäden mitgesperrt werden.

Zudem ist der technisch mögliche Anwendungsbereich der DNS-Sperre noch etwas kleiner als der der IP-Sperre. DNS-Sperren können nur insoweit wirksam werden, wie die Internet-Anwendung auf das DNS-System zurückgreift, und dies ist in erster Linie im World Wide Web der Fall.

Insgesamt muss daher – wie bereits bei der IP-Sperre – festgestellt werden, dass die Effektivität der Datenverkehrsregulierung in der Form der DNS-Sperre gering ist.[136] Die Anzahl an Rechtsverletzungen durch einen gesperrten Anbieter werden gegebenenfalls verringert, die Anzahl an Rechtsverletzungen insgesamt am Schutzgut allerdings kaum, da die Nutzer der Sperre selbst sowie auch dem gesperrten Anbieter problemlos ausweichen können.

5. Effektivität der Deep Packet Inspection

Datenverkehrsregulierende Maßnahmen, die Filtersysteme verwenden, die auf einer Deep Packet Inspection basieren, sind wenig anfällig für diejenigen Umgehungsmaßnahmen, unter denen die Effektivität von IP- und DNS-Sperren leidet. Dies liegt daran, dass DPI-Filter aufgrund ihrer hohen Anforderungen an verfügbare Rechenleistung zwar aufwändiger zu installieren und zu betreiben sind, sie dafür aber bei den widerrechtlich übertragenen Daten selbst ansetzen. IP- und DNS-Sperren müssen hingegen mit den deutlich einfacher gehaltenen, aber in Bezug auf ihren Gehalt auch beschränkteren Informationen auskommen, die die oberen Schichten des TCP/IP-Systems ihnen zur Verfügung stellen können.

Unterschiedliche DPI-Maßnahmen ermöglichen eine unterschiedlich hohe Treffer-Rate bei der Identifikation urheberrechtswidrigen Datenverkehrs. In dieser Hinsicht weniger leistungsfähig ist das 5-Tupel-Verfahren. Obwohl nur wenige Daten mit auf den ersten Blick geringem Informationswert verarbeitet werden, kann auf diese Weise mit geringem Rechenaufwand bereits eine gewisse Klassifizierung des Datenverkehrs vorgenommen werden. Will der Internet Service Provider etwa Peer-to-Peer-Datenverkehr identifizieren und klassifizieren, reicht es womöglich aus, Internet- und Transportschicht auszulesen, da so bereits mit einiger Sicherheit auf die Art der Web-Anwendung geschlossen werden kann. Im Vergleich zum Zustand etwa bis Mitte der 00‘er Jahre hat die Genauigkeit einer Daten-Klassifizierung, die sich nur auf das 5-Tupel stützt, jedoch abgenommen.[137] Dies liegt vor allem daran, dass Ports heute von den Anwendungen oft nicht mehr so starr

---

[136] Vgl. oben Kap. 1 IV 3 (S. 39).

[137] *Cascarano u.a.*, An Experimental Violation of the Computational Cost of a DPI Traffic Classifier, in: IEEE Globecom 2009, 2009, S. 1.

verwendet werden wie früher, sondern die Anwendungen auf Host- und Server-Seite flexibel einen freien Port untereinander aushandeln.[138]

Die Analyse des Headers der Anwendungsschicht erlaubt ähnlich dem 5-Tupel-Verfahren die Ermittlung der Anwendung, für die das Datenpaket bestimmt ist. Daraus lassen sich mit einiger Wahrscheinlichkeit Indizien ableiten, dass es sich um urheberrechtswidrigen Datenverkehr handeln könnte. Die identifizierte Anwendung ist allerdings für den ISP lediglich ein Indiz. Auch wenn der ISP die Web-Anwendung zweifelsfrei identifiziert hat, lassen sich noch keine zweifelsfreien Aussagen darüber treffen, ob ein bestimmter Datenübertragungsvorgang das Urheberrecht verletzt, da auch Web-Anwendungen, die typischerweise für unerlaubtes Filesharing verwendet werden, für zulässige Datenübertragungen genutzt werden können. Genauso können Web-Anwendungen, über die üblicherweise urheberrechtlich unproblematische Datentransfers abgewickelt werden, sich zur Übertragung von Raubkopien eignen.

Will der Provider mit größerer Wahrscheinlichkeit wissen, welche Daten im Einzelfall übertragen werden, muss er den Payload selbst untersuchen und klassifizieren.

Gegenmaßnahmen wie Server-Umzüge oder Umbenennungen des Angebots, die bei IP- und DNS-Sperren wirksam sein können, laufen bei DPI-Filtern ins Leere, da diese nicht auf die Namen oder Adressen des Angebots angewiesen sind, um effektiv urheberrechtlich rechtswidrige Übertragungen zu identifizieren. Will man ein DPI-Filtersystem umgehen, muss man den Payload verschleiern. Auch eine Umbenennung der problematischen Dateien reicht in vielen Fällen nicht, da DPI-Filtersysteme sich nicht auf den Namen einer Datei verlassen müssen, sondern auch die spezifische Signatur einer Datei – vergleichbar mit einem digitalen „Fingerabdruck“ – zur Analyse heranziehen können.[139] Andere Verfahren ermöglichen sogar die Echtzeitanalyse des Datenverkehrs auf spezifische Audio-, Video-, Software- und Bild-Inhalte.[140]

Eine wirksame Maßnahme gegen eine Datenverkehrsregulierung mittels DPI kann hingegen in der Verschlüsselung der Kommunikation liegen. Die Logik dahinter ist, dass eine Untersuchung des Inhalts eines Datenpakets bzw. -stroms scheitern muss, wenn das Filtersystem die Nutzdaten nicht interpretieren kann. Zu unterscheiden sind hier die Form der Verbindungsverschlüsselung (engl. *link encryption*) und die der Ende-zu-Ende-Verschlüsselung (engl. *end-to-end encryption*).

Bei der Verbindungsverschlüsselung (oder auch Punkt-zu-Punkt-Verschlüsselung) werden die kompletten Datenpakete inklusive der Verbindungsdaten verschlüsselt. Zwar ist dies die umfangreichere Verschlüsselungsmethode. Um die Paketdaten aber übers Internet übertragen zu können, müssen die Pakete von den Routern bei der Übertragung jedoch

---

[138] *Stalla-Bourdillon u.a.*, CLSR 2014, 670 (672).
[139] *Dreger u.a.*, Network Intrusion Detection, in: Proceedings of the 15th Conference on USENIX Security Symposium, 2006, S. 257 (259 f.).
[140] *Kastl*, GRUR 2016, 671 (672 ff.).

wieder entschlüsselt werden, damit diese an die Routing-Informationen gelangen können.[141] Dann würde jedoch genau dort der Verschlüsselungsschutz wegfallen, an dem eine Deep Packet Inspection stattfinden kann.

Die Alternative zur Verbindungsverschlüsselung ist die Ende-zu-Ende-Verschlüsselung. Hier wird lediglich die Anwendungsschicht des Datenpakets verschlüsselt, die Verbindungsdaten bleiben unverschlüsselt.[142] So bleiben zwar die Verbindungsdaten für den ISP auslesbar. Allerdings entfällt die Notwendigkeit, die Verschlüsselung in den Routern aufzuheben, um überhaupt eine Datenverbindung herstellen zu können. Als Umgehungsmaßnahme für DPI-Filtersysteme kommt daher nur die Ende-zu-Ende-Verschlüsselung in Betracht.

Auch Ende-zu-Ende-Verschlüsselung führt jedoch nicht mit Sicherheit zur Umgehung eines DPI-Filters. Wendet der ISP eine klassische Nutzdaten-Analyse an, so kann er versuchen, die verschlüsselten Daten bei sich zu entschlüsseln. Dies ist jedoch im Vergleich zu einer Analyse unverschlüsselter Daten mit hohen Kosten für den ISP verbunden. Über den Erfolg eines Entschlüsselungsversuchs entscheidet letztlich nur die Leistungsfähigkeit der Hard- und Software des Providers und der Aufwand, den er für die Analyse zu betreiben bereit ist.[143]

Auch die oben[144] bereits erwähnte heuristische Analyse des Daten-Flows anhand statistischer Parameter, um anhand der Ergebnisse eine zuverlässige Klassifizierung des Inhalts treffen zu können, ist gegen Ende-zu-Ende-Verschlüsselung weitgehend immun.[145]

Kombinieren lassen sich auch beide Ansätze, um eine Verschlüsselung aufzuheben. So lässt sich über eine statistische Analyse des verschlüsselten Datenstroms typischer Filesharing-Verkehr von eher unverdächtigem Datenverkehr trennen. Im Anschluss kann der ISP dann seine Entschlüsselungsanstrengungen auf den verdächtigen Verkehr konzentrieren und spart auf diese Weise.[146]

DPI-Filter zu umgehen ist folglich für die Nutzer deutlich aufwändiger, als wenn sie dies bei einer Eingriffen in den Datenverkehr mittels IP- oder DNS-Sperre erreichen wollen. Der Datenverkehr, der nicht vom Filter aufgehalten werden soll, muss zunächst ver-

---

[141] *Królikowski*, Packet Inspection, in: Telemedicus Soko 2014, S. 140 (148).
[142] *Królikowski*, Packet Inspection, in: Telemedicus Soko 2014, S. 140 (148).
[143] Zu einigen zur Verfügung stehenden Verfahren *Królikowski*, Packet Inspection, in: Telemedicus Soko 2014, S. 141 (149 f.).
[144] Vgl. oben Kap. 1 III 3 b) (S. 26).
[145] Sen u.a., Accurate, Scalable In-network Identification of P2P Traffic Using Application Signatures, in: Proceedings of the 13th International Conference on World Wide Web 2004, 2004, S. 512 (520).
[146] Vgl. Dreger u.a., Network Intrusion Detection, in: Proceedings of the 15th Conference on USENIX Security Symposium, 2006, S. 257 (259); *Hjelmvik/John*, Breaking and Improving Protocol Obfuscation, 2010, S. 18, abrufbar unter https://www.iis.se/docs/hjelmvik_breaking.pdf (zuletzt besucht am 09.10.2021); *Królikowski*, Packet Inspection, in: Telemedicus Soko 2014, S. 141 (149).

schlüsselt werden, was einen nicht unerheblichen Aufwand voraussetzt. Auch eine erfolgreiche Verschlüsselung garantiert zudem nicht, dass unerlaubtes Filesharing nicht als solches identifiziert wird, da den ISP Mittel zur Verfügung stehen, Verschlüsselung zu durchbrechen oder in ihrer Wirksamkeit herabzusetzen.

Nicht zu vernachlässigen ist zudem die Tatsache, dass der Nutzer bei DPI-Filtern nicht einfach auf andere Angebote ausweichen kann, die nicht von der Maßnahme betroffen sind. Im Gegensatz zu DNS- und IP-Sperren richten sich DPI-Filtersysteme nicht gegen konkrete Filesharing-Angebote, die unter bestimmten Adressen zu erreichen sind, sondern setzen direkt bei den übertragenen Daten an. Der Datenverkehr, der von einer solchen DVR überwacht wird, umfasst potentiell die kompletten Daten, die die Router eines ISP durchlaufen, unabhängig von der Quelle. Da sich solch eine Datenverkehrsregulierung nicht nur gegen ausgewählte Anbieter richtet, sind die Ausweichmöglichkeiten des Nutzers sehr begrenzt.

Das Zusammenspiel an fehlenden Ausweichmöglichkeiten und komplizierten und nur eingeschränkt wirksamen möglichen Gegenmaßnahmen führt zu einer hohen potentiellen Effektivität von DPI-Filtern bei der Durchsetzung des Urheberrechts, insbesondere im Vergleich mit IP- und DNS-Sperren. Der Schutz digitaler Güter, der durch ein DPI-Filtersystem durchgesetzt wird, ist in hohem Maße effektiv, selbst wenn die illegalen Angebote weiterhin existieren und besucht werden können.

Kapitel 2 – Vereinbarkeit der DVR mit europäischem Primärrecht

Will der Staat durch Eingriffe in den Datenverkehr das Urheberrecht durchsetzen, hat er verschiedene tatsächliche und rechtliche Optionen, muss dabei allerdings die rechtlichen Grenzen höherrangigen Rechts, insbesondere europäisches Primärrecht und das Grundgesetz, beachten. Das betrifft die zum einen materielle Fragen – z.B. wie tief darf ein ISP auf staatliche Anordnung in den Datenverkehr hineinschauen –, aber auch formelle Aspekte, wie z.B. die Form der Anordnung (gesetzlich, gerichtlich oder behördlich) oder die Gewährleistung von Rechtsschutz für die betroffenen Parteien. Entsprechende Regelungen dürften nicht in Widerspruch zu höherrangigem Recht stehen, wobei hier sowohl eine europarechtliche als auch eine mitgliedstaatliche bzw. deutsche Perspektive angezeigt ist.

Die rechtlichen Grenzen von Eingriffen in den Datenverkehr im Allgemeinen und zur Durchsetzung des Urheberrechts im Besonderen sind bislang nicht abschließend geklärt. Der europäische Gesetzgeber hat auf sekundärrechtlicher Ebene einige – allerdings sehr offen formulierte – Regelungen getroffen.[147] Der deutsche Gesetzgeber ist bislang im Hinblick auf eine DVR zur Urheberrechtsdurchsetzung noch nicht tätig geworden, sieht man

[147] Auf europäischer Ebene etwa Art. 8 Abs. 3 der RL 2001/29/EG. Ein konkreter geregelter Filteransatz, der allerdings nicht im Internet, sondern direkt beim Host- oder Content-Provider ansetzt, findet sich in Art. 17 der RL 2019/790/EU (Urheberrechtsrichtlinie), der bis zum 07. Juni 2021 in mitgliedstaatliches Recht umgesetzt worden sein muss.

einmal vom umstrittenen § 7 Abs. 4 TMG ab.[148] Der EuGH und die deutsche Fachgerichtsbarkeit haben sich hingegen bereits mit der Thematik auseinandergesetzt.[149] Viele Schranken, die bei Eingriffen in den Datenverkehr berücksichtigt werden müssen, sind jedoch noch nicht abschließend geklärt. Die Dogmatik der deutschen Grundrechte sowie die Rechtsprechung von EuGH und Europäischem Gerichtshof für Menschenrechte (EGMR) bieten jedoch in Verbindung mit einer in ihrem Umfang und ihrer inhaltlichen Tiefe beachtlichen Aufarbeitung der Thematik in der rechtswissenschaftlichen Literatur sowie in der unterinstanzlichen Rechtsprechung ein solides Fundament, aus dem sich Schlussfolgerungen über die Grenzen für DVR-Maßnahmen im Urheberrecht ableiten lassen.

Da das europäische Recht dem nationalen bzw. mitgliedstaatlichen Recht nach der hier vertretenen Auffassung übergeordnet ist,[150] soll im Folgenden zunächst die Vereinbarkeit von Eingriffen in den Datenverkehr zur Durchsetzung des Urheberrechts mit Europarecht geprüft werden.

I. Überblick über die Systematik des EU-Rechts

1. Definition Europarecht

Der Begriff des Europarechts ist mehrdeutig, und nicht in jeder Deutungsweise ist das Europarecht hier von näherem Interesse. Daher bedarf es einer näheren Definition des Begriffs, um für die zu behandelnden Fragen einen sinnvollen Prüfungsrahmen vorzugeben. Dazu muss unterschieden werden zwischen dem Europarecht *im engeren Sinne* und dem Europarecht *im weiteren Sinne*.

Die Bezeichnung „*Europarecht im engeren Sinne*“ hat sich in der Rechtswissenschaft für das Recht der Europäischen Gemeinschaften bzw. der heutigen Europäischen Union und der Europäischen Atomgemeinschaft (EURATOM) herausgebildet.[151] Das Europarecht im engeren Sinne umfasst zum einen das Primärrecht der Europäischen Union (EU), also die Gesamtheit der Normen, die in den Gründungsverträgen enthalten sind.[152] Namentlich sind dies heute der Vertrag über die Europäische Union (EUV) und der Vertrag über die

---

[148] Der persönliche Anwendungsbereich von § 7 Abs. 4 TMG ist jedoch umstritten. Vgl. zu dieser Frage unten D II 1 b) (4) (S. 140 ff.)

[149] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959; EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192; BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82; BGH, Urt. v. 26.11.2015, I ZR 3/14, 3dl.am; das Bundesverfassungsgericht hingegen hat eine Verfassungsbeschwerde gegen die Goldesel-Entscheidung des BGH nicht zur Entscheidung angenommen, weil diese sich nur auf die Urteilsgründe, nicht aber auf den Tenor der Entscheidung bezog, vgl. BVerfG, Nichtannahmebeschl. v. 20.11. 2018, 1 BvR 1502/16, Rn. 2a (juris).

[150] Siehe dazu unten Kap. 2 I 4 a) (2) (S. 49 ff.).

[151] *Haratsch u.a.*, Europarecht, Kap. 1 I (Rn. 2); *Herdegen*, Europarecht, § 1 I (Rn. 2); *Streinz*, Europarecht, § 1 I (Rn. 1).

[152] *Haratsch u.a.*, Europarecht, Kap. 1 I (Rn. 2).

Arbeitsweise der Europäischen Union (AEUV) inklusive Anhängen und Protokollen sowie der Charta der Grundrechte der Europäischen Union („Charta“).[153] Diese Rechtsquellen enthalten das Primärrecht der EU.

Weiterhin umfasst der Begriff des Europarechts im engeren Sinne das gesamte Sekundärrecht der EU, also jegliche Normen, die abgeleitet von den im europäischen Primärrecht festgelegten Regeln von Institutionen der Europäischen Union erlassen werden.[154] Rechtlich verbindlich sind von diesen Regeln Verordnungen, Richtlinien und Beschlüsse.[155]

Das Primärrecht der EU ist gegenüber dem Sekundärrecht vorrangig. Sekundärrecht darf zudem nur erlassen werden, soweit es dafür eine primärrechtliche Ermächtigungsgrundlage gibt.[156]

Europarecht im weiteren Sinne umfasst einen Rahmen von Normen, der über die Rechtsnormen der Europäischen Union hinausgeht. Europarecht *im weiteren Sinne* bezeichnet daher das Recht, das den Formen institutionalisierter Zusammenarbeit in Europa zugrunde liegt.[157]

Einige dieser Institutionen sind schließlich in größeren Gebilden aufgegangen oder wurden von der Geschichte überholt und mittlerweile abgewickelt.[158] Verbliebene wichtige europäische Organisationen, die selbstständig neben der EU bestehen, sind in erster Linie die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) sowie der Europäische Rat.[159] Insbesondere der Europäische Rat hat mit der Europäischen Konvention der Menschenrechte (EMRK) eine auch im Rahmen dieser Arbeit bedeutende europäische Rechtsquelle geschaffen, da die in der EMRK enthaltenen Menschenrechte durch Verweise in EUV und Charta eingebunden werden und durch den Beitritt der Bundesrepublik zur EMRK auch im nationalen Recht Wirkung entfalten.

2. Europarecht als Prüfungsmaßstab

Normen des Europarechts *im engeren Sinne* bilden den Kern der folgenden Rechtmäßigkeitsprüfung im europäischen Rahmen. Im Primärrecht betrifft dies insbesondere die

---

[153] Geschaffen durch den Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft v. 13.12.2007, ABl. C 2007/C 306/01.
[154] *Herdegen*, Europarecht, § 8 IV (Rn. 48).
[155] *Nettesheim* in: Oppermann u.a., Europarecht, § 9 I 2 d) (Rn. 15 ff.); *Streinz*, Europarecht, § 1 II (Rn. 4).
[156] *Hobe/Fremuth*, Europarecht, § 10 V (Rn. 21).
[157] *Haratsch u.a.*, Europarecht, Kap. 1 I (Rn. 2); *Herdegen*, Europarecht, § 1 I (Rn. 2); *R. Schulze/Kadelbach* in: R. Schulze u.a., Europarecht: Handbuch für die deutsche Rechtspraxis, Einführung Kap. 1 IV (Rn. 14 f.).
[158] So etwa die Westeuropäische Union (WEU), die ein Verteidigungsbündnis im Kalten Krieg darstellte, sowie Organisation für Europäische Wirtschaftliche Zusammenarbeit (Organisation for Economic Cooperation – OEEC), die inzwischen in der Organisation for Economic Cooperation and Development (OECD) aufging.
[159] Vgl. *Hobe/Fremuth*, Europarecht, § 4 I, IV (Rn. 2 ff., 9 ff.).

Charta, die über einen Verweis im EUV in den Rang vollwertigen EU-Primärrechts erhoben wird,[160] sowie die Grundfreiheiten der Europäischen Union, die unmittelbar im AEUV zu finden sind.

Auch die EMRK ist für die Beurteilung der Rechtmäßigkeit von Eingriffen in den Datenverkehr zur Durchsetzung des Urheberrechts von Bedeutung, so dass auch Europarecht *im weiteren Sinne* im Folgenden Berücksichtigung findet.[161]

3. EU-Recht als Schranke des Handelns der Organe der Europäischen Union

Europarecht im engeren Sinne bindet die Organe der Europäischen Union. Dies gilt in erster Linie für die Beachtung des Primärrechts bei der Verabschiedung europäischen Sekundärrechts. Ebenso sind der EuGH und der Gerichtshof erster Instanz bei der Rechtsprechung an EU-Recht gebunden, genau wie die europäische Verwaltung bei der Ausführung Primär- und Sekundärrechts. Zwar sind Verstöße der Mitgliedstaaten gegen europäisches Recht in der Praxis häufiger anzutreffen, doch beschäftigen auch Verstöße der europäischen Institutionen die Gerichte. Wichtige Anwendungsfälle, in denen europäische Institutionen an Europarecht gemessen werden, sind etwa die Entscheidungen der EU-Kommission auf dem Gebiet des Kartellrechts, die regelmäßig von den jeweils Betroffenen vor Gericht angegriffen werden.[162] Allerdings hat der EuGH auch bereits europäisches Sekundärrecht für rechtswidrig erklärt, wenn es mit den europäischen Grundrechten, die im Rang von Primärrecht stehen, nicht vereinbar war.[163]

4. EU-Recht als Schranke mitgliedstaatlichen Handelns

Wenn man sich die Frage stellt, inwieweit EU-Recht gerade mitgliedstaatlichen Maßnahmen, die den Datenverkehr zur Durchsetzung des Urheberrechts regulieren sollen, rechtliche Grenzen zu setzen in der Lage ist, muss zunächst die Vorfrage beantwortet werden, in welchem Konkurrenzverhältnis das EU-Recht überhaupt zum mitgliedstaatlichen Recht steht.

a. Bindung mitgliedstaatlichen Handelns an EU-Recht

Die grundsätzliche Fähigkeit europäischen Rechts im engeren Sinne, mitgliedstaatlichem Handeln Schranken zu setzen, gründet einerseits in der Verpflichtung, unmittelbar geltendes EU-Recht anzuwenden und umzusetzen, andererseits in dem unbedingten Vorrang des EU-Rechts vor mitgliedstaatlichem Recht.

(1) Anwendung und Umsetzung von EU-Recht durch die Mitgliedstaaten

Art. 4 Abs. 3 UAbs. 2 EUV verpflichtet die staatliche Gewalt in den Mitgliedstaaten, alle geeigneten Maßnahmen zu ergreifen, um ihre Verpflichtungen zu erfüllen, die sich aus

---

[160] *Streinz*, Europarecht, § 1 II (Rn. 3).

[161] Vgl. zum Verhältnis EMRK zu den Grundrechten der Charta unten Kap. 2 III 3 (S. 63 f.).

[162] Vgl. z.B. EuGH, Urt. v. 06.04.1995, C-241/91 P, C-242/91 P, Magill, Slg. 1995, I-00743; EuGH, Urt. v. 10.09.2009, C-97/08 P, Akzo Nobel, Slg. 2009, I-08237; EuGH, Urt. v. 06.12.2012, Rs. C-457/10 P, AstraZeneca, EU:C:2012:770; EuGH, Urt. v. 10.07.2014, Rs. C-295/12 P, Telefónica, EU:C:2014:2062.

[163] EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C-594/12, Digital Rights Ireland, EU:C:2014:238.

den Verträgen oder den Handlungen der Organe der EU ergeben. Damit wird eine umfassende Pflicht der Mitgliedstaaten begründet, geltendes und unmittelbar wirkendes EU-Recht anzuwenden und umzusetzen. Bedeutsam ist dies insbesondere auch deshalb, weil die EU nur über geringe eigene Kapazitäten öffentlicher Verwaltung verfügt und daher auf die Hilfe der Mitgliedstaaten bei der Vollziehung von Unionsrecht zwingend angewiesen ist.[164] Das Gebot des Art. 4 Abs. 3 UAbs. 2 EUV betrifft Legislative, Exekutive und Judikative gleichermaßen.

Für die gesetzgebende Gewalt bedeutet dies, dass sie nationale Gesetze erlassen, aufheben oder ändern muss, damit die vom EU-Recht getroffenen Regeln vollständig und effektiv umgesetzt werden. Die bedeutendste konkrete Auswirkung dieser Regel ist die Pflicht des mitgliedstaatlichen Gesetzgebers zur vollständigen und fristgerechten Umsetzung von Richtlinien gemäß Art. 4 Abs. 3 UAbs. 2 EUV i.V.m. Art. 288 Abs. 3 AEUV.[165]

Die Verwaltung der Mitgliedstaaten hingegen ist gemäß Art. 197 Abs. 1, 291 Abs. 1 AEUV dort für den Vollzug von Unionsrecht zuständig, wo die Union dieses nicht selbst vollzieht. Ist der Vollzug von Unionsrecht durch die Verwaltung der Mitgliedstaaten damit rechtstechnisch gesehen nur subsidiär, ist sie mit wenigen Ausnahmen dennoch der absolute Regelfall.[166] Zu beachten ist dabei, dass sich die Art und Weise des Vollzugs nach mitgliedstaatlichem Verwaltungsverfahrensrecht richtet,[167] solange EU-Recht hierzu keine spezielle Regelung enthält.[168] Das Verwaltungsverfahrensrecht ist allerdings dabei so auszulegen, dass das europäische Recht effektiv durchgesetzt wird („effet utile“).[169]

Schließlich sind auch die mitgliedstaatlichen Gerichte gegenüber der Europäischen Union dazu verpflichtet, geltendes EU-Recht anzuwenden. Die Gerichte müssen sicherstellen, dass sie Rechte des Einzelnen, die dem EU-Recht entspringen, gewährleisten. Ähnlich wie beim Vollzug des EU-Rechts durch die Verwaltung des Mitgliedstaats, der sich im Wesentlichen nach nationalem Verwaltungsverfahrensrecht richtet, ist es dabei nicht notwendig, originäre europarechtliche Rechtsbehelfe zu schaffen, solange der Schutz der subjektiven Rechte aus europäischem Recht auch mit den bestehenden, nationalen Rechtsbehelfen durchgesetzt werden kann.[170]

(2) Vorrang des Unionsrechts

Zwar lässt der EUV, wie soeben festgestellt, ausdrücklich keinen Zweifel daran, dass die Mitgliedstaaten Europarecht grundsätzlich umsetzen und vollziehen zu müssen. Es stellt

---

[164] *Obwexer* in: Groeben u.a., Europäisches Unionsrecht, Bd. 1, Art. 4 EUV Rn. 95.
[165] *W. Kahl* in: Calliess/Ruffert, EUV/AEUV, Art. 4 EUV Rn. 54.
[166] *W. Kahl* in: Calliess/Ruffert, EUV/AEUV, Art. 4 EUV Rn. 60.
[167] Vgl. Art. 291 Abs. 1 AEUV.
[168] *W. Kahl* in: Calliess/Ruffert, EUV/AEUV, Art. 4 EUV Rn. 60.
[169] EuGH, Urt. v. 21.09.1989, Rs. C-68/88, Republik Griechenland, Slg. 1989, S. 2965, Rn. 24.
[170] EuGH, Urt. v. 13.03.2007, Rs. C-432/05, Unibet, Slg. I-02271, Rn. 38 ff.

sich dennoch die weiterführende Frage, wie zu verfahren ist, wenn EU-Recht und mitgliedstaatliches Recht sich widersprechen.

Grundsätzlich gilt, dass eine mitgliedstaatliche Norm, die im Widerspruch zu einer Vorschrift des EU-Rechts steht, insoweit nicht angewendet werden darf. Dies ist nicht selbstverständlich, da es an einer entsprechenden ausdrücklichen Vorschrift in den europäischen Verträgen fehlt, wie der Konflikt im Falle der Kollision europäischen Rechts mit mitgliedstaatlichem Recht aufzulösen ist. Während der gescheiterte Entwurf einer Europäischen Verfassung eine entsprechende Norm enthielt, die den Anwendungsvorrang des EU-Rechts vor mitgliedstaatlichem Recht vorsah, ist dies im Vertrag von Lissabon nicht der Fall.[171] Die Ausgestaltung des Rangverhältnisses zwischen europäischem Recht und dem Recht der Mitgliedstaaten wurde damit faktisch den Gerichten überlassen.

Der EuGH geht ungeachtet des unklaren Vertragswortlauts von einem strikten Vorrang des Unionsrechts vor mitgliedstaatlichem Recht aus.[172] Hintergrund ist, dass der EuGH annimmt, dass es sich bei EU-Recht um ein Recht eigener Art und nicht um Völkerrecht handelt. Die Mitgliedstaaten hätten mit dem EWG-Vertrag[173] dauerhaft Hoheitsrechte abgetreten und damit eine Institution mit eigenen Organen und Rechtsfähigkeit sowie insbesondere mit eigenen Hoheitsrechten geschaffen. Die vertraglich festgeschriebenen Ziele dieser eigenständigen Organisation würden aber gefährdet, wenn es den Mitgliedstaaten offen stünde, durch mitgliedstaatliche Rechtsakte solche des europäischen Rechts in Frage zu stellen. Daher könne kein mitgliedstaatliches Recht, gleich welcher Art, solchem Recht entgegenstehen, dass aus der autonomen Rechtsquelle des europäischen Rechts (*im engeren Sinn)* hervorgegangen sei.[174]

Daraus folgt, dass nach Ansicht des EuGH auch nachrangiges EU-Recht mitgliedstaatlichem Recht in jedem Fall vorgeht, selbst wenn es sich bei dem mitgliedstaatlichen Recht um ein *lex posterior*, ein *lex specialis* oder gar um Verfassungsrecht handeln sollte.[175] Eine Ausnahme stellt insoweit nur nichtiges Unionsrecht dar. Doch kann die Nichtigkeit von Unionsrecht ausschließlich mit der Nichtigkeitsfeststellungsklage vor dem EuGH geltend gemacht werden; die mitgliedstaatlichen Gerichte besitzen für Europäisches Recht keine

---

[171] Vgl. Art. I–6 des Vertrags über eine Verfassung für Europa. Dem Vertrag von Lissabon ist lediglich eine Erklärung Nr. 17 beigefügt (die gemäß Art. 51 EUV jedoch Bestandteil des Vertrages ist), deren Inhalt sich dergestalt zusammenfassen lässt, dass aus dem Fehlen einer expliziten Norm im EUV, die den Anwendungsvorrang von EU-Recht festschreibt, nicht zu folgern ist, dass der Vorrang des EU-Recht vor demjenigen der Mitgliedstaaten durch die Vertragsparteien abgelehnt werde.

[172] Ständige Rechtsprechung seit EuGH, Beschl. v. 03.06.1964, Rs. C-6/64, Costa/E.N.E.L., Slg. 1964, S. 1253.

[173] Der Vertrag zur Gründung der Europäischen Wirtschaftsgemeinschaft (EWG-Vertrag) v. 25.03.1957 ist ein Vorgängervertrag der heutigen Europäischen Verträge.

[174] EuGH, Beschl. v. 03.06.1964, Rs. C-6/64, Costa/E.N.E.L., Slg. 1964, S. 1251 (1269 ff.).

[175] EuGH, Urt. v. 17.12.1970, Rs. C-11/70, Slg. 1970, S. 1125, Rn. 3; EuGH, Urt. v. 09.03.1978, Rs. C-106/77, Simmenthal, Slg. 1978, S. 629 (644 f.) Rn. 21 ff.

Verwerfungskompetenz und müssen auch nichtiges EU-Recht bis zu einer entsprechenden Entscheidung des EuGH als gültig behandeln.[176]

Das Bundesverfassungsgericht hat in der Vergangenheit den Vorrang des Unionsrechts vor nationalem Verfassungsrecht, insbesondere was den Vorrang nachrangigen, also sekundärem EU-Recht vor deutschen Grundrechten angeht, mit wechselnden Vorzeichen entschieden.

In einer frühen Entscheidung erkannte das BVerfG zunächst die Tatsache des grundsätzlichen Vorrangs des Europarechts an. In demselben Beschluss entschied das BVerfG zudem, dass Verordnungen der Europäischen Wirtschaftsgemeinschaft, die schließlich in der EU aufging, nicht unmittelbar mit einer Verfassungsbeschwerde angegriffen werden könnten.[177]

In der sogenannten „Solange-I-Entscheidung", die ein richterliches Normenkontrollverfahren gemäß Art. 100 Abs. 1 GG abschloss, stellte das BVerfG hingegen fest, dass es kompetent sei, eine Norm des europäischen Sekundärrechts auf seine Vereinbarkeit mit den Grundrechten des Grundgesetzes hin zu überprüfen. Dies allerdings erst subsidiär, nachdem der Grundrechtsschutz durch den Europäischen Gerichtshof im Rahmen eines Vorlageverfahrens vor dem EuGH versagt habe.

Diese Prüfungskompetenz wollte das BVerfG so lange in Anspruch nehmen, wie die Entwicklung europäischen Rechts noch nicht den Punkt erreicht hätte, dass es einen mit dem deutschen Grundrechtsschutzstandard vergleichbaren, parlamentarisch legitimierten Grundrechtskatalog besitze.[178] Bemerkenswert an dieser Entscheidung ist unter anderem, dass das Bundesverfassungsgericht den Vorrang der europäischen Rechtsordnung gleich doppelt herausforderte. Zum einen hielt es das Grundgesetz, also mitgliedstaatliches Recht, für ranghöher als europäisches Sekundärrecht, und zum anderen sah es sich als kompetent an, über die Anwendbarkeit europäischen Rechts zu entscheiden.

Diese Rechtsauffassung hatte einige Jahre Bestand. So ließ das BVerfG in seinem sogenannten „Vielleicht-Beschluss" vom 25.07.1979 offen, ob die *ratio* des Solange-I-Beschlusses weiterhin ohne Einschränkungen Geltung beanspruche.[179]

In seiner Solange-II-Entscheidung[180] vollzog das Bundesverfassungsgericht einige Jahre später jedoch eine teilweise Abkehr von seiner bisherigen Rechtsprechung. Zwar blieb das BVerfG in der Begründung nah an seiner Auffassung aus Solange I, dass sich europäisches Sekundärrecht grundsätzlich an deutschen Grundrechten messen lassen müsse. Im Ergebnis jedoch nahm es mit der Solange-II-Entscheidung eine inhaltliche Kehrtwende

---

[176] EuGH, Urt. v. 22.10.1987, Rs. C-314/85, Foto-Frost, Slg. 1987, S. 4199 (4230), Rn. 11 ff.
[177] BVerfG, Urt. v. 18.10.1967, 1 BvR 248/63, 1 BvR 216/67, EWG-Verordnung, BVerfGE 22, 293 (296 f.).
[178] BVerfG, Urt. v. 29.05.1974, 2 BvL 52/71, Solange 1, BVerfGE 37, 271 (280).
[179] BVerfG, Beschl. v. 25.07.1979, 2 BvL 6/77, Vielleicht-Beschluss, BVerfGE 52, 187, (202 f.).
[180] BVerfG, Urt. v. 22.10.1986, 2 BvR 197/83, Solange II, BVerfGE 73, 339.

vor, indem es – jedenfalls einstweilen – auf seine Prüfungskompetenz für die Vereinbarkeit europäischen Sekundärrechts mit deutschen Grundrechten verzichtete.

Diese Volte gelang dem BVerfG dadurch, dass es im Ergebnis voraussetzte, dass sich seit der Solange-I-Entscheidung die faktischen Gegebenheiten derart geändert hätten, dass zwar die Kriterien für einen Prüfungsvorbehalt gegenüber europäischem Sekundärrecht unverändert seien, die rechtliche Wirklichkeit diese aber nicht mehr erfülle. Das BVerfG zeichnet in der Solange-II-Entscheidung nach, welche Schritte die Europäischen Gemeinschaften im Allgemeinen und der EuGH im Besonderen seit dem Solange-I-Beschluss unternommen hätten, um den Grundrechtsschutz in Europa auf ein höheres Niveau zu bringen.[181] Der Schutz der Grundrechte würde nunmehr demjenigen des Grundgesetzes im Wesentlichen gleichstehen.[182] Vor allen Dingen sei die Geltung von Grundrechten im Europarecht im Prinzip von den Organen der Europäischen Gemeinschaften anerkannt.[183] Auch dem Erfordernis, der europäische Grundrechtsschutz müsse einer parlamentarischen Legitimation unterliegen, sei dadurch genügt, dass die europäischen Organe, darunter auch das zwischenzeitlich erstmals gewählte Europäische Parlament, offiziell erklärt hätten, die allgemeinen Grundrechte und sonstigen Verfassungsgrundsätze der Mitgliedstaaten seien ebenfalls europäisches Recht im Rang von Primärrecht. Auf die gleiche Weise sei auch die EMRK, die zu diesem Zeitpunkt bereits von allen damaligen Mitgliedstaaten parlamentarisch ratifiziert worden war, zu einem Maßstab geworden, an dem sich europäisches Recht *im engeren Sinne* messen lassen müsse.[184] Das BVerfG nennt dies Prinzip *normative Verklammerung* der Grundrechte.[185]

Aus den soeben genannten Gründen verzichte das Bundesverfassungsgericht so lange darauf, über die Vereinbarkeit europäischen Sekundärrechts, das die deutsche Staatsgewalt verpflichte, mit deutschen Grundrechten zu entscheiden, wie der EuGH in seinem Kompetenzbereich einen Grundrechtsstandard gewährleiste, der vom Standpunkt des Grundgesetzes aus unabdingbar sei. Mit seiner Prüfungskompetenz gab das BVerfG in der Konsequenz zugleich praktisch den Anspruch auf, dass Europarecht am Grundgesetz gemessen werde.[186]

In diesem Sinne konnte man auch die Ausführungen des BVerfG zur Prüfung europäischen Sekundärrechts anhand der Grundrechte des Grundgesetzes in dessen Maastricht-

---

[181] BVerfG, Urt. v. 22.10.1986, 2 BvR 197/83, Solange II, BVerfGE 73, 339 (378 ff.)
[182] BVerfG, Urt. v. 22.10.1986, 2 BvR 197/83, Solange II, BVerfGE 73, 339, (378 f.).
[183] BVerfG, Urt. v. 22.10.1986, 2 BvR 197/83, Solange II, BVerfGE 73, 339 (383 f.).
[184] Das Problem der parlamentarischen Legitimation europäischer Grundrechte dürfte sich spätestens mit der Ratifizierung des Vertrages von Lissabon, der die Charta der Grundrechte der Europäischen Union auch ausdrücklich in den Rang von Primärrecht erhebt, durch das Europäische Parlament und die nationalen Parlamente der Mitgliedstaaten erledigt haben.
[185] BVerfG, Urt. v. 22.10.1986, 2 BvR 197/83, Solange II, BVerfGE 73, 339 (384).
[186] BVerfG, Urt. v. 22.10.1986, 2 BvR 197/83, Solange II, BVerfGE 73, 339 (387).

Urteil lesen. Demzufolge übe das Bundesverfassungsgericht seine Rechtsprechung zusammen mit dem EuGH in einem Kooperationsverhältnis aus.[187] Eine Relativierung des Prüfungsvorbehalts war aus dem Wortlaut dieses Urteils nicht zwingend abzuleiten,[188] zumal nach den Ausführungen des BVerfG eine Verletzung von Grundrechten durch europäisches Sekundärrecht mit einer Verfassungsbeschwerde oder Richtervorlage nur geltend gemacht werden könne, wenn in der Begründung dargelegt werde, dass die europäische Rechtsentwicklung einschließlich der Rechtsprechung des EuGH seit der Solange-II-Entscheidung unter den erforderlichen Grundrechtsstandard abgesunken sei. Die Begründung müsse dazu im Einzelnen darlegen, dass der als unabdingbar gebotene Grundrechtsschutz generell und nicht nur im Einzelfall nicht gewährleistet sei.[189] Weiterhin sei die Solange-II-Rechtsprechung ausdrücklich nicht nur auf Verordnungen, sondern auch auf Richtlinien zu beziehen.

Nunmehr hat sich das Bundesverfassungsgericht in dieser Frage neu positioniert. Das BVerfG erklärt sich in der Entscheidung „Recht auf Vergessen II" nunmehr in allen Fällen als zuständig, in denen das Unionsrecht einen Sachverhalt vollständig vereinheitlicht, also insbesondere im Fall unionsrechtlicher Verordnungen. In diesen Fällen prüft das Bundesverfassungsgericht nunmehr die Anwendung des Unionsrechts durch deutsche Stellen anhand der Grundrechte der Charta, ohne dass ein generelles Absinken des Grundrechtsschutzes auf EU-Ebene geltend gemacht werden müsste.[190]

Der dogmatische Hintergrund der Rechtsprechung des BVerfG ist, dass dieses keinen *unbedingten* Vorrang des Unionsrechts anerkennt, sondern den Vorrang nur im Grundsatz akzeptiert. Unionsrecht genieße nur im Umfang des Rechtsanwendungsbefehls des Zustimmungsgesetzes zu den Europäischen Verträgen Geltung.[191] Eine Übertragung von Hoheitsrechten der Bundesrepublik auf die Europäische Union richte sich nach Art. 23 Abs. 1 GG, der allerdings der Übertragung in seinem Abs. 1 Satz 3 die Schranken der Unabänderlichkeitsgarantie des Art. 79 Abs. 3 GG setze. Danach könnten die in den Art. 1–20 GG festgelegten Grundsätze nicht veräußert werden. Weiterhin könne der deutsche Staat Hoheitsrechte gemäß Art. 23 Abs. 2 GG nur übertragen, um die in Art. 23 Abs. 1 Satz 1 GG genannten Integrationsziele zu erreichen, nämlich solche zur Errichtung einer Europäischen Union, die *„demokratischen, rechtsstaatlichen, sozialen und föderativen Grundsätzen und dem Grundsatz der Subsidiarität verpflichtet [sei] und einen diesem Grundgesetz im [W]esentlichen vergleichbaren Grundrechtsschutz [gewährleiste]"*. An dieser im Grundgesetz festgeschriebenen Identitätskontrolle, die das Bundesverfassungsgericht für die Bestimmung der Grenzen der Hoheitsübertragung in seinem Urteil

---

[187] BVerfG, Urt. v. 12.10.1993, 2 BvR 2134/92, 2 BvR 2159/92, Maastricht, BVerfGE 89, 155 (175).
[188] So auch *F. Kirchhof*, NJW 2011, 3681 (3685).
[189] BVerfG, Urt. v. 07.06.2000, 2 BvL 1/97, Bananenmarktverordnung, BVerfGE 102, 147 (164).
[190] BVerfG, Beschl. v. 06.11.2019, 1 BvR 276/17, Recht auf Vergessen II, BVerfGE 152, 216 (juris-Rn. 47 ff.).
[191] *Herdegen*, Europarecht, § 10 III 1 (Rn. 24).

zum Lissabon-Vertrag vorschreibt,[192] richtet sich folgerichtig auch seine Rechtsprechung zum Vorrang des EU-Rechts aus.[193]

Da sowohl die Solange-II-Rechtsprechung des BVerfG (in seiner Modifikation durch „Recht auf Vergessen II") als auch die Rechtsprechung des unbedingten Anwendungsvorrangs europäischen Rechts durch den EuGH weiterhin Geltung beanspruchen, sind die *dogmatischen* Differenzen über die unterschiedlichen Auslegungen des Vorrangs des EU-Rechts durch den EuGH und das BVerfG letztlich weiterhin ungelöst. In der rechtlichen Praxis könnten jedoch nach der jüngsten Rechtsprechung des BVerfG in absehbarer Zukunft Konflikte zwischen den Gerichten auftreten, da verbindliches Europarecht nunmehr sowohl vom EuGH als auch vom BVerfG anhand von Charta-Grundrechten geprüft wird.

b. Rechtsfolgen der Kollision von EU-Recht und mitgliedstaatlichem Recht

Auch die konkreten Rechtsfolgen einer Kollision von EU-Recht mit mitgliedstaatlichen Vorschriften sind nicht in den Verträgen festgehalten. Der EuGH hat sich in seiner Rechtsprechung für einen Anwendungsvorrang des Unionsrechts anstelle eines Geltungsvorrangs entschieden. Eine Kollision führt daher nicht zur Nichtigkeit der nachrangigen Norm, wie dies etwa bei einem Konflikt zwischen einem vor- und einem nachrangigen Gesetz im Geltungsbereich des Grundgesetzes der Fall ist.[194] Vielmehr gilt der sogenannte Anwendungsvorrang des Unionsrechts. Das bedeutet, dass die mitgliedstaatliche Norm weiterhin ihre Gültigkeit für solche Sachverhalte behält, auf die die kollidierende EU-Vorschrift keine Anwendung findet.[195] Dies kann etwa in den Fällen relevant werden, die lediglich Inländer- oder Drittländerbezug haben. Eine weitere denkbare Variante ist, dass sich das EU-Recht ändert oder eine europäische Norm entfällt. Dies hätte dann zur Folge, dass die verdrängte nationale Vorschrift wiederauflebt.[196]

c. Regelungskompetenz der EU in der Datenverkehrsregulierung im Urheberrecht

Damit sich der grundsätzliche Vorrang des EU-Rechts und die Bindung jeglichen mitgliedstaatlichen Handelns an dieses im Einzelfall (also hier der Datenverkehrsregulierung zum Urheberrechtsschutz) durchsetzen kann, ist allerdings Voraussetzung, dass der Europäischen Union die Kompetenz zur Regelung dieses Sachverhalts von den Mitgliedstaaten zugewiesen wurde. Im Recht der EU gilt gemäß Art. 5 Abs. 1 EUV das Prinzip der begrenzten Einzelermächtigung. Die Europäische Union darf lediglich in den Bereichen tätig werden, für welche die Mitgliedstaaten ihr in den Verträgen zur Verwirklichung der darin enthaltenen Ziele ausdrücklich die Zuständigkeit zugesprochen haben, Art. 5 Abs. 2 Satz 1 EUV. Nicht jeder rechtliche oder tatsächliche Sachverhalt ist daher

---

[192] BVerfG, Urt. v. 30.06.2009, 2 BvE 2/08, 2 BvE 5/08, 2 BvR 1010/08, 2 BvR 1022/08, 2 BvR 1259/08 ..., Lissabon-Urteil, BVerfGE 123, 267 (352).
[193] *Herdegen*, Europarecht, § 10 III 1 (Rn. 27 ff.).
[194] Vgl. etwa Art. 31 GG.
[195] EuGH, Urt. 04.04.1968, Rs. C-34/67, Lück, Slg. 1968, S. 364 (373).
[196] *Nettesheim* in: Oppermann u.a., Europarecht, § 10 I 3 (Rn. 32).

an EU-Recht zu messen, und die EU kann sich auch keine Kompetenzen selbst zuweisen.[197]

Die Europäische Union legt die ihr gegebenen Kompetenzen trotz Art. 5 Abs. 2 Satz 2 EUV allerdings recht weit aus, so dass ihr letztlich ein weiter Zuständigkeitsbereich gegeben ist. Dies wird zusätzlich durch einige sehr generell formulierte Zuweisungsnormen wie etwa den Art. 114 AEUV begünstigt, der der Europäischen Union die Aufgabe überträgt, für die Angleichung desjenigen Rechts der Mitgliedstaaten zu sorgen, das die Errichtung und das Funktionieren des Binnenmarkts zum Gegenstand hat.[198] Für die hier behandelten Fragen bedeutet das, dass das Unionsrecht anwendbar ist, wenn die EU für die Regulierung des Internet-Datenverkehrs und/oder des Urheberrechts aufgrund einer Ermächtigung der Mitgliedstaaten zuständig ist.

Wenn mitgliedstaatliche Normen den Datenverkehr über das Internet zwischen den Mitgliedstaaten beeinflussen, ist es immer denkbar, dass die Grundfreiheiten (hier: die Warenverkehrsfreiheit, Art. 28 ff. AEUV, die Niederlassungsfreiheit, Art. 49 ff. AEUV oder die Dienstleistungsfreiheit, Art. 56 ff. AEUV) davon berührt werden. Diese Freiheiten dienen der Verwirklichung des gemeinsamen Binnenmarkts.[199] Dessen Errichtung ist nach Art. 3 Abs. 3 Satz 1 EUV und Art. 26 AEUV eine der Kernaufgaben, die der EU durch die Mitgliedstaaten übertragenen Kernaufgaben. Wird das Internet reguliert, ist die EU also bereits deshalb zuständig, weil bei einer Regulierung des Internetdatenverkehrs eine Verletzung europäischer Grundfreiheiten droht.[200]

Die EU ist außerdem auch im Bereich des Urheberrechts zuständig. Ihre Zuständigkeit stützen die Organe der Union insbesondere auf die Kompetenzzuweisungen der Art. 53 Abs. 1 AEUV (ex-Art. 47 Abs. 2 EG) und Art. 114 AEUV (ex-Art. 95 EG). In der Richtlinie (RL) 2001/29/EG vom 22. Mai 2001[201] (InfoSoc-Richtlinie) wird dies in Erwägungsgrund 1 damit begründet, dass der Vertrag die Schaffung eines Binnenmarkts und die Etablierung von Regeln vorsieht, die den Wettbewerb auf diesem Binnenmarkt vor Verzerrungen schützen. Die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten zum Urheberrecht würde dabei helfen.

Die EU ist folglich zum Treffen von Regelungen in den Bereichen der Datenverkehrsregulierung und des Urheberrechts zuständig, so dass geltendes EU-Recht den Maßstab mitgliedstaatlichen Handelns auf diesen Gebieten bildet.

---

[197] Vgl. näher dazu *Hobe/Fremuth*, Europarecht, § 7 II (Rn. 24 ff.).
[198] *Hobe/Fremuth*, Europarecht, § 7 II 1 a) (Rn. 31).
[199] *Hobe/Fremuth*, Europarecht, § 15 II 1 (Rn. 9).
[200] *Maennel*, MMR 1999, 187 (187); *Schilling*, Präventive staatliche Kontrollmaßnahmen im Internet und ihre Vereinbarkeit mit dem Europarecht, S. 119.
[201] Richtlinie zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft.

II. Sekundärrechtlicher Rahmen der Intermediärshaftung im Urheberrecht

Der europäische Gesetzgeber hat von seiner Regelungskompetenz im Bereich des Urheberrechts und des Internets auch Gebrauch gemacht. Zwar ist das europäische Sekundärrecht wegen seiner Flüchtigkeit nicht Kern dieser Untersuchung. Dennoch ist das Sekundärrecht Teil des regulatorischen Umfelds, in dem die Fragestellungen dieser Arbeit relevant werden. Zum Verständnis insbesondere der Rechtsprechung in diesem Bereich ist es hilfreich, einen Überblick über die einschlägigen europäischen Richtlinien zu besitzen.

Eingriffe in den Datenverkehr zur Urheberrechtsdurchsetzung finden im Spannungsfeld gleich mehrerer Richtlinien statt, die jeweils unterschiedliche Aspekte mitgliedstaatlichen Rechts im Internet- und Urheberrecht aufeinander abstimmen und vereinheitlichen sollen.

1. RL 2000/31/EG

Die Richtlinie 2000/31/EG[202] spielt für die in dieser Arbeit gestellten Fragen eine wichtige Rolle, auch wenn die in dieser RL geregelten Sachverhalte recht allgemeiner Natur sind und nicht ausschließlich auf den Bereich des geistigen Eigentums zielen. Schwerpunkt der Richtlinie sind wirtschaftliche Fragen im Zusammenhang mit dem Internet, unter anderem geht es um die Reichweite der Haftung von Internet Service Providern für den Datenverkehr, den diese ihren Nutzern vermitteln.[203]

Gemäß Art. 12 Abs. 1 der Richtlinie ist ein ISP, der sich lediglich auf die nichtdiskriminierende Übertragung von Datenverkehr über das Internet beschränkt, nicht verantwortlich für die über sein Netz übermittelten Inhalte. Gemäß Art. 12 Abs. 3 der Richtlinie handelt es sich dabei jedoch nicht um ein Verbot für mitgliedstaatliche Behörden oder Gerichte, dem ISP gegenüber Maßnahmen anzuordnen, um Rechtsbrüche zu unterbinden, die in der Übermittlung des Datenverkehrs begründet liegen. Diese Vorschrift wird durch die Erwägungsgründe 45 und 47 der Richtlinie weiter konkretisiert. Die Anordnungen müssen dazu dienen, Überwachungspflichten *„in spezifischen Fällen“* aufzuerlegen, und können die Entfernung rechtswidriger Daten oder die Sperrung des Zugangs zu diesen zum Inhalt haben.

Art. 15 Abs. 1 der Richtlinie andererseits verbietet den Mitgliedstaaten, aus der soeben dargestellten Möglichkeit gemäß Art. 12 Abs. 3, die Provider zur Rechtsdurchsetzung in der Weise zu verpflichten, indem diesen eine allgemeine Überwachungspflicht aufgebürdet würde. Die Provider sind danach also ausdrücklich nicht verpflichtet, über ihr Netz übertragene Informationen generell auf Rechtsbrüche hin zu untersuchen.

---

[202] Richtlinie 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).

[203] Vgl. Erwägungsgrund 1 Abs. 2 der RL 2000/31/EG: „*Diese Richtlinie sorgt […] für eine Angleichung bestimmter für die Dienste der Informationsgesellschaft geltender innerstaatlicher Regelungen, die […] die Verantwortlichkeit von Vermittlern betreffen.*“

2. RL 2001/29/EG

Die sogenannte InfoSoc-Richtlinie ist eng verwandt mit der Richtlinie 2000/31/EG und konkretisiert diese im Hinblick auf urheberrechtliche Regelungen in der Informationsgesellschaft.[204] Dies betrifft insbesondere auch staatliche Maßnahmen gegenüber Internet Service Providern zur Urheberrechtsdurchsetzung. So weist die Richtlinie bereits in ihren Erwägungsgründen auf Urheberrechtsverstöße über das Internet hin, und dass die ISP wegen ihrer besonderen Möglichkeiten, diese zu unterbinden, möglicher Adressat entsprechender gerichtlicher Anordnung sein müssten. Daran ändere auch die Tatsache nichts. dass diese haftungsprivilegiert seien.[205]

Dieser Gedanke wird dann in Art. 8 Abs. 1 und 3 der InfoSoc-Richtlinie aufgenommen: Die Mitgliedstaaten müssen wirksame, verhältnismäßige und abschreckende Sanktionen und Rechtsbehelfe gegen die Verletzung von Urheberrechten und verwandter Schutzrechte vorsehen. Die Rechtsinhaber müssen in dem Zuge von den Mitgliedstaaten die Möglichkeit eingeräumt bekommen, gegen Vermittler gerichtliche Anordnungen beantragen zu können, wenn deren Dienste für Urheberrechtsverletzungen genutzt würden.

3. RL 2004/48/EG

Die Richtlinie 2004/48/EG, die sogenannte Enforcement-Richtlinie,[206] hatte sich zum Ziel gesetzt, auch die Durchsetzung im Bereich des geistigen Eigentums europaweit zu harmonisieren, nachdem dies hinsichtlich des materiellen Urheberrechts bereits weitgehend geschehen war.[207] Sie nimmt dabei Bezug sowohl auf die soeben besprochene InfoSoc-Richtlinie als auch auf die RL 2000/31/EG. In ihrem 23. Erwägungsgrund stellt die Richtlinie fest, dass die Mitgliedstaaten die Voraussetzungen und Verfahren regeln müssten, nach denen betroffene Schutzrechtsinhaber gerichtliche Anordnungen gegen Intermediäre erwirken können, wenn die Dienste der Intermediäre von Dritten für Verletzungen geistigen Eigentums genutzt würden. Dies solle jedoch keinen Einfluss auf Art. 8 Abs. 3 der InfoSoc-Richtlinie haben, da bezüglich des Urheberrechts bereits ein hohes Maß an Harmonisierung bestehe.

So schreibt die RL 2004/48/EG dann auch in Art. 11 mit einem dem Art. 8 Abs. 3 der RL 2001/29/EG sehr nahekommenden Wortlaut den Mitgliedstaaten vor, dass es Rechteinhabern möglich sein muss, Anordnungen gegenüber Intermediären zum Schutz des geistigen Eigentums zu beantragen. Weiterhin müssten diese Anordnungen gemäß Art. 3 Abs. 2 der Enforcement-Richtlinie (analog Art. 8 Abs. 1 der InfoSoc-Richtlinie) auch wirksam, verhältnismäßig und abschreckend sein. Die Enforcement-Richtlinie holt folglich in Bezug auf gerichtliche Anordnungen gegenüber Internet Service Providern nur für die restlichen Bereiche des Geistigen Eigentums nach, was die InfoSoc-RL im Bereich des Urheberrechts

---

[204] So verweist Erwägungsgrund 16 der InfoSoc-Richtlinie auf die Wichtigkeit einer zeitgleichen Umsetzung beider Richtlinien, da die RL 2000/31/EG wichtige allgemeine Regelungen für die InfoSoc-RL treffe.

[205] Erwägungsgrund 59 der RL 2001/29/EG.

[206] Richtlinie des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums.

[207] Vgl. Erwägungsgrund 3 der RL 2004/48/EG.

bereits geregelt hatte. Die Vorschriften der InfoSoc-Richtlinie werden durch die Enforcement-RL also nicht verdrängt, sondern teilweise auf andere Bereiche des geistigen Eigentums erweitert.

Andererseits werden die Vorschriften der InfoSoc-RL durch die Enforcement-Richtlinie auch ergänzt. In Art. 3 Abs. 1 der Enforcement-RL wird beispielsweise festgestellt, dass die Maßnahmen zur Durchsetzung des geistigen Eigentums nicht nur fair und gerecht sein müssen, sondern auch „*nicht unnötig kompliziert oder kostspielig sein und keine unangemessenen Fristen oder ungerechtfertigten Verzögerungen mit sich bringen*" dürften.

Schließlich bleiben gemäß Art. 2 Abs. 3 lit. a) der Enforcement-RL auch die Vorschriften über Haftungsprivilegierungen der Internet Service Provider aus der Richtlinie 2004/48/EG bestehen.

4. DSGVO sowie die Richtlinie 2002/58/EG

Soweit der Datenschutz und der Schutz der Vertraulichkeit der Kommunikation eine Rolle spielen, sind zudem die Verordnung (EU) 2016/679 – auch bekannt als Datenschutz-Grundverordnung (DSGVO) – und die im Bereich des Datenverkehrs teils speziellere Richtlinie 2002/58/EG[208] zu beachten. [209]

In Art. 5 Abs. 1 der RL 2002/58/EG wird die Vertraulichkeit der über die öffentlichen Kommunikationsnetze übertragenen Nachrichten und den zugehörigen Verkehrsdaten angeordnet, die die Mitgliedstaaten durch Rechtssetzung sicherstellen müssen. Insbesondere wird das Mithören, das Abhören, das Speichern und andere Arten des Abfangens oder Überwachens durch andere Personen als die Nutzer verboten, wenn der Nutzer seine Einwilligung nicht erklärt hat. Ausgenommen von diesem Grundsatz sind die Daten, die zur Weiterleitung der Nachricht notwendigerweise gespeichert werden müssen, also im Wesentlichen die IP-Adressen.

Beschränkungen dieses Grundsatzes gemäß Art. 15 Abs. 1 der RL 2002/58/EG sind zulässig, wenn sie für die „Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig" sind.[210] Dazu dürften Daten für einen begrenzten Zeitraum aufbewahrt werden, wenn dies durch Rechtsvorschriften angeordnet wird.

---

[208] Richtlinie des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (ePrivacy-Richtlinie).

[209] Die DSGVO ersetzt die Datenschutz-Richtlinie 95/46/EG (Richtlinie des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr). Die Rechtsprechung des EuGH zur Richtlinie kann zur Auslegung der Vorschriften der DSGVO jedoch in weiten Teilen uneingeschränkt weiter herangezogen werden.

[210] Weitere, hier nicht relevante Schutzgüter, die eine Beschränkung des Grundsatzes gemäß Art. 5 der RL sind die nationale Sicherheit, die Landesverteidigung und die öffentliche Sicherheit.

Urheberrechtsverletzungen könnten, soweit es sich um Straftaten handelt, durchaus von der Beschränkungsmöglichkeit des Art. 15 Abs. 1 der RL 2002/58/EG erfasst sein. Der europäische Gesetzgeber weist allerdings ausdrücklich darauf hin, dass alle Beschränkungen gemäß Art. 15 Abs. 1 mit den auf europäischer Ebene geltenden Grundrechten vereinbar sein müssen.

5. RL (EU) 2019/790

Die Richtlinie (EU) 2019/790 über das Urheberrecht und verwandte Schutzrechte im digitalen Binnenmarkt (auch als Urheberrechtsrichtlinie bekannt) ändert u.a. die Richtlinien 2000/31/EG und 2001/29/EG in einigen Punkten, insbesondere hinsichtlich urheberrechtlicher Schrankenregelungen, ab, ersetzt oder ändert jedoch keine der im Kontext dieser Arbeit wichtigen Regelungen.

Aus der Perspektive dieser Arbeit interessant ist hingegen die Regelung des Art. 17 der Richtlinie. Art. 17 Abs. 3 Urheberrechtsrichtlinie sieht vor, dass die Mitgliedstaaten Regelungen erlassen, nach denen bestimmte Diensteanbieter unter gewissen Umständen nicht mehr gemäß Art. 14 Enforcement-RL haftungsprivilegiert sind, wenn sie Inhalte ihrer Nutzer im Sinne einer öffentlichen Wiedergabe oder Zugänglichmachung teilen. Bei diesen Diensteanbietern handelt es sich ausweislich Art. 3 Nr. 6 Urheberrechtsrichtlinie nicht um Access oder Network Provider. Art. 17 Urheberrichtlinie hat daher keine unmittelbare Relevanz für diese Arbeit. Es wird jedoch vertreten, dass die Diensteanbieter, um einer Haftung für Urheberrechtsverstöße ihrer Nutzer zu entgehen, Filtermaßnahmen ergreifen müssen, die einer Deep Packet Inspection ähneln.[211] Solche Filtermaßnahmen könnten daher teilweise ähnliche grundrechtliche Fragestellungen aufwerfen wie die in dieser Arbeit behandelten.

III. Schutz der Grundrechte nach der Charta der Grundrechte in der Europäischen Union

Als potentielle rechtliche Grenzen für Eingriffe in den Datenverkehr zur Urheberrechtsdurchsetzung kommen auf EU-Ebene in erster Linie Grundrechte der von den Regulierungsmaßnahmen betroffenen Bürger und Unternehmen in Frage.

1. Systematik des EU-Grundrechtsschutzes

Der EUV selbst enthält unmittelbar keinen eigenen Grundrechtskatalog. Allerdings hält er mit Art. 6 EUV eine Regelung bereit, die die Grundlage für den Grundrechtsschutz in der EU bildet, indem sie die insoweit einschlägigen (externen) Rechtsquellen benennt.

Über den Verweis in Art. 6 Abs. 1 UAbs. 1 HS 1 EUV werden die in der Charta der Grundrechte der Europäischen Union niedergelegten Grundrechte von der Europäischen Union anerkannt. In Art. 6 Abs. 1 UAbs. 1 HS 2 EUV wird explizit festgestellt, dass die Charta

---

[211] *Heidrich/Koch,* MMR 2020, 581 (583); *Klass*, ZUM 2020, 353 (Fn. 2); *Pravemann*, GRUR 2019, 783 (783 f.); *Schwartmann/Hentsch*, MMR 2020, 207 (210 f.).

und die Europäischen Verträge ihrem Rang nach gleichgestellt nebeneinander stehen. Auch bei der Charta handelt es sich demnach um europäisches Primärrecht.[212]

Eine weitere Rechtsquelle für Grundrechte auf EU-Ebene sind – in der Stellung als allgemeine Grundsätze des Unionsrechts – gemäß Art. 6 Abs. 3 EUV die Grundrechte, die sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten und der Europäischen Konvention der Menschenrechte ergeben. Dabei sind die Grundrechte als allgemeine Grundsätze echte Rechtsquellen, die ebenfalls in Abs. 3 erwähnten Verfassungstraditionen und die EMRK hingegen Rechtserkenntnisquellen.[213] Rechtserkenntnisquellen lassen sich als Auslegungshilfe bei der grundsätzlich selbstständigen Auslegung der Charta und der Grundrechte als allgemeine Grundsätze verstehen.[214]

Im AEUV hingegen findet sich wie im EUV kein eigener Katalog von Grundrechten. Allerdings sind hier die sogenannten Grundfreiheiten der Europäischen Union festgeschrieben, die weitere subjektive Rechte von primärrechtlichem Rang gewähren und unterschiedliche Formen der wirtschaftlichen Betätigung im Binnenmarkt der EU schützen.[215]

Beide Rechtskomplexe – also Grundrechte und Grundfreiheiten – unterscheiden sich teilweise stark in ihren Schutzzwecken. Das Gleiche gilt für den tatsächlichen und rechtlichen Kontext, in dem sie relevant werden. Dies ist in erster Linie aus ihrer Entstehungsgeschichte zu erklären. Grundfreiheiten sind jedoch ebenso wie die Grundrechte subjektive Rechte im Rang europäischen Primärrechts und daher potentielle Schranken für Eingriffe in den Verkehr.

2. Entstehungsgeschichte des Grundrechtsschutzes in der EU

Der Grundrechtsschutz in der Europäischen Union hat im Laufe der Geschichte der europäischen Einigung eine stetig größer werdende Bedeutung erlangt. Seine kontinuierliche Weiterentwicklung wird insbesondere durch die Tatsache deutlich, dass in den Römischen Verträgen der Grundrechtsschutz noch gänzlich ausgespart wurde, seit dem Inkrafttreten des Vertrags von Lissabon die Charta der Grundrechte der Europäischen Union und die Grundrechte als Rechtsgrundsätze der EU allerdings über den zentralen Grundrechts-Artikel 6 EUV unmittelbar Geltung beanspruchen. [216] Für die Zukunft gibt Art. 6 Abs. 2 EUV der Europäischen Union gar den Auftrag zum Beitritt zur Europäischen Menschenrechtskonvention auf.

Die Entwicklung eines vertieften, eigenständigen Grundrechtsschutzes auf europäischer Ebene wurde durch einige Grundsatzentscheidungen des EuGH schließlich auch notwen-

---

[212] *Frenz*, Europarecht, Kap. 9 A III 1 (Rn. 968); *Wolffgang* in: Lenz u.a., EU-Verträge, Art. 6 EUV Rn. 57.
[213] *Schorkopf* in: Grabitz u.a., Recht der Europäischen Union, Art. 6 EUV Rn. 51 (Stand: 68. Erg.-Lfg., Oktober 2019); *Beutler* in: Groeben u.a., Europäisches Unionsrecht, Bd. 1, Art. 6 EUV Rn. 22.
[214] *Jarass*, Charta der Grundrechte der Europäischen Union, Einleitung Rn. 47.
[215] Vgl. dazu ausführlich unten Kap. 2 V (S. 119 ff.).
[216] *Kingreen* in: Calliess/Ruffert, EUV/AEUV Art. 6 EUV Rn. 4.

dig. Seit der EuGH-Entscheidung Formaldehyd stand fest, dass Europarecht auch unmittelbar gegenüber den Bürgern und nicht nur gegenüber den Mitgliedstaaten Geltung beanspruchen kann.[217] EU-Recht genießt zudem gegenüber mitgliedstaatlichem Recht seit der EuGH-Entscheidung Costa/ENEL Anwendungsvorrang und wird daher in der Regel nicht an nationalem Verfassungsrecht gemessen.[218] Der Anwendungsvorrang gilt umso mehr, wenn Europarecht nicht mit Verfassungsrecht, sondern einfachen Gesetzen kollidiert. Dies hat zur Folge, dass EU- bzw. Gemeinschaftsrecht auch nicht unmittelbar durch die EMRK beschränkt wurde, da die EMRK in den Mitgliedstaaten lediglich den Rang eines formellen Gesetzes genießt.[219]

Auch wenn der Grundrechtsschutz noch keine Erwähnung in den Gründungsverträgen fand, wurden Grundrechte bereits früh im europäischen Einigungsprozess als Teil der europäischen Rechtsordnung anerkannt. Dieser Schritt ging in erster Linie vom EuGH aus. Dieser hat mit seiner Rechtsprechung wesentlich zur Etablierung eines Grundrechtsschutzes auf europäischer Ebene beigetragen.

Bereits bevor sich der EuGH mit Freiheits- und Gleichheitsgrundrechten beschäftigte, befasste er sich mit grundlegenden rechtsstaatlichen Prinzipien als Schranken des Europarechts. So wurde der Grundsatz der Verhältnismäßigkeit von der Rechtsprechung des EuGH erstmals 1956 als Richtschnur und Schranke des Handelns der Gemeinschafts- bzw. Unionsorgane anerkannt und dann in weiteren Entscheidungen bestätigt.[220] Auch die Geltung des Gebots der Gesetzmäßigkeit der Verwaltung[221] und des Vertrauensschutzgrundsatzes[222] im Europarecht sind dank des EuGH frühzeitig im Europarecht verankert worden.

Grundrechte im eigentlichen Sinn in Form von Freiheits- und Gleichheitsgarantien als Bestandteile des Gemeinschaftsrechts wurden vom EuGH schließlich seit dem *Stauder*-Urteil Ende der 1960er Jahre anerkannt.[223] Der EuGH berief sich in der Folge darauf, dass die Grundrechte zu den allgemeinen Grundsätzen der Gemeinschaftsrechtsordnung gehören würden, die er zu bewahren habe.[224]

---

[217] EuGH, Urt. v. 05.02.1963, Rs. C-26/62, Formaldehyd, Slg. 1963, S. 3 (27).
[218] EuGH, Beschl. v. 03.06.1964, Rs. C-6/64, Costa/E.N.E.L., Slg. 1964, S. 1253; EuGH, Urt. v. 17.12.1970, Rs. C-11/70, Slg. 1970, S. 1125.
[219] Vgl. *Haratsch u.a.*, Europarecht, Kap. 3 I 3 (Rn. 685); *Wolffgang* in: Lenz u.a., EU-Verträge, Art. 6 EUV Rn. 7; siehe auch BVerfG, Beschl. v. 14.10.2004, 2 BvR 1481/04, Görgülü, BVerfGE 111, 307, (319 f.).
[220] EuGH, Urt. v. 29.11.1956, Rs. C-8/55, Slg. 1955, S. 297 (311); EuGH, Urt. v. 12.06.1958, Rs. C-15/57, Slg. 1958, S. 161, Slg. 1958, 161 (202); EuGH, Urt. v. 13.06.1958, Rs. C-9/56, Meroni, Slg. 1958, S. 11 (43).
[221] EuGH, Urt. v. 13.06.1958, Rs. C-9/56, Meroni, Slg. 1958, S. 11 (41).
[222] EuGH, Urt. v. 01.06.1961, Rs. C-15/60, Slg. 1961, 241 (259).
[223] EuGH, Urt. v. 12.11.1969, Rs. C-29/69, Stauder, Slg. 1969, S. 419 (425); zuvor allerdings vermied es der EuGH, selbstständig Grundrechtsschutz zu gewähren, da er keine Prüfungskompetenz besäße, vgl. EuGH, Urteil v. 02.02.1958, Rs. C- 1/58, Storck, Slg. 1959, S. 45 (63); EuGH, Urt. v. 15.07.1960. Rs. C-36/59, C-37/59, C-38/59 und C-40/59, Nold, Slg. 1960, S. 887 (920).
[224] EuGH, Urt. v. 17.12.1970, Rs. C-11/70, Slg. 1970, S. 1125, Rn. 4.

Auf stabilere dogmatische Füße stellte der EuGH die Herleitung der allgemeinen Rechtsgrundsätze 1974 in seiner Nold-Entscheidung. Diese entsprängen zum einen den von den „Verfassungen der Mitgliedstaaten anerkannten und geschützten Grundrechten", auf der anderen Seite den völkerrechtlichen Verträgen zum Schutz der Menschenrechte, deren Vertragsparteien die Mitgliedstaaten geworden seien. Auch jene könnten im Rahmen des Europarechts berücksichtigt werden müssen.[225] Damit meint der EuGH im Wesentlichen die EMRK.

Auch die übrigen Organe der EG erkannten in der Folge – wenn auch zunächst lediglich informell – die Geltung der Grundrechte für das Gemeinschaftsrecht an. 1977 bekannten diese sich in einer Gemeinsamen Grundrechtserklärung des Europäischen Parlaments, des Rates und der Kommission zur Geltung der Grundrechte, wie sie vor allem aus den Verfassungsüberlieferungen der Mitgliedstaaten und der EMRK hervorgingen und gelobten, sich an diese auch zukünftig zu halten.[226] In der Präambel der Einheitlichen Europäischen Akte von 1987 bekräftigten die Mitgliedstaaten, die europäische Einigung auch zur Wahrung der Menschenrechte voranzutreiben.[227]

Mit Gründung der EU durch den Vertrag von Maastricht, der im November 1993 in Kraft trat, wurden die Grundrechte als allgemeine Grundsätze des Unionsrechts schließlich erstmals ausdrücklich als Primärrecht in den Europäischen Verträgen anerkannt.[228]

Der größte strukturelle Nachteil der Grundrechte als allgemeine Grundsätze hängt mit ihrer Natur als Richterrecht zusammen. Es fehlte eine schriftliche Kodifikation, die den Bürgern ihre Grundrechte transparent aufzeigt und so Rechtssicherheit und Vertrauen in die Institutionen der Europäischen Union schafft. Daher wurde schließlich ein Grundrechte-Konvent eingesetzt, der die europäischen Grundrechte kodifizieren sollte. Der Konvent vereinte neben Vertretern der europäischen Institutionen, also der Staats- und Regierungschefs, der Europäischen Kommission und des Europäischen Parlaments auch Vertreter der nationalen Parlamente der Mitgliedstaaten, was dem Konvent ein großes Maß an demokratischer Legitimation verlieh. Die vom Konvent in den Jahren 1999 und 2000 unter dem Vorsitz des ehemaligen Bundespräsidenten Roman Herzog erarbeitete Charta wurde am 02.10.2000 der Öffentlichkeit präsentiert und am 07.12.2000 von Europäischer Kommission, Parlament und Rat feierlich proklamiert. Die Charta blieb jedoch zunächst rechtlich unverbindlich. Der Plan, die Charta der Grundrechte zum vollwertigen Teil des Europäischen Verfassungsvertrags[229] zu machen, scheiterte zusammen mit der Verfassung an den ablehnenden Volksabstimmungen in Frankreich und den Niederlanden. [230]

---

[225] EuGH, Urt. v. 14.05.1974, C-4/73, Nold, Slg. 1974, S. 491, Rn. 13.
[226] Vgl. *Tomuschat* in: Isensee/P. Kirchhof, HStR XI, § 226 Rn. 53.
[227] Einheitliche Europäische Akte v. 01.07.1987, ABl. L 169 vom 29.6.1987.
[228] Vgl. Art. 6 des Vertrags über die Europäische Union (Vertrag von Maastricht) v. 01.11.1993, ABl. C 191 vom 29.7.1992.
[229] Vertrag über eine Verfassung für Europa v. 29.10.2004 (nicht in Kraft getreten).
[230] Haratsch u.a., Europarecht, 3. Kap. 1 III 9 (Rn. 33).

In einem zweiten Anlauf wurde die Charta jedoch fester und vollwertiger Teil des europäischen Primärrechts mit Inkrafttreten des Vertrags von Lissabon am 01. Dezember 2009. Inkorporiert wird die Charta durch einen Verweis von Art. 6 Abs. 1 EUV. Dieser Makel entfaltet jedoch letztlich keine rechtlichen Folgen. Zudem ist es auch konsequent. Die aktuellen Europäischen Verträge wollen gerade keine Verfassung sein, und ein Abschnitt über Grundrechte wäre ein traditioneller Teil einer solchen.

Die Charta der Grundrechte der Europäischen Union bindet gemäß Art. 51 Abs. 1 Satz 1 Charta die Organe, Einrichtungen und sonstigen Stellen der Europäischen Union. Auch die Mitgliedstaaten der EU sind an die Grundrechte der Charta gebunden. Dies allerdings nur dann, wenn sie EU-Recht ausführen. Insbesondere sind die Mitgliedstaaten verpflichtet, bei der Auslegung von Richtlinien eine Auslegungsvariante zu wählen, die keine Grundrechte der Charta oder der anderen allgemeinen Grundsätze des Unionsrechts verletzt.[231]

3. Bedeutung der EMRK im EU-Grundrechtsschutz

Die Europäische Konvention der Menschenrechte ist ein multilateraler völkerrechtlicher Vertrag, der dem Europarecht im weiteren Sinne zuzuordnen ist. Die EMRK ist nicht direkt Bestandteil des EU-Primär- oder Sekundärrechts, da die EU der EMRK bislang nicht als Vertragspartner beigetreten ist.

Die Konvention geht zurück auf einen Entwurf des Europarats, der bereits 1950, also deutlich vor Errichtung der Europäischen Gemeinschaften im Jahr 1957, von den Mitgliedern des Europarats unterzeichnet wurde. Im Jahr 1953 trat die Konvention dann in Kraft.[232] Inhaltlich gewährleistet die EMRK mit ihren Zusatzprotokollen ein breites Bündel an Menschenrechten, Freiheitsrechten und weiteren Garantien. Die Vertragsparteien, also alle Mitglieder des Europarats, sind gemäß Art. 1 EMRK verpflichtet, allen ihrer *„Hoheitsgewalt unterstehenden Personen“* die in der Konvention aufgeführten Menschenrechte zuzusichern. Der EMRK kommt für die Gewährleistung der Grundrechte der Bürger der Unterzeichnerstaaten eine bedeutende Rolle zu. Zum einen stellen die in ihr verbrieften Garantien einen gewissen Mindeststandard an Grundrechtsschutz im Gebiet der Vertragsstaaten sicher. Zum anderen besitzt die EMRK mit dem Europäischen Gerichtshof für Menschenrechte eine eigene und unabhängige Gerichtsbarkeit, die den subjektiven Grundrechtsschutz auch durchzusetzen in der Lage ist.[233]

Der EUV erklärt die Grundrechte der EMRK in Art. 6 Abs. 3 zu Grundsätzen des Unionsrechts. Art. 52 Abs. 3 Satz 1 Charta besagt, dass die durch die Charta garantierten Rechte die gleiche Reichweite und Bedeutung wie die entsprechenden Grundrechte der EMRK besitzen. Damit ist die EMRK auch für die Europäische Union bereits vor dem in

---

[231] Vgl. zu letzterem EuGH, Urt. v. 29.01.2008, Rs. C-275/06, Promusicae, Slg. 2008, I-00271, Rn. 68.
[232] *Bernhardt* in: Merten/Papier, Handbuch der Grundrechte VI/1, § 137 Rn. 19 ff.
[233] Vgl. *Bernhardt* in: Merten/Papier, Handbuch der Grundrechte VI/1, § 137 Rn. 57 ff., 76 ff.

Art. 6 Abs. 2 Satz 1 EUV angekündigten Beitritt zur Konvention faktisch bindendes Recht.

Da die Europäische Union der Europäischen Konvention der Menschenrechte entgegen des Auftrags des Art. 6 Abs. 2 EUV bislang nicht beigetreten ist, stellt sich die Frage, inwieweit die Organe der EU Urteile des Europäischen Gerichtshofs für Menschenrechte berücksichtigen müssen. Bis zum Beitritt der EU zur EMRK können Hoheitsakte der EU jedenfalls kein Prüfungsgegenstand eines Verfahrens vor dem EGMR sein.[234] Auch über den Umweg einer Inpflichtnahme der Mitgliedstaaten der EU, die etwa Richtlinien der Union in nationales Recht umgewandelt haben, scheidet nach der Rechtsprechung des EGMR eine Überprüfung von EU-Recht aus, solange die EU ein der EMRK zumindest gleichwertiges materielles Schutzniveau bietet.[235]

4. Verhältnis zwischen der Charta und den Grundrechten als Grundsätze des Unionsrechts

Gemäß Art. 6 Abs. 3 EUV stehen neben den Grundrechten der Charta und den Grundrechten der EMRK[236] als dritte Säule des Grundrechtsschutzes in der EU die *Grundrechte als allgemeine Grundsätze des Unionsrechts*. Rechtserkenntnisquelle zu den allgemeinen Grundsätzen sind neben der EMRK die überlieferten gemeinsamen Verfassungstraditionen der Mitgliedstaaten.

Die weitere rechtliche Relevanz der Grundrechte als Grundsätze – auch nach Inkrafttreten der Charta – ist allerdings umstritten. In der Diskussion dieser Problematik unterscheiden sich die Argumentationslinien der Kritiker, und zwar abhängig davon, welche Rechtserkenntnisquelle – EMRK oder Verfassungstraditionen – den allgemeinen Grundsätzen im konkreten Fall zugrunde gelegt wird.

So stellt sich die Frage, ob die Grundrechte als Grundsätze des EU-Rechts nach Inkrafttreten der Charta noch eine eigenständige rechtliche Bedeutung haben, soweit sie sich auf die überlieferten Verfassungstraditionen der Mitgliedstaaten beziehen. Frenz etwa hält dies für unnötig. Die Charta selbst sei bereits die Kodifizierung der gemeinsamen Verfassungstraditionen, was sich aus dem 5. Erwägungsgrund der Präambel der Charta ergebe.[237]

Diese Schlussfolgerung greift dennoch etwas zu kurz. Zwar will die Charta laut Erwägungsgrund 5 der Präambel der Charta u.a. die Verfassungstraditionen der Mitgliedstaaten bekräftigen, indem sie diesen eine schriftliche Form gibt. Es wird aber an jener Stelle

---

[234] *Schorkopf* in: Grabitz u.a., Recht der Europäischen Union Art. 6 EUV Rn. 47 (Stand: 68. Erg.-Lfg., Oktober 2019).
[235] EGMR, Urt. v. 20.06.2005, Nr. 45036/98, Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi ./. IRL, Rep. 2005-VI, S. 107, Rep. 2005-VI, § 157. Insoweit ähnelt die Lösung des EGMR der Solange-Rechtsprechung des Bundesverfassungsgerichts.
[236] Nach einem Beitritt der EU zur EMRK (wie in Art. 6 Abs. 2 Satz 1 EUV aufgegeben).
[237] Vgl. *Frenz*, Europarecht, Kap. 9 A II (Rn. 974).

nicht festgestellt, dass die Verfassungstraditionen der Mitgliedstaaten in der Charta abschließend berücksichtigt wurden. Dem EuGH muss es also in der Konsequenz weiter offenstehen, die Verfassungstraditionen der Mitgliedstaaten als Rechtserkenntnisquelle zur Auslegung der Grundsätze des Unionsrecht heranzuziehen und die Grundrechte auf dieser Basis gegebenenfalls über die materielle Reichweite der Charta hinaus zu erweitern.[238]

Daher ist etwa der Schutz der allgemeinen Handlungsfreiheit, der in der Charta keine Berücksichtigung findet, aber vom EuGH als allgemeiner Rechtsgrundsatz des Unionsrechts in der Rechtsprechung anerkannt ist, weiterhin gemäß Art. 6 Abs. 3 EUV durch das EU-Recht garantiert.[239] Zudem besitzen die Grundrechte als Grundsätze des EU-Rechts auf dem gesamten Territorium der Europäischen Union uneingeschränkt Gültigkeit, während dieses bezüglich der Charta wegen Art. 1 f. des Protokolls Nr. 30 zum Vertrag von Lissabon für Polen und das Vereinigte Königreich nicht gilt.[240] Daher ist ein Grundrechtsschutz durch den Rückgriff auf die Rechtsgrundsätze der EU mit Inkrafttreten der Charta nicht überflüssig geworden. Es spricht also vieles für eine fortbestehende eigenständige Bedeutung des Art. 6 Abs. 3 EUV.

Umstritten ist auch, ob die Grundrechte als Grundsätze des Unionsrechts, soweit Art. 6 Abs. 3 EUV zu deren Begründung auf die EMRK verweist, auch dann eigenständige Relevanz behalten werden, wenn die EU einmal der Europäischen Konvention der Menschenrechte beigetreten sein wird, wie dies der EU in Art. 6 Abs. 2 EUV aufgegeben wird. Da dies bislang jedoch nicht geschehen ist, bleiben die Grundsätze insoweit bis auf weiteres relevant.[241]

5. Gerichtliche Durchsetzung der Grundrechte im EU-Recht

Das Rechtsschutzsystem für die Bürger der Europäischen Union im Hinblick auf ihre europäischen Grundrechte ist anders aufgebaut als dasjenige des Grundgesetzes. EU-Bürger können sich nicht direkt an den EuGH wenden, um dort die Verletzung ihrer Grundrechte durch die Mitgliedstaaten zu rügen. Es gibt keinen der Verfassungsbeschwerde ge-

---

[238] *Ludwig*, EuR 2011, 715 (733); *Schmitz*, EuR 2004, 691 (708); kritisch insoweit hingegen *Scholz* in: Merten/Papier, Handbuch der Grundrechte VI/2, § 170 Rn. 7.

[239] *Kingreen* in: Calliess/Ruffert, EUV/AEUV, Art. 6 EUV Rn. 18.

[240] Für einen Überblick zu dieser Problematik vgl. *Borowsky* in Meyer/Hölscheidt, Charta der Grundrechte, Art. 51 Rn. 62 ff.; siehe auch EuGH, Urt. v. 21.12.2011, Rs. C-411/10 und C-493/10, C-411/10 , C-493/10, Slg. 2011, I-13905, Slg. 2011, I-13905, Rn. 116 ff..

[241] So hält etwa *Frenz*, Europarecht, Kap. 9 A II (Rn. 974), Art. 6 Abs. 3 EUV insoweit für redundant, da die EU mit einem Beitritt zur EMRK unmittelbar an diese gebunden wäre. *Pache/Rösch*, NVwZ 2008, 473 (475) und *Streinz u.a.*, Der Vertrag von Lissabon, § 14 V 1 (123) sind der Ansicht, dass die EMRK auch weiterhin als Rechtserkenntnisquelle für die allgemeinen Grundsätze des EU-Rechts ihre Bedeutung behalte. Diese Frage bedarf hier jedoch nicht der Klärung, da ein Beitritt der Union zur EMRK bislang nicht erfolgt ist und auch nicht unmittelbar bevor steht. Abseits der theoretischen Überlegungen weist *F. Kirchhof*, NJW 2011, 3681 (3686) zudem darauf hin, dass sich die zukünftige Bedeutung des Art. 6 Abs. 3 EUV wohl erst in der Praxis der Gerichte nach dem Beitritt der EU zur EMRK erweisen werde.

mäß Art. 93 Abs. 1 Nr. 4 GG vergleichbaren Rechtsbehelf im EU-Recht. Deutschen Bürger. steht allerdings der Rechtsweg in Form einer Verfassungsbeschwerde vor dem Bundesverfassungsgericht offen.[242]

Der in der Praxis für den Grundrechtsschutz der EU-Bürger einzig relevante Rechtsbehelf vor dem EuGH ist das Vorabentscheidungsverfahren gemäß Art. 267 EUV. Danach entscheidet der EuGH über die Auslegung der Europäischen Verträge und die Gültigkeit und die Auslegung der EU-Organe. Der EuGH kann im Verfahren nach Art. 267 EUV also abschließend über die Auslegung von EU-Recht entscheiden oder etwa europäisches Sekundärrecht für ungültig erklären. Die Urteile sind – anders als Urteile des EGMR – über den zu entscheidenden Einzelfall hinaus verbindlich.

Beim Vorabentscheidungsverfahren handelt es sich um einen indirekten Rechtsbehelf. Das bedeutet, dass der Bürger sich nicht direkt an den EuGH wenden kann. Sieht der Bürger sich in seinen Rechten aus dem EU-Recht verletzt, muss er Rechtsschutz im mitgliedstaatlichen Instanzenzug suchen. Hält das mitgliedstaatliche Gericht eine bislang ungeklärte Frage zur Auslegung über die Vertragsauslegung (dazu zählen auch die Grundrechte) oder Sekundärrecht für entscheidungserheblich, kann er die Entscheidung dem EuGH zur Entscheidung vorlegen. Handelt es sich beim mitgliedstaatlichen Gericht um die letzte Instanz im Rechtszug, ist es zur Vorlage verpflichtet.[243]

Dazu setzt das mitgliedstaatliche Gericht das Verfahren aus und stellt dem EuGH abstrakt formulierte Fragen zur Auslegung des Unionsrecht. Der EuGH beantwortet dann in seiner Entscheidung die ihm vorgelegten Fragen. Anhand dieser Auslegung entscheidet das mitgliedstaatliche Gericht schließlich den ihm vorliegenden Sachverhalt.[244]

6. Grundrechtsverpflichtete der Charta

Die Charta verpflichtet gemäß Art. 51 Abs. 1 Charta zum einen die Organe und sonstigen Einrichtungen der EU, zum anderen die Mitgliedstaaten. Die Mitgliedstaaten sind allerdings nur insoweit an die Grundrechte gebunden, soweit sie Unionsrecht ausführen. Im Umkehrschluss bedeutet dies, dass die Mitgliedstaaten nicht an die Grundrechte der Charta gebunden sind, soweit sie weder europäisches Primärrecht noch Richtlinien oder Verordnungen umsetzen oder ausführen. Die Grundrechtsberechtigung ergibt sich jeweils direkt aus dem jeweiligen Grundrecht.

Im Rahmen einer Datenverkehrsregulierung zur Durchsetzung des Urheberrechts sind die Mitgliedstaaten an die Grundrechte der Charta gebunden, da dieser Komplex durch europäisches Sekundärrecht geregelt ist.[245]

---

[242] BVerfG, Beschl. v. 06.11.2019, 1 BvR 276/17, Recht auf Vergessen II, BVerfGE 152, 216 (juris-Rn. 53)
[243] *Haltern*, Europarecht, Bd. II, Rn. 118.
[244] *Haltern*, Europarecht, Bd. II, Rn. 121.
[245] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 1; vgl. auch oben Kap. 2 III 1–4 (S. 56 ff.).

IV. Vereinbarkeit der Datenverkehrsregulierung mit den Grundrechten der Charta nach der Rechtsprechung des EuGH

Die wichtigsten Erkenntnisquellen bei der Ermittlung des europarechtlich zulässigen Rahmens für Eingriffe in den Datenverkehr zur Urheberrechtsregulierung sind das europäische Primärrecht sowie die einschlägige Judikatur des EuGH. Zur Interpretation der Rechtsprechung und Auslegung des Primärrechts sind zudem die Schlussanträge der Generalanwälte des EuGH bisweilen von Bedeutung, auch wenn diese keine rechtliche Verbindlichkeit besitzen: Jedenfalls wenn die Spruchkammer des EuGH den Empfehlungen des jeweiligen Generalanwalts folgt, liegt der Gedanke nahe, dass die dogmatischen Ausführungen der Generalanwälte den Gerichtshof in den meisten Fällen bei seiner Entscheidungsfindung leiten und somit in gewissem Maße dem Urteil zugrunde liegen.[246]

Die durch das europäische Primärrecht gesetzten Grenzen werden in erster Linie durch die auf europäischer Ebene garantierten Grundrechte bestimmt, die aus den in der Charta verbürgten Garantien und den allgemeinen Grundsätzen des EU-Rechts zu entnehmen sind und durch die Entscheidungen des EuGH ausgelegt werden. Die EMRK und die Urteile des EGMR sind dabei für die Auslegung beider Rechtsquellen von erheblicher Bedeutung.[247]

Der EuGH hat in zwei Entscheidungen bereits zu einem großen Teil das definiert, was auf europarechtlicher Ebene den oben angesprochenen Rahmen einer Datenverkehrsregulierung zum Urheberrechtsschutz bildet.

In der Entscheidung SABAM ./. Scarlet Extended (im Folgenden auch: Scarlet-Entscheidung) hatte der EuGH über eine sehr weitgehende und grundrechtsintensive Form der Datenverkehrsregulierung zu urteilen.[248] Konsequenterweise gab dies dem EuGH dann auch die Gelegenheit, festzustellen, welche Art von Datenverkehrsregulierung zum Urheberrechtsschutz *auf jeden Fall* europarechtswidrig ist.

Umgekehrt lag dem Urteil UPC Telekabel ./. Constantin/Wega (im Folgenden auch: UPC-Entscheidung) ein vergleichsweise sanfter Sachverhalt zu Grunde in Bezug auf die mit

---

[246] Darauf weist z.B. die Tatsache hin, dass der EuGH seine Entscheidungen auf seinem Internet-Auftritt zusammen mit den zugehörigen Schlussanträgen der Generalanwälte veröffentlicht, vgl. etwa https://curia.europa.eu/jcms/jcms/P_106320?rec=RG&jur=C (zuletzt besucht am 09.10.2021).
[247] Siehe oben Kap. 2 III 1 (S. 60) und Kap. 2 III 3 (S. 63).
[248] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 15 ff. die Entscheidung ist nicht zu verwechseln mit EuGH, Urt. v. 16.02.2012, SABAM, Rs. C-360/10, EU:C:2012:85, die ein Vorgehen SABAMs gegen den Betreiber eines Internet-Plattformbetreibers zum Thema hat. Im Wesentlichen sind der Tenor und ein großer Teil der Entscheidungsgründe mit Scarlet ./. SABAM gleichlautend. Die technischen und grundrechtlichen Implikationen bei einem Content Provider sind allerdings weniger drastisch als bei der Regulierung des Datenverkehrs beim Internet Service Provider, z.B. weil die Überwachung auf einen kleineren Nutzerkreis beschränkt bleibt und keine vergleichbaren Kosten verursacht, da die Überprüfung der Daten nicht in Echtzeit erfolgen muss und sie auch vom Charakter eher repressiv als präventiv ist.

der streitgegenständlichen Datenverkehrsregulierung verbundenen Grundrechtbeeinträchtigungen.[249]

Da die europarechtliche Rechtsprechung zur Datenverkehrsregulierung bislang im Wesentlichen auf den soeben genannten Entscheidungen des EuGH basiert, ist es sachgerecht, die Vereinbarkeit von Eingriffen in den Datenverkehr zur Urheberrechtsdurchsetzung mit europäischen Grundrechten ausgehend von diesen Entscheidungen und dem zugrunde liegenden Sachverhalt zu untersuchen und diese zugleich kritisch zu würdigen.

1. SABAM ./. Scarlet Extended

Die Scarlet-Entscheidung erging in einem Vorabentscheidungsverfahren gemäß Art. 267 EUV. Die dem EuGH vorgelegten Fragen traten auf im Rahmen eines Rechtsstreits zwischen einer belgischen Rechteverwertungsgesellschaft, der „Société belge des auteurs, compositeurs et éditeurs SCRL“ (im Folgenden: SABAM), die Autoren, Komponisten und Herausgeber von Musik vertritt, und dem ebenfalls belgischen Internet Service Provider Scarlet Extended SA (im Folgenden: Scarlet).

SABAM hatte herausgefunden, dass die Nutzer gewisser Peer-to-Peer-Netzwerke urheberrechtlich geschützte Werke teilten, die zu ihrem Repertoire gehörten. Dafür hatten diese aber weder eine Erlaubnis eingeholt noch Gebühren entrichtet. Der ganze Vorgang war u.a. über das Telekommunikationsnetz von Scarlet erfolgt. Kurz gesagt: Kunden von Scarlet hatten sich in illegalem Filesharing betätigt.

SABAM verlangte daher von Scarlet, den Datenverkehr zu filtern, der durch Scarlets Netz über Peer-to-Peer-Programme übertragen wird, um derartige Urheberrechtsverletzungen zukünftig zu unterbinden. Nachdem Scarlet sich geweigert hatte, der Aufforderung von SABAM nachzukommen, verklagte SABAM den ISP schließlich im Jahr 2004 vor einem belgischen Gericht. Zwar behauptete sie nicht, dass Scarlet selbst Täter der Urheberrechtsverletzungen sei. Der illegale Austausch der Musikdateien sei jedoch im Rahmen einer Inanspruchnahme von Dienstleistungen der Scarlet erfolgt. Außerdem befinde sich der ISP in einer idealen faktischen Position, solcherlei Rechtsverletzungen zu unterbinden.[250]

SABAM beantragte dann im Wesentlichen, Scarlet zu verurteilen, das illegale Filesharing abzustellen, indem sie es ihren Kunden unmöglich machen sollte, Musik aus dem Repertoire von SABAM in irgendeiner Form über ein Peer-to-Peer-Programm zu senden oder zu empfangen.[251]

Wie bereits oben kurz erwähnt, ist die Datenverkehrsregulierung, die diesem Fall zu Grunde liegt, eine in ihrer Intensität sehr weitreichende. Das wird durch Darstellung noch einmal deutlich. Scarlet sollte

---

[249] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 11 ff.
[250] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959 Rn. 15 ff.
[251] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959 Rn. 20.

- auf eigene Kosten
- zeitlich unbegrenzt
- für sämtliche Kunden generell
- präventiv
- *jegliche* ein- und ausgehende *Kommunikation*
- durchsuchen, um

- *behauptete* Urheberrechtsverletzungen zu
- identifizieren und
- durch *Filtern* oder *Blocken* zu verhindern.[252]

Es ist schwerlich eine datenverkehrsregulierende Maßnahme vorstellbar, die noch höhere Anforderungen an den ISP stellt und noch tieferes Eingreifen in den Datenverkehr und die Grundrechte der Nutzer verlangt. Nicht nur soll nach dieser Variante der Datenverkehrsregulierung der ISP, der selbst kein Täter ist, die Kosten für die Verhinderung von Rechtsverletzungen tragen.

Die Maßnahme wäre auch nicht auf den Einzelfall beschränkt, sondern auf Dauer angelegt. Die Überwachung würde sich nicht auf die Kommunikation verdächtiger Teilnehmer bei konkreten Verdachtsmomenten beschränken, sondern präventiv die gesamte Kommunikation auch sämtlicher unbescholtener Teilnehmer ins Ziel nehmen. Hinzu käme, dass die Eingriffe in den Datenverkehr nicht nur gegen solche Werke gerichtet wäre, an denen SABAM nachgewiesenermaßen Rechte besäße. Der Antrag SABAMs verlangte, dass die bloße Behauptung SABAMs genügen müsste, dass die Rechte Teil ihres Repertoires seien.

Aus technischer Perspektive handelt es sich bei dieser Form der Datenverkehrsregulierung um eine Deep Packet Inspection. Eine DPI ist das Auslesen und/oder die elektronische Verarbeitung von über das Internet gesendeter Daten, die innerhalb der Transport- und der Anwendungsschicht im TCP/IP-Referenzsystem liegen und in deren Auslesen und/oder deren Verarbeitung der Absender nicht schon deshalb zugestimmt hat, weil die von ihm veranlasste Kommunikation ansonsten aus logisch zwingenden Gründen nicht stattfinden könnte.[253] Das „streitige Filtersystem“, wie der EuGH die fragliche Datenverkehrsregulierung in dieser Entscheidung bezeichnet,[254] würde erfordern, dass der ISP, in diesem Fall Scarlet, die über sein Netz übertragenen Daten ausliest und auf die Frage hin analysiert, ob es sich um spezifische urheberrechtlich geschützte Werke handelt, an denen die SABAM behauptet, Rechte zu besitzen, und ob diese über Peer-to-Peer-Netzwerke übertragen wurden.

---

[252] Vgl. den Wortlaut der ersten Vorlagefrage: EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 28.
[253] Vgl. oben Kap. 1 III 3 c) (S. 26).
[254] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 29.

Datenverkehr kann sich beispielsweise dadurch als Peer-to-Peer-Kommunikation zu erkennen geben, dass er für diese Anwendung typische Protokolle in der Anwendungsschicht verwendet. Zur Identifizierung des Peer-to-Peer-Datenverkehrs ist es daher erforderlich, mit einer Datenanalyse bis hinunter in die Anwendungsschicht (Layer 4) des TCP/IP-Stapels vorzudringen, um durch eine Analyse des Headers dieser Schicht die verwendeten Protokolle zu ermitteln. Eine Identifizierung über die Analyse der Internet-Schicht kann die für das geforderte Filtersystem gesetzten Ziele nicht erreichen, da die IP-Adresse über die verwendeten Anwendungsprotokolle keine Aussagekraft besitzt. Ein Blick in die Transportschicht würde nur eine sehr begrenzte Effektivität versprechen. Zwar verwendeten Peer-to-Peer-Anwendungen einst standardmäßig gewisse Ports, mittlerweile haben sich diese Programme jedoch größtenteils von dieser Praxis verabschiedet.

Mit der Untersuchung des Headers der L_4 ist es jedoch bei diesem Filtersystem nicht getan. Hat der ISP festgestellt, dass sein Netzwerk für Peer-to-Peer-Kommunikation genutzt wird, ist für eine Datenverkehrsregulierung, wie SABAM sie verlangte, zwingend auch ein Blick in die Nutzdaten des Datenpakets erforderlich. Denn um die übertragenen Dateien als solche Werke zu identifizieren, an denen SABAM Rechte zustehen sollen, muss der ISP eine Datenbank vorhalten, die einen Abgleich der übertragenen mit den geschützten Daten ermöglicht. Auf Seite der übertragenen Daten ist es jedoch – unabhängig vom informationstechnischen Verfahren – denknotwendig, diese auf ihren Inhalt zu untersuchen und den Inhalt auch zu identifizieren. Der Payload der über das Netzwerk gesendeten Datenpakete wird dem ISP bei einem solchen Filtersystem also offengelegt, zumindest soweit die Kommunikation über Peer-to-Peer-Programme erfolgt.

Schließlich werden die Daten dann nach Durchlaufen des Abgleichs mit der Datenbank der geschützten Musiktitel je nach Ergebnis dieser Datenverarbeitung unterschiedlich weiterverarbeitet: Entweder dürfen sie ungehindert passieren oder der ISP unterbricht den Kommunikationsvorgang.

Das Auslesen und die Datenverarbeitung sind zudem auch kein logisch notwendiger Schritt, um eine Kommunikation des Nutzers zu ermöglichen. Zweck des Filtersystems ist die Durchsetzung des Urheberrechts an bestimmten Werken, nicht die technische Realisierung der Kommunikation.[255]

Scarlet sah in der Anordnung einer solchen Form der Datenverkehrsregulierung eine Verletzung von Art. 15 der Richtlinie 2000/31/EG[256] (E-Commerce-Richtlinie). Durch die Anordnung werde sie gezwungen, sämtliche Kommunikation in ihrem Netz zu überwachen.[257] Die DVR würde auch unionsrechtliche Vorschriften des Datenschutzes und der

---

[255] Vgl. zu den vorangegangenen technischen Ausführungen die Erläuterungen zur Funktionsweise der Deep Packet Inspection oben Kap. 1 III 3 (S. 19 ff.).
[256] Richtlinie 2000/31/EG über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt.
[257] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 25.

Vertraulichkeit des Datenverkehrs verletzen. Es sei zudem unklar, ob eine solche Institution tatsächlich effektiv sei; jedenfalls auf Dauer würde sie sicherlich von den Nutzern umgangen werden.[258] Zudem stünden technische Probleme wie die Grenzen der Netzkapazität der Datenverkehrsregulierung entgegen.[259]

Nachdem das erstinstanzliche Gericht der Klage zunächst stattgegeben hatte und Scarlet Berufung eingelegt hatte, kamen dem Berufungsgericht (dem Cour d'appel de Bruxelles) Zweifel, ob die Pflichten zur Überwachung und Filterung, die Scarlet auferlegt werden sollten, mit Europarecht vereinbar seien. Daher rief das Berufungsgericht in einem Vorlageverfahren den EuGH an und legte diesem zwei Fragen zur Auslegung des in diesem Fall einschlägigen Europarechts vor.[260] Die erste Frage lautete, ob Vorschriften der Richtlinien 2001/29/EG[261] (InfoSoc-Richtlinie) und 2004/48/EG[262] (Enforcement-Richtlinie) in Verbindung mit der Richtlinie 95/46/EG[263] (Datenschutz-Richtlinie), der E-Commerce-Richtlinie und der Richtlinie 2002/58/EG[264] (ePrivacy-Richtlinie) die richterliche Anordnung dieser Form von Datenverkehrsregulierung zum Urheberrechtsschutz erlauben, wenn sie im Lichte von Art. 8 und Art. 10 der EMRK ausgelegt werden.[265] Mit der zweiten Frage wollte das Vorlagegericht zudem erfahren, ob – wenn die erste Frage mit Ja beantwortet würde – bei der richterlichen Entscheidung über die Anordnung der Datenverkehrsregulierung der Verhältnismäßigkeitsgrundsatz zu beachten wäre, insbesondere im Hinblick auf die Wirksamkeit und die abschreckende Wirkung der Maßnahme.

Der EuGH erklärt die in diesem Fall streitige Datenverkehrsregulierung für nicht mit dem EU-Recht vereinbar.[266] Die Begründung seiner Entscheidung ist knapp. Dennoch

---

[258] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 26.
[259] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 24.
[260] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 28.
[261] Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft.
[262] Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums.
[263] Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Die Richtlinie wurde am 25.05.2018 durch die VO (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO) ersetzt.
[264] Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.
[265] Art. 8 EMRK garantiert das Recht auf Achtung des Privat- und Familienlebens, Art. 10 EMRK das Recht auf freie Meinungsäußerung. Die entsprechenden Grundrechte der Charta sind Art. 7 (Achtung des Privat und Familienlebens) und Art. 11 Charta (Freiheit der Meinungsäußerung und Informationsfreiheit). Darüber hinaus gewährt Art. 8 Charta das eigenständige Grundrecht auf den Schutz personenbezogener Daten. Die fehlende Bezugnahme des vorlegenden mitgliedstaatlichen Gerichts auf die korrespondierenden Grundrechte der Charta erklärt sich womöglich daraus, dass die EuGH-Vorlage dem Januar/Februar 2010 entstammt und die Charta zu diesem Zeitpunkt erst seit kurzer Zeit in Kraft getreten war. Der EuGH hingegen befasst sich konsequent in den Gründen seiner Entscheidung mit den Grundrechten der Charta anstelle derer der EMRK.
[266] Auf die zweite Vorlagefrage geht der EuGH dementsprechend nicht ausdrücklich ein. In EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 36 stellt der Gerichtshof jedoch fest, dass Überwachungsmaßnahmen für Provider gerecht und verhältnismäßig zu sein haben. Dazu verweist er auf Art. 3 der Enforcement-Richtlinie sowie seine Rechtsprechung im Fall EuGH, Urt. v. 12.07.2011, Rs. C-324/09, L'Oreal/eBay, Slg. 2011, I-06011, Rn. 139.

lässt der EuGH teilweise erkennen, wo er rote Linien zieht. Zudem gibt der EuGH ein (sehr grobes) Prüfungsprogramm vor, das er in vergleichbaren Fällen zukünftig anzuwenden wird.

Zunächst stellt der EuGH in den Entscheidungsgründen fest, dass das streitige Filtersystem gegen Sekundärrecht verstoße, und zwar gegen Art. 15 Abs. 1 der E-Commerce-Richtlinie. Dieser verbietet es den Mitgliedstaaten, Internet Service Providern wie Scarlet eine *„allgemeine Verpflichtung“* aufzuerlegen, die über ihr Telekommunikationsnetz übertragenen Daten zu überwachen oder von sich aus nach rechtwidrigem Verhalten zu suchen. Dies schließe eine Überwachung im Einzelfall zwar nicht aus, wohl aber die hier streitgegenständliche präventive und flächendeckende Deep Packet Inspection, die eine generelle Überwachung des Datenverkehrs darstelle.[267]

Primärrechtlich beruht die Entscheidung auf drei Säulen. Ausgangspunkt der Prüfung ist aber zunächst Art. 17 Abs. 2 Charta. Die Anordnung des Filtersystems solle die Urheberrechte der SABAM schützen. Diese seien als geistiges Eigentum gemäß Art. 17 Abs. 2 Charta geschützt. Allerdings werde die Eigentumsfreiheit, dessen Teil die Gewährleistung des geistigen Eigentums sei, nicht schrankenlos gewährleistet. Es werde durch konkurrierende Grundrechte begrenzt. Daher sei zu beachten, dass Gerichte und Behörden, die Maßnahmen zum Schutz des geistigen Eigentums anordnen, ein angemessenes Gleichgewicht mit den Grundrechten derjenigen sicherstellen müssten, die durch die Maßnahmen betroffen sind.[268]

Das erste mit der Eigentumsfreiheit konkurrierende Grundrecht, das der EuGH prüft, ist die unternehmerische Freiheit des ISP, die durch Art. 16 Charta[269] garantiert wird. Der EuGH erklärt die unternehmerische Freiheit durch die Anordnung eines DPI-Filtersystems als *verletzt*, da es bei einem solchen System an einem angemessenen Gleichgewicht zwischen dem Schutz des geistigen Eigentums der Urheberrechtsinhaber und dem Schutz der unternehmerischen Freiheit der Internet Service Provider fehle. Die Gründe für dieses fehlende Gleichgewicht sieht der EuGH darin, dass der ISP *sämtliche* Kommunikation in seinem Netz überwachen solle, die Überwachung zudem nicht *in der Dauer begrenzt* sei, sich dabei ferner auch auf *zukünftige* Verletzungen beziehen und schließlich auch solche Werke schützen solle, die im Zeitpunkt der Anordnung noch gar *nicht geschaffen* worden seien.

---

[267] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959 Rn. 35 ff.
[268] Vgl. EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 42 ff. mit Verweis auf EuGH, Urt. v. 29.01.2008, Rs. C-275/06, Promusicae, Slg. 2008, I-00271, Rn. 62 ff.
[269] Art. 16 Charta geht u.a. auf einen allgemeinen Grundsatz des Unionsrechts zurück, vgl. ABl 2007/C 303/17 (23), dort mit Verweisen auf EuGH, Urt. v. 15.07.1960. Rs. C-36/59, C-37/59, C-38/59 und C-40/59, Nold, Slg. 1960, S. 887 (921); EuGH, Urt. v. 27.09.1979. Rs. C-230/78, Slg. 1979, S. 2749 (2768, 2771), Rn. 20 und 31; EuGH, Urt. v. 16.01.1979, Rs. C-151/78, Slg. 1079, S. 1 (13), Rn. 19 und EuGH, Urt. v. 05.10.1999, Rs. C-240/97, Slg. 1999, I-6571, Rn. 99. Weiterhin stützt sich Art. 16 Charta auf die Anerkennung des freien Wettbewerbs durch Art. 119 Abs. 1 und 3 AEUV.

Im Ergebnis führe dies zu einer *qualifizierten* Beeinträchtigung des ISP, da er verpflichtet würde, ein *kompliziertes, kostspieliges, auf Dauer angelegtes* und *allein auf seine Kosten betriebenes* System zur technischen Überwachung aufzubauen und zu betreiben. Im Übrigen verstoße diese DVR aus denselben Gründen auch gegen Art. 3 Abs. 1 der *Enforcement*-Richtlinie, der bestimmt, dass Institutionen zur Durchsetzung des Urheberrechts nicht unnötig kompliziert und kostspielig sein dürfen.[270]

Das nächste Grundrecht, auf das der EuGH hier eingeht, ist das durch Art. 8 Charta garantierte Recht auf den Schutz personenbezogener Daten. Dabei gehe es nicht wie soeben um ein Grundrecht des ISP, sondern um das Grundrecht der Internet-Nutzer, die über das Netz des ISP kommunizieren. Dieses Recht sieht der EuGH nach dem Wortlaut der Entscheidung nicht zwingend als verletzt, aber jedenfalls als *beeinträchtigt* an. Der EuGH stellt knapp fest, dass das streitige Filtersystem systematisch alle über das Netz des Internet Service Providers übertragenen Inhalte analysiere und dann die IP-Adressen all derer sammle, die an der Übertragung der geschützten Inhalte beteiligt seien. Bei den IP-Adressen handele es sich jedoch um personenbezogene Daten, da über die IP-Adressen die Möglichkeit bestünde, die Nutzer eindeutig zu identifizieren, die hinter der Adresse stünden.[271]

Weiterhin sieht der EuGH durch das DPI-Filtersystem das Recht auf Informationsfreiheit gemäß Art. 10 Abs. 1 EMRK bzw. Art. 11 Charta beeinträchtigt. Dies begründet er damit, dass ein Filtersystem zwar womöglich zwischen geschützten und nicht geschützten Werken unterscheiden könne, nicht jedoch zwischen urheberrechtlich zulässigen und unzulässigem Datenverkehr. Der Austausch von geschützten Werken sei jedoch nicht zwangsläufig illegal, da in den Mitgliedstaaten der EU verschiedene gesetzliche Ausnahmen vom Urheberrecht bestünden, etwa wenn das Werk gemeinfrei oder die geteilte Datei kostenfrei von den jeweiligen Urhebern ins Netz gestellt worden sei.[272]

Die soeben skizzierte Entscheidung gibt einige Antworten auf die hier gestellten Fragen, lässt aber leider ebenfalls wesentliche Fragen ungeklärt oder wirft gar neue Fragen auf.

Positiv feststellen lässt sich zunächst, dass der EuGH die Grundrechte der Charta bestimmt hat, die er von einer Deep Packet Inspection berührt sieht. Dies sind die Eigentumsfreiheit gemäß Art. 17 Charta auf Seiten der Urheber und Verwerter, die unternehmerische Freiheit gemäß Art. 16 Charta auf Seiten der Internet Service Provider und die Informationsfreiheit gemäß Art. 11 Charta sowie das Recht auf den Schutz personenbezogener Daten gemäß Art. 8 Charta der Internet-Nutzer.

a. Unternehmerische Freiheit, Art. 16 Charta

Eine besondere Rolle in der Scarlet-Entscheidung des EuGH nimmt die unternehmerische Freiheit gemäß Art. 16 Charta ein. Der EuGH stellt fest, dass eine Deep Packet Inspection

---

[270] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 47 f.
[271] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 51.
[272] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 52.

des gesamten Internet-Datenverkehrs, der durch das Netz eines Internet Service Providers läuft, zum Zweck der Durchsetzung des Urheberrechts nicht mit der Gewährleistung der unternehmerischen Freiheit vereinbar ist, wenn die DPI hohe Kosten verursacht und ausschließlich auf Rechnung des ISP erfolgt.

Aus dieser Aussage jedoch abzuleiten, dass jegliches DPI-Filtersystem nach Ansicht des EuGH gegen die unternehmerische Freiheit verstößt, könnte falsch sein. Die vordergründig klare Aussage, dass die Verpflichtung eines ISP zur Überwachung und Analyse des gesamten Internet-Datenverkehrs zur Durchsetzung des Urheberrechts die unternehmerische Freiheit verletze, relativiert sich in ihrer allgemeinen Bedeutung, wenn man berücksichtigt, dass sie gleich zwei Einschränkungen unterliegt. Zum einen müsse das einzurichtende EDV-System sehr kostspielig sein, zum anderen der Internet Service Provider selbst die Kosten der Einrichtung und des Betriebs des Systems tragen.

Der EuGH geht nicht darauf ein, wie sich die Rechtslage darstellen würde, wenn diese zwei Bedingungen sich zukünftig ändern sollten. Die Kosten für ein solches System könnten schließlich mit dem technischen Fortschritt sinken. Außerdem ist es denkbar, dass in Zukunft die Urheberrechtsverwerter oder die Allgemeinheit bereit sein könnten, die Kosten ganz oder zumindest teilweise zu übernehmen. Von Interesse wäre, wie der EuGH in solch einem Fall bezüglich der Verletzung von Art. 16 Charta entscheiden würde.

b. Gewährleistung des Schutzes personenbezogener Daten, Art. 8 Charta

Der EuGH sieht durch die streitige Variante der Datenverkehrsregulierung auch die Gewährleistung des Schutzes personenbezogener Daten beeinträchtigt. Er begründet dies damit, dass das streitige Filtersystem das Sammeln und Identifizeren der IP-Adressen derjenigen Nutzer erfordere, die sich als Filesharer betätigen. Bei diesen IP-Adressen handele es sich um personenbezogene Daten, da die hinter diesen Adressen stehenden Nutzer eindeutig identifiziert werden könnten.[273]

Die Personenbezogenheit insbesondere dynamisch an die Nutzer vergebener IP-Adressen war in der Rechtswissenschaft lange Zeit umstritten, da eine IP-Adresse isoliert betrachtet keinen Personenbezug aufweist. Sie ist grundsätzlich nicht mehr als eine Zahl, die einen an das Internet angeschlossenen Rechner für einen anderen Rechner erreichbar macht, der sich an einem anderen Ort befindet. Damit handelt es sich dem Grunde nach um ein Datum, das sich unmittelbar auf eine Sache und damit gerade nicht auf eine Person bezieht.[274]

Eignet sich allerdings die IP-Adresse im Einzelfall oder generell auch dazu, einen über das Internet abgewickelten konkreten Kommunikationsvorgang einer spezifischen Person eindeutig zuzuordnen, wird die potentielle Personenbezogenheit deutlich. Unproblematisch ist die Personenbezogenheit der Daten daher stets für den Access Provider des In-

[273] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 51.
[274] EuGH, Urt. v. 19.10.2016, Rs. C-582/14, Breyer, EU:C:2016:779, Rn. 38.

ternet-Nutzers. Der Access Provider besitzt die Möglichkeit der Datenzuordnung zur Person in jedem Fall. Bei ihm sind zum einen Kunden- und Abrechnungsdaten zu einem Netzanschluss (die sogenannten Bestandsdaten) hinterlegt, zum anderen ordnet er selbst dem Anschluss des Nutzers dessen IP-Adresse zu. Er kann die Daten problemlos zusammenführen.[275] Zwar weiß auch der Access Provider nicht mit Sicherheit, wer hinter dem Rechner sitzt, der die diesem zugewiesene IP-Adresse nutzt. Er kennt jedoch zumindest den Besitzer des Netzanschlusses, über den kommuniziert wird. Für einen Access Provider (und damit auch für die meisten ISPs) handelt es sich bei der Erhebung und Verarbeitung von IP-Adressen daher immer um personenbezogene Daten.[276]

Wenig diskutabel ist die Frage auch für statische IP-Adressen. Hier ist der Personenbezug unabhängig von der Stelle, bei der sie anfallen, in der Regel zu bejahen.[277] Statische IP-Adressen sind solche, die einem Nutzer dauerhaft zugewiesen sind. In erster Linie besitzen institutionalisierte Nutzer statische IP-Adressen, also Anbieter von Webseiten und Internet-Dienste, Universitäten etc. Diese IP-Adressen sind naturgemäß den ISPs der Nutzer bekannt, die die IP-Adressen schließlich dem konkreten Anschluss zuordnen. Sie sind aber auch für Dritte relativ einfach den dahinterstehenden Personen zuzuordnen, etwa über sogenannte WHOIS-Anfragen, die jedermann unter Behauptung eines berechtigten Interesses stellen kann.[278] Nutzer statischer IP-Adressen sind im Kontext des Filesharings letztlich jedoch wenig relevant, da der weit überwiegende Teil der Filesharer keine statische Adresse besitzt.

Der eigentliche Streitpunkt war, ob es sich für Personen und Stellen, die dynamische IP-Adressen erheben und verarbeiten und keine ISPs sind, auch um personenbezogene Daten handelt. Hier treffen in der Rechtswissenschaft zwei Schulen aufeinander. Die eine möchte den Personenbezug von Daten *absolut* bestimmen, die andere *relativ*.

Bei einem absoluten Verständnis der Personenbezogenheit sind Daten unabhängig von der Stelle, die die Daten verarbeitet, als personenbezogen anzusehen, wenn das Datum von einer beliebigen dritten Stelle einer Person zugeordnet werden könnte.[279] Nach dieser Lehre handelt es sich sowohl bei statischen als auch bei dynamischen IP-Adressen unabhängig von der verarbeitenden Stelle um personenbezogene Daten.

---

[275] EuGH, Urt. v. 19.10.2016, Rs. C-582/14, Breyer, EU:C:2016:779, Rn. 49; *Gerlach*, CR 2013, 478 (479). Vgl. auch Art. 2 lit. a und Erwägungsgrund 26 der Richtlinie 95/46 bzw. Art. 4 und Erwägungsgrund 30 der DSGVO.

[276] Vgl. auch BGH, Urt. v. 13.01.2011, II ZR 146/10, Rn. 17 (juris); *Eckhardt*, CR 2011, 339 (340).

[277] So auch z.B. *Eckhardt*, CR 2011, 339 (340); *Krüger / Maucher*, MMR 2011, 433 (434).

[278] Eine einfache Suchanfrage in einer etablierten Internet-Suchmaschine der Wahl nach „WHOIS IP“ fördert eine Vielzahl einschlägiger Angebote zu Tage.

[279] So AG Berlin-Mitte, Urt. v. 27.03.2007, 5 C 314/06, Rn. 14 (juris); *Weichert* in: Däubler u.a., BDSG, § 3 BDSG Rn. 13 ff.; Die Obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten, 2009, abrufbar unter https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/B_Datenschutzkonforme%20Ausgestaltung%20von%20Analyseverfahren%20zur.pdf (zuletzt besucht am 09.10.2021).

Die Schule, die den Datenbezug *relativ* bestimmen möchte, grenzt nach der Fähigkeit der datenverarbeitenden Stelle ab, die Daten einer Person mit vertretbarem Aufwand selbst zuzuordnen.[280] Eine IP-Adresse könnte also für die eine Stelle personenbezogen sein, für die andere hingegen nicht. Relevant wird dies bei dynamischen IP-Adressen.

Privaten Nutzern, also solchen, die eher auf der Nachfrager- oder Host-Seite des Netzes stehen, werden in der Regel von ihren ISP keine statischen, sondern dynamische IP-Adressen zugewiesen. Hintergrund ist die Vielzahl an Nutzern und die nur beschränkte Anzahl an verfügbaren Adressen im IPv4-Adressraum. Den Access Providern stehen nicht genügend IP-Adressen für alle ihre Kunden zur Verfügung, denen sie Zugang zum Netz versprochen haben.

Allerdings wollen nicht alle Nutzer zeitgleich ins Netz. Wählt sich ein Nutzer ins Internet ein, bekommt er eine IP-Adresse, die in jenem Moment von keinem anderen Nutzer des ISP verwendet wird. Bei einer erneuten Einwahl wird dies jedoch nach aller Wahrscheinlichkeit eine andere Adresse sein als die, die dem Nutzer beim letzten Einwahlversuch zugeteilt wurde, da die Verteilung zufällig erfolgt. Die dynamische IP-Adresse eines Nutzers ist dabei grundsätzlich nur seinem Access Provider bekannt. Aus dessen Sicht handelt es sich also um ein personenbezogenes Datum. Schwieriger ist dies für andere Stellen zu beantworten. Es besteht keine Möglichkeit einer WHOIS-Abfrage. Um hinsichtlich einer bestimmten Stelle von Personenbezogenheit sprechen zu können, müsste diese Stelle daher auf die eine oder andere Weise an die Daten des ISP gelangen können.

Manche Stimmen haben geäußert, der EuGH hätte bereits mit dem Scarlet-Urteil den Streit zugunsten der absoluten Interpretation der Personenbezogenheit entschieden, jedenfalls, soweit dies IP-Adressen anbelange.[281] Der Wortlaut der Entscheidung lässt diese Interpretation grundsätzlich zu. Der EuGH stellte fest, dass IP-Adressen personenbezogene Daten seien, ohne dabei zu relativieren. Er traf insoweit keine weitere Differenzierung danach, ob die datenverarbeitende Stelle tatsächlich Zugriff auf die IP-Adressen hat.

Der EuGH entschied die Frage des Personenbezugs von IP-Adressen jedoch mittlerweile unmissverständlich in der sogenannten Breyer-Entscheidung und ordnete gleichzeitig die entsprechenden Äußerungen in der Scarlet-Entscheidung: Zwar habe der EuGH in der Scarlet-Entscheidung festgestellt, dass IP-Adressen personenbezogene Daten seien. Dies habe sich jedoch nur auf den dort zu entscheidenden Fall bezogen, dass IP-Adressen vom Access Provider verarbeitet würden, der zugleich die zur Identifizierung der Nutzer notwendigen weiteren Informationen besitze.[282] In Fällen, in denen die datenverarbeitende

---

[280] OLG Hamburg, Beschl. v. 03.11.2010, 5 W 126/10; LG Berlin, v. 31.01.2013, 57 S 87/08; *Gerlach*, CR 2013, 478 (481), der den Personenbezug sowohl von statischen als auch dynamischen IP-Adressen verneint, die vom Internet Service Provider vergeben wurden, da in beiden Fällen eine WHOIS-Abfrage gleichermaßen ins Leere laufe; *Gola/Klug/Körffer* in: Gola/Schomerus, BDSG (12. Aufl. 2015), § 3 Rn. 10; *Meyerdierks*, MMR 2009, 8 (13); *Krüger/Maucher*, MMR 2011, 433 (439).
[281] So beispielsweise *Hawellek*, ZD-Aktuell 2011, 129 (130); *Schliesky u.a.*, Drittwirkung im Internet, Fn. 344.
[282] EuGH, Urt. v. 19.10.2016, Rs. C-582/14, Breyer, EU:C:2016:779, Rn. 33 ff.

Stelle diese weiteren Informationen nicht besitzt, kommt der EuGH zu einem Ergebnis, das dogmatisch einer relativen Bestimmbarkeit des Personenbezugs von IP-Adressen entspricht. Die Hürden an eine Herstellbarkeit des Personenbezugs für die verarbeitende Stelle stellt der EuGH aber derart niedrig, dass die Auslegung des EuGH letztlich in der Praxis der absoluten Personenbezogenheit von IP-Adressen ähnelt: Für eine datenverarbeitetende Stelle, die nicht selbst im Besitz der erforderlichen Informationen sei, um die IP-Adressen einer bestimmten Person zuordnen zu können, handle es sich dann bei IP-Adressen um personenbezogene Daten, wenn sie rechtliche Mittel besitzt, diese Person über die einem ISP zur Verfügung stehenden Informationen identifizieren zu lassen.[283] Für nicht erforderlich hält es der EuGH hingegen, dass die Informationen, die für die Identifizierung notwendig seien, alle in der Hand einer Person sein müssten.[284] Der EuGH begründet seine Auslegung damit, dass aus Art. 2 lit. a der Richtlinie 95/46/EG hervorgehe, dass auch die indirekte Bestimmbarkeit einer Person über ein Datum ausreiche, um einen Personenbezug des Datums zu bejahen.[285] Ob eine Person indirekt bestimmbar sei, entscheide sich gemäß Erwägungsgrund 26 der RL 95/46/EG danach, ob die datenverarbeitende Stelle den Personenbezug mit vertretbarem Aufwand herstellen könne.[286]

Nach der Breyer-Entscheidung des EuGH hat die Frage, ob der Personenbezug von IP-Adressen nun relativ oder absolut zu bestimmen ist, für diese Arbeit nur noch akademische Relevanz. Die Datenverarbeitung im Rahmen von Eingriffen in den Datenverkehr findet bei den ISPs statt, und diese haben, zumindest wenn es sich um Access Provider handelt, ohnehin alle Informationen, um den Personenbezug herzustellen. Auch Network Provider haben in der Regel Möglichkeiten, an diese Informationen zu gelangen.[287]

Eingriffe in den Datenverkehr mittels DPI-Filter beeinträchtigen auch das Recht auf Schutz personenbezogener Daten gemäß Art. 8 Charta, da sie in der praktischen Umsetzung stets mit einer Verarbeitung personenbezogener Daten einhergehen. Eine Beeinträchtigung des Schutzbereichs des Art. 8 Charta liegt bereits in jeder Verarbeitung personenbezogener Daten.[288]

---

[283] EuGH, Urt. v. 19.10.2016, Rs. C-582/14, Breyer, EU:C:2016:779, Rn. 49.
[284] EuGH, Urt. v. 19.10.2016, Rs. C-582/14, Breyer, EU:C:2016:779, Rn. 43.
[285] EuGH, Urt. v. 19.10.2016, Rs. C-582/14, Breyer, EU:C:2016:779, Rn. 40.
[286] EuGH, Urt. v. 19.10.2016, Rs. C-582/14, Breyer, EU:C:2016:779, Rn. 42.
[287] Vgl. dazu BGH, Urt. v. 16.05.2017, VI ZR 135/13, NJW 2017, 2416, (2417). Beachtenswert ist insoweit auch das Argument von *Eckhardt*, CR 2011, 339 (340) und *Heidrich/Wegener*, DuD 2010, 172 (174), dass die Personenbezogenheit einer Maßnahme immer nach ihrem schwächsten Glied bemessen werden muss. Da bei datenverkehrsregulierenden Maßnahmen allerdings nicht nur dynamische, sondern auch vereinzelt statische IP-Adressen verarbeitet werden, ist hier der Personenbezug ohnehin gegeben.
[288] EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C-594/12, Digital Rights Ireland, EU:C:2014:238, Rn. 36; Jarass, Charta der Grundrechte der Europäischen Union, Art. 8 Rn. 9. Eine qualifizierte Beeinträchtigung ist für eine Beeinträchtigung des Schutzbereichs hingegen nicht verantwortlich. So aber früher das Bundesverfassungsgericht zur entsprechenden Rechtslage in Deutschland: Das

Zwar erfordert eine Deep Packet Inspection theoretisch nicht zwangsläufig die Analyse des IP-Headers des Datenpakets, in dem die IP-Adresse liegt. Das DPI-System kann, wenn gewünscht, beispielsweise so konfiguriert werden, dass es seinen Blick ausschließlich auf die Anwendungsschicht des IP-Pakets richtet und nur die dortigen Daten analysiert. Die IP-Adresse wird zur Analyse der transportierten Daten eigentlich nicht benötigt. Insoweit könnte man von einer anonymisierten Deep Packet Inspection sprechen.[289]

Praktisch ist die Verarbeitung der IP-Adresse als integraler Bestandteil der DPI allerdings die Regel. Denn wie *Hawellek* richtig bemerkt, ist ein einzelnes IP-Paket im Vergleich zu den bei einem einzelnen Filesharing-Vorgang anfallenden Datenmengen bemerkenswert klein.[290] Ein Datenpaket kann maximal eine Größe von 64 Kilobyte besitzen.[291] Bei einer stark komprimierten Musikdatei, bei der eine Minute Laufzeit etwa 1 MByte an Daten verschlingt, entspricht die maximale Länge eines IP-Pakets etwa 3,5 Sekunden Musik.

Selbst wenn die Analyse eines so kurzen Datenfragments sich einigermaßen zuverlässig mit der Datenbank abgleichen ließe, in der die geschützten Werke hinterlegt sind (was wegen der bei starker Komprimierung auftretenden Datenartefakte und der damit einhergehenden Veränderung des digitalen Fußabdrucks eine technischen Herausforderung darstellen dürfte), lässt sich aus einem solch kurzen Musikausschnitt keine eindeutige Zuordnung zu einem geschützten Werk herleiten. Wegen der verbreiteten Musikproduktionstechnik des Samplings, bei dem existierende Ausschnitte – also Kopien bereits bestehender Musikwerke – neu arrangiert und kombiniert werden, kann ein Musikausschnitt von nur 3,5 Sekunden unter Umständen zeitgleich und gleichberechtigt vielen Werken zugeordnet werden.[292]

BVerfG verlangte für einen Eingriff in Art. 10 Abs. 1 GG bzw. das Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1, Art. 1 Abs. 1 GG, dass eine gewisse Erheblichkeitsschwelle der Grundrechtsbeeinträchtigung überschritten sein muss, BVerfG, Urt. v. 11.03.2008, 1 BvR 2074/05, 1 BvR 1254/07, Kfz-Kennzeichenkontrollen 1, BVerfGE 120, 378 (399) m.w.N. Mittlerweile hat das BVerfG die Anforderungen an die Erheblichkeit allerdings erheblich herabgesenkt, vgl. BVerfG, Beschl. v. 18.12.2018, 1 BvR 142/15, Kfz-Kennzeichenkontrollen 2, BVerfGE 150, 244 (265 f.) und unten Kap. 3 IV 2 b (S. 202 f.).

[289] Sollten auch in der Anwendungsschicht personenbezogene Daten enthalten und vom Filtersystem verarbeitet werden, liegt auch insoweit eine Beeinträchtigung des Art. 8 Charta vor.

[290] *Hawellek*, ZD-Aktuell 2011, 129 (130).

[291] Vgl. *Meinel/Sack*, Internetworking, 7.3.3 (S. 537 ff.). Dies gilt jedenfalls, soweit IPv4 verwendet wird. Hintergrund ist, dass die Angabe „Total Length" im IP-Header des Datagramms, mit dem sich Router signalisieren, wie groß das weiterzuleitende Paket ist, lediglich 16 Bit lang ist, womit ein Zahlenraum bis 65535 Byte (64 KByte) abgedeckt werden kann.

[292] Kulturelle und wissenschaftliche Werke generell bauen auf der Kombination und neuer Anordnung und Interpretation bereits bestehender Themen, Ergebnisse und Werke auf. Dies ist oft die eigentliche urheberrechtlich geschützte und schützenswerte Leistung. Dies wird z.B. bei der Technik des Sampling deutlich, die bei der Produktion von Musik angewendet wird. Kurze Ausschnitte – Samples – werden teilweise unverfälscht, teilweise verzerrt, aus ihrem Kontext gerissen und in einen neuen musikalischen oder inhaltlichen Zusammenhang gestellt, vgl. *Lessig*, Remix schlüssig aufzeigt.

Um das Problem zu kleiner Datenmengen zu lösen (und auch, weil es ressourcenschonender als die individuelle Behandlung jedes einzelnen IP-Pakets ist), können in den Routern des Providers Datenströme, sogenannte Flows, gebildet werden. Ein Flow kann gedacht werden als das künstliche logische Gegenstück des Internets etwa zu einem Telefonanruf.[293] Über einen Flow wird also keine technische, aber eine logische Verbindung abgebildet. Da aufeinanderfolgende Reihen von Datenpaketen in IP-Netzwerken definitionsgemäß nicht ausweisen, ob sie zu einer logischen Verbindung gehören oder nicht, muss ein System, das eine logische Verbindung erkennen möchte, die zur Verfügung stehenden Daten interpretieren.[294] Dazu reichen in der Regel die Informationen der Internet- und der Transportschicht aus. Passieren die IP-Pakete einen Router des ISP, werden dazu die Header der Internet-Schicht und der Transportschicht ausgelesen und die Informationen mit einem Zeitstempel versehen gespeichert.[295] Sind die gesammelten IP-Adressen von Absender und Empfänger und die Portnummern eines Datenstroms identisch und liegt ein enger zeitlicher Zusammenhang vor, kann man jedenfalls mit einiger Gewissheit sagen, dass es sich um einen logischen Kommunikationsvorgang zwischen den beteiligten Sockets handelt.[296]

Flows erlauben es also, in einem verbindungslosen Netzwerk wie dem Internet auf den Rechner des ISP dennoch größere zusammenhängende Datenmengen als Verbindungen abzubilden, zu untersuchen oder in anderer Weise zu verarbeiten. Um beim Beispiel der MP3-Datei zu bleiben: Auf der Ebene der miteinander kommunizierenden Anwendungen – und auch der Ebene der dahinterstehenden Nutzer – handelt es sich bei der Übertragung eines Musiktitels um einen einheitlichen Prozess, um eine einheitliche logische Verbindung. Auf der Ebene der Internet-Schicht des TCP/IP-Protokolls, ist technisch gesehen eine solche einheitliche Verbindung nicht gegeben. Das Abbilden eines Flows erlaubt es dem ISP jedoch durch Interpretation von IP-Adresse und Portnummer zu erkennen, dass eine logische Verbindung besteht, und sie als solche zu untersuchen. Die Datenmenge eines Flows ist in der Regel deutlich größer als die maximale Größe eines IP-Pakets mit seiner Beschränkung auf 64 KByte, so dass die Analyse der zusammenhängenden Nutzdaten des Flows eine deutlich höhere Chance hat, einen Musiktitel zu einem gespeicherten Werk eindeutig zuzuordnen, als dies bei einem einzelnen IP-Paket möglich wäre. Die Bildung eines Flows ist folglich – wenn auch theoretisch nicht in jedem Fall einer Deep Packet Inspection zur Urheberrechtsdurchsetzung notwendig – letztlich deren praktische Grundvoraussetzung. Daraus folgt, dass die Verarbeitung von IP-Adressen ein integraler

---

[293] Zu den technischen Hintergründen von Flows vgl. ausführlich *Brownlee u.a.*, Traffic Flow Measurement: Architecture, 1999, abrufbar unter https://www.hjp.at/doc/rfc/rfc2722.html (zuletzt besucht am 09.10.2021).

[294] Im Internet wird eine logische Verbindung nicht zwangsläufig auch in einer technischen Verbindung gespiegelt, schon gar nicht bereits in der Internet-Schicht. Das Internet ist ein verbindungsloses Netzwerk. Erst gegebenenfalls auf der Transportschicht (bei Verwendung von *TCP*, nicht aber bei UDP) oder spätestens der Anwendungsschicht wird eine künstliche Verbindung etabliert. Vgl. dazu oben Kap. 1 I 4 (S. 9 f.).

[295] *Cao u.a.*, J. Comput. Graph. Stat. 2003, 865 (867).

[296] *Cleveland/Sun*, JASA 2000, 979 (980 ff.).

Bestandteil der Durchführung einer Deep Packet Inspection ist, wenn ein Flow mithilfe der IP-Header der Datagramme eines Kommunikationsvorganges gebildet wird.[297]

Zu bedenken ist allerdings, dass die Zuordnung zu einem Flow nicht nur aufgrund der IP-Adressen und Port-Nummern erfolgen kann. Technisch aufwendiger, aber dennoch denkbar, ist es, einen Flow mit Hilfe tiefer im Datagramm liegender Informationen zu ermitteln. Dabei kommen Informationen aus dem Header der Anwendungsschicht oder sogar aus dem Payload des Pakets infrage. Der Flow könnte also grundsätzlich direkt aus der Deep Packet Inspection selbst heraus erfolgen – und die Daten aus der Internet- und Transportschicht absichtlich ausblenden, um Anonymität herzustellen.[298]

Aus wirtschaftlicher Sicht ist ein solches Vorgehen jedoch nicht unbedingt sinnvoll. Die Verarbeitung von Daten mittels Deep Packet Inspection erfordert gegenüber dem Auslesen der Schichten bis einschließlich der Transportschicht wegen der höheren Standardisierung der Datenstruktur erheblich weniger Aufwand an Rechenleistung als eine Analyse der tieferliegenden Inhalte.[299]

Lässt man das Kostenargument beiseite, etwa weil Rechenleistung zukünftig erheblich günstiger werden könnte oder Verfahren entwickelt würden, die den Rechenaufwand einer Deep Packet Inspection verringerten, und erzeugt den Flow deshalb nicht unter Zuhilfenahme der IP-Adresse, so spielt diese bei einem DPI-Filtersystem dennoch eine Rolle. Spätestens nach erfolgter Deep Packet Inspection muss das System eine Antwort auf die Frage ausgeben, ob der Datenverkehr unverändert, verändert oder gar nicht an den Empfänger ausgeliefert werden soll.[300] Die Daten, die sich auf ihrem Transportweg beim ISP befinden, sollen schließlich grundsätzlich noch zu ihrem Empfänger weitergeleitet werden, wozu dessen IP-Adresse benötigt wird. Ob dies in der Weise geschieht, welche sich die Nutzer hinter den IP-Adressen vorgestellt haben, oder auf andere Weise, gerade darüber entscheidet das Filtersystem. Das Ergebnis des Datenverarbeitungsprozesses wird daher auch aus diesem Grund zwangsläufig in Beziehung zur IP-Adresse aller Nutzer gesetzt.

Eine Beeinträchtigung von Art. 8 Charta scheitert hier nicht daran, dass der Nutzer sich konkludent mit Verarbeitung seiner IP-Adresse einverstanden zeige. Der Nutzer ist nur miteiner inhaltlich neutralen Verwendung seiner IP-Adresse zu Routing-Zwecken einverstanden. Eingriffe in den Datenverkehr zur Urheberrechtsdurchsetzung erfolgen mit dem Ziel, bestimmte Inhalte nicht an den durch die IP-Adresse (bzw. den *Socket*) ausgewiesenen Empfänger zu transportieren. Ein entsprechendes Einverständnis des Nutzers dazu,

---

[297] So unterstellt *Hawellek*, ZD-Aktuell 2011, 129 (130) dem EuGH, derartige Überlegungen im Sinne eines „ganzheitlichen Ansatzes"; EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 51 zugrunde gelegt zu haben.

[298] Auf diese Möglichkeit weist *Hawellek*, ZD-Aktuell 2011, 129 (130) hin.

[299] *Aceto u.a.*, PortLoad: Taking the Best of Two Worlds in Traffic Classification, in: 2010 INFOCOM – IEEE Conference on Computer Communications Workshops, S. 3.

[300] Bzw. gegebenenfalls alternativ oder zusätzlich, ob der Nutzer identifiziert werden soll, um ihn staatlichen oder privaten Stellen als *Filesharer* zu melden, oder eben nicht.

dass seine IP-Adresse zu den mit der Datenverkehrsregulierung beabsichtigten Zwecken, etwa der Durchsetzung des Urheberrechts, verarbeitet wird, ist zweckgebunden und kann für eine DVR nicht unterstellt werden.

Die Intensität der Beeinträchtigung des Rechts auf den Schutz personenbezogener Daten ist bei Eingriffen in den Datenverkehr im Vergleich zu einem simplen Routing zudem erheblich stärker, da der Eingriff wegen der Verknüpfung des Pakets (das auch die IP-Adresse enthält) zu seinem (vermeintlichen) Inhalt erfolgt. Die Voraussetzungen, die zur Rechtfertigung des Eingriffs erforderlich sind, sind daher entsprechend strenger. Werden die IP-Adressen beim ISP tatsächlich auch *zu Zwecken* der Datenverkehrsregulierung verarbeitet und/oder mit dem Inhalt tatsächlich und nicht nur potentiell verknüpft, steigt die Eingriffsintensität noch weiter an.

Die Datenverkehrsregulierung beeinträchtigt folglich auch deshalb den Schutz aus Art. 8 Charta, weil dabei stets IP-Adressen mitverarbeitet werden, die es ermöglichen, die dahinterstehenden Nutzer gegebenenfalls zu identifizieren oder zu ent-anonymisieren.[301] Dass es sich aus technischer Perspektive im Einzelfall um zwei voneinander trennbare Prozesse handelt, die tatsächlich nicht miteinander kommunizieren müssen, ist nicht entscheidend. Eine auf diese Art gewonnene gewillkürte Anonymisierung reicht als Schutz der personenbezogenen Daten nicht aus, da deren Aufrechterhaltung von der Systemkonfiguration abhängig ist und jederzeit geändert werden kann.

Die Würdigung des EuGH ist insoweit mithin stimmig: Im Zusammenhang mit Eingriffen in den Datenverkehr handelt es sich bei IP-Adressen um personenbezogene Daten, und die Gewährleistung des Schutzes personenbezogener Daten ist auch wegen der systembedingten Mitverarbeitung der IP-Adressen stets beeinträchtigt.

Der näheren Betrachtung bedarf hingegen noch, wie intensiv das streitige Filtersystem nach Ansicht des EuGH den Schutz personenbezogener Daten beeinträchtigt. Der EuGH stellt ausdrücklich fest, dass Art. 8 Charta von einer allumfassenden Deep Packet Inspection, die das streitige Filtersystem fordert, beeinträchtigt sei. Den Entscheidungsgründen ist hingegen weder ausdrücklich zu entnehmen, dass Art. 8 Charta von dem hier streitigen Filtersystem *verletzt* sei, noch dessen Gegenteil. Der EuGH stellt lediglich fest, dass Art. 8 Charta durch die Anordnung des streitigen Filtersystems nicht in einen angemessenen Ausgleich mit Art. 17 Charta gebracht werde, wobei in die fällige Abwägung gemäß Art. 52 Abs. 1 Charta auch die Beeinträchtigung der Informationsfreiheit und die Verletzung der unternehmerischen Freiheit mit einfließen.

Die Betonung der Unterscheidung zwischen *Beeinträchtigung* eines Grundrechts und seiner *Verletzung* legen eine bewusst differenzierte Verwendung der Begriffe nahe. Art. 16 Charta, den der EuGH verletzt sieht, wird zudem von den beiden anderen beeinträchtigten Grundrechten in den Urteilsgründen abgegrenzt und ausführlicher gewürdigt. Der EuGH sieht bei Art. 16 Charta ferner eine *qualifizierte* Beeinträchtigung gegeben.

---

[301] *Nietsch*, Anonymität und die Durchsetzung urheberrechtlicher Ansprüche im Internet, S. 153.

Diese Aussage fehlt bei den anderen geprüften Grundrechten. Dies kann man als Hinweise verstehen, dass der EuGH Art. 16 Charta in seinem Kernbereich verletzt sieht, während die Beeinträchtigungen der Art. 8 und Art. 11 Charta lediglich im Rahmen der Abwägung kollidierender Grundrechte gemäß Art. 52 Abs. 1 Charta Bedeutung erlangen.

c. Informationsfreiheit, Art. 11 Charta

Auch die Informationsfreiheit gemäß Art. 11 Charta sieht der EuGH durch das streitige Filtersystem beeinträchtigt. Diese Analyse ist richtig, da die heute möglichen Filtersysteme die (urheber-)rechtliche Bewertung des Datenverkehrs nicht leisten können. Die streitgegenständliche Anordnung erfordert, dass der Internet Service Provider ermittelt, bei welchem als geschütztes Werk der SABAM identifizierten Datenverkehr es sich um illegales und bei welchem es sich um legales Filesharing handelt. Ansonsten käme es schnell zu der Situation, dass auch der vom Gesetz her legale Austausch von Daten unterbunden würde. Die rechtliche Position der Rechteinhaber würde faktisch deutlich erweitert und zugleich durchgesetzt.

Ein technisches System, dass zwischen legalem und illegalem Filesharing unterscheiden kann, ist nicht bekannt. Es liegt in der Natur digitaler Daten, dass die Kopie mit dem Original identisch ist. Eine Identifizierung des illegalen Anteils an getauschten Dateien beim Filesharing könnte daher lediglich auf der als rechtswidrig bekannten Quelle der Daten beruhen oder darauf, dass Filesharing bezüglich bestimmter Daten generell verboten ist.

Ein solches generelles Verbot des Filesharings besteht allerdings nicht im Rechtsraum der Europäischen Union. Das Urheberrecht ist nicht absolut gewährleistet, sondern unterliegt gewissen Einschränkungen zugunsten der Allgemeinheit. Das private Teilen von Werken etwa ist in den Mitgliedstaaten der EU unter gewissen Voraussetzungen erlaubt. Ebenso gibt es unterschiedliche lang gewährleistete Schutzdauern oder es sind auf nationale Märkte begrenzte gemeinfreie Veröffentlichungen denkbar.

Eine Diskriminierung anhand der Quelle der Daten ist hingegen beim Filesharing jedenfalls über Peer-to-Peer-Netzwerke nicht möglich, da die IP-Adresse des Filesharers beim Austausch über Peer-to-Peer-Netzwerke in der Regel keine Aussage über dessen Berechtigung zum Filesharing erlaubt. Hier tauschen in der Regel Privatpersonen mit dynamischen IP-Adressen geschützte und ungeschützte Dateien aller Art aus. Die Dezentralität der Datenverteilung und die Heterogenität der Nutzer eines solchen Netzwerks ist sozusagen der Clou an dieser Technik.

Aus der bloßen Tatsache, dass ein Nutzer ein Peer-to-Peer-Netzwerk zum Austausch von Daten verwendet, können zunächst keine Rückschlüsse auf dessen Legalität gezogen werden. Dies ist ein wichtiger Unterschied zu großen zentralisierten und institutionellen Anbietern wie bestimmten Filehostern, Streaming-Plattformen oder Nur-Listern, deren IP-Adresse oft vor einem beobachteten Tauschvorgang bereits bekannt ist und bei denen –

vorsichtig formuliert – die Annahme, dass aus deren Quelle urheberrechtlich geschütztes Material illegal über das Netz verbreitet wird, auf sichereren Füßen steht.[302]

Eine unterschiedliche Behandlung des Datenverkehrs danach, ob es sich um legales oder illegales Filesharing handelt, ist daher – jedenfalls und erst recht beim Peer-to-Peer-Filesharing, um das es in der Scarlet-Entscheidung geht – nicht möglich. Den ISPs bleibt als Maßnahme daher nur das flächendeckende Blockieren desjenigen Datenverkehrs, der als geschütztes Werk der *SABAM* identifiziert wurde, übrig.

Interessant ist somit, dass der EuGH das Auftreten von *false positives*[303] in dieser Entscheidung nicht per se als eine Verletzung, sondern nur als eine Beeinträchtigung des Art. 11 Charta bezeichnet. Ein Hinweis darauf, dass der Wesensgehalt der Informationsfreiheit im Sinne des Art. 52 Abs. 1 Satz 1 Charta durch das streitige Filtersystem angetastet würde, fehlt in der Entscheidung.[304] In derselben Entscheidung wird dies hingegen bei der Frage nach dem Schutz der unternehmerischen Freiheit anders gehandhabt, welche der EuGH *verletzt* sieht.

Die Beeinträchtigung der Informationsfreiheit durch das Overblocking wird vielmehr lediglich im Rahmen einer Grundrechtsabwägung berücksichtigt, wie sie seit der Promusicae-Entscheidung des EuGH geboten ist. In dieser Abwägung stehen sich laut EuGH die Eigentumsfreiheit auf der einen Seite und die Art. 8, 11 und 16 Charta auf der anderen Seite gegenüber. Dass die Abwägung in der Scarlet-Entscheidung nicht zugunsten der Eigentumsfreiheit ausgehen würde, wird bereits dadurch entschieden, dass die unternehmerische Freiheit der ISPs durch DPI-Filter verletzt wird. Eine Beeinträchtigung der Art. 8 und 11 Charta ist für das Ergebnis der Abwägung daher nicht mehr entscheidend. Umso aufschlussreicher wäre es daher gewesen, wenn der EuGH sich ausführlicher bzw. überhaupt dazu geäußert hätte, für wie schwerwiegend er die Beeinträchtigung der Informationsfreiheit hält. Dies gilt im gleichen Maße für die Beeinträchtigung des Schutzes personenbezogener Daten. Die fehlende Auseinandersetzung mit der Schwere der Beeinträchtigung lässt hier wenig Rückschlüsse darauf zu, wie der EuGH entscheiden würde, wenn das datenverkehrsregulierende System weniger intensiv in die unternehmerische Freiheit eingreifen würde als in der Scarlet-Entscheidung.

d. Zusammenfassende Bewertung der Scarlet-Entscheidung

Die Zahl der abstrahierbaren Rechtssätze, die sich der Scarlet-Entscheidung entnehmen lassen, ist begrenzter, als es der oft wenig differenzierende Wortlaut der Entscheidung erwarten lässt. Die auf den ersten Blick pauschalen Formulierungen des EuGHmüssen nicht zwingend zu dem Schluss führen, dass der EuGH zu den ihm vorgelegten Fragen

---

[302] Auch hier besteht jedoch das Problem des Overblockings.
[303] Ein *false positive* bedeutet in diesem Zusammenhang: Ein datenverkehrsregulierendes System gibt bei einer im konkreten Fall legal getauschten Datei das Ergebnis aus, dass es sich um einen illegalen Tauschvorgang handele.
[304] Vgl. dazu EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 52.

eine sehr entschiedene Haltung einnimmt und eine ausführlichere und intensivere Befassung mit den Fragen aus seiner Sicht überflüssig sei. Der der Entscheidung zugrunde liegende Sachverhalt könnte für den EuGH vielmehr ein derart eindeutiger Fall gewesen sein, dass die Verhältnismäßigkeit des von SABAM geforderten Filtersystems aus seiner Sicht offensichtlich nicht gegeben war. Der EuGH wäre daher auch nicht zu differenzierenden Ausführungen veranlasst.

Auf jeden Fall lässt sich aber festhalten, dass Eingriffe in den Datenverkehr zur Durchsetzung des Urheberrechts wegen einer Verletzung der unternehmerischen Freiheit unzulässig sind, wenn sie eine hohe finanzielle und organisatorische Belastung für die ISP darstellen. Ebenso steht nach der Scarlet-Entscheidung fest, dass *Overblocking* die Informationsfreiheit beeinträchtigt. Ob und unter welchen Umständen hatte der EuGH jedoch zunächst noch offen gelassen. Gleiches gilt für Art. 8 Charta. Das Recht auf den Schutz personenbezogener Daten ist bei jeder Form der Datenverkehrsregulierung *beeinträchtigt*. Unklar bleibt auch nach der Scarlet-Entscheidung jedoch, ab welcher Grenze Art. 8 Charta durch eine Datenverkehrsregulierung zur Durchsetzung des Urheberrechts auch *verletzt* wird.

Die Scarlet-Entscheidung lässt daher einige Fragen ungeklärt, deren Klärung im Sinne größerer Rechtsklarheit wünschenswert gewesen wäre:

- Verletzt ein Filtersystem auch dann noch die unternehmerische Freiheit, wenn es weniger Kosten verursacht oder andere Stellen als die ISP die Kosten von Einrichtung und Betrieb übernehmen?
- Wie intensiv werden Art. 8 und Art. 11 Charta durch das in der Entscheidung streitige DPI-Filtersystem beeinträchtigt? Wie wirken sich diese Beeinträchtigungen auf eine Abwägung mit der Eigentumsfreiheit des Art. 17 Charta aus?
- Welche Auswirkungen auf die Beeinträchtigung des Schutzes personenbezogener Daten hat die notwendige Verwendung von Deep Packet Inspection im Rahmen des streitigen Filtersystems, die eine größere Bedrohung für die Persönlichkeitsrechte darstellt als bloße DNS- oder IP-Sperren?
- Und schließlich: Wie sind die Auswirkungen des streitigen Filtersystems auf Art. 7 Charta zu bewerten, der die Achtung der Privatsphäre und der Kommunikation garantiert?

2. Constantin Film/Wega ./. UPC Telekabel

Das Verfahren Constantin Film/Wega ./. UPC Telekabel[305] betraf in vielerlei Hinsicht ähnliche Rechtsfragen wie das Scarlet-Verfahren. Allerdings lag ersterem ein etwas anderer Sachverhalt zugrunde, insbesondere waren die streitigen Filter-Maßnahmen technisch andere. Das gab dem EuGH die Gelegenheit, die Aussagen seiner Rechtsprechung aus SABAM ./. Scarlet zu konkretisieren, offengelassene Fragen zu beantworten und auch

[305] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192.

zwischen den rechtlichen Auswirkungen verschiedener Maßnahmen der Datenverkehrsregulierung zu differenzieren.

Im Ausgangsverfahren stritten sich auf der einen Seite die Constantin Film (Scarlet: ebenfalls Constantin Film) und Wega, beides Filmproduktionsgesellschaften, und auf der anderen Seite UPC Telekabel, die ihren Kunden Internetzugangsleistungen anbot. Wie bei SABAM ./. Scarlet bestand der Konflikt also zwischen Rechteverwertern und einem Internet Service Provider. Inhaltlich ging es darum, dass auf der Web-Seite „kino.to“[306] Filmwerke der Produktionsgesellschaften, die urheberrechtlich geschützt waren, ohne Erlaubnis der Öffentlichkeit zugänglich gemacht wurden. UPC als Intermediär zwischen dem Anbieter der Website und den Konsumenten der dort angebotenen Filmwerke sollte von einem österreichischen Gericht verpflichtet werden, ihren Nutzern den Zugriff auf die Dienste von kino.to zu verwehren. Das erstinstanzliche Gericht – das Handelsgericht Wien – gab der Klage statt. UPC sollte ihren Nutzern den Zugriff auf die Website kino.to blockieren, indem sie eine IP- und eine DNS-Sperre[307] für die Seite einrichten müssten.[308]

Das Berufungsgericht – das Oberlandesgericht Wien – hingegen hielt den Tenor zwar grundsätzlich aufrecht, änderte ihn allerdings insoweit ab, als die Mittel, mit denen die UPC den Zugang zur Website verweigern müsste, ihr nicht vorgegeben werden dürften. Bei der nationalen Rechtsnorm, auf die sich die Anordnung der DVR stütze, handele es sich um die Umsetzung von Art. 8 Abs. 3 der InfoSoc-Richtlinie. Danach sei zwar eine Verfügung zulässig, die UPC verbiete, ihren Nutzern den Zugriff auf kino.to zu gestatten, dabei dürfe es sich aber lediglich um ein Erfolgsverbot handeln. Ob UPC dies Verbot mittels einer DNS-Sperre, IP-Sperre oder einer sonstigen Maßnahme umsetze, bleibe ihr überlassen.[309]

Gegen dieses Urteil legte UPC Revision beim Österreichischen Obersten Gerichtshof Revision ein. Die Argumentation der UPC war jene, dass sie kein Vermittler im Sinne des Art. 8 Abs. 3 InfoSoc-Richtlinie sei, dessen Dienste von Dritten zur Verletzung des Urheberrechts genutzt würden. Sie stehe mit den Betreibern von *kino.to* in keiner Geschäftsbeziehung und dass ihre eigenen Kunden das Urheberrecht verletzen würden, sei nicht bewiesen. Die möglichen Sperren seien außerdem technisch zu umgehen und teilweise unverhältnismäßig teuer.

---

[306] *Kino.to* war eine bekannte Streaming-Plattform, über die Nutzer kostenlos urheberrechtlich geschützte Filme ansehen konnten.
[307] Zur Funktionsweise einer IP-Sperre vgl. oben Kap. 1 III 2 (S. 18 ff.), zu der einer DNS-Sperre vgl. oben Kap. 1 III 1 (S. 16 ff.).
[308] Vgl. EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 12 f.
[309] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 14.

Der Oberste Gerichtshof rief daraufhin den EuGH zur Beantwortung von vier Fragen an. Zwei der Fragen wurden letztlich vom EuGH nicht weiter beantwortet, weil die Bedingungen, unter denen er auf diese hätte eingehen sollen, nicht eintraten.[310] Auf Frage 1 und Frage 3 ging der EuGH hingegen ein. Frage 1 hatte im Wesentlichen zum Inhalt, ob ein ISP Vermittler im Sinne des Art. 8 Abs. 3 InfoSoc-Richtlinie sei und daher grundsätzlich Adressat von Sperrverfügungen bei Urheberrechtsverletzungen über sein Netz sein könne, was der EuGH bejahte.[311] Der Schwerpunkt des Interesses liegt hier jedoch bei Frage 3. Der Oberste Gerichtshof wollte wissen, ob es mit den EU-Grundrechten der Betroffenen zu vereinbaren sei, wenn einem ISP durch Anordnung konkreter Maßnahmen verboten werde, seinen Kunden den Aufruf bestimmter Internet-Angebote zu ermöglichen, soweit dort zumindest größtenteils urheberrechtswidrig Inhalte zum Abruf bereitgestellt würden und der ISP Beugestrafen aus der Verletzung eines solchen Verbots abwenden könne, indem er nachweist, dass er alle ihm zumutbaren Maßnahmen bereits ergriffen habe.[312]

Der EuGH hatte also über eine Institution zur Regulierung des Datenverkehrs zu entscheiden, die den Provider verpflichtet

- auf eigene Kosten
- zeitlich unbegrenzt
- ein- und ausgehende *Kommunikation*
- zu durchsuchen, um

- *unstreitige* Urheberrechtsverletzungen zu
- verhindern
- durch Mittel *nach Wahl* des ISP und
- mit *Befreiungsmöglichkeit* des ISP bei Nachweis des Ergreifens aller *zumutbaren* Maßnahmen.

---

[310] Zum einen handelte es sich um die interessante Frage 2 des Obersten Gerichtshofs, ob eine Vervielfältigung zum privaten Gebrauch (Art. 5 Abs. 2 lit. b der Richtlinie 2001/29/EG) und eine flüchtige und begleitende Vervielfältigung (Art. 5 Abs. 1 der Richtlinie 2001/29/EG) nur dann zulässig sind, wenn die Vorlage der Vervielfältigung rechtmäßig vervielfältigt, verbreitet oder öffentlich zugänglich gemacht wurde. Die Frage zielt darauf, ob sich die Konsumenten eines Internet-Streams aus einer offensichtlich nicht berechtigten Quelle auch selbst rechtswidrig verhalten. Der EuGH ging hierauf nicht weiter ein, vgl. EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 17, 41. Zum anderen wollte der Oberste Gerichtshof mit Frage 4 wissen, ob es mit dem EU-Recht, insbesondere mit der erforderlichen Abwägung zwischen den Grundrechten der Beteiligten, vereinbar sei, einem Internet Service Provider bestimmte Maßnahmen aufzutragen, um seinen Kunden den Zugang zu einer Website mit einem rechtswidrig zugänglich gemachten Inhalt zu erschweren, wenn diese Maßnahmen einen nicht unbeträchtlichen Aufwand erfordern, aber auch ohne besondere technische Kenntnisse leicht umgangen werden können. Diese Frage beantwortete der EuGH en passant bei der Beantwortung von Frage 3, vgl. EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192 Rn. 17, 65.

[311] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 17, 40.

[312] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 17.

Der EuGH erklärte – um das Ergebnis vorweg zu nehmen – eine datenverkehrsregulierende Institution, wie die, über die sie hier zu entscheiden hatte, für vereinbar mit Europarecht. Bei der Begründung hielt der EuGH sich nicht lange mit Sekundärrecht auf, sondern begann gleich mit der Prüfung europäischer Grundrechte. Ähnlich wie bei SABAM ./. Scarlet sah der EuGH auf der Seite der Rechteinhaber das Grundrecht auf geistiges Eigentum gemäß Art. 17 Abs. 2 Charta betroffen, das mit der unternehmerischen Freiheit der ISP gemäß Art. 16 Charta und der durch Art. 11 Charta geschützten Informationsfreiheit der Internet-Nutzer in ein angemessenes Gleichgewicht gebracht werden müsse.[313] Im Gegensatz zu SABAM ./. Scarlet sprach der EuGH diesmal allerdings nicht an, ob er durch die Anordnung der DVR das durch Art. 8 Charta garantierte Recht auf den Schutz personenbezogener Daten berührt sehe.[314]

Art. 16 Charta ist nach Ansicht des EuGH durch die Anordnung der datenverkehrsregulierenden Maßnahme nicht verletzt. Das Recht auf unternehmerische Freiheit umfasse zwar auch das Recht der Unternehmen, über die Verwendung seiner „*wirtschaftlichen, technischen und finanziellen Ressourcen*“ frei bestimmen zu können. Dieses Recht werde durch die streitgegenständlichen Maßnahmen eingeschränkt, da der ISP die ihm zur Verfügung stehenden Ressourcen nicht mehr in Gänze so verwenden könne, wie er wolle. Er werde gezwungen, ein System einzurichten, das ihm möglicherweise hohe Kosten verursache und die Erarbeitung von komplexen technischen Lösungen sowie umfangreiche Umstellungen seiner wirtschaftlichen Tätigkeiten abverlange.[315]

Die Anordnung der Datenverkehrsregulierung verletze die unternehmerische Freiheit dennoch nicht, da der Gerichtshof durch die Anordnung deren Wesensgehalt nicht angetastet sehe. Diesen Schluss zieht der EuGH aus zwei Argumenten. Zum einen überlasse die konkrete Ausgestaltung dieser datenverkehrsregulierenden Institution, wie sie in Vorlagefrage 3 dem EuGH zur Entscheidung vorgelegt wird, dem ISP selbst die Wahl über die von ihm zu ergreifenden Mittel. Der ISP könne daher die Maßnahme auswählen, die die ihm zur Verfügung stehenden Möglichkeiten am effizientesten nutze und ihn am wenigsten finanziell und organisatorisch belaste.[316]

Zum anderen lasse die Institution dem ISP die Möglichkeit, sich durch den Nachweis, alle zumutbaren Maßnahmen ergriffen zu haben, von der Haftung für ausbleibenden Erfolg

---

[313] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 46 f.
[314] Vgl. dazu EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 51. Zu möglichen Gründen hierfür vgl. unten Kap. 2 V 3 b) (S. 109 ff.).
[315] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 49 f.
[316] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 52.

der Anordnung zu befreien. Da diese Möglichkeit bestehe, sei der ISP im Umkehrschluss auch nicht zu Maßnahmen verpflichtet, die ihm unzumutbar seien.[317]

Die Anordnung von Eingriffen in den Datenverkehr zur Urheberrechtsdurchsetzung verstößt nach Ansicht des EuGH auch nicht *per se* gegen das Recht der Internet-Nutzer auf Informationsfreiheit gemäß Art. 11 Charta. Der ISP müsse bei der Wahl der Mittel, mit denen er die Verfügung umzusetzen gedenkt, allerdings darauf achten, dass die Informationsfreiheit gewahrt werde. Tue er dies nicht oder sei ihm dies nicht möglich, sei die Datenverkehrsregulierung – jedenfalls als Mittel zur Durchsetzung des Urheberrechts – nicht gerechtfertigt. Die getroffenen Maßnahmen müssten ausschließlich auf das Ziel gerichtet sein, die Urheberrechtsverletzungen zu beenden, ohne dabei die Nutzer daran zu hindern, die Dienste des ISP auf rechtmäßige Weise zu nutzen. Die Nutzer dürften durch die Eingriffe in den Datenverkehr nicht davon abgehalten werden, rechtmäßig auf Informationen zuzugreifen.[318]

Um den Schutz der Informationsfreiheit sicherzustellen, verlangt der Gerichtshof zudem eine verfahrensrechtliche Absicherung. Im nationalen Verfahrensrecht müsse es daher eine Möglichkeit für die Internet-Nutzer geben, gegen Beschränkungen des freien Zugangs zu Informationen durch die Maßnahmen des ISP gerichtlich vorzugehen, da es den Gerichten nicht *a priori* möglich sei, dies im Vollstreckungsverfahren der Anordnung der Datenverkehrsregulierung zu leisten, wenn diesbezüglich nicht bereits entsprechende Beanstandungen vorlägen.[319]

Nachdem der EuGH also festgestellt hatte, dass die unternehmerische Freiheit und die Informationsfreiheit unter gewissen Umständen hinter den Schutz des Urheberrechts zurücktreten müssten, schränkte er andererseits auch die Gewährleistung des geistigen Eigentums ein, um die widerstreitenden Grundrechte gemäß Art. 52 Abs. 1 Charta in einen angemessen Ausgleich zu bringen. Art. 17 Charta werde schließlich nicht schrankenlos gewährleistet.

Die im UPC-Verfahren streitgegenständliche Anordnung mit ihren Einschränkungen einer absoluten Durchsetzung des Urheberrechts sei also nicht bereits deshalb nicht mit Art. 17 Charta zu vereinbaren, weil der Schutz des Urheberrechts durch diese Institution möglicherweise nicht lückenlos gewährleistet werden könne. Dies sei nach Ansicht des EuGH nicht zu verhindern. Zum einen seien die ISP nicht zu Maßnahmen verpflichtet,

---

[317] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 53. Der EuGH begründet die Angemessenheit einer Befreiungsmöglichkeit, obwohl das geistige Eigentum grundrechtlich geschützt sei, damit, dass nicht der ISP selbst als Adressat einer Anordnung von Datenverkehrseingriffen Täter der Urheberrechtsverletzung sei. Dieses Argument steht in Einklang mit der ratio der kurze Zeit zuvor veröffentlichten Entscheidung des BGH, Urt. v. 12.07.2012, I ZR 18/11, Alone in the Dark, BGHZ 194, 339, Rn. 21 ff. zum Zusammenhang zwischen Filehostern als Anordnungsadressaten zumutbaren Maßnahmen und der rechtlichen Nähe des Intermediärs zur deliktischen Täterschaft oder Beteiligung.

[318] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 55 ff.

[319] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 57.

die zwar dem geistigen Eigentum absolute Geltung verschaffen würden, andererseits jedoch dem ISP nicht zumutbar seien.[320] Zum anderen existiere womöglich einfach kein Verfahren zur Datenverkehrsregulierung, dass nicht mit mehr oder weniger Aufwand von den Nutzern umgangen werden könnte.[321]

Im Ergebnis seien die in der Entscheidung diskutierten Sperrmaßnahmen allerdings grundsätzlich mit Europarecht vereinbar, wenn dem Urheberrecht zwar kein lückenloser, aber ein hinreichend effektiver Schutz gewährt und die miteinander konkurrierenden Grundrechte ausreichend gewahrt würden.[322]

Eine Auswertung der UPC-Entscheidung hinsichtlich allgemeingültiger Aussagen zur europarechtlichen Zulässigkeit ist herausfordernd, da der EuGH – auch bedingt durch die Formulierung der Vorlagefragen – sich teilweise missverständlich äußert.

Die streitgegenständliche Anordnung von Sperrmaßnahmen sollte ursprünglich dem ISP sowohl DNS- als auch IP-Sperren auferlegen. Die Berufungs- und Revisionsinstanzen hielten es allerdings für Unrecht, dem ISP die Wahl der Mittel vorzuschreiben, wie er den Erfolg der angeordneten Maßnahme herbeizuführen hätte. Zudem sollte er keine Maßnahmen durchführen müssen, die ihm nicht zumutbar seien. Daher wurden die Mittel zur Erreichung der Urheberrechtsdurchsetzung in der Vorlagefrage offengelassen.

Dem EuGH wurde so die Möglichkeit eröffnet, ganz allgemein über Netzsperren zu entscheiden, ohne sich dabei um die Rechtmäßigkeit der tatsächlichen technischen und organisatorischen Maßnahmen zu deren Umsetzung weiterführende Gedanken machen zu müssen. Die konkrete Ausgestaltung der Maßnahmen ist jedoch für das Urteil über deren grundrechtliche Zulässigkeit das eigentlich Interessante. Die Intensität, mit der die betroffenen Grundrechte beschränkt werden, ergibt sich gerade aus der Wirkung der konkreten Maßnahme.

Die Entscheidung bleibt daher in weiten Strecken hinter dem zurück, was an Rechtssicherheit und Klärung der Bedeutung der Grundrechte im Rahmen datenverkehrsregulierender Maßnahmen möglich gewesen wäre. Zwar enthält die Entscheidung einige relevante und substantielle Aussagen genereller Art zur Intermediärshaftung und zur Informationsfreiheit. Die sonstigen Aussagen der Entscheidung sind jedoch für den Rechtsanwender hinter dem Möglichen zurückgeblieben, da ein Großteil der Ausführungen ohne Bezugnahme zu konkreten Maßnahmen wie IP-Sperren, DNS-Sperren oder DPI-Filtersystemen praktisch wenig verwertbar ist.

---

[320] Beispielhaft ist etwa das in EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959 streitige Filtersystem, das eine Deep Packet Inspection erfordert, vgl. auch oben Kap. 2 V 1 a) (S. 73).
[321] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 60.
[322] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 63.

a. Unternehmerischen Freiheit, Art. 16 Charta

Ein Internet Service Provider kann grundsätzlich – d.h. unter gewissen Voraussetzungen – nach europäischem Recht Adressat hoheitlicher Anordnungen sein, die ihm aufgeben, Verstöße gegen das Urheberrecht zu unterbinden.[323]

Eine solche Maßnahme, die auf den ISP hinsichtlich seiner unternehmerischen Tätigkeit Zwang ausübt, schränkt die unternehmerische Freiheit im Sinne des Art. 16 Charta ein. Der EuGH sieht durch die Anordnung solcher Maßnahmen erhebliche Kosten, Einschränkungen seiner Entscheidungsfreiheit bei der Organisation der unternehmerischen Tätigkeit sowie die Einrichtung komplexer und diffiziler Technik auf den ISP zukommen. Im Gegensatz zur Scarlet-Entscheidung sieht der Gerichtshof Art. 16 Charta jedoch nicht automatisch durch die streitgegenständlichen Maßnahmen als verletzt an, da der ISP die Möglichkeit besitze, die entsprechende Maßnahme selbst auszuwählen und für ihn unzumutbare Maßnahmen dabei außer Acht lassen zu können.[324]

Damit macht es sich der EuGH in gewisser Weise einfach, denn selbstverständlich gibt es für den ISP nicht unendlich viele technische Möglichkeiten, den Datenverkehr von und zu einer bestimmten Quelle zu unterbinden, aus denen er dann frei auswählen könnte. Quellen mutmaßlich urheberrechtsverletzender Inhalte weisen sich für einen ISP entweder über ihren Domain-Namen oder über ihre IP-Adresse aus, wenn das Mittel der Deep Packet Inspection nicht infrage kommt. Da der EuGH in der Scarlet-Entscheidung gerade erst ein Filtersystem, das den gesamten Datenverkehr inhaltlich überwacht (inhaltsbasiertes Filtersystem im Gegensatz zum hier gegenständlichen quellenbasierten Filtersystem), wegen der hohen Kosten für den ISP als unvereinbar mit Art. 16 Charta befunden hat, kann sich die streitige Anordnung auf ein solches System nicht beziehen.

Es muss sich also bei den zu wählenden Maßnahmen um gezielte, quellenbasierte Filterung handeln, die entsprechend geringere Kosten für den ISP verursacht. Dies könnte bei DNS- und IP-Sperren möglicherweise der Fall sein. Wie gerade festgestellt, lassen sich Internet-Angebote über ihren Domain-Namen und ihre IP-Adresse identifizieren, so dass man, wenn man nur den Datenverkehr eines bestimmten Angebots zielgenau blocken möchte, am besten an dieser Stelle ansetzen sollte.

Bei DNS-Sperren ist die Menge an Datenverkehr, der für Eingriffe in den Datenverkehr zur Durchsetzung des Urheberrechts untersucht werden muss, tatsächlich überschaubar. DNS-Anfragen gehen an spezielle dafür vorgesehene Server. Eine Datenverkehrsregulierung, die über das Domain Name System funktioniert, kann einfach den dortigen Datenverarbeitungsprozess manipulieren, indem es eine andere als die erwartete IP-Adresse zurücksendet.[325] Der Eingriff in den Datenverkehr bleibt in diesen Fällen auf die Anfragen beschränkt, die an die DNS-Server gesendet werden, und erfordert keine aufwändig installierte zusätzliche Hardware. Der Aufwand beschränkt sich im Wesentlichen auf die

---

[323] Vgl. zur Haftung des ISPs als Intermediär oben S. 56 ff.
[324] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 50.
[325] Ausführlich zu den technischen Details oben S. 16 ff.

Pflege der Datenbank mit den Domain-Namen und den zugehörigen IP-Adressen der zu sperrenden Angebote.

Etwas anders stellt sich der Fall dar, dass die Sperrmaßnahme über eine IP-Sperre realisiert werden soll. Der Datenverkehrsüberwachung ist hier in gewisser Weise schon *generell*, da theoretisch jedes einzelne IP-Paket auf Absender- und/oder Empfänger-IP-Adresse kontrolliert werden muss.[326]

Entscheidend für die Beeinträchtigung der unternehmerischen Freiheit sind allerdings Aufwand und Kosten der ISPs für die Durchführung der Datenverkehrsregulierung. Diese halten sich bei IP-Sperren im Vergleich zu einer DPI in Grenzen. Zur Erinnerung: Das Internet ist als nicht-intelligentes Netzwerk konzipiert. Rechenintensive Anwendungen sollen beim Server und beim Client erfolgen, die Router der Provider lesen lediglich die Daten der Internet-Schicht der Datagramme aus. Die Verarbeitung der Routing-Informationen ist jedoch wegen der hohen Standardisierung und der geringen Informationsmenge mit sehr wenig Rechenleistung zu bewerkstelligen, zumal die vorhandene Hardware zu genau diesem Zweck ausgelegt wurde.[327] Nichtsdestotrotz müssen die im Router durchgeleiteten IP-Pakete dennoch auf bestimmte IP-Adressen untersucht und mit einer Blacklist abgeglichen werden, wozu die ursprünglich installierte Hard- und Software nicht ausgerichtet ist.

Als weiterer zusätzlicher Datenverarbeitungsschritt kommt eine Entscheidung darüber hinzu, ob das Datagramm weitergeleitet oder verworfen wird – oder gegebenenfalls auf einen Server mit einer Sperrnachricht umzuleiten ist, was zudem einen weiteren Datenverarbeitungsschritt, nämlich die Manipulation der IP-Adresse voraussetzen würde). Insgesamt sollten die anfallenden Kosten dennoch im Vergleich zu einer flächendeckenden Deep Packet Inspection gering sein, so dass eine IP-Sperre in dieser Hinsicht nicht ohne weiteres mit jener gleichgesetzt werden kann.

Der EuGH setzt sich daher nicht in Widerspruch zur Scarlet-Entscheidung, wenn er feststellt, dass die unternehmerische Freiheit durch die Kosten der Datenverkehrsregulierung bei DNS- und IP-Sperren nicht automatisch verletzt sei. Denn die fraglichen Maßnahmen verursachen nicht zwangsläufig die gleichen Kosten wie eine DPI. Insoweit kommt es auf den Einzelfall an, den der EuGH zu entscheiden hat. In der Scarlet-Entscheidung sah der EuGH die Grenze der zumutbaren Kosten überschritten. In der UPC-Entscheidung war das anzuwendende Verfahren hingegen nicht weiter durch die Vorlagefrage konkretisiert. Die tatsächlichen Kosten der streitigen Maßnahme blieben damit im Unklaren. Folglich konnte der der EuGH die Zumutbarkeit dieser Kosten auch nicht

---

[326] Dies ist eine verkürzte Darstellung. Praktisch würde es wegen der geringen Größe einzelner Datagramme wohl ausreichen, lediglich einen Bruchteil dieser zu untersuchen und bei einem „positiven Treffer“ genauer hinzuschauen, um unerwünschten Datenverkehr eines bestimmten Internet-Angebots zu unterbinden. Dennoch wäre eine enorme Menge an Datenverkehr zu überwachen, da jede logische Verbindung zum zu sperrenden Angebot entdeckt werden müsste.
[327] Vgl. oben Kap. 1 III 2 (S. 19).

bewerten. Allerdings stellte der EuGH fest, dass ein Betroffener ISP darlegen könne, dass ihm die Maßnahme nicht zumutbar sei, sobald diese konkret werde.[328]

Für die betroffenen ISPs wäre ein Mehr an Rechtssicherheit hingegen hilfreich gewesen. Der EuGH kam zu einem abstrakten Ergebnis der Zulässigkeit von Maßnahmen, es wäre ihm aber dennoch möglich gewesen, in seiner Urteilsbegründung darauf hinzudeuten, wie er die infrage kommenden konkreten Sperrmaßnahmen im Hinblick auf ihre Zumutbarkeit einschätzt. So verbleiben für die ISP und die jeweiligen Fachgerichte Unsicherheiten bei der Beurteilung der Rechtmäßigkeit einer konkreten datenverkehrsregulierenden Maßnahme. Für die Internet Service Provider bedeutet dies ein hohes Haftungsrisiko.[329] Die ISPs könnten damit in eine Situation kommen, in der sie unwillentlich eine zumutbare Datenverkehrsregulierung nicht implementieren oder umgekehrt eine unzumutbare Datenverkehrsregulierung aus Angst vor Zwangsmaßnahmen einrichten.

Dass der EuGH die oben dargestellten Überlegungen zu den Kosten von IP- und DNS-Sperre nicht in der UPC-Entscheidung nicht ausdrücklich anstellt, und somit letztlich offenlässt, wie er DNS- und IP-Sperren in Hinblick auf Art. 16 Charta einordnet, lässt dem EuGH und den Mitgliedstaatenandereseits für die Zukunft Entscheidungsspielräume.

b. Informationsfreiheit, Art. 11 Charta

Auch bei den Ausführungen zur Informationsfreiheit fällt auf, dass der EuGH in entscheidenden Punkten unkonkret bleibt.

Der EuGH gibt dem Internet Service Provider, der Adressat einer Anordnung zur Implementierung von Netzsperren geworden ist, auf, bei der Wahl der Sperrmaßnahme die Informationsfreiheit der Nutzer zu berücksichtigen. Die Maßnahme müsse streng auf das Ziel gerichtet sein, den Zugang zu illegalen Inhalten zu verhindern, ohne dass der Zugang der Nutzer zu legalen Inhalten beeinträchtigt werde.[330] Der Wortlaut der Entscheidung enthält an dieser Stelle diesbezüglich keine weiteren Einschränkungen.

An anderer Stelle in derselben Entscheidung hingegen heißt es, der ISP dürfe seinen Nutzern nicht unnötig den rechtmäßigen Zugang zu Informationen verstellen.[331] Da sich der

---

[328] Die Frage der Unzumutbarkeit muss sich im Übrigen nicht nur nach den Aufwendungen, zu denen der ISP gezwungen wird richten, sondern auch nach den sonstigen Belastungen des ISP bei der Durchführung der Maßnahme. Der Internet Service Provider muss sich mit seinen Kunden auseinandersetzen, denen die Maßnahmen in den seltensten Fällen gefallen dürften. Inwiefern deren Proteste den Provider belasten, wird ganz wesentlich von den konkret getroffenen Maßnahmen im Einzelfall abhängen.

[329] In diesem Sinne kritisch auch *Assion*, K&R 2014, 329 (334); *Nazari-Khanachayi*, GRUR 2015, 115 (119 f.); *Stadler*, Internetsperren: EuGH lässt Provider mit der Verantwortung allein, 2013, abrufbar unter http://www.lto.de/recht/hintergruende/h/eugh-urt-c-314-12-internetsperren-gerichte/ (zuletzt besucht am 09.10.2021).

[330] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 56.

[331] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 63 und erneut in Rn. 64.

EuGH jedoch nicht weiter zu dem Thema auslässt, bleibt die Frage, ob er eine datenverkehrsregulierende Maßnahme generell für unzulässig hält, sobald ein Overblocking auftritt. Denkbar wäre auch, dass beim Auftreten von Overblocking eine Abwägung der Informationsfreiheit mit anderen rechtlich geschützten Interessen stattfinden muss. Es sprechen gute Argumente dafür, dass der EuGH hier eher zu einer Abwägungslösung tendiert.[332]

Schon in der Scarlet-Entscheidung sah der EuGH die Informationsfreiheit der Internet-Nutzer wohl eher beeinträchtigt als notwendigerweise verletzt.[333] Der EuGH erklärt Eingriffe in den Datenverkehr zur Urheberrechtsdurchsetzung konsequenterweise in der UPC-Entscheidung auch nicht generell für unzulässig, obwohl jedes denkbare System mit „false positives", also Fällen, in denen das System fälschlicherweise in den Datenverkehr eingreift, zu kämpfen hat. Dies gilt für DPI-Systeme, bei denen spezifische Inhalte geblockt werden, noch mehr allerdings für IP- und DNS-Sperren. [334] Den letztgenannten Maßnahmen ist gemein, dass sie den Zugang zu bestimmten Content Providern insgesamt verhindern anstatt spezifische Inhalte zu filtern. Auch solche Provider, die sich auf Angebote für Raubkopierer spezialisiert haben, werden in überschaubarem Umfang rechtmäßige Informationen zum Abruf bereitstellen. Bei IP-Sperren kommt im Gegensatz zu DNS-Sperren noch erschwerend hinzu, dass ein solches Filtersystem in der Regel zu grob auflöst, um zielgenau ein bestimmtes Angebot zu sperren. Unter einer IP-Adresse sind oft mehrere Angebote zu erreichen, die bei einer Sperre als Kollateralschaden mit dem rechtswidrigen Angebot mitgesperrt würden.[335]

Das Problem liegt an dieser Stelle jedoch weniger darin, dass der EuGH sich nicht eindeutig äußert, ob ein Overblocking generell die Informationsfreiheit verletzt, sondern darin, dass er keine Anhaltspunkte dafür liefert, wann eine Grundrechtsabwägung die Verletzung der Informationsfreiheit zum Ergebnis hätte. Die Beantwortung dieser Frage wird den ISPs überlassen, denen für eine derart anspruchsvolle Grundrechtsabwägung allerdings die Kompetenz und die Legitimation fehlen.[336]

Dies stellt nicht nur ein Problem für die Internet Service Provider dar, sondern auch für die Nutzer dar. So weist *Stadler* zurecht darauf hin, dass die ISPs wegen sogenannter „Chilling Effects"[337] im Zweifel eher großzügig und bereits ohne gerichtliche Anordnung

---

[332] So wird der EuGH auch von BGH, Urt. v. 26.11.2015, I ZR 3/14, 3dl.am, Rn. 44 (juris); BGH, Urt. v. 26.11.2015, Goldesel, I ZR 174/14, BGHZ 208, 82, Rn. 55; sowie *Leistner/Grisse*, GRUR 2015, 105 (109) interpretiert.

[333] Das Scarlet-Urteil betraf allerdings auch ein Filtersystem, das von den zur DVR geeigneten Maßnahmen noch am ehesten *zielgenau* ist.

[334] Vgl. *Kastl*, GRUR 2016, 671 (673).

[335] Siehe oben Kap. 2 III 2 (S. 19); vgl. auch *Sieber/Nolde*, Sperrverfügungen, S. 50.

[336] *Spindler*, MMR 2018, 48 (52); *Assion*, K&R 2014, 329 (334) hält eine „staatsferne" Verwaltungsbehörde gegenüber Zivilgerichten und Providern für am ehesten geeignet, diese Abwägungen vorzunehmen; *Möller*, CR 2011, 733 (734).

[337] Chilling Effects sind Einschüchterungseffekte, die nach *Assion*, Überwachung und Chilling Effects, in: Telemedicus Soko 2014, S. 31 (32) dann entstehen, wenn durch breites hoheitliches Handeln die Bürger von der Ausübung ihrer Grundrechte abgehalten werden.

den Zugang zu bestimmten Angeboten sperren werden, selbst wenn sie dazu rechtlich nicht verpflichtet wären, da ihnen die Haftungsgefahr zu groß sein könnte.[338] Google – wenn auch kein ISP, so doch ein Intermediär in ähnlicher Stellung – kann hier als Beispiel dienen. Der Suchmaschinenbetreiber blendet bestimmte Seiten, die vermeintlich das Urheberrecht verletzen, freiwillig und weitgehend ungeprüft aus den Ergebnissen seiner Internet-Suche aus, wenn sie von Rechteinhabern darauf aufmerksam gemacht werden.[339] Dies führt zu einer massiven Einschränkung des Zugangs zu Informationen, die vom haftenden Provider nicht unbedingt beabsichtigt wird, aber einen Kollateralschaden seiner Bemühungen darstellt, sich rechtlich abzusichern zu wollen.

Abhilfe schafft das vom EuGH geforderte gerichtliche Rechtsschutzverfahren für Internet-Nutzer, mit dessen Hilfe Fälle des Overblockings abgestellt werden sollen, nur theoretisch. Eine datenverkehrsregulierende Maßnahme sei nur dann mit Europarecht vereinbar, wenn die Internet-Nutzer eine Möglichkeit hätten, ihr Recht auf freien Zugang zu Informationen vor Gericht geltend zu machen, sobald die vom ISP getroffenen Maßnahmen bekannt seien.[340] *Assion* merkt zurecht an, dass es interessant wäre zu erfahren, wie der EuGH sich einen solchen praktisch durchführbare zivilprozessualen Rechtsbehelf für massenhaft betroffene Internet-Nutzer vorstelle – zumal im Rahmen des Vollstreckungsverfahrens gegen die ISPs.[341]

Man kann daher festhalten, dass der EuGH in der UPC-Entscheidung zwar erkennt, dass die Einrichtung einer Datenverkehrsregulierung zur Urheberrechtsdurchsetzung für die Informationsfreiheit der Internet-Nutzer wegen Overblockings problematisch ist. Die erforderliche Grundrechtsabwägung im konkreten Einzelfall legt er jedoch den dafür ungeeigneten Intermediären auf. Noch schwieriger macht der EuGH die Angelegenheit für die

---

[338] *Stadler*, Internetsperren: EuGH lässt Provider mit der Verantwortung allein, 2013, abrufbar unter https://www.lto.de/recht/hintergruende/h/eugh-urt-c-314-12-internetsperren-gerichte/ (zuletzt besucht am 09.10.2021).

[339] Bis zum 14.10.2020 wurde bei Google die Löschung von knapp 5 Mrd.URLs auf 3 Mio. Domains beantragt; vgl. Google, Entfernungen von Inhalten aufgrund von Urheberrechtsverletzungen – Google Transparenzbericht, abrufbar unter https://transparencyreport.google.com/copyright/overview (zuletzt besucht am 09.10.2021). An diesem Beispiel zeigt sich auch deutlich, dass in Anbetracht der puren Masse an Sperranfragen eine Abwägung der Grundrechte im Einzelfall weder für ein Zivilgericht noch für eine Verwaltungsbehörde und erst recht nicht für einen Provider praktisch machbar ist. Daher bleibt für die entscheidende Stelle nur, pauschal zu sperren oder pauschal nicht zu sperren, bis irgendwann einmal ein neuronales Netz oder ein vergleichbares EDV-System zu solchen Entscheidungen in der Lage sein wird.

[340] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 57.

[341] Vgl. dazu EuGH, Urt. v. 27.03.2014, Rs. C-314/12, Rn. 57. Der EuGH sagt hier wörtlich, dass die nationalen Gerichte „nicht die Möglichkeit [hätten], eine solche Kontrolle im Stadium des Vollstreckungsverfahrens vorzunehmen, wenn keine dahingehende Beanstandung erfolgt" sei. Es sei allerdings angemerkt, dass der EuGH den Begriff „Vollstreckungsverfahren" hier wohl nicht (nur) im technischen Sinne etwa des deutschen Prozessrechts verwendet, sondern vielmehr den Zeitraum nach Implementierung der DVR-Maßnahme meint. Das grundsätzliche Argument Assions, K&R 2014, 329 (334) greift dies jedoch nicht an.

ISPs dadurch, dass er zur formellen Absicherung des Schutzes der Informationsfreiheit der Internet-Nutzer ein Verfahren vorgibt, das praktisch kaum durchführbar sein dürfte.

c. Geeignetheit der DVR zum Schutz des geistigen Eigentums, Art. 17 Abs. 2 Charta

Der EuGH setzt in der UPC-Entscheidung seine Rechtsprechung aus den Entscheidungen Promusicae und Scarlet fort, dass das geistige Eigentum nicht vorbehaltlos gewährleistet werde, sondern sich mit anderen anwendbaren Grundrechten gemäß Art. 52 Abs. 1 Satz 2 2. HS Charta arrangieren müsse.[342] Erstmalig konkretisiert er jedoch, inwieweit die Rechteinhaber Einschränkungen bei der Effektivität der datenverkehrsregulierenden Maßnahme hinnehmen müssen, und wie sich dies auf das Ergebnis der Abwägung auswirkt.

d. Erforderlichkeitsmaßstab für die Effektivität der DVR

Nach Ansicht des EuGH ist eine datenverkehrsregulierende Maßnahme, die Verletzungen des Urheberrechts nicht vollständig verhindern kann,[343] nicht schon aus diesem Grund ungeeignet, ein angemessenes Gleichgewicht mit den anderen anwendbaren Grundrechten herzustellen. Andererseits müsse die Maßnahme auch für Art. 17 Charta ein hinreichendes Schutzniveau bieten. Unerlaubte Zugriffe auf unrechtmäßig angebotene Werke müssten *zumindest erschwert* werden. Der Zugriff der Internet-Nutzer müsste *zuverlässig* unterbunden werden.[344] Hinreichend ist also eine Maßnahme, die den Zugriff insoweit erschwert, dass man ihn noch als *zuverlässig* beschreiben kann. Fällt das Niveau des Schutzes des Urheberrechts also unter ein *zuverlässiges* Maß, wäre die Datenverkehrsregulierung europarechtlich unzulässig.

Der EuGH äußert sich an dieser Stelle leider etwas widersprüchlich, wenn er einerseits feststellt, dass die magische Grenze erreicht sei, wenn unerlaubte Zugriffe *zumindest erschwert* werden, andererseits aber *zuverlässig* unterbunden werden müssen, ohne sich mit dem Verhältnis der beiden Kriterien auseinanderzusetzen. Eine wortlautgetreue Interpretation muss hier – je nach Formulierung – zu einem unterschiedlich hohen Schutzniveau kommen.

Ein Zugriff auf urheberrechtlich geschützte Werke wäre bereits *zumindest erschwert*, ohne dass dazu ein einziger Download verhindert worden sein müsste. Der Zugriff müsste lediglich mit ein wenig mehr Aufwand verbunden sein. Betrachtet man dieses Kriterium isoliert, stellt es das absolute Minimum dessen dar, was sich als „effektiv" bezeichnen lässt.

Anders hingegen das Merkmal des *zuverlässigen Unterbindens* unberechtigter Zugriffe auf die urheberrechtlich geschützten Werke. Damit stellt der Gerichtshof klar, dass eine

---

[342] EuGH, Urt. v. 29.01.2008, Rs. C-275/06, Promusicae, Slg. 2008, I-00271, Rn. 62 ff.; vgl. auch EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 43; EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 61.
[343] Sogenanntes „Underblocking".
[344] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 62.

DVR zur Urheberrechtsdurchsetzung die geschützten Werke überwiegend effektiv sichern muss, und zwar in einem Maß, dass die Schutzzwecke des Urheberrechtsschutzes für das konkrete Werk im Einzelfall durchgesetzt werden, das Urheberrecht am Werk also nicht leerläuft.

Diese Abgrenzung anhand zweier sich quantitativ unterscheidender Merkmale ist auch durchaus sinnig, wenn man berücksichtigt, dass die rechtlichen Konsequenzen der Tatsache, dass gewisse Formen der Datenverkehrsregulierung leicht von den Nutzern umgangen werden können, Bestandteil der im UPC-Verfahren zu beantwortenden Vorlagefragen war. Vorlagefrage 4 stellt die Verhältnismäßigkeit einer Maßnahme der DVR in diesen Fällen in Zweifel.[345] Der EuGH stellt mit seiner Abgrenzung daher zunächst einmal klar, dass die Datenverkehrsregulierung die Verletzung des Urheberrechts *zumindest erschweren* muss, und dass eine Maßnahme der DVR nicht bereits deshalb unrechtmäßig ist, weil sie keinen *absoluten* Schutz des Urheberrechts gewährleistet.[346] Das Kriterium des *zuverlässigen Unterbindens* ist dahingegen der eigentliche Maßstab, an dem eine Maßnahme der DVR zur Durchsetzung des Urheberrechts im Rahmen der Informationsfreiheit zu messen ist.

Auch dogmatisch ist dies ein sauberes Vorgehen des Gerichtshofs, denn er trennt hier sauber – allerdings ohne sie so zu benennen – die auch im europäischen Recht zu beachtenden Prüfungspunkte der Geeignetheit („*zumindest erschwert*“) und der Verhältnismäßigkeit im engeren Sinn („*zuverlässiges Unterbinden*“).[347]

Der Abgrenzung ist im Grunde zuzustimmen. Der Schutz geistigen Eigentums wird mit den anderen betroffenen Grundrechten in einen vertretbaren Ausgleich gebracht. Auch die mit Art. 17 Charta konkurrierenden Grundrechte werden nicht uneingeschränkt gewährleistet. Dass der Schutz des geistigen Eigentums in einer Grundrechtsabwägung grundsätzlich hinter diese zurücktreten müsste, wäre kaum vertretbar.

Umgekehrt muss ein anderer Punkt berücksichtigt werden, den der EuGH hier nicht explizit anspricht: Aus Sicht der anderen betroffenen Grundrechte ist deren Beeinträchtigung umso eher hinzunehmen, je größer der durch die Maßnahme erlangte Schutz für das Urheberrecht ausfällt. In Anbetracht der Schwere und des Ausmaßes der Beeinträchtigungen der konkurrierenden Grundrechte könnte ein nur minimaler Schutz des geistigen

---

[345] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 17.
[346] Diese Auslegung wird zudem auch durch die Ausführungen unter EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 63 gestützt, die im unmittelbaren textlichen Zusammenhang mit dem Kriterium der Mindesterschwerung in Rn. 62 stehen.
[347] Vgl. zum Prüfungsprogramm der Verhältnismäßigkeit im Europarecht *Borowsky* in: Meyer/Hölscheidt, Charta der Grundrechte, Art. 52 Rn. 37 ff; vgl. auch EuGH, Urt. v. 10.03.2005, Rs. C-96/03 und C-97/03, C-96/03, C-97/03, Tempelmann/van Schaijk, Slg. 2005, I-1895, Rn. 47; EuGH, Urt. v. 09.03.2010, Rs. C-379/08 und C-380/08, C-379/08 , C-380/08, Slg. 2010, I-2007, Rn. 86; EuGH, Urt. v. 08.07.2010, Rs. C-343/09, Afton Chemical, Slg. 2010, I-7023, Rn. 45; EuGH, Urt. v. 22.01.2013, Rs. C-283/11, Sky Österreich, EU:C:2013:28, Rn. 50 ff.

Eigentums für eine DVR nicht ausreichend sein. Zu fordern ist ein qualifiziertes Schutzniveau. Es wäre unverhältnismäßig, wenn die Grundrechte der Internet Service Provider und der Internet-Nutzer massiv eingeschränkt würden für ein System, das keinen spürbaren Schutz für ein konkurrierendes Grundrecht zur Folge hätte.[348]

Auch die Wahl des Begriffs zur Abgrenzung ist treffend gewählt. Der unbestimmte Rechtsbegriff *„zuverlässig"* ist trotz seiner Offenheit noch ausreichend bestimmt, um deutlich zu machen, dass die Effektivität der Datenverkehrsregulierung einerseits nicht absolut gewährleistet sein, andererseits jedoch über ein minimales Schutzniveau hinausgehen muss. Zudem ist er offen genug, um den vielfältigen möglichen Sachverhaltskonstellationen und zukünftigen Änderungen des institutionellen und technischen Umfelds Rechnung zu tragen, deren Beurteilung dem Tatgericht oder den mitgliedstaatlichen Parlamenten bzw. dem Europäischen Parlament belassen bleiben kann. Nicht zuletzt ist ein offener Rechtsbegriff wegen der Wechselwirkungen mit den anderen anwendbaren Grundrechten in der Abwägung gemäß Art. 52 Abs. Hs. 2 Charta vonnöten.

e. Schutzniveaubezogenes Verständnis des Effektivitätserfordernisses

Die Effektivität der Eingriffe in den Datenverkehr bei der Durchsetzung des Urheberrechts ist somit ein mitentscheidender Faktor, wenn es um die Rechtmäßigkeit der DVR-Maßnahmen geht. Wie der EuGH Effektivität im vorliegenden Kontext allerdings genau versteht, ist umstritten: Ist auf die Durchführung der konkreten datenverkehrsregulierenden Maßnahme oder auf die Verringerung der Rechtsverletzungen insgesamt in Bezug auf das geschützte Werk abzustellen? Mit anderen Worten: Reicht es aus, wenn die beschlossene Maßnahme zum Schutz eines oder mehrerer Werke erfolgreich ist? Dann wäre beispielsweise danach zu fragen, ob eine eingerichtete DNS-Sperre, die Nutzer davon abhalten soll, ein bestimmtes Angebot eines Content Providers aufzurufen, den Aufruf zu jenem Angebot *zuverlässig unterbindet*. Oder ist die Effektivität zweckbezogen zu ermitteln? Dann wäre die Maßnahme erst dann hinreichend effektiv, wenn der Zweck des Eingriffs in den Datenverkehr erfüllt und der Zugriff der Nutzer auf den Schutzgegenstand selbst, gleich auf welche Art dieser erfolgt, *zuverlässig* verhindert würde.

Maßnahmebezogen wird das Effektivitätskriterium des EuGH jedenfalls vom Bundesgerichtshof (BGH) verstanden. Entscheidend sei nicht, ob die Datenverkehrsregulierung einen Einfluss auf die Gesamtheit der illegalen Zugriffe auf ein geschütztes Werk habe, sondern die Auswirkungen der Maßnahme auf die konkret beanstandete Website. Der Grund liege darin, dass andernfalls die Rechteinhaber massenhaft begangenen Rechtsverletzungen im Internet schutzlos gegenüber stünden.[349]

---

[348] So auch OLG Hamburg, Urt. v. 21.11.2013, 5 U 68/10, 3dl.am, Rn. 76 (juris).

[349] BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 47; zustimmend: *Finger/Conrath*, MMR 2016, 186 (187); ähnlich auch High Court of Justice London (Chancery Division), Urteil v. 17.10.2014, GRUR 2015, 178, Rn. 173, dort in Bezug auf die Effektivität einer Netzsperre zur Verhinderung von Markenrechtsverletzungen auf Grundlage von Art. 3 Abs. 2 Enforcement-Richtlinie.

Diese Interpretation des BGH der UPC-Entscheidung entspricht allerdings nicht deren Wortlaut und greift auch gedanklich zu kurz. Der EuGH geht nicht von der erfolgreichen Durchführung der Maßnahme, sondern von derem erfolgreich erreichten Zweck aus. Durch die Maßnahme müsse bewirkt werden, dass illegale Zugriffe auf die urheberrechtlich geschützten Werke *„verhindert oder zumindest erschwert"* würden. Die Nutzer des ISP müssten *„zuverlässig"* daran gehindert werden, auf die rechtswidrig zugänglich gemachten Werke zuzugreifen.[350] Der EuGH formuliert hier erfolgsorientiert unter Bezug auf den Schutzgegenstand und nicht hinsichtlich einer effektiven Unterdrückung der Verletzungshandlung des zu sperrenden Online-Angebots. Der Begriff des EuGH von der Effektivität deckt sich folglich mit dem in dieser Arbeit vertretenen Verständnis von Effektivität datenverkehrsregulierender Maßnahmen.[351]

Interpretiert man die Anforderungen des EuGH an die Effektivität maßnahmebezogen wie der Bundesgerichtshof, so geht man lediglich auf das Kriterium ein, dass ein Zugriff auf die Schutzgegenstände *zumindest erschwert* werden müsse, ignoriert dabei jedoch völlig die zweite Anforderung des *zuverlässigen Unterbindens* der Rechtsverletzung. Gerade diese Anforderung stellt aber erst den Maßstab dar, anhand dessen eine Abwägung gemäß Art. 52 Abs. 1 Satz 2 Charta mit anderen Grundrechten und eine Berücksichtigung des Übermaßverbots unter Beachtung der Effektivität der Maßnahme möglich wird.

Eine maßnahmebezogene Interpretation der Mindesteffektivität ist hier daher nicht angezeigt. Vielmehr ist auf den tatsächlichen Effekt des Eingriffs in den Datenverkehr auf die Bedrohung des Schutzgegenstands abzustellen. Dem Rechteinhaber ist hinsichtlich seines Rechtsschutzzieles nicht geholfen mit einer Maßnahme, die mit der größten denkbaren Effektivität in Bezug auf das bezeichnete Angebot umgesetzt wird (also etwa das beanstandete Internet-Angebot faktisch unerreichbar macht), während dies gleichzeitig ohne nennenswerte Auswirkungen auf das Ausmaß der Verletzungen seines Rechtsguts bleibt. Der BGH geht aber genau diesen Weg, sich nicht auf die rechtlichen und technischen Fragen, sondern das Verhalten des Verletzers der Rechte zu konzentrieren.[352] Anders herum erreicht der Rechteinhaber sein Rechtsschutzziel auch dann, wenn die Effektivität in Bezug auf die gewählte Maßnahme eher gering ist (weil das Angebot z.B. durch technische Umgehungsmaßnahmen oder Ineffektivitäten im Filtermechanismus grundsätzlich erreichbar bleibt), dafür aber die Verletzungen des Schutzgegenstands insgesamt substantiell abnehmen.[353]

---

[350] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 62.
[351] Vgl. oben Kap. 1 IV 2 (S. 37).
[352] Dem BGH hier zustimmend *Finger/Conrath*, MMR 2016, 186 (188).
[353] Teilweise im Widerspruch zu seiner maßnahmebezogenen Auslegung der Effektivität der DVR lässt der BGH in der Entscheidung BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 48 im Ergebnis dieses Argument nicht unberücksichtigt und führt sonstige positive Wirkungen einer Netzsperre an, die sich selbst im Falle der Umgehung der streitgegenständlichen Sperrmaßnahme durch z.B. ein gesteigertes Unrechtsbewusstsein des Nutzers, der auf eine Netzsperre trifft, auswirken würden.

3. In den Entscheidungen Scarlet und UPC in Bezug auf die Zulässigkeit der DVR offengelassene Fragen mit Grundrechtsbezug

Der EuGH lässt in seiner Rechtsprechung zur Vereinbarkeit der Datenverkehrsregulierung mit europäischen Grundrechten einige im Verfahren aufgeworfenene Fragen mit Grundrechtsbezug zunächst offen, so dass diese bislang keiner abschließenden höchstrichterlichen Klärung zugeführt sind. Um den Rahmen des potentiell rechtlich Zulässigen in der Datenverkehrsregulierung zu bestimmen, sind diese offengelassenen Fragen darzustellen

a. Eingriff in das Recht auf Privatleben und das Kommunikationsgeheimnis, Art. 7 Charta

Der EuGH erwähnt Beeinträchtigungen der durch Art. 7 Charta geschützten Grundrechte in seiner Rechtsprechung zur Datenverkehrsregulierung zur Urheberrechtsdurchsetzung mit keiner Silbe. Dies ist schon deshalb erstaunlich, weil Art. 7 Charta bzw. der entsprechende Art. 8 EMRK Bestandteil der Vorlagefrage in der Scarlet-Entscheidung waren.[354] Auch Generalanwalt *Cruz Villalón* sich in seinen Schlussanträgen zur Scarlet-Entscheidung mit einer Beeinträchtigung des Art. 7 Charta durch das streitige Filtersystem befasst.[355]

Art. 7 Charta sieht vor, dass jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation besitzt. Art. 7 Charta schützt damit vier Teilbereiche der Privatsphäre. Bei Art. 7 Charta handelt es sich um ein echtes Grundrecht und nicht bloß um einen Grundsatz im Sinne des Art. 52 Abs. 5 Charta. Es ist ein vollwertiges subjektives Recht.[356] Ob es sich dabei um ein einheitliches Recht auf Privatsphäre oder um mehrere eigenständige Rechte handelt, ist umstritten.[357] Unbestritten ist jedenfalls, dass diese unterschiedlichen Aspekte des Privatsphärenschutzes sich überschneiden.

Die Überschneidungen schlagen sich in dem Ergebnis nieder, dass EuGH und EGMR keine saubere Abgrenzung zwischen dem Recht auf Achtung des Privatlebens, der Vertraulichkeit der Kommunikation (sowie dem Schutz der personenbezogenen Daten, Art. 8 Charta) vornehmen.[358] Die Rechtsprechung zu den einzelnen Aspekten von

---

[354] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 28.
[355] *Cruz Villalón*, Schlussanträge des Generalanwalts v. 14.04.2011, Rs. C-70/10, Slg. 2011, I-11962, Rn. 81 ff.
[356] *Jarass*, Charta der Grundrechte der Europäischen Union, Art. 7 Rn. 7; *Streinz* in: Streinz, EUV/AEUV, Art. 7 Charta Rn. 10.
[357] Für eigenständige Grundrechte argumentierend *Bernsdorff* in: Meyer/Hölscheidt, Charta der Grundrechte, Art. 7 Rn. 15 ff; offen lassend: *Jarass*, Charta der Grundrechte der Europäischen Union, Art. 7 Rn. 2; a.A. *Kingreen* in: Calliess/Ruffert, EUV/AEUV, Art. 7 Charta Rn. 1; *Frenz*, Handbuch Europarecht – Bd. 4, Rn. 1168; *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 7 Charta Rn. 8.
[358] Vgl. nur EGMR, Urt. v. 16.02.2000, Nr. 27798/95, Amman ./. Schweiz, Rep. 2000-II, S. 201, §§ 68 ff.; EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C-594/12, Digital Rights Ireland, EU:C:2014:238, Rn. 32 ff.

Art. 7 Charta ist folglich zu wenig ausdifferenziert, um hier eine strenge Binnenunterscheidung vorzunehmen.

Art. 7 Charta ist Art. 8 EMRK wörtlich nachgebildet.[359] Damit sind die Rechte aus Art. 7 Charta gemäß Art. 52 Abs. 3 Satz 1 Charta so auszulegen, dass sie der Bedeutung und der Tragweite der in der EMRK garantierten korrespondierenden Rechte entsprechen. Unschädlich ist insoweit, dass die Charta den Begriff der „Korrespondenz" in Art. 8 Abs. 1 durch den Begriff der „Kommunikation" ersetzt, da der Wortlaut des Schutzbereichs des Art. 7 Charta insoweit nicht wesentlich von dem der EMRK abweicht.[360] Die Rechtsprechung des EGMR gewinnt dadurch über das ohnehin schon vorhandene Maß bei der Auslegung des Art. 7 Charta an zusätzlicher Bedeutung. Das Recht auf Privatleben[361] und das Briefgeheimnis[362] sind zudem als allgemeine Rechtsgrundsätze des Unionsrechts anerkannt.

Bei der Datenverkehrsregulierung kommen im Rahmen des Art. 7 Charta insbesondere Eingriffe in das Recht auf Achtung des Privatlebens und der Kommunikation in Betracht. Wie soeben schon angedeutet, bereitet hier die Abgrenzung Schwierigkeiten, da es in diesem Zusammenhang im Europarecht an einer gewachsenen Dogmatik wie etwa im deutschen Recht fehlt.

Mit der Achtung der Kommunikation meint die Charta den Schutz des kommunikativen Übermittlungsvorgangs.[363] Die Kommunikation entspricht inhaltlich der durch Art. 8 EMRK geschützten Korrespondenz und umfasst dabei jede technische Form der Kommunikation unter Abwesenden.[364] Sie beinhaltet also sowohl den Schutz klassischer Arten der Verständigung wie Brief oder Telefon als auch deren digitale Formen über das Internet. Der Kommunikationsbegriff ist dynamisch und entwicklungsoffen.[365] Hintergrund des besonderen Schutzes der Fernkommunikation ist die Gefährdung der Vertraulichkeit des Kommunikationsinhaltes, wenn man diesen einem Dritten zur Übermittlung anvertraut, da man etwa dem Postunternehmen oder dem Internet Service Provider damit den faktischen Zugriff auf die Kommunikation ermöglicht.[366]

Weniger leicht zu beschreiben ist der geschützte Bereich des Privatlebens. In der Rechtsprechung des EGMR ist die Achtung des Privatlebens ein weit gefasster Begriff und einer abschließenden Definition nicht zugänglich.[367] Es umfasst u.a. das Recht auf Identität und persönliche Entwicklung sowie das Recht, Beziehungen zu anderen Menschen und zur

---

[359] ABl 2007/C 303/17 (20). Lediglich der Begriff „Korrespondenz" wurde durch den aktuelleren Begriff „Kommunikation" ersetzt, um damit die technischen Entwicklungen nachzuvollziehen.
[360] *Ziegenhorn*, Einfluss der EMRK, S. 152 f.
[361] Vgl. EuGH, Urt. v. 08.04.1992, Rs. C-62/90, Slg. 1992, I-02575, Rn. 23.
[362] Vgl. EuGH, Urt. v. 26.06.1980, Rs. C-136/79, National Panasonic, Slg. 1980, S. 2033 (2056 f.), Rn. 17 ff.; EuGH, Urt. v. 18.05.1982, C-155/79, S. 1577 (1610), Rn. 18 ff.
[363] *Kingreen* in: Calliess/Ruffert, EUV/AEUV, Art. 7 EU-Charta Rn. 10.
[364] ABl 2007/C 303/17 (20).
[365] *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 7 Charta Rn. 38.
[366] *Bernsdorff* in: Meyer/Hölscheidt, Charta der Grundrechte. Art. 7 Rn. 20.
[367] *Bernsdorff* in: Meyer/Hölscheidt, Charta der Grundrechte, Art. 7 Rn. 15.

Außenwelt einzugehen und zu entwickeln.[368] Zudem werden alle Bereiche geschützt, in denen der Bürger aufgrund der Umstände vernünftigerweise den Schutz der Privatheit erwarten kann.[369] *Bernsdorff* ordnet dem durch Art. 7 Charta geschützten Bereich des Privatlebens alle Bereiche des Lebens zu, die andere Personen nicht betreffen.[370] Dem Privaten gegenüber steht das zur Öffentlichkeit hin gerichtete Leben. Dies kann man als den Teil des Lebens verstehen, den man freiwillig nach außen hin offenlegt.[371]

Bei einer derart offenen Definition des Schutzbereiches könnte ein Blick darauf, wann ein Eingriff in diesen vorliegt, zur genaueren Abgrenzung hilfreich sein. Dies wird von der Rechtsprechung jedoch auf abstrakter Ebene ähnlich vage und selbstreferenziell wie beim Schutzbereich abgegrenzt: Ein Eingriff in die Privatsphäre liegt vor, wenn eine Regelung erlassen wird, die das Privatleben betrifft oder jedenfalls faktisch auf diese einwirkt.[372] Nicht erforderlich ist nach der Rechtsprechung von EGMR und EuGH, dass die betroffenen Informationen sensibler Natur sind. Ebenso wenig müssen dem Betroffenen tatsächlich Nachteile durch den Eingriff entstanden sein.[373] Ein Eingriff in die Kommunikationsfreiheit liegt vor, sobald eine Maßnahme den Kommunikationsvorgang betrifft und dies zur Kenntnis entweder der Inhalte der Kommunikation oder der Kommunikationsdaten wie Absender, Adressat oder Zeitpunkt der Kommunikation führt.[374] Dies gilt ausdrücklich auch für die Beobachtung der Internet-Nutzung.[375]

Die europäische Rechtsprechung zu Art. 8 EMRK/Art. 7 Charta beinhaltet glücklicherweise einige Entscheidungen, die auch für die in dieser Arbeit relevanten Sachverhalte aufschlussreich sind, auch wenn sie nicht direkt eine Datenverkehrsregulierung betreffen. So hat der EGMR festgestellt, dass bereits die Erhebung und Speicherung von Informationen über das Privatleben eines Individuums Eingriffe in Art. 8 EMRK darstellen.[376]

Das relevanteste und gleichzeitig aktuellste Urteil in diesem Kontext ist die Vorratsdatenspeicherungs-Entscheidung des EuGH von 2014. Danach stellen die Erhebung und

---

[368] EGMR, Urt. v. 02.09.2010, Nr. 35623/05, Uzun ./. Deutschland, Rep. 2010/VI, S. 1, http://hudoc.echr.coe.int/eng?i=001-100293 (HUDOC), §§ 43 ff., dort m.w.N.
[369] EGMR, Urt. v. 26.07.2007, Nr. 64209/01, Peev ./. Bulgarien, http://hudoc.echr.coe.int/eng?i=001-81914 (HUDOC), §§ 38 f. EGMR, Urt. v. 02.09.2010, Nr. 35623/05, Uzun ./. Deutschland, Rep. 2010/VI, S. 1, http://hudoc.echr.coe.int/eng?i=001-100293 (HUDOC), § 45.
[370] *Bernsdorff* in: Meyer/Hölscheidt, Charta der Grundrechte, Art. 7 Rn. 15.
[371] Vgl. EGMR, Urt. v. 02.09.2010, Nr. 35623/05, Uzun ./. Deutschland, Rep. 2010/VI, S. 1, http://hudoc.echr.coe.int/eng?i=001-100293 (HUDOC), § 44.
[372] *Jarass*, Charta der Grundrechte der Europäischen Union, Art. 7 Rn. 27 f.
[373] EGMR, Urt. v. 16.02.2000, Nr. 27798/95, Amman ./. Schweiz, Rep. 2000-II, S. 201, § 70; EuGH, Urt. v. 20.05.2003, Rs. C-465/00, Österreichischer Rundfunk, Slg. 2003, I-04989, Rn. 75; EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C-594/12, Digital Rights Ireland, EU:C:2014:238, Rn. 33.
[374] *Jarass*, Charta der Grundrechte der Europäischen Union, Art. 7 Rn. 31.
[375] EGMR, Urt. v. 03.07.2007, Nr. 62617/00, Copland ./. Vereinigtes Königreich, Rep. 2007-I, S. 317, § 41.
[376] EGMR, Urt. v. 16.02.2000, Nr. 27798/95, Amman ./. Schweiz, Rep. 2000-II, S. 201, § 70.

Speicherung von Metadaten[377] der elektronischen Kommunikation (z.B. kontaktierte Telefonnummern, Empfangsadressen von E-Mails, GPS-Daten und aufgerufene IP-Adressen) durch einen Internet-Provider einen Eingriff in Art. 7 (und Art. 8) Charta dar, da aus diesen Daten detaillierte Rückschlüsse auf das Privatleben geschlossen werden können.[378] Dies betrifft etwa Gewohnheiten des täglichen Lebens, häufige oder vorübergehende Aufenthaltsorte, das soziale Umfeld und die darin gelebten Beziehungen.[379] Ein Eingriff in das Recht auf Achtung des Privatlebens besteht also im europäischen Grundrechtsschutz bereits bei der Erhebung der Umstände der Kommunikation und nicht erst dann, wenn deren Inhalt berührt wird.[380]

Auch liegt bereits ein Eingriff in der erstmaligen Erhebung und Speicherung personenbezogener Daten. Der EuGH hat entschieden, dass es sich bei einer eventuellen Weiterleitung der erhobenen Daten an eine andere Stelle lediglich um einen erneuten Eingriff handelt.[381]

Lässt sich diese Rechtsprechung nun ohne weiteres auf Fälle der Datenverkehrsregulierung übertragen? Stellt es also automatisch einen Eingriff in das Recht auf Achtung des Privatlebens und der Kommunikation dar, wenn – wie bei allen Spielarten der Datenverkehrsregulierung üblich – Metadaten der Kommunikation wie die IP-Adresse des Nutzers und des Servers verarbeitet werden? Folgt man dem EuGH und dem EGMR, ist dies wohl die zwingende Konsequenz. Jedenfalls aus der Perspektive der Kommunikationsfreiheit liegt danach eindeutig ein Eingriff vor. Bei jeder Form der Datenverkehrsregulierung erlangt der Provider Kenntnis von den Umständen der Kommunikation, zumindest die Information, wer auf welches Internetangebot zugreifen möchte.

Bei der Deep Packet Inspection kommt hinzu, dass zudem auch von den Inhalten der Kommunikation Kenntnis genommen wird. Ein Eingriff unter dem Aspekt des Schutzes des Privatlebens liegt zwar nicht allein deshalb vor, weil Daten wie bei der Vorratsspeicherung gespeichert würden und sich über Verknüpfungen der Daten Profile erstellen lassen. Je nach Verfahren werden Daten bei der DVR teilweise nur in Echtzeit oder im Rahmen eines *Flows* verarbeitet. Diese Daten reichen bei nur kurzfristiger Speicherung nicht aus, um umfangreiche Profile einzelner Nutzer zu erstellen. Andererseits wird jedoch notwendigerweise zumindest kurzfristig von Umständen Kenntnis genommen, die der Nut-

---

[377] Metadaten werden hier verstanden als solche Daten, die nicht den Inhalt einer Kommunikation bilden, aber anlässlich der Kommunikation anfallen.
[378] EGMR, Urt. v. 03.07.2007, Nr. 62617/00, Copland ./. Vereinigtes Königreich, Rep. 2007-I, S. 317, § 44; EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C-594/12, Digital Rights Ireland, EU:C:2014:238, Rn. 34.
[379] EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C-594/12, Digital Rights Ireland, EU:C:2014:238, Rn. 26 f.
[380] Um den Inhalt der Kommunikation geht es in diesem Fall nicht, sondern um die Informationen über sein Privatleben, die der Nutzer mit den Metadaten preisgibt.
[381] EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C-594/12, Digital Rights Ireland, EU:C:2014:238, Rn. 35.

zer nicht mit der Allgemeinheit zu teilen beabsichtigt und daher seinem Privatleben zuzurechnen sind. Dies gilt sowohl für die Metadaten als auch für die Kommunikationsinhalte. Selbst wenn diese im Zweifel unverfänglich sein sollten und dem Nutzer kein Schaden durch die Kenntnisnahme entsteht, handelt es sich um einen Eingriff.

Ein (eigener) Eingriff in die Kommunikationsfreiheit des Art. 7 Charta liegt auch dann vor, wenn der Datenverkehr nicht bloß beobachtet wird, sondern auch als Folge tatsächlich umgeleitet, blockiert oder in sonstiger Weise manipuliert wird. Dies hat der EGMR für Art. 8 EMRK entschieden.[382] Im Falle einer DVR ist also ein zusätzlicher Eingriff gegeben, wenn und sobald das Filtersystem zu der Entscheidung gelangt, eine bestimmte Übertragung zu unterbinden.

Problematisch ist, dass sich Art. 7 und Art. 8 Charta inhaltlich stark überschneiden und der Schutz personenbezogener Daten auf den ersten Blick das speziellere Grundrecht zu sein scheint. Wenn der Gerichtshof Art. 8 Charta als *lex specialis* zum Schutz der Privatsphäre aus Art. 7 Charta auffasst, könnte dies die gleichzeitige Anwendung von Art. 7 Charta ausschließen, soweit der Schutzbereich von Art. 8 Charta berührt ist. Doch auch ein solcher Grundsatz lässt sich aus der Rechtsprechung des EuGH nicht ableiten.

Ob es sich dabei in dem Sinne um eine *lex specialis* handelt, so dass es in seinem Anwendungsbereich Art. 7 Charta verdrängen würde, ist nicht einfach zu beantworten.[383] Dies liegt an der inhaltlichen Verwandtschaft, aber systematischen Trennung der beiden Grundrechte. Art. 8 Charta ist gegenüber Art. 7 Charta von seiner systematischen Stellung her ein eigenständiges Grundrecht. Nicht nur in der deutschen Verfassungstradition,[384] sondern auch in der Europäischen Menschenrechtskonvention (Art. 8 EMRK) [385] und den Grundrechten der Charta[386] findet der Schutz personenbezogener Daten jedoch

---

[382] EGMR, Urt. v. 15.02.1992, Nr. 10802/84, Pfeifer und Plankl ./. Österreich, Serie A Nr. 227, §§ 43 ff. EGMR, Urt. v. 04.09.2002, Nr. 37471/97, William Faulkner ./. Vereinigtes Königreich, http://hudoc.echr.coe.int/eng?i=001-60492 (HUDOC), § 11. Der EGMR hatte in beiden Verfahren über abgefangene Briefpost bzw. Zensur von Textpassagen einer Briefkorrespondenz von Strafgefangenen zu urteilen. Der Fall ist auf blockierten Internet-Datenverkehr und Art. 7 Charta übertragbar, da der Kommunikationsbegriff technologieneutral ist und Art. 8 EMRK ansonsten Art. 7 Charta entspricht. So auch; *Jarass*, Charta der Grundrechte der Europäischen Union, Art. 7 Rn. 25. Differenzierter ist die Situation beim Telekommunikationsgeheimnis nach Art. 10 GG zu beurteilen. In dessen Rahmen wird lediglich die Vertraulichkeit der Kommunikation geschützt, nicht aber die Möglichkeit der Kommunikation an sich. Vgl. hierzu *Jarass*, Charta der Grundrechte der Europäischen Union, Art. 7 Rn. 31. Zudem ausführlich unten Kap. 3 IV 2 b) (1) (S. 200).

[383] So *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 7 Charta Rn. 17.

[384] Seit BVerfG, Urt. v. 15.12.1983, 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83 ..., Volkszählung, BVerfGE 65, 1 (41 ff.).

[385] Statt vieler: EGMR, Urt. v. 04.12.2008, Nr. 30562/04, 30566/04, S. and Marper ./. Vereinigtes Königreich, Rep. 2008-V, S. 167, § 66 f.; vgl. auch *Meyer-Ladewig*, EMRK, Art. 8 Rn. 40 ff.

[386] EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C-594/12, Digital Rights Ireland, EU:C:2014:238, Rn. 62; *Kokott*, Schlussanträge der Generalanwältin v. 18.07.2007, Rs. C-275/06, Slg. 2008, I-00271, Rn. 51.

seinen Ursprung im Schutz der Privatsphäre. Art. 8 Charta umgekehrt findet keine direkte Entsprechung in der EMRK.

Da Art. 7 Charta jedoch im Wesentlichen so wie Art. 8 EMRK auszulegen ist, wird deutlich, dass ohne die Existenz von Art. 8 Charta der Schutz personenbezogener Daten auch bei den EU-Grundrechten in Art. 7 Charta zu verorten wäre. Die Motivation des Grundrechtekonvents, das Grundrecht auf Datenschutz aus dem Schutz der Privatsphäre herauszulösen, liegt wohl in der eigenständigen EU- bzw. gemeinschaftsrechtlichen Tradition des Datenschutzrechts. Die Erläuterungen des Präsidiums des Grundrechtekonvents zu Art. 8 Charta verweisen neben einer Referenz auf die EMRK auch auf Art. 286 EGV (Vertrag von Nizza, jetzt Art. 16 AEUV) und die Datenschutz-Richtlinie 95/46/EG.[387]

Überschneiden sich die Schutzbereiche, ist es fraglich, weshalb der allgemeinere Art. 7 Charta nach allgemeinen Auslegungsregeln hier nicht zurücktreten sollte. Der EuGH wendet Art. 7 und Art. 8 Charta allerdings auch durchaus parallel auf denselben Sachverhalt an. In seiner Entscheidung zum biometrischen Pass stellte der EuGH (4. Kammer) fest, dass sich aus Art. 7 und Art. 8 Charta insgesamt ergebe, dass es stets einen Eingriff in diese beiden Rechte bedeuten könne, wenn personenbezogener Daten durch Dritte verarbeitet würden.[388] In diesem Sinne erkannte die Große Kammer *des* EuGH ein Recht aus Art. 7 und Art. 8 Charta auf *„Achtung des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten“* an.[389]

Die Große Kammer *des* EuGH ging in der parallelen Anwendung der beiden Grundrechte noch einen Schritt weiter und rückte von dieser Gesamtbetrachtung ab.[390] Der EuGH sah die Speicherung von Daten über das Privatleben einer Person und deren Kommunikation sowie den Zugriff nationaler Behörden auf diese Daten als eigenständige Eingriffe in Art. 7 Charta an, während der Eingriff in Art. 8 Charta in der weiteren Verarbeitung der personenbezogener Daten liegen sollte.[391]

Diese auf den ersten Blick nicht besonders greifbare Differenzierung wird durch die Lektüre der Schlussanträge in dieser Rechtssache erhellt. Zentrale These des Generalanwalts *Cruz Villalón* zur Konkurrenz der Art. 7 und 8 Charta ist, dass diese zwar sehr eng verwandt seien, das soeben angesprochene Grundrecht aus Art. 7 und Art. 8 Charta auf Achtung des Privatlebens auf die Verarbeitung personenbezogener Daten jedoch nicht „*systematisch*“ angewendet werden könne in dem Sinne, dass die Art. 7 und Art. 8 Charta bloß

---

[387] ABl (EU) 2007, C 303/17 (20).
[388] EuGH, Urt. v. 17.10.2013, Rs. C-291/12, Biometrischer Reisepass, EU:C:2013:670, Rn. 12.
[389] EuGH, Urt. v. 09.11.2010, Rs. C-92/09 und C-93/09, C-92/09 , C-93/09, Agrarbeihilfen, Slg. 2010, I-11063, Rn. 52.
[390] EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C-594/12, Digital Rights Ireland, EU:C:2014:238, Rn. 32 ff.
[391] EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C-594/12, Digital Rights Ireland, EU:C:2014:238, Rn. 34 ff.

unterschiedliche Aspekte ein und desselben Grundrechts seien.[392] Es gebe Fälle, in denen die Verarbeitung personenbezogener Daten nach Art. 8 (Abs. 2 und 3) Charta gerechtfertigt sei, gleichwohl dieselbe fragliche Regelung einen unzulässigen Eingriff in Art. 7 Charta darstelle.[393]

Das Verhältnis der beiden Artikel zueinander sei stets nach der Art der betroffenen personenbezogenen Daten zu bestimmen.[394] Manche Daten seien zwar personenbezogen, aber von Dauerhaftigkeit und gewisser Neutralität geprägt, wie der Name oder die Adresse. Auf den Schutz dieser Daten seien die Garantien des Art. 8 Charta auch in erster Linie ausgerichtet. Andere personenbezogene Daten würden sich hingegen qualitativ auf das Privatleben beziehen. Für diese Daten sei vorrangig der Schutz des Art. 7 Charta einschlägig. *Cruz Villalón* sieht die Erhebung solcher privater Daten als zeitlich vorrangiges Rechtsproblem an, während die eventuell folgende weitere Verarbeitung dieser Daten in erster Linie an Art. 8 Charta zu messen sei.[395]

Diese Abgrenzung *Cruz Villalóns*, die in seinen Schlussanträgen zu den Rechtssachen *Scarlet* und *UPC* so noch nicht formuliert wurde, löst die systematisch kniffelige Frage der Konkurrenz der Art. 7 und 8 Charta inhaltlich in eleganter Weise auf und überzeugt. Der Generalanwalt löst sich im Ergebnis von der Annahme, dass Art. 7 Charta in jedem Fall allgemeiner ist und Art. 8 Charta dessen *lex specialis*. *Cruz Villalón* geht von dem Grundsatz aus, dass die Persönlichkeitssphäre weiter reicht als die durch Art. 7 Charta geschützte Privatsphäre, die deren Kern darstelle. Art. 8 Charta hingegen schütze alle Daten der Persönlichkeitssphäre, inklusive der eher neutralen Informationen, und sei somit aus dieser Perspektive allgemeinerer Natur als Art. 7 Charta, der nur gewisse Arten von Daten schütze. Daher sei es auch hinnehmbar, dass die Verarbeitung solcher personenbezogener Daten, die nicht der Privatsphäre entstammen, nach den gegebenenfalls materiell weniger strengen Art. 8 Abs. 2 und 3 Charta gerechtfertigt werden könnten, solange solche Daten, die privaterer Natur sind, den intensiveren Schutz des Art. 7 Charta genießen.

Das weitere Merkmal, das *Cruz Villalón* vermeintlich zur Abgrenzung heranzieht, namentlich, dass der Eingriff in Art. 7 Charta dem in Art. 8 Charta vorgelagert sei, ist dagegen weniger verallgemeinerbar. Im Gegensatz zu der soeben besprochenen Abgrenzung nach der Tiefe des Eindringens in die Persönlichkeitssphäre des Grundrechtsträgers han-

---

[392] *Cruz Villalón*, Schlussanträge des Generalanwalts v. 12.12.2013, Rs. C-293/12 u. C-594/12, Vorratsdatenspeicherung, EU:C:2013:845, Rn. 62 f.
[393] *Cruz Villalón*, Schlussanträge des Generalanwalts v. 12.12.2013, Rs. C-293/12 u. C-594/12, Vorratsdatenspeicherung, EU:C:2013:845, Rn. 61.
[394] Dieser Gedanke war möglicherweise in seinen Schlussanträgen in der Rs. SABAM bereits angelegt, wurde jedoch nicht näher ausgeführt; vgl. hierzu *Cruz Villalón*, Schlussanträge des Generalanwalts v. 14.04.2011, Rs. C-70/10, Slg. 2011, I-11962, Rn. 79.
[395] *Cruz Villalón*, Schlussanträge des Generalanwalts v. 12.12.2013, Rs. C-293/12 u. C-594/12, Vorratsdatenspeicherung, EU:C:2013:845, Rn. 63 ff.

delt es sich wohl um eine Anwendung jenes Grundsatzes auf den Einzelfall der einschlägigen Rechtssache. Denn letztlich ist auch hier die Qualität der personenbezogenen Daten ausschlaggebend.

In der Rechtssache, auf die sich die soeben zitierten Schlussanträge beziehen, ging es um die Zulässigkeit der Vorratsdatenspeicherung. Diese beinhaltet die Erhebung und Sammlung personenbezogener Telekommunikationsdaten und die mögliche spätere Übermittlung an und Auswertung durch die Strafverfolgungsbehörden. Der Generalanwalt sah in der Erhebung schwerpunktmäßig Art. 7 Charta betroffen, in der weiteren Verarbeitung hingegen schwerpunktmäßig Art. 8 Charta.[396]

Dies ist bei einer Abgrenzung nach der Qualität der Daten in Bezug auf deren Positionierung in der Persönlichkeitssphäre konsequent. Bis zu ihrer erstmaligen Erhebung und Speicherung sind diese Daten privat, da sie sich im rechtlich geschützten persönlichen Bereich des Telekommunikationsteilnehmers befinden. Durch die Erhebung und Speicherung der Daten beim Provider werden die Informationen dieser Privatheit entrissen. Die Daten werden aus Sicht der Öffentlichkeit erst geschaffen, da sie mit dem Akt der Erhebung erstmalig potentiell der Öffentlichkeit für den Zugriff zur Verfügung stehen. Auch wenn dies streng genommen auch eine Verarbeitung personenbezogener Daten darstellt, ist das schwerpunktmäßig beschränkte Grundrecht hier der Privatsphärenschutz.

Eine weitere Verarbeitung hingegen, etwa eine Übermittlung an die Strafverfolgungsbehörden, betrifft die bereits für die Verwendung durch die Öffentlichkeit gewonnenen Daten. Diese sind noch genauso personenbezogen wie zuvor, sie befinden sich aber weniger tief in der Persönlichkeitssphäre, da sie durch die vorangegangene Erhebung und Speicherung bereits ein wenig ans Licht der Öffentlichkeit geholt wurden.[397]

Eine parallele Anwendung der Art. 7 und 8 Charta ist auch bei der Datenverkehrsregulierung angezeigt. Beim Auslesen der zur DVR benötigten Informationen handelt es sich um eine Verarbeitung personenbezogener Daten.[398] Doch liegt darin auch gleichzeitig ein Eingriff in das Privatleben der Internet-Nutzer. Der Nutzer gibt diese Daten, die, wenn

---

[396] Vgl. *Cruz Villalón*, Schlussanträge des Generalanwalts v. 12.12.2013, Rs. C-293/12 u. C-594/12, Vorratsdatenspeicherung, EU:C:2013:845, Rn. 65 f. Die Betonung liegt hier jedoch auf „schwerpunktmäßig". Beide Grundrechte sind nachrangig auch bei dem jeweils anderen Eingriff einschlägig.

[397] Auf diese Weise findet die Intensität der Privatheit der erhobenen Daten nicht erst auf der Ebene der Rechtfertigung Berücksichtigung, sondern kann bei einer weiteren Übermittlung gegebenenfalls zu einem Vorrang von Art. 7 Charta führen. Wie weit die betreffenden Daten durch die erstmalige Erhebung aus der Privatsphäre gelockert wurden, muss maßgeblich von ihrer Grundrechtssensibilität, sprich ihrer Nähe zur Intimsphäre abhängen. Für die Fälle der bei der Vorratsdatenspeicherung erhobenen Daten ist die obige Abgrenzung allerdings korrekt. Anders kann dies jedoch für eine mögliche weitere Verarbeitung der übermittelten Daten, insbesondere deren Verknüpfung, bei den Strafverfolgungsbehörden zu beurteilen sein, da in diesem Fall neue Informationen aus der Privatsphäre gewonnen werden können; vgl. dazu BVerfG, Urt. v. 02.03.2006, 2 BvR 2099/04, Telekommunikationsüberwachung III, BVerfGE 115, 166, (189 f.); *Leutheuser-Schnarrenberger*, ZRP 2007, 9 (11).

[398] Vgl. oben Kap. 2 IV 1 b) (S. 81).

sie gesammelt und verarbeitet werden, viel über sein Leben aussagen können, nicht freiwillig an die Öffentlichkeit. Die Daten sind im Normalfall nicht allgemein einsehbar und letztlich nur ein Nebenprodukt der Kommunikation mit einem anderen Rechner. Diesen Gedanken hat der europäische Gesetzgeber für die Zuordnung der Metadaten zur Privatsphäre sogar sekundärrechtlich festgeschrieben. Das Vertrauen in die Vertraulichkeit der Kommunikationsinhalte und Metadaten wird durch Vorschriften der *Richtlinie zur Vertraulichkeit der Kommunikation über das Internet* geschützt. Gemäß Art. 5 der *RL 2002/58* wird die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten sichergestellt. Der Gesetzgeber hat also selbst einen zusätzlichen Umstand geschaffen, der den Nutzer den Schutz seines Privatlebens erwarten lässt.[399]

Tatsächlich liegt bei Art. 7 Charta auch nach dem hier vertretenen Verfahren zur Abgrenzung der beiden Grundrechte der Schwerpunkt des Eingriffs. Die personenbezogenen Daten, die im Rahmen der Datenverkehrsregulierung verarbeitet werden, sind bei jedem in Frage kommenden Filtersystem von qualifiziert privater Natur. Es handelt sich eben nicht lediglich um die Information, dass ein bestimmter Anschlussinhaber überhaupt im Internet unterwegs ist, was beim Verbreitungsgrad der Internet-Nutzung, der mittlerweile erreicht wurde, keine besonders aussagekräftige Information über das Privatleben eines Menschen mehr ist. Bei der IP-Adresse von Sender und Empfänger (IP-Sperre) bzw. IP-Adresse des Absenders und dem angesteuerten Domain-Namen (DNS-Sperre) handelt es sich um Daten, die unter Umständen tiefe Einblicke in die privaten Gewohnheiten des Nutzers zulassen. Ebensolche Informationen waren zudem bereits in der Vorratsdatenspeicherungsentscheidung Gegenstand des Verfahrens gewesen.[400] Noch deutlicher ist dies bei der Deep Packet Inspection, bei der zusätzlich auch die Inhalte der Kommunikation verarbeitet werden.[401]

Im Unterschied zur Vorratsdatenspeicherung findet bei der Datenverkehrsregulierung nach den hier besprochenen Modellen keine dauerhafte Speicherung der personenbezogenen Daten statt, auf die dritte Stellen zur weiteren zivil- oder strafrechtlichen Verfolgung

---

[399] Obwohl er dies nicht explizit so ausdrückt, argumentiert in diese Richtung wohl auch der EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C-594/12, Digital Rights Ireland, EU:C:2014:238, Rn. 32.

[400] EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C-594/12, Digital Rights Ireland, EU:C:2014:238, Rn. 26 f.

[401] Bei der DPI wäre möglicherweise nach der neuesten Rechtsprechung der Großen Kammer des Gerichtshofs gar die absolut geschützte Intimsphäre betroffen, vgl. EuGH, Urt. v. 06.10.2015, Rs. C-362/14, Schrems I, EU:C:2015:650, Rn. 94: „*Insbesondere verletzt eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des durch Art. 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens[...]*“; ähnlich schon EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C-594/12, Digital Rights Ireland, EU:C:2014:238, Rn. 39: „*[Die Richtlinie 2006/24/EG ist nicht geeignet, den] Wesensgehalt [des Art. 7 Charta] anzutasten, da die Richtlinie, wie sich aus ihrem Art. 1 Abs. 2 ergibt, die Kenntnisnahme des Inhalts elektronischer Kommunikation als solchen nicht gestattet*“.

zugreifen könnten.[402] Art. 8 Charta ist hier also an keiner Stelle das im Schwerpunkt betroffene Grundrecht. Es ist daher nicht unbedingt notwendig, bei der Datenverkehrsregulierung vertieft Art. 8 Charta zu prüfen. Die Prüfung von Art. 7 Charta ist jedoch zwingend. Prüft man stattdessen lediglich Art. 8 Charta, hat dies auch potentiell praktische Konsequenzen, da sich die Voraussetzungen der Rechtfertigung der Eingriffe in beide Grundrechte unterscheiden.

Der Rechtsprechung von EuGH und EGMR zur Frage, wann die Verarbeitung von Daten der Kommunikation, seien es Meta- oder Inhaltsdaten, einen (eingehend zu prüfenden) Eingriff in Art. 7 Charta/Art. 8 EMRK darstellt, ist insgesamt nicht nur zuzustimmen, sondern abseits der Scarlet- und UPC-Entscheidungen ist sie auch stringent. Umso erstaunlicher, dass Art. 7 Charta in keiner der beiden einschlägigen Entscheidungen zur DVR im Urheberrecht eine Rolle spielt.

Eine mögliche Erklärung könnte sein, dass der EuGH jedenfalls in der Scarlet-Entscheidung keine Notwendigkeit gesehen hatte, auch noch auf Art. 7 Charta einzugehen, da das Filtersystem bereits aus anderen Gründen europarechtswidrig war. Generell hat der Gerichtshof sich in seinem Urteil kaum mit dem Themenkomplex der personenbezogenen Daten auseinandergesetzt. Auch mit Art. 8 Charta findet kaum eine inhaltliche Auseinandersetzung statt. Die unterschiedlichen Anforderungen an eine Rechtfertigung kommen praktisch nicht zum Tragen, da eine Prüfung einer möglichen Rechtfertigung im Hinblick auf den ohnehin feststehenden Tenor unterbleiben konnte.

Im Rahmen der UPC-Entscheidung hingegen kann dieses Argument nicht gelten. Schließlich erklärt der EuGH die Datenverkehrsregulierung hier für nicht unzulässig. Eine vermeintliche Rechtswidrigkeit des Eingriffs in Art. 7 Charta hätte zu einem anderen Tenor geführt. Allerdings war im UPC-Verfahren auch keine konkrete Ausgestaltung des Filtersystems durch die Vorlagefrage vorgegeben. Der EuGH dachte sich womöglich, unter diesen Umständen sich nicht mit Art. 7 Charta auseinandersetzen zu müssen. Diese Herangehensweise ist dann konsequent, wenn man nicht davon ausgeht, dass Art. 7 Charta bei jeder denkbaren Form der DVR beeinträchtigt wird.[403]

Angemerkt sei hierzu auch, dass sich die Dogmatik des Art. 7 Charta noch in der Entwicklung befindet. In jüngerer Zeit hat die *Große Kammer des* EuGH hier in Zusammenarbeit mit den Generalanwälten Fortschritte gemacht, die der *3. Kammer* zum Zeitpunkt ihrer Scarlet-Entscheidung noch nicht bekannt waren.[404]

---

[402] Dies wäre technisch gesehen allerdings möglich.
[403] Zur hier vertretenen gegenteiligen Ansicht siehe oben S. 99.
[404] EuGH, Urt. v. 09.11.2010, Rs. C-92/09 und C-93/09, C-92/09 , C-93/09, Agrarbeihilfen, Slg. 2010, I-11063, Rn. 47, 50 ff.; EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C-594/12, Digital Rights Ireland, EU:C:2014:238, Rn. 29 ff.; EuGH, Urt. v. 06.10.2015, Rs. C-362/14, Schrems I, EU:C:2015:650, Rn. 39 ff.; *Cruz Villalón*, Schlussanträge des Generalanwalts v. 12.12.2013, Rs. C-293/12 u. C-594/12, Vorratsdatenspeicherung, EU:C:2013:845, Rn. 55 ff., 100 ff.

Der Schluss, dass eine Datenverkehrsregulierung im Urheberrecht aus Sicht des EuGH zu keiner erwähnenswerten Beeinträchtigung des Schutzes des Privatlebens führe und die Frage daher keiner Auseinandersetzung wert sei, ist mit der sonstigen Rechtsprechung zu Art. 7 Charta dagegen nicht vereinbar.

In Anbetracht der bezüglich Art. 7 Charta und Eingriffen in den Datenverkehr entwickelten Grundsätze steht es nach dem oben Gesagten zu erwarten, dass bei einer künftigen Entscheidung des EuGH zu einer konkreten datenverkehrsregulierenden Maßnahme die Vereinbarkeit dieser mit Art. 7 Charta einen zentralen Bestandteil der Prüfung einnehmen wird.

b. Eingriff in den Schutz personenbezogener Daten im UPC-Verfahren, Art. 8 Charta

Auffällig ist auch, dass der Gerichtshof in der UPC-Entscheidung weder auf Art. 7 Charta eingeht noch – im Gegensatz zum Scarlet-Urteil – Art. 8 Charta erwähnt.[405] Der Grund hierfür ist vermutlich der gleiche wie der im letzten Abschnitt angesprochene, der einer Auseinandersetzung mit Art. 7 Charta im Rahmen der UPC-Entscheidung entgegensteht. Der EuGH sieht womöglich kein durch die Vorlagefrage ausreichend konkret definiertes Filtersystem, um etwas zu der Frage der Beeinträchtigung des Schutzes personenbezogener Daten sagen zu müssen.[406] Wie bereits angesprochen, ist dies ein falscher Schluss. Denn jede denkbare Datenverkehrsregulierung, die helfen könnte, das Urheberrecht durchzusetzen, greift zwangsläufig in Art. 8 Charta ein.[407]

Nach dem hier vertretenen Verfahren zur Abgrenzung von Art. 7 und 8 Charta ist eine eigenständige Prüfung von Art. 8 Charta in einer zukünftigen Entscheidung, die sich mit der Zulässigkeit der Datenverkehrsregulierung zur Durchsetzung des Urheberrechts beschäftigt, nicht unbedingt erforderlich, wenn kein erneuter Zugriff auf die einmal erhobenen Daten möglich oder beabsichtigt ist und zugleich eine eingehende Prüfung einer möglichen Verletzung der durch Art. 7 Charta garantierten Rechte durch die streitgegenständliche Maßnahme stattfindet.

Eine zukünftige Entscheidung zur Datenverkehrsregulierung, die erneut ohne Auseinandersetzung mit Art. 7 oder Art. 8 Charta erginge, wäre hingegen erstaunlich.

---

[405] Auch in den Schlussanträgen zur Rechtssache wird auf Art. 8 Charta nicht eingegangen; vgl. *Cruz Villalón*, Schlussanträge des Generalanwalts v. 26.11.2012, Rs. C-314, UPC Telekabel, EU:C:2013:781.

[406] Die Aussparung dieser Frage ist ein weiterer Hinweis darauf, dass Generalanwalt und Gerichtshof bei dieser Rechtssache UPC an Filtersysteme unter Ausschluss solcher auf Basis von Deep Packet Inspection, dachten. In der Scarlet-Entscheidung wurde schließlich, wenn auch nur am Rande, eine Beeinträchtigung des Schutzes personenbezogener Daten noch geprüft. Dies liegt vor allem deshalb nahe, weil im österreichischen Ausgangsverfahren in der ersten Instanz noch IP- und DNS-Sperren die streitgegenständlichen Filtersysteme darstellten; vgl. dazu EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 12.

[407] Vgl. oben S. 81.

c. Eingriff in die Freiheit der Meinungsäußerung und Informationsfreiheit der Content Povider, Art. 11 Charta

Eine weitere wichtige Frage spricht der EuGH in den einschlägigen Entscheidungen nicht an: Wie steht es um die Rechtmäßigkeit des Eingriffs in die Meinungsfreiheit der Content Provider, auf deren Inhalte der Zugriff Dritter durch die datenverkehrsregulierenden Maßnahmen erschwert oder verhindert wird?[408]

Die Meinungsfreiheit auf EU-Ebene ist zusammen mit der Informationsfreiheit als einheitliches Grundrecht in Art. 11 Abs. 1 Charta geregelt.[409] Danach hat *„[j]ede Person […] das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen […] weiterzugeben"*. Zur Auslegung sind sowohl die Rechtsprechung des EuGH als auch die des EGMR heranzuziehen. Die Meinungsfreiheit ist zudem bereits seit längerem ein vom EuGH anerkannter allgemeiner Grundsatz des Unionsrechts.[410] Außerdem ist Art. 11 Charta dem Art. 10 Abs. 2 Satz 1 EMRK wörtlich nachgebildet, so dass Art. 52 Abs. 3 Charta Anwendung findet.

Zwar wurde dieses Grundrecht sowohl in der Scarlet- als auch in der UPC-Entscheidung geprüft.[411] Die Perspektive war jedoch beide Male die der Internet-Nutzer, deren Freiheit beeinträchtigt wurde, sich ohne staatliche Beschränkungen zu informieren. Außer Acht gelassen wurde jedoch das Grundrecht der Inhalte-Anbieter, Informationen weiterzugeben, ohne daran durch den Staat gehindert zu werden. Auch Content Provider sind Träger des Grundrechts aus Art. 11 Charta.[412]

Da der EuGH bislang noch keine Bemühungen zur Entwicklung einer eigenständigen Dogmatik zu Art. 11 Abs. 1 Charta unternommen hat, kann zur Definition des Schutzbereichs bedenkenlos auf die Rechtsprechung des EGMR zurückgegriffen werden.[413] Der sachliche Schutzbereich des Art. 11 Abs. 1 Charta ist danach denkbar weit gefasst. Als Meinung geschützt werden alle Ansichten, Überzeugungen, Einschätzungen, Stellungnahmen, Tatsachenäußerungen und Werturteil, ohne dass dabei Rücksicht auf Qualität

---

[408] Kritisch zu diesem Umstand auch *Assion*, K&R 2014, 329 (334).
[409] *Jarass*, Charta der Grundrechte der Europäischen Union, Art. 11 Rn. 2.
[410] EuGH, Urt. v. 17.01.1984, Rs. C-43/82, 63/82, Festpreise für Bücher, Slg. 1984, S. 19 (62), Rn. 33 f.; EuGH, Urt. v. 13.12.1989, Rs. 100/88, Slg. 1989, S. 4285 (4309), Rn. 16; EuGH, Urt. v. 18.06.1991, Rs. C-260/89, Slg. 1991, I-2925, Rn. 44; EuGH, Urt. v. 04.10.1991, Rs. C-159/90, Slg. 1991 I-04685, Rn. 30 f.
[411] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 52; EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 55.
[412] *Calliess* in: Calliess/Ruffert, EUV/AEUV, Art. 11 Charta Rn. 9.
[413] *Cornils* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 11 Charta Rn. 32.

und Thematik genommen wird.[414] Es werden also grundsätzlich alle Kommunikationsinhalte geschützt, welcher Art sie auch sein mögen.[415] Dies gilt nicht nur für eigene Inhalte, sondern auch, wenn fremde Inhalte weitergegeben werden.[416] Ebenfalls in den Schutzbereich fallen nach der Rechtsprechung des EGMR leichte Unterhaltung,[417] Werbung,[418] verletzende, schockierende und beunruhigende Äußerungen[419]. Eine Einschränkung des Schutzbereichs gilt allerdings für hassverbreitende und rassistische Äußerungen.[420]

Umfasst wird allerdings lediglich die Individual-, nicht hingegen die Massenkommunikation. Letztere wird durch Art. 11 Abs. 2 Charta geschützt und ist nach herrschender Meinung als eigenständiges Grundrecht zu verstehen.[421] Ob man dies im Ergebnis so sieht oder nicht, hat allerdings eher Konsequenzen für die objektivrechtlichen Garantien der Medienfreiheit im Hinblick etwa auf Fragen der Medienpluralität als auf die Rolle des Art. 11 Charta als subjektives Abwehrgrundrecht in den hier relevanten Fällen.[422]

Bei den Inhalten, die Content Provider über das Internet anbieten und teilen, handelt es sich um von Art. 11 Abs. 1 Charta geschützte Äußerungen.[423] Dies gilt zum einen für die

---

[414] So zusammenfassend *Trstenjak*, Schlussanträge der Generalanwältin v. 24.11.2010, Rs. C-316/09, Slg. 2011, I-03249, Rn. 77; vgl. auch *Bernsdorff* in: Meyer/Hölscheidt, Charta der Grundrechte, Art. 11 Rn. 12 mit umfassenden weiteren Nachweisen zur einschlägigen Rechtsprechung von EuGH und EGMR zum Schutzbereich von Art. 11 Abs. 1 Charta in Fn. 11; *Jarass*, Charta der Grundrechte der Europäischen Union, Art. 11 Rn. 10; zurückgehend auf: EGMR, Urt. v. 07.12.1976, Nr. 5493/72, Handyside ./. Vereinigtes Königreich, Serie A Nr. 24, § 49.

[415] *Jarass*, Charta der Grundrechte der Europäischen Union, Art. 11 Rn. 10 ff.

[416] *Trstenjak*, Schlussanträge der Generalanwältin v. 24.11.2010, Rs. C- 316/09, Slg. 2011, I-03249, Rn. 81.

[417] EGMR, Urt. v. 28.03.1990, Nr. 10890/84, Groppera Radio AG and Others ./. Schweiz, Serie A Nr. 173, § 54 f.

[418] EGMR, Urt. v. 20.11.1989, Nr. 10572/83, markt intern Verlag GmbH und Klaus Beermann ./. Deutschland, Serie A Nr. 165, § 26.

[419] EGMR, Urt. v. 07.12.1976, Nr. 5493/72, Handyside ./. Vereinigtes Königreich, Serie A Nr. 24, § 49; EGMR, Urt. 26.04.1995, Nr. 15974/90, Prager und Oberschlick ./. Österreich, Serie A Nr. 313, § 38.

[420] EGMR, Urt. v. 23.09.1994, Nr. 15890/89, Jersild ./. Dänemark, Serie A Nr. 298, § 35; EGMR, Urt. v. 04.12.2003, Nr. 35071/97, Gündüz ./. Türkei, Rep. 2003-XI, S. 229, § 38.

[421] *Calliess* in: Calliess/Ruffert, EUV/AEUV, Art. 11 Charta Rn. 6; *Bernsdorff* in: Meyer/Hölscheidt, Charta der Grundrechte, Art. 11 Rn. 12; so auch *Jarass*, Charta der Grundrechte der Europäischen Union, Art. 11 Rn. 2, mit Einschränkungen: Der Eigenständigkeit der Medienfreiheit in der Charta stehe der Lösung des Art. 10 EMRK gegenüber, der die Individual- und Massenkommunikation einheitlich schütze.

[422] So weist *Jarass*, Charta der Grundrechte der Europäischen Union, Art. 11 Rn. 28, 40 darauf hin, dass unabhängig von der Antwort auf die Frage, ob die Massenkommunikation durch Art. 11 Abs. 2 Charta in einem eigenständigen Grundrecht geschützt wird, die Einschränkungsmöglichkeiten doch die gleichen bleiben.

[423] Nach der hier vertretenen Auffassung ergibt es wenig Sinn, wie EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959 und EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192 die Informationsfreiheit der Internetnutzer gemäß Art. 11 Abs. 1 Charta beschränkt zu sehen, andererseits die Meinungsfreiheit der Content Provider auf Art. 11 Abs. 2

Inhalte derjenigen Anbieter, die angeboten werden, ohne Urheberrechte zu verletzen, die allerdings der Gefahr eines *Overblockings* ausgesetzt sind. Da alle Arten von geteilten Inhalten geschützt sind, muss an dieser Stelle nicht weiter differenziert werden. Dasselbe gilt aber auch für Inhalte, die sich auf urheberrechtsverletzenden Internet-Angeboten befinden, seien sie nun selbst Täter der Urheberrechtsverletzung oder nicht. Die Frage, ob das Angebot gewisser Informationen durch urheberrechtsdurchsetzende Maßnahmen beschränkt werden kann, ist keine Frage des Schutzbereichs, sondern gegebenenfalls der Rechtfertigung eines Eingriffs in Art. 11 Abs. 1 Charta.

Mit einer Datenverkehrsregulierung ist ein Eingriff in die Meinungsfreiheit der Inhalte-Anbieter verbunden. Ein Eingriff liegt in jeder bezweckten oder unmittelbar bewirkten Behinderung der durch Art. 11 Abs. 1 Charta geschützten Kommunikation durch einen Grundrechtsverpflichteten.[424]

Das Mittel datenverkehrsregulatorischer Maßnahmen ist es gerade, einem Internet Service Provider aufzugeben, die Übermittlung bestimmter Kommunikationsinhalte zu unterbinden.

Wie bereits bei der Frage nach einer möglichen Verletzung von Art. 7 Charta hat sich der Gerichtshof entschlossen, trotz eines klaren Eingriffs in die Meinungsfreiheit der von Datenverkehrsregulierung betroffenen Content Provider diesen Aspekt weder in der Scarlet- noch in der UPC-Entscheidung anzusprechen, geschweige denn zu prüfen. Dem Art. 11 Abs. 1 Charta liegt ein sehr ganzheitliches Konzept von Meinungs- und Informationsfreiheit als zwei Seiten desselben Rechts zugrunde.[425]

Man könnte daher argumentieren, die Informationsfreiheit der Nutzer, auf die der EuGH insbesondere in der UPC-Entscheidung eingeht,[426] decke damit in gewisser Weise auch die Meinungsfreiheit der Content Provider ab. Zum einen spricht der EuGH eine solche Absicht jedoch nicht an. Zum anderen wäre dies auch bei konsequenter Anwendung einer solchen Auslegung eine kaum hinnehmbare Verkürzung des Grundrechtsschutzes der Content Provider.

Die Sichtweise, dass Informations- und Meinungsfreiheit lediglich verschiedene Aspekte desselben Grundrechts sein mögen, mag ihre Berechtigung haben. Eine Betrachtung nur der einen Seite würde aber die berechtigten und geschützten Interessen der anderen Seite ausblenden. Praktisch wäre dies insbesondere auf der Rechtfertigungsebene von Bedeu-

---

Charta zu stützen, wenn wie im Internet üblich ein individuell veranlasster Abruf von Informationen stattfindet und zugleich Meinungs- und Informationsfreiheit von der Rechtsprechung als einheitliches Grundrecht betrachtet werden. Praktische Auswirkungen hätte es jedoch auch dann nicht, wenn man hier stattdessen Art. 11 Abs. 2 Charta beeinträchtigt sähe.

[424] *Calliess* in: *Calliess/Ruffert*, EUV/AEUV, Art. 11 Charta Rn. 27; *Jarass*, Charta der Grundrechte der Europäischen Union, Art. 11 Rn. 20.

[425] *Bernsdorff* in: Meyer/Hölscheidt, Charta der Grundrechte, Art. 11 Rn. 12 f.

[426] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 47, 55 f.

tung. Die gemäß Art. 52 Abs. 3 Satz 1 Charta auf Eingriffe in Art. 11 Abs. 1 Charta Anwendung findenden Schranken des Art. 10 Abs. 2 EMRK erfordern zur Rechtfertigung eines Eingriffs unter anderem eine Güterabwägung zwischen der Meinungs- und Informationsfreiheit und einem legitimen Eingriffszweck.[427] Dabei wirkt die Freiheit des Art. 11 Abs. 1 Charta umso stärker, je höher ihre Bedeutung für die demokratische Willensbildung ist. So kann beispielsweise das Recht, Beiträge zur politischen Debatte zu verbreiten, ein stärkeres Gewicht beanspruchen als Inhalte, an deren Verbreitung der Anbieter ein rein kommerzielles Interesse hat.[428] Die Interessen des betroffenen Content Providers sind aber nicht stets gleich schützenswert wie die der Internet-Nutzer daran, sich über ein bestimmtes Internet-Medium zu informieren. Weiterhin ist zu bedenken, dass der Nutzer, der Inhalte einer bestimmten Art sucht, möglicherweise ohne große Probleme zu einem vergleichbaren Anbieter wechseln kann, während die Meinungsfreiheit des Content Providers durch dieselbe Maßnahme bereits in ihrem Wesensgehalt berührt sein kann, wenn ihm keine Ausweichmöglichkeiten zur Verbreitung seiner Meinungen offenstehen.

Der EuGH könnte es also nicht einfach mit diesem dogmatischen Argument begründen, die Meinungsfreiheit der Content Provider bei der Frage der Zulässigkeit der Datenverkehrsregulierung nicht zu berücksichtigen. Der Grund dürfte wiederum darin liegen, dass der EuGH sich bei der Datenverkehrsregulierung bislang mit tiefergehenden rechtlichen Erörterungen sehr zurückhält. Sollte es zu einer weiteren Entscheidung des EuGH zur DVR kommen, wird der EuGH auch mit dieser Frage auseinandersetzen müssen.

d. Auswirkungen dynamischer Kosten der DVR auf die unternehmerische Freiheit, Art, 16 Charta

Fraglich ist auch, ob eine Datenverkehrsregulierung, die auf einer umfassenden Deep Packet Inspection basiert, auch dann noch verfassungswidrig wäre, wenn diese für den Internet Service Provider weniger Kosten verursachen würde, als dies zum Zeitpunkt der Scarlet-Entscheidung der Fall gewesen wäre.

Der EuGH hat sich in den Scarlet- und UPC-Urteilen jeweils hauptsächlich mit der unternehmerischen Freiheit der Internet Service Provider auseinandergesetzt. Das ist insoweit nachvollziehbar, als die streitigen Parteien in den Ausgangsverfahren, die eine Beschränkung ihrer Grundrechte behauptet haben (*Scarlet* bzw. *UPC/Telekabel*), durch die Datenverkehrsregulierung hauptsächlich in ihrer unternehmerischen Freiheit betroffen

---

[427] *Calliess* in: Calliess/Ruffert, EUV/AEUV, Art. 11 Charta Rn. 29; *Cornils* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 11 Charta Rn. 38 ff.; *Meyer-Ladewig* in: Meyer-Ladewig, EMRK, Art. 10 Rn. 43 f.

[428] EGMR, Urt. v. 24.06.2004, Nr. 59320/00, von Hannover ./. Deutschland, Rep. 2004-VI, S. 1, § 77; EuGH, Urt. v. 25.03.2004, Rs. C-71/02, Slg. 2004, I-03025, Rn. 51; EGMR, Urt. v. 11.04.2006, Nr. 71343/01, Brasilier ./. Frankreich, http://hudoc.echr.coe.int/eng?i=001-73200 (HUDOC), § 41; EuGH, Urt. v. 12.12.2006, Rs. C-380/03, Slg. 2006, I-11573, Rn. 155; EuGH, Urt. v. 02.04.2009, Rs. C-421/07, Damgaard, Slg. 2009, I-02629, Rn. 27.

waren. Die anderen durch die DVR beeinträchtigten Grundrechte waren solche der Internet-Nutzer oder der Content Provider, die jedoch keine Parteien des dem Vorabentscheidungsverfahren zugrunde liegenden Rechtsstreits waren.

Kernaussage der Scarlet-Entscheidung in dieser Hinsicht ist, dass ein auf öffentliche Anordnung hin auf eigene Kosten des Providers installiertes Filtersystem, das generell, umfassend und für noch unbekannte Sachverhalte den Datenverkehr reguliert, mit Art. 16 Charta wegen der hohen Kosten und des großen organisatorischen Aufwands unvereinbar sei.[429] Die Kernaussage der UPC-Entscheidung in dieser Hinsicht ist hingegen, dass sich dies nicht automatisch auf jede datenverkehrsregulierende Maßnahme übertragen lässt, sondern der Einzelfall betrachtet werden muss.[430]

Verändern sich die wirtschaftlichen Umstände, wird also eine Deep Packet Inspection günstiger und lässt sie sich ohne großen organisatorischen Aufwand beim Provider implementieren, dürfte dies Einfluss auf eine vermeintliche Verletzung des Art. 16 Charta haben.[431] Das Gleiche dürfte für den Fall gelten, dass die Kosten des Filtersystems nicht vom ISP, sondern von den Rechteinhabern oder einer staatlichen Stelle getragen würden. Der EuGH könnte sich für eine Rechtswidrigkeit der DPI zur Durchsetzung des Urheberrechts wohl nicht mehr auf die unternehmerische Freiheit stützen, sondern müsste in eine tiefere Prüfung anderer Grundrechte einsteigen, wenn er sein Verbot von DPI-*Filtern* in der Urheberrechtsdurchsetzung aufrecht erhalten möchte.

e. Vorbehalt des Gesetzes

Gemäß Art. 52 Abs. 1 Satz 1 Charta muss *„jede Einschränkung der Ausübung der in [der] Charta anerkannten Rechte und Freiheiten […] gesetzlich vorgesehen sein“*. Damit verlangt die Charta für Grundrechtseinschränkungen einen Gesetzesvorbehalt, wobei diesem genügt wird, wenn das Gesetz die Einschränkung selbst festlegt oder dieses zur Einschränkung ermächtigt.[432] Nicht ausdrücklich bestimmt ist die Form, die das Gesetz annehmen muss, um den Anforderungen des Art. 52 Abs. 1 Satz 1 Charta zu genügen. Einschränkungen können jedenfalls sowohl durch Rechtsakte der Union als auch durch solche der Mitgliedstaaten vorgenommen werden.[433] Da die konkrete Regelung der Urheberrechtsdurchsetzung nach dem derzeitigen Ansatz sowohl des europäischen Gesetzgebers[434] als

---

[429] Vgl. EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 48; vgl. oben S. 73.

[430] Vgl. EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 51 ff.

[431] Neue informationstechnologische Verfahren und der technische Fortschritt verringern trotz steigender Datenmengen die Kosten der Deep Packet Inspection bei steigender Genauigkeit der Datenverkehrs-Klassifizierung dramatisch, wie *Aceto u.a.*, PortLoad: Taking the Best of Two Worlds in Traffic Classification, in: 2010 INFOCOM – IEEE Conference on Computer Communications Workshops, S. 3 f.; *Cascarano u.a.*, J. Netw. Syst. Manag. 2010, 7 (29 ff.) aufzeigen.

[432] *Jarass*, Charta der Grundrechte der Europäischen Union, Art. 52 Rn. 23.

[433] Vgl. *Jarass*, Charta der Grundrechte der Europäischen Union, Art. 52 Rn. 24; *Borowsky* in: Meyer/Hölscheidt, Charta der Grundrechte, Art. 52 Rn. 20.

[434] Vgl. etwa Art. 8 Abs. 1, 3 der *InfoSoc-Richtlinie* oder den 23. Erwägungsgrund der *Enforcement-Richtlinie*.

auch des EuGH – dem Grundsatz der Subsidiarität folgend – im Wesentlichen den Mitgliedstaaten überlassen wird, ist hier vorrangig ein Blick auf Grundrechtseinschränkungen durch mitgliedstaatliches Recht relevant.

Ob die Charta ein formelles (also parlamentarisches) mitgliedstaatliches Gesetz verlangt oder auch ein Gesetz im materiellen Sinne genügen lässt, hat der EuGH bislang nicht ausdrücklich geklärt. Insbesondere in der Scarlet-Entscheidung hätte der EuGH Gelegenheit gehabt, diese Frage zu klären – zumal im Zusammenhang mit einer Datenverkehrsregulierung zur Urheberrechtsdurchsetzung. Dies wäre schon deshalb zu erwarten gewesen, weil der Generalanwalt in seinen Schlussanträgen die gerichtliche Anordnung des streitigen Filtersystems unter anderem deshalb für unvereinbar mit der Charta hielt, weil die Rechtsnorm, auf die das Filtersystem gestützt werden sollte, nicht den Anforderungen an den Vorbehalt des Gesetzes im Sinne der Charta genügen würde. Der Vorbehalt des Gesetzes erfordere eine Auseinandersetzung des Parlaments mit der Sachfrage und müsse die Voraussetzungen und Rechtsfolgen hinreichend genau regeln. Diesen Anforderungen würde das mitgliedstaatliche Umsetzungsgesetz, das im Wesentlichen den Inhalt von Art. 8 Abs. 3 InfoSoc-Richtlinie und Art. 11 der Enforcement-Richtlinie wiederholt, nicht gerecht (Damit ist auch klar, dass nicht bereits die einschlägigen Vorschriften der entsprechenden europäischen Richtlinien dem Vorbehalt des Gesetzes gerecht werden).[435]

Zur Auslegung des Vorbehalts des Gesetzes im Sinne der Charta liegt es jedoch nahe, auf die bei der Anwendung der EMRK durch den EGMR gewohnte Dogmatik zurückzugreifen. Auf diese Weise verfährt der Europäische Gerichthof zumindest bei der verwandten Frage nach der Bestimmtheit der Regelung.[436]

Die EMRK verlangt nicht in jedem Fall einer Grundrechtseinschränkung ein formelles Gesetz, sondern sieht einen weitgefassten Rechtssatzvorbehalt vor. Der Grund hierfür sind in erster Linie die in ihren Rechtstraditionen sehr unterschiedlichen Mitgliedstaaten der EMRK, denen dadurch Rechnung getragen werden soll. Das Erfordernis eines formellen Gesetzes würde insbesondere die Mitgliedstaaten, die ein *Common-Law-System* besitzen, vor nicht überwindbare Schwierigkeiten bei der Respektierung des Gesetzesvorbe-

---

[435] *Cruz Villalón*, Schlussanträge des Generalanwalts v. 14.04.2011, Rs. C-70/10, Slg. 2011, I-11962, Rn. 88 ff. Die Grenzen zwischen der formellen rechtsstaatlichen Frage eines parlamentarischen Gesetzes und der materiellen Frage der ausreichenden Bestimmtheit, die aus dem deutschen Verfassungsrecht bekannt ist, wird im europäischen Grundrechtsschutz so nicht gezogen. Insbesondere in einem Fall, in dem nur eine generalklauselartige Ermächtigungsgrundlage existiert, bei deren Erlass der problematische Sachverhalt nicht bedacht wurde, ist eine solche strenge Unterscheidung jedoch auch gekünstelt.

[436] EuGH, Urt. v. 08.04.2014, Rs. C-293/12, C-594/12, Digital Rights Ireland, EU:C:2014:238 Rn. 54; so auch: *Borowsky* in: Meyer/Hölscheidt, Charta der Grundrechte, Art. 52 Rn. 20.

halts stellen. Neben parlamentarischen und von der Exekutive erlassenen Rechtsnormen[437] können daher auch Gewohnheitsrecht und richterliche Rechtsfortbildung[438] Einschränkungen von Grundrechten „*gesetzlich vorsehen*", solange es sich um abstrakt-generelle Regelungen handelt.[439]

Der Gesetzesvorbehalt der EMRK (und der Charta) ist damit grundsätzlich der eines Gesetzes im materiellen Sinne. Dabei ist jedoch zusätzlich auch die Rechtstradition des konkreten das Grundrecht einschränkenden Mitgliedstaats zu beachten. Die Einschränkung muss also dem Vorbehalt des Gesetzes, wie er im jeweiligen Mitgliedstaat gelebt wird, gerecht werden.[440] Für ein Land wie Deutschland bedeutet dies, dass richterliche Rechtsfortbildung in selteneren Fällen den Anforderungen des Vorbehalts des Gesetzes genügen wird, als dies etwa im Vereinigten Königreich, das als Common-Law-Rechtssystem sein Recht weitgehend auf Präzedenzfällen aufbaut, der Fall ist.[441]

Zwar besteht auch in Deutschland grundsätzlich die Möglichkeit, aufgrund jeglichen materiellen Gesetzes in Grundrechte einzugreifen, wenn nicht im Einzelfall besondere formelle Anforderungen an die Grundrechtsschranke im Grundgesetz ausdrücklich vorgeschrieben sind.[442] Über diese besonderen Schranken hinaus besagt allerdings die sogenannte Wesentlichkeitstheorie, die das Bundesverfassungsgericht entwickelte, dass der Gesetzgeber verpflichtet ist, in grundlegenden normativen Bereichen alle wesentlichen Entscheidungen selbst zu treffen und nicht anderen Normgebern zu überlassen.[443] Solche wesentlichen Entscheidungen, die einem formellen Gesetz vorbehalten bleiben, sind die, die für die Grundrechtsausübung wesentlich sind.[444] In Anbetracht der hohen Grundrechtsrelevanz, die eine Datenverkehrsregulierung zur Durchsetzung des Urheberrechts besitzt, ist auch im Hinblick auf die neben dem Telekommunikationsgeheimnis betroffenen Grundrechte nach dem Erfordernis eines formellen Gesetzes bei einer mitgliedstaatlichen Regelung einer DVR zu fragen.

---

[437] EGMR, Urt. v. 18.06.1971, Nr. 2832/66; 2835/66; 2899/66, De Wilde, Ooms und Versyp ./. Belgien, Serie A Nr. 12, § 93; EGMR, Urt. v. 25.03.1985, Nr. 8734/79, Barthold ./. Deutschland, Serie A Nr. 98, § 46.
[438] EGMR, Urt. v. 26.04.1979, Nr. 6538/74, The Sunday Times ./. Vereinigtes Königreich, Serie A Nr. 30, § 47; EGMR, Urt. v. 24.02.1994, Nr. 15450/89, Casado Coca ./. Spanien, Serie A Nr. 285-A, § 43.
[439] EGMR, Urt. v. 10.11.2005, Nr. 44774/98, Leyla Şahin ./. Türkei, Rep. 2005-XI, S. 115, § 88.
[440] *Jarass*, Charta der Grundrechte der Europäischen Union, Art. 52 Rn. 26; *Meyer-Ladewig*, EMRK, Art. 8 Rn. 100; *Borowsky* in: Meyer/Hölscheidt, Charta der Grundrechte, Art. 52 Rn. 20.
[441] *Kingreen* in: Calliess/Ruffert, EUV/AEUV, Art. 52 Charta Rn. 63.
[442] BVerfG, Beschl. v. 28.10.1975, 2 BvR 883/73, 2 BvR 379/74, 2 BvR 497/74, 2 BvR 526/74, BVerfGE 40, 237 (250).
[443] BVerfG, Beschl. v. 09.05.1972, 1 BvR 518/62, 1 BvR 308/64, Facharztbeschluss, BVerfGE 33, 125 (158 f.); BVerfG, Beschl. v. 21.12.1977, 1 BvL 1/75, 1 BvR 147/75, Sexualkundeunterricht, BVerfGE 47, 46 (55 f.).
[444] BVerfG, Beschl. v. 21.12.1977, 1 BvL 1/75, 1 BvR 147/75, Sexualkundeunterricht, BVerfGE 47, 46 (83).

4. Ergebnis

Trotz der Feststellung des EuGH, gerichtliche Anordnungen zu Eingriffen in den Datenverkehr zur Urheberrechtsdurchsetzung seien nicht in jedem Falle mit europäischen Grundrechten unvereinbar, hinterlässt der EuGH Rechtsunsicherheit.[445] Zwar erklärt der EuGH, dass datenverkehrsregulierende Maßnahmen unter bestimmten theoretischen Bedingungen nicht gegen ausgewählte Grundrechte verstoßen (ohne im Hinblick auf andere Grundrechte abschließend geprüft zu haben). Der EuGH lässt jedoch offen, ob die Anforderungen, die er an die Zulässigkeit einer DVR stellt, in der Praxis erfüllbar sind.[446]

Von den drei diskutierten Optionen DPI-, DNS- und IP-Sperre erklärte der EuGH bereits im Scarlet-Urteil eines für mit EU-Grundrechten für unvereinbar: Auf Kosten des Internet Service Providers installierte und betriebene umfassende DPI-Filtersysteme seien nicht vereinbar mit Art. 16 Charta. An gleicher Stelle warf er Probleme bei der Vereinbarkeit mit weiteren Grundrechten auf, musste diese allerdings nicht abschließend prüfen, weil dies für die Beantwortung der Vorlagefragen nicht zwingend notwendig war.[447]

Unter Berücksichtigung der Scarlet-Entscheidung verbleiben als Maßnahmen, die dem ISP auferlegt werden könnten, lediglich die DNS- und die IP-Sperre. Der Gerichtshof prüft in der UPC-Entscheidung allerdings keine dieser Maßnahmen konkret und stellt somit nicht ausdrücklich fest, dass eines dieser Systeme mit den Grundrechten der Charta vereinbar wäre. Vielmehr legt der Gerichtshof einige Kriterien fest, die eine Datenverkehrsregulierung zur Urheberrechtsrechtsdurchsetzung erfüllen muss, um nicht gegen europäische Grundrechte zu verstoßen. Genauer: Die konkrete Art der Maßnahme muss dem belasteten ISP überlassen bleiben, dabei jedoch Urheberrechtsverletzungen mit einer hohen Effektivität verhindern sowie wenigstens weitgehend Overblocking vermeiden. Erfüllt keine Maßnahme diese Voraussetzungen, ohne den ISP dabei über Gebühr in seiner Tätigkeit zu belasten, ist die Anordnung einer DVR insgesamt rechtswidrig.[448]

Ob IP- und DNS-Sperren diesen Kriterien entsprechen können, bestehen große Zweifel. Am ehesten könnte dies – anders bei einem DPI-System – bei der unternehmerischen Freiheit gemäß Art. 16 Charta der Fall sein. Der mit IP- und DNS-Sperren verbundene technische Aufwand für einen ISP ist vergleichsweise gering.[449] Sie belasten den Internet Service Provider daher potentiell in einem für diesen zumutbaren Rahmen. Problematischer ist die Situation bei der Effektivität. Das Filtersystem muss seine Aufgabe zwar

---

[445] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 64.
[446] Kritisch insoweit auch *Szupanar*, Schlussanträge des Generalanwalts v. 16.03.2016, Rs. C-484/14, McFadden, EU:C:2016:170, Rn. 118 ff.
[447] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959.
[448] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 64.
[449] Vgl. oben Kap. 1 III 1–2 (S. 16 ff.).

lediglich *zuverlässig* erfüllen.[450] Aufgrund unkomplizierter und einfacher Umgehungsmöglichkeiten ist dies bezüglich einer IP- und DNS-Sperre jedoch fraglich.[451]

Zweifelhaft ist die Erfüllung der Kriterien des EuGH im Hinblick für die Wahrung des Rechts auf Informationsfreiheit der Internet-Nutzer. Diese wäre verletzt, wenn die Maßnahme nicht zielgenau die urheberrechtswidrigen Inhalte sperrt, sondern auch in unnötiger Weise legale Inhalte.[452] Zielgenau einsetzbar wäre am ehesten die bereits das Grundrecht der unternehmerischen Freiheit verletzende Deep Packet Inspection. Vor allen Dingen die IP-Sperre hat große Probleme mit Overblocking, doch auch bei der Verwendung von DNS-Sperren werden bei Websites, die nicht ausschließlich widerrechtlich urheberrechtlich geschützte Inhalte anbieten, zwangsläufig Inhalte blockiert, die urheberrechtlich unproblematisch sind. Der EuGH setzt in beschränktem Rahmen Grenzen für die rechtliche Zulässigkeit der Datenverkehrsregulierung zur Durchsetzung des Urheberrechts, lässt dabei den Mitgliedstaaten jedoch weitgehende Spielräume für eigenständige Regelungen der Materie.[453]

Am Konkretesten wird der Gerichtshof bei der Frage, inwieweit unterschiedliche Spielarten der Datenverkehrsregulierung zur Urheberrechtsdurchsetzung mit Art. 16 Charta vereinbar sind. Eine DVR mit umfassender Deep Packet Inspection auf Kosten des Internet Service Providers ist europarechtswidrig, jedenfalls solange Kosten und Aufwand einer DPI sich nicht wesentlich verringern.

Weiterhin ist eine DVR wegen der Verletzung der Informationsfreiheit der Internet-Nutzer rechtswidrig, wenn sie nicht zielgenau urheberrechtswidrig geteilte Inhalte filtert, sondern auch unnötig anderen Datenverkehr (Overblocking).

Der EuGH macht zudem Vorgaben an das Mindestmaß an Effektivität, das eine Datenverkehrsregulierung zur Urheberrechtsdurchsetzung leisten muss, um nicht unverhältnismäßig zu sein. Eine Maßnahme der DVR muss die Verletzung des Schutzgegenstandes zunächst zumindest erschweren und diese darüber hinaus *zuverlässig unterbinden*, was ein nicht zwingend perfektes, aber doch in qualifizierter Weise gewährleistetes Schutzniveau des betreffenden geistigen Eigentums bedeutet. Die Effektivität muss sich dabei auf

---

[450] Vgl. oben Kap. 2 V 2 d) (S. 95).

[451] Mit dem Vorschlag einer „hybriden Sperrmaßnahme", also einer kombinierten Anwendung von IP- und DNS-Sperre, wollen *Leistner/Grisse*, GRUR 2015, 19 (26 f.) die Effektivität der Datenverkehrsregulierung steigern, ohne auf Deep Packet Inspection ausweichen müssen.

[452] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 63 f.; vgl. auch oben Kap. 2 V 2 b) (S. 92).

[453] So auch: *Brinkel/Osthaus*, CR 2014, 642 (646). Diese Beschränkung auf einen groben Rahmen, den die Rechtsprechung des EuGH bereitstellt, entspricht auch dem Ansatz des europäischen Gesetzgebers, bei der DVR zur Urheberrechtsdurchsetzung sekundärrechtlich auf Richtlinien (statt auf Verordnungen) und dort auf einen weiten Gestaltungsspielraum der Mitgliedsstaaten zu setzen, und der durch die Art. 51 Abs. 1 Satz 1, 51 Abs. 2, 52 Abs. 4, 52 Abs. 6 und 53 Charta bestimmten umfangreichen Subsidiarität der Grundrechte der Charta. Aus der angeordneten Subsidiarität folgert *F. Kirchhof*, NJW 2011, 3681 (3684 ff.) dann auch einen ausgeprägten Dialog zwischen den europäischen und den mitgliedsstaatlichen Gerichten und eine enge Abstimmung mit den nationalen Grundrechten.

die Auswirkungen auf das Schutzniveau des Schutzgegenstands insgesamt und nicht lediglich auf die Effektivität der Maßnahme selbst beziehen.[454]

Zum grundrechtlichen Prüfungsprogramm im Kontext von Eingriffen in den Datenverkehr gehört nach der Rechtsprechung des EuGH zudem auch das Recht auf Schutz personenbezogener Daten der Internet-Nutzer gemäß Art. 8 Charta. Ob dies seiner Meinung nach auch in nennenswerter Weise für die Meinungsäußerungsfreiheit der Content Provider gemäß Art. 11 Abs. 1 Charta und den Schutz des Privatlebens der Internet-Nutzer gemäß Art. 7 Charta gilt, lässt der EuGH hingegen ebenso offen wie die Frage, ob eine DPI (oder sonstige Art der Datenverkehrsregulierung) gegen Art. 8 und 11 Charta verstößt oder nur einen isoliert betrachtet gerechtfertigten Eingriff darstellt.

V. Die europäischen Grundfreiheiten

Neben dem EU-Vertrag in Verbindung mit der Charta haben auch Vorschriften aus dem AEUV für die Datenverkehrsregulierung im Urheberrecht ihre Bedeutung. Hier sind in erster Linie die Grundfreiheiten relevant.[455]

Die Grundfreiheiten dienen der Verwirklichung des gemeinsamen Binnenmarkts in der EU. Den Binnenmarkt definiert Art. 26 Abs. 2 AEUV als *„einen Raum ohne Binnengrenzen, in dem der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital gemäß den Bestimmungen der Verträge gewährleistet ist“*. Der dort angesprochene freie Verkehr wird durch die institutionalisierten Grundfreiheiten abgesichert.[456]

Die Grundfreiheiten entfalten unmittelbare Wirkung und sind als subjektive Rechte der europäischen Bürger und Unternehmen vom EuGH anerkannt. Ein vorheriger Umsetzungsakt des Primärrechts durch den Mitgliedstaat in nationales Recht ist nicht notwendig.[457] Primärrecht (ebenso wie auch Sekundärrecht) geht mitgliedstaatlichem Recht grundsätzlich vor.[458]

Zweck der Grundfreiheiten ist es, gerade den *grenzüberschreitenden* freien Verkehr zu gewährleisten. Staatliche Beschränkungen, die nur den freien Verkehr innerhalb eines Mitgliedstaats betreffen, werden von den Grundfreiheiten hingegen nicht erfasst.[459] Voraussetzung der Verletzung einer Grundfreiheit ist folglich stets, dass ein grenzüberschreitender Sachverhalt vorliegt. Weiterhin ist den Grundfreiheiten gemein, dass sie nur dann verletzt sind, wenn eine zumindest faktische Ungleichbehandlung von Inländern

---

[454] Siehe oben Kap. 2 V 2 e) (S. 98).
[455] So auch *Schilling*, Präventive staatliche Kontrollmaßnahmen im Internet und ihre Vereinbarkeit mit dem Europarecht, S. 125 (zum EGV).
[456] Die Warenverkehrsfreiheit wird in Art. 28 ff. AEUV näher ausgestaltet und die Dienstleistungsfreiheit in den Art. 56 ff. AEUV. Die übrigen Grundfreiheiten sind im Rahmen dieser Arbeit nicht von weiterer Bedeutung.
[457] EuGH, Urt. v. 05.02.1963, Rs. C-26/62, Formaldehyd, Slg. 1963, S. 3 (25).
[458] Vgl. oben Kap. 2 I 4 a) (2) (S. 50 f.).
[459] *Nettesheim* in: Oppermann u.a., Europarecht, § 22 I 1 (Rn. 2).

und Unionsbürgern vorliegt und dies nicht gerechtfertigt werden kann.[460] Die Grundfreiheiten richten sich dabei vor allem an die Mitgliedstaaten. Praktisch weniger bedeutsam, wenn auch theoretisch ebenso weitreichend, ist die Bindung der Organe der EU an die Grundfreiheiten.[461]

Nicht alle Grundfreiheiten sind hier jedoch gleichermaßen relevant. So liegen mögliche Verletzungen der Kapitalverkehrsfreiheit und der Arbeitnehmerfreizügigkeit in Bezug auf Eingriffe in den Datenverkehr zum Urheberrechtsschutz eher fern. Anders bei Dienstleistungs- und Warenverkehrsfreiheit, da bei der Datenverkehrsregulierung kommerzielle Angebote, die über das Netz angeboten werden (z.B. Streaming), behindert werden könnten. Die Dienstleistungsfreiheit verdient daher Scarlet eine nähere Betrachtung. Andererseits kann auch der Austausch digitaler Güter, die dauerhaft beim Empfänger bleiben, beschränkt werden, so dass man auch an einen Eingriff in die Warenverkehrsfreiheit denken könnte.

Weder die eine noch die andere Grundfreiheit kann absoluten Vorrang beanspruchen, wenn beide Freiheiten betroffen sind. Die Auflösung der Konkurrenz bei Konflikten zwischen der Warenverkehrs- und der Dienstleistungsfreiheit ist durch die Rechtsprechung des EuGH vorgegeben. Der EuGH prüft eine nationale Maßnahme, die sowohl den freien Warenverkehr als auch den freien Dienstleistungsverkehr betrifft, grundsätzlich nur im Hinblick auf eine dieser beiden Grundfreiheiten, wenn eine der beiden Freiheiten gegenüber der anderen völlig zweitrangig ist und dieser zugeordnet werden kann.[462]

Wenn sowohl die Warenverkehrs- als auch die Dienstleistungsfreiheit betroffen sind, dabei allerdings kein Vorrang der einen oder der anderen Freiheit festgestellt werden kann, sind hingegen beide Grundfreiheiten nebeneinander zu prüfen.[463]

1. Warenverkehrsfreiheit

Die Warenverkehrsfreiheit ist in den Art. 28 ff. AEUV geregelt. Während die Art. 28 – 33 AEUV sich mit der hier inhaltlich weniger interessanten Abschaffung der Binnenzölle in der Union beschäftigen, behandeln die Art. 34 ff. AEUV mengenmäßige Beschränkungen des freien Warenverkehrs und Maßnahmen gleicher Wirkung.

---

[460] *Nettesheim* in: Oppermann u.a., Europarecht, § 22 I 1 (Rn. 4).

[461] *Haratsch u.a.*, Europarecht, Kap. 3 IV 3 d) (Rn. 866); *Nettesheim* in: Oppermann u.a., Europarecht, § 22 I 2 (Rn. 7). Schließlich kommt auch in gewissem Umfang eine „Drittwirkung der Grundfreiheiten" grundsätzlich in Betracht. In diesem Fall haben sich auch privatrechtliche Subjekte die Grundfreiheiten zu beachten (Siehe z.B. EuGH, Urt. v. 15.12.1995, Rs. C-415/93, Bosman, Slg. 1995, I-04921, Rn. 82 ff.).

[462] EuGH, Urt. v. 24.03.1994, Rs. C-275/92, Her Majesty's, Slg. 1994, I-01039, Rn. 22; EuGH, 02.12.2010, Rs. C-108/09, Slg. 2010, I-12213, Rn. 43; EuGH, Urt. v. 04.10.2011, Rs. C-403/08 und C-429/08, C-403/08, C-429/08, Murphy, Slg. 2011, I-09083, Rn. 78.

[463] EuGH, Urt. v. 22.01.2002, Rs. C-390/99, Canal Satélite Digital, Slg. 2002, I-607, Rn. 29 ff.; EuGH, Urt. v. 04.10.2011, Rs. C-403/08 und C-429/08, C-403/08, C-429/08, Murphy, Slg. 2011, I-09083, Rn. 79.

Der Anwendung der Warenverkehrsfreiheit auf eine Datenverkehrsregulierung zur Durchsetzung des Urheberrechts steht allerdings eine enge Definition des sachlichen Schutzbereiches entgegen, da es sich bei über das Internet übertragenen Daten nicht um eine Ware im Sinne der Art. 28 ff. AEUV handelt.

Es handelt sich grundsätzlich dann um eine Ware, wenn es sich um eine körperliche Sache handelt, die einen Handelswert hat und die Gegenstand von Handelsgeschäften sein kann.[464] Gemäß der vom EuGH angelegten Abgrenzung zur Dienstleistung, nach der die Leistung körperlicher Natur zu sein hat, um unter die Warenverkehrsfreiheit zu fallen, liegt hier jedoch kein Anwendungsfall der Warenverkehrsfreiheit vor. Internetdatenverkehr, insbesondere in der Form von urheberrechtlich geschützten Gütern, ist eine nichtkörperliche Leistung. Beim Filesharing über das Internet werden zwar Güter ausgetauscht, technisch gesehen handelt es sich jedoch lediglich um Informationen, die übertragen werden, da kein körperlicher Gegenstand die Staatsgrenzen überschreitet. Ein Anbieter von Informationen – z.B. ein Filehoster oder ein Teilnehmer in einem Peer-to-Peer-Netzwerk – sendet die Daten, aus denen das urheberrechtlich geschützte Werkstück besteht, auf Anfrage als elektromagnetische Signale zum Nutzer. Diese Signale kann man nicht anfassen, es wird lediglich die in ihnen enthaltene Information übertragen.

Zwar gibt es zweifellos im Einzelfall Wege, die übermittelte Information zu nutzen, um ihr beim Empfänger eine materielle Verkörperung zu geben, also mit ihrer Hilfe ein Werkstück herzustellen. Die Möglichkeiten reichen dabei von einer dauerhaften Speicherung der Daten auf einer Festplatte oder einem optischen Datenträger bis zum Druck eines urheberrechtlich geschützten Gegenstands mittels eines 3D-Druckers. Dies ändert allerdings nichts an der Tatsache, dass die Daten auf dem Transportweg und damit auch bei der Überquerung einer mitgliedstaatlichen Grenze im Binnenmarkt keine körperliche Gestalt besitzen.[465]

2. Dienstleistungsfreiheit

Infrage kommt allerdings eine unzulässige Beschränkung der Dienstleistungsfreiheit. Die Dienstleistungsfreiheit ist in den Art. 56 ff. AEUV geregelt. Sie schützt die wirtschaftliche Betätigung im Binnenmarkt durch die Gewährleistung des grenzüberschreitenden Ange-

---

[464] EuGH, Urt. v. 10.12.1968, Rs. C-7/68, Slg. 1968, S. 634 (642 f.); EuGH, Urt. v. 09.07.1992, C-2/90, Slg. 1992, I-04431, Rn. 26; EuGH, Urt. v. 28.04.1998, C-120/95, Slg. 1998, I-01831, Rn. 24; *Haratsch u.a.*, Europarecht, Kap. 3 IV 6 b) (Rn. 880); *Nettesheim* in: Oppermann u.a., Europarecht, § 22 II 1 (Rn. 18).

[465] Diese Art der Abgrenzung anhand der Körperlichkeit des wirtschaftlichen Guts wird zukünftig schwierig beizubehalten sein. Die Digitalisierung sorgt zunehmend dafür, dass die Produktion nahe beim Nachfrager erfolgen wird, die Wertschöpfung jedoch an einem anderen Ort geschieht. „Waren" werden dennoch Grenzen innerhalb des Binnenmarkts passieren, nur eben nicht auf der Straße, sondern über Glasfaserleitungen. Während die ökonomischen Unterschiede zwischen dem Anbieten einer Dienstleistung und dem Handel in gewissem Rahmen bestehen bleiben werden, wird das in der analogen Welt geeignete Abgrenzungsmerkmal der Körperlichkeit im digitalen Geschäftsverkehr mehr und mehr an Bedeutung verlieren. Eine eingehende Behandlung dieser sehr interessanten Problematik kann aus inhaltlichen Gründen an dieser Stelle jedoch nicht erfolgen.

bots von Dienstleistungen. Art. 57 AEUV definiert eine Dienstleistung u.a. als eine entgeltliche gewerbliche Tätigkeit, die weder den freien Waren- noch den freien Kapital- oder Personenverkehr betrifft. Sie ist im Wesentlichen die Entsprechung der Warenverkehrsfreiheit hinsichtlich unkörperlicher Produkte.[466] Dabei wird nicht nur die Freiheit des Dienstleistungserbringers geschützt, diese in einem anderen Mitgliedstaat zu erbringen,[467] sondern auch die Freiheit, eine Dienstleistung zu empfangen[468] sowie die Freiheit, sogenannte Korrespondenzdienstleistungen zu erbringen, bei denen lediglich die Dienstleistung eine Binnenmarktgrenze überquert, nicht aber der Empfänger oder der Erbringer.[469] Die Dienstleistungsfreiheit ist folglich zugleich Personen- wie Produktfreiheit.[470] Damit die Dienstleistungsfreiheit einschlägig ist, muss die Dienstleistung in dem Mitgliedstaat, in dem der Dienstleistungserbringer ansässig ist, legal in ähnlicher Weise erbracht werden.[471]

Bei der Datenverkehrsregulierung zur Durchsetzung des Urheberrechts wird die gewerbliche Tätigkeit bestimmter Content Provider mit einem bestimmten Geschäftsmodell beschränkt. Beschränkungen der Dienstleistungsfreiheit sind alle Maßnahmen, die die Ausübung der Freiheit durch deren Träger „*unterbinden, behindern oder weniger attraktiv machen*".[472] Beschränkt wird die Dienstleistungsfreiheit durch Eingriffe in den Datenverkehr in erster Linie in für Korrespondenzdienstleistungen.[473] Korrespondenzdienstleistungen umfassen auch solche Dienstleistungen, die auf elektronischem Wege erbracht werden.[474]

Wird in den Internet-Datenverkehr eingegriffen, um Urheberrechtsverletzungen zu verhindern, sind oft auch gewerbliche Anbieter betroffen. Potentiell Betroffene sind Betreiber von Internet-Angeboten, deren Dienstleistung die Speicherung und das Bereitstellen von

---

[466] *Kluth* in: Calliess/Ruffert, EUV/AEUV, Art. 57 AEUV Rn. 1
[467] *Kluth* in: Calliess/Ruffert, EUV/AEUV, Art. 57 AEUV Rn. 5.
[468] EuGH, Urt. v. 31.01.1984, Rs. C-286/82, C-26/83, Slg. 1984, S. 377 (401), Rn. 10: Der EuGH bezeichnet diese Freiheit als „*notwendige Ergänzung*" zur Freiheit des Dienstleistungserbringers.
[469] EuGH, Urt. v. 24.10.1978, Rs. C-15/78, Koestler, Slg. 1978, S. 1971 (1979), Rn. 3.
[470] *Kluth* in: Calliess/Ruffert, EUV/AEUV Art. 57 AEUV Rn. 32 m.w.N.; *Randelzhofer/Forsthoff* in: Grabitz u.a., Recht der Europäischen Union, Art. 56/57 AEUV Rn. 77 (Stand: 43. Erg.-Lfg., März 2011).
[471] EuGH, Urt. v. 08.09.2009, Rs. C-42/07, Slg. 2009, I-07633, Rn. 51; EuGH, Urt. v. 04.10.2011, Rs. C-403/08 und C-429/08, C-403/08, C-429/08, Murphy, Slg. 2011, I-09083, Rn. 85.
[472] EuGH, Urt. v. 25.07.1991, Rs. C-76/90, Säger, Slg. 1991, I-04221, Rn. 12; EuGH, Urt. v. 09.08.1994, Rs. C-43/93, Slg. 1994, I-03803, Rn. 14; EuGH, Urt. v. 28.03.1996, Rs. C-272/94, Slg. 1996, I-01905, Rn. 10; EuGH, Urt. v. 18.06.1998, Rs. C-266/96, Corsica Ferries France, Slg. 1998, I-03949, Rn. 56; EuGH, Urt. v. 23.11.1999, Rs. C-369/96, C-376/96, Arblade, Slg. 1999, I-08453 Rn. 33; EuGH, Urt. v. 20.02.2001, Rs. C-205/99, Slg. 2001, I-01271, Rn. 21; EuGH, Urt. v. 15.01.2002, Rs. C-439/99, Slg. 2002, I-00305, Rn. 22.
[473] Für einen umfassenden Überblick über alle Konstellationen, in denen die Dienstleistungsfreiheit bei der Datenverkehrsregulierung beschränkt wird, siehe *Schilling*, Präventive staatliche Kontrollmaßnahmen im Internet und ihre Vereinbarkeit mit dem Europarecht, S. 126 ff.
[474] EuGH, Urt. v. 30.04.1974, Rs. C-155/73, Sacchi, Slg. 1974, S. 409 (428), Rn. 6; EuGH, Urt. v. 04.10.2011, Rs. C-403/08 und C-429/08, C-403/08, C-429/08, Murphy, Slg. 2011, I-09083, Rn. 85 ff. *Kluth* in: Calliess/Ruffert, EUV/AEUV, Art. 57 AEUV Rn. 33; *Randelzhofer/Forsthoff* in: Grabitz u.a., Recht der Europäischen Union, Art. 56/57 AEUV Rn. 54 (Stand: 43. Erg.-Lfg., März 2011).

Dateien zum Abruf über das Internet umfasst. Werden sie zum Gegenstand von Netzsperren, wird ihnen die Durchführung dieser Dienstleistungen erheblich erschwert.

Der konkrete Anwendungsfall wären hier beispielsweise Filehoster und Streaming-Seiten, deren Geschäftsmodell in der Übertragung von Daten (auch zwischen Mitgliedstaaten) zu ihren Kunden liegt. Wird in einem Mitgliedstaat ein Filtersystem eingerichtet, das diesen Datenverkehr blockt, um Urheberrechtsverletzungen, die von dieser Seite ausgehen, zu unterbinden, werden dabei grenzüberschreitende Dienstleistungen beschränkt. Online-Dienstleistungen sind technisch nicht an nationale Grenzen gebunden, sondern können grundsätzlich von jedem Staat aus unabhängig vom Standort des Servers oder der Niederlassung des Content Providers aus abgerufen werde. Auf diese Weise entsteht Datenverkehr, der vor mitgliedstaatlichen Grenzen nicht Halt macht.

Die fraglichen Angebote der Content Provider sind auch nicht zwangsläufig in dem Mitgliedstaat illegal, in dem der Dienstleistungsempfänger ansässig ist, nur weil diese Dienstleistung in einem anderen Mitgliedstaat, der dieses Online-Angebot blockieren möchte, nicht erlaubt ist. In den einzelnen Mitgliedstaaten bestehen unterschiedliche Urheberrechtsregimes, auch wenn sie europarechtlich teilharmonisiert sind. Es existieren beispielsweise je nach Mitgliedstaat unterschiedliche Schranken des Urheberrechts. Ein weiterer Punkt ist, dass Verwertungsrechte in der Regel für nationale Märkte vergeben werden und dort unterschiedlichen Inhalts sein können. So ist es denkbar, dass ein Werk in einem Land frei zwischen den Nutzern geteilt werden darf, in einem anderen hingegen nicht. Der Filehoster Megaupload wurde im Januar 2012 vom Justizministerium der Vereinigten Staaten wegen nach dort vertretener Ansicht krimineller Aktivitäten (inklusive Verstoßes gegen das Urheberrecht) geschlossen.[475] Der Filehoster Rapidshare, dem ein vergleichbares Geschäftsmodell wie Megaupload zugrunde lag, wurde vom BGH hingegen nicht verboten. Dass Rapidshare dennoch schließen musste, lag nicht an illegalen Aktivitäten, vielmehr stellte der Filehoster seine Dienstleistungen später aus wirtschaftlichen Gründen ein.[476]

Zudem ist die Legalität des Geschäftsmodells eines Internet-Angebots selbst in dem Land, in dem der Anbieter seine Niederlassung hat, oft umstritten, so dass dieser Sachverhalt auch auf nationaler Ebene rechtlich unterschiedlich bewertet wird. Die Illegalität des Ge-

---

[475] *Fowler u.a.*, U.S. Shuts Offshore File-Share „Locker", in: Wall Street Journal online, 2012, abrufbar unter https://www.wsj.com/articles/SB10001424052970204616504577171060611948408 (zuletzt besucht am 09.10.2021).

[476] SPIEGEL ONLINE Redaktion, Rapidshare macht dicht, in: SPIEGEL ONLINE, 10.02.2015, abrufbar unter https://www.spiegel.de/netzwelt/web/rapidshare-filehoster-stellt-den-betrieb-ein-a-1017771.html (zuletzt besucht am 09.10.2021).

schäftsmodells von Rapidshare war innerhalb der deutschen Justiz zwischenzeitlich umstritten. Eine Täterschaft oder Teilnahme an Urheberrechtsverstößen hat der BGH im Ergebnis allerdings wiederholt verneint.[477]

Die rechtliche Beurteilung eines Dienstes wie einem Filehoster in den Mitgliedstaaten der EU kann also durchaus unterschiedlich gesehen werden. Dies ist auch dem EuGH bewusst, so dass er in der Scarlet-Entscheidung auf diesen Aspekt hinweist.[478]

Nicht alle Beschränkungen der Dienstleistungsfreiheit sind allerdings per se verboten. Sie können unter bestimmten Umständen gerechtfertigt sein. Neben den geschriebenen (und hier nicht weiter relevanten) Rechtfertigungsgründen der Art. 52 und 106 Abs. 2 AEUV hat der EuGH in ständiger Rechtsprechung ungeschriebene Rechtfertigungsgründe herausgearbeitet.[479]

Die erste Voraussetzung zur Rechtfertigung ist, dass die Beschränkungen nicht anhand der Staatsangehörigkeit diskriminieren. Dies ist ein absolutes Verbot, das so uneingeschränkt zumindest für offene Diskriminierungen gilt.[480] Eine offene oder versteckte Diskriminierung aufgrund der Staatszugehörigkeit der Content Provider stellt bei Eingriffen in den Datenverkehr zur Durchsetzung des Urheberrechts allerdings in der Regel kein Problem dar, so dass diese Voraussetzung erfüllt sein sollte.

Vielmehr handelt es sich bei der DVR um eine Regelung, die zwar nicht diskriminierend ist, aber dennoch die Freiheit beschränkt, eine gewisse Dienstleistung im gesamten Binnenmarkt anbieten zu können. Solche Beschränkungen dürfen nur zur Erreichung bestimmter qualifizierter Ziele auferlegt werden. Bei diesen Zielen muss es sich um zwingende Gründe des Allgemeininteresses handeln.

Die hier diskutierten Maßnahmen der Datenverkehrsregulierung erfolgen zum Schutz des Urheberrechts. Bei diesem ist seit der Coditel-Entscheidung des EuGH in ständiger

---

[477] So zur Eigenschaft des Filehosters Rapidshare als Täter oder Teilnehmer einer Urheberrechtsverletzung: OLG Köln, Urt. v. 21.09.2007, 6 U 86/07, Rn. 9 ff. (juris); OLG Düsseldorf, Urt. v. 21.12.2010, I-20 U 59/10, 20 U 59/10, Rn. 13 (juris); bestätigend BGH, Urt. v. 12.07.2012, I ZR 18/11, Alone in the Dark, BGHZ 194, 339, Rn. 15 ff. und BGH, Urt. v. 15.08.2013, I ZR 80/12, Filehosting-Dienst, NJW 2013, 3245, (3247); offenlassend OLG Hamburg, v. 02.07.2008, 5 U 73/07, Rn. 83 (juris).

[478] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 52.

[479] EuGH, Urt. v. 31.03.1993, Rs. C-19/92, Slg. 1993, I-01663 Rn. 32; EuGH, Urt. v. 30.11.1995, Rs. C-55/94, Slg. 1995, I-04165, Rn. 37; EuGH, Urt. v. 28.03.1996, Rs. C-272/94, Slg. 1996, I-01905, Rn. 11; vgl. *Kluth* in: Calliess/Ruffert, EUV/AEUV, Art. 57, Fn. 243 f. m.w.N.

[480] Vgl. dazu: EuGH, Urt. v. 03.10.2002, Rs. C-136/00, Danner, Slg. 2002, I-08147, Rn. 56. In der Rechtswissenschaft ist umstritten, ob nur offene Diskriminierungen einem absoluten Verbot unterliegen oder auch indirekte, versteckte Behinderungen. In diese Richtung etwa *Kingreen*, Die Struktur der Grundfreiheiten des Europäischen Gemeinschaftsrechts, S. 63; *Kluth* in: Calliess/Ruffert, EUV/AEUV, Art. 57 AEUV Rn. 56; a.A. *Nowak/Schnitzler*, EuZW 2000, 627 (627 ff.). Da bei der Datenverkehrsregulierung zur Durchsetzung des Urheberrechts weder die eine noch die andere Form der Diskriminierung im Raum steht, braucht es zu dem Problem an dieser Stelle keine Stellungnahme.

Rechtsprechung anerkannt, dass es sich um einen gewichtigen Grund des Allgemeininteresses handelt, der Einschränkungen der Grundfreiheiten grundsätzlich rechtfertigen kann.[481] Dies ist im Übrigen vor dem Hintergrund konsequent, dass zwingende Gründe des Allgemeininteresses auch in der Gewährleistung von Grundrechten liegen können.[482] Der auf Unionsebene grundrechtlich verbürgte Schutz des Urheberrechts wird dabei noch einmal durch Art. 17 Abs. 2 Charta eindeutig klargestellt.[483]

Weiterhin müssen die Beschränkungen geeignet sein, die Erreichung dieser Ziele zu fördern.[484] Dass Maßnahmen der Datenverkehrsregulierung grundsätzlich geeignet sind, Verletzungen des Urheberrechts wenigstens in Teilen zu erschweren, daran bestehen hier kaum Zweifel, auch wenn der Grad der Effektivität im Hinblick auf dieses Ziel je nach Art der ergriffenen Maßnahme schwanken mag.[485]

Die Eingriffe müssen schließlich auch im europarechtlichen Sinne verhältnismäßig sein. Unter dem Gebot der Verhältnismäßigkeit versteht der EuGH das Verbot, Maßnahmen zu ergreifen, welche die Freiheiten stärker einschränken, als dies zur Erreichung des Zieles erforderlich ist. Ob eine Datenverkehrsregulierung zur Urheberrechtsdurchsetzung diese Voraussetzung einer zulässigen Beschränkung der Dienstleistungsfreiheit erfüllen würde, ist allerdings mit Zweifeln versehen. Dies könnte auch davon abhängen, in welcher Form die konkrete Maßnahme der DVR angewandt würde.

Damit sie verhältnismäßig sein kann, dürfte eine Datenverkehrsregulierung den Austausch von Daten zwischen den Mitgliedstaaten nicht stärker einschränken, als dies zur Durchsetzung des Urheberrechts notwendig ist. Damit wird deutlich, dass sich die Aussagen des EuGH in der UPC-Entscheidung zum Overblocking im Kontext der Meinungs- und Informationsfreiheit des Art. 11 Charta auch auf die Verhältnismäßigkeitsprüfung im Rahmen der Dienstleistungsfreiheit übertragen lassen. In jenem Urteil stellte der EuGH fest, dass eine Maßnahme der DVR den Internet-Nutzern nicht unnötig den Zugriff auf verfügbare Informationen vorenthalten dürfe.[486] Wann eine DVR eigentlich zulässigen Datenverkehr in unnötiger Weise blockt, dürfte in beiden Prüfungen identisch zu beurteilen sein, da eine unterschiedliche Auslegung – etwa durch eine unterschiedliche Schutzrichtung der primärrechtlichen Gewährleistungen – hier keine ersichtliche Grundlage hat. Wie schon bei der Prüfung der zulässigen Beschränkung der Informationsfreiheit ge-

---

[481] EuGH, Urt. v. 18.03.1980, Rs. C-62/79, Coditel, Slg. 1980, S. 881 (903 f.), Rn. 16; EuGH, Urt. v. 20.01.1981, Rs. C-55/80, C-57/80, Gebührendifferenz II, Slg. 1981, S. 147 (161), Rn. 9; EuGH, Urt. v. 04.10.2011, Rs. C-403/08 und C-429/08, C-403/08, C-429/08, Murphy, Slg. 2011, I-09083, Rn. 94.
[482] EuGH, Urt. v. 14.10.2004, Rs. C-36/02, Gespieltes Töten, Slg. 2004, I-09609, Rn. 35.
[483] Zur Bedeutung der in der Charta verbrieften Grundrechte für die mögliche Beschränkung von Grundfreiheiten vgl. *Tiedje* in: Groeben u.a., Europäisches Unionsrecht Bd. 1, Rn. 82., Art. 56 AEUV,
[484] Vgl. EuGH, Urt. v. 25.07.1991, Rs. C-76/90, Säger, Slg. 1991, I-04221, Rn. 15; EuGH, Urt. v. 31.03.1993, Rs. C-19/92, Slg. 1993, I-01663, Rn. 32; EuGH, Urt. v. 23.11.1999, Rs. C-369/96, C-376/96, Arblade, Slg. 1999, I-08453, Rn. 35.
[485] Vgl. dazu oben S. ff.
[486] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 63.

mäß Art. 11 Charta dürften die IP-Sperren auch bei der Rechtfertigung einer Beschränkung der Dienstleistungsfreiheit den vergleichsweise schwersten Stand aller Formen der DVR haben, da sie das größte Potential für Overblocking bieten.

Die Verhältnismäßigkeit der Beschränkung der Dienstleistungsfreiheit durch eine DVR zur Durchsetzung des Urheberrechts hängt folglich davon ab, ob sie in hohem Maße dazu fähig ist, Overblocking zu vermeiden. Dieses Ergebnis hat zur Konsequenz, dass eine solche Datenverkehrsregulierung nur dann die Dienstleistungsfreiheit unrechtmäßig beschränkt, wenn sie zugleich die Informationsfreiheit der Internet-Nutzer verletzt.

VI. Ergebnis

Keine technische Methode zum Eingriff in den Internet-Datenverkehr zur Urheberrechtsdurchsetzung ist nach der Rechtsprechung des EuGH derzeit eindeutig mit EU-Recht vereinbar. Die Unvereinbarkeiten betreffen sowohl die europäischen Grundrechte als auch die Dienstleistungsfreiheit. Insbesondere ist eine umfassende Form der DVR mittels Deep Packet Inspection vom EuGH ausdrücklich mit der unternehmerischen Freiheit gemäß Art. 16 Charta für unvereinbar erklärt worden.

Diese Aussage ist nach der oben erfolgten Analyse der Rechtsprechung allerdings nicht zwangsläufig auf jedes Filtersystem übertragbar, das DPI einsetzt. Offen lässt der EuGH weiterhin sowohl, ob eine DVR andere Grundrechte verletzt, als auch, ob andere konkrete Formen der DVR zur Durchsetzung des Urheberrechts europarechtskonform sind. Im Übrigen stellt der EuGH abstrakt fest, dass eine beliebige DVR nicht bereits deshalb rechtswidrig wäre, wenn sie nicht zu 100 Prozent effektiv bei der Durchsetzung des Urheberrechts wäre, und postuliert Anforderungen, die eine hypothetische DVR erfüllen müsste, um mit europäischen Grundrechten, insbesondere Art. 11 Charta, vereinbar zu sein.[487]

Durch diese Feststellungen zur Informationsfreiheit stellt der Gerichtshof zudem einen Gleichlauf in der Bewertung der Zulässigkeit der mit der DVR einhergehenden Beschränkung der Dienstleistungsfreiheit her, auch wenn er diese Konsequenz nicht ausdrücklich anspricht.[488]

---

[487] Vgl. oben Kap. 2 V 4 (S. 117 f.)

[488] Vgl. soeben Kap. 2 VI 2 (S. 126). Durch den so hergestellten Gleichlauf ist im Rahmen einer gerichtlichen Entscheidung ist eine gesonderte Prüfung der rechtmäßigen Beschränkung der Grundfreiheiten neben derjenigen des Art. 11 Charta im Ergebnis nicht notwendig, da sie zu keinem eigenständigen, abweichenden Ergebnis führen würde.

Kapitel 3 – Vereinbarkeit der DVR mit nationalem Verfassungsrecht

Grenzen werden einer Datenverkehrsregulierung nicht nur durch europäisches Recht gesetzt. Derartige Eingriffe in den Datenverkehr müssen sich grundsätzlich auch an nationalem Verfassungsrecht messen lassen. Bezogen auf die Rechtslage in Deutschland sind hier zum einen die Grundrechte des Grundgesetzes releavant.

Die einschlägigen Grundrechte schützen die jeweiligen Grundrechtsberechtigten dabei vor drei grob abgrenzbaren Gefahrenkomplexen.

Der erste Komplex betriff die wirtschaftlichen Interessen der privaten Betreiber von Internet-Zugangsdiensten (die Internet Service Provider). Diese möchten grundsätzlich nicht als „Hilfspolizisten" des Staates in Anspruch genommen werden. Insoweit könnten sie durch die in Art. 12 Abs. 1 GG verbriefte Berufsfreiheit geschützt sein.[489]

Der zweite Komplex ist der des freien Informationsflusses, der die Endnutzer des Internets betrifft. Die Möglichkeit, sich frei zu informieren, wird durch Art. 5 Abs. 1 Satz 1 Alt. 2 GG geschützt.[490]

Der dritte Komplex betrifft den Schutz der Persönlichkeit. Dieser wird durch eine Vielzahl an geschriebenen und ungeschriebenen Grundrechten des Grundgesetzes garantiert. Die für Eingriffe in den Datenverkehr zur Durchsetzung des Urheberrechts relevanten Grundrechte sind dabei das Telekommunikationsgeheimnis, Art. 10 Abs. 1 GG, und das Allgemeinen Persönlichkeitsrecht gemäß Art. 2 Abs. 1, 1 Abs. 1 GG in seiner Ausformung als Recht auf informationelle Selbstbestimmung.[491]

Zum anderen müssen datenverkehrsregulierende Maßnahmen auch die rechtsstaatlichen Prinzipien des Grundgesetzes beachten (insbesondere den Vorbehalt des Gesetzes sowie das Zitiergebot).[492]

I. Anwendbarkeit des Grundgesetzes im Geltungsbereich des EU-Rechts

Es ist nicht selbstverständlich, dass sich datenverkehrsregulierende Maßnahmen auch einer Prüfung anhand des Grundgesetzes stellen müssen. Diese bewegen sich nämlich im

---

[489] Das entsprechende Grundrecht der Charta ist die unternehmerische Freiheit des Art. 16 Charta. Zu dessen Beschränkungen bezüglich einer Datenverkehrsregulierung zur Durchsetzung des Urheberrechts siehe oben Kap. 2 V 1 a) (S. 73) und Kap. 2 V 2 a) (S. 90 ff.).

[490] Auch in der Charta wird dieser Bereich geschützt, namentlich durch Art. 11 Charta. Vgl. oben Kap. 2 V 1 c) (S. 82) und Kap. 2 V 2 b) (S. 92) zu den Beschränkungen, die die europarechtlich garantierte Meinungs- und Informationsfreiheit einer DVR zur Urheberrechtsdurchsetzung auferlegt.

[491] In der Charta ist das dem Recht auf informationelle Selbstbestimmung korrespondierende Grundrecht Art. 8 Charta (Recht auf den Schutz personenbezogener Daten) und für die Telekommunikationsfreiheit sowie den Schutz der Privatsphäre Art. 7 Charta (Recht auf Privatleben).

[492] Vgl. BGH, Urt. v. 26.11.2015, I ZR 3/14, 3dl.am, Rn. 32 f. (juris); BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 33 f.

Geltungsbereich des EU-Rechts. Grundsätzlich geht das Europarecht in seinem Anwendungsbereich dem Recht der Mitgliedstaaten vor. Daher wird europäisches Recht nicht an mitgliedstaatlichen Grundrechten gemessen, solange auf europäischer Ebene ein ausreichender Grundrechtsschutz garantiert wird.[493] Wird ein ISP zu einer Maßnahme der Datenverkehrsregulierung zur Durchsetzung des Urheberrechts verpflichtet, handelt es sich dabei um eine Maßnahme in einem europarechtlich geregelten Bereich.[494]

Bei den sekundärrechtlichen Vorgaben zur Inanspruchnahme von Providern zur Urheberrechtsdurchsetzung handelt es sich um Vorschriften aus den Richtlinien 2000/31/EG, 2001/29/EG und 2004/48/EG. Richtlinienvorschriften sind allerdings nur teilweise verbindlich. Zwar sind die Mitgliedstaaten verpflichtet, die mit einer Richtlinie verfolgten verbindlichen Ziele durch innerstaatliche Rechtsetzung umzusetzen.[495] Art. 288 Abs. 3 AEUV erlaubt den Mitgliedstaaten dabei jedoch ausdrücklich, die Form und Mittel selbst zu wählen. Das hier einschlägige Sekundärrecht lässt den Mitgliedstaaten darüber hinaus weiteren Spielraum. So schreibt etwa Art. 8 Abs. 3 der InfoSoc-Richtlinie vor, dass Rechtsinhaber gerichtliche Anordnungen gegenüber ISP zur Urheberrechtsdurchsetzung erwirken können müssen. Gemäß Erwägungsgrund 59 derselben Richtlinie sind Bedingungen und Modalitäten solcher Anordnungen jedoch der Regelung durch die Mitgliedstaaten vorbehalten.

Die Mitgliedstaaten besitzen folglich einen beträchtlichen Spielraum bei der Umsetzung einer Datenverkehrsregulierung zur Durchsetzung des Urheberrechts. Sie können sich zwar nicht über den oben herausgearbeiteten primärrechtlichen Rahmen hinwegsetzen, den die Grundrechte der Charta, die Grundfreiheiten, die zugehörige Auslegung des EuGH und letztlich auch das Sekundärrecht vorschreiben.[496] Der durch die Richtlinien offen gelassene weite Spielraum bei der konkreten Ausgestaltung einer DVR und die Zurückhaltung des Europäischen Gerichtshofs bei der Ziehung konkreter Grenzen der Datenverkehrsregulierung lassen den Mitgliedstaaten jedoch Freiheiten.[497]

Die Ausnutzung dieser Umsetzungsspielräume des Mitgliedstaats muss sich, jedenfalls in Deutschland, an nationalem Verfassungsrecht messen lassen, jedenfalls solange das Schutzniveau nicht hinter das der Charta zurückfällt.[498] Der Anwendungsvorrang des Europarechts steht dem nicht entgegen. Gemäß Art. 53 Charta ist keine Bestimmung der

---

[493] Zur sogenannten „Solange-Rechtsprechung" des Bundesverfassungsgerichts s. BVerfG, Urt. v. 29.05.1974, 2 BvL 52/71, Solange 1, BVerfGE 37, 271 und BVerfG, Urt. v. 22.10.1986, 2 BvR 197/83, Solange II, BVerfGE 73, 339; vgl. auch oben Kap. 2 I 4 a) (2) (S. 51 ff.).
[494] Vgl. oben Kap. 2 III (S.56 ff.)
[495] *Schroeder* in: Streinz, EUV/AEUV, Art. 288 Rn. 63.
[496] Vgl. oben Kap. 2 I 4 a) (2) (S. 50).
[497] So auch *Nazari-Khanachayi*, GRUR 2015, 115 (119 ff.).
[498] BVerfG, Beschl. v. 13.03.2007, 1 BvF 1/05, Emissionshandel, BVerfGE 118, 79 (96); bekräftigt durch BVerfG, Beschl. v. 06.11.2019, 1 BvR 16/13, Recht auf Vergessen I, BVerfGE 152, 152 (juris-Rn. 42 f.).. Im Übrigen muss sich der Mitgliedsstaat bei der Umsetzung auch nach den Grundrechten der Charta richten, da es sich bei Anordnungen gegenüber ISP zur Urheberrechtsdurchsetzung

Charta als eine Einschränkung oder Verletzung der Menschenrechte und Grundfreiheiten auszulegen, die in dem jeweiligen Anwendungsbereich durch das Recht der Union sowie durch die Verfassungen der Mitgliedstaaten anerkannt werden.

II. Das Grundrecht der Internet Service Provider auf freie Berufsausübung gemäß Art. 12 Abs. 1 GG

Zunächst stellt sich die Frage nach der Vereinbarkeit der DVR mit der Berufsfreiheit. Da eine Datenverkehrsregulierung, in welcher Form sie auch auftreten mag, beim ISP erfolgt und durch diesen umgesetzt werden muss, was zum einen Arbeits-, Betriebs- und Materialaufwand für diesen beinhaltet, zum anderen auch die Beziehungen zu seinen Kunden beeinflussen kann, könnte die Berufsfreiheit der verpflichteten Internet Service Provider verletzt sein.

1. Schutzbereich der Berufsfreiheit

Art. 12 Abs. 1 GG schützt die Freiheit des Bürgers, jeden Beruf zu ergreifen und auszuüben, für den er sich geeignet hält.[499] Im Zusammenhang mit der Frage, ob eine Datenverkehrsregulierung im Urheberrecht den Schutzbereich der Berufsfreiheit berührt und ob ein Internet Service Provider sich auf dieses Grundrecht in diesen Fällen überhaupt berufen kann, stellen sich einige Probleme.

a. Sachlicher Schutzbereich

Fraglich ist zunächst, ob Eingriffe in den Datenverkehr den sachlichen Schutzbereich der Berufsfreiheit berühren. Dazu muss die inhaltliche Reichweite des Art. 12. Abs. 1 GG bestimmt werden. Dieser hält fest, dass *„[a]lle Deutschen [...] das Recht [haben], Beruf, Arbeitsplatz und Ausbildungsstätte frei zu wählen. Die Berufsausübung kann durch Gesetz oder auf Grund eines Gesetzes geregelt werden“*. Der Begriff des Berufs ist hier also für die inhaltliche Reichweite zentral.

Der Begriff des Berufs ist weit auszulegen.[500] Ein Beruf i.S.v. Art. 12 Abs. 1 ist jede auf Dauer angelegte und nicht bloß vorübergehende, der Schaffung und Erhaltung einer Lebensgrundlage dienende erlaubte Betätigung, unabhängig von verfestigten Berufsbildern.[501] Sachlich geschützt ist gemäß Art. 12 Abs. 1 Satz 1 GG die Berufswahl, gemäß Satz 2 die Berufsausübung. Bei der Berufsfreiheit handelt es sich – auch wenn der

---

letztlich um eine Umsetzung sekundärrechtlicher Vorschriften handelt. Vgl. EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 44; konkret auch zur DVR zur Urheberrechtsdurchsetzung: BGH, Urt. v. 26.11.2015, I ZR 3/14, 3dl.am, Rn. 30 (juris); BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 31.

[499] BVerfG, Urt. v. 11.06.1958, Apotheker-Urteil, BVerfGE 7, 377 (397); BVerfG, Urt. v. 01.03.1979, 1 BvR 532/77, 1 BvR 533/77, 1 BvR 419/78, 1 BvL 21/78, Mitbestimmungsurteil, BVerfGE 50, 290 (362).

[500] *Scholz* in: Maunz/Dürig, Art. 12 GG Rn. 267 (Stand: 47. Erg.-Lfg., Juni 2006).

[501] Ständige Rechtsprechung des Bundesverfassungsgerichts, vgl. etwa BVerfG, Urt. v. 07.01.1959, 1 BvR 100/57, Arzneifertigware, BVerfGE 9, 73 (77 f.); BVerfG, Beschl. v. 17.07.1961, 1 BvL 44/55,

Wortlaut zunächst etwas anderes nahelegt – dennoch um ein einheitliches Grundrecht, da die Berufsausübung lediglich die wiederholte Aufnahme der beruflichen Betätigung ist.[502] Ob eine Maßnahme den Schutzbereich der Berufsausübungsfreiheit oder der Berufswahlfreiheit betrifft, wird lediglich auf der Ebene der Rechtfertigung des Eingriffs bedeutsam.[503]

Die von der Berufsfreiheit umfasste Freiheit der Berufsausübung schützt auch die Art und Weise der unternehmerischen Tätigkeit, inklusive die *„Freiheit eines Unternehmers, über seine wirtschaftlichen, technischen und finanziellen Ressourcen zu verfügen"*.[504] Ein Internet Service Provider bietet Dritten dauerhaft und gegen Bezahlung Zugang zum Internet an (*Access Provider*) bzw. vermittelt Datenübertragungen zwischen entfernten computerisierten Endgeräten (*Network Provider*). Diese gewerbliche Tätigkeit und die Art und Weise, wie die dem ISP zur Verfügung stehenden Ressourcen zu diesem Zweck verwendet werden, fällt folglich in den sachlichen Schutzbereich des Art. 12 Abs. 1 GG.[505]

Der sachliche Schutzbereich der Berufsfreiheit ist bei Eingriffen in den Datenverkehr zur Urheberrechtsdurchsetzung daher unzweifelhaft eröffnet.

b. Persönlicher Schutzbereich der Berufsfreiheit

Um in den Genuss des Schutzes von Art. 12 Abs. 1 GG zu kommen, müssten die Internet Service Provider auch in den persönlichen Schutzbereich der Berufsfreiheit fallen.

(1) Schutz der Berufsfreiheit für Unternehmen

Problematisch ist zunächst die grundsätzliche Befähigung von Internet Service Providern als Unternehmen, Träger des Grundrechts aus Art. 12 Abs. 1 GG zu sein. Internet Service Provider sind keine natürlichen, sondern juristische Personen. Auch auf juristische Personen sind die Grundrechte gemäß Art. 19 Abs. 3 GG jedoch anwendbar, soweit dies ihrem Wesen nach möglich ist. Juristische Personen können erwerbswirtschaftlichen Tätigkeiten, namentlich dem Betrieb eines Gewerbes, nachgehen, so dass Art. 12 Abs. 1 GG auch

---

Handwerksordnung, BVerfGE 13, 97 (104 f.); BVerfG, Urt. v. 21.02.1962, 1 BvR 198/57, Ladenschlussgesetz I, BVerfGE 14, 19 (22); BVerfG, Beschl. v. 18.06.1980, 1 BvR 697/77, Buchführungsprivileg, BVerfGE 54, 301 (312 f.); BVerfG, Urt. v. 17.02.1998, 1 BvF 1/91, Kurzberichterstattung im Fernsehen, BVerfGE 97, 228 (252 f.).

[502] *Kingreen/Poscher*, Grundrechte – Staatsrecht II, § 21 II 1 a) (Rn. 936).

[503] *Scholz* in: Maunz/Dürig, Art. 12 GG, Rn. 335 (Stand: 47. Erg.-Lfg., Juni 2006).

[504] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 47 ff.; BGH, Urt. v. 26.11.2015, I ZR 3/14, 3dl.am, Rn. 36 (juris); BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 37 mit ausdrücklichem Verweis auf den Schutzbereich des Art. 16 Charta. An dieser Stelle wird der Einfluss der Grundrechte der Charta und der Rechtsprechung des EuGH auf die Auslegung der Grundrechte des Grundgesetzes deutlich.

[505] BGH, Urt. v. 26.11.2015, I ZR 3/14, 3dl.am, Rn. 37 (juris); BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 36; OLG Hamburg, Urt. v. 21.11.2013, 5 U 68/10, 3dl.am, Rn. 100 (juris); OLG Köln, Urt. v. 18.07.2014, I-6 U 192/11, 6 U 192/11, Goldesel, Rn. 941 (juris).

auf Unternehmen Anwendung findet.[506] ISPs im Besonderen stellen Dritten den Zugang zum Internet gegen Entgelt zur Verfügung, so dass sie insoweit Träger der Berufsfreiheit sind.[507]

(2) Berufsfreiheit als Bürgergrundrecht

Weitgehend unproblematisch dürfte weiterhin sein, dass Art. 12 Abs. 1 GG ein Bürgerrecht ist, seinem Wortlaut nach also nur deutschen Staatsbürgern bzw. Unternehmen gemäß Art. 116 Abs. 1 GG Schutz gewährt. Zwar können ebenso ausländische ISPs in Deutschland tätig sein, und ausländische Unternehmen können sich grundsätzlich nicht auf Art. 12 GG berufen, sondern werden auf Art. 2 Abs. 1 GG verwiesen.[508] Bürger und Unternehmen aus dem EU-Ausland werden jedoch im Rahmen der Grundrechte unabhängig von der dogmatischen Herleitung dieser Ausnahme nach wohl herrschender Meinung gleich stark wie deutsche Staatsbürger bzw. Unternehmen geschützt.[509] Damit dürfte jedenfalls im Ergebnis der weit überwiegende Teil der auf dem europäischen Markt tätigen Internet Service Provider sich auf Art. 12 Abs. 1 GG berufen können.[510]

(3) Mögliche Beleihung von ISPs

Je nach Ausgestaltung des Verhältnisses zwischen Staat und Internet Service Provider bei der DVR kann das Staat – Bürger-Verhältnis in Frage stehen, das Voraussetzung für die Eröffnung des Schutzbereichs eines Grundrechts ist. So problematisiert *Heliosch*, dass bei einer Datenverkehrsregulierung der ISP gegebenenfalls selbst eine hoheitliche Aufgabe durchführt, wenn er als erweiterter Arm des Staates dessen Ziele durch Eingriffe in

---

[506] BVerfG, Beschl. v. 16.03.1971, 1 BvR 52/66, 1 BvR 665/66, 1 BvR 667/66, 1 BvR 754/66, Erdölbevorratung, BVerfGE 30, 292, Rn. 55; BVerfG, Urt. v. 01.03.1979, 1 BvR 532/77, 1 BvR 533/77, 1 BvR 419/78, 1 BvL 21/78, Mitbestimmungsurteil, BVerfGE 50, 290, Rn. 172; BverfG, Beschl. v. 26.06.2002, 1 BvR 558/91, 1 BvR 1428/91, Glykolwarnung, BVerfGE 105, 252, Rn. 41; *Ruffert* in: Epping/Hillgruber, BeckOK Grundgesetz, Art. 12 Rn. 38.

[507] BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 37.

[508] BVerfG, Beschl. v. 10.05.1988, 1 BvF 1/91, Heilpraktikergesetz, BVerfGE 78, 179, (196 f.); *Hufen*, Staatsrecht II, § 35 II 3 (Rn. 11); *Scholz* in: Maunz/Dürig, Art. 12 GG Rn. 104 (Stand: 47. Erg.-Lfg., Juni 2006).

[509] *Ehlers*, JZ 1996, 776 (778); *Ruffert* in: Epping/Hillgruber, BeckOK Grundgesetz, Art. 12 Rn. 37; *Breuer* in: Isensee/P. Kirchhof, HStR VIII, § 170 Rn. 43; *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 12 Rn. 12, 13a; *Kluth*, JURA 2001, 371 (371); a.A. *Lücke*, EuR 2001, 112 (117); *Scholz* in: Maunz/Dürig, Art. 12 GG Rn. 105 (Stand: 47. Erg.-Lfg., Juni 2006); *Kämmerer* in: v. Münch/Kunig, Grundgesetz Bd. 1, 7. Aufl. 2021, Art. 12 Rn. 21: Für eine Gleichbehandlung fehle es an einer rechtspolitischen Notwendigkeit, da Unionsbürger durch die Grundfreiheiten und Sekundärrecht ausreichend geschützt seien.

[510] Für die Frage europarechtlicher Schranken bei Zwangsmaßnahmen gegen Internet Service Provider vgl. ausführlich *Schilling*, Präventive staatliche Kontrollmaßnahmen im Internet und ihre Vereinbarkeit mit dem Europarecht, Teil 3 Kap. 2 , S. 125 ff.. Das Problem tritt in der Praxis allerdings schon deshalb nicht auf, weil ISPs, die auf dem deutschen Markt tätig werden wollen, schon aus anderen Gründen in der Regel eine deutsches oder zumindest europäisches Tochterunternehmen als Betreiber gründen.

den Datenverkehr umsetzt.[511] Es handelt sich dann um einen Fall der sogenannten *funktionalen Privatisierung*.[512]

In diesem Fall treten Fragen bezüglich der Fähigkeit eines solchermaßen verpflichteten Providers auf, sich gegenüber dem Staat auf seine Grundrechte, namentlich seine Berufsfreiheit, zu berufen. Dies ist je nach Sachverhalt unterschiedlich zu beurteilen, und hängt auch davon ab, ob es sich bei der Anordnung der Datenverkehrsregulierung an den Provider um eine Indienstnahme, eine Anordnung der Verwaltungshilfe oder um eine Beleihung handelt. Denn soweit der Provider den Status eines Beliehenen tragen sollte, ist er in das staatliche Gefüge eingebunden und kann sich nicht im gleichen Maße gegen den Staat zur Wehr setzen, wie er dies im einfachen Staat – Bürger-Verhältnis könnte. Innerorganisatorische Maßnahmen, die eine übergeordnete Behörde ihrer nachgeordneten Behörde aufträgt, unterfallen grundsätzlich nicht dem Schutz der Grundrechte. Beliehene sind den Grundrechten verpflichtet, aber nicht grundrechtsberechtigt. [513] Ausgenommen sind davon allerdings die Fälle, in denen der Beliehene in seiner Rechtsstellung als Privater betroffen ist.[514]

Diese Frage nach einer möglichen Beleihung tritt vor allen Dingen dann auf, wenn die verfahrenstechnischen Grundlagen der Anordnung einer DVR so ausgestaltet sind, dass der ISP von der staatlichen Verwaltung einen konkreten Sperrauftrag erhält.[515] Die Beleihung setzt voraus, dass Private Verwaltungsaufgaben erfüllen, und der Staat ihnen durch oder aufgrund eines Gesetzes die Befugnis erteilt hat, die Verwaltungsaufgaben selbstständig, in den Handlungsformen des öffentlichen Rechts und im eigenen Namen – notfalls durch Verwaltungszwang – wahrzunehmen.[516] Für seine Tätigkeit wird der Beliehene entschädigt, entweder durch Zuwendungen des Staates oder durch die Ermächtigung zur Gebühreneinziehung.

Verwaltungshelfer hingegen sind natürliche oder juristische Personen des Privatrechts, die nicht selbstständig, sondern für eine Behörde nach außen tätig werden, und dabei im Namen, im Auftrag oder auf Weisung der Behörde handeln, indem sie diese vorbereitend

---

[511] *Heliosch*, Sperrmaßnahmen im Internet, S. 72.
[512] Die funktionale Privatisierung ist ein Oberbegriff für alle Fälle, in denen Private in die Erfüllung öffentlich-rechtlicher Aufgaben eingebunden werden. Die Zuständigkeit und die Verantwortung verbleibt beim Staat, Planung, Vollzug oder Finanzierung der Aufgabe werden jedoch auf einen Privaten übertragen und von diesem durchgeführt. Vgl. *Gröpl* in: Maunz/Dürig, Art. 90 GG Rn. 67 ff. (Stand: 89. Erg.-Lfg., Oktober 2019) m.w.N.; *Maurer/Waldhoff*, Allgemeines Verwaltungsrecht, § 23 VI 2 b) (Rn. 64).
[513] *Ehlers/Schneider* in: Schoch *u.a.*, VwGO, § 40 VwGO, Rn. 276 (Stand: 28. Erg.-Lfg., März 2015).
[514] BVerfG, v. 20.02.1986, 1 BvR 859, 937/81; *Bormann/Böttcher*, NJW 2011, 2758 (2759); *Kaltenborn/Schnapp*, JuS 2000, 937 (938).
[515] Das Modell, die Provider über die Anordnungen einer spezialisierten Behörde zu verpflichten, wird in der Literatur teilweise für überlegen gegenüber gerichtlichen Anordnungen gehalten, vgl. *Assion*, K&R 2014, 329 (334). Dies war auch der Weg, den das Zugangserschwerungsgesetz für die Sperrung kinderpornographischer Online-Angebote gehen sollte (zuständige Behörde war das BKA).
[516] *Reimer* in: Posser/Wolff, VwGO, § 40 VwGO, Rn. 49; *Ehlers/Schneider* in: *Schoch u.a.*, VwGO, § 40 VwGO 275 (Stand: 28. Erg.-Lfg., März 2015).

oder rein ausführend bei einer weiterhin der Behörde zugewiesenen Aufgabe unterstützen.[517]

Die Indienstnahme wiederum bezeichnet die Verpflichtung einer Person des Privatrechts, gegen deren Willen im Rahmen einer grundrechtlich geschützten Freiheitsausübung gemeinwohlbezogene Pflichten auszufüllen, die nicht notwendiger Teil der grundrechtlich geschützten Freiheitsausübung sind. Diesen Pflichten muss der Indienstgenommene eigenverantwortlich, selbstständig und mit Mitteln des Privatrechts nachkommen.[518]

Um als Beliehener zu gelten, müsste ein Internet Service Provider im Anschluss an einen formellen staatlichen Beleihungsakt bei der Implementierung einer DVR also selbstständig und im eigenen Namen die Entscheidung über das Ob einer Implementierung treffen. Typisch für eine Beleihung wäre zudem, dass der Beliehene für seine Tätigkeit entlohnt wird und die Beleihung nicht gegen den Willen des Beliehenen erfolgt. Diesen Kriterien wird eine Datenverkehrsregulierung zur Urheberrechtsdurchsetzung in der Regel aus praktischen wie aus rechtlichen Gründen wohl nicht entsprechen.

Der ISP hat in der Regel kein Interesse daran, wie eine Behörde aufzutreten und den Datenverkehr zu regulieren. Das Kerngeschäft eines ISP ist es, Datenverkehr ohne Rücksicht auf den Inhalt weiterzuleiten, und nicht, für den Staat die Durchsetzung privater Rechte sicherzustellen. Ein Internet Service Provider wird eine Datenverkehrsregulierung zur Urheberrechtsdurchsetzung mitsamt den Belastungen, die ihm dadurch entstehen, daher kaum freiwillig übernehmen. Aus Sicht des Staates ist es ohnehin wenig attraktiv, die ISPs für eine Tätigkeit finanziell zu entschädigen, die der Staat womöglich durch eine andere rechtliche Gestaltung auch umsonst bekäme.

Entscheidend dürfte im Ergebnis sein, dass den ISPs die rechtliche Kompetenz und Legitimation fehlen, um selbstständig über das Ob einer Implementierung von Datenverkehrsregulierung im Einzelfall entscheiden zu können. Eine gegebenenfalls verbliebene Restkompetenz bei der Wahl der konkreten Maßnahme (also das Wie der technischen Umsetzung) fällt demgegenüber nicht so stark ins Gewicht, dass bei wertender Betrachtung diese Entscheidung als eine eigenverantwortliche öffentlich-rechtliche Handlung zu werten wäre.[519]

Ob es sich andererseits bei der Tätigkeit des ISP um eine Indienstnahme oder Verwaltungshilfe handelt, hängt von der konkreten institutionellen Ausgestaltung ab. Naheliegend wäre eine Ausgestaltung in der Form der Indienstnahme, da die Internet Service

---

[517] *Ehlers/Schneider* in: Schoch u.a., VwGO, § 40 Rn. 281 (Stand: 28. Erg.-Lfg., März 2015), dort mit umfassenden weiteren Nachweisen.
[518] *Ehlers/Schneider* in: Schoch u.a., VwGO, § 40 Rn. 290 (Stand: 28. Erg.-Lfg., März 2015).
[519] So auch mit ähnlichen Argumenten zu einer DVR nach Maßgabe des Zugangserschwerungsgesetzes *Heliosch*, Sperrmaßnahmen im Internet, S. 73 f. Vgl. allgemein auch *Koreng*, Zensur im Internet, S. 144.

Provider sich in der Regel nicht freiwillig in der Ausübung ihrer Berufsfreiheit beschränken lassen werden. Die Umsetzung einer Datenverkehrsregulierung durch die Provider ist auch nicht auf formelle öffentlich-rechtliche Handlungsformen angewiesen.

Letztlich ist die Antwort auf diese Frage nicht entscheidend. Sowohl als Verwaltungshelfer als auch als Indienstgenommener ist ein ISP im Verhältnis gegenüber dem Staat als Privater und damit als Grundrechtsträger anzusehen.[520] Und selbst ein Beliehener wäre in seinem Grundverhältnis zum Staat durch die Grundrechte geschützt (insoweit, wie es seine öffentlich-rechtliche Stellung betrifft).[521] Zumindest der Akt der Beleihung (nicht aber für konkrete Anordnungen einer DVR im Einzelfall) wäre daher an den Grundrechten zu messen.

Im Ergebnis kann ein ISP sich bei einer behördlichen Anordnung einer Datenverkehrsregulierung zur Durchsetzung des Urheberrechts daher unabhängig vom rechtlichen Status seiner Einbindung in die Verwaltung auf seine Grundrechte berufen. Dies gilt jedenfalls für die grundsätzliche Verpflichtung zur DVR auch dann, wenn er als Beliehener einzustufen wäre. Allerdings würde es sich bei einer Beleihung um eine angesichts der Interessenlage der beteiligten Parteien sehr ungewöhnliche Ausgestaltung handeln.

(4) Grundzüge der Intermediärshaftung im deutschen Recht

Zum weiteren Verständnis ist es sinnvoll, zunächst die Grundlagen und die Dogmatik der Störerhaftung in ihren Grundzügen darzustellen. Die Störerhaftung –wertneutraler: die Intermediärshaftung[522] – ist nicht ausdrücklich (formell) gesetzlich geregelt, sondern vielmehr ein Fall der richterlichen Rechtsfortbildung.[523] Zu dieser sahen sich die Gerichte durch Probleme bei der Durchsetzung des Schutzes absoluter Rechte genötigt. Die Störerhaftung ist nicht auf das Internet beschränkt, entfaltet dort jedoch in erster Linie seine praktische Bedeutung. Im Internet tritt vermehrt die Situation auf, dass die Rechtsdurchsetzung gegen den Täter einer Verletzungshandlung selbst aussichtlos erscheint, die Intermediäre allerdings rechtlich greifbar sind.

Die Rechtswissenschaft und die Gerichte sehen sich mit dem Problem konfrontiert, die Provider als Intermediäre nicht über das Schadensersatzrecht in die Pflicht nehmen zu können. Eine Schadensersatzhaftung der Intermediäre im Internet für Rechtsverletzungen Dritter scheidet wegen der Haftungsprivilegierungen für Internet Provider der §§ 7 – 10 TMG aus.[524] Diese Vorschriften lassen sich vom nationalen Gesetzgeber auch

---

[520] *Jani*, Die partielle verwaltungsrechtliche Inpflichtnahme Privater, S. 89.
[521] *Bormann/Böttcher*, NJW 2011, 2758 (2760).
[522] Ohly, ZUM 2015, 308 (308): „Ein Intermediär ist ein Vermittler, der eine Voraussetzung dafür schafft, dass der unmittelbar Handelnde seine Tätigkeit ausüben kann".
[523] BGH, Urt. v. 15.10.1998, I ZR 120/96, Möbelklassiker, NJW 1999, 1960, (1960); BGH, Urt. v. 18.10.2001, I ZR 22/99, Meißner Dekor, GRUR 2002, 618, (619); BGH, Urt. v. 11.03.2004, I ZR 304/01, Internet-Versteigerung I, BGHZ 158, 236 (244 f.); BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 74.
[524] Insoweit zweifelnd mit Verweis auf vorrangige sekundärrechtliche Regelungen *Czychowski/J. B. Nordemann*, GRUR 2013, 986 (989 f.).

nicht einfach abändern, da sie der Umsetzung der Art. 12 – 15 der E-Commerce-Richtlinie dienen. Man behilft sich also mit einem rechtlichen Kniff. Die Gerichte argumentieren, die Haftungsprivilegierungen der §§ 7 – 10 TMG würden die Provider nur vor einer Schadensersatzhaftung bewahren, nicht jedoch vor einer Inanspruchnahme aus Beseitigungs- und Unterlassungsansprüchen. Diesen Schluss zog der BGH erstmalig in seiner Entscheidung *„Internet-Versteigerung I"* aus § 7 Abs. 2 Satz 2 TMG, wonach Verpflichtungen zur Entfernung oder Sperrung von Informationen nach den allgemeinen Gesetzen auch dann bestünden, wenn der Provider nach den §§ 7–10 TMG nicht haften würde.[525]

Die Störerhaftung beruht dogmatisch auf einer Analogie zu § 1004 BGB, welcher die Beseitigung und Unterlassung von Störungen des Eigentums regelt.[526] Die Störerhaftung zieht den Kreis der Rechtsgutverletzungen weiter als § 1004 BGB und bezieht alle absoluten Rechte und demzufolge auch das Urheberrecht mit ein.[527] Nach den Grundsätzen der Störerhaftung haftet ein Intermediär konsequenterweise auf Unterlassung und Beseitigung von Urheberrechtsverletzungen, soweit deren Voraussetzungen vorliegen.

Die Störerhaftung ist zunächst subsidiär zur täterschaftlichen Haftung. Ist ein Provider nach den allgemeinen deliktsrechtlichen Regeln selbst Täter oder Teilnehmer einer Verletzungshandlung, so haftet er unmittelbar als solcher, etwa aus § 823 Abs. 1, Abs. 2 BGB oder § 97 UrhG.[528] In allen anderen Fällen, in denen die Dienste eines Intermediärs für Rechtsgutsverletzungen verwendet werden, verlangt die Rechtsprechung für eine quasinegatorische Haftung als Störer das kumulative Vorliegen folgender Voraussetzungen: Der Intermediär muss willentlich und adäquat kausal zur Verletzung des geschützten

---

[525] BGH, Urt. v. 11.03.2004, I ZR 304/01, Internet-Versteigerung I, BGHZ 158, 236 (246 f.); fortgesetzt in: BGH, Urt. v. 19.04.2007, I ZR 35/04, Internet-Versteigerung II, BGHZ 172, 119 (Rn. 45); BGH, Urt. v. 25.10.2011 (Versäumnisurteil), VI ZR 93/10, Blogspot, BGHZ 191, 219, Rn. 19; Dieser Schluss wurde aus europarechtlichen Gründen zurecht stark kritisiert, etwa von *Härting*, Internetrecht, Rn. 2575; *Leible/Sosnitza*, NJW 2007, 3324 (3224 f.); *Lehmann/Rein*, CR 2008, 97 (101). So hat der EuGH auch die Haftungsprivilegierungen der Art. 12–15 der Enforcement-Richtlinie auf Unterlassungsansprüche gegen Provider angewendet; vgl. EuGH, Urt. v. 23.03.2010, C-236/08 bis C-238/08, C-236/08 , C-237/08, C-238/08, Slg. 2010, I-02417; EuGH, Urt. v. 16.02.2012, SABAM, Rs. C-360/10, EU:C:2012:85.

[526] *Hetmank*, Internetrecht, 7.1.4 (S. 185); *Ohly*, ZUM 2015, 308 (311). Letzterer sieht eine solche Analogie aus methodischen Gründen allerdings kritisch. So zweifelt Ohly das Vorhandensein einer planwidrigen Regelungslücke an, da der Gesetzgeber im Jahr 2008 im Rahmen der Umsetzung der Enforcement-Richtlinie den Bereich der Rechtsfolgen von Schutzrechtsverletzungen neu geregelt habe. Zudem übe der Intermediär im Gegensatz zum sachenrechtlichen Störer eine sozial erwünschte Tätigkeit aus, so dass es schon an der vergleichbaren Interessenlage fehle.

[527] *Hetmank*, Internetrecht, 7.1.4 (S. 185).

[528] *Hetmank*, Internetrecht, 7.1 (S. 180 ff.).

Rechts beitragen;[529] sein Verhalten muss die Gefährdung des Rechtsguts zumindest erhöht haben;[530] der Intermediär muss in der Lage sein, die Verletzung abzustellen;[531] und schließlich muss er zumutbare Prüfungs- und Verhaltenspflichten verletzt haben.[532]

Die rechtlich bei weitem interessanteste dieser Voraussetzungen ist das Kriterium der Verletzung zumutbarer Prüfungs- und Verhaltenspflichten. Internet-Provider üben für die gesellschaftliche Wohlfahrt notwendige und erwünschte Funktionen aus. Dieser Tatsache wird durch den unbestimmten Rechtsbegriff der zumutbaren Prüfungs- und Verhaltenspflichten Rechnung getragen. Der Vielzahl der unterschiedlichen Sachverhaltskonstellationen und Interessen der Beteiligten (insbesondere auch hinsichtlich deren Schutzwürdigkeit), die von dem ansonsten sehr weit formulierten Tatbestand erfasst werden, kann so mit der notwendigen flexiblen Lösung im Einzelfall begegnet werden. Je näher ein Internet-Dienst einer täterschaftlichen Begehung des Delikts steht, umso eher sind ihm Handlungen zur Verhinderung der Rechtsverletzung zuzumuten und umso weitreichender sind seine Prüfungs- und Überwachungspflichten zu ziehen.

Zunächst sollte man sich daher klarmachen, dass Content Provider, also solche Anbieter, die im Internet *eigene* Angebote öffentlich zugänglich machen, von den Haftungsprivilegierungen der §§ 7 ff. TMG überhaupt nicht erfasst sind.[533] Sie haften daher sowohl deliktisch als auch (quasi-)negatorisch uneingeschränkt. Wer also beispielsweise ein urheberrechtlich geschütztes Werk bei einem Filehoster hochlädt und den Link zu der Datei bekannt macht, der haftet selbstverständlich *auch* auf Schadensersatz, und die Unterlassung und Beseitigung der Verletzungshandlung sind ihm stets zumutbar.[534]

Ist der in Anspruch Genommene ein Content Provider, so ist dies rechtlich in der Regel wenig problematisch, eben da die Frage der Zumutbarkeit der Prüf- und Überwachungspflichten sich nicht stellt und auch die Schadensersatzhaftung im Raum steht. Wichtig wird deshalb gegebenenfalls die Abgrenzung des Content Providers zum Host-Provider: Wird ein Intermediär, der ein Host-Provider ist, wegen einer Urheberrechtsverletzung, die über seine Dienste erfolgt, in Anspruch genommen, so greift die Provider-Privilegierung der §§ 7 ff. TMG, und die Grundsätze der Störerhaftung verlangen eine Prüfung, ob der Anbieter zumutbare Pflichten verletzt hat. Dies ist gegebenenfalls deshalb fraglich,

---

[529] BGH, Urt. v. 12.05.2010, I ZR 121/08, Sommer unseres Lebens, BGHZ 185, 330, Rn. 19; BGH, Urt. v. 08.01.2014, I ZR 169/12, BearShare, BGHZ 200, 76, Rn. 22; *Hofmann*, NJW 2016, 769 (770); *Lettl*, BB 2015, 2371 (2376).
[530] BGH, Urt. v. 17.07.2003, I ZR 259/00, Paperboy, BGHZ 156, 1 (12); *Ahrens u.a.*, WRP 2007, 1281 (1287); *Ohly*, ZUM 2015, 308 (312); a.A.: *Czychowski/J. B. Nordemann*, GRUR 2013, 986 (990).
[531] *Ohly*, ZUM 2015, 308 (312).
[532] BGH, Urt. v. 12.05.2010, I ZR 121/08, Sommer unseres Lebens, BGHZ 185, 330, Rn. 22; BGH, Urt. v. 12.07.2012, I ZR 18/11, Alone in the Dark, BGHZ 194, 339, Rn. 22.
[533] *Roggenkamp/Stadler* in: Heckmann/Paschke, Internetrecht, Kap. 1.4 Rn. 101.
[534] Einmal ganz abgesehen von der unmittelbaren Verursachung der Rechtsgutsgefährdung, ist es für den Content Provider auch ohne weiteres möglich, die Rechtsgutsgefährdung zu beseitigen, da in der Regel derjenige, der einen Inhalt ins Netz gestellt hat, diesen auch wieder aus diesem entfernen kann. Vgl. dazu *Dustmann*, Die privilegierten Provider, S. 36; *Heliosch*, Sperrmaßnahmen im Internet, S. 111; *Sieber*, Verantwortlichkeit, Rn. 97.

weil der Grat zwischen dem bloßen Hosting fremder Informationen und dem Sich-zu-eigen-machen dieser Information schmal sein kann.[535] Aber auch wenn es sich um das Hosting *fremder* Informationen handelt, haftet der Provider unter der Voraussetzung der Verletzung zumutbarer Prüf- und Überwachungspflichten immer noch auf Beseitigung und Unterlassung.[536] Zur Frage, wann eine solche Pflichtverletzung vorliegt, hat der BGH in den vergangenen Jahren eine umfangreiche Judikatur entwickelt.

Die äußere Grenze des Zumutbaren ist gesetzlich festgelegt: Provider sind gemäß § 7 Abs. 2 Satz 1 TMG nicht verpflichtet, die von Dritten über ihre Dienste bereitgestellten Informationen vorsorglich und anlasslos zu überwachen. Dies ist auch von Rechtsprechung und Literatur anerkannt.[537] Das Verbot allgemeiner Überwachungspflichten schließt allerdings nicht die Fälle mit ein, in denen dem Provider Anlass gegeben wurde, nach einer bestimmten Verletzungshandlung Dritter, die über die Dienste des Providers begangen wurde, nachzuforschen. Der Anlass besteht in der Regel darin, dass der Intermediär auf die Rechtsverletzung mithilfe seiner Dienste hingewiesen wurde.[538] Im Anschluss muss der Provider gegebenenfalls nicht bloß die fragliche Information aus seinem Dienst entfernen, sondern zudem auch dafür Sorge tragen, dass gleichartige Verletzungen über seine Dienste zukünftig nicht mehr geschehen.[539]

Der Umfang der Prüf- und Überwachungspflichten, die dem Host-Provider zumutbar sind, richtet sich stets nach dem konkreten Einzelfall. Um die zumutbaren Pflichten zu bestimmen, zieht die Rechtsprechung ein nicht abschließendes Bündel an Kriterien heran.[540]

---

[535] Vgl. *Schneider* in: Schneider, Handbuch des EDV-Rechts, Teil B Rn. 1161 ff.

[536] BGH, Urt. v. 11.03.2004, I ZR 304/01, Internet-Versteigerung I, BGHZ 158, 236 (251).

[537] BGH, Urt. v. 11.03.2004, I ZR 304/01, Internet-Versteigerung I, BGHZ 158, 236 (251 f.); BGH, Urt. v. 12.07.2007, I ZR 18/04, Jugendgefährdende Medien bei eBay, BGHZ 173, 188, Rn. 41; OLG Hamburg, Urt. v. 22.08.2006, 7 U 50/06, heise.de, MMR 2006, 744 (746); OLG Hamburg, Urt. v. 04.02.2009, 5 U 167/07, Mettenden, MMR 2009, 479, (480); *Gercke*, MMR 2006, 493 (493); *Hoeren*, EWiR 2006, 651 (651); *Roggenkamp/Stadler* in: Heckmann/Paschke, Internetrecht, Kap. 1.40 Rn. 105 ff. A.A. noch LG Hamburg, Urt. v. 02.12.2005, 324 O 721/05, Rn. 16 f. (juris); Der BGH ist hier allerdings nicht immer konsequent. Für den Betrieb von WLANs etwa fordert er von den jeweiligen „Anbietern", diese anlasslos im Vorhinein gegen Missbrauch zu sichern, BGH, Urt. v. 12.05.2010, I ZR 121/08, Sommer unseres Lebens, BGHZ 185, 330 Rn. 22; vgl. dazu auch Erwägungsgrund 47 und Art. 15 Abs. 1 der Richtlinie 2000/31/EG und EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 35.

[538] BGH, Urt. v. 12.07.2007, I ZR 18/04, Jugendgefährdende Medien bei eBay, BGHZ 173, 188, Rn. 42; BGH, Urt. v. 29.04.2010, I ZR 69/08, Vorschaubilder I, BGHZ 185, 291, Rn. 39; vgl. auch EuGH, Urt. v. 23.03.2010, C-236/08 bis C-238/08, C-236/08 , C-237/08, C-238/08, Slg. 2010, I-02417, Rn. 109.

[539] BGH, Urt. v. 17.08.2011, I ZR 57/09, Stiftparfüm, BGHZ 191, 19, Rn. 21; BGH, Urt. v. 11.03.2004, I ZR 304/01, Internet-Versteigerung I, BGHZ 158, 236 (251 f.); vgl. auch EuGH, Urt. v. 12.07.2011, Rs. C-324/09, L'Oreal/eBay, Slg. 2011, I-06011, Rn. 131; dazu: *J. B. Nordemann*, GRUR 2011, 977 (977).

[540] *Leistner*, GRUR-Beil. 2010, 1 (8) und *Ohly*, ZUM 2015, 308 (312) sehen hierin methodisch ein „bewegliches System". Vgl. grundlegend zum „beweglichen System" *Wilburg*, Entwicklung eines beweglichen Systems im bürgerlichen Recht.

Dieses Bündel enthält unter anderem die Frage der Kosten[541] der Prüf- und Überwachungsmaßnahmen, die Gefahrgeneigtheit des Dienstes,[542] den Grad des aktiven Verursachungsbeitrags,[543] die gesellschaftliche Bedeutung des Dienstes,[544] die Möglichkeiten des Geschädigten, gegen den Verletzer selbst vorzugehen[545] und die Konsequenzen für das Geschäftsmodell eines Providers, sobald er nicht nur im Einzelfall in Anspruch genommen[546] wird.[547]

Demzufolge wird der Zumutbarkeitsmaßstab von der Rechtsprechung in Abhängigkeit vom konkreten Dienst sehr unterschiedlich weit gezogen.[548] Die DENIC, die die Vergabe der Internet-Domains mit der Endung „*.de*" verwaltet, hat als im Wesentlichen rein technischer Anbieter nur sehr eingeschränkte Prüfpflichten. Sie muss lediglich dann in eine rechtliche Prüfung eintreten, wenn sie ohne weitere Nachforschungen zweifelsfrei feststellen kann, dass eine Rechtsverletzung vorliegt. Dies ist etwa dann der Fall, wenn ein rechtskräftiger Titel eine konkrete Rechtsverletzung festgestellt hat oder eine Rechtsverletzung sich offensichtlich aufdrängen muss.[549] Host-Provider wie Foren und Auktionsplattformen, die rechtswidrige Inhalte Dritter auf ihren Plattformen ohne großen technischen Aufwand entfernen können und von der Eröffnung ihres Marktplatzes und den damit verbundenen Gefahren für die Rechtsgüter Dritter wirtschaftlich profitieren, müssen eine bekannte Rechtsgutsverletzung entfernen und zukünftig mit im Einzelfall zu bestimmendem Aufwand unter Einsatz von Personal und automatisierten Scannern gleichartige Rechtsgutsverletzungen verhindern.[550]

Im Extremfall besonders gefahrgeneigter Angebote, z.B. manchen Filehostern, deren Geschäftsmodell auf Rechtsverletzungen seiner Nutzer ausgelegt ist, führt dies dazu, dass

---

[541] OLG Köln, Urt. v. 18.07.2014, I-6 U 192/11, 6 U 192/11, Goldesel, Rn. 987 (juris); in Anlehnung an EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 48.
[542] BGH, Urt. v. 15.01.2009, I ZR 57/07, Cybersky, GRUR 2009, 841, (843); *Leistner*, GRUR-Beil. 2010, 1 (31 f.).
[543] BGH, Urt. v. 12.07.2012, I ZR 18/11, Alone in the Dark, BGHZ 194, 339, Rn. 21.
[544] BGH, Urt. v. 17.05.2001, I ZR 251/99, ambiente.de, BGHZ 148, 13 (19); BGH, Urt. v. 11.03.2004, I ZR 304/01, Internet-Versteigerung I, BGHZ 158, 236 (251 f.).
[545] BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 81 ff.
[546] OLG Hamburg, Urt. v. 14.01.2009, 5 U 113/07, Spring nicht (Usenet I), MMR 2009, 631, (635); einschränkend aber: BGH, Urt. v. 15.08.2013, I ZR 80/12, Filehosting-Dienst, NJW 2013, 3245, (3249).
[547] Übersichten zu diesen und weiteren Kriterien, die sich auf die zumutbaren Prüfpflichten auswirken, finden sich bei Specht in: *T. Dreier/G. Schulze*, Urheberrechtsgesetz, § 97 Rn. 29 ff.; *Roggenkamp/Stadler* in: Heckmann/Paschke, Internetrecht, Kap. 1.4 Rn. 150 ff. m.w.N. und *Ohly*, ZUM 2015, 308 (312).
[548] *Härting*, Internetrecht, Rn. 2609 kritisiert die Unbestimmtheit und Unvorhersehbarkeit der Reichweite der Prüfpflichten, bevor ein Gericht diese Prüfpflichten im Einzelfall bestimmt hat.
[549] BGH, Urt. v. 17.05.2001, I ZR 251/99, ambiente.de, BGHZ 148, 13 (21 f.).
[550] BGH, Urt. v. 17.08.2011, I ZR 57/09, Stiftparfüm, BGHZ 191, 19, Rn. 39; – *Härting*, Internetrecht, Rn. 2611 ff. weist allerdings unter Bezugnahme auf BGH, Urt. v. 22.07.2010, I ZR 139/08, Kinderhochstühle im Internet I, GRUR 2011, 152, (159); BGH, Urt. v. 30.06.2009, VI ZR 210/08, FOCUS online, GRUR 2009, 1093, (1095 f.); BGH, Urt. v. 27.03.2012, VI ZR 144/11, RSS-Feeds, NJW 2012, 2345, (2346) darauf hin, dass der BGH von der Verpflichtung des Host-Providers, auch zukünftige gleichartige Verletzungen verhindern zu müssen, in einigen Fällen wieder abweicht.

die Host-Provider nicht nur ihre eigene Plattform maschinell und manuell auf gleichartige Rechtsverletzungen überprüfen, sondern auch Linkseiten dritter Anbieter regelmäßig daraufhin untersuchen müssen, ob diese auf bislang nicht entdeckte Rechtsverletzungen auf der eigenen Plattform verweisen.[551]

Ob auch Internet Service Provider nach den Grundsätzen der Intermediärshaftung als Störer in Anspruch genommen werden können, ist umstritten.[552] Eine Beseitigungs- und Unterlassungsverfügung nimmt in solchen Fällen die Form der Anordnung einer Datenverkehrsregulierung an. Der BGH hat diese Frage (im Nachgang zur UPC-Entscheidung des EuGH)[553] jedenfalls zwischenzeitlich im Grundsatz bejahend entschieden.[554] Nunmehr könnte der BGH entsprechende Ansprüche hingegen auf eine analoge Anwendung des § 7 Abs. 4 TMG stützen.[555]

Diese Grundsatzentscheidungen des BGH hatten bereits einen gewissen Vorlauf. Die gerichtliche Inanspruchnahme der Internet Service Provider zur Durchsetzung des Urheberrechts hatte in den letzten Jahren beträchtlich an praktischer Bedeutung gewonnen. Zunächst war – wie im Fall der Arcor-Netzsperren – lediglich mit gerichtlichen Verfahren gedroht worden.[556] Die Fälle *3dl.am*[557] und *Goldesel*[558] gelangten schließlich über die Instanz-Gerichte bis vor den BGH. Auch den EuGH-Entscheidungen *Scarlet*[559] und *UPC Telekabel*[560] gingen zivilgerichtliche Verfahren über die Anordnung von Datenverkehrsregulierung zur Durchsetzung des Urheberrechts voraus.[561] Insbesondere wurde in der UPC-

---

[551] BGH, Urt. v. 12.07.2012, I ZR 18/11, Alone in the Dark, BGHZ 194, 339, Rn. 32 ff.
[552] Ablehnend: *Szupanar*, Schlussanträge des Generalanwalts v. 16.03.2016, Rs. C-484/14, McFadden, EU:C:2016:170, Rn. 132, 150 (betreffend WLAN-Betreiber als Access Provider); LG Kiel, Urt. v. 23.11.2007, 14 O 125/07, CR 2008, 126, Rn. 47 (juris); OLG Frankfurt, Beschl. v. 22.01.2008, 6 W 10/08, Rn. 11 f. (juris). Im Ergebnis auch OLG Hamburg, Urt. v. 21.11.2013, 5 U 68/10, 3dl.am, Rn. 82 (juris), vgl. aber Rn. 72; OLG Köln, Urt. v. 18.07.2014, I-6 U 192/11, 6 U 192/11, Goldesel, Rn. 1008 (juris); *Roggenkamp/Stadler* in: Heckmann/Paschke, Internetrecht, Kap. 1.4 Rn. 190 ff.; *Spindler*, CR 2010, 592 (598).
[553] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 64.
[554] BGH, Urt. v. 26.11.2015, I ZR 3/14, 3dl.am, Rn. 33; BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 34.
[555] BGH, Urt. v. 26.07.2018, Rs. I ZR 64/17, Dead Island, BGHZ 219, 276, Rn. 49.
[556] Ein deutscher Anbieter von Online-Pornografie drohte u.a. dem Internet Service Provider Arcor mit gerichtlichen Schritten, wenn er nicht die Angebote anderer Online-Porno-Plattformen sperren würde. Tatsächlich wurde hier allerdings noch mit möglichen Verletzungen des Jugendmedienschutzes und nicht mit dem Urheberrecht argumentiert. Vgl. zu diesem Fall *Schnabel*, K&R 2008, 26.
[557] OLG Hamburg, Urt. v. 21.11.2013, 5 U 68/10, 3dl.am (BGH, Urt. v. 26.11.2015, I ZR 3/14, 3dl.am).
[558] OLG Köln, Urt. v. 18.07.2014, I-6 U 192/11, 6 U 192/11, Goldesel (juris) (BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82).
[559] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959.
[560] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192.
[561] Auch in anderen Mitgliedsstaaten der EU ist in den vergangenen Jahren die Anordnung einer DVR zur Durchsetzung des Urheberrechts Gegenstand (erfolgreicher) gerichtlicher Verfahren gewesen. Dazu *J. B. Nordemann*, ZUM 2014, 499 (499) mit weiteren Nachweisen.

Entscheidung durch den EuGH festgestellt, dass die europäischen Grundrechte solchen Anordnungen zumindest nicht prinzipiell entgegenstehen.[562]

Zur Abschaffung der Intermediärshaftung und als Reaktion auf die UPC- und die McFadden-Entscheidung des EuGH hat der deutsche Gesetzgeber die §§ 7 und 8 des Telemediengesetzes angepasst.[563] Schon zuvor hatte § 8 Abs. 1 TMG neutrale Provider, zu denen insbesondere Internet Service Provider zählen, umfangreich haftungsprivilegiert. Die Intermediärshaftung konnte aber zumindest bis zur jüngsten Novellierung des TMG dennoch greifen, weil der BGH sich auf den Standpunkt gestellt hatte, dass die Privilegierungen sich lediglich auf Schadensersatzansprüche, nicht jedoch auf Unterlassungsansprüche bezögen.[564] § 8 Abs. 1 Satz 2 TMG (n.F.) stellt nun allerdings (vermeintlich) klar, dass auch Ansprüche auf Beseitigung und Unterlassung unter die Haftungsprivilegierung des § 8 Abs. 1 Satz 1 TMG (n.F.) fallen.

Die Widersprüche, die sich durch den ebenfalls novellierten § 7 TMG im Zusammenspiel mit § 8 Abs. 1 Satz 2 TMG ergeben, sind jedoch kaum aufzulösen, so dass die Reichweite der Haftungsprivilegierung auch nach der Novellierung weiter im Unklaren bleibt.[565] Im Grunde besteht hauptsächlich folgendes Problem: § 7 Abs. 4 n.F. TMG legt nahe, dass auch weiterhin Sperrmaßnahmen gegen Access Provider bei Verletzungen geistigen Eigentums angeordnet werden können, dies aber nur insoweit gelten soll, wie es sich bei den Access Providern um Betreiber von WLAN-Hotspots betrifft.[566] Alle anderen Formen der Access Provider wären dann von der Möglichkeit ausgenommen, dass sie zu datenverkehrsregulierenden Maßnahmen verpflichtet würden, und ausgerechnet die WLAN-Hotspot-Betreiber wären einer erweiterten Haftung ausgesetzt.[567] Dies widerspricht jedoch der Gesetzesbegründung der Bundesregierung, deren Ziel bei der Novellierung des TMG es ausschließlich gewesen ist, die Betreiber von Hotspots von der Störerhaftung zu befreien.[568]

---

[562] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 64.
[563] Vgl. EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192; EuGH, Urt. v. 15.09.2016, Rs. C-484/14, Mc Fadden, EU:C:2016:689; Gesetzentwurf der Bundesregierung: Entwurf eines Dritten Gesetzes zur Änderung des Telemediengesetzes, BT-Drs. 18/12202, 2017, S. 1.
[564] *Spindler*, MMR 2018, 48 (49).
[565] Vgl. ausführlich zu den methodischen Problemen die §§ 7, 8 TMG n.F. auszulegen *Timo u.a.*, GRUR-Prax 2017, 206 (206 ff.); *Höfinger*, ZUM 2018, 382; *Mantz*, GRUR 2017, 969; *Nicolai*, ZUM 2018, 33; *Spindler*, CR 2017, 333.
[566] Im Gesetzentwurf der Bundesregierung: Entwurf eines Dritten Gesetzes zur Änderung des Telemediengesetzes, BT-Drs. 18/12202, 2017, S. 12 zählt die Bundesregierung als mögliche Maßnahmen die Sperrung von Ports, aber auch die in dieser Arbeit gegenständlichen Formen von Netzsperren als mögliche Sperrmaßnahmen auf. Vgl. auch *Nicolai*, ZUM 2018, 33 (37).
[567] *Spindler*, CR 2017, 333 (334).
[568] LG München I, Urteil v. 01.02.2018, 7 O 17752/17, abrufbar unter http://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-002857, Rn. 34 ff.; *Höfinger*, ZUM 2018, 382 (384).

Das LG München zieht daher in einer Entscheidung aus dem Februar 2018 aus diesen Widersprüchen den Schluss, den Wortlaut des § 8 Abs. 1 Satz 2 TMG teleologisch zu reduzieren und so auszulegen, dass dieser sich nur auf die WLAN-Hotspot-Betreiber beziehe. An der Störerhaftung für klassische Access und Network Provider würde sich somit nach dieser Auslegung durch die Novellierung des TMG nichts ändern.[569]

Mit der Dead-Island-Entscheidung hat der BGH einen Unterlassungsanspruch gegen einen Access Provider, der drahtgebunden einen Zugang zum TOR-Netzwerk vermittelte, nun allerdings unter Aufgabe der Störerhaftung auf eine analoge Anwendung des § 7 Abs. 4 TMG gestützt, da die Interessenlage bei der Zugangsvermittlung technikneutral sei.[570]

Es bleibt abzuwarten, ob sich diese Rechtsprechung auch bei kommerziellen Access Providern festigen wird. Teilweise wird dies in der rechtswisenschaftlichen Literatur mit der Begründung angezweifelt, dass es sich beim Dead-Island-Urteil um eine Einzelfallentscheidung handele, die sich auf kommerzielle Access Provider nicht übertragen lasse.[571]

(5) Grundrechtsberechtigung der ISPs bei zivilgerichtlichen Anordnungen

Von dem soeben besprochenen Fall, dass ein Internet Service Provider durch eine behördliche Anordnung zur Implementierung einer Datenverkehrsregulierung zur Durchsetzung des Urheberrechts verpflichtet wird, muss die Situation unterschieden werden, in der dem ISP die Einrichtung einer DVR im Wege einer richterlichen Anordnung nach vorangegangenem Zivilprozess aufgetragen wurde. Das in der deutschen Rechtsordnung einschlägige rechtliche Instrument, das private Rechteinhaber nutzen können, um Intermediäre zu verpflichten, die nicht selbst die Rechtsgutsverletzung begehen, die Verletzungen ihrer Rechte abzustellen, ist die Störerhaftung. Bei zivilrechtlichen Inanspruchnahmen stellt sich dann die Frage, ob die Grundrechte anwendbar sind.

Die Störerhaftung ist ein zivilrechtliches Institut, das unter Privaten wirkt.[572] Die Grundrechte sind hingegen in erster Linie Abwehrrechte Privater gegenüber dem Staat.[573] Privatrechtssubjekte sind keine Grundrechtsadressaten und können daher nicht selbst in Grundrechte eingreifen. Konsequenterweise können sich Grundrechtsträger nicht unmittelbar gegen einen Grundrechtseingriff durch Private wehren.[574]

Auch im Privatrecht werden die grundrechtlichen Schutzbereiche jedoch mittelbar gewährleistet, da die Grundrechte die gerichtliche Auslegung des Privatrechts beeinflussen.

---

[569] LG München I, Urteil v. 01.02.2018, 7 O 17752/17, abrufbar unter http://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-002857, Rn. 29; i.E. zustimmend und mit weiteren Argumenten *Höfinger*, ZUM 2018, 382 (384 f.).
[570] BGH, Urt. v. 26.07.2018, Rs. I ZR 64/17, Dead Island, BGHZ 219, 276, Rn. 49.
[571] *Müller*, MMR 2019, 426 (428); eine Analogie des § 7 Abs. 4 TMG ebenfalls ablehnend *Sesing*, GRUR 2019, 898 (899 f.) m.w.N. aaO in Fn. 21; eine Analogie hingegen befürwortend *Ohly*, JZ 2019, 251 (253).
[572] *Hoeren u.a.*, Handbuch Multimedia-Recht, Teil 18.2 Rn. 19 (Stand: 41. Erg.-Lfg., März 2015).
[573] Ipsen, Staatsrecht II, § 2 III 3 c) (Rn. 91); vgl. auch Art. 1 Abs. 3 GG: „*Die [...] Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht*".
[574] *Ipsen*, Staatsrecht II, § 2 III 2 b) (Rn. 68 ff.).

Im Lüth-Urteil stellte das Bundesverfassungsgericht bereits früh fest, dass die Grundrechte mehr seien als klassische Abwehrrechte gegenüber dem Staat. Diese würden zudem auch eine objektive Werteordnung bilden, die in die gesamte Rechtsordnung ausstrahle. Auch Normen des Zivilrechts seien daher im Lichte der Grundrechte, also grundrechtsfreundlich, auszulegen. Dazu biete sich insbesondere eine entsprechende Interpretation der in den zivilrechtlichen Normen enthaltenen unbestimmten Rechtsbegriffe an.[575]

Diese sogenannte *mittelbare Drittwirkung der Grundrechte* findet auch bei der Intermediärshaftung Anwendung.[576] Bei der gerichtlichen Gewährung von Unterlassungsansprüchen werden die aus den Grundrechten abzuleitenden objektiv-rechtlichen Schutzpflichten des Staates auf privatrechtlichem Wege unmittelbar umgesetzt,[577] wobei Anordnungen einer Datenverkehrsregulierung aus der Sicht der Internet Service Provider deren Berufsausübung im gleichen Maße einschränken, wie dies bei einer behördlichen Anordnung der Fall wäre.

In Anbetracht der Schwere der Grundrechtsbeeinträchtigungen kann es auch keinen Unterschied machen, ob eine Datenverkehrsregulierung dem Internet Service Provider von einer Behörde oder einem Gericht auferlegt wird. Der Staat kann sich nicht dadurch seiner Bindung an die Grundrechte entziehen, dass er die Durchsetzung eines regulatorischen Zwecks nicht öffentlich-rechtlich ausgestaltet, sondern ins Privatrecht auslagert.

Hinzu kommen im speziellen Fall der Datenverkehrsregulierung über den Weg der Störerhaftung zwei weitere Punkte, die dafür sprechen, die Anordnung entsprechender Maßnahmen durch ein Zivilgericht an den Grundrechten zu messen. Zum einen betrifft die DVR potentiell auch in nachteiliger Weise Grundrechte der Internet-Nutzer und Anbieter von Online-Angeboten, die nicht unmittelbar am Zivilverfahren beteiligt sind. Würde das

---

[575] Ständige Rechtsprechung: erstmals in BVerfG, Urt. v. 15.01.1958, 1 BvR 400/51, Lüth, BVerfGE 7, 198, (205 ff.); fortgesetzt u.a. in BVerfG, Beschl. v. 26.02.1969, 1 BvR 619/63, Blinkfüer, BVerfGE 25, 256 (263); BVerfG, Beschl. v. 07.02.1990, 1 BvR 26/84, Handelsvertreter, BVerfGE 81, 242 (254 f.); BVerfG, Beschl. v. 19.10.1993, 1 BvR 567/89, 1 BvR 1044/89, Bürgschaftsvertrag, BVerfGE 89, 214 (231 f.); BVerfG, Beschl. v. 19.04.2005, 1 BvR 1644/00, 1 BvR 188/03, Pflichtteilsentziehung, BVerfGE 112, 332 (358); so auch *Jarass* in: Merten/Papier, Handbuch der Grundrechte II, § 38 Rn. 60 f.; *Stern* in: Isensee/P. Kirchhof, HStR VIII, § 185 Rn. 83.

[576] So ausdrücklich: BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 32; BGH, Urt. v. 26.11.2015, I ZR 3/14, 3dl.am, Rn. 31 (juris); OLG Hamburg, Urt. v. 21.11.2013, 5 U 68/10, 3dl.am, Rn. 83 (juris); OLG Köln, Urt. v. 18.07.2014, I-6 U 192/11, 6 U 192/11, Goldesel, Rn. 931 (juris); *Durner*, ZUM 2010, 833 (837); *Frey u.a.*, MMR-Beil. 2012, 1 (7 f.).

[577] *Schliesky u.a.*, Drittwirkung im Internet, S. 61 f.; *Jarass* in: Jarass/Pieroth, Grundgesetz, Vorb. v. Art. 1 Rn. 33; vgl. auch *Hufen*, Staatsrecht II, § 7 VIII 2 (Rn. 9); *Schwabe*, Drittwirkung, S. 9, die den Begriff der „mittelbaren Drittwirkung" kritisieren und mit Recht darauf hinweisen, dass zwar nicht die Privatrechtssubjekte, sehr wohl aber die Zivilgerichte Grundrechtsadressaten seien. Daher bedürfe es nicht der umständlichen dogmatischen Konstruktion einer Ausstrahlungswirkung der Grundrechte ins Privatrecht. Auf das Ergebnis der hier diskutierten Frage hat dieser Streit jedoch keinen Einfluss, so dass mit der herrschenden Meinung hier das Konzept der „mittelbaren Drittwirkung" angewendet werden soll.

Gericht keine umfassende grundrechtliche Überprüfung vornehmen, wären diese Grundrechtsträger weitgehend schutzlos gestellt.[578]

Ein weiteres Argument gründet auf der Tatsache, dass es sich bei der Störerhaftung lediglich um Richterrecht handelt. Die Legislative, die grundsätzlich dafür zuständig ist, Recht zu setzen und damit auch dafür, die Voraussetzungen und Rechtsfolgen der Störerhaftung auszugestalten, ist an die Grundrechte gebunden. Dies gilt auch für den Privatrechtsgesetzgeber.[579] Hintergrund ist zum einen, dass das Grundgesetz nicht zwischen dem Privatrechtsgesetzgeber und der Legislative im Übrigen unterscheidet, neben diesem formalen Argument allerdings auch, dass der Gesetzgeber sich im Bereich des Grundrechtsschutzes entscheiden kann, ob er diesen privatrechtlich oder öffentlich-rechtlich ausgestalten will.[580]

So liegt der Fall auch bei der Datenverkehrsregulierung zur Durchsetzung des Urheberrechts. In Ermangelung einer öffentlich-rechtlichen Vorschrift greifen die Gerichte hier teilweise auf das richterrechtliche Institut der Störerhaftung zurück. Das Institut der Störerhaftung wurde allerdings nicht durch einen gesetzgeberischen Akt, der der verfassungsrechtlichen Überprüfung hätte zugeführt werden können, sondern durch die Fachgerichte erfunden. Insoweit bieten sich nur die gerichtlichen Entscheidungen, die die Störerhaftung begründen und ausgestalten, zur Überprüfung anhand der Grundrechte an. Dieser Weg darf dem Grundrechtsträger nicht abgeschnitten werden. Ein ISP kann sich daher bei einer zivilgerichtlichen Anordnung im Ergebnis in gleicher Weise auf Art. 12 Abs. 1 GG berufen wie im Falle einer behördlichen Anordnung.

Im Ergebnis können sich die Internet Service Provider folglich gegen eine Datenverkehrsregulierung in beinahe allen denkbaren Konstellationen auf den Schutz des Art. 12 GG berufen.

2. Eingriff in die Berufsfreiheit

Zu klären ist weiterhin die Frage, ob es sich bei der Datenverkehrsregulierung zur Urheberrechtsdurchsetzung um einen Eingriff in die Berufsfreiheit handelt. Bei der Datenverkehrsregulierung handelt es sich nur dann um eine Beschränkung der Berufsfreiheit, die

---

[578] So auch OLG Köln, Urt. v. 18.07.2014, I-6 U 192/11, 6 U 192/11, Goldesel, Rn. 931 (juris); *Frey u.a.*, MMR-Beil. 2012, 1 (19).

[579] BVerfG, Urt. v. 15.01.1958, 1 BvR 400/51, Lüth, BVerfGE 7, 198, (206 f.); BVerfG, Beschl. v. 04.05.1971, 1 BvR 636/68, Spanier-Entscheidung, BVerfGE 31, 58 (72 ff.); BVerfG, Beschl. v. 14.02.1973, 1 BvR 112/65, Soraya, BVerfGE 34, 269 (282); BVerfG, Urt. v. 15.12.1999, 1 BvR 653/96, Caroline von Monaco II, BVerfGE 101, 361 (387); Jarass in: *Jarass/Pieroth*, Grundgesetz, Art. 1 Rn. 49; a.A.: *Epping*, Grundrechte, Kap. 7 II 2 b) cc) (Rn. 372).

[580] Grundlegend insoweit die Ausführungen des BVerfG, Urt. v. 15.01.1958, 1 BvR 400/51, Lüth, BVerfGE 7, 198, (206): „Der Einfluß grundrechtlicher Wertmaßstäbe wird sich vor allem bei denjenigen Vorschriften des Privatrechts geltend machen, die zwingendes Recht enthalten und so einen Teil des ordre public – im weiten Sinne – bilden, d. h. der Prinzipien, die aus Gründen des gemeinen Wohls auch für die Gestaltung der Rechtsbeziehungen zwischen den einzelnen verbindlich sein sollen und deshalb der Herrschaft des Privatwillens entzogen sind. Diese Bestimmungen haben nach ihrem Zweck eine nahe Verwandtschaft mit dem öffentlichen Recht, dem sie sich ergänzend anfügen. Das muß sie in besonderem Maße dem Einfluß des Verfassungsrechts aussetzen".

einer Rechtfertigung bedarf, wenn es sich bei der Beschränkung um einen verfassungsrechtlich relevanten Eingriff in den Schutzbereich des Art. 12 Abs. 1 GG handelt.[581] Das moderne Verständnis eines Grundrechtseingriffs beinhaltet jedes staatliche Handeln, durch das einem Grundrechtsträger ein Verhalten oder der Genuss einer Freiheit, die in den Schutzbereich eines Grundrechts fällt, zumindest in Teilen unmöglich macht. Unerheblich ist, ob der Effekt beabsichtigt oder unbeabsichtigt, mittelbar oder unmittelbar, rechtlich oder auf tatsächlicher Ebene eintritt und ob er mit oder ohne Befehl und Zwang durchgesetzt wird.[582]

Bei Anordnungen einer Datenverkehrsregulierung handelt es sich um solche Eingriffe in die Berufsfreiheit der Internet Service Provider. Datenverkehrsregulierende Maßnahmen zur Durchsetzung des Urheberrechts bezeichnen nach der in dieser Arbeit verwendeten Definition hoheitliche Eingriffe in den Datenverkehr des Internets, die in die Praxis umgesetzt werden, indem staatliche Einrichtungen diejenigen Internet Service Provider, über die sie rechtliche Gewalt ausüben können, zu entsprechenden Handlungen verpflichten. Die in erster Linie in Frage kommenden Maßnahmen sind das Blockieren und die Umleitung des Datenverkehrs. Technisch umsetzbare Maßnahmen sind die IP-Sperre, die DNS-Sperre und die Deep Packet Inspection.

Der Provider muss dazu entweder durch eine gesetzliche, eine behördliche oder eine gerichtliche Anordnung zur Durchführung solcher Maßnahmen verpflichtet werden. Eine Verpflichtung des ISP kann weiterhin entweder so ausgestaltet werden, dass der ISP anbieterbezogen in den Datenverkehr eines kompletten unter einer Domain aufrufbaren Internetangebots eingreift, oder aber der Provider inhaltsbezogen den Datenverkehr bestimmten urheberrechtlich geschützten Inhalts manipulieren soll. Auch Mischformen sind möglich.

Durch solche Maßnahmen wird ein Internet Service Provider in seiner grundrechtlich geschützten Freiheit eingeschränkt, über seine wirtschaftlichen, technischen und finanziellen Ressourcen zu verfügen. Eine DVR verlangt von den ISPs gezielt, ihre technischen Systeme und ihre innerbetriebliche Organisation anzupassen, um zur Verhinderung oder Unterbindung von Urheberrechtsverletzungen in den Datenverkehr eingreifen zu können.[583] Die Einrichtung und der Unterhalt von Filtersystemen zur Durchsetzung des Urheberrechts ist für die ISPs zudem mit erheblichen Kosten verbunden, wenn sie das notwendige

---

[581] *Ipsen*, Staatsrecht II, § 3 II (Rn. 136 ff.).

[582] *Kingreen/Poscher*, Grundrechte – Staatsrecht II, § 6 III 2 (Rn 293 ff.); *Jarass* in: Jarass/Pieroth, Grundgesetz, Vbm. vor Art. 1 Rn. 28 f. Im Gegensatz dazu steht das engere klassische Verständnis des Grundrechtseingriffs: Als solcher wird gemäß BVerfG, Beschl. v. 26.06.2002, 1 BvR 670/91, Psychosekte, BVerfGE 105, 279 (300) ein „*rechtsförmiger Vorgang verstanden, der unmittelbar und gezielt (final) durch ein vom Staat verfügtes, erforderlichenfalls zwangsweise durchzusetzendes Ge- oder Verbot, also imperativ, zu einer Verkürzung grundrechtlicher Freiheiten führt*". Diese klassische Definition des Eingriffs ist jedoch mittlerweile überholt.

[583] BGH, Urt. v. 26.11.2015, I ZR 3/14, 3dl.am, Rn. 36 (juris); BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 37. So auch *Heliosch*, Sperrmaßnahmen im Internet, S. 78; *Sieber/Nolde*, Sperrverfügungen, S. 62.

Personal für die fortdauernde technische Betreuung und Überwachung der DVR und die erforderlichen Sachinvestitionen selbst aufbringen müssen. [584]

Dies gilt für jede Form der Datenverkehrsregulierung. Für IP- und DNS-Sperren, die von den technischen Anforderungen her weniger anspruchsvoll sind, müssen jedoch Filterlisten gepflegt werden. Das erfordert insbesondere die ständige Überwachung der Domains und IP-Adressen, unter denen das zu sperrende Angebot erreichbar ist, und die Aktualisierung der entsprechenden Einträge am DNS-Server bzw. in Routing-Tabellen.[585] Hierzu müssen in erster Linie Mitarbeiter des Internet Service Providers abgestellt und entsprechende Überwachungs- und Implementierungsprozesse etabliert werden. Die Überwachung des Datenverkehrs auf bestimmte Inhalte mithilfe einer Deep Packet Inspection verlangt hingegen nach umfangreichen Investitionen in Überwachungstechnik und Rechenleistung beim ISP. [586] Selbst wenn die Infrastruktur für eine Deep Packet Inspection beim ISP bereits vorhanden sein sollte, sind die Ressourcen zur Überwachung und Manipulation des Datenverkehrs begrenzt und könnten von den Providern zu anderen Zwecken als der Durchsetzung des Urheberrechts eingesetzt werden, zum Beispiel zum Traffic Management.[587] Die Anordnung einer DVR zur Urheberrechtsdurchsetzung würde diese Ressourcen für Zwecke reservieren, die unter Umständen nicht im Eigeninteresse des ISP sind, und Nachrüstungen erforderlich machen.

Datenverkehrsregulierung stellt im Übrigen nicht nur nach dem weiten modernen, sondern auch nach dem engeren klassischen Verständnis eines Grundrechtseingriffs einen solchen dar. Unter einem klassischen Eingriff wird ein *„rechtsförmiger Vorgang verstanden, der unmittelbar und gezielt (final) durch ein vom Staat verfügtes, erforderlichenfalls zwangsweise durchzusetzendes Ge- oder Verbot, also imperativ, zu einer Verkürzung grundrechtlicher Freiheiten führt“*.[588] Anordnungen einer Datenverkehrsregulierung sind final, da es sich bei diesen um das Mittel der (staatlichen) Wahl handelt und nicht um eine bloße unbeabsichtigte Folge staatlichen Handelns. Bei der Anordnung einer Datenverkehrsregulierung liegt es auch fern, von einer nur mittelbaren Einschränkung zu sprechen, da eine solche Anordnung sich direkt an die Internet Service Provider richtet. Bei

---

[584] Die tatsächlichen Kosten einer Datenverkehrsregulierung hängen von dem zugrunde liegenden Verfahren und den Gegebenheiten beim konkreten ISP ab, beispielsweise von der Menge des zu kontrollierenden Datenverkehrs oder der bereits vorhandenen Technik zur Überwachung und Manipulation des Datenverkehrs. Einen Anhaltspunkt bietet OLG Köln, Urt. v. 18.07.2014, I-6 U 192/11, 6 U 192/11, Goldesel, Rn. 1001 (juris). Dort schätzt die Beklagte in einem Verfahren, in dem sie zur Einrichtung von DNS- und IP-Sperren hinsichtlich der Nurlister-Seite Goldesel.de zur Durchsetzung des Urheberrechts diverser Musiktitel verpflichtet werden soll, die ihr entstehenden Kosten auf eine Million Euro.

[585] Vgl. auch *Sieber/Nolde*, Sperrverfügungen, S. 50. Hinweise auf die möglichen einmaligen – nicht auf die laufenden – Kosten von IP- und DNS-Sperren mag VG Köln, Urt. v. 03.03.2005, 6 K 7151/02, Rn. 23 (juris) geben, wo von 28.000,- EUR bzw. 17.500,- EUR die Rede ist.

[586] Vgl. oben Kap. 2 V 1 a) (S. 73 f.).

[587] Vgl. oben Kap. 1 III 3 d) (S. 27 ff.).

[588] Vgl. BVerfG, Beschl. v. 26.06.2002, 1 BvR 670/91, Psychosekte, BVerfGE 105, 279 (300). Die klassische Definition des Eingriffs ist jedoch mittlerweile überholt, *Kingreen/Poscher*, Grundrechte – Staatsrecht II, § 6 III 2 (Rn. 293).

legislativen, behördlichen oder gerichtlichen Anordnungen ist ein ISP zudem rechtlich und nicht nur tatsächlich verpflichtet, diesen nachzukommen. Um die Verpflichtung eines Providers durchzusetzen, wird der Staat daher geeignete rechtliche Zwangsmaßnahmen zu diesem Zweck vorsehen.

Nachdem nun festgestellt ist, dass ein Eingriff in den Schutzbereich von Art. 12 Abs. 1 GG vorliegt, muss in der weiteren Prüfung eine dogmatische Besonderheit der Berufsfreiheit Berücksichtigung finden. Denn es stellt sich die Frage, auf welcher Stufe des Schutzbereichs des Art. 12 Abs. 1 GG eingegriffen wird.

Das BVerfG hat in seinem Apotheker-Urteil im Hinblick auf den Wortlaut des Art. 12 Abs. 1 GG, der zwischen Berufswahl (Satz 1) und Berufsausübung (Satz 2), auch im Hinblick auf die Schranken, unterscheidet, die sogenannte Drei-Stufen-Theorie entwickelt. In der Drei-Stufen-Theorie werden hoheitliche Eingriffe in die Berufsfreiheit in drei verschiedene Kategorien eingeteilt, die sich in ihrer Eingriffsintensität unterscheiden und an deren Rechtfertigung in der Folge unterschiedlich hohe Voraussetzungen zu knüpfen sind.[589] Insoweit stellt sich die Frage, auf welcher Stufe die Datenverkehrsregulierung in die Berufsfreiheit eingreift.

Objektive Einschränkungen der Berufswahl sind solche Maßnahmen, die die Ergreifung eines Berufs mit der Erfüllung bestimmter Voraussetzungen verbinden, bei denen es sich nicht um solche handelt, die in der persönlichen Qualifikation des Berufsanwärters für den Beruf liegen.[590]

Auf der zweiten Stufe stehen solche Berufswahleinschränkungen, die an die persönlichen Fähigkeiten oder Eigenschaften des Bürgers anknüpfen (subjektive Einschränkungen der Berufswahl). Dabei kann es sich beispielsweise um schulische, berufliche oder akademische Abschlüsse, die berufsbezogene Zuverlässigkeit oder das Alter des Bürgers handeln.[591] Nicht mehr erforderlich ist im Gegensatz zu früher, dass der Bürger diese Kriterien beeinflussen können muss.[592]

Schließlich sind von den objektiven und subjektiven Einschränkungen der Berufswahl staatliche Maßnahmen zu unterscheiden, die die Berufsausübung regeln (Berufsaus-

---

[589] BVerfG, Urt. v. 11.06.1958, Apotheker-Urteil, BVerfGE 7, 377 (405 ff.); *Ipsen*, Staatsrecht II, § 15 III 1 Rn. 652 ff.).
[590] *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 12 Rn. 36.
[591] BVerfG, Urt. v. 11.06.1958, Apotheker-Urteil, BVerfGE 7, 377 (406); BVerfG, Beschl. v. 16.06.1959, 1 BvR 71/57, Hebammenaltersgrenze, BVerfGE 9, 338 (345); BVerfG, Beschl. v. 17.07.1961, 1 BvL 44/55, Handwerksordnung, BVerfGE 13, 97 (115).
[592] BVerfG, Beschl. v. 16.06.1959, 1 BvR 71/57, Hebammenaltersgrenze, BVerfGE 9, 338 (345); Breuer in: *Isensee/P. Kirchhof*, HStR VI, § 148 Rn. 38; *Jarass/Pieroth*, Grundgesetz, Art. 12 Rn. 35; anders noch: BVerfG, Urt. v. 11.06.1958, Apotheker-Urteil, BVerfGE 7, 377 (406).

übungsregelungen). Dabei handelt es sich *„einfach [um] die übrigen Eingriffe in die Berufsfreiheit“*, also solche, die die Art und Weise der Berufsausübung und nicht das Ob regeln.[593]

Bei einer Datenverkehrsregulierung handelt es sich für den Internet Service Provider um eine Berufsausübungsregelung. Durch die Verpflichtung, in den Datenverkehr einzugreifen und damit gegebenenfalls Tätigkeiten auszuführen, die zuvor nicht zu den Operationen des Unternehmens gehört haben, wird kein eigenständiges neues Berufsbild geschaffen. Durch die Anordnung von Maßnahmen der DVR werden die ISPs weder gezwungen, ihre bisherige gewerbliche Tätigkeit aufzugeben, noch werden sie dazu verpflichtet, einen neuen Beruf zu ergreifen. Dies gilt auch dann, wenn die aufgetragenen Tätigkeiten – wie hier – nicht zum Kerngeschäft des Unternehmens gehören oder nicht einmal in dessen Interesse liegen.[594] Zur Abgrenzung zwischen Berufswahl- und Berufsausübungsregelung bei der Verpflichtung zur Durchführung neuer Aufgaben hat das Bundesverfassungsgericht festgestellt, dass es sich dann um eine Berufsausübungsregelung handelt, wenn die Tätigkeit, die der Staat dem Unternehmer abverlangt, in beliebiger Weise an die eigentliche wirtschaftliche Tätigkeit des Unternehmens anknüpft.[595] Genau dies tut der Staat, wenn er die berufliche Tätigkeit der ISPs, den Internet-Datenverkehr zu transportieren, mit gewissen Kontrollen und Manipulationen dieses Verkehrs verbindet.[596]

Schließlich besitzen Anordnungen einer Datenverkehrsregulierung gegenüber den ausführenden Internet Service Providern auch eine *objektiv-berufsregelnde Tendenz*. Dieses Kriterium fordert das BVerfG bei Beschränkungen der Berufsausübung zusätzlich, damit aus einer nicht dem Rechtfertigungsvorbehalt unterliegenden bloßen Beeinträchtigung der Berufsfreiheit ein zu rechtfertigender Eingriff wird.[597] Notwendig ist das Erfordernis einer *objektiv berufsregelnden Tendenz*, weil sich beinahe jede Regelung, die sich auf jeden

---

[593] *Kingreen/Poscher*, Grundrechte – Staatsrecht II, § 21 II 2 (Rn. 963).

[594] Im Ergebnis auch: *Heliosch*, Sperrmaßnahmen im Internet, S. 78; *J. Kahl*, SächsVBl. 2010, 180 (185); *Sieber/Nolde*, Sperrverfügungen, S. 62.

[595] BVerfG, Beschl. v. 16.03.1971, 1 BvR 52/66, 1 BvR 665/66, 1 BvR 667/66, 1 BvR 754/66, Erdölbevorratung, BVerfGE 30, 292 (312 f.).

[596] Dies gilt trotz weitläufiger Diskussion dieser Frage bei *Sieber/Nolde*, Sperrverfügungen, S. 62 f. auch für ISPs, die sich bislang lediglich auf das Routing und die Verarbeitung der Internet-Schicht beschränkt haben, nun aber auf staatliche Anordnung hin auf tieferen Ebenen des TCP/IP-Stapels arbeiten sollen. Wie *Sieber/Nolde* richtigerweise anmerken, besteht nach der Verkehrsanschauung und natürlicher Betrachtung kein eigenständiges Berufsbild des lediglich auf der Internet-Schicht arbeitenden Providers. Ohnehin zurecht kritisch in Bezug auf die Berufsbildlehre *Kämmerer* in: v. Münch/Kunig, Grundgesetz Bd. 1, 7. Aufl. 2021, Art. 12 Rn. 28 m.w.N.

[597] BVerfG, Beschl. v. 30.10.1961, 1 BvR 833/59, Schankerlaubnissteuer, BVerfGE 13, 181 (186); BVerfG, Urt. v. 22.05.1963, 1 BvR 76/56, Werkfernverkehr, BVerfGE 16, 147, Werkfernverkehr, Rn. 63; BVerfG, Beschl. v. 29.11.1967, 1 BvR 175/66, Coupon-Steuer, BVerfGE 22, 380 (384); BVerfG, Beschl. v. 18.07.1979, 2 BvR 488/76, Rechtsanwaltsausschluss, BVerfGE 52, 42 (54); kritisch nicht in der Sache, wohl aber bezüglich des Begriffs: *Ipsen*, Staatsrecht II, § 15 III 1 (Rn. 658). Eine objektive berufsregelnde Tendenz stelle nach seinem Wortlaut zum einen auf die Intention des Gesetzgebers, zum anderen auf den tatsächlichen (objektiven) Effekt einer Regelung ab. Zu bevorzugen sei eine rein objektive Beurteilung. Im Ergebnis so wohl auch das Bundesverfassungsgericht, vgl. BVerfG, Urt. v. 03.11.1982, 1 BvL 4/78, Tierpräparator, BVerfGE 61, 291 (308).

Bürger gleichermaßen auswirkt, auch Einfluss auf die Berufsausübung hat. Ohne ein Korrektiv würden daher die Unterschiede in den Grundrechten eingeebnet.[598] Die Bejahung der objektiv berufsregelnden Tendenz bereitet hier jedoch keine Probleme, da es sich, wie oben bereits festgestellt, bei der Anordnung einer DVR um eine gezielte Beschränkung der Berufsausübung handelt und nicht um einen bloß unbeabsichtigten Nebeneffekt.

3. Schranken der Berufsfreiheit

Eingriffe in Grundrechte können jedoch in einem bestimmten Umfang gerechtfertigt sein. Die erste Voraussetzung dafür ist, dass die Beschränkungsmöglichkeit vom Grundgesetz vorgesehen wurde (Schranke). Allerdings zieht das Grundgesetz auch für diese Beschränkungsmöglichkeiten wieder Grenzen (sogenannte „Schranken-Schranken"). Die zweite Voraussetzung ist daher, dass auch die Schranken-Schranken berücksichtigt werden.[599]

Nicht jedes Grundrecht ist vorbehaltslos gewährleistet. Dies gilt auch für die Berufsausübungsfreiheit. Das Grundgesetz sieht vor, dass die Berufsausübungsfreiheit beschränkt werden kann. Ein Eingriff ist danach allerdings an eine gewisse Form gebunden.

Art. 12 Abs. 1 Satz 2 GG besagt, dass die *„Berufsausübung […] durch Gesetz oder auf Grund eines Gesetzes geregelt werden [kann]"*.[600] Damit ordnet das Grundgesetz einen Gesetzesvorbehalt an.[601] Ein Eingriff in die Berufsfreiheit muss daher auf einem formellen (Parlaments)-Gesetz beruhen. Der Eingriff kann entweder direkt auf dieser Ebene angeordnet werden, oder in manchen Fällen auch durch untergesetzliche Normen wie Rechtsverordnungen und Satzungen, wenn denn diese auf eine formell-gesetzliche Ermächtigung zurückgehen. Diesem Grundsatz wird auch ein Ansatz gerecht,[602] Maßnahmen der

---

[598] *Kämmerer* in: v. Münch/Kunig, Grundgesetz Bd. 1, 7. Aufl. 2021, Art. 12 Rn. 89.

[599] *v. Coelln* in: Gröpl u.a., Grundgesetz, Vbm. Grundrechte Rn. 101 f.

[600] Nach h.M. erstreckt sich dieser Gesetzesvorbehalt auch auf Regelungen der Berufswahl, bei der Beschränkung auf die Berufsausübung handele es sich um ein Redaktionsversehen. Vgl. BVerfG, Beschl. v. 19.07.2000, 1 BvR 539/96, Spielbankgesetz Baden-Württemberg, BVerfGE 102, 197 (213); BVerfG, Urt. v. 28.03.2006, 1 BvR 1054/01, Sportwettenmonopol, BVerfGE 115, 276 (303 f.); *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 12 Rn. 27; *Kämmerer* in: v. Münch/Kunig, Grundgesetz Bd. 1, 7. Aufl. 2021, Art. 12 Rn. 78.

[601] Der Vorbehalt des Gesetzes, wie er nach dem nationalen Verfassungsrecht gilt, gilt im Übrigen auch für die Beurteilung mitgliedstaatlicher Umsetzungsakte des Unionsrechts anhand des Vorbehalts des Gesetzes, wie ihn die Charta der Grundrechte der Europäischen Union in Art. 52 Abs. 1 Satz 1 Charta vorschreibt (Gemäß Art. 52 Abs. 1 Satz 1 Charta muss *„jede Einschränkung der Ausübung der in [der] Charta anerkannten Rechte und Freiheiten […] gesetzlich vorgesehen sein"*). Dies gilt jedenfalls dann, wenn der Mitgliedstaat gewisse Mindeststandards bezüglich der formellen Beschaffenheit des einschränkenden Gesetzes einhält. Damit besteht insoweit ein weitestgehender Gleichlauf bezüglich der formellen Anforderungen des europäischen wie des mitgliedstaatlichen Grundrechtsregimes an ein Gesetz, das Art. 12 Abs. 1 GG bzw. Art. 16 Charta einschränkt.

[602] BGH, Urt. v. 26.11.2015, I ZR 3/14, 3dl.am. Vgl. BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82.

DVR auf Grundlage der Störerhaftung anzuordnen, da die Störerhaftung sich immerhin von den zivilrechtlich normierten negatorischen Ansprüchen ableitet.[603]

4. Schranken-Schranken

Als Schranken-Schranken hat der Normgeber insbesondere das Verbot des Einzelfallgesetzes, Art. 19 Abs. 1 Satz 1 GG, das Gebot, das eingeschränkte Grundrecht im einschränkenden Gesetz zu zitieren (Zitiergebot), Art. 19 Abs. 1 Satz 2 GG, das Verbot, ein Grundrecht in seinem Wesensgehalt anzutasten (Wesensgehaltsgarantie), Art. 19 Abs. 2 GG, den Bestimmtheitsgrundsatz, den Vorbehalt des Gesetzes und den Schutz des erzeugten Vertrauens zu beachten.

Die bedeutendste Rechtfertigungsschranke ist allerdings der Grundsatz der Verhältnismäßigkeit.[604] Gesetzliche Normen, die Grundrechte einschränken, dürfen nicht gegen das Übermaßverbot verstoßen. Ein Eingriff in ein Grundrecht, der nicht verhältnismäßig ist, ist selbst dann verfassungswidrig, wenn die ausdrücklich im Grundgesetz angelegten Schranken der Grundrechte beachtet wurden. Die dogmatische Grundlage des Verhältnismäßigkeitsgrundsatzes wird teilweise in Art. 19 Abs. 2 GG gesucht,[605] teilweise im Rechtsstaatsprinzip.[606] Ein Eingriff in ein Grundrecht ist dann verhältnismäßig, wenn dieser einem legitimen Zweck dient und zur Erreichung dieses Zwecks geeignet, erforderlich und angemessen ist.[607]

a. Legitimer Zweck

Ein Eingriff in den Schutzbereich eines Grundrechts kann nur dann verhältnismäßig sein, wenn dieser Eingriff einem legitimen Zweck dient, hinter dem die Beschränkung dieses Grundrechts zurückstehen muss. Der Eingriff in die Berufsfreiheit durch datenverkehrsregulierende Maßnahmen ist daher nur dann verhältnismäßig, wenn mit den Maßnahmen ein legitimer Zweck verfolgt wird.[608] Nicht jedes Grundrecht kann zur Erreichung jedes beliebigen Zieles eingeschränkt werden. Grundsätzlich verlangt das Übermaßverbot des Grundgesetzes, dass das zu erreichende Ziel in einem angemessenen Verhältnis zur Wertigkeit des Grundrechts und der Intensität des Eingriffs steht. Die Ziele, die eine Rechtfertigung des Eingriffs in ein Grundrecht erlauben, sind daher von Grundrecht zu Grundrecht unterschiedlich. Legitime Ziele lassen sich teilweise aus den jeweiligen Schrankenregelungen des Grundgesetzes ableiten. Dies ist etwa bei Art. 5 Abs. 2 GG der Fall, der Eingriffe in die Grundrechte des Art. 5 Abs. 1 GG unter anderem zu Zwecken des Ehr-

---

[603] Zur Herleitung der Störerhaftung siehe oben Kap. 3 II 1 b) (4) (S. 134). Zum weitergehenden Problem des Vorbehalts des Parlamentsgesetzes siehe unten Kap. 3 V (S. 217 ff.).
[604] Vgl. *Sachs* in: Sachs, Grundgesetz, Vor Art. 1 Rn. 134 f.
[605] *Krebs* in: v. Münch/Kunig, Grundgesetz Bd. 1, 6. Aufl. 2012, Art. 19 GG Rn. 25.
[606] BVerfG, Beschl. v. 03.06.1992, 2 BvR 1041/88, 2 BvR 78/89, BVerfGE 86, 288 (346 f.); BVerfG, Beschl. v. 05.03.1968, 1 BvR 579/67, Zeugen Jehovas, BVerfGE 23, 127 (133 f.); *Grzeszick* in: Maunz/Dürig, Art. 20 GG, VII Rn. 108 (Stand: 57. Erg.-Lfg., Januar 2010); *Sachs* in: Sachs, Grundgesetz, Art. 20 GG Rn. 146.
[607] BVerfG, Beschl. v. 16.03.1971, 1 BvR 52/66, 1 BvR 665/66, 1 BvR 667/66, 1 BvR 754/66, Erdölbevorratung, BVerfGE 30, 292 (316 f.); *Badura*, Staatsrecht, C 2 (Rn. 28).
[608] *Hufen*, Staatsrecht II, § 9 III 3 (Rn. 19).

und des Jugendschutzes erlaubt.[609] Ist jedoch in den Grundrechtsschranken kein spezifischer Zweck bestimmt, der zum Eingriff berechtigt, sind grundsätzlich alle Aufgaben des Staates legitime Zwecke.[610]

Das Bundesverfassungsgericht hat allerdings aus den Grundrechten und dem Verhältnismäßigkeitsgrundsatz weitere Voraussetzungen an die legitimen Ziele zur Einschränkung mancher Grundrechte formuliert. Den Rahmen für die Zwecke, zu deren Erreichung die Berufsfreiheit eingeschränkt werden darf, hat das BVerfG etwa mit der sogenannten Drei-Stufen-Theorie vorgegeben: Da das Verbot, einen Beruf auszuüben, die Freiheit der Bürger (und Unternehmen) aus abstrakter Perspektive intensiver einschränkt als Vorschriften, die lediglich die Art und Weise der Berufstätigkeit ausgestalten, sind Eingriffe in die Berufsausübung aus weniger gewichtigen Gründen einschränkbar als Eingriffe in die Berufswahl bzw. Berufsergreifung.[611]

Im Gegensatz zu objektiven[612] und subjektiven[613] Berufswahlregelungen sind nach der Drei-Stufen-Theorie des Bundesverfassungsgerichts Einschränkungen der Berufsfreiheit durch Berufsausübungsregelungen bereits dann zu rechtfertigen, wenn die fragliche Regelung vernünftigen Erwägungen des Allgemeinwohls dient.[614]

Die Durchsetzung des Urheberrechts – jedenfalls soweit es die Verhinderung illegalen Filesharings betrifft – dient in erster Linie der Verwirklichung der Eigentumsgarantie des

---

[609] *Ipsen*, Staatsrecht II, § 3 III 2 a) (Rn. 186).
[610] *Hufen*, Staatsrecht II, § 9 III 3 (Rn. 19); *Ipsen*, Staatsrecht II, § 3 III 2 b) (Rn. 187).
[611] Zugleich müssen an die Dringlichkeit objektiver Beschränkungen der Berufsfreiheit strengere Maßstäbe angelegt werden als an subjektive Beschränkungen, da der Eingriff bei objektiven Beschränkungen wiederum intensiver ist; vgl. BVerfG, Urt. v. 11.06.1958, Apotheker-Urteil, BVerfGE 7, 377 (406).
[612] Objektive Einschränkungen der Berufswahl sind nur zulässig, wenn sie für den Schutz überragend wichtiger Gemeinschaftsgüter, die abstrakt höherrangig als die Freiheit des Einzelnen zu bewerten sind, vor nachweisbaren oder höchstwahrscheinlichen Gefahren zwingend geboten sind. Siehe dazu BVerfG, Urt. v. 11.06.1958, Apotheker-Urteil, BVerfGE 7, 377 (406); BVerfG, Beschl. v. 18.12.1968, 1 BvL 5/64, 1 BvL 14/64, 1 BvL 5/65, 1 BvL 11/65, 1 BvL 12/65, Mühlengesetz, BVerfGE 25, 1 (11 f.); BVerfG, Beschl. v. 05.05.1987, 1 BvR 981/81, BVerfGE 75, 284 (296); BVerfG, Beschl. v. 19.07.2000, 1 BvR 539/96, Spielbankgesetz Baden-Württemberg, BVerfGE 102, 197 (214 f.); *Kingreen/Poscher*, § 21 II 3 (Rn. 984).
[613] Einschränkungen der Berufsfreiheit durch subjektive Berufswahlregelungen sind nur zu rechtfertigen, wenn der Allgemeinheit ansonsten durch die Ausübung des Berufs Gefahren drohen würden. Der mit subjektiven Beschränkungen der Berufswahl verfolgte Zweck darf daher zur ordnungsgemäßen Erfüllung der Berufstätigkeit nicht außer Verhältnis stehen. Dazu BVerfG, Urt. v. 11.06.1958, Apotheker-Urteil, BVerfGE 7, 377 (406 f.); BVerfG, Beschl. v. 18.11.1980, 1 BvR 228/73, 1 BvR 311/73, BVerfGE 55, 185 (196); BVerfG, Beschl. v. 12.03.1985, 1 BvL 25/83, 1 BvL 45/83, 1 BvL 52/83, Steuerberaterprüfung, BVerfGE 69, 209 (218); BVerfG, Beschl. v. 20.03.2001, 1 BvR 491/96, Altersgrenze für Kassenärzte, BVerfGE 103, 172 (183); *Ipsen*, Staatsrecht II, § 15 III 1 (Rn. 662); *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 12 GG Rn. 46.
[614] BVerfG, Urt. v. 11.06.1958, Apotheker-Urteil, BVerfGE 7, 377 (406); BVerfG, Urt. v. 29.11.1961, 1 BvR 760/57, Ladenschlussgesetz II, BVerfGE 13, 237 (240); BVerfG, Urt. v. 30.07.2008, 1 BvR 3262/07, 1 BvR 402/08, 1 BvR 906/08, Rauchverbot, BVerfGE 121, 317 (346); *Ipsen*, Staatsrecht II, § 15 III 2 a) (Rn. 673).

Art. 14 Abs. 1 GG. Beim Urheberrecht handelt es sich um Eigentum im verfassungsrechtlichen Sinne.[615] Die Durchsetzung des Urheberrechts hilft zudem auch der Durchsetzung der Rechtsordnung und der Funktionsfähigkeit des Marktes für geistige und kulturelle Werke.[616] Bei der Durchsetzung des Urheberrechts handelt es sich daher um eine vernünftige Erwägung des Allgemeinwohls, so dass zu diesem Zweck die Berufsausübungsfreiheit grundsätzlich in legitimer Weise eingeschränkt werden kann.[617]

b. Geeignetheit

Eine Datenverkehrsregulierung müsste zur Durchsetzung des Urheberrechts auch geeignet sein. Nach der Rechtsprechung des Bundesverfassungsgerichts ist eine Maßnahme bereits dann zur Erreichung eines legitimen Zwecks geeignet, wenn der Erfolg, der mit der Maßnahme erreicht werden soll, *„gefördert werden kann"*.[618] Dabei genügt es, wenn die Erreichung des Zwecks möglich ist. Auch ist es nicht notwendig, dass der Erfolg in jedem Einzelfall und vollständig eintritt.[619] Dem Gesetzgeber steht zudem eine weite Einschätzungsprärogative zu, welche Maßnahmen er als geeignet ansieht und welche nicht.[620]

Um diesem Maßstab gerecht zu werden, müsste eine DVR also wenigstens potentiell dazu geeignet sein, die Durchsetzung des Urheberrechts zu fördern. Insbesondere wäre es nicht notwendig, das Urheberrecht mit der DVR flächendeckend und in jedem Einzelfall durchzusetzen.

---

[615] BVerfG, Beschl. v. 07.07.1971, 1 BvR 765/66, Schulbuchprivileg, BVerfGE 31, 229 (239); *Grzeszick*, ZUM 2007, 344 (344); *P. Kirchhof*, Der verfassungsrechtliche Gehalt des geistigen Eigentums, in: FS Zeidler, S. 1639 (1653); *Ohly*, JZ 2003, 545 (546); *Paulus/Wesche*, ZGE 2010, 385 (389).

[616] *Bisges*, ZUM 2014, 930 (932 ff.); *Kirchner*, GRUR Int. 2004, 603 (605).

[617] A.A. ist (bezogen auf eine DVR mittels Deep Packet Inspection) *Schnabel*, MMR 2008, 281 (284) mit dem Argument, dass es an einem legitimen Zweck fehle, da Art. 14 GG zwar die vermögenswerten Elemente des Urheberrechts schütze, indem dieser die Ergebnisse der schöpferischen geistigen Arbeit ihrem Urheber zuordnen würde. Nicht jede denkbare Verwertungsmöglichkeit sei hingegen durch das Grundgesetz gesichert. Während letzterem grundsätzlich zugestimmt werden kann, so vergisst *Schnabel* an dieser Stelle andererseits eine Differenzierung danach, ob ein bestimmtes Geschäftsmodell, das auf der Verwertung des Urheberrechts aufbaut, in der Abwägung mit anderen rechtlich relevanten Interessen geschützt werden darf oder muss. Der Staat hat nicht die Aufgabe, den Schutz des Art. 14 GG gegen andere Grundrechte durchzusetzen, koste es, was es wolle. Dem Staat ist es jedoch auch nicht grundsätzlich verwehrt, konkrete Geschäftsmodelle zu schützen, wenn diese der Verwirklichung der Grundrechte dienen. Dies muss dem Gesetzgeber grundsätzlich möglich sein, zumal in dem normativ geprägten grundrechtlichen Bereich des Art. 14 GG, und ist daher auch nicht illegitim. Die Abwägung mit anderen grundrechtlich geschützten Interessen ist dogmatisch dann in den späteren Stufen der Verhältnismäßigkeitsprüfung zu verorten.

[618] BVerfG, Beschl. v. 16.03.1971, 1 BvR 52/66, 1 BvR 665/66, 1 BvR 667/66, 1 BvR 754/66, Erdölbevorratung, BVerfGE 30, 292 (316).

[619] BVerfG, Beschl. v. 18.07.2005, 2 BvF 2/01, Risikostrukturausgleich, BVerfGE 113, 167, Rn. 174; BVerfG, Urt. v. 28.03.2006, 1 BvR 1054/01, Sportwettenmonopol, BVerfGE 115, 276, (308 f.); vgl. auch EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 63.

[620] Vgl. *Sachs* m.w.N. in: Sachs, Grundgesetz, Art. 20 Rn. 151.

Auf die Effektivität der Datenverkehrsregulierung im Hinblick auf eine verbesserte Durchsetzung des Urheberrechts wurde im Rahmen dieser Arbeit bereits weiter oben eingegangen.[621] Insbesondere die IP-Sperre und die DNS-Sperre sind nur eingeschränkt dazu fähig, die massenweise Verletzung von Urheberrechten über das Internet zu verhindern.[622] Ein DPI-Filtersystem hingegen ist potentiell hochgradig effektiv bei der Durchsetzung des Urheberrechts, selbst bei technisch erfahrenen Nutzern.[623]

Neben sicherlich vorhandenen technischen Schwächen der unterschiedlichen Formen der Datenverkehrsregulierung darf nicht außer Acht gelassen werden, dass Situationen denkbar sind, in denen auch IP- und DNS-Sperren eine gewisse Mindesteffektivität beweisen. Der Nutzer, der ein gefiltertes Angebot aufruft und sich durch die Konfrontation mit der Sperrmaßnahme mit seinem vermeintlichen Fehlverhalten auseinandersetzen muss, könnte einsichtig werden und sich von seinem Vorhaben zurückziehen.[624] Eine weitere Möglichkeit besteht darin, dass es für den Nutzer zwar Umgehungsmöglichkeiten gibt, die ihm auch bekannt sind und die er anzuwenden weiß, ihm der Aufwand aber letztlich als zu groß erscheint.[625]

Offensichtlich gänzlich nutzlos zur Förderung des Ziels der Urheberrechtsdurchsetzung ist daher keines der in Frage kommenden Instrumente. Somit sind die Maßnahmen der Datenverkehrsregulierung im Ergebnis zur Durchsetzung des Urheberrechts im verfassungsrechtlichen Sinn geeignet.[626] Zwar sind Zweifel an der Effektivität gewisser Maßnahmen der Datenverkehrsregulierung in quantitativer Hinsicht nicht von der Hand zu

---

[621] Vgl. oben Kap. 1 IV 3–5 (S. 37 ff.).

[622] LG Kiel, Urt. v. 23.11.2007, 14 O 125/07, CR 2008, 126 (127); *LG Hamburg*, Urt. v. 12.03.2010, 308 O 640/08, CR 2010, 534 (537). Wenn das Gericht hier allerdings davon spricht, die Sperrmaßnahmen seien nicht „hinreichend geeignet", um dem ISP die Einrichtung der Sperrmaßnahmen zuzumuten, ist damit nicht die „Geeignetheit" im verfassungsrechtlichen Sinn gemeint, vielmehr wird an jener Stelle eine Interessenabwägung vorgenommen (dies jedoch im verfassungsrechtlichen Sinne interpretierend wohl *Heliosch*, Sperrmaßnahmen im Internet, S. 91); *Höhne*, jurisPR-ITR 2010 Anm. 2, III 1, abrufbar unter: https://www.juris.de/perma?d=jpr-NLITADG000310 (zuletzt besucht am 09.10.2021); *J. Kahl*, SächsVBl. 2010, 180 (188 f.); *Moos/Gosche*, K&R 2009, 275 (275).

[623] So erlauben die Filtermaßnahmen unter Zuhilfenahme der Deep Packet Inspection ein hohes Maß an Zielgenauigkeit und ein ebenso hohes Maß an Intensität und Ausmaß der Durchsetzung, während gleichzeitig aktive Umgehungsmaßnahmen vergleichsweise umständlich und nicht vor Gegenmaßnahmen des Regulierers gefeit sind. IP- und/oder DNS-Sperren hingegen sind relativ leicht zu umgehen; auch dies erfordert jedoch ein aktives Tun des Empfängers oder des Verbreiters der geschützten Güter.

[624] *Sieber/Nolde*, Sperrverfügungen, S. 197; *Faber*, Jugendschutz im Internet, S. 179.

[625] Ähnlich *Heliosch*, Sperrmaßnahmen im Internet, S. 100 in Bezug auf gesperrte kinderpornographische Inhalte.

[626] So auch BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 45 ff. *J. Kahl*, SächsVBl. 2010, 180 (188); *Spindler*, GRUR 2016, 451 (454); a.A.: *Stadler*, Haftung für Informationen, S. 188 ff.; *Stadler*, Internetsperren: EuGH lässt Provider mit der Verantwortung allein, 2013, abrufbar unter http://www.lto.de/recht/hintergruende/h/eugh-urt-c-314-12-internetsperren-gerichte/ (zuletzt besucht am 09.10.2021); zweifelnd: *Schnabel*, MMR 2008, 281 (284).

weisen, diese sind jedoch tendenziell eher bei der Frage nach der Angemessenheit des Eingriffs zu berücksichtigen.[627]

c. Erforderlichkeit

Eine Datenverkehrsregulierung muss zudem auch erforderlich sein, um das Regulierungsziel zu erreichen. Erforderlich ist eine Maßnahme im verfassungsrechtlichen Sinn, wenn der Staat aus allen gleich gut geeigneten Mitteln, die ihm zur Erreichung des Ziels zur Verfügung stehen, das mildeste, also das die Berufsfreiheit schonendste Mittel wählt.[628] Damit eine grundsätzlich geeignete Maßnahme nicht erforderlich ist, muss also eine alternative Maßnahme bestehen, die die Wahrscheinlichkeit des Erfolges unzweifelhaft in gleichem Maße steigert.[629] Eine Maßnahme ist allerdings auch dann erforderlich, wenn eine Alternativmaßnahme den Regelungsadressaten weniger belastet, damit aber eine höhere Belastung für Dritte oder die Allgemeinheit einhergeht.[630] Generell gilt im Rahmen der Erforderlichkeit, dass dem Gesetzgeber ein weiter Einschätzungsspielraum zur Verfügung steht, welche Maßnahme er für erforderlich erachtet. Eine Maßnahme ist also bereits dann erforderlich, wenn nicht mit Sicherheit feststeht, dass die Regelungsalternative den Regulierungszweck gleichwertig erreicht.[631]

Um das Urheberrecht im Internet durchzusetzen, sind grundsätzlich eine Vielzahl an Maßnahmen denkbar, insbesondere auch solche, die nicht in den Datenverkehr eingreifen.

---

[627] Im Ergebnis trotz unglücklicher Wortwahl wohl auch *LG Hamburg*, Urt. v. 12.03.2010, 308 O 640/08, CR 2010, 534, (537); a.A. *Schnabel*, JZ 2009, 996 (1000), der diese Frage auf der Stufe der Geeignetheit prüfen will.

[628] BVerfG, Beschl. v. 14.03.1989, 1 BvR 1033/82, 1 BvR 174/84, Multiple-Choice-Verfahren, BVerfGE 80, 1 (29 f.); BVerfG, Urt. v. 30.07.2008, 1 BvR 3262/07, 1 BvR 402/08, 1 BvR 906/08, Rauchverbot, BVerfGE 121, 317 (354); BVerfG, Urt. v. 06.12.2016, 1 BvR 2821/11, 2 BvR 321/12, 2 BvR 1456/12. BVerfGE 143, 246, Rn. 289.

[629] BVerfG, Beschl. v. 06.10.1987, 1 BvR 1086/82, 1 BvR 1468/82, 1 BvR 1623/82, Arbeitnehmerüberlassung, BVerfGE 77, 84 (109); BVerfG, Beschl. v. 18.12.1968, 1 BvL 5/64, 1 BvL 14/64, 1 BvL 5/65, 1 BvL 11/65, 1 BvL 12/65, Mühlengesetz, BVerfGE 25, 1 (19 f.); *Sachs* in: Sachs, Grundgesetz, Art. 20 Rn. 152.

[630] BVerfG, Beschl. v. 06.10.1987, 1 BvR 1086/82, 1 BvR 1468/82, 1 BvR 1623/82, Arbeitnehmerüberlassung, BVerfGE 77, 84 (106 f.); BVerfG, Beschl. v. 14.11.1989, 1 BvL 14/85, 1 BvR 1276/84, Mietwagenunternehmer, BVerfGE 81, 70 (90 ff.); *Hillgruber* in: Isensee/P. Kirchhof, HStR IX, § 201 Rn. 64; *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 20 Rn. 119; *Grzeszick* in: Maunz/Dürig, Art. 20 GG, VII Rn. 114 (Stand: 48. Erg.-Lfg., November 2006).

[631] Ständige Rechtsprechung: BVerfG, Beschl. v. 16.03.1971, 1 BvR 52/66, 1 BvR 665/66, 1 BvR 667/66, 1 BvR 754/66, Erdölbevorratung, BVerfGE 30, 292 (319); BVerfG, Beschl. v. 14.11.1989, 1 BvL 14/85, 1 BvR 1276/84, Mietwagenunternehmer, BVerfGE 81, 70 (90); BVerfG, Beschl. v. 05.02.2002, 2 BvR 305/93, 2 BvR 348/93, Sozialpfandbrief, BVerfGE 105, 17 (36); *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 20 Rn. 123.

Dazu gehören, um nur einige zu nennen, straf- und zivilrechtliche Abschreckungsmaßnahmen (z.B. die Abmahnung von Urheberrechte verletzender Nutzer;[632] die strafrechtliche Verfolgung von Anbietern urheberrechtswidriger Internet-Angebote[633]), Öffentlichkeitsarbeit, um Nutzer für die Bedeutung des Urheberrechts zu sensibilisieren,[634] oder das Löschen urheberrechtsverletzender Angebote.[635]

Diese Maßnahmen werden allerdings bereits ergriffen und stehen überwiegend nicht in einem alternativen Verhältnis zu einer Datenverkehrsregulierung, sondern sind zusätzlich einsetzbar. Im Übrigen sind andere Maßnahmen lediglich eingeschränkt effektiv, konnten sie doch bislang die massenhafte Verletzung von Urheberrechten im Internet nicht stoppen.[636] Vielmehr stellt sich die Frage, ob datenverkehrsregulierende Maßnahmen zusätzlich zu den bereits ergriffenen Maßnahmen eingeführt werden sollten. Wie oben festgestellt, sind Eingriffe in den Datenverkehr durchaus förderlich zur Durchsetzung des Urheberrechts im Vergleich zum *status quo*. Datenverkehrsregulierung ersetzt im Wesentlichen keine bereits eingeführten Maßnahmen, sondern versucht, das Problem an einem anderen Ansatzpunkt anzugehen.[637]

(1) Löschung urheberrechtswidriger Angebote im World Wide Web

Eine tatsächlich mit der DVR in der Wirkungsweise vergleichbare Maßnahme könnte die Löschung illegaler Angebote von den Servern der Host-Provider sein. Die Löschung eines Angebots soll hier definiert sein als die vollständige, dauerhafte und ersatzlose Entfernung seines Inhalts von den Servern eines konkreten Host-Providers.[638]

Betrachtet man die Art, wie Datenverkehrsregulierung das Urheberrecht schützen soll, dann stellt sie eine tatsächliche Unterbrechung des Datenverkehrs zwischen Anbieter und Nutzer dar. Eine solche Maßnahme, die jedoch nicht in den Datenverkehr eingreift, sondern das Problem an seiner Wurzel angeht, stellt auch die Löschung des illegalen Ange-

---

[632] Vgl. *Brüggemann*, MMR 2013, 278 (278); *Frey*, ZUM 2014, 554 (555); instruktiv zur Rechtslage in Deutschland: *J. B. Nordemann/Olaf Wolters*, ZUM 2014, 25 (25).

[633] *Norrie*, Anhörung in Neuseeland: Kim Dotcom wehrt sich gegen Auslieferung, in: SPIEGEL ONLINE, 29.08.2016, abrufbar unter https://www.spiegel.de/netzwelt/web/anhoerung-in-neuseeland-dotcom-wehrt-sich-gegen-auslieferung-a-1109396.html (zuletzt besucht am 09.10.2021).

[634] Vgl. *Sieber/Nolde*, Sperrverfügungen, S. 197 f.

[635] *Danaher/Smith*, IJIO 2014, 1 (2); *Fowler u.a.*, U.S. Shuts Offshore File-Share „Locker", Wall Street Journal 2012, 2012, abrufbar unter http://www.wsj.com/articles/SB10001424052970204616504577171060611948408.

[636] *Danaher/Smith*, IJIO 2014, 1 (8).

[637] Nach dem Ansatz von *Lessig*, Code, S. 123 wird Verhalten durch (gesellschaftliche) Normen, Gesetze, den Markt und Architektur reguliert. Während sonstige Maßnahmen zur Durchsetzung des Urheberrechts bei den anderen Faktoren angesetzt haben, setzt DVR bei der Architektur des Netzes, seinem Code, an.

[638] *Degen*, Freiwillige Selbstkontrolle, S. 136 und *Heliosch*, Sperrmaßnahmen im Internet, S. 106 definieren die Löschung abweichend als dauerhafte Entfernung aus dem World Wide Web. Dies kann eine Löschungsanordnung, selbst wenn sie erfolgreich ist, allerdings nicht garantieren, da es von vielen Faktoren abhängt, ob ein Angebot auf dem Server eines anderen Hosting Providers wieder im WWW auftaucht.

bots beim Host-Provider dar. Ein gelöschtes Angebot müsste bzw. könnte nicht mehr Adressat einer Maßnahme der DVR sein, so dass beide Maßnahmen tatsächliche Alternativen darstellen. Daher verdient der Ansatz des Löschens hier eine vertiefte Betrachtung, ob er ein zumindest in gleicher Weise geeignetes, aber milderes Mittel darstellt.

Die Löschung eines Angebots von den Servern eines Host-Providers könnte gegenüber datenverkehrsregulierenden Maßnahmen ein milderes Mittel sein. Bei der Beurteilung, ob eine Maßnahme milder ist als eine andere, kann ein weites Spektrum an Argumenten herangezogen werden. Dieses umfasst beispielsweise die Anzahl der Betroffenen der Maßnahme,[639] die abstrakte Gewichtigkeit und Intensität der Grundrechtsbeeinträchtigung[640] sowie sonstige Nebenwirkungen.[641]

Besteht allerdings ein mehrpoliges Rechtsverhältnis, werden also durch eine Maßnahme unterschiedliche Rechtsgüter oder Rechtsgüter mehrerer Personen betroffen, muss die Alternativmaßnahme für jede der kollidierenden Positionen einen positiven Effekt bewirken. Ist letzteres nicht der Fall, ist die Maßnahme erforderlich. Die Abwägung und Gewichtung der Vor- und Nachteile der zu prüfenden Maßnahme und die Beantwortung der Frage, ob dies zu einer Verfassungswidrigkeit des Regelungsvorhabens führt, sind unter dem Prüfungspunkt der Angemessenheit, nicht der Erforderlichkeit der Maßnahme vorzunehmen.[642]

Vergleicht man die verschiedenen Maßnahmen, mit denen Urheberrechtsverletzungen im Internet mittels Eingriffen in den Datenverkehr verhindert werden können, mit der Löschungsanordnung gegen den Host-Provider, welcher das urheberrechtswidrige Angebot bereitstellt, so ist der Eingriff in die Grundrechte bei der Löschungsanordnung in mancherlei Hinsicht weniger intensiv. So stellt es sich jedenfalls bezüglich der noch eingehender zu prüfenden Informationsfreiheit gemäß Art. 5 Abs. 1 Satz 1 GG dar.[643]

Die Löschung eines Angebots ist erheblich zielgenauer als insbesondere die IP-Sperre, die stark mit dem Problem des Overblockings zu kämpfen hat.[644] Der Host-Provider kann den Bereich seines Servers, auf dem das illegale Angebot liegt, gezielt löschen. Andere Anbieter, die ihr Angebot unter derselben IP-Adresse gespeichert haben, sind von so der Maßnahme nicht betroffen. Anders verhält es sich bei einer IP-Sperre. Da auch Löschungsanordnungen gegen Content Provider in Frage kommen, ist es bei dieser Form der Regulierung sogar möglich, ein Angebot, das teils legale, teils illegale Inhalte mit dem Netz teilt, online zu lassen und lediglich die Löschung der illegalen Anteile zu veranlassen.[645] Auch

---

[639] *Grzeszick* in: Maunz/Dürig, Art. 20 GG, VII Rn. 115 (Stand: 48. Erg.-Lfg., November 2006).
[640] *Michael*, JuS 2001, 148 (149).
[641] *Sachs* in: Sachs, Grundgesetz, Art. 20 Rn. 152 m.w.N.; *Voßkuhle*, JuS 2007, 429.
[642] BVerfG, Beschl. v. 14.03.2006, 1 BvR 2087/03, 1 BvR 2111/03, Geschäfts- und Betriebsgeheimnisse, BVerfGE 115, 205 (233 f.); *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 20 Rn. 119; a.A. *Sachs* in: Sachs, Grundgesetz, Art. 20 Rn. 154.
[643] Vgl. unten Kap. 3 III 4 (S. 175).
[644] Siehe oben S. 93 f.
[645] Ähnlich auch *Heliosch*, Sperrmaßnahmen im Internet, S. 107 f.

die Privatsphäre der Nutzer ist bei Löschungen urheberrechtsverletzender Angebote nicht betroffen.

Ein milderes Mittel ist die Löschung illegaler Angebote auf den ersten Blick auch hinsichtlich der Berufsausübungsfreiheit. Da bei einer Löschungsanordnung keine belastende Maßnahme gegen den Internet Service Provider ergeht, ist dessen Berufsfreiheit erkennbar nicht mehr betroffen. Es liegt jedoch spiegelbildlich ein Eingriff in die Berufsausübungsfreiheit des Host-Providers vor; dieser mag im Vergleich einfacher zu rechtfertigen sein, da der Host-Provider, auch wenn er lediglich eine technische Dienstleistung erbringt (wie auch der Internet Service Provider), „tatnäher" als letzterer ist.[646]

Die Löschung eines Angebots ist im Hinblick auf den Aspekt, dass im Vergleich zur Datenverkehrsregulierung der Adressat der Maßnahme wechselt, nicht aus jeder Position betrachtet eine mildere.[647] Die Abwägung zwischen der Berufsausübungsfreiheit von ISPs und Host-Providern ist keine Frage der Erforderlichkeit, sondern der Angemessenheit der Datenverkehrsregulierung. Als Konsequenz scheitert die Erforderlichkeit einer DVR bereits deshalb nicht daran, dass illegale Angebote statt gesperrt auch gelöscht werden können.

Sehr viel deutlicher als bei der Frage nach dem milderen Mittel wird die Erforderlichkeit der Datenverkehrsregulierung bei der Frage der gleichen Effektivität des Löschungsansatzes. Die Löschung des illegalen Angebots müsste in zumindest gleicher Weise dazu geeignet sein, Urheberrechtsverletzungen zu verhindern.

Dieser von einigen Stimmen vertretene Standpunkt stützt sich auf das Argument, dass das rechtsverletzende Angebot bei einer Löschungsanordnung komplett entfernt wird, anstatt dass – wie es bei einer Datenverkehrsregulierung der Fall wäre – lediglich der Zugriff auf die rechtsverletzenden Inhalte erschwert werde.[648]

Rechtlich bedarf es zu einer Löschung einer Anordnung gegen den Host-Provider des Servers, auf dem das illegale Angebot bereitgestellt wird. Technisch ist die Umsetzung der Anordnung denkbar einfach: Der Host-Provider muss lediglich das Angebot von seinem Server löschen, was sich im Aufwand nicht erheblich vom Löschen einer Computer-Datei vom Heim-PC unterscheidet. Der Aufwand der Löschung ist also gering, und technische Umgehungsmaßnahmen der Nutzer laufen ins Leere. Es muss schließlich nicht bloß ein

---

[646] Der Hosting-Provider einen Vertrag über die öffentliche Bereitstellung mit dem Betreiber des illegalen Angebots geschlossen und partizipiert über seine Vergütung indirekt an den Einnahmen durch die Urheberrechtsverletzungen. Ein ISP steht in der Regel in keiner Vertragsbeziehung mit den gesperrten Content Providern.

[647] Anderer Ansicht ist insoweit *Heliosch*, Sperrmaßnahmen im Internet, S. 108. Danach sei die Angebotslöschung das mildere Mittel im Vergleich zu datenverkehrsregulierenden Maßnahmen.

[648] Für eine Übersicht zur zivilgesellschaftlichen und politischen Diskussion zur Verabschiedung des ZugErschwG *Heliosch*, Sperrmaßnahmen im Internet, S. 105 f. und *J. Kahl*, SächsVBl. 2010, 180 (189 f.) dort m.w.N.

Hindernis auf dem Weg zum Ziel umgangen werden, vielmehr ist das Ziel einer erfolgreichen Löschung nicht mehr existent.

Manches spricht allerdings gegen eine gleiche oder bessere Einschätzung der Effektivität von Lösch-Maßnahmen. So ist die räumliche Reichweite der effektiven Durchsetzung von Löschanordnungen begrenzt. Die Anordnung eines deutschen Gerichts oder einer deutschen Behörde, einen bestimmten Inhalt zu löschen, mag Autorität haben bei Host-Providern in Deutschland oder dem EU-Ausland, ebenfalls in Drittstaaten, die über entsprechende Verträge verpflichtet sind. Die Durchsetzung wird allerdings schwierig bis unmöglich, wenn der Host-Provider in einem Drittstaat – wie beispielsweise Russland – seinen Sitz hat. Eine effektive Vollstreckung ist nicht weltweit möglich. [649] Dabei liegt es in der Natur des Internets, dass der Standort des Servers, auf dem ein Angebot gespeichert und abrufbar ist, für die Erreichbarkeit ohne großen Belang ist. Anbieter illegaler Inhalte können daher ihre Inhalte auf Servern im rechtlich schwierig zu erreichenden Ausland speichern. Sie sind somit in der Theorie vor der Löschung ihrer Angebote relativ sicher.[650] Nicht zu vernachlässigen ist zudem die Tatsache, dass der Löschungsnsatz nur dann funktioniert, wenn das illegale Angebot auf dem Server eines Intermediärs liegt, nicht hingegen, wenn es über ein Peer-to-Peer-Netzwerk verbreitet wird.[651]

Ferner können die Anbieter der illegalen Angebote nach der Löschung ihres Angebots beim einen Host-Provider einfach zu einem anderen umziehen, mitsamt aller Inhalte und

---

[649] Daher trennt *J. Kahl*, SächsVBl. 2010, 180 (189) bei seinen Überlegungen zur verfassungsrechtlichen Erforderlichkeit von Netzsperren zwischen nationalen und internationalen Sachverhalten, da bei nationalen Sachverhalten der Grundsatz Löschen vor Sperren gehen müsse. Der Standort eines Servers im Internet ist für die angebotene Leistung jedoch irrelevant, so dass ein Content Provider, der von einer Löschungsanordnung betroffen ist, im Zweifel seinen Standort wechseln wird. Eine Differenzierung nach nationalen und internationalen Sachverhalten ist daher nicht sachdienlich, da der Anbieter illegaler Inhalte eine rein nationale Regulierung auf diese Weise einfach umgehen wird.

[650] Tatsächlich zeigt eine aktuelle Studie der Bundesregierung, Bericht über die im Jahr 2013 ergriffenen Maßnahmen zum Zweck der Löschung von Telemedienangeboten mit kinderpornografischem Inhalt im Sinne des § 184b des Strafgesetzbuchs, BT-Drs. 18/2590, dass Löschungsanfragen auch bei ausländischen Host-Providern durchaus in erstaunlichem Ausmaß Gehör finden und umgesetzt werden. Es ist allerdings fraglich, ob sich diese Faktenlage auf urheberrechtliche Sachverhalte uneingeschränkt übertragen lässt. Zum einen ist die Rechtslage bei Kinderpornografie weltweit sehr viel einheitlicher als bei Urheberrechtsverstößen. Zum anderen dürfte die moralische Ächtung von Kinderpornographie weltweit deutlich stärker ausfallen als diejenige von Urheberrechtsverstößen. Mit anderen Worten: Mit dem einen wird man auch ohne rechtlichen Druck keine Geschäfte machen wollen, beim anderen würde man es sich möglicherweise genau überlegen, ob man ohne Zwang auf Umsätze verzichten möchte.

[651] Aufgrund der dezentralen Struktur der Peer-to-Peer-Netzwerke sind die widerrechtlich geteilten Angebote teilweise auf einer unüberschaubaren Anzahl von Endgeräten gespeichert. Um eine effektive Löschung durchzuführen, müsste jede einzelne dieser Dateien zeitgleich gelöscht werden. Alle Dateien zeitgleich ausfindig zu machen, eine Löschungsanordnung zu erwirken und weltweit durchzusetzen ist jedoch praktisch nicht umsetzbar. Vgl. auch zum Parallelproblem bei IP- und DNS-Sperren oben Kap. 1 IV 3–4 (S. 37 ff.).

der Domain. Dies setzt allerdings voraus, dass die Content Provider eine lokale Sicherung ihres Angebots zu ihrer Verfügung haben.[652]

Im Vergleich mit der IP-Sperre ist das Löschen des Angebots also teils effektiver, teils jedoch nicht. Die IP-Sperre hat gegenüber dem Lösch-Ansatz den gewichtigen Vorzug, dass sie die Erreichbarkeit des Angebots auch dann erschwert, wenn der Server des Host-Providers im Ausland steht, während Löschungsverfügungen in diesem Fall wirkungslos bleiben können. Die Reichweite einer Löschung ist jedoch räumlich unbegrenzt, während die IP-Sperre lokal auf die an den ISP angeschlossenen Nutzer begrenzt bleibt. Sowohl die Löschungsverfügung als auch die IP-Sperre sind wirkungslos gegenüber illegalem *Filesharing* über Peer-to-Peer-Netzwerke, und beide Varianten sind anfällig gegen den Umzug des Anbieters mit seinem Angebot auf einen neuen Server. Bei der IP-Sperre deshalb, weil mit einem Server-Umzug gleichzeitig auch die IP-Adresse wechselt zu einer Adresse, die bislang nicht gesperrt ist. Bei der Löschung hingegen, weil keine Lösch-Verpflichtung für den neuen Host-Provider besteht.[653]

Weder die DNS-Sperre noch die Löschung des Angebots können etwas gegen *Filesharing* über Peer-to-Peer-Netzwerke ausrichten. Allerdings ist für die Wirksamkeit einer DNS-Sperre ein Server-Umzug des Content Providers unerheblich – im Gegensatz zur Löschung des Angebots. Andererseits gilt auch hier, dass – wenn die Löschung *endgültig* und *dauerhaft* gelingt – die Löschung des Angebots aus dem Netz naturgemäß effektiver ist als eine Sperre, die sich mit geringem Aufwand seitens des Nutzers umgehen lässt. Eine DNS-Sperre ist zudem (ähnlich wie die IP-Sperre) auf ein bestimmtes Gebiet beschränkt. Dies bedingt andersherum jedoch wieder den Vorteil der DNS-Sperre, dass diese in dem Rechtsgebiet durchgesetzt wird, in dem die Maßnahme verhängt wurde.

Vergleicht man die Effektivität einer Löschung mit der eines Filtersystems unter Verwendung von Deep Packet Inspection, bleiben wenig Vorteile hinsichtlich der Effektivität auf Seiten der Löschung des Angebots erkennbar. Im Wesentlichen besteht der Vorteil der Löschung darin, dass die Deep Packet Inspection in ihrer Wirkung auf die Netze beschränkt bleibt, in denen sie implementiert wurde, anstatt globale Wirkung wie eine Löschung zu entfalten. Die Deep Packet Inspection kann innerhalb ihres Einsatzgebietes – je nach betriebenem Aufwand – urheberrechtlich problematischen Datenverkehr annä-

---

[652] Vgl. *Heuner*, Sperrung des Zugangs zu kinderpornographischen Seiten im Internet, in: *Taeger/Wiebe*, Inside the Cloud, S. 107 (120) zu Erfahrungen nach der Löschung kinderpornografischer Angebote. Entgegen der Ansicht von *Heliosch*, Sperrmaßnahmen im Internet, S. 107 ist es beim Anbieten von Internet-Diensten üblich, dass der Content Provider wenigstens eine lokale (Offline-)Kopie des Angebots im eigenen Arbeitsbereich besitzt. Dies hat mehrere Gründe: Die lokale Kopie ermöglicht beispielsweise die unkomplizierte Überarbeitung des Angebots auch ohne Internet-Verbindung sowie den schnellen Wechsel des Host-Providers und stellt nicht zuletzt eine Sicherung gegen Datenverlust dar (sowohl bei einer beabsichtigten wie auch bei einer unbeabsichtigten Löschung des Angebots auf dem Server des Host-Providers).

[653] Zu bedenken ist allerdings der soeben diskutierte Einwand, dass der Content Provider kein Backup des illegalen Angebots besitzen könnte, womit ihm durch die Löschung auch die Möglichkeit eines Umzugs genommen wäre.

hernd flächendeckend filtern, und das unter Einbezug des Peer-to-Peer-Filesharings. Zudem funktioniert ein DPI-Filtersystem selbst dann, wenn der Content Provider sein illegales Angebot auf einem anderen Server unterbringt, da ein DPI-Filter unabhängig von der Quelle des Angebots den Datenverkehr kontrolliert. Schließlich ist ein DPI-Filtersystem auch nicht auf die Durchsetzung der Maßnahme durch Stellen in einem Drittland angewiesen.

Zusammenfassend lässt sich sagen, dass Löschungsmaßnahmen nicht in jeder Hinsicht und vor allen Dingen nicht evident in wenigstens gleicher Weise effektiv wie Maßnahmen der Datenverkehrsregulierung sind. Dies gilt in besonderer Weise im Vergleich zu DPI-Filtersystemen. Der Ansatz „*Löschen statt Sperren*" steht einer Erforderlichkeit der DVR daher nicht im Wege.

(2) Datenverkehrsregulierung durch den Staat

Weiterhin wäre daran zu denken, ob das Erfordernis der Erforderlichkeit staatlicher Maßnahmen nicht verlangt, dass der Staat die Datenverkehrsregulierung eigenständig durchführt, anstatt diese Aufgabe auf die Internet Service Provider abzuwälzen.

Aus Sicht eines Internet Service Providers stellt sich eine ausschließlich staatliche organisierte und durchgeführte Datenverkehrsregulierung, die den ISP vom organisatorischen und finanziellen Aufwand der DVR befreit, jedenfalls als milderes Mittel im Vergleich zu einer DVR dar, die er auf eigene Kosten und in eigener technischer Verantwortung zu tragen hätte.

Die europäischen Staaten haben sich allerdings seit Ende der 1980er Jahre aus dem öffentlichen Betrieb der Telekommunikationsnetze – und damit auch dem Betrieb des Internets – im Zuge der von der Europäischen Gemeinschaft vorangetriebenen Liberalisierungen und Privatisierungen der staatlichen Monopole weitgehend zurückgezogen.[654] Als Konsequenz fehlt es den staatlichen Institutionen an einem direkten Zugriff auf die Netzinfrastruktur.[655] Der Zurückerwerb der Netze durch den Staat würde zu immensen Kosten für den Steuerzahler führen. Eine Maßnahme, die zu erheblich höheren Ausgaben für den Steuerzahler führt, ist allerdings nach herrschender Meinung kein milderes Mittel.[656]

---

[654] Vgl. *Paulweber/Weinand*, EuZW 2001, 232 (233).

[655] Abgesehen von den Geheimdiensten, die die Netze an strategisch bedeutsamen Netzknoten abhören. Vgl. *Kaminski*, Wo lauscht der BND?, in Augsburger Allgemeine online, 2015, abrufbar unter https://www.augsburger-allgemeine.de/politik/Wo-lauscht-der-BND-id33960927.html, zuletzt besucht am 14.10.2020; Sauerbrey, NSA-Untersuchungsausschuss: BND lauscht bis heute bei der Telekom, 2014, abrufbar unter http://www.tagesspiegel.de/politik/nsa-untersuchungsausschuss-bnd-lauscht-bis-heute-bei-der-telekom/11075868.html. Dabei handelt es sich jedoch – soweit bekannt – um eine passive Infrastruktur, die Abhören erlaubt, den Datenverkehr jedoch nicht manipuliert.

[656] BVerfG, Beschl. v. 06.10.1987, 1 BvR 1086/82, 1 BvR 1468/82, 1 BvR 1623/82, Arbeitnehmerüberlassung, BVerfGE 77, 84 (110); BVerfG, Beschl. v. 13.06.2006, 1 BvL 9/00, 1 BvL 11/00, 1 BvL 12/00, 1 BvL 5/01, 1 BvL 10/04, Fremdrentengesetz, BVerfGE 116 (127); *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 20 Rn. 119.

Zudem wären die mit der Enteignung der Netzbetreiber, die ihre Telekommunikationsnetze nicht freiwillig verkaufen möchten, einhergehenden Eingriffe in deren durch Art. 14 GG garantierte Eigentumsfreiheit zu beachten.

(3) Kostentragung durch dritte Parteien

Denkbar wäre es jedoch, eine Datenverkehrsregulierung, die Internet Service Provider finanziell für ihren Aufwand bei der Durchführung der Maßnahmen schadlos stellt, als ein milderes, aber gleich geeignetes Mittel zu betrachten. Aus Sicht eines ISP ist dies selbstverständlich die ihn weniger belastende Institution gegenüber einer, in der er selbst die Kosten trägt. Auch ist kein Grund ersichtlich, weshalb die Kostentragung durch den Staat oder die Rechteinhaber gegenüber derjenigen durch die Bereitsteller der Infrastruktur die Effektivität einer Datenverkehrsregulierung nachteilig beeinflussen sollte. Auch hier gilt jedoch wie bereits soeben festgestellt, dass die Verlagerung von Kosten auf eine dritte Partei nicht isoliert aus der Perspektive des Betroffenen beurteilt werden kann. Eine Maßnahme ist eben nicht deshalb milder, weil die Kosten von der einen Person zur anderen verschoben werden.[657] Dies muss dann konsequenterweise nicht nur für die Kostenverlagerung zum Staat, sondern auch für eine Verlagerung auf private Dritte gelten. Die Möglichkeit, die Kosten einer DVR dem Staat oder den Rechteinhabern aufzuerlegen, führt folglich nicht dazu, dass eine Datenverkehrsregulierung, deren Kosten der Internet Service Provider tragen muss, nicht erforderlich wäre.[658]

(4) Wahlfreiheit der Mittel für ISPs

In der Folge der UPC-Entscheidung des Gerichtshofs[659] drängt sich eine weitere Frage auf, die hier im Rahmen der Erforderlichkeit erörtert werden muss: Ist die Anordnung einer datenverkehrsregulierenden Maßnahme milder, die dem Internet Service Provider unter gewissen Voraussetzungen[660] die Wahl überlässt, welche *konkrete* ihm zumutbare Maßnahme er zur Durchsetzung des Urheberrechts ergreift, als wenn ihm die *konkrete* Maßnahme vorgeschrieben wird?

Der EuGH ist jedenfalls genau dieser Ansicht. Der Wesensgehalt des Rechts auf unternehmerische Freiheit werde gerade deshalb von einer DVR nicht angerührt, weil der ISP die Hoheit über seine Mittel behalte und so die ihn am wenigsten belastende, effektive Maßnahme frei wählen könne.[661]

---

[657] Vgl. oben Kap. 3 II 4 c) (1) (S. 155).

[658] Die Frage des Kostenschuldners ist verfassungsrechtlich nicht irrelevant, es ist allerdings keine Frage der Erforderlichkeit. Es geht dabei vielmehr darum, für wen die Kostentragung *angemessen* ist.

[659] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192.

[660] Erste Voraussetzung ist die Effektivität der Maßnahme in Hinblick auf die Durchsetzung des Urheberrechts, zweite Voraussetzung die Gewährleistung der Informationsfreiheit der Internetnutzer. Vgl. EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 63 f. und 55 f.

[661] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 51 ff.

Der EuGH setzt sich bei dieser Feststellung allerdings nicht damit auseinander, dass diese Freiheit, die Mittel der DVR selbst wählen zu können, im Ergebnis dazu führen kann, dass der ISP das Risiko trägt, ein nicht ausreichend effektives Mittel gewählt zu haben – oder aber eines, das in rechtswidriger Weise in die Rechte Dritter eingreift. Die daraus resultierenden rechtlichen Haftungsrisiken sind eine zusätzliche Belastung des Providers. Vergleicht man die Vorteile der Freiheit der Mittel und die Nachteile der unüberschaubaren Haftungsrisiken, die die ISPs bei der eigenverantwortlichen Entscheidung eingehen, ob und welche Maßnahmen zur Urheberrechtsdurchsetzung sie im Einzelfall ergreifen, lässt sich nicht ohne weiteres feststellen, ob der eine Vorteil den anderen Nachteil aufwiegt. Weder die klare Vorgabe einer bestimmten DVR-Maßnahme noch die Überlassung der Entscheidung über die zu ergreifenden Mittel an die ISPs sind evident gegenüber dem anderen das mildere Mittel aus Sicht eines Internet Service Providers. Insoweit scheitert eine Erforderlichkeit der auf die eine oder die andere Weise ausgestalteten Anordnung nicht an dieser Frage. Es bleibt allerdings andererseits festzuhalten, dass der EuGH den ISPs mit der Gewährung dieser Freiheit ein vergiftetes Geschenk gemacht hat, das für die Provider neue Probleme schafft, die genauso schwer wiegen können wie die damit einhergehenden Erleichterungen.

d. Angemessenheit

Im Rahmen der Prüfung der Verhältnismäßigkeit von Eingriffen in den Datenverkehr zur Durchsetzung des Urheberrechts ist schließlich danach zu fragen, ob solche Maßnahmen unter Berücksichtigung der Einschränkungen, die damit für die Berufsausübungsfreiheit einhergehen, auch angemessen sind. Dies ist dann der Fall, wenn die Beeinträchtigungen durch die datenverkehrsregulierenden Maßnahmen bei einer umfassenden Gesamtbetrachtung der betroffenen Interessen zumutbar sind, da sie nicht außer Verhältnis zum damit verfolgten Zweck stehen.[662] Weder darf die Einschränkung übermäßig belastend sein, noch darf sie weiter gehen, als es die Gemeinwohlbelange, hier der Schutz der grundgesetzlichen Eigentumsgarantie, erfordern.[663]

Um diese Frage zu beantworten, sind die zu schützenden öffentlichen Belange den durch die Grundrechtseinschränkung des Bürgers verursachten Belastungen gegenüberzustellen. Je stärker das zu schützende öffentliche Interesse wiegt, umso größere Belastungen muss der Internet Service Provider tendenziell in Kauf nehmen.[664]

Bei abstrakter Betrachtung ist weder die Berufsausübungsfreiheit noch die Eigentumsfreiheit gemäß Art. 14 Abs. 1 GG höher zu gewichten. Bei beiden Grundrechten handelt es sich um solche, die einem Gesetzesvorbehalt unterliegen. Gemäß Art. 12 Abs. 1 Satz 2 GG kann die Berufsausübung durch Gesetz oder auf Grund eines Gesetzes geregelt werden, und auch Inhalt und Schranken des Eigentums werden gemäß

---

662 BVerfG, Beschl. v. 06.02.1979, 2 BvL 5/76, BVerfGE 50, 217 (226 f.); BVerfG, Beschl. v. 09.05.1989, 1 BvL 35/86, BVerfGE 80, 103, (107); *Grzeszick* in: Maunz/Dürig, Art. 20 GG, VII Rn. 117 (Stand: 48. Erg.-Lfg., November 2006); *Sachs* in: Sachs, Grundgesetz, Art. 20 Rn. 154.
663 BVerfG, Beschl. v. 15.12.1965, 1 BvR 513/65, BVerfGE 19, 342 (350 f.).
664 *Gröpl* in: Gröpl u.a., Grundgesetz, Art. 12 Rn. 69.

Art. 14 Abs. 1 Satz 2 GG durch die Gesetze bestimmt. Auch aus der systematischen Stellung im Grundgesetz lässt sich ein Vorrang weder des einen noch des anderen Grundrechts ableiten. Sowohl die Berufsausübungsfreiheit als auch die Eigentumsgarantie bilden als „Wirtschaftsgrundrechte“ die Pfeiler der Wirtschaftsordnung der Bundesrepublik und sind abstrakt gleichgewichtige Rechte. Beide erfüllen zudem nicht nur eine rein abwehrrechtliche Funktion, sondern sind ans Allgemeinwohl rückgekoppelt und daher nicht unbeschränkt gewährleistet.[665]

Neben der abstrakten Betrachtung ist auch und insbesondere in Augenschein zu nehmen, ob die geschützten öffentlichen Interessen im hier konkret gegebenen Fall die Eingriffe in die Berufsausübungsfreiheit überwiegen. Ist dies der Fall, so spricht dies dafür, dass eine Datenverkehrsregulierung durch einen ISP hinzunehmen ist, im umgekehrten Fall jedoch dagegen.[666]

Hier verstandenes Ziel einer DVR zur Urheberrechtsdurchsetzung ist es, Verletzungen des Urheberrechts an einem konkreten urheberrechtlich geschützten Werk insgesamt zu verringern, also nicht lediglich auf einen bestimmten Vorfall bezogen.[667] Diesem Anspruch werden die unterschiedlichen technischen Ansätze der DVR unterschiedlich gerecht.

IP-Sperren sind leicht zu umgehen und weisen erhebliche Schutzlücken auf, so dass ihre Effektivität gering ist.[668] Die konkrete Rechtsverletzung durch den gesperrten Anbieter wird erschwert und gegebenenfalls im Einzelfall verhindert, wenn der Nutzer keine Maßnahmen zur Umgehung der Sperre ergreift. Die Rechtsverletzungen am Schutzgut *insgesamt* werden durch die IP-Sperre allerdings kaum verhindert, sondern finden in der Regel einfach bei einem anderen Anbieter statt.[669]

Ähnliches gilt für die Technik der DNS-Sperren. Auch diese sind wenig effektiv im Hinblick auf das Regulierungsziel, da sie leicht zu umgehen sind und wie IP-Sperren nicht beim Inhalt, sondern beim rechtswidrigen Anbieter ansetzen.[670]

Die DVR mit dem Mittel der Deep Packet Inspection ist, wie oben dargelegt wurde, die mit Abstand effektivste der verfügbaren technischen Lösungen beim Schutz gegen Urheberrechtsverletzungen, da sie in der Lage ist, Urheberrechtsverletzungen an einem

---

[665] Für die Eigentumsfreiheit ist die Sozialbindung des Eigentums ausdrücklich in Art. 14 Abs. 2 GG normiert.
[666] BVerfG, Beschl. v. 13.06.2007, 1 BvR 1550/03, 1 BvR 2357/04, 1 BvR 603/05, Kontenabfrage, BVerfGE 118, 168 (195).
[667] Vgl. oben Kap. 1 IV 2 (S. 37).
[668] Peer-to-Peer-Filesharing kann beispielsweise nicht mit IP-Sperren geblockt werden.
[669] Vgl. dazu ausführlich oben Kap. 1 IV 3 (S. 37 ff.).
[670] Für eine detaillierte Untersuchung der Effektivität der DNS-Sperren vgl. oben Kap. 1 IV 4 (S.39 ff.).

Schutzgegenstand insgesamt und nicht nur im Hinblick auf eine konkrete Rechtsverletzung Einhalt zu gebieten. Zudem ist sie nur mit Mühen durch Anbieter und Nutzer zu umgehen.[671]

Das öffentliche Interesse an einer effektiven Erreichung der Regulierungsziele ist stärker zu gewichten als dasjenige an einer weniger effektiven Regulierung.[672] Nach dem soeben Gesagten muss ein Internet Service Provider bei einer Deep Packet Inspection grundsätzlich stärker belastende Eingriffe hinnehmen als bei IP- und DNS-Sperren.

Wie stark wird ein ISP also durch die unterschiedlichen technischen Sperrmaßnahmen in seiner Berufsausübungsfreiheit beschränkt? In erster Linie wird ein ISP durch die Kosten der Anschaffung, Einrichtung und des laufenden Betriebs des Sperrsystems belastet.[673] Bei den Kosten des laufenden Betriebs kommen zu den Kosten für Wartung, Strom und Reparaturen noch die Kosten für die inhaltliche Pflege des Sperrsystems hinzu, also die Kuratierung der gesperrten IP-Adressen, Domain-Namen und Dateisignaturen.[674]

Die Kosten eines ISP dürften sich für die unterschiedlichen Systeme erheblich unterscheiden. Vergleicht man lediglich IP- und DNS-Sperre, so dürfte wegen der größeren Notwendigkeit der häufigen Aktualisierung der gesperrten Adressen der Aufwand der Datenbankpflege bei der IP-Sperre erheblich über dem entsprechenden Aufwand bei einer DNS-Sperre liegen. Die DNS-Sperre benötigt zudem lediglich eine (kostengünstige) Manipulation an zentralen Servern, während für IP-Sperren in das komplette Routing-System eingegriffen werden muss. Die DNS-Sperre ist daher tendenziell wirtschaftlich weniger belastend und greift weniger stark in die Berufsfreiheit des ISP ein. Eine DVR, die mit Adress-Sperren arbeiten will, sollte aus der Perspektive einer gewünschten Vereinbarkeit mit der Berufsausübungsfreiheit daher zur Anordnung von DNS-Sperren tendieren.[675]

Die Kosten einer DVR mittels Deep Packet Inspection sind ebenfalls abstrakt kaum zu bestimmen. Auch hier gilt, dass die Kosten von diversen dynamischen Faktoren abhängen. Dennoch lässt sich auch auf abstrakter Ebene festhalten, dass die Kosten des Betriebs eines DPI-Filtersystems diejenigen von DNS- und IP-Sperren übersteigen dürften. Auf technischer Ebene lässt sich dies aus den erheblichen Rechenanforderungen ableiten,

---

[671] Vgl. oben Kap. 1 IV 5 (S.42 ff.).
[672] Eine evident ineffektive Regulierungsmaßnahme wäre hingegen bereits *ungeeignet* im verfassungsrechtlichen Sinn.
[673] *Assion*, K&R 2014, 329 betont zurecht, dass die ISPs bei bestimmten Ausgestaltungen der DVR auch dadurch in ihrer Berufsfreiheit belastet würden, dass sie ein Prozessrisiko sowohl aus der Richtung der Content-Anbieter (bei Overblocking) als auch von Seiten der Rechteinhaber (bei Underblocking) tragen würden.
[674] Da der ISP bei widerrechtlicher Sperrung eines Angebots der Gefahr zivilrechtlicher Schadensersatzforderungen des Content Providers ausgesetzt sein könnte, dürfte es ihm kaum zumutbar sein, die Kontrolle über die Pflege der Datenbanken den Rechteinhabern zu überlassen, auch wenn die Bereitstellung einer einfachen Schnittstelle seinen Aufwand erheblich verringern könnte.
[675] Die Frage, ob nicht die Freiheit des ISP, zwischen IP- und DNS-Sperre wählen zu können, dem ebenso Rechnung tragen könnte, wurde bereits oben auf Kap. 3 II 4 c) (4) (S. 160 f.) angesprochen und im Hinblick auf die entstehende Rechtsunsicherheit für den ISP bezweifelt.

die eine allgemeine Überwachung der tiefen Schichten des Internet-Datenverkehrs beanspruchen würde. Dies gilt jedenfalls im Vergleich zu den verhältnismäßig geringen technischen Anforderungen, die DNS- und IP-Sperren erfordern würden. Letztere müssen schließlich „lediglich" einen Teil des Datenverkehrs bzw. nur dessen obere Schichten überwachen.[676]

Den hohen Kosten der Deep Packet Inspection steht jedoch eine enorme Effektivität gegenüber, die diese durchaus aus der Perspektive der Berufsausübungsfreiheit rechtfertigen könnten, wenn sich die Kosten dennoch in einem zumutbaren Rahmen halten würden. Das Ergebnis dieser potentiell durchaus schwierigen Abwägung nimmt der europäische Gesetzgeber allerdings vorweg. Art. 3 Abs. 1 der Enforcement-Richtlinie bestimmt, dass Institutionen zur Durchsetzung des Urheberrechts nicht unnötig kompliziert und kostspielig sein dürfen. Dass dies bei einer Deep Packet Inspection der Fall wäre, hat der EuGH ausdrücklich festgestellt.[677] Europäisches Sekundärrecht ist höherrangig als das deutsche Grundgesetz, daher ist auch Art. 12 Abs. 1 GG hier so auszulegen, dass er mit der Enforcement-Richtlinie konform geht.[678] Eine DPI zur Durchsetzung des Urheberrechts ist daher nach aktueller Rechtslage mit Art. 12 Abs. 1 GG, ausgelegt in Übereinstimmung mit Art. 3 Abs. 1 Enforcement-Richtlinie, nicht zu vereinbaren.

Beachtet werden soll hier allerdings, dass europäisches Sekundärrecht zwar grundsätzlich im Rang über mitgliedstaatlichem Verfassungsrecht steht, durch eine einfache Handlung des europäischen Gesetzgebers jedoch ersetzt, geändert oder gestrichen werden kann. Wegen dieser Flüchtigkeit des Sekundärrechts ist durchaus auch die Frage interessant, wie die Rechtslage ohne Art. 3 Abs. 1 der Enforcement-Richtlinie aussähe.

Eine DPI zur Durchsetzung des Urheberrechts verletzt unter gewissen Umständen auch europäisches Primärrecht, namentlich die unternehmerische Freiheit gemäß Art. 16 Charta.[679] Dies hat der EuGH ebenfalls in seiner Scarlet-Entscheidung festgestellt: Ein DPI-Filtersystem würde die ISPs verpflichten, *„ein kompliziertes, kostspieliges, auf Dauer angelegtes und allein auf seine Kosten betriebenes Informatiksystem"* einzurichten.[680]

Primärrecht, insbesondere die Charta der Grundrechte, ist auf Dauer angelegtes Recht, dass auch nicht im täglichen politischen Prozess abgeändert werden kann. Es handelt sich um eine sehr robuste und beständige Institution.

---

[676] Im Ergebnis sieht dies auch der EuGH so, der in EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959 die Vereinbarkeit eines DPI-Filtersystems an Art. 16 Charta scheitern lässt, IP- und DNS-Sperren in EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192 jedoch nicht.
[677] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 48.
[678] Jedenfalls solange sein Kernbereich dadurch nicht verletzt wird, was hier nicht in Frage steht.
[679] Art. 16 Charta ist in diesem Fall die EU-rechtliche Entsprechung der Berufsausübungsfreiheit der Internet Service Provider.
[680] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 49; vgl. oben Kap. 2 V 1 (S. 73).

Dennoch sind durch die Scarlet-Entscheidung nicht alle zukünftigen Türen für eine DPI rechtlich verschlossen. Bei der Scarlet-Entscheidung handelt es sich um eine Einzelfallentscheidung, bei der man nur sehr zurückhaltend allgemeingültige Schlüsse aus den dort getroffenen Aussagen ziehen sollte. Beurteilt wurde in jenem Urteil ein konkretes DPI-Filtersystem, zudem im institutionellen Umfeld der damaligen Zeit, die nunmehr auch bereits einige Jahre zurückliegt. Es stellt sich die Frage, wie der EuGH in Bezug auf die Verletzung der unternehmerischen Freiheit urteilen würde, wenn ein zum Einsatz kommendes DPI-Filtersystem heute nicht mehr als derart *„kompliziert und kostspielig"* wie im Jahre 2011 einzuschätzen wäre. Zudem wurde durch das Scarlet-Urteil nicht entschieden, wie die Lage zu beurteilen wäre, würde das System zwar von den ISPs betrieben, aber von anderen Interessenvertretern finanziert.

Das zentrale Problem an dieser Stelle, ob es nun um DNS-, IP- oder DPI-Filter geht, ist daher die Frage, welche Kosten für die ISPs im Angesicht der Effektivität der Regulierungsbemühungen noch zumutbar wären und welche nicht. Aufgrund der Dynamik der technischen Entwicklung und der vielen denkbaren Varianten, wie sich ein ISP in diesem Bereich organisatorisch aufstellen könnte, ist die Zumutbarkeit des Eingriffs in Art. 12 Abs. 1 GG durch eine IP- oder DNS-Sperre schwierig abstrakt zu beurteilen. Viele potentiell mitentscheidende Faktoren lassen sich nur dem Einzelfall entnehmen: Ob und zu welchem Zeitpunkt der ISPs eine rein automatische Lösung finden kann, die im laufenden Betrieb wenig Arbeitskosten verursacht; wie sich variable und Fixkosten verteilen und wie sich diese zum Umsatz eines bestimmten ISP verhalten; oder ob es sich beim Internet Service Provider um ein sehr marktstarkes Unternehmen handelt, das seine Kosten im Einzelfall problemlos an seine Kunden durchreichen kann. Vor diesem Hintergrund wird auch noch einmal deutlich, weshalb die Kernaussage des UPC-Urteils des EuGH zwar nicht falsch ist und gerade auch die technische und organisatorische Dynamik und Unvorhersehbarkeit berücksichtigt, aber letztlich in der Praxis für den Rechtsanwender nicht besonders hilfreich ist. Dies deshalb, da lediglich festgestellt wird, dass IP- und DNS-Sperren nicht per se gegen die Berufsausübungsfreiheit verstoßen, wenn dem ISP die Entscheidung über das *Wie* der Sperre überlassen wird. Die Frage, bis zu welchen Grenzen denn Eingriffe in die Berufsausübungsfreiheit noch zumutbar wären, lässt der EuGH jedoch offen.[681]

Eine rechtliche Regelung über eine DVR, die die Frage der zumutbaren Kosten für den Adressaten unbeantwortet lässt und ihm gleichzeitig das Risiko aufbürdet, bei eigenen Fehleinschätzungen in diesem Punkt von den Rechteinhabern in Anspruch genommen zu werden, zwingt den Internet Service Provider zu kostspieligen Absicherungsmaßnahmen,[682] die die eigentlichen Kosten einer Sperrmaßnahme potentiell übertreffen und den ISPs so in seiner wirtschaftlichen Bewegungsfreiheit erheblich einschränken. Eine solche Regelung weckt allein aus diesem Grund bereits Zweifel an ihrer Vereinbarkeit mit

---

[681] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, vgl. oben Kap. 2 V 2 a) (S. 91).

[682] Etwa in der Form von Rückstellungen für die Führung zivilrechtlicher Gerichtsverfahren.

Art. 12 Abs. 1 GG. Will der Gesetzgeber Urheberrechtverletzungen mit Hilfe von Maßnahmen der Datenverkehrsregulierung bekämpfen, sollte er daher für eine ausreichende Rechtssicherheit des ISP bei der Frage sorgen, welche Belastungen denn aus seiner Sicht noch zumutbar seien.

Aber welche Grenze bietet sich hier an? Da unterschiedliche ISP wirtschaftlich unterschiedlich stark von der Durchführung von Internet-Sperren belastet würden, sollte die Möglichkeit bestehen, bei der Anordnung in Abhängigkeit des Adressaten eine Einzelfallregelung zu finden. Andererseits sollte aus soeben dargelegten Gründen Rechtsunsicherheit weitgehend vermieden werden. Ein denkbarer Ausweg aus diesem Dilemma bestünde darin, Kosten bis zu einem gewissen prozentualen Anteil des Jahresumsatzes als Zumutbarkeitsgrenze heranzuziehen.[683] Eine so errechnete Marke müsste allerdings in einem Bereich zu verorten sein, der *unterhalb einer für ISP wirtschaftlich spürbaren Grenze* liegt. Die Effektivität einer DVR mittels Adress-Sperren ist so gering, dass ihr Nutzen ansonsten in keinem Verhältnis zur Belastung des ISPs stünde.[684]

Kommt hingegen ein DPI-Filtersystem zum Einsatz, ist das Fordern von Kosten *unterhalb einer wirtschaftlich spürbaren Grenze* wegen der größeren Effektivität und damit dem größeren öffentlichen Nutzen ein zu strenges Kriterium. Nichtsdestotrotz müssten auch hier die wirtschaftlichen Belastungen eng begrenzt werden, um nicht der Scarlet-Entscheidung des EuGH zu widersprechen. Ein erfolgsversprechender Weg für den Gesetzgeber, die Gefahr der Verfassungswidrigkeit wegen Verstoßes gegen Art. 12 GG zu vermeiden, wäre es hingegen, den ISPs von vornherein die Kostenlast abzunehmen. Filtersysteme könnten von ISPs betrieben, aber staatlich oder von den Rechteinhabern finanziert werden.[685] Es würde zwar dennoch weiterhin ein organisatorischer Overhead die Berufsfreiheit der ISPs belasten, da dieser mit dem Betrieb eines Filtersystems einhergeht.[686] Der Schwerpunkt der potentiellen Unzumutbarkeit liegt jedoch bei der finanziellen Beschwer.

Zudem werden die ISPs weniger belastet, wenn sie lediglich subsidiär in Anspruch genommen würden. Jedenfalls DNS- und IP-Sperren würden bei einer nur sporadischen Inanspruchnahme weniger Verwaltungsaufwand verursachen. Bei der DPI ist die Situation hingegen ein wenig anders gelagert. Auch bei subsidiärer Inanspruchnahme müsste eine DPI den kompletten Datenverkehr überwachen. Dennoch müsste der Datenverkehr auf

---

[683] *Heliosch*, Sperrmaßnahmen im Internet, S. 178 fordert eine gesetzliche Entschädigungsverpflichtung für die Kostenbelastung der ISPs. Dies würde aus meiner Sicht das hier bestehende rechtliche Problem zwar in vergleichbarer Weise wie der sogleich gemachte Vorschlag angehen, dürfte jedoch wegen eines zu erwartenden immensen Bürokratieaufwands, der wiederum Kosten mit sich bringen würde, an praktische Grenzen stoßen.

[684] Hinzu kommt, dass die Effektivität der Sperrmaßnahmen in dem Maße weiter abnimmt, wie ISPs aus ihrer Pflichtigkeit zur Sperre entlassen werden, weil ihr Jahresumsatz GGf. die Schwelle nicht überschreitet.

[685] Vgl. *Cruz Villalón*, Schlussanträge des Generalanwalts v. 26.11.2012, Rs. C-314, UPC Telekabel, EU:C:2013:781, Rn. 106.

[686] *Schnabel*, MMR 2008, 281 (286) weist daraufhin, dass es schlicht nicht die originäre Aufgabe der ISP sei, die übertragenen Inhalte zu überwachen.

weniger urheberrechtlich geschützte Werke hin durchsucht werden, was zu einer Verringerung des Rechenaufwands führen könnte. Angesichts des fehlenden Verschuldens der ISPs bezüglich der Urheberrechtsverletzung sollten ISPs daher lediglich subsidiär in Anspruch genommen werden können, nachdem zuvor bereits ein Vorgehen gegen den unmittelbaren Verletzer oder den Host-Provider, die jeweils einen größeren Verursachungsbeitrag zur Rechtsverletzung leisten, fehlgeschlagen ist oder von vornherein ohne Aussicht auf Erfolg war. Insoweit ist dem BGH zuzustimmen.[687]

5. Ergebnis

Zusammenfassend lässt sich daher sagen, dass Eingriffe in die Berufsfreiheit der Internet Service Provider zur Urheberrechtsdurchsetzung nicht angemessen und damit unverhältnismäßig sind, soweit sie zur Deep Packet Inspection verpflichten. Dies gilt erst recht, solange Art. 3 Abs. 1 der Enforcement-Richtlinie in der heutigen Form in Kraft ist. Selbst wenn dieser außer Kraft gesetzt würde, ist eine Verletzung der Berufsausübungsfreiheit aber nur dann zu verneinen, wenn die Kosten der DPI für den ISP eng begrenzt würden. Dies könnte beispielsweise dadurch erreicht werden, dass der Staat oder die Rechteinhaber die Kosten der Datenverkehrsregulierung tragen. Die Kosten des ISP müssten dabei erheblich unterhalb der Schwelle derjenigen Kosten bleiben, die das Filtersystem, welches im Scarlet-Verfahren untersucht wurde, verursacht.

Eingriffe in die Berufsfreiheit durch IP- oder DNS-Sperren hingegen sind zur Durchsetzung des Urheberrechts nicht per se unangemessene Maßnahmen. Der Gesetzgeber müsste allerdings sicherstellen, dass die Kosten der ISPs *unterhalb einer wirtschaftlich spürbaren Grenze* bleiben.

III. Das Grundrecht der Internet-Nutzer auf Informationsfreiheit, Art. 5 Abs. 1 Satz 1 Alt. 2 GG

Nicht lediglich die Grundrechte der Internet Service Provider werden potentiell durch Eingriffe in den Datenverkehr zur Durchsetzung des Urheberrechts berührt, sondern auch diejenigen der Teilnehmer an diesem Datenverkehr, den Nutzern des Internets. Insbesondere könnten Eingriffe in den Datenverkehr die Informationsfreiheit und das Telekommunikationsgeheimnis verletzt sein.

Zunächst sollen an dieser Stelle potentielle Beeinträchtigungen der Informationsfreiheit der Internet-Nutzer untersucht werden.

1. Schutzbereich der Informationsfreiheit

Deep Packet Inspection, IP- und DNS-Filter könnten in den Schutzbereich des Art. 5 Abs. 1 Satz 1 Alt. 2 GG eingreifen. Die Schutzrichtung der Informationsfreiheit ist in erster Linie die eines subjektiven Abwehrrechts. Es ist Teil der menschlichen Existenz und seiner Grundbedürfnisse, sich aus einer Vielzahl verschiedener Informationsquellen

---

[687] BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 82; *Ahrens u.a.*, WRP 2007, 1281 (1287, 1290); *Spindler*, CR 2012, 176 (178).

zu unterrichten, um den eigenen Horizont zu erweitern und die Persönlichkeit zu entfalten. Neben diese subjektive Komponente tritt zudem noch eine objektive: Eine Demokratie benötigt, um existieren zu können, eine in öffentlicher Debatte gebildete, in einem Mindestmaß informierte und freie Meinung.[688]

Der persönliche Schutzbereich ist bei einer Datenverkehrsregulierung unproblematisch eröffnet. Erfasst werden alle natürlichen und juristischen Personen (letztere in den Grenzen des Art. 19 Abs. 3 GG), und damit auch alle Internet-Nutzer.[689]

Nähere Betrachtung verdient hingegen der sachliche Schutzbereich der Informationsfreiheit. Die Informationsfreiheit schützt die ungehinderte Unterrichtung aus allgemein zugänglichen Quellen.

Informationsquellen im Sinne des Art. 5 Abs. 1 Satz 1 GG sind alle Träger von Daten und Informationen, gleich welcher technischer Beschaffenheit, und unabhängig davon, ob die vermittelten Informationen Tatsachen oder Meinungen betreffen. Insbesondere sind auch sämtliche öffentlichen Gebiete des Internets umfasst.[690] Unerheblich ist es, ob die Informationen hinsichtlich der öffentlichen Meinungsbildung relevant erscheinen. Der Bereich der erfassten Informationen ist umfassend.[691] Ebenso ist es unerheblich, ob sich die Informationsquelle in Deutschland oder im Ausland befindet.[692] Datenbanken und Server im Internet, unabhängig von der Art der Daten, die sie zum Abruf bereitstellen, seien sie urheberrechtlich geschützt oder nicht, und unabhängig von ihrem physischen Standort, sind mithin Informationsquellen im Sinne des Art. 5 Abs. 1 Satz 1 GG.

Allgemein zugänglich ist eine Informationsquelle, wenn sie technisch geeignet und dazu bestimmt ist, der Allgemeinheit, also einem individuell nicht bestimmbaren Personenkreis, Informationen zu verschaffen.[693] Ob eine Informationsquelle für die Allgemeinheit zugänglich ist, bestimmt gemäß der Rechtsprechung des Bundesverfassungsgerichts derjenige, dem die Rechtsordnung dieses Recht zuweist.[694] Was zunächst nach Zirkelschluss klingt, bedeutet letztlich in der Regel, dass der Inhaber oder der die Quelle direkt Beherrschende die Bestimmungsbefugnis besitzt. Die Bestimmungsbefugnis liegt folglich im

---

[688] BVerfG, Beschl. v. 03.10.1969, 1 BvR 46/65, Leipziger Volkszeitung, BVerfGE 27, 71 (81); vgl. auch *Schmidt-Jortzig* in: Isensee/P. Kirchhof, HStR VII, § 162 Rn. 34; *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 5 Rn. 21.
[689] *Gröpl* in: Gröpl u.a., Grundgesetz, Art. 5 Rn. 23.
[690] *Gröpl* in: Gröpl u.a., Grundgesetz, Art. 5 Rn. 25; *Kube* in: Isensee/P. Kirchhof, HStR IV, § 91 Rn. 12 ff.
[691] BVerfG, Urt. v. 24.01.2001, 1 BvR 2623/95, 1 BvR 622/99, Gerichtsfernsehen, BVerfGE 103, 44 (60); *Grabenwarter* in: Maunz/Dürig, Art. 5 Abs. 1, Abs. 2 GG Rn. 87 (Stand: 68. Erg.-Lfg., Januar 2013); *Wendt* in: v. Münch/Kunig, 7. Aufl. 2021, Grundgesetz Bd. 1, Art. 5 Rn. 49.
[692] BVerfG, Beschl. v. 09.02.1994, 1 BvR 1687/92, Parabolantenne, BVerfGE 90, 27 (32).
[693] BVerfG, Beschl. v. 03.10.1969, 1 BvR 46/65, Leipziger Volkszeitung, BVerfGE 27, 71 (83); BVerfG, Beschl. v. 09.02.1994, 1 BvR 1687/92, Parabolantenne, BVerfGE 90, 27 (32); BVerfG, Urt. v. 24.01.2001, 1 BvR 2623/95, 1 BvR 622/99, Gerichtsfernsehen, BVerfGE 103, 44 (60).
[694] BVerfG, Urt. v. 24.01.2001, 1 BvR 2623/95, 1 BvR 622/99, Gerichtsfernsehen, BVerfGE 103, 44 (60 f.).

Kontext illegalen Filesharings über das Internet beim jeweiligen Anbieter des geschützten Werks.[695]

Der sachliche Schutzbereich ist also zunächst einmal insoweit sehr weit gefasst, so dass alle Arten von Informationen unabhängig von ihrem Inhalt den Schutz des Grundrechts umfassend genießen. Andererseits bietet die Informationsfreiheit keinen Anspruch auf Zugang zu jedweder, gegebenenfalls vertraulicher Information. Erst das Angebot des Bestimmungsberechtigten, die Information der Öffentlichkeit zugänglich zu machen, führt zur Eröffnung des Schutzbereichs.[696]

Einer näheren Erörterung wert ist die Frage, wo die Abgrenzung verläuft zwischen den an die Allgemeinheit gerichteten Informationen im Internet, die von der Informationsfreiheit erfasst werden, und den sonstigen Informationen. Viele Inhalte, gerade solche, die unter illegalem Filesharing zu subsumieren sind, sind nicht unmittelbar jedermann zugänglich. So erfordern insbesondere manche Filehoster eine vorherige Anmeldung mit einem Benutzerkonto, um eine bestimmte Datei herunterladen zu können. Üblicherweise wird eine unbegrenzte Anzahl von Downloads und in hoher Geschwindigkeit zudem nur dann gestattet, wenn diese Dienste zuvor bezahlt wurden. Dadurch werden bestimmte Zugriffshürden gesetzt, die verhindern, dass sich die Allgemeinheit ohne weitere Schritte Zugang zu bestimmten Informationen verschafft, also beispielsweise erst nach einer vorherigen Registrierung. Nach richtiger Ansicht können diese Maßnahmen nicht dazu führen, diese Quellen aus dem Schutzbereich der Informationsfreiheit auszunehmen.[697] Solche Maßnahmen dienen nicht dazu, konkrete Individuen von der Kenntnisnahme auszugrenzen oder die Informationen nur bestimmten Individuen zukommen zu lassen. Vielmehr geht es in der Regel um die Durchsetzung von Sicherheits-, Monetarisierungs- oder Jugendschutz-Interessen. Im Ergebnis sind daher die weit überwiegende Anzahl an Filesharing-Angeboten im Internet allgemein zugängliche Informationsquellen.

Unerheblich für die Betroffenheit des Schutzbereichs ist im Übrigen, ob das Filesharing im konkreten Fall unter Strafe gestellt ist. Die §§ 106 ff. UrhG stellen beispielsweise ver-

---

[695] Anbieter beim P2P-Filesharing sind demnach diejenigen, die den Inhalt öffentlich zugänglich machen. Beim *Filesharing* über zentrale Server ist diese Frage schwieriger zu beantworten, da hier die Abgrenzung von Content Provider und Host-Provider zu Problemen führen kann. In der Regel dürfte es in der verfassungsrechtlichen Beurteilung jedoch keinen Unterschied ausmachen.

[696] BVerfG, Urt. v. 24.01.2001, 1 BvR 2623/95, 1 BvR 622/99, Gerichtsfernsehen, BVerfGE 103, 44 (60).

[697] So BGH, Urt. v. 18.10.2007, I ZR 102/05, ueber18.de, GRUR 2008, 534, (538); *Berger*, MMR 2003, 773 (774); *Liesching*, MMR 2008, 802. Anderer Ansicht ist hingegen *Heliosch*, Sperrmaßnahmen im Internet, S. 180, die „geschlossene Benutzergruppen", die bereits durch die Verwendung von Altersverifikation-Systemen entstünden, vom Schutzbereich der Informationsfreiheit ausnehmen möchte. Diese Ansicht ist jedoch zu restriktiv. Effektiv wäre damit ein Großteil der im Internet veröffentlichten Informationen dem Anwendungsbereich der Informationsfreiheit entzogen, in weitaus größerem Maße, als dies offline der Fall wäre. Geschlossene Benutzergruppen, die eine Anwendung von Art. 5 Abs. 1 Satz 1 GG hier ausschließen würden, könnten hingegen Internet-Foren sein, die nur untereinander bekannten Personen offenstehen.

schiedene Handlungen im Zusammenhang mit Filesharing unter Strafe. Könnte der Gesetzgeber auf diese Art und Weise allerdings bereits die Betroffenheit des Schutzbereichs der Informationsfreiheit verengen, indem er den Abruf bestimmter Arten von Informationen unter Strafe stellt, liefe der Schutz der Informationsfreiheit weitgehend leer.[698] Zwar lassen sich gewisse Äußerungen *Baduras* auch so verstehen, dass die Beschaffung von Informationen durch strafbare Handlungen vom Schutzbereich der Informationsfreiheit ausgenommen wären.[699] Wenn die Informationsfreiheit ein effektives Schutzrecht sein soll, muss man in dieser Frage differenzieren. Nicht von der Informationsfreiheit gedeckt ist es, wenn zur Informationsbeschaffung ein Hindernis der Allgemeinzugänglichkeit rechtswidrig überwunden wird. In diesen Fällen fehlt es allerdings bereits am Kriterium der Allgemeinzugänglichkeit, und das Verbotsgesetz dient lediglich deren Durchsetzung.[700] Werden hingegen sonstige Rechtsgüter Dritter[701] – wie beispielsweise Urheberrechte – durch Filesharing verletzt, werden diese nach der hier vertretenen Ansicht erst auf der Rechtfertigungsebene eines Eingriffs berücksichtigt.[702] Eine staatliche Manipulation des Internetdatenverkehrs berührt daher den Schutzbereich in jedem Falle, also unabhängig von der Frage, ob es sich beim Verhalten des Bürgers um legales oder um illegales Filesharing handelt.[703]

Besteht nach dem soeben Gesagten eine allgemein zugängliche Informationsquelle, gewährleistet Art. 5 Abs. 1 Satz 1 GG die Freiheit, sich ungehindert aus dieser zu unterrich-

---

[698] Die Informationsfreiheit des Art. 5 Abs. 1 Satz 1 GG ist eine Reaktion des Verfassungsgesetzgebers gerade darauf, dass zur Zeit des Nationalsozialismus die Information an bestimmten Quellen, z.B. ausländischen Rundfunksendern, verboten war. Dies sollte dem Staat in der Bundesrepublik nicht möglich sein. Vgl. *Jarass* in: Jarass/Pieroth, Grundgesetz Art. 5 GG, Rn.21.

[699] Vgl. *Badura*, Staatsrecht, C 7 (Rn. 63), insoweit missverständlich, als es nicht ganz klar wird, ob *Badura* sich nicht eventuell auf die Rechtfertigungs- anstelle der Schutzbereichsebene bezieht („Die Informationsfreiheit erlaubt nicht etwa die Beschaffung durch strafbare Handlungen", jedoch im Kontext des Schutzbereichs). Dabei stützt er sich auf die Entscheidung BVerfG, Urt. v. 11.03.1969, 1 BvR 665/62, 1 BvR 152/69, Zeugnisverweigerungsrecht, BVerfGE 25, 296, die jedoch weder die eine noch die andere Interpretation stützt, da die mit Strafe bewehrte Beschaffung von Informationen dort gar nicht Gegenstand des Verfahrens war. Ähnlich (auch ähnlich missverständlich) die Position der Bezirksregierung Düsseldorf im Verfahren VG Düsseldorf, Urt. v. 10.05.2005, 27 K 5968/02, Rn. 6 (juris), nicht jedoch das Gericht selbst, das in Rn. 81 ff. den Schutzbereich wohl berührt sieht.

[700] H.M., vgl. nur BVerfG, Beschl. v. 25.01.1984, 1 BvR 272/81, Springer/Wallraff, BVerfGE 66, 116 (137 f.); *Wendt*, AfP 2004, 181 (184); *ders.*, in: v. Münch/Kunig, Grundgesetz Bd. 1, 7. Aufl. 2021, Art. 5 Rn. 57.

[701] Mit „Dritten" sind hier solche Personen oder Stellen gemeint, die nicht über ein Bestimmungsrecht bezüglich der Allgemeinzugänglichkeit verfügen.

[702] *Schmidt-Jortzig* in: Isensee/P. Kirchhof, HStR VII, § 162 Rn. 38 f.; *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 5 Rn. 23; *Wendt* in: v. Münch/Kunig, 7. Aufl. 2021, Grundgesetz Bd. 1 Art. 5 Rn. 57.

[703] Vgl. *Greiner*, CR 2002, 620 (623). So auch im Ergebnis *Heliosch*, Sperrmaßnahmen im Internet, S. 181 f. und *Sieber/Nolde*, Sperrverfügungen, S. 78.

ten. „Unterrichten“ ist dabei weit zu verstehen. Es wird sowohl die untätige Entgegennahme als auch die aktive Beschaffung der Information geschützt, nicht lediglich der Konsum der Information, sondern auch die Speicherung und Aufarbeitung.[704]

2. Eingriff

Ein Eingriff in den Schutzbereich der Informationsfreiheit liegt stets dann vor, wenn der Bürger durch einen hoheitlichen Akt gehindert wird, sich aus einer allgemein zugänglichen Quelle zu unterrichten. Der Begriff des „Behinderns“ ist hier weit zu verstehen, damit aufgrund der vielfältigen Typen von Informationen und Informationsquellen ein umfassender Schutz gewährleistet werden kann. Erfasst sind daher alle hoheitlichen Verbote und Strafdrohungen, aber auch Realhandlungen wie die staatliche Beobachtung des Informationsverhaltens des Bürgers und die faktische (beispielsweise technische) Verhinderungen des Unterrichtens.[705] Ein Eingriff ist auch dann gegeben, wenn die Behinderung des Unterrichtens des Bürgers nur in einer nicht geringfügigen Informationsverzögerung resultiert.[706]

Hoheitliche datenverkehrsregulierende Maßnahmen sind daher stets Eingriffe in den Schutzbereich der Informationsfreiheit. Dies betrifft die technischen Manipulationen am Datenverkehr selbst, aber auch die entsprechenden rechtlichen Grundlagen wie behördliche oder gerichtliche Anordnungen oder Gesetze, die Maßnahmen der DVR anordnen.

Da auch bloße Verzögerungen des Unterrichtens Eingriffe darstellen, kommt es insoweit auch nicht darauf an, ob eine datenverkehrsregulierende Maßnahme die Information dauerhaft unerreichbar macht. In der Entscheidung des Bundesverfassungsgerichts, in der die Frage einer verzögerten Unterrichtung aus einer allgemein zugängliche Quelle Verfahrensgegenstand war, begründete das Bundesverfassungsgericht dies damit, dass gewisse tagesaktuelle Informationen bereits nach kurzer Zeit ihren Wert für den Nutzer verlieren würden.[707] Der Sachverhalt betraf damals die verzögerte Zustellung einer Tageszeitung. In der heutigen Informationsgesellschaft ist allerdings bereits ein wesentlich kürzerer Verzögerungszeitraum geeignet, einen Vorgang des Unterrichtens dauerhaft zu entwerten. Zum Zeitpunkt der zitierten Entscheidung (1969) war die Anzahl der Informationsquellen für viele Bürger auf einige wenige Massenmedien beschränkt. Die Taktung, in der die Bürger Zugriff auf neue Informationen bekamen, war in der Regel täglich. Im Zeitalter des Internets wird die Aufmerksamkeit des Nutzers jedoch von einer schwer überschaubaren Menge an Informationsquellen beansprucht, und Informationen verlieren oft bereits nach wenigen Stunden oder gar Minuten ihre Aktualität und damit ihre Bedeutung. Deep Packet Inspection, IP- und DNS-Sperren sind daher alle, wenn auch in

---

[704] BVerfG, Beschl. v. 03.10.1969, 1 BvR 46/65, Leipziger Volkszeitung, BVerfGE 27, 71 (82 f.); *Schmidt-Jortzig* in: Isensee/P. Kirchhof, HStR VII, § 162 Rn. 41; *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 5 Rn. 25; *Wendt* in: v. Münch/Kunig, Grundgesetz Bd. 1, 7. Aufl. 2021, Art. 5 Rn. 57.
[705] Vgl. dazu *Schmidt-Jortzig* in: Isensee/P. Kirchhof, HStR VII, § 162 Rn. 42 mit weiteren Beispielen.
[706] BVerfG, Beschl. v. 14.10.1969, 1 BvR 30/66, Verzögerte Postauslieferung, BVerfGE 27, 88 (98 f.).
[707] BVerfG, Beschl. v. 14.10.1969, 1 BvR 30/66, Verzögerte Postauslieferung, BVerfGE 27, 88 (99).

unterschiedlichem Maße, dazu geeignet, den Zugang des Bürgers zu Informationsquellen zu verhindern, zu verzögern oder mit zusätzlichem Aufwand zu versehen und somit Informations- und Aufmerksamkeitsströme umzuleiten.

Auch wenn viele Nutzer insbesondere IP- und DNS-Sperren mit ein wenig investiertem Aufwand umgehen können, wird dies in einigen Fällen doch dazu führen, dass damit zumindest eine Verzögerung einhergeht, die die schließlich erlangte Information entwerten kann; oder aber der zur Umgehung der Maßnahme notwendige Aufwand könnte den Nutzer dazu verleiten, sich einer konkurrierenden Informationsquelle zuzuwenden.[708] Ob dies ein verfassungsrechtlich zulässiges oder gar regulatorisch gewünschtes Ergebnis ist, ist eine Frage der Rechtfertigung eines Eingriffs, nicht der des Vorliegens eines Grundrechtseingriffs selbst.

Maßnahmen der DVR greifen zudem mittelbar durch sogenannte *Chilling Effects* in die Informationsfreiheit ein. Wenn Internet-Nutzer bemerken, dass in ihren Datenverkehr von außen eingegriffen wird, und dies insbesondere deshalb, weil sie auf bestimmte Inhalte zugreifen wollten, wird dies ihr zukünftiges Informationsverhalten im Sinne einer Selbstzensur beeinflussen, schon weil sie sich nicht mehr unbeobachtet fühlen.[709]

3. Schranken der Informationsfreiheit

Die Informationsfreiheit ist kein vorbehaltlos gewährleistetes Grundrecht. Wie alle Grundrechte des Art. 5 Abs. 1 GG unterliegt es gemäß Art. 5 Abs. 2 GG den Schranken der allgemeinen Gesetze, der Jugendschutzbestimmungen sowie des Rechts der persönlichen Ehre.

Maßnahmen zur Durchsetzung des Urheberrechts unterfallen weder dem Ehrschutz noch handelt es sich um Jugendschutzbestimmungen. Sie können daher nur dann rechtmäßig in die Informationsfreiheit eingreifen, wenn es sich um allgemeine Gesetze im Sinne des Art. 5 Abs. 1 Satz 2 GG handelt. Allgemeine Gesetze im vorliegenden Kontext sind nach ständiger Rechtsprechung solche Gesetze, die sich nicht gegen die Informationsfreiheit an sich richten, sondern den Schutz eines schlechthin, ohne Rücksicht auf eine bestimmte Meinung, zu schützenden Rechtsguts bezwecken. Dieses Rechtsgut muss allgemein, das heißt unabhängig davon geschützt sein, ob es durch Meinungsäußerungen oder auf andere Weise verletzt werden kann.[710]

---

[708] Im Ergebnis ebenso: *Heliosch*, Sperrmaßnahmen im Internet, S. 181; *Sieber/Nolde*, Sperrverfügungen, S. 78.

[709] BVerfG, Beschl. v. 07.12.1976, 1 BvR 460/72, Flugblatt, BVerfGE 43, 130 (136); *Grabenwarter* in: Maunz/Dürig, Art. 5 Abs. 1, Abs. 2 GG Rn. 103 f. (Stand: 70. Erg.-Lfg., Dezember 2013); *Heliosch*, Sperrmaßnahmen im Internet, S. 192; *Holznagel*, ZUM 2000, 1007 (1011); *Jestaedt* in: Merten/Papier, Handbuch der Grundrechte IV, § 102 Rn. 51; *J. Kahl*, SächsVBl. 2010, 180 (194); *Nolte/Wimmers*, GRUR 2014, 16.

[710] BVerfG, Urt. v. 15.01.1958, 1 BvR 400/51, Lüth, BVerfGE 7, 198 (209 f.); BVerfG, Beschl. v. 10.10.1995, 1 BvR 1476/91, 1 BvR 1980/91, 1 BvR 102/92, 1 BvR 221/92, Soldaten sind Mörder,

Will der Staat die Informationsfreiheit durch Filtersysteme einschränken, muss dies folglich zunächst einmal auf (wenigstens materielle) Gesetze zurückgehen, da es sich bei Art. 5 Abs. 2 GG um einen qualifizierten Gesetzesvorbehalt handelt.[711] In Anbetracht des gewichtigen Eingriffs in diverse Grundrechte ist nach der Wesentlichkeitstheorie des Bundesverfassungsgerichts bei Eingriffen in den Datenverkehr zur Durchsetzung des Urheberrechts allerdings sogar ein formelles Gesetz als Grundlage zu fordern.

Ein Gesetz, dass die Durchsetzung des Urheberrechts zum Zweck hat, ist als allgemeines Gesetz im Sinne von Art. 5 Abs. 2 GG zu qualifizieren. Zwar richten sich gesetzliche Normen, die bestimmte Inhalte aus dem Datenverkehr zu filtern beabsichtigen, direkt gegen den Vorgang des Sich-Unterrichtens. Ziel eines solchen Gesetzes ist es allerdings nicht, den Bürger von bestimmten Inhalten fernzuhalten, sondern vielmehr die privatrechtliche Ansprüche Dritter aus dem Urheberrecht durchzusetzen. Urheberrechte sind durch das Grundgesetz in Art. 14 GG und durch die einfachrechtliche Rechtsordnung umfassend geschützt, ganz unabhängig davon, ob sie durch Netzsperren oder anderweitig durchgesetzt werden.[712]

Insbesondere besteht das Verbot illegalen Filesharings unabhängig davon, ob der Staat diese durch Filtersysteme zu verhindern sucht. Maßnahmen der Datenverkehrsregulierung selbst regeln nicht, ob ein bestimmter Inhalt erlaubt ist oder nicht, sondern beziehen sich lediglich auf die Durchsetzung bereits bestehender urheberrechtlicher Normen. Der Staat verhält sich bei einer Datenverkehrsregulierung auch inhaltlich neutral. Die Maßnahmen richten sich nicht gegen eine bestimmte Form von Information oder Meinungsäußerung. Jeglicher urheberrechtlicher Inhalt kann, losgelöst von seinem Informations- oder Meinungsgehalt, unter Maßnahmen der DVR fallen oder eben nicht, da diese nur auf die privatrechtliche Befugnis des Content Providers abstellen, die urheberrechtlich geschützten Inhalte anzubieten.

4. Schranken-Schranken

Die Schranke gemäß Art. 5 Abs. 2 GG gilt nicht absolut. Auch in diesem Fall ist die Möglichkeit, die Grundrechte einzuschränken, wiederum durch die sogenannten Schranken-Schranken eingeschränkt. Als solche ist hier in erster Linie der Grundsatz der Verhältnismäßigkeit relevant. Dieser verlangt, dass ein Eingriff in die Informationsfreiheit einem

---

BVerfGE 93, 266 (291); BVerfG, Beschl. v. 23.06.2004, 1 BvQ 19/04, NPD-Kundgebung, BVerfGE 111, 147 (155); BVerfG, Urt. v. 27.02.2007, 1 BvR 538/06, 1 BvR 2045/06, CICERO, BVerfGE 117, 244 (260); BVerfG, Beschl. v. 26.02.2008, 1 BvR 1602/07, 1 BvR 1606/07, 1 BvR 1626/07, Caroline von Monaco III, BVerfGE 120, 180 (200).

[711] Vgl. BVerwG, Urt. v. 24.10.1985, 7 C 55/84, Friedenszeichen, BVerwGE 72, 183, (186); *Gröpl* in: Gröpl u.a., Grundgesetz, Art. 5 Rn. 67.

[712] An dieser Stelle lässt sich sicher argumentieren, dass das gesamte Urheberrecht dem Zweck dient, den freien Zugang der Allgemeinheit zu Information rechtlich zu begrenzen, um bestimmten Privatrechtssubjekten die Kontrolle über den Fluss dieser Information zu geben, damit diese daraus ideelle und materielle Gewinne ziehen können. Andererseits ist das Urheberrecht auch ein Anreizsystem, Informationen überhaupt erst zu produzieren, wodurch auch die Allgemeinheit einen Wohlfahrtsgewinn zieht. Sinn und Zweck des Urheberrechts an und für sich sind jedoch nicht das Thema dieser Arbeit.

legitimen Zweck gilt, zur Erreichung dieses Zwecks geeignet und erforderlich ist und insbesondere die Angemessenheit (Verhältnismäßigkeit im engeren Sinne) gewahrt bleibt.[713]

Legitimer Zweck der Einschränkung der Informationsfreiheit ist der Schutz des Urheberrechts.[714] Zur Erreichung dieses Zwecks im verfassungsrechtlichen Sinne sind auch einerseits die Deep Packet Inspection und andererseits DNS- wie IP-Sperren geeignet, obwohl letztere als weniger effektiv als DPI-Filtersysteme einzuschätzen sind.[715]

Etwas nähere Betrachtung verlangt hier die Erforderlichkeit datenverkehrsregulierender Maßnahmen.[716] Wie oben bereits festgestellt,[717] ist eine Maßnahme im verfassungsrechtlichen Sinn erforderlich, wenn der Staat aus allen gleich gut geeigneten Mitteln, die ihm zur Erreichung des Ziels zur Verfügung stehen, das mildeste, also das Grundrecht – hier: die Informationsfreiheit – schonendste Mittel auswählt.[718]

Dabei bietet es sich an, bei der notwendigen Gegenüberstellung der infrage kommenden Maßnahmen zu differenzieren und zunächst Eingriffe in den Datenverkehr anderen möglichen Maßnahmen zur Durchsetzung des Urheberrechts gegenüberzustellen. In einem zweiten Schritt werden dann IP-, DNS- und DPI-Systeme untereinander zu vergleichen sein.

Stellt man Maßnahmen der Datenverkehrsregulierung sonstigen Maßnahmen zur Durchsetzung des Urheberrechts gegenüber, so ergibt sich die Erforderlichkeit in der Regel bereits daraus, dass diese nicht in einem Konkurrenzverhältnis zueinander stehen, sondern kumulativ oder ergänzend eingesetzt werden können. Zudem sind die konkurrierenden Ansätze nicht immer besonders effektiv. So ist etwa der Ansatz, das Urheberrecht verletzende Angebote zu löschen anstatt sie zu sperren, nicht zwingend effektiver als Datenverkehrseingriffe, da Angebote in anderen Rechtsräumen von Löschungsverfügungen oft nicht erreicht werden.[719]

---

[713] Vgl. *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 5 Rn. 68 m.w.N.
[714] Nach BVerfG, Beschl. v. 04.11.2009, 1 BvR 2150/08, Wunsiedel-Versammlung, BVerfGE 124, 300 (331) ist grundsätzlich jedes öffentliche Interesse legitim, das den „substantiellen Gehalt der Rechte“ aus Art. 5 Abs. 1 GG nicht negiert.
[715] Vgl. dazu ausführlich bereits oben Kap. 3 II 4 b) (S. 151 ff.).
[716] Da die Erforderlichkeit sehr stark von der Beeinträchtigung des konkreten Grundrechts abhängig ist, kann an dieser Stelle nicht einfach nach oben zu den Ausführungen zur Berufsfreiheit verwiesen werden.
[717] Siehe oben Kap. 3 II 4 c) (S. 153 f.)
[718] BVerfG, Beschl. v. 14.03.1989, 1 BvR 1033/82, 1 BvR 174/84, Multiple-Choice-Verfahren, BVerfGE 80, 1 (29 f.); BVerfG, Urt. v. 30.07.2008, 1 BvR 3262/07, 1 BvR 402/08, 1 BvR 906/08, Rauchverbot, BVerfGE 121, 317 (354); BVerfG, Urt. v. 06.12.2016, 1 BvR 2821/11, 2 BvR 321/12, 2 BvR 1456/12. BVerfGE 143, 246, Rn. 289.
[719] Oben Kap. 3 II 4 c) (1) (S. 154 ff.) erfolgt eine nähere Auseinandersetzung mit der Erforderlichkeit des Ansatzes „Löschen statt Sperren“ insbesondere im Hinblick auf die Berufsausübungsfreiheit. Auf diese kann hier weitgehend verwiesen werden. Zu beachten ist allerdings, dass dem Ansatz der Löschung oben abgesprochen wurde, dass im Vergleich zu Maßnahmen der DVR nicht in

Vergleicht man die Deep Packet Inspection, IP- und DNS-Sperren untereinander, so greifen diese unterschiedlich tief in die Informationsfreiheit ein. An anderer Stelle wurde bereits festgestellt, dass Deep Packet Inspection Overblocking gegebenenfalls effektiver vermeiden kann als IP- und DNS-Sperren.[720] IP-Sperren schneiden in der Regel mehrere Angebote, die auf einem Server zu erreichen sind, gleichzeitig vom Zugriff von außen ab, DNS-Sperren immerhin noch das gesamte unter einer Website erreichbare Informationsangebot. Die Deep Packet Inspection besitzt hingegen das Potential, zielgenau lediglich den illegalen Abruf spezifischer Inhalte zu unterbinden. Da mit der Deep Packet Inspection also der Zugriff auf möglichst wenige Informationsquellen, insbesondere aber auch auf möglichst wenige urheberrechtlich unbedenkliche Quellen beschränkt werden kann, stellt sie gegenüber DNS- und insbesondere IP-Sperren im isolierten Hinblick auf die Informationsfreiheit ein milderes Mittel dar.[721]

Dennoch stellt sich hier die Frage der Erforderlichkeit etwas anders dar als bei der Berufsfreiheit. Dort – und damit selbstverständlich auch an dieser Stelle – ist die DPI die effektivste datenverkehrsregulierende Maßnahme zur Urheberrechtsdurchsetzung. Gleichzeitig ist die Deep Packet Inspection im Hinblick auf die Informationsfreiheit aber auch die mildeste Maßnahme. Jedenfalls die Deep Packet Inspection ist also erforderlich.

Betrachtet man die Erforderlichkeit der Maßnahmen isoliert im Hinblick auf die Informationsfreiheit, wäre die Deep Packet Inspection als einzige DVR-Maßnahme zur Durchsetzung des Urheberrechts erforderlich, nicht hingegen IP- und DNS-Sperren. Die Frage der Erforderlichkeit lässt sich nach herrschender Meinung allerdings nicht lediglich im Hinblick auf ein bestimmtes Grundrecht betrachten. Auch die Auswirkungen der Maßnahmen auf andere, ebenfalls betroffene Grundrechte müssen berücksichtigt werden.[722] Da die Beurteilung der Frage des mildesten Mittels sich im Hinblick auf die Beeinträchtigung anderer Grundrechte, insbesondere in Bezug auf die Berufsfreiheit gemäß Art. 12 Abs. 1 GG, anders verhält als bei der Informationsfreiheit, ist die Erforderlichkeit auch von IP- und DNS-Sperren hier gegeben.

---

jeder Hinsicht mildere Mittel zu sein, da es nicht den Internet Service Provider, sondern den Host-Provider adressiert. Für die Informationsfreiheit gilt dies so nicht. Für den in Art. 5 Abs. 1 Fall 2 GG beschwerten Internet-Nutzer ist die Informationsfreiheit unabhängig vom Maßnahme-Adressaten verkürzt, wenn ihm der Zugang zu einer bestimmten Informationsquelle verwehrt wird. Löschmaßnahmen können im Einzelfall genauer auflösen als insbesondere die IP-Sperre und so GGf. Overblocking verhindern. Da die Einschätzung, dass „Löschen statt Sperren" nicht unbedingt effektiver ist als Maßnahmen der Datenverkehrsregulierung, jedoch unangetastet bleibt, wird dadurch auch die Erforderlichkeit von Datenverkehrseingriffen in Bezug auf die Informationsfreiheit nicht angegriffen.

[720] Vgl. oben Kap. 2 V 2 b) (S. 93).

[721] Zu der Tatsache, dass auch eine Deep Packet Inspection false positives nicht vollständig würde vermeiden können und damit ein gewisses Maß an Overblocking produzieren würde, vgl. *Cruz Villalón*, Schlussanträge des Generalanwalts v. 14.04.2011, Rs. C-70/10, Slg. 2011, I-11962, Rn. 86.

[722] BVerfG, Beschl. v. 14.03.2006, 1 BvR 2087/03, 1 BvR 2111/03, Geschäfts- und Betriebsgeheimnisse, BVerfGE 115, 205 (233 f.); vgl. bereits oben Kap. 2 V 1 c) (S. 82 f.).

Schließlich stellt sich die Frage, ob und unter welchen Bedingungen Maßnahmen der DVR zur Durchsetzung des Urheberrechts angemessen sein können. Dies beantwortet sich anhand einer Güterabwägung zwischen der beeinträchtigten Informationsfreiheit und den mit der Maßnahme zu schützenden Interessen.[723] Zum einen muss das der Datenverkehrsregulierung zugrunde liegende *allgemeine Gesetz „durch hinreichend wichtige Gemeinwohlbelange oder schutzwürdige Rechte oder Interessen Dritter"* gerechtfertigt sein.[724] Zum anderen muss nach der sogenannten Wechselwirkungslehre des Bundesverfassungsgerichts das allgemeine Gesetz seinerseits wieder im „im Lichte" der Informationsfreiheit ausgelegt werden, damit dessen überragende Bedeutung auch bei der Rechtsanwendung Berücksichtigung findet.[725]

Fraglich ist, ob bereits bei abstrakter Betrachtung der beiden hier widerstreitenden grundrechtlich geschützten Rechte – die Informationsfreiheit und die Durchsetzung des durch Art. 14 GG[726] geschützten Urheberrechts – das eine Recht schwerer wiegt als das andere.

Art. 14 Abs. 1 Satz 1 GG gewährleistet in Bezug auf das Urheberrecht, dass die wirtschaftlich verwertbaren Ergebnisse der schöpferischen Leistung dem Urheber durch die Ausgestaltung des Privatrechts zugeordnet werden müssen, sowie die Freiheit, über die wirtschaftlich verwertbaren Ergebnisse eigenverantwortlich verfügen zu können.[727] Diese Gewährleistung gilt allerdings nicht uneingeschränkt. Dem Gesetzgeber wird durch Art. 14 Abs. 1 Satz 2 GG erlaubt, das Eigentum durch Gesetze zu beschränken und aufgegeben, dessen Inhalt durch Gesetze auszugestalten. Sieht man von dem Sonderfall der Enteignung ab, die das Bundesverfassungsgericht von den Inhalts- und Schrankenbestimmungen ausdrücklich unterscheidet[728] und deren besondere Zulässigkeitsvoraussetzungen in Art. 14 Abs. 3 GG geregelt werden, ist die Eigentumsgarantie ein Grundrecht mit einfachem Gesetzesvorbehalt.[729] Die Sozialbindung des Eigentums gemäß Art. 14 Abs. 2 GG hält den Gesetzgeber zudem ausdrücklich zur Berücksichtigung von

---

[723] BVerfG, Beschl. v. 01.10.1987, 2 BvR 1434/86, Beschlagnahme von Filmmaterial, BVerfGE 77, 65 (75).
[724] BVerfG, Urt. v. 12.12.2000, 1 BvR 1762/95, 1 BvR 1787/95, Benetton-Werbung I, BVerfGE 102, 347 (363); BVerfG, Beschl. v. 11.03.2003, 1 BvR 426/02, Benetton-Werbung II, BVerfGE 107, 275 (281); *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 5 Rn. 69.
[725] BVerfG, Urt. v. 15.01.1958, 1 BvR 400/51, Lüth, BVerfGE 7, 198 (208); BVerfG, Beschl. v. 01.10.1987, 2 BvR 1434/86, Beschlagnahme von Filmmaterial, BVerfGE 77, 65 (75); BVerfG, Beschl. v. 04.11.2009, 1 BvR 2150/08, Wunsiedel-Versammlung, BVerfGE 124, 300 (331 f.); *Gröpl* in: Gröpl u.a., Grundgesetz, Art. 5 Rn. 81 f.
[726] Vgl oben Kap. 1 IV 2 (S. 36 ff.).
[727] BVerfG, Beschl. v. 07.07.1971, 1 BvR 765/66, Schulbuchprivileg, BVerfGE 31, 229 (240 f.).
[728] BVerfG, Beschl. v. 12.06.1979, 1 BvL 19/76, Kleingarten-Entscheidung, BVerfGE 52, 1 (27 f.); BVerfG, Beschl. v. 19.06.1985, 1 BvL 57/79, Fischerei-Rechte, BVerfGE 70, 191 (199 f.); BVerfG, Beschl. v. 22.05.2001, 1 BvR 1512/97, 1 BvR 1677/97, Baulandumlegung, BVerfGE 104, 1 (9 f.).
[729] *Grochtmann*, Art. 14 GG – Rechtsfragen der Eigentumsdogmatik, S. 320.

Gemeinwohlinteressen bei der Ausgestaltung der Eigentumsinteressen an.[730] Dies gilt umso mehr, je größer die soziale Funktion des Eigentumsobjekts ist.[731]

Demgegenüber ist die Informationsfreiheit ein Grundrecht, dass nur unter den qualifizierten Voraussetzungen des Art. 5 Abs. 2 GG eingeschränkt werden darf. Neben den *allgemeinen Gesetzen* können dies Bestimmungen zum Jugendschutz oder der persönlichen Ehre sein. Während man daraus den Schluss ziehen könnte, dass der Ehr- und der Jugendschutz im Zweifel abstrakt etwas höher zu gewichten sei, so dass aufgrund dieser Zwecke die Informationsfreiheit leichter eingeschränkt werden könnte, fehlt in Art. 5 Abs. 2 GG eine explizite Nennung der (geistigen) Eigentumsrechte, so dass man hieraus ableiten könnte, das Urheberrecht sei abstrakt jedenfalls nicht höherrangig als die Informationsfreiheit.[732] Nicht zuletzt hebt das Bundesverfassungsgericht in großer Regelmäßigkeit die überragende Bedeutung der Grundrechte aus Art. 5 Abs. 1 GG für das politische und gesellschaftliche System der BRD hervor.[733]

Bei rein abstrakter Betrachtung ist das Gewicht der Informationsfreiheit folglich höher einzuschätzen als dasjenige des Urheberrechts.[734] Damit ist allerdings keine Vorentscheidung hinsichtlich einer Rechtswidrigkeit von Eingriffen in den Datenverkehr zur Durchsetzung des Urheberrechts getroffen, sondern lediglich eine Tendenz etabliert, die sich auf die konkrete Beurteilung des Grundrechtseingriffs einseitig auswirkt. Kollidieren zwei Grundrechte, so sind sie im Sinne praktischer Konkordanz in einen möglichst schonenden Ausgleich zu bringen.[735]

Im Rahmen dieser Abwägung müssen zwei grundverschiedene Situationen differenziert werden. Dies hat seinen Grund in den Unterschieden zwischen dem abstrakten, urheberrechtlich-inhaltlichen Teil des weitgehenden Verbots nicht lizenzierten Filesharings und der mit Eingriffen in den Datenverkehr bezweckten Durchsetzung dieses Verbots. Zum einen sind (hypothetische) zielgenaue Eingriffe in den Blick zu nehmen, die ausschließlich

---

[730] BVerfG, Beschl. v. 07.07.1971, 1 BvR 765/66, Schulbuchprivileg, BVerfGE 31, 229 (241).
[731] *Gröpl* in: Gröpl u.a., Grundgesetz, Art. 14 Rn. 57 m.w.N.
[732] In diese Richtung jedenfalls *Baum*, Jugendmedienschutz als Staatsaufgabe, S. 294 und *Heliosch*, Sperrmaßnahmen im Internet, S. 187. Ob sich aus der expliziten Nennung in Art. 5 Abs. 2 GG jedoch tatsächlich ein abstraktes Rangverhältnis systematisch ableiten lässt, soll hier bezweifelt werden. Plausibler erscheint es, dass mit der Aufzählung der besonderen Gefährdung des Ehr- und Jugendschutzes gerade durch die von den Kommunikationsfreiheiten geschützten Verhaltensweisen Rechnung getragen werden soll.
[733] BVerfG, Urt. v. 19.07.1966, 2 BvF 1/65, Parteienfinanzierung II, BVerfGE 20, 56 (97 f.); BVerfG, Beschl. v. 14.10.1969, 1 BvR 30/66, Verzögerte Postauslieferung, BVerfGE 27, 88 (98); BVerfG, Beschl. v. 09.02.1994, 1 BvR 1687/92, Parabolantenne, BVerfGE 90, 27 (33 f.); BVerfG, Urt. v. 12.12.2000, 1 BvR 1762/95, 1 BvR 1787/95, Benetton-Werbung I, BVerfGE 102, 347 (363); *Schmidt-Jortzig* in: Isensee/P. Kirchhof, HStR VII, § 162 Rn. 52; *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 5 Rn. 69.
[734] Eher in Richtung einer abstrakten Gleichrangigkeit zwischen Informationsfreiheit und Art. 14 GG tendierend hingegen BVerfG, Beschl. v. 09.02.1994, 1 BvR 1687/92, Parabolantenne, BVerfGE 90, 27 (34).
[735] BVerfG, Beschl. v. 17.12.1975, 1 BvR 63/68, Simultanschule, BVerfGE 41, 29 (50 f.); BVerfG, Beschl. v. 16.05.1995, 1 BvR 1087/91, Kruzifix-Entscheidung, BVerfGE 93, 1 (21).

den Zugriff des Bürgers auf urheberrechtsverletzende Inhalte verhindern. Zum anderen ist das Augenmerk auf die tatsächlich verfügbaren datenverkehrsregulierenden Maßnahmen zu richten, die allesamt, wenn auch in unterschiedlichem Maße, neben illegalem *Filesharing* auch den Zugriff des Bürgers auf urheberrechtlich unproblematische Informationen verhindern („Overblocking").

a. Maßnahmen gegen ausschließlich das Urheberrecht verletzende Inhalte

Weniger problematisch aus der Perspektive der Informationsfreiheit ist das zielgenaue Sperren urheberrechtlich geschützter Inhalte, d.h. ausschließlich solcher Inhalte, die urheberrechtswidrig angeboten werden.

Dies ergibt sich zwar nicht bereits unmittelbar aus der gesetzgeberischen Wertung, illegales Filesharing zivil- (vgl. §§ 97 ff. UrhG) und strafrechtlich (vgl. §§ 106 ff. UrhG) mit Sanktionen zu belegen. Der Gesetzgeber kann sich nicht dadurch dem Anwendungsbereich der Informationsfreiheit entziehen, indem er den Zugriff auf bestimmte Informationen verbietet. Auf diesem Wege könnte der Staat ansonsten die vom Grundgesetz gesetzten Grenzen seines Handelns aus Art. 5 Abs. 1 GG umgehen, so dass die effektive Schutzgarantie der Informationsfreiheit vollständig leerlaufen würde.[736] Die gesetzgeberische Wertung, die letztlich als Ergebnis der Abwägung in einem parlamentarischen Prozess zustande gekommen ist, Verstößenn gegen das Urheberrecht notfalls mit strafrechtlichen Sanktionen entgegenzutreten, soll hier nichtsdestotrotz in die rechtliche Bewertung einfließen.

Auch das Verhindern des Unterrichtens aus einer Quelle, die offensichtlich urheberrechtswidrig ist, greift in die Informationsfreiheit ein. Gewissermaßen ist ein großer Teil des Urheberrechtsschutzes insgesamt letztlich ein Eingriff in die Informationsfreiheit, jedenfalls sobald das reine Privatrecht verlassen wird und der Staat dessen Durchsetzung verfolgt.[737]

Das Urheberrechtsgesetz schützt jedoch nicht ausschließlich die Interessen der Urheber, sondern wird u.a. durch diverse Schrankenbestimmung den durch die Informationsfreiheit geschützten Interessen der Bürger auf Zugang zu Informationen gerecht.[738] Insoweit trägt das Urheberrecht bereits einen gewissen Ausgleich der sich gegenüberstehenden Interessen in sich, so dass die von der Wechselwirkungslehre geforderte Berücksichtigung

---

[736] *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 5 Rn. 23. Vgl. bereits oben Kap. 3 III 1 (S. 169).

[737] Zur Frage der Bindung des Privatrechtsgesetzgebers an die Grundrechte und die Ausstrahlung der Grundrechte ins Privatrecht s. bereits oben Kap. 3 II 1 b) (5) (S. 141) und grundlegend BVerfG, Urt. v. 15.01.1958, 1 BvR 400/51, Lüth, BVerfGE 7, 198 (205 ff.).

[738] *Kröger*, Informationsfreiheit und Urheberrecht, S. 331; kritisch dazu hingegen: *Berger*, ZUM 2004, 257 (264 f.). Sein Argument, dass die Informationsfreiheit gerade nicht einschlägig sei, da der Gesetzgeber durch die Verleihung von Ausschließlichkeitsrechten die Quellen der „allgemeinen Zugänglichkeit" entreiße, vernachlässigt, dass die urheberrechtlichen Schranken nicht isoliert betrachtet werden können und erst einen harmonischen Ausgleich konkurrierender Grundrechte im Urheberrecht herzustellen versuchen. Die Verleihung der Ausschließlichkeitsrechte muss sich schließlich ebenfalls (u.a.) an Art. 5 Abs. 1 Satz 1 GG messen lassen und wird erst durch die urheberrechtlichen Schranken den Anforderungen der Wechselwirkungslehre gerecht.

der Informationsfreiheit bei der Anwendung des allgemeinen Gesetzes hier bereits auf legislativer Ebene erfolgt ist.

Ergibt eine Überprüfung anhand des Urheberrechtsgesetzes, dass das Filesharing eines bestimmten Werkes trotz der Berücksichtigung der Informationsfreiheit, insbesondere im Rahmen der urheberrechtlichen Schrankenregelungen, illegal ist, so soll die Rechtmäßigkeit der Durchsetzung des Verbots, das Werk zu teilen, hier nicht in Frage gestellt werden. Ein zielgenaues Sperren urheberrechtswidriger Inhalte ohne jegliches Overblocking ist folglich eine angemessene Beschränkung der Informationsfreiheit. Dies gilt unabhängig von der Art der Durchsetzungsmaßnahme und generell, allerdings selbstverständlich nur, soweit es durch die Maßnahme nicht zu Einschränkungen anderer Grundrechte und grundgesetzlich geschützter Interessen oder der Informationsfreiheit Dritter kommt.

Letzteres ist jedoch in Form von Overblocking bei jeder Form von Sperr- und Filtermaßnahmen in unterschiedlichem Ausmaß der Fall; in geringerem Maße bei der DPI und am stärksten bei IP-Sperren. Netzsperren und -Filter zur Durchsetzung des Urheberrechts sind zum gegenwärtigen Stand der Technik nicht denkbar, ohne dass sie zugleich Overblocking mit sich bringen würden.[739]

b. Overblocking

Praktisch relevant ist daher vor allem die Frage, ob auch Maßnahmen, die zu *Overblocking* führen oder führen können, angemessene Eingriffe in die Informationsfreiheit darstellen können, und wenn ja, unter welchen Voraussetzungen der Fall ist.

Denkbar sind grundsätzlich drei verschiedene Wege, den Konflikt zwischen den hier widerstreitenden Interessen aufzulösen. Zum einen gäbe es die Möglichkeit, der Durchsetzung der urheberrechtlich geschützten Interessen absoluten Vorrang zu gewähren und die Informationsfreiheit bezüglich unbeabsichtigt mitgesperrter Informationen im Zweifel stets zurücktreten zu lassen.[740]

Die zweite Möglichkeit wäre, Eingriffe in den Datenverkehr zur Urheberrechtsdurchsetzung generell als Verletzung der Informationsfreiheit einzustufen und damit auch generell als unzulässig zu verwerfen.

Als dritte Option verbliebe die Möglichkeit, Maßnahmen der DVR zur Durchsetzung des Urheberrechts für eingeschränkt zulässig zu erachten, wenn das Ausmaß des Overblockings im Verhältnis zum erreichten Regulierungsziel (also der Verhinderung illegalen Filesharings) eine bestimmte Grenze nicht überschreitet.[741]

---

[739] Wie zuvor bereits festgestellt, vgl. oben Kap. 2 V 2 b) (S. 93 f.).
[740] So etwa *Nazari-Khanachayi*, Zulässigkeit von Zugangserschwerungsverfügungen gegen Access-Provider bei (drohenden) Urheberrechtsverletzungen, S. 83.
[741] *Trstenjak*, GRUR Int. 2012, 393 (401).

Der Durchsetzung des Urheberrechts absoluten Vorrang zu gewähren, ist eine verfassungsrechtlich nicht gangbare Option. Im Extremfall gedacht, würde dies eine Vollsperrung des Internets zur Verhinderung der Verletzung der Rechte an einem einzigen geschützten Werk bedeuten. Doch es bedarf nicht dieses dramatischen Beispiels mit seinem evident unzulässigen Ergebnis, um zu dieser Schlussfolgerung zu kommen. Wie soeben festgestellt, ist das abstrakte Gewicht der Informationsfreiheit als höher einzuschätzen als dasjenige des Urheberrechts.

Der möglichst freie Zugang zu Informationen mitsamt seiner Bedeutung für eine funktionierende demokratische Republik und Gesellschaft kann nicht der Durchsetzung einzelner Vermögensrechte abwägungsfrei geopfert werden, während der ökonomische Effekt der Durchsetzungsmaßnahmen bislang weder hinreichend quantifizierbar noch überhaupt in der ökonomischen Forschung unumstritten ist. Ein absoluter Vorrang der Durchsetzung des Urheberrechts würde zum einen eine Vielzahl urheberrechtlich unproblematischer Inhalte betreffen, die die Anzahl der urheberrechtlich problematischen Inhalte bei weitem übertreffen. Wird eine IP-Sperre verwendet, kann dies sogar Inhalte betreffen, die keine Verbindung zum ins Ziel genommenen Content Provider besitzen und nur zufällig auf demselben Server gehostet werden.[742]

Zum anderen ist aber nicht nur die Extensität, sondern auch die Intensität der Beeinträchtigung der Informationsfreiheit zu beachten, wenn etwa versehentlich einige wenige, aber bezüglich der politischen Meinungsbildung besonders wertvolle Informationen den Netzsperren als Kollateralschaden zum Opfer fallen. Eine Maßnahme zur Sperrung von Inhalten, die die Betroffenheit von Art. 5 Abs. 1 Satz 1 Alt. 2 GG nicht im Einzelfall berücksichtigt, kann den Anforderungen der Wechselwirkungslehre nicht gerecht werden.

Der Gerichtshof tendiert in dieser Frage, wie oben bereits ausführlich besprochen, wohl zu einer Abwägungslösung, ohne aber zu klären, ob der derzeitige Stand der Technik nicht doch dazu führt, dass in Anbetracht der großen Effektivitätsdefizite im Ergebnis keine technisch durchführbare Maßnahme vor der Informationsfreiheit Bestand hat.[743] Eingriffe in den Datenverkehr können laut EuGH nur dann mit der Informationsfreiheit zu vereinbaren sein, wenn sie den Zugang zu rechtmäßigen Inhalten jedenfalls nicht *unnötig* verhindern. [744] Da der EuGH in der betreffenden Entscheidung wohl davon ausgegangen sein dürfte, dass DPI-Filtersysteme generell unzulässig seien,[745] kann man diese Aussage so deuten, dass IP- und DNS-Sperren die Informationsfreiheit nicht verletzen, wenn a) im Einzelfall kein Overblocking stattfindet, oder b), wenn zwar Overblocking stattfindet, aber die Maßnahme gewählt wird, die die geringste Beeinträchtigung der Informationsfreiheit bedeutet, und sie so effektiv ist, dass der unberechtigte Zugriff der Internet-Nutzer auf

---

[742] *Sieber/Nolde*, Sperrverfügungen, S. 50.
[743] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192.
[744] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 63 f.
[745] Vgl. EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959.

den Schutzgegenstand insgesamt zuverlässig verhindert wird, gleich auf welche Art dieser erfolgt.[746]

Dieser Abwägungsmaßstab entspricht nicht eins zu eins der deutschen Grundrechtsdogmatik. Der wesentliche Unterschied besteht darin, dass der EuGH auf den ersten Blick nicht die Schwere der Beeinträchtigung der Informationsfreiheit im Einzelfall berücksichtigt, sondern lediglich die Effektivität der Maßnahme.[747] Dieses Vorgehen ist mit der Wechselwirkungslehre, die stets die Berücksichtigung der Bedeutung der Informationsfreiheit auch im Einzelfall verlangt, schwerlich zu vereinbaren.[748] Ein wirklicher Konflikt besteht hier allerdings nicht, da das UPC-Urteil lediglich einen Mindestschutz für die Meinungsfreiheit vorgibt, seine Rechtsprechung einem stärkeren Schutz der Informationsfreiheit auf nationaler Ebene hier allerdings nicht entgegensteht.[749] In der Prüfung einer Verletzung von Art. 5 Abs. 1 Satz 1 GG ist daher auch der Umfang und die Intensität der Beeinträchtigung der Informationsfreiheit im Einzelfall zu berücksichtigen.

(1) Zulässiges Ausmaß von Overblocking

Für den Fall, dass das Overblocking lediglich legale Inhalte auf dem zu sperrenden Internet-Angebot betrifft, hat der Bundesgerichtshof aus der soeben zitierten UPC-Entscheidung des EuGH den Schluss gezogen, dass Netzsperrungsverfügungen nicht zwingend gegen die Informationsfreiheit verstoßen würden. Ansonsten bestünde für die Anbieter illegaler Inhalte die Möglichkeit, sich durch das Angebot einiger weniger legaler Angebote auf derselben Website der Durchsetzung des Urheberrechts entziehen zu können.[750] Ausschlaggebend sei daher das Verhältnis zwischen rechtswidrigen und rechtmäßigen Inhalten, wobei die rechtmäßigen Inhalte allerdings „*nicht ins Gewicht fallen*“ dürften.[751]

---

[746] Vgl. dazu oben Kap. 2 V 4 (S. 118).

[747] Die dogmatischen Ausführungen des EuGH dazu sind knapp. Es ist nicht auszuschließen, dass der Gerichtshof in seiner Entscheidung auch die Schwere der Beeinträchtigung der Informationsfreiheit berücksichtigen wollte. Er deutet dies mit der sich nicht vollständig mit dem Rest seiner Ausführungen inhaltlich vereinbarenden Aussage an, dass Internet-Nutzer nicht bei dem Versuch, rechtmäßig Zugang zu Informationen zu erlangen, durch Maßnahmen der DVR beeinträchtigt werden dürften, vgl. EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 56. Denkbar wäre eine solche Interpretation des EuGH, dass er die Schwere der Grundrechtsbeeinträchtigung durchaus in eine Abwägungsentscheidung mit einfließen lassen hat, sich hier aber unpräzise ausdrückte.

[748] *Wendt* in: v. Münch/Kunig, Grundgesetz Bd. 1, 7. Aufl. 2021, Art. 5 Rn. 120.

[749] EuGH, Urt. v. 26.02.2013, Rs. C-617/10, EU:C:2013:105, Rn. 19; BVerfG, Urt. v. 24.04.2013, 1 BvR 1215/07, Antiterrordatei, BVerfGE 133, 277, Rn. 91.

[750] BGH, Urt. v. 12.07.2007, I ZR 18/04, Jugendgefährdende Medien bei eBay, BGHZ 173, 188, Rn. 60; BGH, Urt. v. 12.07.2012, I ZR 18/11, Alone in the Dark, BGHZ 194, 339, Rn. 45; BGH, Urt. v. 15.08.2013, I ZR 80/12, Filehosting-Dienst, NJW 2013, 3245, (3250); *J. B. Nordemann* in: Fromm/Nordemann, Urheberrecht, § 97 Rn. 170; *Leistner*, ZUM 2012, 722 (730); *Leistner/Grisse*, GRUR 2015, 105 (108 f.).

[751] BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 55; BGH, Urt. v. 26.11.2015, I ZR 3/14, 3dl.am, Rn. 44 (juris). Danach seien mitgesperrte legale Inhalte mit einem Gesamtanteil an den gesperrten Inhalten in Höhe von 4 % kein Grund, eine Verletzung der Informationsfreiheit anzunehmen; ebenso *Leistner/Grisse*, GRUR 2015, 105 (109); a.A.: OLG Köln, Urt. v. 18.07.2014, I-6 U 192/11, 6 U 192/11, Goldesel, Rn. 974 (juris).

Wie zu entscheiden wäre, würden die Angebote anderer Anbieter mitgesperrt, die zufällig unter derselben IP-Adresse wie das Ziel der Sperrmaßnahme zu erreichen sind, erklärt der BGH mangels Sachverhaltsrelevanz weder in seiner Goldesel-[752] noch in seiner 3dl.am-Entscheidung.[753] Denkt man allerdings die Formel des BGH zu Ende, dass die rechtmäßigen Inhalte nicht ins Gewicht fallen dürften, wird man wohl zu dem Ergebnis gelangen, dass das relevante Gewicht aus seiner Sicht bei – in der Regel vollständig – blockierten Drittinhalten überschritten sein dürfte.[754] Dies müsste umso mehr gelten, als zum einen in diesem Fall nicht das Risiko besteht, dass der Anbieter der illegalen Inhalte hier versucht, sein Angebot durch ein Feigenblatt legaler Inhalte der Rechtsdurchsetzung zu entziehen, und zum anderen der Anbieter der legalen Inhalte vollumfänglich schutzwürdig wäre.[755]

Gegen diese Ausführungen des BGH bzw. die gedankliche Fortführung seiner Argumentation ist aus verfassungsrechtlicher Perspektive wenig vorzubringen, da der Ausgleich zwischen Art. 5 Abs. 1 Satz 1 Alt. 2 GG auf der einen und Art. 14 Abs. 1 GG auf der anderen Seite gelingt. Es handelt sich dabei um die äußersten Grenzen dessen, welcher Umfang an *Overblocking* zulässig sein dürfte, wenn denn zusätzlich die anderen Voraussetzungen einer Vereinbarkeit mit der Informationsfreiheit erfüllt werden: Ist der Content Provider schutzwürdig, weil er in keinerlei Verbindung zur Rechtsverletzung steht, darf dem Nutzer auch nicht der Zugriff auf dessen Inhalte verweigert werden. Mögliche Urheberrechtsverletzungen durch Dritte müssen dann gegebenenfalls hingenommen werden.[756]

Ist der Content Provider hingegen nicht schutzwürdig, da die von ihm angebotenen Inhalte weit überwiegend illegal sind, wäre es nicht verhältnismäßig, das Interesse des Urhebers an seiner Rechtsdurchsetzung einzig mit dem Argument abzuwehren, dass einige wenige vom Content Provider bereitgestellte Inhalte rechtmäßig sind. Wo exakt diese Grenze zu ziehen ist, muss eine Frage des Einzelfalles bleiben. Eine feste quantifizierbare Grenze, unabhängig von der Frage, ob diese von einer absoluten Zahl an illegalen Inhalten oder aber von einem Verhältnis zwischen legalen und illegalen Angeboten ausgeht, greift

---

[752] BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82.
[753] BGH, Urt. v. 26.11.2015, I ZR 3/14, 3dl.am.
[754] So auch *Spindler*, GRUR 2016, 451 (455).
[755] Auch der Internet-Nutzer, der auf legal bereitgestellte Inhalte zugreifen möchte, dürfte in der Regel in höherem Maße schutzwürdiger sein als derjenige, der sich aus oftmals eindeutig rechtswidrigen Quellen bedient.
[756] Anderer Ansicht ist *Heliosch*, Sperrmaßnahmen im Internet, S. 191. Technisch bedingt unvermeidbares Overblocking könne für sich allein genommen nicht dazu führen, dass der staatliche Schutzzweck hinter die Informationsfreiheit zurücktreten müsse. Entscheidend sei, dass das Overblocking nicht beabsichtigt sei. Dem Argument kann hier nicht zugestimmt werden. Der Eingriff in Art. 5 Abs. 1 GG bleibt aus Sicht des Nutzers unverändert intensiv, ob dies nun bezweckt ist oder nicht. Eine Rechtsgrundlage für DVR-Maßnahmen, die auf absichtliches Blocken rechtmäßiger Inhalte zielen würde, könnte im Übrigen bereits Probleme haben, als allgemeines Gesetz qualifiziert zu werden.

zu kurz.[757] Eine solche Grenze könnte nämlich nicht berücksichtigen, wenn es sich bei den von Overblocking betroffenen Inhalten um besonders schützenswerte Informationsquellen mit hoher Bedeutung für die öffentliche Meinungsbildung handelt.[758] Bei der fälligen Abwägung im Einzelfall ist zudem stets das oben festgestellte abstrakt höhere Gewicht der Informationsfreiheit zu berücksichtigen.

(2) Möglichkeiten effektiven Rechtsschutzes gegen Overblocking

Weiterhin gibt der EuGH vor, dass eine DVR-Maßnahme nur dann rechtmäßig sei, wenn dem von Overblocking betroffenen Nutzer auch nach erfolgter DVR-Maßnahme die Möglichkeit gegeben sei, diese auf eine Verletzung der Informationsfreiheit hin überprüfen zu lassen. Die genaue Ausgestaltung des Rechtsschutzes überlässt er dabei den Mitgliedstaaten.[759]

Die Notwendigkeit einer Rechtsschutzmöglichkeit für den Internet-Nutzer, gegen eine eventuelle Verletzung von Art. 5 Abs. 1 Satz 1 Alt. 2 GG durch Datenverkehrseingriffe vorzugehen, dürfte auch nach nationalem Verfassungsrecht bestehen. Der einzelne Internet-Nutzer wird in einem Sperrverfahren, ob man dies nun behördlich oder durch die Gerichte durchführt, nicht als Partei vertreten sein.

Die Garantie effektiven Rechtsschutzes gegen Akte öffentlicher Gewalt gemäß Art. 19 Abs. 4 GG verlangt jedoch, dass der Internet-Nutzer, dessen Grundrecht auf Informationsfreiheit durch datenverkehrsregulierende Maßnahmen beschränkt wird, diese gerichtlich auf ihre Rechtmäßigkeit hin überprüfen lassen kann.[760] Neben seiner Eigenschaft als subjektives Recht stellt Art. 19 Abs. 4 GG darüber hinaus eine institutionelle Garantie dar, die eine Organisation der Rechtsschutzmöglichkeiten in einer Weise verlangt, dass dem Bürger wirksamer Rechtsschutz, d.h. insbesondere auch in angemessener Zeit, offen steht.[761]

---

[757] Die Rechtsprechung, namentlich der Bundesgerichtshof in BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 55 und das OLG Köln, Urt. v. 18.07.2014, I-6 U 192/11, 6 U 192/11, Goldesel, Rn. 974 f. (juris) näherten sich der Frage quantitativ, sind sich aber bei der Beurteilung eines 4-Prozent-Anteils legaler Inhalte uneins.

[758] Auch aus diesem Grund kann die letzte Entscheidung, ob eine Netzsperre einzurichten ist oder nicht, nicht beim ISP liegen. Internet Service Provider besitzen weder die Qualifikation noch die Legitimation, diese Art von Grundrechtsabwägungen zu leisten. Dies ist ein Vorwurf, dem sich die ISPs kaum entgegenstellen würden. Grundrechtsabwägungen dieser Art im Einzelfall durchzuführen, ist in Deutschland den Gerichten und Behörden mit staatsfern besetzen Aufsichtsgremien vorbehalten. Vgl. dazu auch *Assion*, K&R 2014, 329 (334), Fn. 12.

[759] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 57.

[760] Dies gilt uneingeschränkt, wenn die Sperrmaßnahme durch eine Behörde angeordnet wird. Doch auch wenn die Maßnahme der DVR durch ein Gericht angeordnet wurde, hat der Bürger Anspruch auf einen gleichwertigen Rechtsschutz. Ob man dieses Recht nun aus Art.19 IV GG oder dem allgemeinen Justizgewährleistungsanspruch ableitet, ist eher eine dogmatische Frage. Vgl. dazu *Papier* in: Isensee/P. Kirchhof, HStR VIII, § 177 Rn. 16. Zudem gilt auch das bereits oben auf Kap. 3 II 1 b) (5) (S. 142) in etwas anderem Kontext gebrachte Argument, dass der Staat sich nicht durch die Ausgestaltung des Verfahrens der Grundrechtsgeltung entziehen können soll.

[761] *Papier* in: Isensee/P. Kirchhof, HStR VIII, § 177 Rn. 3.

Der BGH sieht die vom EuGH geforderte Rechtsschutzmöglichkeit im deutschen Recht bereits ohne weiteres angelegt. Der Nutzer könne seinen ISP auf Basis des zwischen ihnen geschlossenen Vertragsverhältnisses auf Aufhebung der Sperre verklagen.[762]

Die bereits oben angedeutete Kritik an der praktischen Durchführbarkeit eines tatsächlich effektiven Rechtsschutzes konnte der BGH mit seinem Lösungsvorschlag jedoch nicht entkräften.[763] Unabhängig von der konkreten rechtlichen Ausgestaltung bleibt das grundsätzliche Problem, dass Prozessrisiken und -dauer für die Internet-Nutzer ein prohibitiver Faktor bei der Rechtsverfolgung sein dürften.[764] Selbst ein mögliches Vorgehen im einstweiligen Rechtsschutz würde für einen Internet-Nutzer in der Regel daran nichts ändern. Anstatt einen Prozess zu führen, wird der ökonomisch denkende Internet-Nutzer vielmehr versuchen, auf eine andere Informationsquelle auszuweichen. Die Kontrollfrage schließlich, die die Absurdität eines solchen gerichtlichen Verfahrens aufzeigt, lautet, was denn passieren würde, wenn die Internet-Nutzer in einem hypothetischen Szenario tatsächlich ihre Rechtsschutzmöglichkeiten ausschöpfen würden. Durch das Overblocking einer beliebten Internet-Seite können schnell Millionen Nutzer in ihrer Informationsfreiheit betroffen sein. Würde davon nur ein Bruchteil den Weg zum Gericht beschreiten, wäre die Justiz in kürzester Zeit überlastet.

Eine praktisch für den Betroffenen wertlose Rechtsschutzmöglichkeit erfüllt allerdings nicht die Erfordernisse des Grundgesetzes.[765] Es muss daher festgehalten werden, dass die Durchführung von Eingriffen in den Datenverkehr nur dann mit dem Grundgesetz vereinbar ist, wenn der Staat einen Verfahrensweg bereitstellt, über den der Bürger auch effektiv sein Recht auf Informationsfreiheit durchsetzen kann.

---

[762] BGH, Urt. v. 26.11.2015, I ZR 3/14, 3dl.am, Rn. 46 (juris); BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82; ebenso: *Leistner/Grisse*, GRUR 2015, 105 (110); *J. B. Nordemann*, ZUM 2014, 499 (500); *Spindler*, GRUR 2014, 826 (833). Zur Kritik aus der Literatur an einer Lösung über das Vertragsrecht de lege lata: *Nazari-Khanachayi*, GRUR 2015, 115 (122) hält den Verweis an die Internet-Nutzer, sich doch über das Vertragsrecht gegenüber ihrem Access Provider ihr Recht zu verschaffen, zumindest noch für eine gangbare Übergangslösung. Dafür müssten die Provider allerdings in der Regel zunächst ihre AGB anpassen. *Nordemann*, ZUM 2014, 499 (500) hält den vertragsrechtlichen Weg für gangbar, schlägt aber dennoch eine Alternativlösung über die richterliche Rechtsfortbildung vor. *Ohly*, ZUM 2015, 308 (318) hingegen hält die vertragsrechtliche Lösung für generell ungeeignet, da es sich um einen grundrechtssensiblen Bereich handle, der andere Ansprüche ans Verfahren stelle. *Spindler*, GRUR 2014, 826 (833 f.) bringt das Argument, dass der Schutz des Bürgers über das Vertragsrecht lückenhaft sei. Insbesondere habe nicht jeder Internetnutzer ein Vertragsverhältnis zu dem ISP, der die Netzsperre umsetzt.

[763] Vgl. oben Kap. 2 V 2 b) (S. 94).

[764] *Marley*, Gewerblicher Rechtsschutz und Urheberrecht 2014, 472 (473) bezeichnet die Vorstellung, dass ein Internet-Nutzer seinen Access Provider auf Zugang zu einer bestimmten gesperrten Website verklage, nicht zu Unrecht als „*mehr als nur ein wenig realitätsfern*". Zudem weist er zurecht auf das absurde Ergebnis hin, dass in diesem Falle zwei Parteien über die Rechtmäßigkeit einer Sperrmaßnahme streiten würden, die an einer Urheberrechtsverletzung gar nicht beteiligt gewesen seien.

[765] Vgl. *Papier* in: Isensee/P. Kirchhof, HStR VIII, § 176 Rn. 22.

Auch der EuGH ist insoweit deutlich, wenn er feststellt, dass Maßnahmen, bei denen dem Bürger eine solche Rechtsschutzmöglichkeit nicht offen stünde, nicht vor den Grundrechten bestehen könnten. Wenn dies nicht möglich sein sollte, dann bleibt lediglich das Ergebnis, dass eine Datenverkehrsregulierung zur Durchsetzung des Urheberrechts generell rechtswidrig ist, wenn auch Overblocking nicht ausgeschlossen werden kann. Dies ist eine Möglichkeit, die der EuGH in seiner UPC-Entscheidung offen lässt. Tenoriert wurde lediglich, dass das Europarecht entsprechenden Maßnahmen nicht entgegenstehe, wenn gewisse Voraussetzungen erfüllt wären.[766]

Einen Ausweg aus dieser Lage könnte jedoch eine Weiterentwicklung des Vorschlags *Assions* bieten, bereits die Anordnung möglicher Netzsperren nicht durch die Justiz, sondern durch eine (staatsfern organisierte) Behörde erfolgen zu lassen.[767] Bei dieser Behörde könnte ein Internet-Nutzer seine Betroffenheit rügen. Eine Behörde kann – zumindest eher als ein Gericht – der Beschwer eines Bürgers durch eine kurzfristige Entscheidung abhelfen. Zwar fordert der EuGH ausdrücklich die *gerichtliche* Überprüfbarkeit der Maßnahme auf Konflikte mit der Informationsfreiheit. Wenn die fragliche Behörde der Beschwerde des Nutzers allerdings nicht abhelfen würde, wäre diese Entscheidung aber auf verwaltungsgerichtlichem Wege überprüfbar.

(3) Erforderliche Mindesteffektivität der DVR-Maßnahmen

Schließlich ist in einer Abwägung zwischen den konkurrierenden schützenswerten Interessen auch die Frage nach der Effektivität der einschlägigen Maßnahmen zu stellen.

Dies ist ein sowohl im Rahmen der europäischen wie auch der nationalen Grundrechtsprüfung zu berücksichtigender Punkt, was den EuGH in seiner UPC-Entscheidung dann auch zu einer Befassung mit den Anforderungen an die Effektivität der Maßnahmen bewogen hat. Konsequenterweise geht auch der BGH in seiner *Goldesel*-Entscheidung auf die vom EuGH aufgestellte Anforderung ein, dass eine Maßnahme der DVR nur dann rechtmäßig sein könne, wenn sie hinreichend wirksam sei. Anders als die Äußerungen des EuGH in dieser Arbeit interpretiert werden,[768] legt der Bundesgerichtshof das Effektivitätskriterium des EuGH streng maßnahmebezogen aus. Der Einfluss der Eingriffe in den Datenverkehr auf die Rechtsverletzungen insgesamt sei irrelevant, es zähle nur die Auswirkung auf die konkret von der Sperrmaßnahme betroffene Website. Doch der BGH geht hier noch weiter. Er erklärt auch das Erfordernis der maßnahmebezogenen Effektivität im Ergebnis für irrelevant: Denn die Tatsache, dass die Anbieter illegaler Inhalte die Sperren mühelos umgehen könnten, sei unerheblich. Eine solch strenge Auslegung hält der Bundesgerichtshof für notwendig, da die Rechteinhaber im Internet ansonsten potentiell schutzlos wären.[769]

---

[766] EuGH, Urt. v. 27.03.2014, Rs. C-314/12, UPC-Telekabel, EU:C:2014:192, Rn. 57, 64.
[767] *Assion*, K&R 2014, 329 (334).
[768] Vgl. oben Kap. 2 V 2 e) (S. 98).
[769] BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 47; zustimmend: *Spindler*, GRUR 2016, 451 (454); zurückhaltender noch in *Spindler*, GRUR 2014, 826 (831 f.), jedenfalls in Bezug auf DNS-Sperren.

Die Effektivität datenverkehrsregulierender Maßnahmen wurde bereits eingehend besprochen.[770] Der EuGH hat hierzu – wenn auch sehr abstrakt – entschieden, welcher Grad an Effektivität aus seiner Sicht mindestens erforderlich sei, damit Eingriffe in den Datenverkehr zur Urheberrechtsregulierung die Grundrechte nicht verletzen würden. Der Maßstab des EuGH ist schutzniveaubezogen.[771] Eine DVR zur Urheberrechtsdurchsetzung müsse die geschützten Werke überwiegend effektiv sichern, und zwar in einem Maß, dass die Schutzzwecke des Urheberrechtsschutzes für das konkrete Werk im Einzelfall durchgesetzt würden, das Urheberrecht am Werk also nicht leerlaufe.[772] Nicht hingegen wird verlangt, dass das geschützte Recht absolut durchgesetzt werde. Geringfügiges Underblocking verhindere also nicht bereits die Vereinbarkeit einer Maßnahme mit der Informationsfreiheit.

Vor diesem Hintergrund wird deutlich, dass die Mindesteffektivität datenverkehrsregulierender Maßnahmen in ihrer Relevanz für die Zulässigkeit dieser Eingriffe nicht beliebig weit unten angesetzt werden kann. Diesen Vorwurf muss sich der BGH hier jedoch gefallen lassen. Zwar ist dem Bundesgerichtshof zuzustimmen, dass das Schutz- und Durchsetzungsdefizit geistigen Eigentums im Internet das stärkste Argument für eine Durchsetzung des Urheberrechts mit Hilfe von Eingriffen in den Datenverkehr ist.[773] In Anbetracht der Vielzahl und der Schwere der Eingriffe in konkurrierende Grundrechte muss eine Mindesteffektivität der Eingriffe in den Datenverkehr schutzniveaubezogen gewahrt sein.

Es kann nicht unberücksichtigt bleiben, ob durch die Durchführung einer datenverkehrsregulierenden Maßnahme die Beeinträchtigungen der Schutzgüter im schlimmsten Falle insgesamt unverändert bleiben, während auf der anderen Seite grundrechtlich geschützte Interessen in jedem Falle massenhaft und intensiv beschränkt werden. Eine bezogen auf den Schutz des Werks womöglich minimal effektive Maßnahme, die lediglich die Transaktionskosten der Nutzer durch leicht erhöhten Zeitaufwand steigert, kann schwere Eingriffe in die Informationsfreiheit und andere Grundrechte nicht rechtfertigen. Die Durchführung einer Maßnahme der DVR nur aus rechtsstaatlich-symbolischen Gründen, weil der Rechteinhaber ansonsten weitgehend rechtsschutzlos stehen würde, widerspricht eklatant dem Grundgedanken des Verhältnismäßigkeitsgrundsatzes.[774]

---

[770] Vgl. oben Kap. 1 IV 3 (S. 37 ff.).
[771] Dazu ausführlich oben Kap. 2 V 2 e) (S. 98).
[772] Vgl. oben Kap. 2 V 2 e) (S. 95).
[773] Vgl. BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 47.
[774] Aus der Perspektive einfachen deutschen Rechts kommt ein weiteres Argument gegen eine maßnahmebezogene Interpretation des Effektivitätskriteriums hinzu. Der Schutz des Urheberrechts im deutschen Recht ist deliktsrechtlich ausgestaltet, vgl. §§ 97 ff. UrhG. Konsequenterweise erkennt der BGH die deliktsrechtlich geprägte Störerhaftung (vgl. auch *Wagner* in: MüKoBGB – Bd. 7: Schuldrecht BT II, Vor § 823 BGB Rn. 39 als Mittel zur Erzwingung datenverkehrsregulatorischer Maßnahmen zur Urheberrechtsdurchsetzung grundsätzlich an, vgl. BGH, Urt. v. 26.11.2015,

Eingriffe in den Datenverkehr zur Urheberrechtsregulierung müssen daher unterbleiben, wenn sie die erforderliche Mindesteffektivität nicht gewährleisten. Dies gilt insbesondere auch dann, wenn zum gegenwärtigen Stand der Technik keines der verfügbaren und nicht bereits aus anderen Gründen unzulässigen Verfahren diese Anforderungen erfüllt. Eingriffe in den Datenverkehr zur Durchsetzung des Urheberrechts wären in diesem Falle insgesamt unzulässig. Ein anderes Ergebnis wird auch vom EuGH im UPC-Urteil nicht vorgegeben. Der EuGH erwähnt an keiner Stelle, dass ein Verfahren existiere, das seinen Anforderungen an die Effektivität gerecht würde. Es mag sein, dass bezüglich einiger konkreter Verletzungshandlungen dann keine Möglichkeit für den Staat besteht, diese Verletzungshandlungen zu unterbinden. Im Einzelfall nicht durchsetzbare Rechte sind jedoch auch in anderen Bereichen nicht immer zu vermeiden, auch dann nicht, wenn es faktische Möglichkeiten der Durchsetzung gäbe, die aber schlichtweg unangemessen wären.

Weder IP-Sperren noch DNS-Sperren bieten die notwendige schutzniveaubezogene Effektivität, um durch Overblocking verursachte Beschränkungen der Informationsfreiheit angemessen erscheinen zu lassen. Maßnahmen unter Verwendung von Deep Packet Inspection können die geforderte Mindesteffektivität leisten, da sie durch einfache Umgehungsmaßnahmen der Anbieter oder der Internet-Nutzer kaum auszuhebeln sind, und zudem so breitflächig eingesetzt werden können, dass mit ihrer Hilfe auch die geforderte schutzniveaubezogene Effektivität gewährleistet werden kann.

(4) Chilling Effects

In einer Abwägung zur Verhältnismäßigkeit von Eingriffen in die Informationsfreiheit durch Manipulationen des Datenverkehrs muss auch ein Aspekt Berücksichtigung finden, der in den einschlägigen Urteilen zur Datenverkehrsregulierung bislang wenig beachtet wurde. In der Literatur hingegen wird dieser Aspekt aber durchaus – auch im Kontext

---

I ZR 3/14, 3dl.am, Rn. 18; BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82. Die verschiedenen Funktionen des Deliktsrechts sind jedoch der Ausgleich des Schadens und die Schadensprävention, nicht jedoch die Bestrafung des deliktisch Handelnden bzw. die Genugtuung des Geschädigten, vgl. BGH, Urt. v. 04.06.1992, IX ZR 149/91, BGHZ 118, 312 (339 f.); *Förster* in: BeckOK BGB, § 823 Rn. 6 ff.; *Hager* in: Staudinger, Buch 2: §§ 823 A-D, Vor § 823 BGB Rn. 11; *Wagner* in: MüKoBGB – Bd. 7: Schuldrecht BT II, Vor § 823 BGB Rn. 43 ff.; einschränkend *Spickhoff* in: Soergel, BGB Bd. 12, Vor § 823 BGB Rn. 37. Der negatorische Schutz (hier in Form der Störerhaftung) ergänzt den repressiven Schutz des klassischen Deliktsrechts mit klarem präventivem Schwerpunkt und ist damit bezüglich der Anforderungen an seine Effektivität noch deutlicher auf die Bewahrung des Schutzgegenstands gerichtet, vgl. *Wagner* in: MüKoBGB – Bd. 7: Schuldrecht BT II, Vor § 823 Rn. 39, 46. Eine Fixiertheit auf die Effektivität der Maßnahme hingegen, die den Erfolg der Umsetzung des Mittels und nicht die Effektivität des Schutzes des Schutzgegenstands in den Mittelpunkt stellt, ist daher systemwidrig.

von Netzsperren – diskutiert: die sogenannten „Chilling Effects“,[775] die sich grob als Einschüchterungseffekte bezeichnen lassen.[776]

Chilling Effects entstehen, wenn staatliche Maßnahmen nicht nur unmittelbar das Verhalten einzelner Personen, sondern auch mittelbar das Verhalten einer Vielzahl von Bürgern dahingehend beeinflussen, dass diese grundrechtlich garantierte Freiheiten nicht mehr ausleben.[777] Durch Chilling Effects wird also vornehmlich der objektiv-rechtliche Gehalt eines Grundrechts betroffen, da dessen Geltungsbereich insgesamt angegriffen wird.[778] Chilling Effects sind ein vom Bundesverfassungsgericht anerkanntes Problem im Rahmen der Grundrechtsgewährleistung.[779] In seiner Entscheidung „Antiterrordatei“ etwa erklärte das Bundesverfassungsgericht eine Norm aufgrund einer Verletzung der Meinungs- und Religionsfreiheit durch Chilling Effects für verfassungswidrig.[780]

Das Thema Chilling Effects wurde oben bereits kurz in anderem Zusammenhang angesprochen: ISPs werden durch Chilling Effects dazu inzentiviert, großzügig und bereits ohne konkrete dahingehende Anordnung den Zugang zu bestimmten Angeboten zu sperren, selbst wenn sie dies rechtlich nicht müssten, weil ihnen die Haftungsgefahr bei Untätigbleiben zu groß ist.[781]

Aber nicht bloß die ISPs, auch die Internet-Nutzer unterliegen durch Eingriffe in den Datenverkehr Einschüchterungseffekten. Alle Maßnahmen der Datenverkehrsregulierung sind – wenn auch je nach Technik unterschiedlich stark – dazu in der Lage, bei den Internet-Nutzern Einschüchterungseffekte hervorzurufen.[782] Dies gilt im besonderen Maße für

---

[775] *U.S. Supreme Court*, Urt. v. 15.12.1952, 344 U.S. 183, Wieman v. Updegraff, abrufbar unter https://supreme.justia.com/cases/federal/us/344/183/case.html; Die in dieser und folgenden Entscheidungen entwickelte ratio wurde von der *Columbia Law Review Association*, Columbia Law Review 1969, 808 (ohne weitere Autorennennung) zur Chilling Effects Doctrine fortentwickelt, dort mit weiteren Nachweisen. Zur dogmatischen Einordnung im deutschen Recht vgl. *Oermann/Staben*, Der Staat 2013, 630 (640).

[776] Kritisch zur Rechtsfigur *Ladeur*, AfP 2010, 224; *Roßnagel*, NJW 2010, 1238 (1240).

[777] *Assion*, Überwachung und Chilling Effects, in: Telemedicus Soko 2014, S. 31, (33); *Youn*, Vanderbilt Law Review 2013, 1474 (1481).

[778] *Assion*, Überwachung und Chilling Effects, in: Telemedicus Soko 2014, S. 31 (46).

[779] BVerfG, Beschl. v. 07.12.1976, 1 BvR 460/72, Flugblatt, BVerfGE 43, 130 (136); BVerfG, Urt. v. 03.03.2004, 1 BvR 2378/98, 1 BvR 1084/99, Großer Lauschangriff, BVerfGE 109, 279 (354 f.); BVerfG, Urt. v. 02.03.2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Vorratsdatenspeicherung, BVerfGE 125, 260 (332); vgl. *Assion*, Chilling Effects: Übersicht über die Rechtsprechung, in: Telemedicus, 07.05.2014, abrufbar unter https://tlmd.in/a/2765 mit umfangreichen weiteren Nachweisen.

[780] BVerfG, Urt. v. 24.04.2013, 1 BvR 1215/07, Antiterrordatei, BVerfGE 133, 277, Rn. 161.

[781] Vgl. oben Kap. 2 V 2 b) (S. 93) m.w.N.

[782] Nicht entscheidend ist hier, dass die Maßnahmen der DVR nicht direkt vom Staat durchgeführt werden. Durch deren gesetzliche, behördliche oder gerichtliche Anordnung ist der mittelbare Einschüchterungseffekt dennoch dem Staat zuzurechnen, *Youn*, Vanderbilt Law Review 2013, 1474 (1495 ff.).

DPI-Maßnahmen, da hier grundsätzlich und anlasslos der gesamte Internet-Datenverkehr der Nutzer durchleuchtet wird, und zwar bis in die tiefsten Schichten mit den potentiell sensiblen Anwendungsdaten hinein.

Die Nutzer des Internets werden im Bewusstsein, dass ihr gesamter Datenverkehr von einer dritten Stelle auf gesetzwidriges Verhalten hin durchsucht wird, versuchen, Internet-Angebote mit vermeintlich kritischen Inhalten und unpopulären Meinungen zu meiden. Selbst wenn man Deep Packet Inspection mit anderen Verfahren kombinieren würde, z.B. mit der Auswertung der IP-Adressen, und auf diese Weise eine vorherige Selektion desjenigen Datenverkehrs durchführt, den man bis hinunter in die Anwendungsschicht untersucht, bleiben erhebliche Chilling Effects bestehen. Zwar wird dann nicht mehr der gesamte Datenverkehr tief durchleuchtet. Das Bewusstsein um die Überwachungsinfrastruktur, die den Datenverkehr auf normgemäßes Verhalten überprüft oder überprüfen kann, bleibt jedoch bestehen.

Auch IP- und DNS-Sperren sind grundsätzlich dazu geeignet, beim Internet-Nutzer ein solches Gefühl der ständigen staatlichen Überwachung auszulösen, wenngleich dieses wegen der weniger intensiven Kontrolle der Kommunikationsinhalte tatsächlich in geringerem Maße gerechtfertigt ist als bei DPI-Filtern.[783] Allerdings wird jedenfalls bei IP-Sperren ähnlich wie bei DPI-Filtern ebenfalls der gesamte Datenverkehr gescannt und mit Routing-Tabellen gesperrter IP-Adressen abgeglichen, auch wenn die Datenpakete nur bis in die Internet-Schicht hinein auf inkriminierende Daten durchsucht werden. IP-Adressen, auch dynamische, sind im Kontext von Netzsperren als personenbezogene Daten zu qualifizieren.[784] Und werden IP-Adressen nicht lediglich für Zwecke des Routings im Sinne des Internet-Nutzers verarbeitet, sondern bei der Verarbeitung in Zusammenhang mit unerlaubten Handlungen gebracht, kommt diesem Vorgang auch eine erhöhte Sensibilität zu, der einen qualifiziert einschüchternden Effekt zur Folge haben kann.[785]

Chilling Effects führen nicht automatisch zu einer Verfassungswidrigkeit. Dafür ist ihre Wirkungsweise zu gestreut. Sie sind jedoch eine verfassungsrechtliche Rechtsfigur, die in dem im jeweiligen Einzelfall gebotenen Umfang bei der Betrachtung der Zweck-Mittel-Relation berücksichtigt werden muss.[786]

Insbesondere die Deep Packet Inspection mit ihrem umfassenden Filteransatz, die zudem auch die Inhalte der Kommunikation nicht ausspart, ist allerdings geeignet, die Art „diffuse Bedrohlichkeit“[787] in der Bevölkerung zu erzeugen, die das alltägliche Kommunikati-

---

[783] Vgl. zu den technischen Grundlagen der DVR oben Kap. 1 III (S. 16 ff.).
[784] EuGH, Urt. v. 19.10.2016, Rs. C-582/14, Breyer, EU:C:2016:779, Rn. 49.
[785] So auch *Heliosch*, Sperrmaßnahmen im Internet, S. 192 f.; *Nazari-Khanachayi*, GRUR 2015, 115 (122).
[786] Vgl. *Assion*, Überwachung und Chilling Effects, in: Telemedicus Soko 2014, S. 31 (80).
[787] BVerfG, Urt. v. 02.03.2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Vorratsdatenspeicherung, BVerfGE 125, 260 (335).

onsverhalten in inakzeptabler Weise beeinflusst. Die Chilling Effects der Deep Packet Inspection streifen daher bereits den Kernbereich der Informationsfreiheit, da die Ausübung des Grundrechts insgesamt erheblich negativ beeinflusst wird.

5. Ergebnis

Fügt man die soeben isoliert voneinander betrachteten Einzelaspekte einander gegenüber und überführt sie in eine Gesamtabwägung, verbleibt wenig Raum für eine verhältnismäßige Einschränkung der Informationsfreiheit.

Eine DVR kann nur insoweit zulässig sein, wie ausgeschlossen werden kann, dass die Internet-Angebote von Drittanbietern unbeabsichtigt mitgesperrt werden. Ein anderes Ergebnis ist weder mit Art. 5 Abs. 1 Satz 1 Alt 1 GG noch mit der Auslegung von Art. 11 Abs. 1 Charta durch den EuGH zu vereinbaren. Dies schließt die Zulässigkeit von IP-Sperren bereits weitgehend aus, da das Mitsperren von Drittanbieterangeboten technisch bedingt nicht verhindert werden kann. Insbesondere können die Internet-Nutzer diesbezüglich kaum auf einen gerichtlichen Rechtsbehelf ex post verwiesen werden. Zwar schlagen EuGH und BGH genau dies vor, ein solcher Rechtsbehelf läuft in der Realität jedoch faktisch leer.[788]Zudem leiden IP-Sperren darunter, dass sie erhebliche Chilling Effects für die Nutzung des Internets durch die Bevölkerung insgesamt verursachen. Setzt man diese Punkte der mäßigen maßnahmebezogenen Effektivität und noch erheblich geringeren schutzniveaubezogenen Effektivität gegenüber, so wird deutlich, dass die Zweck-Mittel-Relation von IP-Sperren nicht stimmt und sie damit die Informationsfreiheit verletzen.

DNS-Sperren schonen die Informationsfreiheit stärker als IP-Sperren. Zwar verursachen auch sie Overblocking, dieses beschränkt sich jedoch auf die legalen Inhalte der ins Visier der Netzsperren genommenen Internet-Angebote. Die Frage, ob die das Urheberrecht verletzenden Inhalte im Einzelfall derart überwiegen, dass das Overblocking nicht dazu führt, dass die Informationsfreiheit verletzt wird, ist damit allerdings noch nicht beantwortet. Ein ISP ist aufgrund seiner Kompetenzen und seiner organisatorischen Stellung nicht dazu in der Lage, auf diese Frage eine Antwort zu geben. Auch ein gerichtlicher Rechtsbehelf der Internet-Nutzer gegen den Internet Service Provider ist dazu aus praktischen Gründen – wie bereits mehrfach erwähnt – nicht geeignet. Zwar besitzt ein Gericht die Kompetenz und die Legitimation, in dieser Frage zu entscheiden, doch würde effektiver Rechtsschutz in aller Regel für den Nutzer zu spät kommen. Ein auf Verwaltungsebene angesiedeltes Rechtsschutzverfahren hingegen könnte je nach Ausgestaltung durch Schnelligkeit in der Abhilfeentscheidung dieses Problem möglicherweise etwas entspannen, wenn auch nicht völlig beseitigen.

---

[788] Zur Verteidigung des EuGH muss hier angemerkt werden, dass dieser auch lediglich abstrakt ausführt, unter welchen Voraussetzungen eine DVR europarechtskonform sein könnte; Nicht hingegen stellt er fest, dass die Erfüllung dieser Voraussetzungen zwingend tatsächlich umsetzbar wäre.

In einer Gesamtabwägung müssen aber immer noch zwei weitere Probleme der DNS-Sperren berücksichtigt werden. Zum einen verursachen auch sie Chilling Effects bei der das Internet nutzenden Bevölkerung. Zum anderen müssen alle Nachteile für die Informationsfreiheit wie Overblocking und Chilling Effects von der Effektivität bei der Erreichung des Regulierungsziels aufgewogen werden. Dies ist jedoch bei DNS-Sperren, die mit der geringsten Effektivität aller in Frage kommenden Maßnahmen aufwarten, im Ergebnis nicht der Fall. Auch DNS-Sperren verletzen daher im Ergebnis als unangemessener Eingriff die Informationsfreiheit.

Fraglich ist mithin das Ergebnis einer Gesamtabwägung bei der Anwendung von Deep Packet Inspection. DPI-Filter sind erstaunlich effektiv bei der Durchsetzung des Urheberrechts. Dies gilt nicht nur für die maßnahmebezogene Effektivität, sondern sogar für die schutzniveaubezogene Effektivität. Außerdem lassen sich DPI-Maßnahmen relativ zielgenau einsetzen. Dies kann Overblocking in der Form von false positives jedoch nicht vollständig verhindern, sondern lediglich minimieren.[789] Die denkbaren Rechtsschutzmöglichkeiten der Internet-Nutzer gegen Overblocking sind wie bei den anderen Verfahren zudem denkbar gering, zumal schon fraglich ist, wie Nutzer bei einzelnen blockierten Inhalten überhaupt erfahren sollen, dass sie versuchen, auf einen gesperrten Inhalt zuzugreifen. Schließlich, und am schwerwiegendsten, sind jedoch die Eingriffe in die Informationsfreiheit der Internet-Nutzer durch die Chilling Effects, wie sie von einer breitflächigen Deep Packet Inspection der ISPs verursacht werden, die eine effektive Durchsetzung des Urheberrechts erfordert. Die Veränderungen des Kommunikationsverhaltens, die sich ein Großteil der Internet-Nutzer auferlegen werden, wenn eine vollständige Überwachung des Internets bis hinein in die Anwendungsschicht Realität werden sollte, wären mit allergrößter Wahrscheinlichkeit immens. Dies ist kein verhältnismäßiger Preis für eine verbesserte Urheberrechtsdurchsetzung, so dass auch DPI-Filter ein unangemessener Eingriff in die Informationsfreiheit sind.

Es bleibt also lediglich festzustellen, dass zumindest gegenwärtig keine der untersuchten Techniken in der Lage ist, das Urheberrecht durchzusetzen, ohne die Informationsfreiheit unverhältnismäßig einzuschränken.

IV. Das Grundrecht der Internet-Nutzer auf das Telekommunikationsgeheimnis, Art. 10 Abs. 1 GG

Ein weiteres Grundrecht der Internet-Nutzer, das durch Eingriffe in den Datenverkehr zur Urheberrechtsregulierung verletzt sein könnte, ist das Fernmelde- bzw. Telekommunikationsgeheimnis gemäß Art. 10 Abs. 1 GG.

---

[789] Cruz Villalón, Schlussanträge des Generalanwalts v. 14.04.2011, Rs. C-70/10, Slg. 2011, I-11962, Rn. 86: „*[E]in bestimmter Kommunikationsvorgang [kann] in einem Land zulässig und in einem anderen unzulässig sein [...], je nach Reichweite des in Rede stehenden Urheberrechts, so dass sich die Frage der Zulässigkeit der Technik entzieht. Soweit ersichtlich, ist offenbar kein Filter- und Sperrsystem imstande, auf eine den Anforderungen von Art. 11 und Art. 52 Abs. 1 der Charta entsprechende Weise zu gewährleisten, dass nur diejenigen Datenaustauschvorgänge gesperrt werden, bei denen konkret festgestellt werden kann, dass sie unzulässig sind*“.

Art. 10 Abs. 1 GG erklärt das Briefgeheimnis sowie das Post- und Telekommunikationsgeheimnis für unverletzlich. Brief- und Postgeheimnis betreffen die Vertraulichkeit verschlossener körperlicher Fernkommunikation.[790] Da der hier besprochene Anwendungsfall des Filesharings im Internet stattfindet und sich damit ausschließlich auf elektronische, also nicht körperliche Kommunikation bezieht, kann das Brief- und das Postgeheimnis hier vernachlässigt und der Blick auf das Telekommunikationsgeheimnis gerichtet werden.

1. Schutzbereich des Telekommunikationsgeheimnisses

Das Telekommunikationsgeheimnis dient einem Teilbereich des Schutzes der Persönlichkeit und der Privatsphäre, nämlich dem Schutz der Integrität der auf elektronischem Wege Entfernungen überbrückenden Kommunikation unter Abwesenden. Dabei schützt Art. 10 Abs. 1 GG insbesondere vor staatlicher Kenntnisnahme, Aufzeichnung und Verarbeitung der Kommunikation.[791] Dieser besondere grundrechtliche Schutz ist notwendig wegen der besonderen Gefahren für die Vertraulichkeit der Kommunikation, die daraus entstehen, dass die Telekommunikation über Intermediäre erfolgt und die Kommunikationsteilnehmer die Gewährleistung der Vertraulichkeit während des Übertragungsvorgangs nur noch eingeschränkt selbst in der Hand haben.[792]

a. Persönlicher Schutzbereich

Der persönliche Schutzbereich des Art. 10 Abs. 1GG ist bei datenverkehrsregulierenden Maßnahmen unproblematisch eröffnet, da diese sich bei den Nutzern des Internets auswirken und zumindest jede natürliche Person vom persönlichen Schutzbereich der Telekommunikationsfreiheit erfasst ist.[793]

b. Sachlicher Schutzbereich

Der sachliche Schutzbereich des Telekommunikationsgeheimnisses ist in dem Sinne weit auszulegen, als er technologieneutral zu bestimmen ist und damit jedenfalls grundsätzlich auch die Kommunikation über das Internet umfasst.[794] Der Schutzbereich umfasst ferner *alle* Kommunikationsinhalte, unabhängig von ihrer gesellschaftlichen oder politischen

---

[790] *Windthorst* in: Gröpl u.a., Grundgesetz, Art. 10 Rn. 17; *Durner* in: Maunz/Dürig, Art. 10 GG Rn. 92, 97 (Stand: 91. Erg.-Lfg., April 2020).

[791] *Böckenförde*, Die Ermittlung im Netz: Möglichkeiten und Grenzen neuer Erscheinungsformen strafprozessualer Ermittlungstätigkeit, S. 172; *Horn* in: Isensee/P. Kirchhof, HStR VII, § 149 Rn. 98 ff.; *Hohmann-Dennhardt*, NJW 2006, 545 (547); *Durner* in: Maunz/Dürig, Art. 10 GG Rn. 106 (Stand: 91. Erg.-Lfg., April 2020).

[792] BVerfG, Beschl. v. 25.03.1992, 1 BvR 1430/88, Fangschaltung, BVerfGE 85, 386 (395 f.); BVerfG, Urt. v. 14.07.1999, 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, Telekommunikationsüberwachung I, BVerfGE 100, 313 (363).

[793] *Windthorst* in: Gröpl u.a., Grundgesetz Art. 10 Rn. 7.

[794] BVerfG, Beschl. v. 09.10.2002, 1 BvR 1611/96, 1 BvR 805/98, Mithörvorrichtung, BVerfGE 106, 28 (35 f.); BVerfG, Urt. v. 27.02.2008, 1 BvR 370/07, 1 BvR 595/07, Online-Durchsuchung, BVerfGE 120, 274 (307).

Bedeutung oder ihrem persönlichkeitsrechtlichen Bezug im Einzelfall.[795] Der Schutz des Art. 10 Abs. 1 GG beschränkt sich allerdings nicht auf die Kommunikationsinhalte, sondern umfasst auch die näheren Umstände der Kommunikation, insbesondere welche Personen wann miteinander kommuniziert haben oder dies jedenfalls versuchten. Die systematische Auswertung der Metadaten der Kommunikation erlaubt es nämlich unter anderem, detaillierte Profile über Verhaltensmuster des Kommunizierenden zu erstellen. Ohne einen (Mit)-Schutz der Umstände der Kommunikation entstünde ansonsten eine Schutzlücke.[796]

Die bei der Telekommunikation anfallenden Informationen werden durch Art. 10 Abs. 1 GG allerdings nur insoweit geschützt, wie die Gefahren für die Vertraulichkeit der Kommunikation gerade im Vorgang der Fernübermittlung liegen. Nur wenn Inhalte und Umstände laufender Telekommunikation im Internet erhoben oder ausgewertet werden, betrifft dies Art. 10 Abs. 1 GG. Dies gilt zwar unabhängig davon, ob der technische Eingriff erst an einem der Endgeräte der Kommunikation erfolgt oder ob dies bereits auf dem Übermittlungsweg geschieht.[797] Die Überwachung von Informationen, die bei der Kommunikation angefallen und nach Beendigung der Verbindung noch auf dem Endgerät gespeichert sind, unterfällt hingegen dem Schutz von Art. 13 Abs. 1 GG oder dem allgemeinen Persönlichkeitsrecht, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, in seiner Ausformung des Grundrechts auf Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme.[798]

Gegenüber der Rundfunkfreiheit, Art. 5 Abs. 1 Satz 2 Var. 2 GG, ist das entscheidende Abgrenzungskriterium, dass Art. 10 Abs. 1 GG die Kommunikation zwischen Individuen schützt und die Rundfunkfreiheit die Massenkommunikation.[799] Dies führt zu gewissen Schwierigkeiten bei der Beantwortung der Frage, ob DVR-Maßnahmen, die sich gegen *Filesharing* richten, überhaupt in den Schutzbereich des Art. 10 Abs. 1 GG fallen können, da es an dem Erfordernis der Individualkommunikation fehlen könnte. Diese Frage wird sehr kontrovers diskutiert. Teilweise wird der Kommunikation über das Internet, jedenfalls im *World Wide Web*, daher der Schutz durch Art. 10 Abs. 1 GG abgesprochen. Vertreter dieser Ansicht differenzieren in der Regel danach, welche Internet-Dienste von einer Maßnahme konkret betroffen sind, und ob es sich bei den betroffenen Diensten um

---

[795] BVerfG, Urt. v. 14.07.1999, 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, Telekommunikationsüberwachung I, BVerfGE 100, 313 (358); BVerfG, Beschl. v. 09.10.2002, 1 BvR 1611/96, 1 BvR 805/98, Mithörvorrichtung, BVerfGE 106, 28 (35 f.).
[796] Vgl. BVerfG, Beschl. v. 20.06.1984, 1 BvR 1494/78, G10, BVerfGE 67, 157, Rn. 46; BVerfG, Urt. v. 12.03.2003, 1 BvR 330/96, 1 BvR 348/99, Handy-Überwachung, BVerfGE 107, 299 (324); BVerfG, Urt. v. 27.02.2008, 1 BvR 370/07, 1 BvR 595/07, Online-Durchsuchung, BVerfGE 120, 274 (307); BVerfG, Urt. v. 20.04.2016, 1 BvR 966/09, 1 BvR 1140/09, BKA-Gesetz, BVerfGE 141, 220, Rn. 248.
[797] BVerfG, Urt. v. 27.02.2008, 1 BvR 370/07, 1 BvR 595/07, Online-Durchsuchung, BVerfGE 120, 274 (307).
[798] BVerfG, Urt. v. 27.02.2008, 1 BvR 370/07, 1 BvR 595/07, Online-Durchsuchung, BVerfGE 120, 274 (307 f.).
[799] *Windthorst* in: Gröpl u.a., Grundgesetz, Art. 10 GG Rn. 14, 27 f.

Individualkommunikation handelt. Teilweise wird der Schutz des Telekommunikationsgeheimnisses allerdings auch generell bejaht.

Relativ unstrittig dürfte mittlerweile – wie bereits kurz angesprochen – sein, dass gewisse Anwendungen, die auf dem Internet aufsetzen, von Art. 10 Abs. 1 GG geschützt werden, da es sich zweifellos um Individualkommunikation handelt. Zu diesen Diensten zählen jedenfalls E-Mail, Internet-Chats und geschlossene Diskussionsforen.[800]

Eine restriktive Ansicht lässt es hingegen bei diesen Anwendungen bewenden. Andere Dienste des Internets seien vom Telekommunikationsgeheimnis nicht umfasst. Vielmehr müsse Art. 10 Abs. 1 GG funktional ausgelegt werden.[801] An die Öffentlichkeit gerichtete Internetdienste ließen die Individualität vermissen, die typisch für die klassischerweise von Art. 10 Abs. 1 GG geschützte Kommunikation zwischen zwei Teilnehmern sei. Bei einer solchen Kommunikation fehle die Intimität, die erst zum Schutz durch Art. 10 Abs. 1 GG Anlass gebe.[802] Andere Stimmen in der Literatur grenzen ähnlich und danach ab, ob ein Kommunikationsprozess, auch wenn er an eine Vielzahl von Empfängern gerichtet ist, sich jedenfalls nicht an die Allgemeinheit richtet. Danach seien dann auch zugangsbeschränkte Websites und Downloads durch Art. 10 Abs. 1 GG geschützt.[803]

Folgt man diesem funktionalen Ansatz, führt die Frage, ob illegales *Filesharing* in den Schutzbereich der Telekommunikationsfreiheit fällt, zu einer tieferen Auseinandersetzung im Einzelfall mit dem spezifischen technischen Übertragungsweg, der zur Übermittlung der geschützten Informationen verwendet wird. Werden die geschützten Werke über ein zentralisiertes Online-Angebot geteilt, etwa über einen Filehoster, dürfte Art. 10 Abs. 1 GG durch DVR-Maßnahmen nicht betroffen sein.[804] Werden hingegen Peer-to-Peer-Netzwerke für das *Filesharing* verwendet, wäre es hingegen durchaus vertretbar, auch nach der restriktiven Auslegung des Schutzbereichs eine Individualkommunikation anzunehmen und den Schutzbereich des Telekommunikationsgeheimnisses als eröffnet anzusehen.[805]

---

[800] So ausdrücklich BVerfG, Urt. v. 27.02.2008, 1 BvR 370/07, 1 BvR 595/07, Online-Durchsuchung, BVerfGE 120, 274 (341); *Durner*, ZUM 2010, 833 (839).
[801] *Albers*, Informationelle Selbstbestimmung, S. 371; *Böckenförde*, JZ 2008, 925 (937); *Czychowski*, MMR 2004, 514 (518); *Durner*, ZUM 2010, 833; *ders.* in: Maunz/Dürig, Art. 10 GG Rn. 118 ff. (Stand: 57. Erg.-Lfg., April 2020); *Kropp*, Die Haftung von Host- und Access-Providern bei Urheberrechtsverletzungen, S. 162; *Pagenkopf* in: Sachs, Grundgesetz, Art. 10 Rn. 14a; *Spindler*, GRUR 2016, 451 (456); dem folgend BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 68.
[802] *Durner*, ZUM 2010, 833 (838 ff.).
[803] *Windthorst* in: Gröpl u.a., Grundgesetz, Art. 10 Rn. 28; *Horn* in: HStR VII, § 149 Rn. 100; *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 10 Rn. 6; *Gusy* in: v. Mangoldt/Klein/Starck, Grundgesetz Bd. 1, Art. 10 Rn. 42; *Martini* in: v. Münch/Kunig, Grundgesetz Bd. 1, 7. Aufl. 2021, Art. 10 Rn. 32 f.
[804] So BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 68 zum Goldesel-Angebot.
[805] Dies würde dann in erster Linie im Rahmen der Überprüfung von DVR-Maßnahmen unter Verwendung von Deep Packet Inspection relevant werden.

Eine andere Strömung hält formell an der Abgrenzung anhand von Individual- und Massenkommunikation fest und greift auf einen technischen Ansatz zurück.[806] Selbst sogenanntes IP-TV, bei dem an ein Massenpublikum gerichtete Fernsehsendungen den Weg zum Zuschauer statt über herkömmliche Rundfunkkanäle über das Internet finden, benötigt für die Datenübertragung technisch gesehen eine individuelle Verbindung zwischen zwei Endgeräten, dem Server und dem Host. Folgt man diesem Argument, sind grundsätzlich alle über das Internet stattfindenden Kommunikationsvorgänge von Art. 10 Abs. 1 GG erfasst. Im Ergebnis vergleichbar wird von anderen jegliche Internet-Kommunikation dem Schutzbereich des Telekommunikationsgeheimnisses zugeordnet, dies jedoch mit wechselnden Argumenten hergeleitet. So wird vertreten, dass jegliche Kommunikation über das Internet Spuren in Form von Metadaten hinterlasse, die die Privatheit des Kommunikations- und Informationsverhaltens kompromittieren könnten und die bei analoger Nutzung von Massenmedien nicht in demselben Maße zu befürchten sei.[807] Eine Abgrenzung anhand von Massen- und Individualkommunikation scheitere im Internet hingegen letztlich an unüberwindbaren praktischen Hürden, so dass eine solche Abgrenzung im Online-Kontext nicht zur Anwendung geeignet sei.[808] *Filesharing* in all seinen Erscheinungsformen wäre nach diesem weiten Verständnis des Telekommunikationsgeheimnisses vom Schutzbereich des Art. 10 Abs. 1 GG erfasst.

Das Bundesverfassungsgericht tendiert in jüngeren Entscheidungen wohl zu einer Erstreckung des Telekommunikationsgeheimnisses auf alle Internet-Kommunikationsvorgänge.[809] Dem ist zuzustimmen. Zwar kann das rein technische Argument, im Internet sei letztlich wegen der Funktionsweise des TCP/IP-Protokolls jede Kommunikation auch Individualkommunikation, allein nicht überzeugen. Beleuchtet man dieses Argument jedoch etwas näher, wird deutlich, dass durch die Tatsache, dass im Internet technisch stets Individualkommunikation vorliegt, auch gerade die Gefahren für die Privatheit entstehen, die üblicherweise mit der elektronischen Fernkommunikation zusammenhängen.

Es macht einen Unterschied, ob ein Bürger anonym eine bestimmte Fernsehsendung über ein klassisches Rundfunkmedium konsumiert oder ob er auf die gleichen Inhalte über das Internet für Dritte nachvollziehbar zugreift. Die Bedrohung der Privatsphäre durch eine Kenntnisnahme des Obs, des Wanns, des Wos und des Mit-wems ist im Gegensatz zur vergleichbaren Situation des Rundfunkempfangs klar vorhanden. Die theoretische Nachvollziehbarkeit aller Kommunikationsvorgänge über das Internet schafft eine spezifische

---

[806] *Determann*, Kommunikationsfreiheit im Internet, S. 462; *Germann*, Strafverfolgung im Internet, S. 117; *Sievers*, Schutz der Kommunikation, S. 129 f.
[807] *Badura* in: W. Kahl u.a., Bonner Kommentar zum Grundgesetz, Art. 10 Rn. 51 (Stand: 166. Erg.-Lfg., März 2014).
[808] *Hermes* in: H. Dreier, Grundgesetz, Bd. 1, Art. 10 Rn. 40; *Frey u.a.*, MMR-Beil. 2012, 1 (6); *Heliosch*, Sperrmaßnahmen im Internet, S. 201; grundlegend kritisch *Degenhart*, CR 2011, 231 (232); *Klescewski* in: Säcker, Berliner Kommentar zum TKG, § 88 Rn. 12.
[809] BVerfG, Urt. v. 27.07.2005, 1 BvR 668/04, Telekommunikationsüberwachung II, BVerfGE 113, 348 (364 f.); BVerfG, Urt. v. 27.02.2008, 1 BvR 370/07, 1 BvR 595/07, Online-Durchsuchung, BVerfGE 120, 274 (304 ff.); BVerfG, Nichtannahmebeschluss v. 06.07.2016, 2 BvR 1454/13, NJW 2016, 3508 (3510).

Gefahr für die Freiheit des Bürgers durch Kenntnisnahme und Verarbeitung der Kommunikationsinhalte und -umstände, die den Gefahren gleicht, vor denen Art. 10 Abs. 1 GG schützen soll. Nicht zuletzt ist eine Einbeziehung der Internetkommunikation in den Schutzbereich des Telekommunikationsgeheimnisses auch vor dem Hintergrund der Kohärenz mit dem Grundrechtschutz auf europäischer Ebene zu begrüßen, wo Internet-Kommunikation generell durch Art. 7 Charta bzw. Art. 8 Abs. 1 EMRK geschützt wird.[810] Datenverkehrsregulierende Maßnahmen berühren also den Schutzbereich der Telekommunikationsfreiheit.

2. Eingriff

Mit der Betroffenheit des Schutzbereichs des Telekommunikationsgeheimnisses ist noch keine Aussage darüber getroffen, ob DVR-Maßnahmen auch in den Schutzbereich des Art. 10 Abs. 1 GG eingreifen.

a. Mittelbarer Eingriff durch ISPs

Problematisch ist bei DVR-Maßnahmen, die letztlich mangels direkter staatlicher Beherrschung der Telekommunikationsnetze durch die ISPs und nicht unmittelbar durch den Staat durchgeführt werden müssen, ob diese Maßnahmen überhaupt in den Anwendungsbereich des Art. 10 Abs. 1 GG fallen. Das Telekommunikationsgeheimnis ist ein klassisches Abwehrrecht gegen den Staat.[811] Die Internet Service Provider sind in aller Regel als Folge der Privatisierungsbemühungen seit den 90er Jahren privatrechtliche Unternehmen und damit nicht mehr Grundrechtsverpflichtete. Im Falle der Anordnung datenverkehrsregulierender Maßnahmen muss sich der Staat diese allerdings als eigene zurechnen lassen. Wenn der Staat die ISP in die Pflicht nimmt, um den Datenverkehr seiner Bürger zu manipulieren, muss er sich diese Maßnahmen wie eigene zurechnen lassen. Das Bundesverfassungsgericht hat diesbezüglich festgestellt, dass die Tatsache, dass es sich bei ISPs um Personen des Privatrechts handelt, nichts am Vorliegen eines Eingriffs in Art. 10 Abs. 1 GG ändert, wenn ISPs unmittelbar vom Staat zur Erfüllung einer hoheitlich gewollten Aufgabe als Hilfspersonen herangezogen werden.[812] Diese Wertung entspricht dem bereits oben im Rahmen der Prüfung von Art. 12 Abs. 1 GG gefundenen Ergebnis, dass der Staat sich nicht dadurch seiner Grundrechtsbindung entziehen können soll, dass er Eingriffe in Grundrechte durch Personen des Privatrechts durchführen lässt.[813]

---

[810] EGMR, Urt. v. 03.07.2007, Nr. 62617/00, Copland ./. Vereinigtes Königreich, Rep. 2007-I, S. 317, Rn. 41.

[811] *Hermes* in: H. Dreier, Grundgesetz, Bd. 1, Art. 10 GG Rn. 51; *Pagenkopf* in: Sachs, Grundgesetz, Art. 10 GG Rn. 18; *Schenke* in: Stern/Becker, Grundrechte-Kommentar, Art. 10 GG Rn. 56.

[812] BVerfG, Urt. v. 02.03.2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Vorratsdatenspeicherung, BVerfGE 125, 260 (311); BVerfG, Urt. v. 12.03.2003, 1 BvR 330/96, 1 BvR 348/99, Handy-Überwachung, BVerfGE 107, 299 (313 f.).

[813] Vgl. oben Kap. 3 II 1 b) (5) (S. 142). Grundsätzlich zur „funktionalen Privatisierung" *Di Fabio*, JZ 1999, 585 (588); *Gersdorf*, JZ 2008, 831 (832); speziell zur Zurechnung der Handlung des ISP zum Staat *Germann*, Strafverfolgung im Internet, S. 445; *Heliosch*, Sperrmaßnahmen im Internet, S. 218; *Koreng*, Zensur im Internet, S. 143; *Schoch*, NVwZ 2008, 241 (246); *Sieber/Nolde*, Sperrverfügungen, S. 60.

Ein Eingriff in das Telekommunikationsgeheimnis liegt immer dann vor, wenn sich staatliche Stellen die Möglichkeit verschaffen, vom Inhalt oder von den näheren Umständen der geschützten Telekommunikation Kenntnis zu nehmen, ohne das die Betroffenen dazu ihre Einwilligung gegeben hätten. Erst recht ist der Fall erfasst, dass der Staat von den Informationen, die er auf diesem Weg erhalten hat, Gebrauch macht.[814]

b. Eingriff durch IP-Sperren

Da DVR-Maßnahmen auf unterschiedliche technische Weise wirken, muss für die Beantwortung der Frage, ob sie auch einen Eingriff in den Schutzbereich des Telekommunikationsgeheimnisses darstellen, zwischen den verschiedenen Maßnahmen differenziert werden.

Für IP-Sperren nutzt ein ISP die Informationen der Internet-Schicht des IP-Pakets. Die Daten der Internet-Schicht werden gegen eine Liste mit gesperrten IP-Adressen abgeglichen. Liegt eine Übereinstimmung zwischen der im Datenstrom identifizierten IP-Adresse und einer zur Sperrung angeordneten IP-Adresse vor, wird der Übermittlungsvorgang abgebrochen. Es werden also weder Informationen des eigentlichen Kommunikationsinhalts, also dem Payload der entsprechenden IP-Pakete, verwendet, noch sonstige Informationen aus deren tieferen Schichten, die direkt oder indirekt über die Inhalte der Kommunikation Auskunft geben könnten.[815] IP-Sperren greifen also nicht auf den Inhalt der Kommunikation zu.

Allerdings berührt der Abgleich der IP-Interessen die ebenfalls von Art. 10 Abs. 1 GG geschützten näheren Umstände der Kommunikation. Das Telekommunikationsgeheimnis ist, wie oben bereits festgestellt, eine besondere Ausformung des Allgemeinen Persönlichkeitsrechts (APR).[816] Wo die Kenntnisnahme und Verarbeitung der Kommunikationsumstände in die Privatsphäre der Bürger eingreift, ist daher das Telekommunikationsgeheimnis einschlägig und verdrängt das Recht auf informationelle Selbstbestimmung. Nach Einschätzung des Bundesverfassungsgerichts ist dies insbesondere bei solchen Daten der Fall, die Auskunft darüber geben, ob, wann und wie oft eine Person mit einer anderen kommuniziert.[817]

---

[814] *Hermes* in: H. Dreier, Grundgesetz, Bd. 1, Art. 10 GG Rn. 53 m.w.N. zur einschlägigen Rechtsprechung des BVerfG; *Martini* in: v. Münch/Kunig, Grundgesetz Bd. 1, 7. Aufl. 2021, Art. 10 GG Rn. 108; vgl. *Proelss/Daum*, AöR 2016, 373 (392), die die nicht ganz widerspruchsfreie Rechtsprechung des BVerfG in Bezug daraufhin untersuchen, ob die bloße Datenerhebung bereits einen Eingriff darstellt.

[815] Siehe zur technischen Funktionsweise der IP-Sperre oben Kap. 1 III 2 (S. 18 f).

[816] *Martini* in: v. Münch/Kunig, Grundgesetz Bd. 1, 7. Aufl. 2021, Art. 10 GG Rn. 4; *Rohlf*, Privatsphäre, S. 163 ff.

[817] Vgl. BVerfG, Beschl. v. 20.06.1984, 1 BvR 1494/78, G10, BVerfGE 67, 157, Rn. 46; BVerfG, Urt. v. 12.03.2003, 1 BvR 330/96, 1 BvR 348/99, Handy-Überwachung, BVerfGE 107, 299 (324); BVerfG, Urt. v. 27.02.2008, 1 BvR 370/07, 1 BvR 595/07, Online-Durchsuchung, BVerfGE 120, 274 (307); BVerfG, Urt. v. 20.04.2016, 1 BvR 966/09, 1 BvR 1140/09, BKA-Gesetz, BVerfGE 141, 220, Rn. 248.

Bei der Bestimmung der näheren Umstände der Kommunikation spielt zudem der Schutzumfang der verwandten Ausprägungen des Allgemeinen Persönlichkeitsrechts eine entscheidende Rolle. Da der speziellere Art. 10 Abs. 1 GG diese innerhalb seines Anwendungsbereichs verdrängt, dürfen für Informationen, die anderweitig durch das Allgemeinen Persönlichkeitsrecht geschützt wären, im Bereich des Telekommunikationsgeheimnisses keine Schutzlücken entstehen. Dies betrifft praktisch vor allem solche Daten, die ansonsten durch das Recht auf informationelle Selbstbestimmung geschützt werden.[818] Nicht zu vergessen ist diesbezüglich allerdings, dass der unmittelbare Bezug der Informationen zum konkreten Telekommunikationsvorgang gegeben sein muss, also nur die sogenannten Verkehrsdaten[819] von Art. 10 Abs. 1 GG geschützt sind.[820] Andere personenbezogene Daten, die zwar im engen Zusammenhang mit dem Kommunikationsvorgang stehen, diesen aber nicht unmittelbar betreffen, werden hingegen nicht von Art. 10 Abs. 1 GG, sondern unmittelbar durch Art. 2 Abs. 1, Art. 1 Abs. 1 GG geschützt, da sie eben keine konkreten Gefahren gerade aus der Fernkommunikation betreffen.[821]

Bei den IP-Adressen, die notwendigerweise für IP-Sperren vom ISP verarbeitet werden müssen, handelt es sich um Verkehrsdaten, die im gegebenen Kontext zudem auch einen deutlichen Personenbezug aufweisen müssen. Dies gilt nicht nur für statische, sondern auch für dynamische IP-Adressen. Für den Fall, dass die IP-Adressen von Access Providern verarbeitet werden, hat dies der EuGH bereits im Scarlet-Verfahren entschieden, da die Access Provider die dynamischen IP-Adressen mit ihren Kunden-Datenbanken abgleichen und den hinter der Adresse verborgenen Anschlussinhaber leicht identifizieren können.[822]

Dies gilt allerdings auch dann, wenn die IP-Adressen von einem anderen Internet Service Provider als dem Access Provider des Internet-Nutzers verarbeitet werden. Für eine IP-Adressen verarbeitende Stelle handelt es sich nach dem Breyer-Urteil des EuGH auch dann um ein personenbezogenes Datum, wenn die Stelle *„über rechtliche Mittel verfügt, die es [ihr] erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen“*.[823] Nach deutschem

---

[818] BVerfG, Urt. v. 14.07.1999, 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, Telekommunikationsüberwachung I, BVerfGE 100, 313 (359); BVerfG, Urt. v. 02.03.2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Vorratsdatenspeicherung, BVerfGE 125, 260 (310).

[819] Verkehrsdaten werden in § 3 Nr. 30 TKG einfachgesetzlich legaldefiniert als „Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden“.

[820] Zum umfassenden Schutz der Verkehrsdaten durch das Telekommunikationsgeheimnis *Graulich* in: Fetzer u.a., TKG, § 88 Rn. 25 ff. (speziell zum Schutz der IP-Adressen Rn. 31); *Bock* in: Geppert/Schütz, BeckOK TKG, § 88 Rn. 14; einschränkend hingegen *Mayen*: in Scheurle/Mayen, TKG, § 88 Rn. 40.

[821] BVerfG, Beschl. v. 24.01.2012, 1 BvR 1299/05, Bestandsdatenspeicherung, BVerfGE 130, 151 (179 f.); *Heliosch*, Sperrmaßnahmen im Internet, S. 205, Fn. 815; *Mayen* in: Scheurle/Mayen, TKG, § 88 Rn. 39; *Wuermeling/Felixberger*, CR 1997, 230 (234); noch offenlassend BVerfG, Urt. v. 02.03.2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Vorratsdatenspeicherung, BVerfGE 125, 260, (313).

[822] EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 51.

[823] EuGH, Urt. v. 19.10.2016, Rs. C-582/14, Breyer, EU:C:2016:779, Rn. 49.

Recht haben Anbieter von Telekommunikationsdiensten, zu denen auch sämtliche Internet Service Provider gehören,[824] jedenfalls unter gewissen Umständen die rechtliche Möglichkeit, die IP-Adresse eines Nutzers dieser Telekommunikationsdienste vom Access Provider des Nutzers dem Anschlussinhaber zuordnen zu lassen und so den Personenbezug im Einzelfall herzustellen.[825] Diese Möglichkeit wird im deutschen Recht gegenwärtig über § 113 Telekommunikationsgesetz (TKG) und § 100j Strafprozessordnung (StPO) eröffnet.[826]

Das Bundesverfassungsgericht betont zudem in der Vorratsdatenspeicherungs-Entscheidung die besondere Relevanz der Auswertung von IP-Adressen für die Privatsphäre. Da die IP-Adressen der durch einen Bürger aufgerufenen Websites, anders als Metadaten der fernmündlichen Kommunikation zwischen zwei Individuen, zugleich Rückschlüsse auf die Inhalte der aufgerufenen Angebote erlaubten, seien IP-Adressen nicht lediglich *„nähere Umstände der Telekommunikation"*, sondern stünden der Kategorie *„Telekommunikationsinhalte"* bereits sehr nahe. Zudem sei die üblicherweise hohe Anzahl von einem Nutzer aufgerufener IP-Adressen ein Faktor, der die Erschaffung eines detaillierten Profils über die vom Nutzer aufgerufenen Medien und Informationsquellen erlaube.[827]

Unerheblich für die Personenbezogenheit ist zudem, dass der Nutzer eines unter einer bestimmten IP-Adresse erreichbaren Anschlusses nicht auch zwingend dessen Inhaber sein muss.[828]

Stellen also IP-Sperren nach dem soeben Gesagten in jedem Fall einen Eingriff in Art. 10 Abs. 1 GG dar? Nach dem soeben Gesagten scheint dies so zu sein.[829] Da ein ISP

---

[824] Vgl. *Fetzer* in: Fetzer u.a., TKG, § 3 Rn. 102 ff.; *Sieber/Höfinger*, MMR 2004, 575 (582).
[825] Gemäß § 3 Nr. 24 TKG sind Telekommunikationsdienste „*in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen*". Internet Service Provider, deren Kernaufgabe die Übertragung von (Internet-)Daten ist, sind folglich der paradigmatische Fall eines Telekommunikationsanbieters im Sinne des TKG.
[826] Vgl. BGH, Urt. v. 16.05.2017, VI ZR 135/13, NJW 2017, 2416, (2418) Die ISPs können demnach mit Hilfe der jeweils zuständigen Behörde und dem Access Provider die IP-Adresse einem bestimmten Anschlussinhaber zuordnen lassen. Dies kann bei Strafanzeige durch den ISP durch die Strafverfolgungsbehörden und bei Gefahren für die öffentliche Sicherheit und Ordnung durch die jeweils für die Gefahrenabwehr zuständige Behörde geschehen. Diese stellen dann ein Auskunftsverlangen an den Access Provider. Eine solche Auskunft kann auch die Zuordnung von Bestandsdaten zu dynamischen IP-Adressen zum Inhalt haben, vgl. BVerfG, Beschl. v. 24.01.2012, 1 BvR 1299/05, Bestandsdatenspeicherung, BVerfGE 130, 151 (210).
[827] BVerfG, Urt. v. 02.03.2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Vorratsdatenspeicherung, BVerfGE 125, 260 (342).
[828] BVerfG, Urt. v. 14.07.1999, 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, Telekommunikationsüberwachung I, BVerfGE 100, 313 (366); BVerfG, Urt. v. 02.03.2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Vorratsdatenspeicherung, BVerfGE 125, 260 (317); so implizit auch EuGH, Urt. v. 19.10.2016, Rs. C-582/14, Breyer, EU:C:2016:779, Rn. 38.
[829] Dies ist nicht nur die Ansicht in der soeben zitierten europäischen und nationalen verfassungsgerichtlichen Rechtsprechung. Auch die Literaturmeinungen gehen in diese Richtung. Vgl. nur

zur Durchführung einer IP-Sperre in jedem Fall IP-Adressen verarbeiten muss, scheinen die Voraussetzungen zunächst offenkundig gegeben.

(1) Eingriff bei Kommunikationsverhinderung

Nichtsdestotrotz ist die Antwort auf diese Frage aus verschiedenen Gründen umstritten. Zum einen wird gegen IP-Sperren als Eingriff in Art. 10 Abs. 1 GG vorgebracht, hier werde nicht in einen bestehenden Kommunikationsprozess eingegriffen, vielmehr würden die Informationen aus der Kenntnisnahme von der IP-Adresse nur dazu verwendet zu verhindern, dass überhaupt eine Telekommunikationsverbindung zustande komme. Im Fall von Kommunikationsverhinderung, -erschwerung oder -unterbrechung liege allerdings kein Eingriff in Art. 10 GG vor.[830] Das dahinterstehende Argument ist – wie *Durner* erklärt –, dass Brief-, Post- und Telekommunikationsgeheimnis einheitlich auszulegen seien. In Bezug auf das Briefgeheimnis sei aber unumstritten, dass die Nichtzustellung von Briefen an einzelne Strafgefangene kein Eingriff in das Briefgeheimnis sei.[831]

Der Ansicht, dass die Kommunikationsverhinderung kein Eingriff in Art. 10 Abs. 1 GG sei, da die Norm eben keine Kommunikation gewährleisten wolle, sondern nur die Privatheit der Kommunikation schützen, ist durchaus grundsätzlich etwas abzugewinnen. Die Gewährleistung des Zustandekommens von Kommunikation wird schließlich bereits durch Art. 5 Abs. 1 Satz 1 u. Satz 2 GG umfassend geschützt. Das Telekommunikationsgeheimnis kann allerdings nur insoweit nicht greifen, wie es tatsächlich lediglich um den Umstand der Verhinderung von Kommunikation geht und nicht um deren gleichzeitige Kenntnisnahme. Denn werden zugleich Kommunikationsinhalte und deren nähere Umstände erfasst, ist diesbezüglich die von Art. 5 Abs. 1 GG nicht geschützte Privatheit der

---

Greiner, Gefahrenabwehr, S. 116; *Heliosch*, Sperrmaßnahmen im Internet, S. 213; *Schnabel*, K&R 2008, 26 (30); *Schmidt*, Gefahrenabwehrmaßnahmen, S. 186; *Sieber/Nolde*, Sperrverfügungen, S. 83.

[830] BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 69; OLG Köln, Urt. v. 18.07.2014, I-6 U 192/11, 6 U 192/11, Goldesel, Rn. 936 (juris); *Hermes* in: H. Dreier, Grundgesetz, Bd. 1, Art. 10 GG Rn. 91; *Durner*, ZUM 2010, 833 (842); *ders*., in: Maunz/Dürig, Art. 10 GG Rn. 71 ff. (Stand: 91. Erg.-Lfg., April 2020); *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 10 GG Rn. 12; *Leistner/Grisse*, GRUR 2015, 19 (22); *Gusy* in: v. Mangoldt/Klein/Starck, Grundgesetz Bd. 1, Art. 10 GG Rn. 57; *Martini* in: v. Münch/Kunig, Grundgesetz Bd. 1, 7. Aufl. 2021, Art. 10 GG Rn. 30.

[831] *Durner*, ZUM 2010, 833 (842); zur Rechtslage beim Abfangen von Gefangenenpost vgl. *ders*. in: Maunz/Dürig, Art. 10 GG Rn. 71 (Stand: 91. Erg.-Lfg., April 2020).

Kommunikation betroffen.[832] In diesen Fällen muss Art. 10 Abs. 1 GG anwendbar bleiben, da ansonsten Schutzlücken entstünden.[833]

Das Bundesverfassungsgericht hat in diesem Kontext folgerichtig entschieden, dass nicht nur die Verarbeitung der näheren Umstände tatsächlich erfolgter Kommunikation, sondern auch diejenige im Rahmen bloßer (fehlgeschlagener) Verbindungsversuche den Schutz des Telekommunikationsgeheimnisses genießt.[834]

Auch das Argument, die Situation bei IP-Sperren sei mit den Gefangengenpost-Fällen vergleichbar, verfängt nicht. Dass einem Strafgefangenen gewisse Briefpost nicht zugestellt wird, ist in Hinsicht auf das Gefährdungspotenzial für die Grundrechte des Betroffenen nicht vergleichbar. Zwar muss sowohl für die Unterbrechung von elektronischem Datenverkehr über IP-Sperren als auch im Fall des Abfangens der Briefpost letztlich die Empfängeradresse ausgewertet werden. In beiden Fällen handelt es sich dabei auch nicht um den Inhalt der Kommunikation, sondern um deren nähere Umstände. Dennoch ist – wie bereits soeben festgestellt wurde – die IP-Adresse eines Internet-Angebots in Verbindung mit anderen Daten dazu in der Lage, einen Großteil des Kommunikationsinhalts mit einiger Wahrscheinlichkeit offenzulegen.[835] Eine Gefahr, die bei der Briefpost nicht in gleichem Maße besteht.[836]

Schließlich wäre es auch im Sinne der Grundrechtskohärenz wenig glücklich, die Unterbrechung und Verhinderung von Internet-Telekommunikation grundsätzlich nicht als Eingriff in das Telekommunikationsgeheimnis zu werten, da die dem Art. 10 Abs. 1 GG

---

[832] Vgl. zur Abgrenzung zwischen Art. 5 Abs. 1 GG und Art. 10 Abs. 1 GG in diesem Sinne BVerfG, Urt. v. 27.07.2005, 1 BvR 668/04, Telekommunikationsüberwachung II, BVerfGE 113, 348 (364). Fälle, in denen staatliche Kommunikationsverhinderung nicht zwangsläufig in das Telekommunikationsgeheimnis eingreifen würden, sind durchaus denkbar. So könnte ein bestimmtes Internet-Angebot auf staatliche Anordnung hin gelöscht werden oder ein bestimmter Server unerreichbar gemacht, indem beispielsweise eine sogenannte Denial-of-Service-Attacke (DoS-Attacke) auf den fraglichen Server ausgeführt würde. Andere Möglichkeiten liegen im Kappen physischer oder funkbasierter Übertragungswege, etwa durch das Durchtrennen von Glasfaserleitungen oder den Einsatz von Störsendern. In diesen Fällen wird Telekommunikation, auch durchaus zielgerichtet, unterbunden, ohne jedoch zugleich Kenntnis von Kommunikationsinhalten oder deren näherer Umstände zu nehmen.

[833] So auch *Frey u.a.*, MMR-Beil. 2012, 1 (9); *Heidrich/Heymann*, MMR 2016, 370 (375); *Schnabel*, K&R 2008, 26 (31); *Sieber/Nolde*, Sperrverfügungen, S. 87.

[834] BVerfG, Urt. v. 12.03.2003, 1 BvR 330/96, 1 BvR 348/99, Handy-Überwachung, BVerfGE 107, 299 (312 f.); BVerfG, Urt. v. 27.02.2008, 1 BvR 370/07, 1 BvR 595/07, Online-Durchsuchung, BVerfGE 120, 274 (307); BVerfG, Urt. v. 02.03.2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Vorratsdatenspeicherung, BVerfGE 125, 260 (309).

[835] BVerfG, Urt. v. 02.03.2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Vorratsdatenspeicherung, BVerfGE 125, 260 (342).

[836] *Frey u.a.*, MMR-Beil. 2012, 1 (9).

auf europäischer Ebene entsprechenden Art. 8 Abs. 1 EMRK bzw. Art. 7 Charta diese Handlungen unstreitig als Eingriff sehen.[837]

(2) Eingriff trotz Verarbeitung bereits zu Routingzwecken

Als weiterer Einwand gegen die Eingriffsqualität von IP-Sperren wird vereinzelt vorgebracht, dass die Internet Service Provider ohnehin die IP-Adressen zu Routing-Zwecken zur Kenntnis nehmen müssten.[838] Verarbeiten die ISPs die IP-Adressen gleichzeitig auch, um auf diese Weise IP-Sperren zu realisieren, würden keine zusätzlichen Daten verarbeitet. Daher existiere keine zusätzliche Beschwer für die Nutzer, so dass in der IP-Sperre kein Eingriff liegen könne.[839]

Diesem Argument kann hier nicht zugestimmt werden. Wie bereits festgestellt, richten sich die Maßstäbe, an denen sich die Verarbeitung personenbezogener Daten im Anwendungsbereich des Art. 10 Abs. 1 GG auszurichten hat, insbesondere auch nach denen des Grundrechts auf informationelle Selbstbestimmung.[840] Eine Zweckänderung bei der Verarbeitung personenbezogener Daten bedarf einer eigenständigen Rechtsgrundlage und ist damit auch eine eigenständige Beschwer.[841] Nichts anderes als eine Zweckänderung ist es jedoch, wenn der ISP eine IP-Adresse nicht mehr zum Zwecke des unbedingten Routings verarbeitet, sondern zum Zwecke der Entscheidung, ob ein Routing stattfinden solle.[842]

(3) Erheblichkeitsschwelle bei Eingriffen in das Telekommunikationsgeheimnis

Schließlich steht ein Eingriff ins Telekommunikationsgeheimnis im Rahmen von IP-Sperren auch deshalb infrage, weil das Bundesverfassungsgericht für Eingriffe in Art. 10 Abs. 1 GG durch Abgleich von Daten mit einer Blacklist eine Erheblichkeits-

---

[837] EGMR, Urt. v. 15.02.1992, Nr. 10802/84, Pfeifer und Plankl ./. Österreich, Serie A Nr. 227; *Kingreen* in: Calliess/Ruffert, EUV/AEUV, Art. 7 Charta Rn. 10; *Hermes* in: H. Dreier, Grundgesetz, Bd. 1, Art. 10 Rn. 7. Vgl. auch oben Kap. 2 V 3 a) (S. 103) m.w.N.

[838] Zur technischen Notwendigkeit der Verarbeitung von IP-Adressen fürs Routing vgl. oben Kap. 1 I 3 (S. 6).

[839] Mit diesem Argument verneint das OLG Köln, Urt. v. 18.07.2014, I-6 U 192/11, 6 U 192/11, Goldesel, Rn. 937 f. (juris) einen Eingriff in das Telekommunikationsgeheimnis durch IP-Sperren (und DNS-Sperren). So auch noch in seiner Master-Arbeit *Schnabel*, Sperrungsverfügungen gegen Access-Provider – Technische Möglichkeiten und rechtliche Zulässigkeit anhand eines praktischen Beispiels, S. 62; später einen Eingriff in Art. 10 Abs. 1 GG ohne weiteres bejahend *Schnabel*, K&R 2008, 26 (31).

[840] BVerfG, Urt. v. 14.07.1999, 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, Telekommunikationsüberwachung I, BVerfGE 100, 313 (359); BVerfG, Urt. v. 02.03.2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Vorratsdatenspeicherung, BVerfGE 125, 260 (310). Vgl. auch oben Kap. 3 IV 2 b) (S. 198) m.w.N.

[841] BVerfG, Urt. v. 14.07.1999, 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, Telekommunikationsüberwachung I, BVerfGE 100, 313 (360). Vgl. zu den grundsätzlich möglichen Rechtsgrundlagen für die Datenverarbeitung Art. 6 Abs. 1 DSGVO.

[842] Im Ergebnis so auch *Heliosch*, Sperrmaßnahmen im Internet, S. 221 f.; *Sieber/Nolde*, Sperrverfügungen, S. 89.

schwelle für notwendig erachtet. Eine Erfassung von Daten stelle keinen Gefährdungstatbestand dar, wenn diese Daten *„nach der Erfassung technisch wieder spurenlos, anonym und ohne die Möglichkeit, einen Personenbezug herzustellen“*, gelöscht würden.[843]

Das Bundesverfassungsgericht beschränkte zudem bislang die Eingriffsqualität auf solche Fälle, in denen ein Positivtreffer erfolgt.[844] Danach würde allenfalls in das Telekommunikationsgeheimnis derjenigen Internet-Nutzer eingegriffen, deren versuchter Zugriff eine gesperrte Seite unterbunden würde. Wäre im Einzelfall hingegen keine IP-Sperre erfolgt, weil der Abgleich der IP-Adressen keine Übereinstimmung ergab, und die Daten sofort gelöscht, läge nach dieser Rechtsprechung im Ergebnis kein Eingriff vor.

Auch *Heliosch* lehnt einen Eingriff in Art. 10 Abs. 1 GG durch IP-Sperren abseits von Positivtreffern ab. Bei unverzüglicher Aussonderung der IP-Adresse liege keine hinreichend intensive Grundrechtsbeeinträchtigung für einen Eingriff vor, da kein Bruch der Vertraulichkeit zu befürchten sei, wenn die IP-Adressen nicht gespeichert würden.

Das Erfordernis des Positivtreffers wurde vom Bundesverfassungsgericht mittlerweile jedoch ausdrücklich aufgegeben. Ein Eingriff liege bereits dann vor, wenn ein Datum erfasst werde und dieses als Grundlage für weitere Maßnahmen diene oder dienen könne. Denn Daten, die für einen Datenabgleich erfasst würden, würden die Daten für einen späteren Abgleich erst verfügbar machen.[845] Das Bundesverfassungsgericht scheint hier einen subjektiven Ansatz zu verfolgen: Werden Daten gezielt und nicht ungewollt erhoben, auch wenn die Erhebung bestimmter Daten nicht der eigentliche Zweck der Maßnahme ist, handelt es sich um einen Grundrechtseingriff. Für einen Eingriff in Art. 10 Abs. 1 GG würde es demnach ausreichen, wenn die Erfassung von IP-Adressen die Grundlage für einen weiteren Verarbeitungsschritt bilden würde.

Dieser weiten Auslegung des Eingriffs in Art. 10 Abs. 1 GG ist zuzustimmen. Schutzweck von Art. 10 Abs. 1 GG ist es, die Vertraulichkeit der Kommunikation zu garantieren. Dem Individuum soll durch das Telekommunikationsgeheimnis als Ausprägung des Allgemeinen Persönlichkeitsrechts bei seiner privaten, also nicht an die Öffentlichkeit gerichteten Kommunikation ein staatsfreier Raum geschaffen werden. Der Mensch soll sich und seine Persönlichkeit mithilfe der Kommunikation frei entfalten können, ohne dass er befürchten müsste, dass die Vertraulichkeit seiner Telekommunikation durch den Staat gebrochen

---

[843] BVerfG, Urt. v. 14.07.1999, 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, Telekommunikationsüberwachung I, BVerfGE 100, 313 (366); BVerfG, Urt. v. 12.03.2003, 1 BvR 330/96, 1 BvR 348/99, Handy-Überwachung, BVerfGE 107, 299 (328); BVerfG, Beschl. v. 04.04.2006, 1 BvR 518/02, Rasterfahndung, BVerfGE 115, 320 (343); BVerfG, Urt. v. 11.03.2008, 1 BvR 2074/05, 1 BvR 1254/07, Kfz-Kennzeichenkontrollen 1, BVerfGE 120, 378 (399); BVerfG, Beschl. v. 18.12.2018, 1 BvR 142/15, Kfz-Kennzeichenkontrollen 2, BVerfGE 150, 244 (265 f.).

[844] BVerfG, Urt. v. 14.07.1999, 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, Telekommunikationsüberwachung I, BVerfGE 100, 313 (366); einen Eingriff bei Positivtreffern bejahend *Heliosch*, Sperrmaßnahmen im Internet, S. 224, wenn diese an Ermittlungsbehörden weitergeleitet würden.

[845] BVerfG, Beschl. v. 18.12.2018, 1 BvR 142/15, Kfz-Kennzeichenkontrollen 2, BVerfGE 150, 244 (265 f.); so auch bereits So allerdings noch Greiner, CR 2002, 620 (623); ders., Gefahrenabwehr, S. 157 f., der einen Eingriff auch bei Negativtreffern annimmt..

würde und daraus möglicherweise nachteilige Konsequenzen für ihn entstehen könnten.[846] Dadurch, dass IP-Adressen mit einer Blacklist abgeglichen werden, wird ein Internet-Nutzer zum Gegenstand einer hoheitlich veranlassten Überwachungsmaßnahme, bei der sich die besonderen Gefahren für die Vertraulichkeit der Telekommunikation realisieren und er im Falle eines Negativ-Treffers nicht einmal Kenntnis von der Überwachungsmaßnahme erlangt.

Zudem ist – den Eingriffscharakter verstärkend – zu beachten, dass für einen ISP (insbesondere einen Access Provider), der eine IP-Sperre durchsetzt, oft die faktische Möglichkeit besteht, die jeweiligen Daten der IP-Adresse des Nutzers, des versuchten Zugriff auf eine gesperrte Website und dessen Bestandsdaten zu einer inkriminierenden Information zusammenzuführen.

IP-Sperren stellen folglich Eingriffe in das Telekommunikationsgeheimnis dar. Dies gilt insbesondere für die Verarbeitung der IP-Adressen bei Positivtreffern. Bei einem Positivtreffer im Rahmen der IP-Sperre wird die Vertraulichkeit der Kommunikation nicht nur – wie bei der Speicherung, die unstreitig einen Grundrechtseingriff darstellt[847] – gefährdet; vielmehr realisiert sich diese Gefahr tatsächlich.

Auch bei Negativ-Treffern liegt jedoch nach dem weiten Verständnis des Bundesverfassungsgerichts ein Eingriff vor. Bei IP-Sperren handelt es sich nicht um eine ungezielte und allein technisch bedingte Erfassung von IP-Adressen. Dies wäre vielmehr beim reinen Internet-Routing der Fall, bei dem die Erfassung der IP-Adressen eine technische Notwendigkeit zur Ermöglichung des Telekommunikationsvorganges darstellt und die Erfassung der Daten keinem eigenen Zweck dient. Bei der Durchführung von IP-Sperren hingegen werden die IP-Adressen einem fremden Zweck zugeführt, nämlich Urheberrechte durchzusetzen. Demjenigen, der IP-Sperren durchführt, kommt es gerade auf den Abgleich der IP-Adressen mit einer Blacklist an.

Zusammengefasst lässt sich also festhalten, dass ein Eingriff in Art. 10 Abs. 1 GG durch IP-Sperren stets vorliegt, wenn ein ISP IP-Adressen im Rahmen einer IP-Sperre mit einer Blacklist abgleicht, unabhängig davon, ob ein Abgleich einen Positiv- oder einen Negativtreffer zur Folge hat.

c. Eingriff durch DNS-Sperren

Auch bei den DNS-Sperren stellt sich die Frage, ob diese einen Eingriff in die Telekommunikationsfreiheit darstellen. Zur Erinnerung: DNS-Sperren machen den Domain-Name-Server-Dienst für den Internet-Nutzer nutzlos. Der DNS-Dienst übersetzt die im World Wide Web verbreiteten Domain-Namen in die für das Routing notwendigen IP-Adressen der WWW-Server. Gibt der Nutzer eine Internet-Domain in seinem Browser ein, wird zunächst an den Domain Name Server eine Anfrage nach der zugehörigen IP-Adresse

---

[846] Vgl. *Durner* in: Maunz/Dürig, Art. 10 GG Rn. 63 (Stand: 91. Erg.-Lfg., April 2020).
[847] BVerfG, Urt. v. 02.03.2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Vorratsdatenspeicherung, BVerfGE 125, 260 (309 f.).

gestellt. In der Regel – also ohne implementierte DNS-Sperre – sendet der Domain Name Server daraufhin die IP-Adresse an den Browser des Nutzers zurück. Mit dieser IP-Adresse baut der Browser dann die Verbindung mit dem Server auf, der unter der IP-Adresse zu erreichen ist. DNS-Sperren nutzen aus, dass das DNS-System zwar technisch nicht zwingend zum Verbindungsaufbau im World Wide Web erforderlich ist, es aber derart gängig und komfortabel ist, dass die Internet-Nutzer es im täglichen Gebrauch nicht hinterfragen. Dazu wird die Zuordnungstabelle des DNS-Servers so manipuliert, dass bei einer Anfrage eine falsche IP-Adresse zurückgesendet oder aber eine Antwort verweigert wird.[848]

Ob der soeben beschriebene Vorgang in den Schutzbereich des Art. 10 Abs. 1 GG eingreift, ist stark umstritten. So lehnen *Sieber* und *Nolde* einen Eingriff in Art. 10 Abs. 1 GG durch DNS-Sperren ab. Ihre Begründung: Bei einer DNS-Sperre richte sich die Sperrverpflichtung an den Betreiber eines DNS-Servers. Dieser kann, muss aber nicht der Access Provider des Nutzers sein. Die DNS-Anfrage müsse dabei losgelöst vom Kommunikationsprozess zwischen den eigentlichen Kommunikationsteilnehmern gesehen werden. Betrachte man nur die Kommunikation zwischen Nutzer und DNS-Server, sei letzterer allerdings kein Intermediär, der die Kommunikationssignale einfach nur weiterleite, sondern selbst Kommunikationsteilnehmer. Das zeige sich auch daran, dass die DNS-Abfrage sich auf der Anwendungsebene des TCP/IP-Protokolls abspiele. Auch technisch gesehen handele es sich also um eine Ende-zu-Ende-Kommunikation zwischen dem Nutzer und dem Betreiber des DNS-Servers. Aus diesem Grund könne es bei der DNS-Sperre keinen Eingriff ins Telekommunikationsgeheimnis geben. Die Nutzung des DNS-Dienstes sei mit einem Blick ins Telefonbuch zu vergleichen, der schließlich auch nicht durch das Telekommunikationsgeheimnis geschützt sei, der folgende Telefonanruf allerdings schon. Durch die DNS-Sperre verwirkliche sich keine spezifische aus dem Übermittlungsvorgang resultierende Gefahr des Kommunikationsprozesses, da sich die Sperre in der Sphäre der Kommunikationsteilnehmer auswirke, die nicht vom Schutzbereich des Telekommunikationsgeheimnisses umfasst sei. Anders gesagt: Wenn der Domain-Name irgendwo auf dem Übertragungsweg zwischen Nutzer und DNS-Server ausgelesen und verarbeitet würde, könnte man sehr wohl von einem Eingriff in Art. 10 Abs. 1 GG sprechen, nicht aber, wenn die Verarbeitung beim Betreiber des DNS-Servers stattfinde.[849]

Der BGH indessen verneint einen Eingriff in den Schutzbereich schon deshalb, weil es sich bei Filesharing nicht um Individualkommunikation sondern um Massenkommunikation handele. Zudem seien DNS-Sperren lediglich Maßnahmen zur Kommunikationsverhinderung, die nicht von Art. 10 Abs. 1 GG erfasst würden.[850]

---

[848] Vgl. dazu oben Kap. 1 III 1 (S. 16 f.)

[849] *Sieber/Nolde*, Sperrverfügungen, S. 85; ähnlich argumentierend *Koreng*, Zensur im Internet, S. 142 f.

[850] *Leistner/Grisse*, GRUR 2015, 19 (22); dem folgend BGH, Urt. v. 26.11.2015, I ZR 3/14, 3dl.am, Rn. 54 ff. (juris); BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 67 ff.

Die Argumentation von *Sieber* und *Nolde* wird in der Literatur zu Recht kritisiert. Die Interpretation, dass der Betreiber des DNS-Servers kein Intermediär sei und es sich um einen isoliert zu betrachtenden Kommunikationsprozess handele, bei dem der Betreiber des DNS-Servers Kommunikationsteilnehmer sei, sei zu technisch gedacht. Auf eine rein technische Betrachtungsweise könne es nicht ankommen, vielmehr müsste der Kommunikationsvorgang wertend betrachtet werden. Dann aber könne man nicht zu dem Schluss kommen, dass die Kommunikationsverbindung zum DNS-Server eine eigenständige Verbindung sei. Aus der Perspektive der Internet-Nutzer bilde die Kommunikation mit dem DNS-Server zusammen mit der Kommunikation mit dem Server des Content Providers, den der Nutzer zu erreichen versucht, einen einheitlichen Vorgang. Der Nutzer wisse in der Regel nichts über die technischen Hintergründe, wie die Verbindung zur Website aufgebaut werde. Er gebe den Domain-Namen in das Adressfeld des Internet-Browsers ein und surfe los. Dass die Daten einen Umweg über einen DNS-Server nähmen, sei ihm nicht bewusst und werde für ihn auch nirgends kenntlich.[851]

Ab dem Zeitpunkt, in dem der Nutzer seinem Browser den Befehl gibt, eine bestimmte Website aufzurufen, wird ein vollständig automatisierter Vorgang angestoßen, der erst mit der Anzeige der aufgerufenen Website endet (oder einer entsprechenden Fehlermeldung bei Nichterreichbarkeit). Da keine weiteren Eingaben des Nutzers nach dem Absenden des Domain-Namens erforderlich sind, würde es an einem Eingriff in den Schutzbereich des Telekommunikationsgeheimnisses auch dann nichts ändern, wenn der Nutzer die genauen technischen Hintergründe kennen würde. Denn diese treten durch die vollständige Automatisierung bei natürlicher Betrachtungsweise gänzlich in den Hintergrund. Auch wer grundsätzlich über die technischen Hintergründe weiß, wird im Alltag bei der Benutzung des Internets kaum einen Gedanken an sie verschwenden. Und selbst wenn doch, so wird der kundige Nutzer dennoch ganz selbstverständlich weiterhin das DNS benutzen, weil es einen integralen Bestandteil des Internets bildet, der ohne große Mühen kaum dauerhaft zu umgehen ist.[852]

Bei einer DNS-Sperre wird zudem auch von näheren Umständen der Kommunikation Kenntnis genommen. Ähnlich wie bei der IP-Sperre gilt, dass der Betreiber des DNS-Servers die IP-Adresse des Internet-Nutzers verarbeitet.[853] Bei DNS-Sperren ist der potenzielle Einschnitt in die Privatsphäre des Nutzers sogar tiefer als bei der IP-Sperre.[854] Denn im Gegensatz zur IP-Sperre nimmt der Betreiber des DNS-Servers dabei nicht nur die näheren Umstände der Kommunikation zur Kenntnis, sondern Kommunikationsinhalte.

---

[851] OLG Hamburg, Urt. v. 21.11.2013, 5 U 68/10, 3dl.am, Rn. 90 (juris); *Frey u.a.*, MMR-Beil. 2012, 1 (8 f.); *Greiner*, CR 2002, 620 (623). *Heliosch*, Sperrmaßnahmen im Internet, S. 215. Im Ergebnis auch: *Marberth-Kubicki*, NJW 2009, 1792 (1794). *Durner*, ZUM 2010, 833 (842) lehnt das Argument *Siebers* und *Noldes* zwar ebenfalls als zu technisch anstatt wertend ab. Im Ergebnis stimmt er dennoch mit ihnen überein, da er der Ansicht ist, dass die Eingriffsintensität nicht ausreiche.

[852] Ähnlich *Frey u.a.*, MMR-Beil. 2012, 1 (9); *Heliosch*, Sperrmaßnahmen im Internet, S. 215.

[853] Die Verarbeitung einer IP-Adresse im Rahmen einer DNS-Abfrage ist schon deshalb notwendig, weil der DNS-Server eine Antwort an den anfragenden Computer zurückschicken muss, der nur unter der IP-Adresse erreichbar ist.

[854] OLG Hamburg, Urt. v. 22.12.2010, 5 U 26/09, Rn. 66 (juris).

Nicht nur, dass der Domain-Name in der tiefsten, der Anwendungsschicht des IP-Pakets als Payload der DNS-Anfrage transportiert wird.

Der Domain-Name gibt zudem in der Regel auch deutlich Auskunft über den Inhalt des aufgerufenen Angebots, da der im Domain-Name enthaltene Text nicht selten beschreibt, worin das damit bezeichnete Angebot inhaltlich besteht.[855] Der angefragte Domain-Name lässt sich auch mit etwas Aufwand dem Anschlussinhaber zuordnen, da die IP-Adresse zeitgleich verarbeitet wird und ein Abgleich der Verkehrsdaten mit den Bestandsdaten des Access Providers des Nutzers rechtlich möglich ist.[856]

Die Sachlage ist folglich mit derjenigen bei einer IP-Sperre zu vergleichen.[857] Sowohl bei Positiv- als auch bei Negativ-Treffern handelt es sich um Eingriffe in Art. 10 Abs. 1 GG. Zusammengefasst bedeutet dies, ein Eingriff nicht nur immer dann erfolgt, wenn die DNS-Sperre einen Treffer ausgibt, so dass dem Nutzer nicht die korrekte IP-Adresse zurückgesendet wird (denn zu diesem Zweck hat der Nutzer seine Daten nicht an den DNS-Server übermittelt). Ein Eingriff liegt bereits immer dann vor, wenn ein DNS-Server, der eine DNS-Sperre durchführt, von einem Internet-Nutzer mit einer DNS-Anfrage kontaktiert wird, und diese Anfrage mit der entsprechenden Blacklist abgleicht.

d. Eingriff durch Deep Packet Inspection

Für Filtersysteme, die auf Deep Packet Inspection aufbauen, muss nach dem soeben zu den IP- und DNS-Sperren Gesagten ein Eingriff ins Telekommunikationsgeheimnis bejaht werden. DPI-Filtersysteme scannen den gesamten Datenverkehr, der einen bestimmten Punkt im Netzwerk durchquert auf die Inhalte der Kommunikation hin.[858] Schwerpunkt der Datenuntersuchung sind nicht (nur) die Umstände der Kommunikation, sondern die erheblich sensibleren Nutzdaten aus der Anwendungsschicht der IP-Pakete.[859]

---

[855] *Heliosch*, Sperrmaßnahmen im Internet, S. 215.

[856] Vgl. dazu oben auf Kap. 3 IV 2 b) (S. 197 ff.) die Ausführungen zum Eingriff der IP-Sperre in Art. 10 Abs. 1 GG.

[857] Teilweise, so etwa OLG Hamburg, Urt. v. 21.11.2013, 5 U 68/10, 3dl.am, Rn. 94 ff. (juris) wird auch das Argument vorgebracht, dass auch der historische Gesetzgeber einen Eingriff in Art. 10 Abs. 1 GG durch DNS-Sperren für gegeben hält. § 11 des Zugangserschwerungsgesetzes, das DNS-Sperren für kinderpornographische Internet-Angebote vorsah, hielt fest, dass dessen §§ 2 und 4 das Telekommunikationsgeheimnis gemäß Art. 10 GG einschränken würden.

[858] Filter-Maßnahmen, die auf Deep Packet Inspection basieren, werden in Literatur und Rechtsprechung teilweise auch als „Proxy-Filter" bezeichnet, da die DPI beim Internet Service Provider auf einem Proxy-Server stattfinden kann, über den der zu scannende Datenverkehr umgeleitet wird. Diese Bezeichnung ist unglücklich gewählt. Zum einen ist es kein technischer Zwang, weshalb eine DPI nicht direkt in den Router integriert wird. Dann ist ein Proxy-Server gar nicht notwendig. Zum anderen enthält die Aussage, dass ein Proxy-Server involviert ist, wenig Aussagekraft darüber, was überhaupt technisch und rechtlich bei dem Vorgang vonstattengeht. Eine andere gängige Bezeichnung für DPI-Filter lautet „URL-Sperre". Dies geht auf die Annahme zurück, dass die Sperrmaßnahme in der Weise realisiert wird, dass spezifische URL, die auf urheberrechtliche Inhalte verweisen, in der Anwendungsschicht des IP-Pakets aufgespürt werden und in der Folge der Datenverkehr unterbrochen wird. Diese Bezeichnung ist ebenfalls unglücklich gewählt, da sie nur eine von vielen möglichen Varianten, wie eine DPI-Sperre umgesetzt werden könnte, beschreibt.

[859] *Sieber/Nolde*, Sperrverfügungen, S. 86.

Das EDV-System, dass die Filtermaßnahme durchführt, muss, um seinen Zweck zu erfüllen, Kenntnis von dem Inhalt der Kommunikation nehmen. Der Inhalt der Kommunikation wird dann mit einer Datenbank abgeglichen werden, in der die Informationen, die eine Unterbrechung des Datenverkehrs auslösen, hinterlegt sind.

Es ist unschwer erkennbar, dass ein Eingriff in den Datenverkehr durch DPI-Filter auch einen Eingriff in Art. 10 Abs. 1 GG bedeutet.[860] Die Kommunikationsdaten werden während der Fernübermittlung zur Kenntnis genommen und verarbeitet, so dass sich damit das typische Risiko der Telekommunikation für die Vertraulichkeit der Daten verwirklicht.[861] Im Gegensatz zur IP-Sperre und mit Einschränkungen auch der DNS-Sperre handelt es sich bei den Informationen, die eine Deep Packet Inspection zur Kenntnis nimmt, nicht um die näheren Kommunikationsumstände, sondern um Daten aus der Anwendungsschicht und insbesondere auch des Payloads.[862] Durch die gleichzeitige Kenntnisnahme der IP-Adresse des Providers lässt sich zudem stets ein Personenbezug zwischen Nutzdaten und Anschlussinhaber herstellen. Der Rückgriff auf die IP-Adresse ist zur Begründung der Personenbezogenheit indes gar nicht notwendig, da der Payload in vielen Szenarien bereits selbst personenbezogene Daten enthält.[863] Die Deep Packet Inspection ist auch nicht technikbedingt notwendig, so dass lediglich nebenbei und unabsichtlich die Anwendungsschicht des Datenverkehrs durchsucht wird. Daher wird man hier auch keine Einwilligung des Nutzers in die Verarbeitung der Daten unterstellen können.[864]

Somit gilt für die Deep Packet Inspection der gleiche Maßstab wie für IP- und DNS-Sperren: Sie stellen einen Eingriff in Art. 10 Abs. 1 GG dar, wenn der Internet Service Provider einen bestimmten Datenstrom mittels Deep Packet Inspection untersucht, unabhängig davon, ob Daten gespeichert werden oder ein Positiv-Treffer erfolgt und ein Telekommunikationsvorgang wegen des Ergebnisses der DPI unterbrochen wird.

Zusammenfassend lässt sich feststellen, dass grundsätzlich jede Art von eingerichteten Eingriffen in den Datenverkehr zur Urheberrechtsregulierung einen Eingriff in den

---

[860] *Frey u.a.*, MMR-Beil. 2012, 1 (14); *Gesmann-Nuissl/Wünsche*, GRUR Int 2012, 225 (228 f.); *Heidrich/Heymann*, MMR 2016, 370 (375); *Marberth-Kubicki*, NJW 2009, 1792 (1794); *Sieber/Nolde*, Sperrverfügungen, S. 85 ff.; a.A. *Heliosch*, Sperrmaßnahmen im Internet, S. 221 ff. mit der Begründung, Maßnahmen der DVR würden nicht die vom Bundesverfassungsgericht geforderte Eingriffsintensität erreichen. BGH, Urt. v. 26.11.2015, I ZR 3/14, 3dl.am, Rn. 54 (juris) und BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 66 sehen bereits den Schutzbereich nicht eröffnet; offenlassend *Leistner/Grisse*, GRUR 2015, 19 (25).

[861] *Heidrich/Heymann*, MMR 2016, 370 (375).

[862] *Sieber/Nolde*, Sperrverfügungen, S. 86.

[863] Zum Beispiel E-Mail-Adressen, Formulardaten, private Nachrichten mit Namensnennung, etc. Die Anzahl der möglichen Beispiele ist unüberschaubar.

[864] Vgl. BVerfG, Urt. v. 14.07.1999, 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, Telekommunikationsüberwachung I, BVerfGE 100, 313 (360 f.). Das OLG Köln, Urt. v. 18.07.2014, I-6 U 192/11, 6 U 192/11, Goldesel, Rn. 939, 943 (juris) sieht durch die hohe persönlichkeitsrechtliche Relevanz der DPI und die Tatsache, dass der ISP für seine Kernaufgabe nicht derart weitreichend von den Kommunikationsdaten Kenntnis nehmen müsse, einen schweren Eingriff in das Telekommunikationsgeheimnis an.

Schutzbereich des Art. 10 Abs. 1 GG darstellt, selbst wenn keine Verkehrsdaten gespeichert werden. Denn jede Maßnahme der DVR wird auch Positivtreffer generieren.[865]

3. Schranken des Telekommunikationsgeheimnisses

Nicht jeder Eingriff in das Telekommunikationsgeheimnis stellt jedoch zugleich auch eine Verletzung dieses Grundrechts dar. Die Grundrechte aus Art. 10 Abs. 1 GG sind nicht schrankenlos gewährleistet. Sie können vielmehr gemäß Art. 10 Abs. 2 Satz 1 GG auf Grund eines Gesetzes beschränkt werden.

Für die Beschränkung des Telekommunikationsgeheimnisses ist also zumindest ein Gesetz im materiellen Sinne notwendig, das wiederum auf ein Parlamentsgesetz zurückgehen müsste.[866] *A maiore ad minus* ist entgegen dem Wortlaut („*auf Grund eines Gesetzes*") auch ein Eingriff möglich, der unmittelbar auf ein formelles Gesetz zurückgeht.[867]

Das Bundesverfassungsgericht hat darüber hinaus für die gesetzliche Grundlage spezielle Anforderungen an die Bestimmtheit der Norm formuliert. Insbesondere muss aus dem Gesetz ausdrücklich hervorgehen, dass ein Eingriff ins Telekommunikationsgeheimnis erfolgt. Wenn dies nur stillschweigend vorausgesetzt wird, ist dies nicht ausreichend. Das BVerfG formuliert damit zusätzlich zum formellen Zitiergebot ein materielles Zitiergebot. Dies sei unabdingbar, da Grundrechtseingriffe in Art. 10 Abs. 1 GG einem Verfahren nachfolgen müssten, in dem die Öffentlichkeit über die parlamentarische Debatte Gelegenheit hatte, sich zur Erforderlichkeit und Reichweite neuer Grundrechtseingriffe eine Meinung zu bilden und diese in einen gesellschaftlichen Diskussionsprozess einzubringen.[868]

4. Schranken-Schranken, insbesondere der Grundsatz der Verhältnismäßigkeit

Auch beim Telekommunikationsgeheimnis gilt, dass Eingriffe in das Grundrecht nicht bereits deshalb verfassungsgemäß sind, weil die Anforderungen der Schranken eingehalten wurden. Die Beschränkungen müssen sich insbesondere am Verhältnismäßigkeitsgrundsatz messen lassen, also einem legitimen Zweck dienen, geeignet, erforderlich und angemessen sein.[869] Bei dem legitimen Zweck, der Geeignetheit und Erforderlichkeit kann

---

[865] So auch im Ergebnis *Greiner*, CR 2002, 620 (623).
[866] *Windthorst* in: Gröpl u.a., Grundgesetz, Art. 10 Rn. 60.
[867] Vgl. BVerfG, Urt. v. 02.03.2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Vorratsdatenspeicherung, BVerfGE 125, 260 (313).
[868] BVerfG, Beschl. v. 25.03.1992, 1 BvR 1430/88, Fangschaltung, BVerfGE 85, 386 (403 f.). Insoweit ist auch das Argument von *Durner*, ZUM 2010, 833 (836) kritisch zu sehen, das Zitiergebot finde bei zivilrechtlichen Anordnungen einer DVR keine Anwendung, da sich das formelle Zitiergebot des Art. 19 Abs. 1 Satz 2 GG nur auf die Eingriffsverwaltung beziehe. Die Beeinträchtigung der Grundrechte bleibt aus Sicht des Bürgers die gleiche, auch wenn es sich nicht um Eingriffsverwaltung handelt. Es ist kein Grund ersichtlich, weshalb das materielle Zitiergebot keine Anwendung finden sollte, wenn ein Eingriff in Art. 10 Abs. 1 GG durch eine zivilgerichtliche Anordnung erfolgen sollte.
[869] BVerfG, Urt. v. 14.07.1999, 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, Telekommunikationsüberwachung I, BVerfGE 100, 313 (359); *Hermes* in: H. Dreier, Grundgesetz, Bd. 1, Art. 10 Rn. 69; *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 10 Rn. 20 ff.

auf die Ausführungen zur verhältnismäßigen Beschränkung der Art. 5 Abs. 1 Satz 1 GG und 12 Abs. 1 GG verwiesen werden, da sich insoweit keine grundrechtsspezifischen Besonderheiten beim Telekommunikationsgeheimnis ergeben.[870]

Übrig bleibt die Frage, ob Eingriffe in das Telekommunikationsgeheimnis mittels datenverkehrsregulierender Maßnahmen zur Durchsetzung des Urheberrechts auch verhältnismäßig im engeren Sinne, also angemessen sind. Da die Eingriffe in Art. 10 Abs. 1 GG hier je nach verwendetem technischen Verfahren unterschiedlich schwerwiegend sind, ist es sinnvoll, die verschiedenen Verfahren getrennt voneinander zu untersuchen.

Auf rein abstrakter Ebene genießt das Telekommunikationsgeheimnis einen etwas höheren Stellenwert als das Urheberrecht, das als Eigentum im verfassungsrechtlichen Sinne ebenfalls – in Gestalt von Art. 14 GG – grundrechtlich geschützt ist.

Der Gesetzgeber darf gemäß Art. 14 Abs. 1 Satz 2 GG das Eigentum durch Gesetze beschränken und ausgestalten. Damit handelt es sich um ein Grundrecht mit einfachem Gesetzesvorbehalt.[871]

Auch das Telekommunikationsgeheimnis kann der Gesetzgeber gemäß Art. 10 Abs. 2 Satz 1 GG durch einfaches Gesetz beschränken.[872] Beim Telekommunikationsgeheimnis kommt allerdings hinzu, dass es eine spezielle Ausprägung des gemäß Art. 2 Abs. 1, 1 Abs. 1 GG geschützten Allgemeinen Persönlichkeitsrechts ist.[873] Diese Nähe zur Garantie der Menschenwürde erhebt die abstrakte Bedeutung des Telekommunikationsgeheimnisses daher leicht über die der Eigentumsfreiheit.

Dies darf jedoch nicht so verstanden werden, als wäre damit bereits eine Vorentscheidung darüber gefallen, dass Eingriffe in den Datenverkehr zur Durchsetzung des Urheberrechts stets unzulässig seien. Vielmehr müssen die konkreten widerstreitenden Interessen gegeneinander abgewogen werden, wobei das abstrakte Übergewicht der Telekommunikationsfreiheit lediglich eine erste Tendenz aufzeigt.

Mitentscheidendes Kriterium im Rahmen der Abwägung ist die Effektivität der Maßnahmen. Der Internet-Nutzer muss Eingriffe in seine Grundrechte grundsätzlich umso eher hinnehmen, je wirksamer damit dem Urheberrecht zur Durchsetzung verholfen wird. Die Effektivität der unterschiedlichen datenverkehrsregulierenden technischen Maßnahmen wurde in dieser Arbeit bereits ausführlich behandelt.[874] Der hier anzulegende Effektivitätsmaßstab ist schutzniveau- und nicht maßnahmebezogen. Die Effektivität bestimmst

---

[870] Siehe oben Kap. 3 II 4 (S. 149 ff.) (Berufsfreiheit) und Kap. 3 III 4 (S. 174 ff.) (Informationsfreiheit).
[871] *Grochtmann*, Art. 14 GG – Rechtsfragen der Eigentumsdogmatik, S. 320. Vgl. zur abstrakten Wertigkeit der Eigentumsgarantie bereits oben Kap. 3 III 4 (S. 176 f.).
[872] *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 10 Rn. 16; *Martini* in: v. Münch/Kunig, Grundgesetz Bd. 1, 7. Aufl. 2021, Art. 10 Rn. 113 f.
[873] *Martini* in: v. Münch/Kunig, Grundgesetz Bd. 1, 7. Aufl. 2021, Art. 10 Rn. 4; *Rohlf*, Privatsphäre, S. 163 ff.
[874] Vgl. oben Kap. 1 IV 4 (S. 39 ff.).

sich also danach, ob durch die Maßnahme Verletzungen des Urheberrechts an einem konkreten Schutzgegenstand insgesamt verringert werden. [875] Wie bereits festgestellt, sind IP-Sperren und DNS-Sperren wenig effektiv, wobei die IP-Sperren ein wenig effektiver als die DNS-Sperren sind. DPI-Filter hingegen zeichnen sich durch eine sehr hohe schutzniveau-bezogene Effektivität aus.39[876]

Auf der anderen Seite ist auch die Intensität der Eingriffe der verschiedenen Maßnahmen in Art. 10 Abs. 1 GG unterschiedlich stark ausgeprägt. Dabei ist sowohl von Bedeutung, wie viele Personen von der Maßnahme betroffen werden, als auch, wie intensiv jeder einzelne Eingriff ist. Ebenso spielen die Einschreitschwellen und die Frage, ob die Eingriffe heimlich erfolgen, eine Rolle.[877]

a. Angemessenheit der Deep Packet Inspection

Die Deep Packet Inspection erfasst grundsätzlich die gesamte Menge an Daten, die einen bestimmten Netzknoten durchquert, an dem sie durchgeführt wird. Würde ein DPI-Filter nur stichprobenartig eingesetzt, würde proportional dazu auch dessen Effektivität abnehmen. Die Überwachung des Datenverkehrs wäre folglich allgemein und flächendeckend. Die besondere Schwere einer solchen umfassenden Kontrolle des Datenverkehrs findet im europäischen Sekundärrecht sogar ihre ausdrückliche Entsprechung in Art. 15 *RL 2000/31/EG*, der diese Art der Überwachung verbietet. Der EuGH hat in seiner Scarlet-Entscheidung zudem festgestellt, dass dies auch aufgrund der europäischen Grundrechte geboten ist.[878]

Nicht nur die Menge der Eingriffe, sondern auch die Intensität der Eingriffe durch die DPI sticht hervor. Zum einen werden DPI-Filter in der Regel für den Betroffenen unerkannt eingesetzt werden. Jeder einzelne untersuchte Datenstrom ist ein Eingriff in das Telekommunikationsgeheimnis der beteiligten Teilnehmer, selbst wenn der Filtermechanismus letztlich nicht ausgelöst wird. Diese darüber stets zu informieren, dürfte technisch und praktisch kaum möglich sein. Hinzu kommt, dass die Information voraussetzen würde, dass das Ergebnis der DPI gespeichert und tatsächlich mit den betroffenen Nutzern in Beziehung gesetzt würde, was die Eingriffsintensität wiederum stark erhöhen würde. Würde ein Nutzer hingegen von der Sperre erfasst (Positivtreffer) und auf eine Sperrseite umgeleitet statt lediglich gesperrt, so wie dies nach dem Zugangserschwerungsgesetz vorgesehen war, würde der Nutzer wiederum *Chilling Effects* ausgesetzt.[879]

---

[875] Vgl. oben Kap. 1 IV 2 (S. 37).
[876] Vgl. oben Kap. 1 IV 4 (S. 39 ff.).
[877] BVerfG, Urt. v. 27.07.2005, 1 BvR 668/04, Telekommunikationsüberwachung II, BVerfGE 113, 348 (382); BVerfG, Beschl. v. 16.06.2009, 2 BvR 902/06, E-Mail-Beschlagnahme, BVerfGE 124, 43 (62).
[878] Vgl. EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Scarlet Ext., Slg. 2011, I-11959, Rn. 53, wobei der Gerichtshof offen lässt, ob der Eingriff in Art. 8 und 11 Charta allein für eine Verletzung europäischer Grundrechte ausgereicht hätte oder ob dies lediglich im Zusammenhang mit den Beeinträchtigungen der unternehmerischen Freiheit der Fall ist. Vgl. dazu auch oben Kap. 2 V 1 d) (S. 83 f.)
[879] Ähnlich OLG Köln, Urt. v. 18.07.2014, I-6 U 192/11, 6 U 192/11, Goldesel, Rn. 940 (juris).

Die Intensität der Eingriffe durch Deep Packet Inspection ist aber vor allen Dingen deshalb als so hoch einzuschätzen, weil sie so tief in die übermittelten Daten hineinschauen muss, um ihre Aufgabe effektiv zu erfüllen.[880] Die DPI untersucht den Payload eines Datenpakets, und nimmt damit die Inhalt jeglicher Kommunikation, die an einem bestimmten Punkt das Internet durchquert, zur Kenntnis. Da sämtlicher Datenverkehr verarbeitet wird, ist es denklogisch, dass auch Informationen aller Art gescannt werden. Diese können lediglich der Sozialsphäre des Internet-Nutzers zuzuordnen sein, zwangsläufig werden aber auch solche Informationen erfasst, die der Privat- oder gar Intimsphäre des Nutzers zuzuordnen sind.

Insbesondere zur Kenntnis genommene Inhalte aus der Intimsphäre sind hier hochproblematisch. Das Bundesverfassungsgericht sieht diesen Kernbereich privater Lebensgestaltung als durch Art. 1 Abs. 1 GG weitgehend absolut geschützt an.[881] Zu diesem Kernbereich zählt das Bundesverfassungsgericht insbesondere Kommunikationsvorgänge, mit denen der Betroffene der Maßnahme ein besonders enges Vertrauensverhältnis teilt, also beispielsweise engen Familienangehörigen oder bestimmten Berufsgeheimnisträgern, aber auch bestimmte Dateien wie tagebuchähnliche Aufnahmen oder private Filmdokumente.[882]

Zwar schließt das BVerfG eine Überwachung des Datenverkehrs, bei dem das Risiko besteht, dass Informationen aus dem Kernbereich privater Lebensführung erhoben werden, nicht in jedem Fall aus. Allerdings ist dies nur unter sehr strengen Bedingungen möglich, die bei einer Datenverkehrsregulierung zur Durchsetzung des Urheberrechts nicht gegeben sind.

Die Ermächtigungsgrundlage müsse weitestgehend sicherstellen, dass Daten mit einem Bezug zum Kernbereich privater Lebensführung nicht erhoben würden.[883] An dieser Stelle lässt sich einer DVR mittels DPI-Filtern entgegenhalten, dass die gesetzliche Grundlage der DPI die Gefahr der Kenntnisnahme von Informationen aus dem Kernbereich privater Lebensgestaltung entgegentreten kann, indem sie die Anwendung von DPI-Filtern verbietet und stattdessen auf die weniger invasiven IP- und DNS-Sperren verweist.

---

[880] OLG Köln, Urt. v. 18.07.2014, I-6 U 192/11, 6 U 192/11, Goldesel, Rn. 939 (juris); OLG Hamburg, Urt. v. 21.11.2013, 5 U 68/10, 3dl.am, Rn. 98 (juris); *Frey/Rudolph*, Haftungsregime, Rn. 172; *Sieber/Nolde*, Sperrverfügungen, S. 85.

[881] BVerfG, Beschl. v. 12.10.2011, 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08, TKÜ-Neuregelung, BVerfGE 129, 208 (245 f.).

[882] BVerfG, Urt. v. 03.03.2004, 1 BvR 2378/98, 1 BvR 1084/99, Großer Lauschangriff, BVerfGE 109, 279 (322); BVerfG, Urt. v. 27.02.2008, 1 BvR 370/07, 1 BvR 595/07, Online-Durchsuchung, BVerfGE 120, 274 (337); BVerfG, Beschl. v. 12.10.2011, 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08, TKÜ-Neuregelung, BVerfGE 129, 208 (258 ff.).

[883] BVerfG, Urt. v. 27.02.2008, 1 BvR 370/07, 1 BvR 595/07, Online-Durchsuchung, BVerfGE 120, 274 (337); BVerfG, Beschl. v. 12.10.2011, 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08, TKÜ-Neuregelung, BVerfGE 129, 208 (245); *Hömig*, JURA 2009, 207 (212); *Durner* in: Maunz/Dürig, Art. 10, Rn. 202 (Stand: 91. Erg.-Lfg., April 2020).

Auch dürfe eine Überwachungsmaßnahme nicht zum Einsatz kommen, wenn bereits im Voraus klar ist, dass diese den Kernbereich privater Lebensführung berühren wird.[884] Gerade dies geht mit flächendeckender Überwachung der Kommunikationsinhalte jedoch zwingend einher. Zwar lässt das Bundesverfassungsgericht in Ausnahmefällen auch dann eine Überwachung zu, wenn die Kenntnisnahme von Informationen aus dem Kernbereich privater Lebensführung unvermeidbar sei, da der Kernbereichsbezug im Einzelfall nicht stets schnell genug vor Kenntnisnahme entdeckt werden könne. Dies betrifft allerdings keine Fälle allgemeiner, anlassloser, flächendeckender Telekommunikationsüberwachung, sondern lediglich Ermittlungsmaßnahmen bei begründetem Verdacht, dass konkrete Individuen schwere Straftaten begangen haben oder diese begehen wollen.[885] Im hier einschlägigen Sachverhalt fehlt es sowohl an der *konkreten* Überwachungsmaßnahme, zum anderen ist nicht-gewerbliches illegales Filesharing von Privatpersonen, auch wenn man es keinen Anlass zur Bagatellisierung gibt, nicht der Schwerkriminalität zuzuordnen.

DPI-Filter stellen daher einen unverhältnismäßigen Eingriff in den Schutzbereich des Telekommunikationsgeheimnisses dar und verstoßen folglich gegen Art. 10 Abs. 1 GG.

b. Angemessenheit von IP- und DNS-Sperren

Fraglich ist außerdem, ob auch IP- und DNS-Sperren unangemessen in den Schutzbereich von Art. 10 Abs. 1 GG eingreifen. Eingriffe in den Kernbereich privater Lebensgestaltung sind hier nicht zu befürchten. Der Kernbereich betrifft in erster Linie Emotionen, Überlegungen, Meinungen und Erfahrungen mit höchstpersönlichem Charakter sowie die Möglichkeit, diese im privaten Kontext äußern zu können, ohne sich davor fürchten zu müssen, dass der Staat diese Äußerungen überwachen könnte.[886] Der Kernbereich privater Lebensgestaltung befindet sich im Rahmen der Telekommunikation also hauptsächlich in den Kommunikationsinhalten. Weder die IP- noch die DNS-Sperre nehmen jedoch unmittelbar den eigentlichen Inhalt der Kommunikation zur Kenntnis. Diese Spielarten der Netzsperren beschränken sich auf die gleichwohl von Art. 10 Abs. 1 GG geschützten näheren Umstände der Kommunikation. Zwar verschwimmen gerade bei den Domain-Namen, mit Einschränkungen auch bei den IP-Adressen ein wenig die Grenzen zwischen den näheren Umständen und den Inhalten der Kommunikation, da die erhobenen Informationen Rückschlüsse auf den Inhalt der aufgerufenen Web-Angebote liefern können. Diese

---

[884] BVerfG, Urt. v. 27.02.2008, 1 BvR 370/07, 1 BvR 595/07, Online-Durchsuchung, BVerfGE 120, 274 (338 f.); *Gudermann*, Online-Durchsuchung im Lichte des Verfassungsrechts, S. 280.
[885] BVerfG, Beschl. v. 12.10.2011, 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08, TKÜ-Neuregelung, BVerfGE 129, 208 (245 f.); *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 10 Rn. 23.
[886] BVerfG, Urt. v. 27.02.2008, 1 BvR 370/07, 1 BvR 595/07, Online-Durchsuchung, BVerfGE 120, 274 (337); BVerfG, Urt. v. 03.03.2004, 1 BvR 2378/98, 1 BvR 1084/99, Großer Lauschangriff, BVerfGE 109, 279 (313 f.).

Tatsache führt daher auch zu einer gesteigerten Intensität des Eingriffs ins Telekommunikationsgeheimnis.[887] Nichtsdestotrotz wird auf diese Weise die Grenze zum Kernbereich privater Lebensführung nicht überschritten.

Im Ergebnis sind IP- wie auch DNS-Sperren dennoch als unverhältnismäßiger Eingriff in den Schutzbereich des Telekommunikationsgeheimnisses zu bewerten, da die Grundrechtsbeschränkungen zu schwer wiegen, als dass die positiven Effekte für den Urheberrechtsschutz diese aufwiegen könnten.

Bei den Eingriffen in Art. 10 Abs. 1 GG handelt es sich um Eingriffe hoher Intensität, die eine Vielzahl an Menschen betreffen. IP- und DNS-Sperren verarbeiten Daten, die Bewegungen der Menschen im Internet nachvollziehbar machen können. Dies können Informationen sein, die lediglich die Sozialsphäre betreffen, beispielsweise wenn ein Internet-Nutzer sich unter seinem Klarnamen in einem öffentlichen Forum äußert. Auch diese Informationen werden bereits durch Art. 10 Abs. 1 GG vor staatlicher Kenntnisnahme geschützt.[888] Ein Großteil der genutzten Internet-Angebote wird jedoch der qualifiziert geschützten Privatsphäre zuzurechnen sein. Die Privatsphäre umfasst alle Umstände, die aufgrund ihres Inhalts üblicherweise als privat angesehen werden.[889] Im Bereich der Internet-Nutzung sind damit all die Aktivitäten umfasst, die man in der Regel nicht mit der Öffentlichkeit teilen möchte, vom Informationsverhalten über den Medienkonsum bis zur Teilnahme an privaten Diskussionsforen.

IP- und DNS-Sperren stellen zudem keine zielgerichteten Maßnahmen dar, die sich auf die Prüfung der näheren Kommunikationsumstände bestimmter, ausgesuchter Individuen beschränken. Der Datenverkehr wird vielmehr umfassend und flächendeckend in Bezug auf die hinterlegten Sperrkriterien verarbeitet. Jede Datenverbindung, die Gegenstand einer Verarbeitung im Rahmen einer IP- oder DNS-Sperre wird, ist als Eingriff in Art. 10 Abs. 1 GG einzustufen.

Auch steht ein Staat, der IP- oder DNS-Sperren vorschreiben will, vor dem Dilemma, dass einerseits problematisch wäre, diese Eingriffe heimlich vorzunehmen,[890] andererseits eine Umleitung des Internet-Nutzers auf eine Sperrseite Chilling Effects bei diesem hervorrufen könnte, die ebenfalls geeignet wären, die Intensität der Grundrechtsbeeinträchtigung zu erhöhen.[891]

Diesen schweren Beeinträchtigungen der Telekommunikationsfreiheit stehen mutmaßlich eher geringe Vorteile bei der Durchsetzung des Urheberrechts gegenüber. IP-Sperren

---

[887] Zur DNS-Sperre: BVerfG, Urt. v. 02.03.2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Vorratsdatenspeicherung, BVerfGE 125, 260 (342); OLG Hamburg, Urt. v. 21.11.2013, 5 U 68/10, 3dl.am, Rn. 66 (juris); *Heliosch*, Sperrmaßnahmen im Internet, S. 215 f.
[888] *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 10 Rn. 8; *Gusy* in: v. Mangoldt/Klein/Starck, Grundgesetz Bd. 1, Art. 10 Rn. 24.
[889] BVerfG, Beschl. v. 24.02.2015, 1 BvR 472/14, Auskunftsanspruch des Scheinvaters, BVerfGE 138, 377, Rn. 29.
[890] *Durner* in: Maunz/Dürig, Art. 10 GG Rn. 192 (Stand: 91. Erg.-Lfg., April 2020).
[891] Vgl. oben Kap. 3 III 4 b) (4) (S. 187 ff.).

und insbesondere DNS-Sperren mangelt es an schutzniveaubezogener Effektivität.[892] Hinzu kommt, dass es sich bei illegalem Filesharing nicht um eine schwere Straftat handelt, für deren Verhinderung gravierende Grundrechtsbeschränkungen hingenommen werden müssten. Zudem besitzt das Telekommunikationsgeheimnis auch abstrakt ein etwas höheres Gewicht als der Urheberrechtsschutz.

c. Gefahr von Mission creep

Nicht unerwähnt bleiben soll hier ein weiteres Argument, dass gegen die Verhältnismäßigkeit von Eingriffen in den Datenverkehr zur Durchsetzung des Urheberrechts spricht und sich inhaltlich am besten bei Art. 10 Abs. 1 GG einfügt, da es im Wesentlichen um die Verhältnismäßigkeit von Überwachungsmaßnahmen geht.

In seiner Entscheidung zur Vorratsdatenspeicherung stellt das Bundesverfassungsgericht fest, dass die *„Freiheitswahrnehmung"* ihrer Bürger zur *„verfassungsrechtlichen Identität"* der BRD gehöre. Diese sei durch die zunehmende Digitalisierung und die damit einhergehenden Möglichkeiten der totalen Überwachung gefährdet. Möchte der Staat eine neue Überwachungsmaßnahme einführen, müsse er nicht nur berücksichtigen, ob diese für sich genommen verhältnismäßig sei, sondern auch, ob diese Maßnahme nicht in einer Gesamtschau mit allen anderen, bereits bestehenden Überwachungsmaßnahmen dazu führen würde, dass beinahe alle Aktivitäten der Bürger sich aus den erhobenen Daten würden nachvollziehen lassen. Die Grenze des insoweit noch Zulässigen sei mit der Vorratsdatenspeicherung beinahe erreicht.[893]

Zum einen lässt sich aus diesen Feststellungen folgende Schlussfolgerung ziehen: Die Anzahl an insgesamt zulässigen staatlichen Überwachungsmaßnahmen ist begrenzt, und jede zusätzliche Maßnahme wird etwas schwieriger zu rechtfertigen als die vorige, weil das Ausmaß an Freiheitswahrnehmung der Bürger mit jeder neuen Maßnahme ein Stück kleiner geworden ist. Das bedeutet für Eingriffe in den Datenverkehr zur Durchsetzung des Urheberrechts, dass Schwierigkeiten bestehen könnten, sie unter diesem Gesichtspunkt zu rechtfertigen, da auch Maßnahmen der Datenverkehrsregulierung zu den vom BVerfG angesprochenen Überwachungsmaßnahmen gehören. Dies gilt umso mehr, als datenverkehrsregulierenden Maßnahmen eine flächendeckende Überwachung des gesamten Online-Verhaltens mit sich bringen würden, und es sich nicht lediglich um eine gezielte anlassbezogene Überwachung handelt.[894]

---

[892] Vgl. oben Kap. 1 IV 3 (S. 37 ff.).

[893] BVerfG, Urt. v. 02.03.2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Vorratsdatenspeicherung, BVerfGE 125, 260 (323 f.).

[894] Zu dieser Einschätzung kommt auch *Roßnagel*, NJW 2010, 1238 (1240 f.). Diese Einschätzung könne sich allerdings dann ändern, wenn für DVR-Maßnahmen andere gewichtige Überwachungsmaßnahmen quasi im Austausch gestrichen würden. Vgl. *Roßnagel*, NJW 2010, 1238 (1240).

Darüber hinaus macht diese „Überwachungs-Gesamtrechnung“[895] des Bundesverfassungsgerichtsauf eine Gefahr aufmerksam, die mit dem Aufbau der technischen, rechtlichen und organisatorischen Überwachungsinfrastruktur, die zur Durchführung datenverkehrsregulierender Maßnahmen erforderlich ist, sowie dem Tabubruch der flächendeckenden Datenverkehrsüberwachung und -diskriminierung einhergeht: Es besteht die Möglichkeit, dass die Überwachungsstruktur auch zur Durchsetzung in anderen Rechtsfeldern herangezogen wird, wenn sie erst einmal für die Durchsetzung des Urheberrechts eingerichtet und im Alltag erprobt wurde.[896] Im englischsprachigen Sprachraum wird dieses Phänomen einprägsam als „Mission creep“ bezeichnet und beschreibt die schleichende Ausweitung von Zuständigkeiten oder Aufgaben einer Organisation oder Institution nach anfänglichen Erfolgen.[897]

Tatsächlich fallen unter Verhältnismäßigkeitsgesichtspunkten wenig rechtliche Argumente ein, weshalb es erlaubt sein sollte, DPI oder andere Formen von Netzsperren zur Durchsetzung des Urheberrechts einzusetzen, aber nicht, um noch gewichtigeren Rechtsgütern Geltung im Internet zu verschaffen, wie beispielsweise dem Kampf gegen Kinderpornographie, oder aber solchen, die auf einer vergleichbaren Ebene anzusiedeln sind, wie der Verhinderung illegalen Glücksspiels.[898]

Heliosch hingegen sieht in Mission creep kein valides verfassungsrechtliches Argument.[899] Dem kann hier allerdings nicht zugestimmt werden. Mit der Überwachungs-Gesamtrechnung hat das Bundesverfassungsgericht das Argument etabliert, dass eine Vielzahl an Überwachungsmaßnahmen gegen das Grundgesetz verstoßen können, auch wenn sie für sich betrachtet jeweils als verfassungsgemäß einzustufen seien. Es sei die Situation zu vermeiden, dass beinahe jeder Teilbereich des menschlichen Lebens überwacht werde.[900]

Damit muss in der Prüfung der Verhältnismäßigkeit einer die Grundrechte beschränkenden Überwachungsmaßnahme die Argumentation zulässig sein, dass die zu überprüfende Maßnahme den Eintritt ebendieser Totalüberwachung faktisch wahrscheinlicher werden

---

[895] Der Bezeichnung „Überwachungs-Gesamtrechnung“ geht zurück auf *Roßnagel*, NJW 2010, 1238.

[896] Diese Gefahr wurde bezüglich Netzsperren in Deutschland in erster Linie im Kontext mit der Einführung des Zugangserschwerungsgesetzes diskutiert, allerdings weniger auf rechtswissenschaftlicher als auf zivilgesellschaftlicher Ebene. Vgl. zu den Stimmen der damaligen Diskussion m.w.N. *Heliosch*, Sperrmaßnahmen im Internet, S. 246. Im rechtswissenschaftlichen Zusammenhang erwähnen das Problem *Assion*, K&R 2014, 329 (333) und *Marberth-Kubicki*, NJW 2009, 1792 (1796). Insbesondere zur Anpassungsfähigkeit für neue Aufgaben der DPI vgl. *Cooper*, DPI Dance, in: Aspray/Doti, Privacy in America, S. 139 (148 f.); *Werbach*, JTHTL 2005, 59 (93).

[897] Wikipedia (en), Suchwort „Mission creep“, Stand der Bearbeitung: 21.09.2020, abrufbar unter https://en.wikipedia.org/wiki/Mission_creep (zuletzt besucht am 09.10.2021).

[898] Sowohl Kinderpornographie (Zugangserschwerungsgesetz) als auch illegales Online-Glücksspiel (Glücksspielstaatsvertrag, GlStV) waren bereits Gegenstand von Bemühungen, in Deutschland Netzsperren einzurichten. Vgl. *Frey u.a.*, MMR-Beil. 2012, 1 (1).

[899] *Heliosch*, Sperrmaßnahmen im Internet, S. 246 f.

[900] Vgl. BVerfG, Urt. v. 02.03.2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Vorratsdatenspeicherung, BVerfGE 125, 260 (323 f.).

lässt, weil sie die tatsächlichen Kosten der Einführung weiterer Überwachungsmaßnahmen erheblich senkt. Das gilt sowohl für die Kosten der Anschaffung und des Betriebs der notwendigen Infrastruktur, als auch für die Kosten der legislatorischen Durchsetzung, da der zu erwartende öffentliche Widerstand gegen weitere Beschränkungen eines bestimmten Grundrechts der Erfahrung nach sinkt, nachdem sich die Bevölkerung an die erstmalige Beschränkung gewöhnt hat.

5. Ergebnis

Es kann daher an dieser Stelle festgehalten werden, dass alle hier diskutierten Eingriffe in den Datenverkehr zur Durchsetzung des Urheberrechts das Telekommunikationsgeheimnis verletzen, da sie unverhältnismäßig in dessen Schutzbereich eingreifen.

V. Vorbehalt des Gesetzes und Wesentlichkeitstheorie

Ein wichtiger Grundsatz des deutschen Verfassungsrechts ist der Vorbehalt des Gesetzes. Grundrechtseingriffe müssen stets auf einer materiell-gesetzlichen Eingriffsermächtigung beruhen. Handelt es sich bei dem Eingriff um einen nicht unbedeutenden Eingriff in Grundrechte, reicht ein bloß materielles Gesetz als Rechtsgrundlage nicht mehr aus. Erforderlich ist dann nach der sogenannten Wesentlichkeitstheorie ein formelles Gesetz. Danach muss der Gesetzgeber alle für die Grundrechtsentfaltung *wesentlichen* Entscheidungen selbst treffen und darf diese nicht der Verwaltung überlassen.[901]

Daraus folgen zugleich Anforderungen an die Bestimmtheit der Norm. Unbestimmte Rechtsbegriffe etwa sind auch bei wesentlichen Eingriffen in die Grundrechte nicht *per se* unzulässig, wenn die Gerichte sie problemlos weiter konkretisieren können.[902] In komplizierteren Fällen sind zu allgemein gehaltene, generalklauselartige gesetzliche Ermächtigungen jedoch nicht mehr ausreichend. So hat das Bundesverwaltungsgericht wiederholt entschieden, dass ein Eingriff in die Berufsfreiheit gegen den Vorbehalt des Gesetzes verstößt, wenn der Eingriff sich auf die polizeiliche Generalklausel stützt und die Verletzung der öffentlichen Ordnung von einer Abwägung abhängt, deren Ergebnis sich aus einer Abwägung undurchschaubarer, weltanschaulich geprägter unterschiedlicher Interessen ergibt.[903]

Fehlt eine spezialgesetzliche Regelung, sind die Gerichte – insbesondere im Zivilrecht – durchaus dazu berufen, das Recht unter Berücksichtigung der Grundrechte mithilfe der

---

[901] BVerfG, Beschl. v. 21.12.1977, 1 BvL 1/75, 1 BvR 147/75, Sexualkundeunterricht, BVerfGE 47, 46 (55).
[902] *Kämmerer* in: v. Münch/Kunig, Grundgesetz Bd. 1, 7. Aufl. 2021, Art. 12 Rn. 83.
[903] BVerwG, Urt. v. 23.02.1960, I C 240.58, BVerwGE 10, 164 (165 f.); BVerwG, Beschl. v. 24.10.2001, 6 C 3/01, BVerwGE 115, 189 (193 f.).

Generalklauseln fortzubilden.[904] Unzulässig ist der Eingriff in Art. 12 Abs. 1 GG hingegen, wenn sich die Rechtsfortbildung zu richterlicher Rechtsschöpfung auswächst.[905] Bildet ein Gericht das Recht in Form einer Analogie fort und greift damit zugleich in ein Grundrecht ein, ist die Grenze zur Rechtsschöpfung überschritten, wenn der Wille des Gesetzgebers nicht mehr beachtet und durch eine autarke richterliche Abwägung der Interessen ersetzt wird.[906]

Da es sich bei der Datenverkehrsregulierung um einen sehr grundrechtssensiblen Bereich handelt, in dem eine Vielzahl grundgesetzlich geschützter Interessen erheblich beeinträchtigt werden und gegeneinander abzuwägen sind, muss eine Datenverkehrsregulierung daher eine formell-gesetzliche Regelung zur Grundlage haben, die erkennen lässt, dass der Gesetzgeber eine eigene Entscheidung darüber getroffen hat, ob er die Internet Service Provider mit einer Datenverkehrsregulierung beauftragen will.[907] Er kann diese Entscheidung – jedenfalls im Grundsatz – nicht einfach an die Verwaltung oder die Gerichte delegieren, da es sich bei der Entscheidung über das *Ob* der DVR um eine wesentliche Entscheidung auf dem Gebiet der Grundrechte handelt. Der Rückgriff auf eine Generalklausel entspricht in einem solchen Fall nicht den Anforderungen der Wesentlichkeitstheorie, so dass hier eine formell- und spezialgesetzliche Ermächtigungsgrundlage erforderlich ist. Dieser Ansicht war offensichtlich im Jahre 2010 auch der deutsche Gesetzgeber, als er das Zugangserschwerungsgesetz erließ, anstatt die Web-Sperre kinderpornographischer Internet-Angebote über die polizeiliche Generalklausel zu verwirklichen.

Vor diesem Hintergrund gibt die Entscheidung des Bundesgerichtshofs Anlass zur Kritik, eine Datenverkehrsregulierung über das richterrechtliche Institut der Störerhaftung (oder – ggf. alternativ – eine analoge Anwendung des § 7 Abs. 4 TMG)[908] entgegen den

---

[904] BVerfG, Beschl. v. 07.02.1990, 1 BvR 26/84, Handelsvertreter, BVerfGE 81, 242, (255 f.); BVerfG, Beschl. v. 26.06.1991, 1 BvR 779/85, BVerfGE 84, 212 (226 f.); BVerfG, Beschl. v. 08.04.1998, 1 BvR 1773/96, Sozietätsverbot, BVerfGE 98, 49 (59); *Jarass* in: Jarass/Pieroth, Grundgesetz Art. 12 GG Rn. 30a; *Kämmerer* in: v. Münch/Kunig, Grundgesetz Bd. 1, 7. Aufl. 2021, Art. 12 GG Rn. 83.

[905] BVerfG, Beschl. v. 19.12.1962, 1 BvR 163/56, Vorkonstitutionelles Gewohnheitsrecht, BVerfGE 15, 226 (233 f.); BVerfG, Beschl. v. 11.06.1963, 1 BvR 156/63, Rechtsanwaltsausschluss, BVerfGE 16, 214 (218 f); BVerwG, Beschl. v. 28.06.1967, 2 BvR 143/61, Entziehung der Verteidigungsbefugnis, BVerfGE 22, 114 (122); *Scholz* in: Maunz/Dürig, Art. 12 GG Rn. 333; *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 12 GG Rn. 30a.

[906] *Badura*, Staatsrecht, Kap. 3 3 e) (Rn. 60).

[907] Vgl. *Ohly*, ZUM 2015, 308 (314 f.).

[908] Vgl. BGH, Urt. v. 26.07.2018, Rs. I ZR 64/17, Dead Island, BGHZ 219, 276, Rn. 49; vgl. auch oben Kap. 3 II 1 b) (5) (S. 140 ff.).

Bedenken etwa des OLG Hamburg[909] und des OLG Köln[910] zu ermöglichen.[911] Die Störerhaftung ist aufgrund der Schwere der Eingriffe in die Grundrechte hier im Speziellen ungeeignet.[912]

Der BGH umgeht die strengen Anforderungen an den Vorbehalt des Gesetzes nach der Wesentlichkeitstheorie, indem er letztere bei der Anordnung einer DVR aufgrund der zivilrechtlichen Verankerung der Störerhaftung für unanwendbar erklärt: Die Wesentlichkeitstheorie finde lediglich im Über-/Unterordnungsverhältnis zwischen Staat und Bürger Anwendung, nicht hingegen im Zivilrecht, wo die Interessen zweier gleichgeordneter Parteien flexibel über unbestimmte Rechtsbegriffe und Generalklauseln gegeneinander abgewogen werden müssten.[913]

Diesem Argument des BGH muss man entgegenhalten, dass es sich bei der Datenverkehrsregulierung eben gerade nicht um die klassische zivilrechtliche Zwei-Parteien-Konstellation handelt.[914] Denn materiell betroffen von einer DVR sind zudem die Rechte an dem Verfahren gar nicht beteiligter Dritter, eben jene der Nutzer des Internets und die der Access Provider. Im Unterschied zu den Fällen, in denen lediglich Host-Provider über die Störerhaftung in die Pflicht genommen werden (und deren Inanspruchnahme über die Störerhaftung den Anforderungen der Wesentlichkeitstheorie entsprechen dürfte), ist die Betroffenheit von Drittrechten weitaus intensiver. Über die Abwägung dieser Rechte hat daher der Gesetzgeber zu entscheiden. Zwar sollen laut dem BGH auch die Rechte Dritter im Rahmen der Auslegung dessen, was im Einzelfall eine zumutbare Maßnahme sei, berücksichtigt werden.[915] Doch können die betroffenen Dritten im Verfahren zwischen ISP und Rechteinhaber keine eigenen Verfahrensrechte geltend machen. Auch im Vollstreckungsverfahren ist es schwer vorstellbar, wie den betroffenen Dritten gegen die DVR ein effektiver Rechtsschutz möglich sein soll.[916]

---

[909] OLG Hamburg, Urt. v. 21.11.2013, 5 U 68/10, 3dl.am, Rn. 91 (juris).
[910] OLG Köln, Urt. v. 18.07.2014, I-6 U 192/11, 6 U 192/11, Goldesel, Rn. 943 (juris), allerdings beschränkt auf DPI-Filter.
[911] Vgl. BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82; OLG Hamburg, Urt. v. 21.11.2013, 5 U 68/10, 3dl.am.
[912] Zudem ist die Störerhaftung (in ihrer Form als Analogie zu den negatorischen Ansprüchen des Sachenrechts) selbst grundsätzlich kritisch zu sehen, da sie sich an der Grenze autonomer richterlicher Rechtsschöpfung bewegt oder gar über diese Grenze hinausgeht. Dies gilt umso mehr, als die Anwendung der Störerhaftung auf Internet Service Provider noch gar nicht breit diskutiert wurde, als der Gesetzgeber sich dazu entschied, diese nicht selbst zu regeln, sondern deren Fortbildung den Gerichten zu überlassen. Vgl. Entwurf eines Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums, BT-Drs. 16/5046, S. 30; weiterführend: *Neuhaus*, Sekundäre Haftung, S. 113 f.
[913] BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 73 f.
[914] Vgl. dazu bereits oben Kap. 3 II 4 c) (1) (S. 155).
[915] BGH, Urt. v. 26.11.2015, I ZR 174/14, Goldesel, BGHZ 208, 82, Rn. 57; ebenso *Leistner/Grisse*, GRUR 2015, 105 (107); *J. B. Nordemann*, ZUM 2014, 499 (500).
[916] In diesem Sinne auch *Ohly*, ZUM 2015, 308 (318); *Spindler*, GRUR 2014, 826 (833 f.); einschränkend jedoch *ders.*, GRUR 2016, 451 (459); *Assion*, K&R 2014, 329 (334) hält eine Verwaltungsbehörde für besser für diese Aufgabe geeignet als ein Gericht.

Diese unglückliche Situation entspringt der Tatsache, dass die deutsche Rechtsprechung bislang versucht, die Internet Service Provider in eine zivilrechtliche Intermediärshaftung zu zwingen.[917] Hier versagt jedoch der verfahrenstechnische Aufbau des Zivilprozesses, da er im Wesentlichen für Zwei-Parteien-Konstellationen geschaffen wurde. Die Abwägung der gegenseitigen Interessen im Rahmen unbestimmter Rechtsbegriffe ist im Zivilprozess dann nicht mehr hinreichend grundrechtsschonend, wenn ein Betroffener keine Möglichkeit hat, seine Rechte im Verfahren auch geltend zu machen. Üblicherweise werden solche Konstellationen daher öffentlich-rechtlich gelöst.

Im Grunde handelt es sich bei der Verhinderung massenhafter Urheberrechtsverletzungen um präventive Gefahrenabwehr, also um eine klassische ordnungsrechtliche Situation, in der üblicherweise eine Behörde eine entsprechende Anordnung aufgrund einer gesetzlichen Grundlage unter Berücksichtigung der rechtlich geschützten Interessen aller Beteiligten trifft. Diese Entscheidung kann dann regelmäßig von den durch die Maßnahme betroffenen Parteien auf verwaltungsrechtlichem Wege angefochten werden. Wenn die im Einzelfall zivilrechtlich durchgesetzte Situation aber ebenso (oder besser) öffentlich-rechtlich durchgesetzt werden kann, können nicht die in normalen Fällen weiteren Spielräume für den Privatrechtsgesetzgeber gelten, da sich der Gesetzgeber ansonsten durch die Wahl der institutionellen Form seinen materiellen Verpflichtungen gegenüber dem Bürger entziehen und dessen Grundrechte untergraben könnte.[918]

Die Wesentlichkeitstheorie muss daher auch bei der DVR zur Urheberrechtsdurchsetzung Anwendung finden.[919] Maßnahmen der DVR auf die Störerhaftung zu stützen, ist verfassungswidrig, da ein formelles Gesetz erforderlich ist.

VI. Zitiergebot, Art. 19 Abs. 1 Satz 2 GG

Art. 19 Abs. 1 Satz 2 GG verpflichtet den Gesetzgeber, einem formellen Gesetz, durch das Grundrechte eingeschränkt werden, einen expliziten Hinweis auf die Einschränkung des Grundrechts beizufügen. Die Rechtsprechung des Bundesverfassungsgerichts beschränkt den Anwendungsspielraum des Zitiergebots jedoch auf diejenigen Grundrechte, die durch

---

[917] LG München I, Urteil v. 01.02.2018, 7 O 17752/17 (abrufbar unter http://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-002857), Rn. 29 stellt fest, dass auch nach dem Dritten Änderungsgesetz zum Telemediengesetz § 8 Abs. 1 Satz 2 TMG einer Inanspruchnahme aus der Störerhaftung nicht entgegensteht.

[918] Vgl. zu diesem Komplex bereits oben Kap. 3 II 1 b) (5) (S. 141 ff.).

[919] Deutsche Gerichte sehen sich hier zugegebenermaßen einer unglücklichen Situation gegenüber: Sie stehen unter dem Druck, europarechtliche Vorgaben umsetzen zu müssen, bekommen vom deutschen Gesetzgeber dafür allerdings nicht die notwendigen Mittel in Form von Gesetzen an die Hand. So bleibt der Rechtsprechung nur die Wahl, sich entweder (vermeintlich) in Widerspruch zum EU-Recht zu setzen oder aber mit den beschränkten Mitteln, die ihr zur Verfügung stehen, bestmöglich zu arbeiten. Auch die Novelle zum TMG 2017 hat insoweit nicht geholfen.

einen speziellen, im Grundgesetz ausdrücklich erwähnten Gesetzesvorbehalt eingeschränkt werden können. Außer Betracht müssten hingegen sonstige, weichere Schranken oder Inhaltsbestimmungen bleiben.[920]

Die Berufsfreiheit kann gemäß Art. 12 Abs. 1 Satz 2 GG *„durch Gesetz oder auf Grund eines Gesetzes geregelt werden"*. Bei Art. 12 Abs. 1 Satz 2 handelt es sich nach herrschender Meinung um einen Ausgestaltungsauftrag des Gesetzgebers, nicht hingegen um eine klassische Beschränkungsmöglichkeit. Das Zitiergebot findet daher auf Einschränkungen der Berufsfreiheit keine Anwendung.[921]

Auch Beschränkungen der Informationsfreiheit benötigen nach der Rechtsprechung des Bundesverfassungsgerichts keinen ausdrücklichen Hinweis auf die Einschränkung des Grundrechts im Gesetz. Das BVerfG begründet dies damit, dass Art. 5 Abs. 2 GG keine eigentliche Beschränkung des Art. 5 Abs. 1 GG sei, sondern die allgemeinen Gesetze von vornherein den Schutzbereich der in diesem enthaltenen Grundrechte verengen.[922]

Wird hingegen Art. 10 Abs. 1 GG wie hier eingeschränkt, ist dies einer der seltenen Fälle, in denen das Zitiergebot im Grundsatz tatsächlich Anwendung findet. Das liegt daran, dass das Grundgesetz den Gesetzgeber in Art. 10 Abs. 2 Satz 1 GG ausdrücklich dazu ermächtigt, das Telekommunikationsgeheimnis zu beschränken. Ein Gesetz, aufgrund dessen in den Datenverkehr zur Durchsetzung des Urheberrechts eingegriffen wird, muss folglich das Zitiergebot beachten. [923]

VII. Ergebnis

Deep Packet Inspection zur Durchsetzung des Urheberrechts beim ISP verletzt die Berufsausübungsfreiheit, die Informationsfreiheit sowie das Telekommunikationsgeheimnis. Bei der Berufsausübungsfreiheit steht diese Aussage allerdings unter dem Vorbehalt des jeweils gegenwärtigen Stands der Technik.

Für IP- und DNS-Sperren gilt dies bei einer Einzelbetrachtung der Eingriffe in die verschiedenen betroffenen Grundrechte nur mit Einschränkungen. Isoliert betrachtet verlet-

---

[920] BVerfG, Beschl. v. 04.05.1983, 1 BvL 46/80, 1 BvL 47/80, Prüfingenieur, BVerfGE 64, 72 (79 f.); BVerfG, Urt. v. 27.07.2005, 1 BvR 668/04, Telekommunikationsüberwachung II, BVerfGE 113, 348 (366); zustimmend *Jarass* in: Jarass/Pieroth, Grundgesetz, Art. 19 Rn. 4; *Kerkemeyer* in: v. Münch/Kunig, Grundgesetz Bd. 1, 7. Aufl. 2021, Art. 19 Rn. 34 ff. Kritisch hingegen etwa *Hillgruber* in: Isensee/P. Kirchhof, HStR VIII, § 201 Rn. 45.

[921] BVerfG, Beschl. v. 04.05.1983, 1 BvL 46/80, 1 BvL 47/80, Prüfingenieur, BVerfGE 64, 72 (80 f.).

[922] BVerfG, Beschl. v. 26. Mai 1970, 1 BvR 657/68, Kriegsdienstgegner, BVerfGE 28, 282 (289); *Windthorst* in: Gröpl u.a., Grundgesetz, Art. 19 Rn. 14.

[923] BVerfG, Urt. v. 27.07.2005, 1 BvR 668/04, Telekommunikationsüberwachung II, BVerfGE 113, 348 (366). Die hier relevanten Datenverkehrseingriffe nimmt allerdings *Durner*, ZUM 2010, 833 (836) vom Zitiergebot aus, soweit diese auf zivilrechtliche Anordnungen zurückgehen würden. Art. 19 Abs. 1 Satz 2 GG gelte nur für die staatliche Eingriffsverwaltung. *J. B. Nordemann*, ZUM 2014, 499 (500) stimmt dem zu und ergänzt, dass das Zitiergebot im Zweifel sekundärrechtlich überlagert werde, so dass ein Verstoß folgenlos bliebe.

zen diese „nur“ die Informationsfreiheit und das Telekommunikationsgeheimnis und können verhältnismäßige Eingriffe in Art. 12 Abs. 1 GG darstellen, wenn die Belastungen der Internet Service Provider durch die Netzsperren unterhalb einer für sie wirtschaftlich spürbaren Grenze bleiben.

Zu beachten ist allerdings, dass die in dieser Arbeit vorgenommen isolierte Untersuchung der Verhältnismäßigkeit der Eingriffe in Grundrechte nur ein Hilfsmittel ist, um die Prüfung übersichtlich zu halten. Die eigentlich zu prüfende Frage ist, ob die Grundrechtsbeschränkungen insgesamt in unverhältnismäßiger Weise in Grundrechte eingreifen. Das Ausmaß der Beschränkungen verschiedener Grundrechte durch dieselbe Maßnahme addiert sich auf der Seite der Verhältnismäßigkeitsabwägung, die gegen eine Angemessenheit spricht, während auf der anderen Seite der Nutzen für den verfolgten Zweck konstant bleibt. Anders ausgedrückt: Viele mittelschwere Beschränkungen verschiedener Grundrechte führen genauso zur Unangemessenheit einer Maßnahme wie viele mittelschwere Beeinträchtigungen nur eines einzigen Grundrechts.[924]

Eine nähere Prüfung, wie sich die Schwere der Beschränkungen in der Addition verhält, ist an dieser Stelle jedoch überflüssig, da das Ergebnis von den isolierten Prüfungen vorweg genommen wurde. Jede der hier geprüften technischen Formen der DVR verstößt gegen mindestens zwei Grundrechte. Ein unverhältnismäßiger Eingriff in ein einziges bestimmtes Grundrecht ist jedoch bereits hinreichende Bedingung für die Unverhältnismäßigkeit insgesamt.

Auch bei IP- und DNS-Sperren handelt es sich daher um insgesamt unverhältnismäßige Grundrechtseingriffe, so dass sie mit dem Grundgesetz nicht vereinbar sind.

Zusammenfassung

I. Gesamtergebnis

Hoheitliche Eingriffe in den Datenverkehr zur Durchsetzung des Urheberrechts sind mit dem Grundgesetz nicht vereinbar.

Europarechtlich ist zu differenzieren. Eingriffe unter Anwendung von Deep-Packet-Inspection-Technologien sind nicht mit dem Primärrecht vereinbar. Die primärrechtliche Zulässigkeit von IP- und DNS-Sperren ist hingegen nicht abschließend höchstrichterlich geklärt.

II. Thesen

1. Eingriffe in den Datenverkehr zur Durchsetzung des Urheberrechts finden im rechtlichen Mehrebenensystem zwischen EU- und mitgliedstaatlichem Recht statt. Sowohl

---

[924] Zur Abwägung gegenläufiger Interessen im mehrpoligen Rechtsverhältnis vgl. BVerfG, Beschl. v. 14.03.2006, 1 BvR 2087/03, 1 BvR 2111/03, Geschäfts- und Betriebsgeheimnisse, BVerfGE 115, 205 (232 ff.); *Hillgruber* in: Isensee/P. Kirchhof, HStR IX, § 201 Rn. 77; *Jarass* in: Jarass/Pieroth, Grundgesetz; Vbm. zu Art. 1 Rn. 46a.

europäische als auch mitgliedstaatliche Grundrechte, Grundfreiheiten und rechtsstaatliche Prinzipien müssen bei einer Datenverkehrsregulierung zur Durchsetzung des Urheberrechts beachtet werden.

2. Der EuGH beschränkt sich in seiner Rechtsprechung zur Datenverkehrsregulierung zur Durchsetzung des Urheberrechts auf die Vorgabe eines rechtlichen Rahmens für die Mitgliedstaaten, innerhalb dessen sich diese bei der Ausgestaltung von Datenverkehrseingriffen bewegen können, ohne dass Grundrechte der Charta verletzt werden.
3. Innerhalb dieser „Leitlinien" besitzen die Mitgliedstaaten Gestaltungsspielräume, nicht nur bei der Ausgestaltung der Details einer DVR, sondern auch bei der Ermittlung der Grenzen des im jeweiligen Mitgliedstaat grundrechtlich Zulässigen.
4. DPI-Filter auf Ebene der ISPs sind – jedenfalls soweit sie der Durchsetzung des Urheberrechts dienen – europarechtlich verboten. Dieses Verbot ergibt sich auf primärrechtlicher Ebene aus einer Verletzung der unternehmerischen Freiheit gemäß Art. 16 Charta sowie Beeinträchtigungen jedenfalls des Rechts auf Schutz personenbezogener Daten, Art. 8 Charta, und der Informationsfreiheit, Art. 11 Abs. 1 Charta.
5. Zu weiteren möglicherweise betroffenen Grundrechten lässt sich der EuGH nicht ein.
6. Andere technische Formen des Eingriffs in den Datenverkehr – sprich: IP- und DNS-Sperren – sind hingegen nicht *a priori* unionsrechtswidrig.
7. Der EuGH legt sich umgekehrt auch nicht derart fest, dass solche Maßnahmen mit Europarecht vereinbar sind. Vielmehr stellt der EuGH einige Kriterien auf, die Netzsperren jedenfalls erfüllen müssten, um mit den Grundrechten der Charta vereinbar zu sein. Die Klärung der Vereinbarkeit im Einzelfall bleibt den mitgliedstaatlichen Gerichten überlassen.
8. Der EuGH lässt offen, ob tatsächlich DVR-Maßnahmen existieren, die die von ihm angelegten Kriterien erfüllen.
9. Das zentrale Zulässigkeitskriterium, das der Gerichtshof formuliert, ist die Vermeidung unnötigen Overblockings. Weiterhin müssten die Maßnahmen Mindestanforderungen an schutzniveau-bezogene Effektivität erfüllen; es müsse dem ausführenden Internet Service Provider überlassen werden, selbst zu entscheiden, ob es ihm im Einzelfall zumutbar ist, eine Netzsperre zu errichten, und wenn ja, welche; schließlich müsste den Internet-Nutzern ein effektiver Rechtsbehelf offenstehen, der es ihnen erlauben würde, gegen Verletzungen ihrer Rechte aus Art. 11 Abs. 1 Charta vorzugehen.
10. Dass diese Voraussetzungen durch IP- oder DNS-Sperren erfüllt werden können, wird hier bezweifelt. Sollten die Maßnahmen den vom EuGH aufgestellten Kriterien nicht ensprechen, steht damit zudem auch ein Verstoß der DVR-Maßnahme gegen die Dienstleistungsfreiheit im Raum.
11. Auf nationaler Ebene gilt: Eingriffe in den Datenverkehr zur Urheberrechtsdurchsetzung müssten sich auf ein formelles Parlamentsgesetz als Rechtsgrundlage stützen. Zudem unterliegt die Rechtsgrundlage dem Gebot, den Eingriff in Art. 10 Abs. 1 GG offenzulegen.
12. Eingriffe in den Datenverkehr zur Urheberrechtsdurchsetzung sind allerdings bereits wegen Verletzungen von Grundrechten des Grundgesetzes rechtswidrig.

13. IP- und DNS-Sperren können unter gewissen Voraussetzungen, die insbesondere von den Kosten der Maßnahme im Einzelfall abhängen, mit der Berufsausübungsfreiheit gemäß Art. 12 Abs. 1 GG der Internet Service Provider vereinbar sein.
14. IP- und DNS-Sperren verstoßen gegen die Informationsfreiheit gemäß Art. 5 Abs. Satz 1 Alt. 2 GG und das Telekommunikationsgeheimnis gemäß Art. 10 Abs. 1 GG, da sie in unverhältnismäßiger Weise in deren Schutzbereich eingreifen.
15. Eingriffe in den Datenverkehr zur Urheberrechtsdurchsetzungen unter Anwendung von Deep Packet Inspection stellen jeweils einen unverhältnismäßigen Eingriff in die Berufsausübungsfreiheit, die Informationsfreiheit sowie das Telekommunikationsgeheimnis des Grundgesetzes dar, obwohl sie sehr effektiv dazu verwendet werden können, Urheberrechte zu schützen.
16. Die Unvereinbarkeit von Maßnahmen der Datenverkehrsregulierung zur Urheberrecchtsdurchsetzung besteht bereits bei isolierter Prüfung der einzelnen Grundrechte. Bei additiver Betrachtung der Grundrechtseingriffe sind die Eingriffe erst recht unverhältnismäßig.
17. Die Verletzung der Grundrechte des Grundgesetzes durch eine Anwendung von Deep Packet Inspection befindet sich im Ergebnis im Gleichlauf mit dem durch den EuGH festgestellten Verstoß gegen die Grundrechte der Charta.
18. Insoweit ist ungeklärt, ob die ratio des EuGH zur Unvereinbarkeit von DPI-Filtern mit den Grundrechten der Charta auch dann Bestand haben wird, wenn durch die fortschreitende technische Entwicklung die Kosten der Deep Packet Inspection erheblich sinken werden. Insoweit könnte die Prüfung der Zulässigkeit von DPI-Filtern auch anhand der Grundrechte des Grundgesetzes dennoch erhebliche praktische Bedeutung erlangen.

Literaturverzeichnis

Aceto, Giuseppe/ Dainotti, Alberto/ Donato, Walter de/ Pescape, Antonio,
PortLoad: Taking the Best of Two Worlds in Traffic Classification, in: 2010 INFOCOM – IEEE Conference on Computer Communications Workshops, San Diego, CA, 2010, S. 3–13.

Aguiar, Luis/ Claussen, Jörg/ Peukert , Christian
Online Copyright Enforcement, Consumer Behavior, and Market Structure, Paper presented at The DRUID Society Conference 2015, Rom (Italien), https://ec.europa.eu/jrc/sites/jrcsh/files/JRC93492_Online_Copyright.pdf (zuletzt besucht am 09.10.2021).

Ahrens, Hans-Jürgen,
21 Thesen zur Störerhaftung im UWG und im Recht des Geistigen Eigentums, WRP 2007, S. 1281–1290.

Albers, Marion,
Informationelle Selbstbestimmung, Baden-Baden 2005 (Habil. HU Berlin, 2002).

Assion, Simon,
5 Fragen zum Netzsperrenurteil des EuGH, in: Telemedicus, 26.11.2011, https://tlmd.in/a/2121 (zuletzt besucht am 09.10.2021).

Assion, Simon,
Überwachung und Chilling Effects, in: Überwachung und Recht – Telemedicus Sommerkonferenz 2014, Berlin 2014, S. 31–82.

Assion, Simon,
Access-Provider kann zu Website-Zugangssperrung verpflichtet werden, K&R 2014, S. 329–334.

Assion, Simon,
Chilling Effects: Übersicht über die Rechtsprechung, in: Telemedicus, 07.05.2014, https://tlmd.in/a/2765 (zuletzt besucht am 09.10.2021).

Badach, Anatol/ Hoffmann, Erwin,
Technik der IP-Netze. Internet-Kommunikation in Theorie und Einsatz, 4. Aufl., München 2019.

Badura, Peter,
Staatsrecht: systematische Erläuterung des Grundgesetzes für die Bundesrepublik Deutschland, 7. Aufl., München 2018.

Bamberger, Heinz Georg/ Roth, Herbert/ Hau, Wolfgang/ Poseck, Roman (Hrsg.),
Beck'scher Onlinekommentar BGB, München o. J., Stand: 59. Edition, August 2021. (zit. *Bearbeiter* in: BeckOK BGB)

Baum, Christoph Georg,
Jugendmedienschutz als Staatsaufgabe, Baden-Baden 2007 (Diss. Münster 2007).

Bedner, Mark,
Rechtmäßigkeit der „Deep Packet Inspection“, https://kobra.bibliothek.uni-kassel.de/bitstream/urn:nbn:de:hebis:34-2009113031192/5/BednerDeepPacketInspection.pdf, Kassel 2009 (zuletzt besucht am 09.10.2021).

Berger, Christian,
Jugendschutz im Internet, „Geschlossene Benutzergruppen” nach § JMSTV § 4 Abs. JMSTV § 4 Absatz 2 Satz 2 JMStV: Am Beispiel personalausweiskennziffergestützter Altersverifikationssysteme, MMR 2003, S. 773–778.

Berger, Christian,
Die Neuregelung der Privatkopie in § 53 Abs. 1 UrhG im Spannungsverhältnis von geistigem Eigentum, technischen Schutzmaßnahmen und Informationsfreiheit, ZUM 2004, S. 257–266.

Billmeier, Eva,
Die Düsseldorfer Sperrungsverfügung. Ein Beispiel für verfassungs- und gefahrenabwehrrechtliche Probleme der Inhaltsregulierung in der Informationsgesellschaft, Berlin 2007 (Diss. Regensburg 2006).

Bisges, Marcel,
Ökonomische Analyse des Urheberrechts, ZUM 2014, S. 930–938.

Böckenförde, Thomas,
Die Ermittlung im Netz. Möglichkeiten und Grenzen neuer Erscheinungsformen strafprozessualer Ermittlungstätigkeit, Tübingen 2003 (Diss. Würzburg 2003).

Böckenförde, Thomas,
Auf dem Weg zur elektronischen Privatsphäre. Zugleich Besprechung von BVerfG, Urteil v. 27.2.2008 – „Online-Durchsuchung“, JZ 2008, S. 925–939.

Bormann, Jens/ Böttcher, Leif,
Notare und Beliehene zwischen Grundrechtsträgerschaft und staatlichem Funktionsverhältnis. Ein Beitrag zur Reichweite von Verwaltungsvorschriften, NJW 2011, S. 2758–2761.

Brinkel, Guido,
Filesharing. Verantwortlichkeit in Peer-to-Peer-Tauschplattformen, Tübingen 2006 (Diss. Göttingen 2005).

Brinkel, Guido/ Osthaus, Wolf,
Netzsperren – rote Linie der Verantwortlichkeit von Internet-Zugangsvermittlern, CR 2014, S. 642–650.

Brüggemann, Sebastian,
Urheberrechtsdurchsetzung im Internet – Ausgewählte Probleme des Drittauskunftsanspruchs nach § 101 UrhG, MMR 2013, S. 278–282.

Calliess, Christian/ Ruffert, Matthias (Hrsg.),
EUV/AEUV. Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta; Kommentar, 5. Aufl., München 2016.

Cao, Jin/ Cleveland, William S./ Sun, X.,
The S-Net System for Internet Packet Streams: Strategies for Stream Analysis and System Architecture, J. Comput. Graph. Stat. 2003, S. 865–892.

Cascarano, Niccolò/ Ciminiera, Luigi/ Risso, Fulvio,
Optimizing Deep Packet Inspection for High-Speed Traffic Analysis, J. Netw. Syst. Manag. 2010, S. 7–31.

Cascarano, Niccolo/ Este, Alice/ Gringoli, Francesco/ Risso, Fulvio/ Salgarelli, Luca,
An Experimental Evaluation of the Computational Cost of a DPI Traffic Classifier, in: IEEE Globecom 2009 – 2009 IEEE Global Telecommunications Conference, Honolulu, HI, 2009, S. 1–8.

Clayton, Richard,
The Phorm "Webwise" System, https://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf, 2008 (zuletzt besucht am 09.10.2021).

Cleveland, William S./ Sun, Don X.,
Internet Traffic Data, JASA 2000, S. 979–985.

Columbia Law Review Association (Hrsg.),
The Chilling Effect in Constitutional Law, Columbia Law Review 1969, S. 808–842.

Conraths, Timo/ Peintinger, Stefan,
§§ 7 und 8 TMG Reloaded: Websperren, GRUR-Prax 2017, S. 206–208.

Cooper, Alissa,
Doing the DPI Dance: Assessing the Privacy Impact of Deep Packet Inspection,
in: Aspray, William/Doty, Philip (Hrsg.), Privacy in America: Interdisciplinary Perspectives, Plymouth (UK), Lanham, Maryland (US) 2011, S. 139–166.

Crotti, Manuel/ Dusi, Maurizio/ Gringoli, Francesco/ Salgarelli, Luca,
Traffic Classification Through Simple Statistical Fingerprinting, SIGCOMM Comput. Commun. Rev. 2007, S. 5–16.

Czychowski, Christian,
Auskunftsansprüche gegenüber Internetzugangsprovidern „vor" dem 2. Korb und „nach" der Enforcement-Richtlinie der EU, MMR 2004, S. 514–519.

Czychowski, Christian/ Nordemann, Jan Bernd,
Grenzenloses Internet – entgrenzte Haftung? – Leitlinien für ein Haftungsmodell der Vermittler, GRUR 2013, S. 986–996.

Dainotti, Alberto/ Pescape, Antonio/ Claffy, Kimberly,
Issues and Future Directions in Traffic Classification, IEEE Network 2012, S. 35–40.

Daly, Angela,
The Legality of Deep Packet Inspection, IJCLP, 14 (2011), S. 1–12.
Danaher, Brett/ Smith, Michael D.,
Gone in 60 Seconds: The Impact of the Megaupload Shutdown on Movie Sales, IJIO 2014, S. 1–8.

Däubler, Wolfgang/ Klebe, Thomas/ Wedde, Peter/ Weichert, Thilo,
Bundesdatenschutzgesetz: Kompaktkommentar zum BDSG, 5. Aufl., Frankfurt am Main 2016.

David P. Reed,
What Your Broadband Provider Knows About Your Webuse: Deep Packet Inspection and Communications Laws and Policies, 110. Kongress (US), (Hearing) 2. Sitzung, Washington 2008, https://www.govinfo.gov/content/pkg/CHRG-110hhrg58071/html/CHRG-110hhrg58071.htm, S. 61–84 (zuletzt besucht am 09.10.2021).

Degen, Thomas A.,
Freiwillige Selbstkontrolle der Access-Provider, Stuttgart 2007 (Diss. Tübingen 2007).

Degenhart, Christoph,
Verfassungsfragen der Internet-Kommunikation, CR 2011, S. 231–237.

Determann, Lothar,
Kommunikationsfreiheit im Internet. Freiheitsrechte und gesetzliche Beschränkungen, Baden-Baden 1999 (Habil. FU Berlin 1999).

Di Fabio, Udo,
Privatisierung und Staatsvorbehalt, JZ 1999, S. 585–592.

Dreger, Holger/ Feldmann, Anja/ Mai, Michael/ Paxson, Vern/ Sommer, Robin,
Dynamic Application-layer Protocol Analysis for Network Intrusion Detection, in: Proceedings of the 15th Conference on USENIX Security Symposium – Volume 15, Article 18, Vancouver, B.C., 2006, S. 257–272.

Dreier, Horst (Hrsg.),
Grundgesetz: Kommentar, Bd. 1–3,
- Band 1: Präambel, Artikel 1–19, 3. Aufl., Tübingen 2013.

Dreier, Thomas/ Schulze, Gernot (Hrsg.),
Urheberrechtsgesetz: Urheberrechtswahrnehmungsgesetz, Kunsturhebergesetz: Kommentar, 6. Aufl., München 2018.

Durner, Wolfgang,
Fernmeldegeheimnis und informationelle Selbstbestimmung als Schranken urheberrechtlicher Sperrverfügungen im Internet, ZUM 2010, S. 833–846.

Dustmann, Andreas,
Die privilegierten Provider: Haftungseinschränkungen im Internet aus urheberrechtlicher Sicht, Baden-Baden 2001 (Diss. Kiel 2001).

Eckhardt, Jens,
IP-Adresse als personenbezogenes Datum – neues Öl ins Feuer, CR 2011, S. 339–344.

Ehlers, Dirk,
Die Weiterentwicklung des Staatshaftungsrechts durch das europäische Gemeinschaftsrecht, JZ 1996, S. 776–783.

Eichin, M.W./ Rochlis, J.A.,
With microscope and tweezers: an analysis of the Internet virus of November 1988, in: Proceedings – 1989 IEEE Symposium on Security and Privacy, Oakland, CA, 1989, S. 326–343.

Engels, Stefan/ Jürgens, Uwe/ Fritzsche, Saskia,
Die Entwicklung des Telemedienrechts im Jahr 2006, K&R 2007, S. 57–68.

Epping, Volker/ Hillgruber, Christian (Hrsg.),
Beck'scher Online-Kommentar | Grundgesetz, München o. J., Stand: 48. Edition, August 2021.

Epping, Volker,
Grundrechte, 9. Aufl., Berlin/Heidelberg 2021.

Faber, Tim,
Jugendschutz im Internet. Klassische und neue staatliche Regulierungsansätze zum Jugendmedienschutz im Internet, Berlin 2005 (Diss. Erlangen-Nürnberg 2004).

Fetzer, Thomas/ Scherer, Joachim/ Graulich, Kurt (Hrsg.),
TKG: Telekommunikationsgesetz: Kommentar, 3. Aufl., Berlin 2021.

Fezer, Karl-Heinz/ Büscher, Wolfgang/ Obergfell, Eva Inés (Hrsg.),
Lauterkeitsrecht. Kommentar zum Gesetz gegen den unlauteren Wettbewerb (UWG),
- Band 1: Internationales Lauterkeitsrecht, Lauterkeitsrechtliche Spezialthemen, Geschichte – Systematik – Grundlagen, §§ 1 bis 3 UWG, 3. Aufl., München 2016.

Finger, Manuela/ Conrath, Timo,
Anmerkung zu einer Entscheidung des BGH, Urteil vom 26.11.2015 (I ZR 174/14) – Zur Haftung eines Access-Providers, MMR 2016, S. 186–188.

Fowler, Geoffrey A./ Barrett, Devlin/ Schechner, Sam,
U.S. Shuts Offshore File-Share „Locker", in: Wall Street Journal online, 2012, https://www.wsj.com/articles/SB10001424052970204616504577171060611948408 (zuletzt besucht am 09.10.2021).

Frenz, Walter,
Handbuch Europarecht. Gesamtwerk in 6 Bänden.
- Band 4: Europäische Grundrechte, Berlin; New York 2009.
(zit. *Frenz*, Handbuch Europarecht, Bd. 4)

Frenz, Walter,
Europarecht, 2. Aufl., Berlin 2016.
(zit. *Frenz*, Europarecht)

Frey, Dieter/ Rudolph, Matthias,
Haftungsregime für Host- und Access-Provider im Bereich der Telemedien: Rechtsgutachten im Auftrag des Bundesverband Digitale Wirtschaft (BVDW) e.V., Norderstedt 2010.

Frey, Dieter/ Rudolph, Matthias/ Oster, Jan,
Internetsperren und der Schutz der Kommunikation im Internet: Am Beispiel behördlicher und gerichtlicher Sperrungsverfügungen im Bereich des Glücksspiel- und Urheberrechts, MMR-Beil. 2012, S. 1–26.

Gabriel, Ulrich/ Albrecht, Stefanie,
Filesharing-Dienste, Grundrechte und (k)eine Lösung?, ZUM 2010, S. 392–397.

Geppert, Martin/ Schütz, Raimund (Hrsg.),
Beck'scher TKG-Kommentar, 4. Aufl., München 2013.

Gercke, Marco,
Anm. zu LG Hamburg, 2005-12-02, 324 O 721/05, MMR 2006, S. 493–494.

Gerlach, Carsten,
Personenbezug von IP-Adressen, CR 2013, S. 478–484.

Germann, Michael,
Gefahrenabwehr und Strafverfolgung im Internet, Berlin 2000 (Diss. Erlangen-Nürnberg 1999).

Gersdorf, Hubertus,
Privatisierung öffentlicher Aufgaben – Gestaltungsmöglichkeiten, Grenzen, Regelungsbedarf, JZ 2008, S. 831–840.

Gersdorf, Hubertus/ Paal, Boris (Hrsg.),
Beck'scher Onlinekommentar Informations- und Medienrecht, München o. J., Stand: 33. Edition, August 2021.

Gesmann-Nuissl, Dagmar/ Wünsche, Kai,
Neue Ansätze zur Bekämpfung der Internetpiraterie – ein Blick über die Grenzen, GRUR Int. 2012, S. 225–234.

Gola, Peter/ Schomerus, Rudolf (Hrsg.),
BDSG: Bundesdatenschutzgesetz: Kommentar, 12. Aufl., München 2015.

Görisch, Christoph,
Netzneutralität – ein Grundsatz des europäischen Regulierungsrechts?, EuZW 2012, S. 494–499.

Grabitz, Eberhard/ Hilf, Meinhard/ Nettesheim, Martin (Hrsg.), Das Recht der Europäischen Union: Grundwerk zur Fortsetzung, Loseblattsammlung, München o. J., Stand: 70. Ergänzungslieferung, Mai 2020.

Greiner, Arved, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, 2001 (Diss. Freiburg 2001).
(zit. *Greiner*, Gefahrenabwehr)

Greiner, Arved, Sperrungsverfügungen als Mittel der Gefahrenabwehr im Internet, CR 2002, S. 620–623.
(zit. *Greiner*, CR 2002)

Grochtmann, Ansgar,
Art. 14 GG – Rechtsfragen der Eigentumsdogmatik, Münster 2000.

Groeben, Hans von der/ Schwarze, Jürgen/ Hatje, Armin (Hrsg.),
Europäisches Unionsrecht: Vertrag über die Europäische Union – Vertrag über die Arbeitsweise der Europäischen Union – Charta der Grundrechte der Europäischen Union.
- Band 1: Europäisches Unionsrecht. 1, Art. 1 bis 55 EUV, Art. 1 bis 54 GRC, Art. 1 bis 66 AEUV, 7. Aufl., Baden-Baden 2015.

Gröpl, Christoph/ Windthorst, Kay/ Coelln, Christian von,
Grundgesetz: Studienkommentar, 4. Aufl., München 2020.

Grzeszick, Bernd,
Geistiges Eigentum und Art. 14 GG, ZUM 2007, S. 344–353.

Gudermann, Anne,
Online-Durchsuchung im Lichte des Verfassungsrechts: die Zulässigkeit eines informationstechnologischen Instruments moderner Sicherheitspolitik, Hamburg 2010 (Diss. Münster 2009).

Hahn, Robert W./ Wallsten, Scott,
The Economics of Net Neutrality, The Economists' Voice vol. 3 (2006),
https://doi.org/10.2202/1553-3832.1194 (zuletzt besucht am 09.10.2021).

Haltern, Ulrich R.,
Europarecht: Dogmatik im Kontext.
- Band II: Rule of Law – Verbunddogmatik – Grundrechte, 3. Aufl., Tübingen 2017.

Harald Frey,
Massenabmahnungen und Social Norm Backlash im Urheberrecht, ZUM 2014, S. 554–558.

Haratsch, Andreas/ Koenig, Christian/ Pechstein, Matthias/ Fuchs, Tobias,
Europarecht, 12. Aufl., Tübingen 2020.

Härting, Niko,
Internetrecht, 6. Aufl., Köln 2017.

Hawellek, Christian,
EuGH: IP-Adressen sind personenbezogene Daten, ZD-Aktuell 2011, S. 129–131.

Heckmann, Dirk/ Paschke, Anna (Hrsg.),
Internetrecht, 7. Aufl., Saarbrücken 2021.

Heidrich, Joerg/ Heymann, Britta,
Die Büchse der Pandora erneut geöffnet: Der BGH und Websperren – Eine kritische Analyse der Rechtsprechung zu Internetsperren durch Access-Provider, MMR 2016, S. 370–376.

Heidrich, Joerg/ Koch, Michael,
Die Nutzer im Netz zwischen Einfluss und Ohnmacht. Macht im Netz V: Rechtspolitik und politische Meinungsbildung durch Social-Media-Kanäle und Internet, MMR 2020, S. 581–586.

Heidrich, Joerg/ Wegener, Christoph,
Datenschutzrechtliche Aspekte bei der Weitergabe von IP-Adressen, DuD 2010, S. 172–177.

Heliosch, Alexandra,
Verfassungsrechtliche Anforderungen an Sperrmaßnahmen von kinderpornographischen Inhalten im Internet, Göttingen 2012. (Diss. Göttingen 2011)

Herdegen, Matthias,
Europarecht, 22. Aufl., München 2020.

Hetmank, Sven,
Internetrecht. Grundlagen, Streitfragen, aktuelle Entwicklungen, Wiesbaden 2016.

Heuner, Lena,
Sperrung des Zugangs zu kinderpornografischen Seiten im Internet, in: Taeger, Jürgen/Wiebe, Andreas (Hrsg.), Inside the Cloud – Neue Herausforderungen für das Informationsrecht: Tagungsband Herbstakademie 2009, Edewecht 2009, S. 107–126.

Hjelmvik, Erik/ John, Wolfgang,
Breaking and Improving Protocol Obfuscation, Department of Computer Science and Engineering, Chalmers University of Technology, Technical Report No. 2010-05, 2010, https://www.iis.se/docs/hjelmvik_breaking.pdf (zuletzt besucht am 09.10.2021).

Hobe, Stephan/ Fremuth, Michael Lysander,
Europarecht, 10. Aufl., München 2020.

Hoeren, Thomas,
Anm. zu LG Hamburg, 2005-12-02, 324 O 721/05, EWiR 2006, S. 651–652.

Hoeren, Thomas/ Sieber, Ulrich/ Holznagel, Bernd (Hrsg.),
Handbuch Multimedia-Recht: Rechtsfragen des elektronischen Geschäftsverkehrs, Loseblattsammlung, München o. J., Stand: 56. Ergänzungslieferung, Mai 2021.

Hoffmann, Christian (Hrsg.),
Die digitale Dimension der Grundrechte. Das Grundgesetz im digitalen Zeitalter, Baden-Baden 2015.

Höfinger, Frank Michael,
Access-Provider haften weiterhin als Störer auf Sperrung von Informationen – Anmerkung zu LG München I, Urteil vom 1.2.2018 – Aktenzeichen 7 O 17752/17, ZUM 2018, S. 382–386.

Hofmann, Franz,
Störerhaftung von Access-Providern für Urheberrechtsverletzungen Dritter, NJW 2016, S. 769–771.

Hogendorn, Christiaan,
Broadband Internet: net neutrality versus open access, IEEP 2007, S. 185–208.

Hohmann-Dennhardt, Christine,
Freiräume – Zum Schutz der Privatheit, NJW 2006, S. 545–549.

Höhne, Focke,
Der (Nicht-)Vollzug des Zugangserschwerungsgesetzes – Rechtliche Problemstellungen und Ausblick, jurisPR-ITR 24/2010, 2010, https://www.juris.de/perma?d=jpr-NLI-TADG000310 (zuletzt besucht am 09.10.2021).

Holznagel, Bernd,
Verantwortlichkeiten im Internet und Free Speech am Beispiel der Haftung für illegale und jugendgefährdende Inhalte, ZUM 2000, S. 1007–1029.

Hömig, Dieter,
Neues Grundrecht, neue Fragen? Zum Urteil des BVerfG zur Online-Durchsuchung, JURA 2009, S. 207–213.

Hopf, Kristina,
Rechtliche Grundlagen des Jugendmedienschutz-Staatsvertrags und die Verantwortlichkeit von Chatbetreibern, ZUM 2008, 207–217.

Hufen, Friedhelm,
Staatsrecht II: Grundrechte, 8. Aufl., München 2020.

Ingham, Kenneth/ Forrest, Stephanie,
A history and survey of network firewalls, in: The University of New Mexico Computer Science Department Technical Report 2002-37, 2002, Albuquerque (NM), https://iar.cs.unm.edu/~treport/tr/02-12/firewall.pdf, (zuletzt besucht am 09.10.2021).

Ipsen, Jörn,
Staatsrecht II. Grundrechte, 24. Aufl., München 2021.

Isensee, Josef/ Kirchhof, Paul (Hrsg.),
Handbuch des Staatsrechts der Bundesrepublik Deutschland:
- Band IV: Aufgaben des Staates, 3. Aufl., Heidelberg 2006.
- Band VI: Bundesstaat, 3. Aufl., Heidelberg 2008.
- Band VII: Freiheitsrechte, 3. Aufl., Heidelberg 2009.
- Band VIII: Grundrechte: Wirtschaft, Verfahren, Gleichheit., 3. Aufl., Heidelberg 2010.
- Band IX: Allgemeine Grundrechtslehren, 3. Aufl., Heidelberg 2011.
- Band XI: Internationale Bezüge, 3. Aufl., Heidelberg 2013.

Jani, Michael,
Die partielle verwaltungsrechtliche Inpflichtnahme Privater zu Handlungs- und Leistungspflicht. Eine Untersuchung von Aufgabenüberbürdungen im Kommunalrecht unter besonderer Berücksichtigung der Rechtslage in Schleswig-Holstein, Pfaffenweiler 1992 (Diss. Kiel 1992).

Janssen, Dirk Thorsten,
Die Regulierung abweichenden Verhaltens im Internet. Eine Untersuchung verschiedener Regulierungsansätze unter besonderer Berücksichtigung der deutschen Rechtsordnung, Baden-Baden 2003 (Diss. Giessen 2003).

Jarass, Hans D.,
Charta der Grundrechte der Europäischen Union: unter Einbeziehung der vom EuGH entwickelten Grundrechte, der Grundrechtsregelungen der Verträge und der EMRK: Kommentar, 4. Aufl., München 2021.

Jarass, Hans D./ Pieroth, Bodo,
Grundgesetz für die Bundesrepublik Deutschland, 16. Aufl., München 2020.

Kahl, Jonas,
Die verfassungsrechtliche Zulässigkeit von Internet-Sperren, SächsVBl 2010, S. 180–191.

Kahl, Wolfgang/ Waldhoff, Christian/ Walter, Christian (Hrsg.),
Bonner Kommentar zum Grundgesetz, Loseblattsammlung, Heidelberg o. J., Stand: 207. Ergänzungslieferung, September 2020.

Kaltenborn, Markus/ Schnapp, Friedrich,
Grundrechtsbindung nichtstaatlicher Institutionen, JuS 2000, S. 937–943.

Kaminski, Simon,
Wo lauscht der BND?, in: Augsburger Allgemeine online, 06.05.2015, https://www.augsburger-allgemeine.de/politik/Wo-lauscht-der-BND-id33960927.html (zuletzt besucht am 09.10.2021).

Kastl, Graziana,
Filter – Fluch oder Segen?, GRUR 2016, S. 671–678.

Kingreen, Thorsten,
Die Struktur der Grundfreiheiten des Europäischen Gemeinschaftsrechts, Berlin 1999 (Diss. Münster 1998).

Kingreen, Thorsten/ Poscher, Ralf,
Grundrechte Staatsrecht II, 36. Aufl., Heidelberg 2019.

Kirchhof, Ferdinand,
Grundrechtsschutz durch europäische und nationale Gerichte, NJW 2011, S. 3681–3686.

Kirchhof, Paul,
Der verfassungsrechtliche Gehalt des geistigen Eigentums, in: Festschrift für Wolfgang Zeidler, Berlin, New York 1987, S. 1639–1662.

Kirchner, Christian,
Innovationsschutz und Investitionsschutz für immaterielle Güter, GRUR Int. 2004, S. 603–607.

Klass, Nadine,
FILTER(N) oder nicht? Der Einsatz von Filtertechnologien im Urheber- und Medienrecht. Einleitung zum gleichnamigen Symposium des Instituts für Urheber- und Medienrecht am 7.2.2020 in München, ZUM 2020, S. 353–355.

Kluth, Winfried,
Das Grundrecht der Berufsfreiheit – Art. 12 I GG, JURA 2001, S. 371–376.

Koch, Frank A.,
Rechtsfragen der Nutzung elektronischer Kommunikationsdienste, BB 1996, S. 2049–2058.

Köhnen, C./ Überall, C./ Adamsky, F./ Rakočević, V./ Rajarajan, M./ Jäger, R.,
Enhancements to Statistical Protocol IDentification (SPID) for Self-Organised QoS in LANs, in: 2010 Proceedings of 19th International Conference on Computer Communications and Networks (ICCCN), 2010, S. 1–6.

Koreng, Ansgar,
Zensur im Internet: der verfassungsrechtliche Schutz der digitalen Massenkommunikation, Baden-Baden 2010 (Diss. Leipzig 2010).

Kreutzer, Till,
Das Modell des deutschen Urheberrechts und Regelungsalternativen. Konzeptionelle Überlegungen zu Werkbegriff, Zuordnung, Umfang und Dauer des Urheberrechts als Reaktion auf den urheberrechtlichen Funktionswandel, Baden-Baden 2008 (Diss. Hamburg 2007).

Kröger, Detlef,
Informationsfreiheit und Urheberrecht, München 2002 (Diss. Chemnitz 2000/2001).

Królikowski, Agata,
Packet Inspection in Zeiten von Big Data, in: Überwachung und Recht – Tagungsband zur Telemedicus Sommerkonferenz 2014, Berlin 2014, S. 141–164.

Kropp, Jonathan,
Die Haftung von Host- und Access-Providern bei Urheberrechtsverletzungen, Frankfurt am Main 2012 (Diss. HU Berlin 2012).

Krüger, Stefan/ Maucher, Svenja-Ariane,
Ist die IP-Adresse wirklich ein personenbezogenes Datum? Ein falscher Trend mit großen Auswirkungen auf die Praxis, MMR 2011, S. 433–439.

Ladeur, Karl-Heinz,
Noch einmal – Die Meinungsfreiheit zwischen Individual- und Allgemeininteresse: Zugleich eine Anmerkung zum Beschluss des BVerfG vom 18-02-2010 (Az. 1 BvR 2477/08), AfP 2010, S. 224–225.

Lehmann, Matthias/ Rein, Christian,
eBay: Haftung des globalen Basars zwischen Gemeinschaftsrecht und BGH, CR 2008, S. 97–103.

Leible, Stefan/ Sosnitza, Olaf,
Haftung von Internetauktionshäusern – reloaded, NJW 2007, S. 3324–3326.

Leistner, Matthias,
Störerhaftung und mittelbare Schutzrechtsverletzung, GRUR-Beil. 2010, S. 1–32.

Leistner, Matthias,
Grundlagen und Perspektiven der Haftung für Urheberrechtsverletzungen im Internet, ZUM 2012, S. 722–740.

Leistner, Matthias/ Grisse, Karina,
Sperrverfügungen gegen Access-Provider im Rahmen der Störerhaftung (Teil 1), GRUR 2015, S. 19–27.

Leistner, Matthias/ Grisse, Karina,
Sperrverfügungen gegen Access-Provider im Rahmen der Störerhaftung (Teil 2), GRUR 2015, S. 105–115.

Lenz, Carl-Otto/ Borchardt, Klaus-Dieter/ Bitterlich, Joachim (Hrsg.),
EU-Verträge Kommentar: EUV – AEUV – GRCh, 6. Aufl., Köln 2013.

Lessig, Lawrence,
Code : version 2.0, 2. Aufl., New York 2006.

Lessig, Lawrence,
Remix: Making Art and Commerce Thrive in the Hybrid Economy, London 2008.

Lettl, Tobias,
BB-Rechtsprechungsreport zum Wettbewerbsrecht 2014/2015, BB 2015, S. 2371–2378.

Leutheuser-Schnarrenberger, Sabine,
Vorratsdatenspeicherung – Ein vorprogrammierter Verfassungskonflikt, ZRP 2007, S. 9–13.

Liesching, Marc,
„Sicherstellung" des Erwachsenenzugangs bei pornografischen und sonst jugendgefährdenden Telemedien, MMR 2008, S. 802–807.

Loewenheim, Ulrich/ Leistner, Matthias/ Ohly, Ansgar (Hrsg.),
Urheberrecht. UrhG – KUG – VGG. Kommentar, 6. Aufl., München 2020.

Lücke, Jörg,
Zur Europarechtskonformität der Deutschen-Grundrechte. Europarechtskonforme Auslegung oder Rechtsfortbildung der Grundrechte?, EuR 2001, S. 112–118.

Ludwig, Thomas Claus,
Zum Verhältnis zwischen Grundrechtecharta und allgemeinen Grundsätzen – die Binnenstruktur des Art. EUV Artikel 6 EUV n. F., EuR 2011, S. 715–735.

Maennel, Frithjof,
Elektronischer Geschäftsverkehr ohne Grenzen – der Richtlinienvorschlag der Europäischen Kommission, MMR 1999, S. 187–192.

Mangoldt, Hermann von (Begr.)/ Friedrich, Klein (fortgef.)/ Starck, Christian (Hrsg.),
Kommentar zum Grundgesetz.
- Bd. 1: Präambel, Artikel 1 bis 19, 7. Aufl., München 2018.

Mantz, Reto,
Die (neue) Haftung des (WLAN-)Access-Providers nach § 8 TMG, GRUR 2017, S. 969–977.

Marberth-Kubicki, Annette,
Der Beginn der Internet-Zensur, NJW 2009, S. 1792–1796.

Marley, Jochen,
Anmerkung zu EuGH, 27.3.2014 – C-314/12 – UPC Telekabel/Constantin Film ua [kino.to], GRUR 2014, S. 472–473.

Maunz, Theodor/ Dürig, Günter (Begr.),
Grundgesetz Kommentar, Loseblattsammlung, München o. J., Stand: 94. Ergänzungslieferung, Januar 2021.

Maurer, Hartmut/ Waldhoff, Christian,
Allgemeines Verwaltungsrecht, 20. Aufl., München 2020.

Meinel, Christoph/ Sack, Harald,
Internetworking. Technische Grundlagen und Anwendungen, Berlin/Heidelberg 2012.

Merten, Detlef/ Papier, Hans-Jürgen (Hrsg.),
Handbuch der Grundrechte in Deutschland und Europa.
- Band II: Grundrechte in Deutschland – Allgemeine Lehren I, Heidelberg/Zürich/St. Gallen 2006.
- Band IV: Grundrechte in Deutschland – Einzelgrundrechte I, Heidelberg/Zürich/St. Gallen 2011.
- Band VI/1: Europäische Grundrechte I, Heidelberg/Zürich/St. Gallen 2010.
- Band VI/II: Europäische Grundrechte II – Universelle Menschenrechte, Heidelberg/Zürich/St. Gallen 2009.

Meyer, Jürgen/ Hölscheidt, Sven (Hrsg.),
Charta der Grundrechte der Europäischen Union, 5. Aufl., Baden-Baden 2019.

Meyerdierks, Per,
Sind IP-Adressen personenbezogene Daten?, MMR 2009, S. 8–13.

Meyer-Ladewig, Jens/ Nettesheim, Martin/ Raumer, Stefan von (Hrsg.),
EMRK Europäische Menschenrechtskonvention, 4. Aufl., Baden-Baden 2017.

Michael, Lothar,
Die drei Argumentationsstrukturen des Grundsatzes der Verhältnismäßigkeit – Zur Dogmatik des Über- und Untermaßverbotes und der Gleichheitssätze, JuS 2001, S. 148–155.

Möller, Simon,
Anmerkung zu LG Köln, Urteil vom 31. 8. 2011 – Az. 28 O 362/10, CR 2011, S. 733–735.

Moore, Andrew W./ Papagiannaki, Konstantina,
Toward the Accurate Identification of Network Applications, in: Dovrolis, Constantinos (Hrsg.), Passive and Active Network Measurement, Boston (US) 2005, S. 41–54.

Moos, Flemming/ Gosche, Anna,
Anmerkung zum Urteil des LG Hamburg vom 12.11.2008 (308 O 548/08) – keine Haftung des Access-Providers für Urheberrechtsverletzung seines Kunden, K&R 2009, S. 275–277.

Müller, Willem,
Die unmittelbare Inanspruchnahme des Access-Providers. Aktuelle Voraussetzungen einer Internetsperre bei Urheberrechtsverletzungen, MMR 2019, 426–431.

Münch, Ingo von (Begr.)/ Kunig, Philip (Hrsg.),
Grundgesetz-Kommentar.
- Band 1: Präambel bis Art. 69, 6. Aufl., München 2012
- Band 1: Präambel bis Art. 69, 7. Aufl., München 2021

Nazari-Khanachayi, Arian,
Access-Provider als urheberrechtliche Schnittstelle im Internet, GRUR 2015, S. 115–122.

Nazari-Khanachayi, Arian,
Zulässigkeit von Zugangserschwerungsverfügungen gegen Access-Provider bei (drohenden) Urheberrechtsverletzungen. Eine Untersuchung des europäischen Rechts unter rechtsvergleichender Betrachtung des deutschen, österreichischen und englischen Rechts, Baden-Baden 2015 (Magister-Arbeit, Frankfurt am Main 2014).

Neuhaus, Stephan,
Sekundäre Haftung im Lauterkeits- und Immaterialgüterrecht. Dogmatische Grundlagen und Leitlinien zur Ermittlung von Prüfungspflichten, Tübingen 2011 (Diss. Bayreuth 2010).

Nicolai, Michael,
Rechtssicherheit für WLAN-Anbieter: Neuer Versuch im 3. TMGÄndG, ZUM 2018, S. 33–43.

Nietsch, Thomas,
Anonymität und die Durchsetzung urheberrechtlicher Ansprüche im Internet, Tübingen 2014 (Diss. Göttingen 2013).

Nolte, Georg/ Wimmers, Jörg,
Wer stört? Gedanken zur Haftung von Intermediären im Internet – von praktischer Konkordanz, richtigen Anreizen und offenen Fragen, GRUR 2014, S. 16–27.

Nordemann, Axel/ Nordemann, Jan Bernd/ Czychowski, Christian (Hrsg.),
Urheberrecht: Kommentar zum Urheberrechtsgesetz, Verlagsgesetz, Urheberrechtswahrnehmungsgesetz, 12. Aufl., Stuttgart 2018.
(zit. *Bearbeiter* in: Fromm/Nordemann, Urheberrecht)

Nordemann, Jan Bernd,
Haftung von Providern im Urheberrecht: Der aktuelle Stand nach dem EuGH-Urteil v. 12. 7. 2011 – EUGH 12.07.2011 Aktenzeichen C-324/09 – L'Oréal/eBay, GRUR 2011, S. 977–981.

Nordemann, Jan Bernd,
Anmerkung zu EuGH, Urteil vom 27. März 2014 – EUGH Aktenzeichen C31412 C-314/12 – UPC Telekabel Wien GmbH/Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH (»Kino.to«), ZUM 2014, S. 499–501.

Nordemann, Jan Bernd/ Wolters, Olaf,
Schwerwiegende Regeländerungen bei urheberrechtlichen Abmahnungen: Neufassung des § 97a UrhG, ZUM 2014, S. 25–31.

Norrie, Cheryl,
Kim Dotcom wehrt sich gegen Auslieferung, in: SPIEGEL ONLINE, https://www.spiegel.de/netzwelt/web/anhoerung-in-neuseeland-dotcom-wehrt-sich-gegen-auslieferung-a-1109396.html, 29.08.2016 (zuletzt besucht am 09.10.2021).

Nowak, Carsten/ Schnitzler, Jörg,
Erweiterte Rechtfertigungsmöglichkeiten für mitgliedstaatliche Beschränkungen der EG-Grundfreiheiten Genereller Rechtsprechungswandel oder Sonderweg im Bereich der sozialen Sicherheit?, EuZW 2000, S. 627–631.

Oermann, Markus/ Staben, Julian,
Mittelbare Grundrechtseingriffe durch Abschreckung? – Zur grundrechtlichen Bewertung polizeilicher „Online-Streifen" und „Online-Ermittlungen" in sozialen Netzwerken, Der Staat 2013, S. 630–661.

Ohly, Ansgar,
Anmerkung zu BGH, Urteil v. 26. 7. 2018 – 1 ZR 64/17 (OLG Düsseldorf), JZ 2019, S. 251–255.

Ohly, Ansgar,
Geistiges Eigentum?, JZ 2003, S. 545–554.

Ohly, Ansgar,
Die Verantwortlichkeit von Intermediären, ZUM 2015, S. 308–318.

Oppermann, Thomas (Begr.)/ Classen, Claus Dieter/ Nettesheim, Martin (Hrsg.),
Europarecht. Ein Studienbuch, 9. Aufl., München 2021.

Pache, Eckhard/ Rösch, Franziska,
Der Vertrag von Lissabon, NVwZ 2008, S. 473–480.

Parsons, Christopher,
Deep Packet Inspection in Perspective: Tracing its lineage and surveillance potentials, Working Paper, 2008, https://qspace.library.queensu.ca/bitstream/handle/1974/1939/WP_Deep_Packet_Inspection_Parsons_Jan_2008.pdf, (zuletzt aufgerufen am 14.10.2020) .

Paulweber, Michael/ Weinand, Armin,
Europäische Wettbewerbspolitik und liberalisierte Märkte, EuZW 2001, S. 232–241.

Pfitzmann, Andreas/ Köpsell, Stefan/ Kriegelstein, Thomas,
Sperrverfügungen gegen Access-Provider. Technisches Gutachten, im Auftrag der KJM, Dresden 2008.

Paulus, Andreas/ Wesche, Steffen,
Urheberrecht und Verfassung, ZGE 2010, S. 385–397.

Posser, Herbert/ Wolff, Heinrich Amadeus (Hrsg.),
Verwaltungsgerichtsordnung: Kommentar, 2. Aufl., München 2014.

Pravemann, Timm,
Art. 17 der Richtlinie zum Urheberrecht im digitalen Binnenmarkt. Eine Analyse der neuen europäischen Haftungsregelung für Diensteanbieter für das Teilen von Online-Inhalten, GRUR 2019, S. 783–788.

Proelss, Alexander/ Daum, Oliver,
Verfassungsrechtliche Grenzen der Routinefernmeldeaufklärung durch den Bundesnachrichtendienst, AöR 2016, S. 373–414.

Read, Darren,
Net neutrality and the EU electronic communications regulatory framework, IJLIT 2012, S. 48–72.

Röhl, Christoph/ Bosch, Andreas,
Musiktauschbörsen im Internet, NJW 2008, S. 1415–1420.

Rohlf, Dietwalt,
Der grundrechtliche Schutz der Privatsphäre. Zugleich ein Beitrag zur Dogmatik des Art. 2 Abs. 1 GG, Berlin 1980 (Diss. Tübingen 1978/79).

Roßnagel, Alexander,
Die „Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung, NJW 2010, S. 1238–1242.

Sachs, Michael (Hrsg.),
Grundgesetz: Kommentar, 9. Aufl., München 2021.

Säcker, Franz Jürgen (Hrsg.),
Berliner Kommentar zum Telekommunikationsgesetz, 3. Aufl., Frankfurt am Main 2013.

Säcker, Franz Jürgen/ Rixecker, Roland/ Oetker, Hartmut/ Limperg, Bettina (Hrsg.),
Münchener Kommentar zum Bürgerlichen Gesetzbuch – Band 7, , 8. Aufl., München 2020.
(zitiert: *Bearbeiter* in: MüKoBGB – Bd. 7)

Saltzer, Jerome H./ Reed, David P./ Clark, David D.,
End-to-End Arguments in System Design, in: Partridge, Craig (Hrsg.), Innovations in Internetworking, Norwood, MA (US) 1988, S. 195–206.
Scheurle, Klaus-Dieter/ Mayen, Thomas (Hrsg.),
Telekommunikationsgesetz: Kommentar, 3. Aufl., München 2018.

Schilling, Aiko,
Präventive staatliche Kontrollmaßnahmen im Internet und ihre Vereinbarkeit mit dem Europarecht, Regensburg 2003 (Diss. Regensburg, 2002/2003).

Schliesky, Utz/ Hoffmann, Christian/ Luch, Anika D./ Schulz, Sönke E./ Borchers, Kim Corinna,
Schutzpflichten und Drittwirkung im Internet. Das Grundgesetz im digitalen Zeitalter, Baden-Baden 2014.
(zit. *Schliesky u.a.*, Drittwirkung im Internet)

Schmidt, Stephan,
Die Rechtmäßigkeit staatlicher Gefahrenabwehrmaßnahmen im Internet unter besonderer Berücksichtigung des Europäischen Gemeinschaftsrechts, Frankfurt am Main u.a. 2006 (Diss. Dresden 2005).

Schmitz, Thomas,
Die Grundrechtecharta als Teil der Verfassung der Europäischen Union, EuR 2004, S. 691–713.

Schnabel, Christoph,
Sperrungsverfügungen gegen Access-Provider. Technische Möglichkeiten und rechtliche Zulässigkeit anhand eines praktischen Beispiels, 2002 (Master-Arbeit Hannover 2002, unveröffentlicht).

Schnabel, Christoph,
Böse Zensur, guter Filter? – Urheberrechtliche Filterpflichten für Access-Provider, MMR 2008, S. 281–286.

Schnabel, Christoph,
„Porn not found" – Die Arcor-Sperre, K&R 2008, S. 26–31.

Schnabel, Christoph,
Das Zugangserschwerungsgesetz – Zum Access-Blocking als ultima ratio des Jugendschutzes, JZ 2009, S. 996–1001.

Schneider, Jochen (Hrsg.),
Handbuch des EDV-Rechts, 5. Aufl., Gotha 2017

Schoch, Friedrich,
Gewährleistungsverwaltung: Stärkung der Privatrechtsgesellschaft?, NVwZ 2008, S. 241–247.

Schoch, Friedrich/ Schneider, Jens-Peter/ Bier, Wolfgang (Hrsg.),
Verwaltungsgerichtsordnung: VwGO, Loseblattsammlung, München o. J., Stand: 38. Ergänzungslieferung, Januar 2020.

Schulze, Reiner/ Janssen, André/ Kadelbach, Stefan (Hrsg.),
Europarecht. Handbuch für die deutsche Rechtspraxis, 4. Aufl., Baden-Baden 2020.

Schwabe, Jürgen,
Die sogenannte Drittwirkung der Grundrechte. Zur Einwirkung der Grundrechte auf den Privatrechtsverkehr, München 1971 (Diss. Marburg 1970).

Schwartzmann, Rolf/ Hentsch, Christian-Henner,
Stufenkonzept gegen Overblocking durch Upload-Filter. Ein erster Vorschlag zur Umsetzung von Art. EU_RL_2019_790 Artikel 17 DSM-RL, MMR 2020, S. 207–213.

Sen, Subhabrata/ Spatscheck, Oliver/ Wang, Dongmei,
Accurate, Scalable In-network Identification of P2P Traffic Using Application Signatures, in: Proceedings of the 13th International Conference on World Wide Web 2004, S. 512–521.

Sesing, Andreas,
Der Sperranspruch nach § 7 IV TMG. Von gesetzgeberischen Kanonen und (anlasslos) verschlüsselnden Spatzen, GRUR 2019, 898–904.

Sieber, Ulrich,
Verantwortlichkeit im Internet. Technische Kontrollmöglichkeiten und multimediarechtliche Regelungen. Zugleich eine Kommentierung von § 5 TDG und § 5 MDStV, München 1999.

Sieber, Ulrich/ Höfinger, Frank Michael,
Drittauskunftsansprüche nach § 101a UrhG gegen Internetprovider zur Verfolgung von Urheberrechtsansprüchen, MMR 2004, S. 575–586.

Sieber, Ulrich/ Nolde, Malaika,
Sperrverfügungen im Internet. Nationale Rechtsdurchsetzung im globalen Cyberspace?, Berlin 2008.

Sievers, Malte,
Der Schutz der Kommunikation im Internet durch Artikel 10 des Grundgesetzes, Baden-Baden 2003 (Diss. Kiel 2002).

Spafford, Eugene H.,
The internet worm incident, in: Ghezzi, C./McDermid, J. A. (Hrsg.), ESEC '89, 1989, S. 446–468.

Soergel, Hans Theodor (Begr.)/ Siebert, Wolfgang/ Spickhoff, Andreas (Hrsg.),
Bürgerliches Gesetzbuch mit Einführungsgesetz und Nebengesetzen.
- BGB Band 12: Schuldrecht 10 §§ 823 – 853 BGB, Produkthaftungsgesetz, Umwelthaftungsgesetz, 13. Aufl., Stuttgart 2005.

Spindler, Gerald,
Haftung für private WLANs im Delikts- und Urheberrecht, CR 2010, S. 592–600.

Spindler, Gerald,
Störerhaftung des Host-Providers bei Persönlichkeitsrechtsverletzungen, CR 2012, S. 176–178.

Spindler, Gerald,
Zivilrechtliche Sperrverfügungen gegen Access Provider nach dem EuGH-Urteil „UPC Telekabel“, GRUR 2014, S. 826–834.

Spindler, Gerald,
Sperrverfügungen gegen Access-Provider – Klarheit aus Karlsruhe?, GRUR 2016, S. 451–460.

Spindler, Gerald,
Der RegE zur Störerhaftung der Provider, insbesondere WLANs – Verschlimmbesserung und Europarechtswidrigkeit, CR 2017, S. 333–335.

Spindler, Gerald,
Haftung ohne Ende?, MMR 2018, S. 48–52.

Spindler, Gerald/ Schuster, Fabian (Hrsg.),
Recht der elektronischen Medien. Kommentar, 4. Aufl., München 2019.

Stadler, Thomas,
Haftung für Informationen im Internet, 2. Aufl., Berlin 2005.

Stadler, Thomas,
Internetsperren: EuGH lässt Provider mit der Verantwortung allein, in: Legal Tribune Online, 27.03.2014, https://www.lto.de/recht/hintergruende/h/eugh-urt-c-314-12-internet-sperren-gerichte/ (zuletzt besucht am 09.10.2021).

Stalla-Bourdillon, Sophie/ Papadaki, Evangelia/ Chown, Tim,
From porn to cybersecurity passing by copyright: How mass surveillance technologies are gaining legitimacy. The case of deep packet inspection technologies, CLSR 2014, S. 670–686.

Staudinger, Julius von (Begr.),
J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch: mit Einführungsgesetz und Nebengesetzen. Buch 2. Recht der Schuldverhältnisse: §§ 823 A-D (Unerlaubte Handlungen 1 – Teilband 1:Rechtsgüter und Rechte; Persönlichkeitsrecht; Gewerbebetrieb), 15. Aufl., Berlin 2017.

Stern, Klaus/ Becker, Florian,
Grundrechte-Kommentar: Die Grundrechte des Grundgesetzes mit ihren europäischen Bezügen, 3. Aufl., Köln 2019.

Streinz, Rudolf,
Europarecht (Schwerpunktbereich), 11. Aufl., Heidelberg 2019.
(zit. *Streinz*, Europarecht)

Streinz, Rudolf (Hrsg.),
EUV/AEUV: Vertrag über die Europäische Union und Vertrag über die Arbeitsweise der Europäischen Union, 3. Aufl., München 2018.
(zit. *Bearbeiter* in: Streinz, EUV/AEUV)

Streinz, Rudolf/ Ohler, Christoph/ Herrmann, Christoph (Hrsg.),
Der Vertrag von Lissabon zur Reform der EU: Einführung mit Synopse; [mit Lissabon-Entscheidung und Begleitgesetz], 3. Aufl., München 2010.

Taeger, Jürgen/ Kremer, Sascha,
Recht im E-Commerce und Internet. Einführung, Frankfurt am Main 2017.

Tanenbaum, Andrew S./ Wetherall, David J.,
Computer Networks, 5. Aufl., Upper Saddle River (NJ, USA) 2010.

Trstenjak, Verica,
Das Verhältnis zwischen Immaterialgüterrecht und Datenschutzrecht in der Informationsgesellschaft im Lichte der Rechtsprechung des Europäischen Gerichtshofs, GRUR Int. 2012, S. 393–402.

Volkmann, Christian,
Verkehrspflichten für Internet-Provider, CR 2008, S. 232–238.

Voßkuhle, Andreas,
Grundwissen – Öffentliches Recht: Der Grundsatz der Verhältnismäßigkeit, JuS 2007, S. 429–430.

Waldenberger, Arthur,
Teledienste, Mediendienste und die "Verantwortlichkeit" ihrer Anbieter, MMR 1998, S. 124–129.

Wandtke, Artur-Axel/ Bullinger, Windried (Hrsg.),
Praxiskommentar Urheberrecht. UrhG, VGG, InsO, UKlaG, KUG, EVtr, InfoSoc-RL, 5. Aufl., München 2019.

Wendt, Rudolf,
Das Recht am eigenen Bild als strafbewehrte Schranke der verfassungsrechtlich geschützten Kommunikationsfreiheiten des Art. 5 Abs. 1 GG, AfP 2004, S. 181–190.

Werbach, Kevin,
Breaking the Ice: Rethinking Telecommunications Law for the Digital Age, JTHTL 2005, S. 59–95.

Wilburg, Walter,
Entwicklung eines beweglichen Systems im bürgerlichen Recht: Rede, gehalten bei der Inaug. als Rector magnificus der Karl-Franzens-Universität in Graz am 22. November 1950, Graz 1950.

Wu, Tim,
Broadband Discrimination, JTHTL 2003, S. 141–179.

Wu, Tim,
Network Neutrality: Competition, Innovation, and Nondiscriminatory Access, 24.04.3006, https://dx.doi.org/10.2139/ssrn.903118 (zuletzt besucht am 09.10.2021).

Wuermeling, Ulrich/ Felixberger, Stefan,
Fernmeldegeheimnis und Datenschutz im Telekommunikationsgesetz, CR 1997, S. 230–238.

Youn, Monica,
The Chilling Effect and the Problem of Private Action, Vanderbilt Law Review 2013, S. 1474–1539.

Ziegenhorn, Gero,
Der Einfluss der EMRK im Recht der EU Grundrechtecharta. Genuin chartarechtlicher Grundrechtsschutz gemäß Art. 52 Abs. 3 GRCh, Berlin 2009 (Diss. Bonn 2008).

Sonstige Materialien

BEREC,
BEREC findings on traffic management practices in Europe, BoR (12) 30, https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/45-berec-findings-on-traffic-management-practices-in-europe, 2012 (zuletzt besucht am 09.10.2021).

BEREC,
BEREC Report on differentiation practices and related competition issues in the scope of net neutrality, BoR (12) 132, https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/1094-berec-report-on-differentiation-practices-and-related-competition-issues-in-the-scope-of-net-neutrality, 2012 (zuletzt besucht am 09.10.2021).

Brack, Jan,
Internet beschleunigen: So konfiguriert ihr einen alternativen DNS-Server, netzwelt.de, 25.12.2019, https://www.netzwelt.de/news/125241-internet-beschleunigen-so-konfiguriert-alternativen-dns-server.html (zuletzt besucht am 09.10.2021).

Brownlee, Nevil/ Mills, Cyndi/ Ruth, Greg,
Traffic Flow Measurement: Architecture, https://www.hjp.at/doc/rfc/rfc2722.html, 1999 (zuletzt besucht am 09.10.2021).

Dudenredaktion,
Suchwort: „Effektivität“, in: Duden. Das Fremdwörterbuch, 11. Aufl., Berlin 2015, S. 287.

FCC,
Pressemitteilung vom 04. August 2008, 2008, https://transition.fcc.gov/Daily_Releases/Daily_Digest/2008/dd080804.html (zuletzt besucht am 09.10.2021.

Google LLC,
Public DNS, https://developers.google.com/speed/public-dns/ (zuletzt besucht am 09.10.2021).

Google LLC,
Entfernungen von Inhalten aufgrund von Urheberrechtsverletzungen – Google Transparenzbericht, https://transparencyreport.google.com/copyright/overview (zuletzt besucht am 09.10.2021).

heise online,
Porno-Abmahnungen: Indizienkette zur IP-Adressen-Ermittlung verdichtet sich, 2013, https://heise.de/-2065879 (zuletzt besucht am 09.10.2021).

Humboldt Universität zu Berlin,
Merkblatt HU-Account, https://www.cms.hu-berlin.de/de/dl/beratung/antrag/merkblatt.html (zuletzt besucht am 09.10.2021).

ipoque,
Product portfolio, https://www.ipoque.com/products (zuletzt besucht am 09.10.2021).

Leach, Paul J./ Berners-Lee, Tim/ Mogul, Jeffrey C./ Masinter, Larry/ Fielding, Roy T./ Gettys, James,
Hypertext Transfer Protocol -- HTTP/1.1, https://tools.ietf.org/html/rfc2616 (zuletzt besucht am 09.10.2021).

manager magazin Redaktion,
Obama votiert gegen Überholspur im Netz, in: manager magazin online, 11.11.2014, https://www.manager-magazin.de/politik/artikel/obama-votiert-gegen-ueberholspur-im-netz-a-1002167.html (zuletzt besucht am 09.10.2021).

Microsoft Corporation,
Ändern der TCP/IP-Einstellungen – Windows-Hilfe, 2021, https://support.microsoft.com/de-de/help/15089/windows-change-tcp-ip-settings (zuletzt besucht am 09.10.2021)

Mogul, Jeffrey C./ Nottingham, Mark,
HTTP Header Field Registrations, https://tools.ietf.org/html/rfc4229, 2005 (zuletzt besucht am 09.10.2021).

Die Obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten, 2009, https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/B_Datenschutzkonforme%20Ausgestaltung%20von%20Analyseverfahren%20zur.pdf, (zuletzt besucht am 09.10.2021)

Reed, David,
What Your Broadband Provider Knows About Your Webuse: Deep Packet Inspection and Communications Laws and Policies, 2008, S. 61 ff., abrufbar unter https://www.govinfo.gov/content/pkg/CHRG-110hhrg58071/html/CHRG-110hhrg58071.htm (zuletzt besucht am 09.10.2021).

Sauerbrey, Anna,
NSA-Untersuchungsausschuss: BND lauscht bis heute bei der Telekom, in: Tagesspiegel.de, https://www.tagesspiegel.de/politik/nsa-untersuchungsausschuss-bnd-lauscht-bis-heute-bei-der-telekom/11075868.html, 05.12.2014 (zuletzt besucht am 09.10.2021).

SPIEGEL ONLINE Redaktion,
Rapidshare macht dicht, in: SPIEGEL ONLINE, https://www.spiegel.de/netzwelt/web/rapidshare-filehoster-stellt-den-betrieb-ein-a-1017771.html, 10.02.2015 (zuletzt besucht am 09.10.2021).

Synology Inc.,
How to set up your domain with Synology DNS Server, https://www.synology.com/en-global/knowledgebase/tutorials/584 (zuletzt besucht am 09.10.2021).

Wikipedia (en),
Suchwort „Mission creep“, Stand der Bearbeitung: 21.09.2020, https://en.wikipedia.org/wiki/Mission_creep (zuletzt besucht am 09.10.2021).

XIP Tech UG,
IP-info, https://IP-info.org (zuletzt besucht am 09.10.2021).