NomosPraxis

Jandt | Steidle [Hrsg.]

Datenschutz und Internet

DS-GVO | BDSG | TDDDG
KI-VO | DMA | DSA

2. Auflage

Nomos

NomosPraxis

Silke Jandt | Roland Steidle [Hrsg.]

Datenschutz und Internet

DS-GVO | BDSG | TDDDG KI-VO | DMA | DSA

2. Auflage

Dr. Jens Ambrock, Referatsleiter beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit | **Dr. Ubbo Aßmus**, Rechtsanwalt und Fachanwalt für Informationstechnologierecht; Geschäftsführer der lawcode GmbH, Lehrbeauftragter an der Hochschule RheinMain | **Dr. Tim Bagger von Grafenstein**, Rechtsanwalt und Fachanwalt für Sportrecht, Partner, München | **Dr. Henning Dehnert**, Referent beim Landesbeauftragten für den Datenschutz Niedersachsen | **Louisa Endrös**, Rechtsanwältin und Fachanwältin für Sport- und Datenschutzrecht, München | **Dr. habil. Christian L. Geminn**, Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) und Privatdozent, Universität Kassel | **Dr. Volker Hammer**, Editor der DIN 66398 „Leitlinie Löschkonzept" und Co-Editor der ISO/IEC 27555, freiberuflicher Berater für Löschprojekte (loeschprojekte.de), Bensheim | **Prof. Dr. Felix Hermonies**, Mag. rer. publ. LL.M., Professor für Datenschutz- und Medienrecht, Hochschule Darmstadt | **Dr. habil. Silke Jandt**, Stellvertretende Referatsleiterin beim Landesbeauftragten für den Datenschutz Niedersachsen | **Dr. Moritz Karg**, Referatsleiter Grundsatzangelegenheiten der Digitalisierung und des EGovernments, Staatskanzlei Schleswig-Holstein | **Dr. Sophie Victoria Knebel**, Fachanwältin für Informationstechnologierecht sowie Senior Legal Counsel bei der Parshipmeet Group | **Henry Krasemann**, Referatsleiter Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Dozent, Jurafunk, Kiel | **Anna Pokutnev**, Referentin bei dem Landesbeauftragten für Datenschutz Niedersachsen | **Dr. Philipp Richter**, Referent beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz | **Dr. Annika Selzer**, Abteilungsleiterin für IT-Recht am Fraunhofer SIT und Co-Forschungsbereichskoordinatorin für IT-Recht in ATHENE | **Dr. Hendrik Skistims**, Rechtsanwalt und Syndikusanwalt bei Union Investment, Frankfurt a.M. | **Dr. Tobias Stadler**, Referatsleiter bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) | **Dr. Roland Steidle**, LL.M. Rechtsanwalt und Fachanwalt für Informationstechnologierecht, Partner, Lehrbeauftragter an der Hochschule Darmstadt, Frankfurt a.M. | **Dr. Stefanie Wegener**, Rechtsanwältin und Fachanwältin für Arbeits- und Informationstechnologierecht, Hamburg | **Prof. Dr. Thomas Wilmer**, Professor für Informationsrecht, Hochschule Darmstadt

Nomos

Zitiervorschlag: Jandt/Steidle Datenschutz-HdB

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-7560-1302-9 (Print)
ISBN 978-3-7489-1810-3 (ePDF)

2. Auflage 2025

Vorwort der Herausgeber

Die erste Ausgabe des Handbuchs „Datenschutz im Internet“ war vor allem durch das Inkrafttreten der europäischen Datenschutz-Grundverordnung am 24. Mai 2016 und deren vorrangiger Geltung vor den nationalen Datenschutzgesetzen in der Union ab dem 25. Mai 2018 motiviert. Die in allen Mitgliedstaaten unmittelbar und einheitlich geltende Verordnung ist nach wie vor ein Meilenstein in der Harmonisierung des europäischen Datenschutzrechts, das bis dahin auf der europäischen Datenschutz-Richtlinie aus dem Jahr 1995 und den jeweils national umgesetzten Datenschutzgesetzen basierte.

In den Jahren nach dem Erscheinen der Erstausgabe des Handbuchs gab es so viele rechtliche Weiterentwicklungen in Bezug auf das Internet, dass eine Neuauflage unvermeidlich war. Selbst beim Schreiben der Zweitauflage wurden die Autorinnen und Autoren immer wieder durch Gesetzesnovellierungen überholt. Nachdem die Datenschutz-Grundverordnung nunmehr seit über sechs Jahren gilt, sind Gerichtsurteile zu einzelnen Vorschriften und zu Auslegungsfragen ergangen und es hat sich gezeigt, wie die europäischen und deutschen Aufsichtsbehörden die Datenschutz-Grundverordnung um- und durchsetzen. Die neuere Rechtsentwicklung ist vor allem durch die Digitalstrategie der Europäischen Kommission mit mehreren Verordnungen sowie den ergänzenden nationalen Vorschriften geprägt, die auch den Datenschutz im Internet tangieren. Hervorzuheben sind hier der Digital Services Act, der Digital Markets Act und das Digitale Dienste Gesetz. Da Techniken der Künstlichen Intelligenz in immer mehr Diensten des Internets und in Apps integriert sind, beeinflusst auch die europäische KI-Verordnung als erstes Gesetz zur Regulierung von Künstlicher Intelligenz den Datenschutz im Internet maßgeblich.

Obschon im Vorwort der Erstauflage festgestellt wurde, dass die heutige Realität der Informationstechnologie und Datenverarbeitung im Internet nur noch wenig mit derjenigen aus dem Jahr 1995 gemein hatte, so hat sich das Rad seit 2018 noch einmal erheblich weiter gedreht. Die bereits 2018 erörterte „Vercloudung“ von Internet-Diensten hat sich fortgesetzt. Im Bereich Social Media haben sich neue Angebote wie zum Beispiel Snapchat und TikTok mit sehr großen Nutzerzahlen auf dem Markt etabliert und auf Large Language Modellen basierende KI-Chatbots gehören zum Alltag. Weiterhin hat die Miniaturisierung von Prozessoren und Netzwerkkomponenten dazu geführt, dass auch kleinste Alltagsgegenstände im „Internet der Dinge“ netzwerkfähig werden und über das Internet miteinander kommunizieren. Sensoren werden zur Ermöglichung autonomen Fahrens in Kraftfahrzeugen verbaut und erheben auch umfangreich personenbezogene Daten von Fahrern, Insassen und Verkehrsteilnehmern. Im sogenannten Metaverse erfolgt eine weitgehende Umgebungserfassung mit dem Ziel, die physisch reale Umgebung mit digitalen Räumen zu verschmelzen. All diese Entwicklungen stellen weitere Meilensteine der Digitalisierung des Alltags dar und erweitern die Anwendung der Datenschutz-Grundverordnung erheblich.

Mit der technischen Weiterentwicklung gehen neue Geschäftsmodelle und Marketingstrategien einher, die noch mehr als bisher auf der Nutzung und Monetarisierung personenbezogener Nutzerdaten basieren. Die Komplexität der Datenverarbeitungspro-

zesse und der eingebundenen Dienstleister hat sich fortwährend erhöht, so dass die Verarbeitungsvorgänge teils kaum noch nachvollziehbar, geschweige denn effektiv kontrollierbar sind. Die nochmals erheblich gestiegenen Datenmengen haben neue Branchen und Anbieter entstehen lassen, unter anderem im Bereich von Big Data und den damit einhergehenden Datenanalysen.

Die aus den neuen Analysemöglichkeiten folgenden Risiken einer ungerechtfertigten Diskriminierung einzelner Personen über Algorithmen, automatisierte Entscheidungen, Prognosen und statistische Ergebnisse, die – zumindest teilweise – ohne eine Verarbeitung personenbezogener Daten herbeigeführt werden, zeigen die Schwächen des Konzepts des Personenbezugs auf. Der Personenbezug bleibt nach der Datenschutz-Grundverordnung weiterhin alleiniger Anknüpfungspunkt für die Geltung datenschutzrechtlicher Bestimmungen. Die Ergänzungen durch den nicht an den Personenbezug anknüpfenden Art. 5 Abs. 3 E-Privacy-Richtlinie sowie § 25 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz zum Schutz von Endgeräten sind zwar ein Schritt in die richtige Richtung. Allerdings stammt die europäische Vorgabe, nach der anbieterseitig Daten auf Endgeräten gespeichert oder ausgelesen werden können, im Kern aus 2002 und ist daher mit Blick auf heutige Trackingtechnologien völlig veraltet.

Bedauerlicherweise hat die Datenschutz-Grundverordnung auch im Übrigen nicht zu einer inhaltlichen Modernisierung mit Blick auf die zunehmende Digitalisierung geführt. Soll das Datenschutzrecht auch all die in einer digitalen Welte anfallenden flüchtigen und meist nicht längerfristig gespeicherten Kommunikationsdaten erfassen? Der Alltag würde dann nicht nur durch Datenverarbeitungen durchdrungen, sondern noch mehr durch Datenschutzregelungen, deren Ursprung aus der Zeit der Großrechner und zentralen Datenverarbeitungen mit klar identifizierbaren Verantwortlichen stammt. Ob diese Datenschutzregelungen in dem beschriebenen künftigen Umfeld praktisch überhaupt noch anwendbar oder gar kontraproduktiv sind, ist diskussionswürdig. Dies betrifft Fragen der Verortung datenschutzrechtlicher Verantwortung in komplexen Geschäftsmodellen mit mehreren Beteiligten oder die Forderung nach umfangreichen Informationspflichten und Dokumentationen mit den damit einhergehenden zusätzlichen Datenspeicherungen. Fragen der Verwendung sensitiver Daten, wie der von Biometriedaten zur Authentifizierung an Endgeräten oder bei Webdiensten, fordern ebenfalls Antworten. Ebenso ist das Verhältnis des Datenschutzrechts zur Meinungsfreiheit – nicht zuletzt wegen des Einflusses von Meinungen, Fakten oder „Fake News“ auf gesellschaftliche Entwicklungen und Wahlen – in den letzten Jahren zunehmend diskutiert worden. Die massiven Herausforderungen des Datenschutzrechts in einer digitalen Gesellschaft zeigen sich anhand vergangener und aktueller Datenschutzpannen und -skandale. Schließlich haben die Entwicklung und das Training von Large Language Modellen der Künstlichen Intelligenz einen noch größeren „Datenhunger“ ausgelöst, der kaum noch zu befriedigen ist. Die dazu technisch notwendigen Datenverarbeitungen laufen nahezu allen Grundsätzen des Datenschutzrechts zuwider – insbesondere der Datenminimierung, der Transparenz und der Zweckbindung. Die KI-Verordnung ist zwar ein Regulativ, enthält aber sehr wenige Datenschutzvorschriften. Die Datenschutz-Grundverordnung bleibt vollumfänglich anwendbar, so dass die aufgeworfenen Fragen anhand der allgemeinen Vorgaben der Datenschutz-Grundverordnung zu beantworten sind.

Obgleich die Europäische Kommission in zwei Evaluierungsberichten die europäische Datenschutz-Grundverordnung mit gut bewertet hat, zeigt ihre mehrjährige Anwendung in der Praxis, dass drängende Fragen des Datenschutzrechts unbeantwortet geblieben sind. Der fehlende Modernisierungsmut des europäischen Gesetzgebers zeigt sich nicht erst bei den ungelösten Problemen der Künstlichen Intelligenz. Eine moderne, die Nutzer schützende und zugleich innovationsfreundliche Regulierung, die die Interessen von Nutzern und Anbietern berücksichtigt und in Einklang bringt, enthält die Verordnung bedauerlicherweise nicht. Einige wenige bereichsspezifische Datenschutzdefizite versucht der europäische Gesetzgeber durch punktuelle Sonderregelungen zum Beispiel im Digital Markets Act und im Digital Services Act zu beheben. Dieser Ansatz ist erstens mit dem Nachteil verbunden, dass das europäische Datenschutzrecht erneut droht, in verschiedenen Gesetzen aufgesplittet zu werden. Darüber hinaus entstehen im föderalen deutschen System durch europäische Verordnungen, die unterschiedliche Regulierungsansätze von Marktregulierung, Verbraucher- und Datenschutz in einem Gesetz verfolgen, behördliche Zuständigkeitsprobleme für die Umsetzung und Kontrolle der Verordnungen.

Während des Gesetzgebungsverfahrens zur Datenschutz-Grundverordnung wurden vor allem die zahlreichen Öffnungsklauseln für nationale Sonderregelungen als erhebliches Risiko für die europaweiten Harmonisierungsbestrebungen eingestuft. Mittlerweile hat sich gezeigt, dass insbesondere drei andere Probleme die Harmonisierung behindern. Erstens zeigen die vom Europäischen Datenschutzausschuss zu verschiedenen Themen erarbeiten Guidelines, dass es bei der Auslegung und Anwendung der Datenschutz-Grundverordnung sehr große Differenzen der europäischen Aufsichtsbehörden gibt, die letztlich nur in Kompromissen „auf dem kleinsten gemeinsamen Nenner“ eingefangen werden. Ungeachtet dessen behalten nationale Aufsichtsbehörden zum Teil ihre frühere, gegebenenfalls strengere Aufsichtspraxis bei, so dass bei der Rechtsdurchsetzung trotz der angestrebten Harmonisierung ein unterschiedliches Niveau bestehen bleibt. Zweitens, und dies wiegt wohl deutlich schwerer, ist die Rechtsdurchsetzung aufgrund der unterschiedlichen Ausstattung und Auslastung der nationalen Aufsichtsbehörden sehr uneinheitlich und langwierig. Die Konzentration der Zuständigkeit für die großen Internetplayer bei der irischen Aufsichtsbehörde mag hier mit hineinspielen, ist aber keinesfalls die Hauptursache. Drittens ergaben sich Schwierigkeiten bei der Rechtsdurchsetzung auch deshalb, da der Europäische Datenschutzausschuss die formalen Hürden in Streitbeilegungsverfahren der nationalen Aufsichtsbehörden sehr hoch gesetzt hat. Daher ist insbesondere das erste große Streitbeilegungsverfahren (Twitter EDPB Binding Decision 01/2020) an Formalien gescheitert. Wesentliche materiell-rechtliche Fragen sind folglich nicht durch den Ausschuss entschieden worden. In weiteren Verfahren ist der Europäische Datenschutzausschuss aber deutlich entschiedener aufgetreten. Er hat sowohl materiell-rechtliche Festlegungen getroffen als auch wesentlichen Einfluss auf die Bußgeldhöhen genommen.

Aus Sicht der datenverarbeitenden Unternehmen ist es in vielen Bereichen der Informationstechnologie und der Internetnutzung nach wie vor sehr schwierig, sich gerichtsfest rechtskonform zu verhalten. Dies gilt insbesondere in innovativen Projekten aber auch bei seit langem bekannten Verarbeitungsvorgängen wie beispielsweise dem Testen

mit Echtdaten in komplexeren IT-Systemen. Angesichts des erheblich erweiterten Bußgeldrahmens zur Sanktionierung von – gegebenenfalls nicht eindeutig erkennbaren – Verstößen ist dies wirtschaftlich riskant. Allerdings zeigt die Bußgeldpraxis der letzten Jahre, dass die Aufsichtsbehörden den Handlungsspielraum der Datenschutz-Grundverordnung jedenfalls im mittelständischen Umfeld eher zurückhaltend nutzen. Bei der aktuellen KI-Forschung und -Entwicklung werden dennoch erneut Stimmen laut, die den Datenschutz und ergänzend die KI-Verordnung als Hemmnis für Innovationen in Europa bewerten. Denn erfolgreiche Entwicklungen und Webangebote stammen meist aus Drittländern, insbesondere aus den USA und China, und führen dann zu faktischen Auswirkungen auch in der Europäischen Union, allein aufgrund der großen Anzahl betroffener Nutzer.

Aufgrund der vorab beschriebenen Herausforderungen sind Auslegungs- und Argumentationshilfen wichtig für die Rechtsanwendung. Das Handbuch soll dieses Bedürfnis befriedigen und Rechtsanwendern aus Wissenschaft, Behörden, Unternehmen sowie Nutzern von Internet- und Webangeboten eine praktische Hilfestellung im Alltag geben. Dazu enthält es fundierte und wissenschaftlich untermauerte Beiträge mit Quellenangaben zu fast allen relevanten Bereichen des Datenschutzrechts im Internet. Eine besondere Berücksichtigung finden die zahlreichen Leitlinien und Stellungnahmen des Europäischen Datenschutzausschusses, in denen internetspezifische Datenschutzthemen konkretisiert werden. Die Autorinnen und Autoren haben verschiedene berufliche Hintergründe, alle lange Jahre Erfahrung im Datenschutzrecht und prägen die Materie in ihren Bereichen mit. Es sind Erfahrungen aus Wissenschaft, Aufsichtswesen und Unternehmen in das Handbuch eingeflossen. Der daraus folgende Mehrwert prägt dieses Handbuch und macht seinen Reiz aus.

Die Herausgeber und Autoren bedanken sich bei den Lesern für kritische Anmerkungen und wünschen Ihnen viel Freude beim Lesen.

Göttingen, Frankfurt, September 2024 *Silke Jandt und Roland Steidle*

Inhaltsübersicht

Inhaltsverzeichnis

Verzeichnis der Autoren

Dr. Jens Ambrock	Referatsleiter beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit
Dr. Ubbo Aßmus	Rechtsanwalt und Fachanwalt für Informationstechnologierecht; Geschäftsführer und Co-Founder der lawcode GmbH, Lehrbeauftragter an der Hochschule RheinMain
Dr. Tim Bagger von Grafenstein	Rechtsanwalt und Fachanwalt für Sportrecht und Partner bei Lentze Stopper Rechtsanwälte in München
Dr. Henning Dehnert	Referent beim Landesbeauftragten für den Datenschutz Niedersachsen
Louisa Endrös	Rechtsanwältin für Sport- und Datenschutzrecht bei Lentze Stopper Rechtsanwälte in München
Dr. habil. Christian L. Geminn	Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) und Privatdozent an der Universität Kassel
Dr. Volker Hammer	Editor der DIN 66398 „Leitlinie Löschkonzept“ und Co-Editor der ISO/IEC 27555, freiberuflicher Berater für Löschprojekte (loeschprojekte.de)
Prof. Dr. Felix Hermonies	Mag. rer. publ. LL.M. (R.L.), Professor für Datenschutz- und Medienrecht an der Hochschule Darmstadt
Dr. habil. Silke Jandt	Stellvertretende Referatsleiterin beim Landesbeauftragten für den Datenschutz Niedersachsen
Dr. Moritz Karg	Staatskanzlei Schleswig Holstein, Referatsleiter Grundsatzangelegenheiten der Digitalisierung und des EGovernments
Dr. Sophie Victoria Knebel	Senior Legal Counsel (Syndikusrechtsanwältin bei der Parshipmeet Group), Rechtsanwältin, Fachanwältin für Informationstechnologierecht sowie zertifizierte Informationssicherheitsbeauftragte (ISO 27001)
Henry Krasemann	Referatsleiter Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Dozent, Jurafunk, Kiel

Dr. Philipp Richter	Referent beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz
Anna Pokutnev	Referentin beim Landesbeauftragten für den Datenschutz Niedersachsen
Dr. Annika Selzer	Abteilungsleiterin für IT-Recht am Fraunhofer SIT und Co-Forschungsbereichskoordinatorin für IT-Recht in ATHENE
Dr. Hendrik Skistims	Rechtsanwalt und Syndikusanwalt bei Union Investment, Frankfurt a.M.
Dr. Tobias Stadler	Referatsleiter bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)
Dr. Roland Steidle, LL.M.	Rechtsanwalt und Fachanwalt für Informationstechnologierecht und Partner bei SWM Rechtsanwälte in Frankfurt am Main, Lehrbeauftragter an der Hochschule Darmstadt
Dr. Stefanie Wegener	Rechtsanwältin und Fachanwältin für Arbeits- und Informationstechnologierecht
Prof. Dr. Thomas Wilmer	Professor für Informationsrecht an der Hochschule Darmstadt

I. Grundlagen des Internets

Eine bereichsspezifische Betrachtung des Datenschutzrechts erfordert einen konkreten Untersuchungsgegenstand.[1] Daher ist es erforderlich, zunächst eine Beschreibung „des Internets" zu versuchen, um als Basis der datenschutzrechtlichen Ausführungen ein einheitliches Verständnis zu erzielen. 1

Abstrakt beschrieben ist das „Internet" die technische Innovation, durch die Datenverarbeitung allgegenwärtig geworden und in jeden Lebensbereich eingedrungen ist. Hinter der **Bezeichnung „Internet"** verbergen sich jedoch unterschiedliche Begriffe und ein unterschiedliches Verständnis. Auf die Frage, wie das „Internet" definiert oder was darunter zu verstehen ist, wird es viele unterschiedliche Antworten geben, je nachdem ob sie von einem Laien, versierten Internetnutzer oder einem Informatiker stammen und auch davon abhängig, in welchem Kontext die Bezeichnung verwendet wird. Formulierungen wie „ins Internet gehen", „im Internet surfen", „per Internet" oder auch schlicht „das Internet" weisen deutlich auf die Mehrdeutigkeit des Begriffes hin. Im allgemeinen Sprachgebrauch ist keine Formulierung falsch oder missverständlich. Sie ergänzen sich und beschreiben zusammengenommen eben nicht eine konkrete Technik oder einen technischen Gegenstand, sondern ein soziotechnisches System, welches als übergeordnete Bezeichnung die gesamte Innovation des „Internets" umfasst. 2

Für die datenschutzrechtliche Betrachtung bietet es sich an, das „Internet" durch eine **Dreiteilung** differenziert zu beschreiben, die in Anlehnung an die technische Perspektive erfolgt.[2] Die erste Ebene ist das **physikalische Netz** als infrastrukturelle Übertragungstechnik, die unter anderem aus Festnetz, Funk, Satellit und Mobilfunknetzen von General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS), Long Term Evolution (LTE) bis zunehmend aus 5G-Netzen besteht. Durch dieses und auf Basis eines einheitlichen **Netzwerkprotokolls** sind zahlreiche Rechner miteinander verbunden. Die technische Netzinfrastruktur auf erster Ebene wird nachfolgend als Internet bezeichnet.[3] Hierauf baut die digitale, transportierende IP-Schicht auf, durch die unterschiedliche sogenannte Overlay-Dienste oder **Internetdienste**, wie das World Wide Web (im Folgenden Web)[4] und E-Mail-Dienste, ermöglicht werden. Die Internetdienste bilden im folgenden Kontext zusammengenommen die zweite Ebene.[5] Schließlich soll als dritte Ebene das Web als Ausschnitt des „Internets" – oder genauer gesagt dieser spezifische Internetdienst – aufgrund seiner gesellschaftlichen Bedeutung vertiefend hinsichtlich seiner konkreter **Webdienste** betrachtet werden, wie **Webseiten, Suchmaschinen, Social Networks, Onlineshops, Wikis, Videoplattformen** und vie- 3

1 Einen besonderen Dank möchte ich an Frau Elena Richter aussprechen, die als Informatikerin beim Landesbeauftragten für Datenschutz in Niedersachsen arbeitet, und mit ihrer technischen Expertise die Ausführungen zur Technik des „Internet" geprüft und erforderlichenfalls ergänzt und korrigiert hat.

2 S. Kloepfer Netzneutralität in der Informationsgesellschaft/Ceulic, S. 20.

3 Eine begriffliche Ungenauigkeit wird im Folgenden teilweise bei der Verwendung umgangssprachlich üblicher Wortverknüpfungen mit Internet, wie zum Beispiel Internetadressen oder Internetnutzer nicht zu vermeiden sein.

4 Die korrekte Abkürzung für das World Wide Web ist „WWW". Für eine bessere Lesbarkeit wird dennoch die Kurzform „Web" verwendet.

5 Kloepfer Netzneutralität in der Informationsgesellschaft/Ceulic, S. 20 unterscheidet die drei Ebenen physikalisches Netz, IP-Schicht sowie Dienste und Applikation.

les mehr. Im Folgenden wird diesbezüglich die Bezeichnung **Webdienst, Web-Service oder Webanwendung** verwendet.

4 Die Erstellung und Gestaltung von Webseiten – das **Webdesign** – kann mittlerweile sehr vielschichtig sein. Sie beschränkt sich schon lange nicht mehr auf das Layout bestehend aus insbesondere Struktur und Aufbau, Farbschema, Typografie durch Schriftarten (Fonts), Bilder und Grafiken, Navigation, die Inhalte – den Content – und integrierte Interaktionselemente, wie Schaltflächen, Bestell- und Kontaktformulare, Zahlungsfunktionen, Chatfunktionen und die Optionen für nutzergeneriete Inhalte. Neben diesen gestalterischen und visuellen Elementen einer Webseite sind in die meisten Webseiten zahlreiche funktionelle Elemente und Dienste implementiert. Diese dienen dem Zweck die Funktionalität und Bedienbarkeit der Webseite für den Nutzer zuverlässig zu gewährleisen. Dazu gehören unter anderem die jederzeitige Verfügbarkeit und schnelle Ladezeiten, die zum Beispiel durch die Content Management Systeme, Content Delivery Networks, Analyse-Tools, Bot-Prototection, Captchas, JavaScripte, Plugins und vieles mehr umgesetzt werden können. Hinzu treten Consent Management Tools für die Abfrage und Speicherung rechtlich erforderlicher Einwilligungen. Schließlich hat auch das Tracking der Nutzer im Web mittlerweile eine solche Bedeutung erlangt, dass sowohl die unterschiedlichen technischen Umsetzungsmöglichkeiten als auch die verschiedenen Auswertungszwecke aufgezeigt werden.

5 Entsprechend der unterschiedlichen Ebenen des „Internets" sind zu dessen Realisierung zahlreiche Akteure, neben den Internetkonsumenten Internetdienstleister und sogenannte **Internet-Mediäre** erforderlich, die funktionsbezogen differenziert werden. Es werden ökonomische Besonderheiten aufgeführt, da diese häufig für normative Entscheidungen insbesondere über die Auflösung von Interessenkollisionen relevant sein können.

1. Internet als technische Netzinfrastruktur

6 Technisch beschrieben ist das Internet ein **dezentral organisiertes, globales Rechnernetzwerk**, das aus beliebig vielen miteinander verbundenen und eindeutig adressierten lokalen und nationalen Netzen besteht und auf einem **einheitlichen und offenen Netzwerkprotokoll** basiert.[6] Das Internet kann als das Straßennetz der Informationsgesellschaft bezeichnet werden.[7] Genau genommen, handelt es sich beim Internet nicht um ein physikalisches Netz, sondern eine Ansammlung verschiedener Netze, die bestimmte gängige Protokolle nutzen und bestimmte allgemeine Dienste zur Verfügung stellen.

7 Die technische Netzinfrastruktur besteht aus **kabelbasierten und kabellosen Techniken**, die grundsätzlich unterschieden werden können. Zu der ersten Gruppe gehören ein für das Internet ausgebautes Glasfaserkabelnetz, das herkömmliche Telefonnetz mit Kupferkabeln und das Kabelfernsehnetz aus Glasfaser- und Koaxialkabeln. Zu den

6 S. BVerfGE 120, 274 (276); Moritz/Dreier E-Commerce-HdB/Federrath/Pfitzmann Teil A Rn. 1; Kilian/Heussen ComputerR-HdB/Polenz Teil 13 Rn. 29 sowie zur Geschichte des Internets Strömer, Online-Recht, S. 3 ff. Der Gesetzgeber beschreibt das Internet sehr abstrakt und funktionsbezogen als „elektronisches Informations- und Kommunikationssystem", BT-Drs. 14/6468, 5.

7 Roßnagel KJ 1990, 267 (268) hat diese Bezeichnung zuvor für die Telekommunikationstechnik gewählt.

nicht kabelbasierten Internet-Techniken für das sogenannte „mobile Internet" gehören Mobilfunk- und Satellitennetze sowie Wireless Area Network (WLAN). Im Anschluss an die analogen Mobilfunknetze der ersten Generation, die keine praktische Relevanz mehr aufweisen, folgte Global System for Mobile Communications (GSM) als zweite, UMTS[8] als dritte, Long Term Evolution (LTE) als vierte und 5G als fünfte Generation der Mobilfunkstandards.[9] Die Entwicklung des nächsten Mobilfunkstandards 5G ist bereits so weit fortgeschrittenen, dass seit 2019 in Europa mit dem kommerziellen Ausbau begonnen wurde.

In Bezug auf den Vorgang der Datenübertragung zwischen zwei Rechnern wird die Internet-architektur als **Client-Server-Infrastruktur** beschrieben.[10] Diese Beschreibung differenziert funktionsbezogen zwischen dem Server als Dienst oder Daten zur Verfügung stellendes System und dem Client als das den Dienst oder Daten anfordernde System.[11] Die Besonderheit im Internet ist, dass jedes Computersystem sowohl als Server als auch als Client fungieren kann. Die Bezeichnung ist abhängig davon, welche Rolle das Computersystem in einem konkreten Kommunikationsprozess einnimmt. In **Peer-to-Peer Netzwerken** vernetzen sich die einzelnen Netzwerkteilnehmer ohne zentrale Server-Komponenten und agieren gleichzeitig als Server und als Client (Servent).[12] 8

Jeder an das Internet angeschlossene Rechner muss zu einem Zeitpunkt eine individuelle Kennung aufweisen, um für den Prozess der Datenübertragung zwischen zwei Rechnern über die technische Infrastruktur eindeutig angesprochen werden zu können. Diese eindeutige Kennung ist im Internet-Netzwerk die **Internet Protocol** (**IP-**)**Adresse**.[13] IP-Adressen sind nummerisch und bestehen nach der noch hauptsächlich verwendeten IPv4-Spezifikation aus 32 Bits – vier jeweils durch einen Punkt voneinander abgetrennten Zahlenblöcken – mit jeweils einer maximal dreistelligen Zahl (8 Bit) im Wert zwischen null und 255 (Bytes). Die IPv4-Spezifikation wird nach und nach (sogenanntes Dual Stack) durch die seit 1998 existierende IPv6-Spezifikation abgelöst, die insgesamt 128 Bits umfasst und in acht Zahlenblöcken von je vier Ziffern (16 Bit) dargestellt wird. In Europa wurden die letzten IPv4-Adressen von der zuständigen Vergabestelle im November 2019 vergeben.[14] Die IPv6-Spezifikation bietet eine deutlich größere Anzahl möglicher Adressen und ermöglicht weitere Funktionalitäten. 9

Um zu gewährleisten, dass jede IP-Adresse tatsächlich eindeutig einem Rechner zugewiesen ist, muss es Regeln und Verantwortliche für die Zuweisung der IP-Adressen geben. Die Koordination der **Vergabe von IP-Adressen** übernimmt die amerikanische **Internet Corporation for Assigned Names and Numbers** (**ICANN**). Eine geregelte 10

8 UMTS wurde in Deutschland Ende 2021 abgeschaltet, s. https://www.lte-anbieter.info/lte-news/umts-abschaltung-das-sind-die-termine-die-sie-kennen-muessen.

9 Zur Entwicklung der 5G-Netzabdeckung in Deutschland, s. die Informationen der Bundesnetzagentur zum Mobilfunk-Monitoring, https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Breitband/MobilesBreitband/start.html#Anker.

10 Moritz/Dreier E-Commerce-HdB/Federrath/Pfitzmann Teil A Rn. 8.

11 Hoeren/Sieber/Holznagel MMR-HdB/Sieber Teil 1 Rn. 20; Erlhofer, Suchmaschinen-Optimierung, S. 183 f.

12 S. die Vortragsfolien von Schiller, Telematics Chapter 10: Peer-to-Peer Networks, Nr. 10.59 f., https://www.mi.fu-berlin.de/inf/groups/ag-tech/teaching/2011-12_WS/L_19531_Telematics/10_P2P-Networks.pdf.

13 S. Moritz/Dreier E-Commerce-HdB/Federrath/Pfitzmann Teil A Rn. 7; Erlhofer, Suchmaschinen-Optimierung, S. 186. Die IP-Adresse kann mit einer Anschrift oder einer Telefonnummer verglichen werden, die ebenfalls mittelbar einer oder mehreren Personen zugeordnet werden können. Zum Beispiel lautet die IP-Adresse der Domain des Bundesverfassungsgerichts 77.87.229.25.

14 S. https://www.teltarif.de/internet-ipv4-adressen-mangel/news/78790.html.

Vergabe selbst erfolgt durch eine der ältesten Institutionen des Internets, die Internet Assigned Numbers Authority (IANA), eine Abteilung der ICANN. Die IANA verteilte in den Anfangsjahren des Internets IPv4-Adressen in großen Adressblöcken direkt an Organisationen, Firmen oder Universitäten, die dann die weitere Verteilung selbstständig übernahmen. Seit Februar 2005 sind fünf regionale Vergabestellen, die Regional Internet Registries (RIR), eingerichtet, denen nunmehr Adressblöcke – typischerweise /8 in CIDR-Notation – zugewiesen werden. Die Vergabe an die Endnutzer erfolgt nach deren eigenen Regelungen für die Zuweisung von Adressen an Provider oder Organisationen, die wiederum ihre IP-Adressen selbst verwalten. Für Europa ist die **Réseaux IP Européens** (**RIPE**) zuständig. Die Vergabe der IP-Adresse ist damit über eine hierarchische Baumstruktur organisiert und stellt eine Ausnahme der Dezentralität des Internets da.

11 Einen engen Zusammenhang zur IP-Adresse weist das **Domain Name System** (**DNS**) auf. Jedem Domain-Namen ist eine numerische IP-Adresse eindeutig zugeordnet. Während für den technischen Zugriff auf einen Server ausschließlich die IP-Adresse erforderlich ist, ist der zusätzliche Domain-Name ein Zugeständnis an die Merkfähigkeit der Menschen, die sich eher einen begrifflichen Domain-Namen als nummerische Adressen merken können, und damit an die Nutzerfreundlichkeit. Domains sind Teilbereiche des hierarchischen DNS. Vergleichbar der Situation der IP-Adressen erfolgt die Zuteilung von Domains über ein Vergabeverfahren, da diese ebenfalls im Internet weltweit einmalig und eindeutig sein müssen. Im Unterschied zum Vergabeverfahren für IP-Adressen werden Domains jedoch nicht zugewiesen, sondern sie sind unter Berücksichtigung vorgegebener Regeln frei wählbar. Die Vorgaben erfassen zunächst den Aufbau von Domains, der hierarchisch[15] ist und sich in festgelegter Reihenfolge aus Top-Level-Domain (TLD),[16] Second-Level-Domain (SLD)[17] zusammensetzt, und können durch Verzeichnis- und Dateinamen ergänzt werden.[18] Die weiteren Regeln für die Domain-Gestaltung sind von der konkreten TLD abhängig, da sie jeweils von der Vergabestelle der TLD – dem Network Information Center (NIC)[19] – festgelegt werden. Die Verwaltung der Länderkennung für Deutschland –.de – obliegt dem **Deutschen Network Information Center eG** – oder kurz **DENIC**.[20] Diese hat insbesondere Regelungen für die Verwendung von Buchstaben, Umlauten und Zeichen im Domain-Namen festgelegt.[21] Des Weiteren erfolgt die Vergabe der Domain nach dem Grundsatz „first come, first served", so dass unter Voraussetzung der Einhaltung der weiteren Domainrichtlinien für

15 Moritz/Dreier E-Commerce-HdB/Federrath/Pfitzmann Teil A Rn. 27.
16 TLD sind entweder geografisch und verweisen auf die Zuordnung der Webseite zu einem bestimmten Land, zum Beispiel de, fr, uk, oder generisch und sind einer bestimmten Gruppe zugeordnet, zum Beispiel com, org, net, gov. Eine Liste der generischen Domains findet sich bei der ICANN, s. https://www.icann.org/en/registry-agreements.
17 Bei der Domain http://www.bundesverfassungsgericht.de ist der zweite Teil – Bundesverfassungsgericht – die SLD.
18 Wie zum Beispiel /index.html.
19 Diese wird auch Domain Name Registry genannt. Sie verwaltet eine oder mehrere Top-Level-Domains im DNS, betreibt hierfür den Nameserver und den Whois-Service mit Kontaktdaten der Domaininhaber.
20 Zu weiteren Informationen s. https://www.denic.de/ueber-denic/.
21 S. die von der DENIC veröffentlichte IDN-Zeichenliste, https://www.denic.de/wissen/idn-domains#code-192-0.

den Antragsteller die gewünschte Domain registriert wird, sofern sie noch verfügbar ist.[22]

In **Overlay-Netzwerken**, wie zum Beispiel Tor (onion), GNUnet (.gnu) oder in dem für die Blockchain-Technologie verwendeten Lightning Netzwerk wird das oben genannte hierarchisch aufgebaute DNS umgangen, in dem Netzwerkverbindungen stattdessen dezentral über eigene Adressräume, Adressierungsregeln und mit Einsatz eigener Routingregeln zustande kommen. Für die Verbindung zu den im Internet verfügbaren Webdiensten werden Proxy-Server oder Outproxy genutzt. 12

In seinem bisherigen Erscheinungsbild weist das „Internet" **vier prägende Charakteristika** auf, die allerdings nicht alle technisch zwingend sind. Dies sind im Einzelnen die **Dezentralität**, **Globalität**, **Zugangsoffenheit** und **Neutralität**.[23] 13

Die beiden Charakteristika der Dezentralität und der Globalität finden sich bereits in der technischen Definition des Internets wieder. **Dezentralität** bedeutet in diesem Zusammenhang, dass die technische Infrastruktur nicht über eine oder mehrere zentrale Einheiten verfügt, über die letztlich alle Rechner miteinander verbunden wären. Es existieren somit keine zentralen technischen Knotenpunkte, die als „Zugangstore" für den Anschluss an das Rechnernetzwerk fungieren, und der Bestand des Internets hängt nicht von einer einzigen funktionierenden Zentrale ab.[24] Entsprechend kann das Netzwerk auch nicht durch einen zentralen Angriff in seiner grundsätzlichen Funktionsfähigkeit beeinträchtigt werden, so dass es eine geringe Verletzbarkeit und damit hohe Zuverlässigkeit aufweist.[25] 14

Globalität bedeutet, dass die technische Infrastruktur weltumspannend ist. Geografische oder natürliche Grenzen können die Ausbreitung der Netzwerkarchitektur nicht beeinträchtigten. 15

Das Charakteristikum der **Zugangsoffenheit** meint, dass grundsätzlich jede Person die Möglichkeit hat, den eigenen Rechner an das Internet anzuschließen und so zum Bestandteil des Rechnernetzwerks zu werden. Die Notwendigkeit, die Dienste eines Zugangsanbieters – oder auf Englisch Access-Provider – in Anspruch nehmen zu müssen, steht der Zugangsoffenheit nicht entgegen. Es bestehen technisch grundsätzlich keine begrenzten Anschlusskapazitäten, die eine Regulierung des Zugangs zum Internet erfordern würden, und der Anschluss ist unabhängig von den verwendeten Betriebssystemen und Netzwerktechniken möglich. Das Rechnernetzwerk kann beliebig ausgeweitet werden und die Anzahl der angeschlossenen Einzelrechner ist faktisch unendlich. Der Zugang zum Internet ist daher insbesondere weder staatlichen Einrichtungen, Unternehmen oder bestimmten Organisationen vorbehalten, noch existieren weitere Zugangsbeschränkungen, wie zum Beispiel Nationalität oder eine allgemeingültige Altersgrenze der Anschlussinhaber. 16

22 S. die Domainrichtlinien der DENIC unter https://www.denic.de/domains/de-domains/domainrichtlinien/.

23 Ursprünglich entwickelt wurde das Internet mit dem Ziel der Hochverfügbarkeit eines Kommunikationsweges, Moritz/Dreier E-Commerce-HdB/Federrath/Pfitzmann Teil A Rn. 10.

24 Nach Mecklenburg ZUM 1997, 525 (528) ist das Gegenstück der Netz- oder Sterntypologie die Baumtypologie der klassischen Medien.

25 S. hierzu ausführlich die Geschichte zur Entwicklung des Internets Tanenbaum/Wetherall, Computernetzwerke, S. 80 ff.

17 Während Dezentralität, Globalität und Zugangsoffenheit Eigenschaften des Netzwerks sind, bezieht sich die **Neutralität** auf die Datenübertragung durch dieses Kommunikationsnetz. Im Kern wird die wertneutrale, technische Funktionsweise der Datenübertragung im Internet durch den Begriff der Netzneutralität zusammengefasst.[26] Der zu übermittelnde Datensatz wird in einzelne Datenpakete zerlegt, die nach dem **Store-and-Forward-Prinzip** transportiert werden. Dies bedeutet, dass die Datenpakete nicht unmittelbar an den Zielrechner geschickt werden, sondern über verschiedene Zwischenrechner, auf denen sie jeweils bis zur nächsten Weiterleitung zwischengespeichert und auf Integrität geprüft werden.[27] Dieses Prinzip hat den Vorteil, dass Blockierungen auf Teilstrecken umgegangen werden können und eine Optimierung der Netzwerkauslastung erreicht wird. Nachteil des Verfahrens sind Verzögerungen beim Transport über Teilstrecken mit Zwischenspeicherungen Es entscheidet über den Weg, den die einzelnen Datenpakete durch das Internet zum Empfängerserver nehmen. Ergänzt wird das Store-and-Forward-Prinzip durch das **Best-Effort-Prinzip**. Danach werden alle Datenpakete gleichberechtigt übertragen, so wie es aufgrund der technischen Bedingungen am schnellsten möglich ist. Die Übermittlung der Datenpakete erfolgt immer über den schnellsten Weg für diese Methode, der nicht gleichzeitig der Kürzeste sein muss. Kommt es an einer Stelle im Netzwerk aus welchen Gründen auch immer zu einer Übermittlungsstörung, werden die Datenpakete automatisch über andere Knotenpunkte weitergeleitet.[28] Im Gegensatz dazu wird für wenig verzögerungstolerante Dienste wie Videostreamings oder Internettelefonie das sog. **Cut-Through-Prinzip** umgesetzt, bei dem auf Integritätsprüfungen zugunsten einer höheren Übertragungsgeschwindigkeit verzichtet wird, wenngleich mit einer höheren Fehlerrate. Zwischen den verschiedenen Prinzipien bestehen auch Mischformen.

18 Technisch wird die **Netzneutralität** durch den Aufbau des Datenpakets und die Regeln für deren Übertragung gewährleistet. Ein Datenpaket setzt sich aus mehreren Bestandteilen zusammen, die verschiedenen Schichten (sogenannte Layer) zugeordnet sind. Das sogenannte **DoD-Schichtenmodell** definiert vier Schichten und wird auch als **TCP/IP-Referenzmodell** bezeichnet.[29] Es ist ein theoretisches Denkmodel, das die systematische Darstellung des komplizierten Prozesses der Datenübertragung ermöglicht, indem auf den einzelnen Schichten die verschiedenen definierten Aufgaben dargestellt

26 S. zum Beispiel Bullinger, Netzneutralität– Wissenschaftliche Dienste des Bundestages 2010 S. 4. An dieser Stelle ist die rein technische Netzneutralität gemeint, so dass hier auf Ausführungen zur politischen und rechtlichen Diskussion der Netzneutralität verzichtet wird. S. zum technisch-traditionellen Begriff sowie zu weiteren Begriffsverständnissen Jäkel, Netzneutralität, S. 5 ff. mwN.

27 Moritz/Dreier E-Commerce-HdB/Federrath/Pfitzmann Teil A Rn. 39.

28 Kröger/Kuner, Internet für Juristen, S. 2 f.; Sieber JZ 1996, 430.

29 RFC 760 – DoD standard Internet Protocol, http://www.faqs.org/rfcs/rfc760.html. Zum Transmission Control Procotol (TCP) s. Moritz/Dreier E-Commerce-HdB/Federrath/Pfitzmann Teil A Rn. 19 f. Die Abkürzung DoD als Bezeichnung des Schichtenmodells bedeutet Department-of-Defence und beruht darauf, dass das Internet vom amerikanischen Verteidigungsministerium entwickelt worden ist. Neben diesem vierschichtigen Modell wird häufig auf das OSI-Schichtenmodell verwiesen, dass später von der International Organization for Standardization (ISO) entwickelt wurde. Insgesamt sind vier Schichten im DoD-Schichtenmodell definiert, die sich mit dem siebenschichten OSI-Schichtenmodell (Open Systems Interconnection Reference Model) vergleichen lassen. Das DoD-Schichtenmodell stellt eine vereinfachte Variante des OSI-Schichtenmodells dar, die in diesem Kontext als ausreichend erachtet wird. In dem ab 1977 entstandenen OSI-Schichtenmodell wurden die Netzzugangs- und die Anwendungsschicht des DoD-Modells granularer dargestellt und mit den damit insgesamt definierten sieben Schichten eine flexiblere und abwärtskompatible Zuordnung der in Computer- und Netzwerk-Technik zu definierenden Vorgänge ermöglicht.

werden. Eine Konkretisierung dieser Aufgaben in Bezug auf ihre Realisierung erfordert darüber hinaus die Definition von Regeln und Konventionen, wie diese Aufgaben auf der jeweiligen Schicht zu erfüllen sind und die Kommunikation zwischen den Schichten zu erfolgen hat. Diese Regeln sind in den sogenannten Protokollen festgelegt.[30]

Die Charakteristika der Dezentralität, Globalität und Zugangsoffenheit führen dazu, dass das Internet insgesamt technisch **heterarchisch** aufgebaut ist. Die technische Infrastruktur bedarf weder zentraler Einheiten oder zentraler Zugangsschnittstellen noch folgt – bisher – die Datenübermittlung hierarchischen Regeln. Lediglich die Vergabe von IP-Adressen und Domain-Namen erfolgt nach festgelegten Regeln und das DNS ist hierarchisch aufgebaut, um die eindeutige Zuordenbarkeit von einmaliger IP-Adresse und Domain-Namen zu gewährleisten. Hiervon unterscheidet sich das sogenannte **Darknet**, das – vereinfacht dargestellt – ein-anonymes abgeschirmtes Netzwerk darstellt, das auf einem dezentralen Overlay-Netzwerk basiert und deshalb ohne zentrale Verwaltungsinstanzen wie das Domain Name System (DNS) auskommt. Für den Zugang zu einem Darknet, beispielsweise in Tor, werden ein spezifischer Browser – TOR-Browser – sowie Zugangsinformationen benötigt. Für die Anonymisierung des kompletten Datenverkehrs leitet der Dienst „The Onion Routing" jedes ein- und ausgehende Datenpaket mit einer zufällig ausgewählten Route über das Tor-Server-Netzwerk um.[31] 19

2. Internetdienste

Die technische Infrastruktur des Internets wird erst durch die zahlreichen **Internetdienste** zum Leben erweckt. Sie stellen das Internet in einen – wenn auch noch sehr abstrakten – Anwendungskontext und ermöglichen dem Menschen die Nutznießung der reinen Internettechnik. Auf dieser hohen Abstraktionsebene kann das „Internet" als Medium zur Kommunikation zwischen Menschen beschrieben werden. Es handelt sich wie bei den Ursprüngen der Telekommunikation über Festnetztelefonie um eine Form technisch vermittelter Kommunikation. Dies allerdings mit dem wesentlichen Unterschied, dass jegliche Inhalte multimedial vermittelt werden können. 20

Grundvoraussetzung für die Nutzung aller Internetdienste ist, dass mit einem Rechner ein Zugang zum Internet als technische Netzinfrastruktur aufgebaut werden kann; es wird ein Internetzugang – auch Internetverbindung oder Internetanschluss – benötigt. Neben der technischen Ausstattung, wie zum Beispiel einem Router, wird für die Datenverbindung eines Computers oder eines Netzwerkes mit dem Internet vor allem eine IP-Adresse benötigt. Die meisten Teilnehmer erreichen die Internetverbindung über einen Internetzugangsdienst (**Access Providing**).[32] Diese Dienstleistung besteht in der Bereitstellung sogenannter Internet-Konnektivität, das bedeutet dem Transfer von IP-Paketen ins und aus dem Internet. 21

30 Hoeren/Sieber/Holznagel MMR-HdB/Sieber Teil 1 Rn. 40.
31 S. Hoffmann, Darknet: So funktioniert es, PC-Magazin vom 13.9.2016, http://www.pc-magazin.de/ratgeber/darknet-funktionsweise-nutzen-3196735-15344.html.
32 S. auch → Rn. 46 f. Im Jahr 2023 waren 91,7 % der Haushalte in Deutschland mit einem Internetzugang ausgestattet, s. https://de.statista.com/statistik/daten/studie/153257/umfrage/haushalte-mit-internetzugang-in-deutschland-seit-2002/.

22 Einer der bekanntesten und wohl auch bedeutendsten Internetdienste ist das **World Wide Web** (**WWW**),[33] das eine Übertragung von multimedialen Webseiten auf der Grundlage des **Hypertext Transfer Protocol** (**HTTP**) ermöglicht.[34] Diese Webseiten können theoretisch von jeder Person, die technischen Zugang zum Internet hat, zur Verfügung gestellt[35] und grundsätzlich von jedem Nutzer des Internets – sei es über einen eigenen oder fremden Internetzugang – abgerufen werden.

23 Eine Schlüsselfunktion für die Nutzung des Webdienstes nehmen **Webbrowser**[36] ein. Der Webbrowser ist eine Software für den Aufruf und die Darstellung von Webseiten und stellt die Benutzeroberfläche für Webanwendungen dar. Im Web stehen verschiedene Webbrowser zum kostenlosen Download zur Verfügung. Sie besitzen regelmäßig eine definierte Startseite, die beim Programmstart angezeigt wird. Wesentliche Bestandteile sind neben einer großen Ansichtsfläche für die Darstellung der Webseiten eine Adressleiste, in die der Domain-Name oder die URL der aufzurufenden Webseite eingegeben wird, und ein Eingabefenster für Suchbegriffe, die direkt eine Suchmaschine ansprechen.[37] Daneben verfügen Webbrowser über zahlreiche weitere Schaltflächen und Funktionen, die das Navigieren im Web erleichtern sollen, wie zum Beispiel die Darstellung eines Verlaufsprotokolls (Chronik), ein Verzeichnis mit Lesezeichen, und den Client vor Maßnahmen des Servers schätzen sollen, wie die Steuerung der Verwendung von Cookies und Proxy-Servern, Sicherheitskontrollen mit Warnhinweisen auf Malware- und Phishing-Angriffe sowie Anti-Tracking-Funktionen. Die in einigen Webbrowsern vorhandene Konfigurationsmöglichkeit für die Proxy-Einstellung ermöglicht einen Zugang zu den außerhalb des regulären Internets erreichbaren Overlay-Netzwerken wie Tor, Freenet und I2P.

24 Ein weiterer sehr wichtiger Internetdienst ist die **E-Mail** als elektronisches Gegenstück zum **Brief.**[38] **Die Versendung von E-Mails basiert im Internet auf dem Simple Mail Transfer Protocol** (**SMTP**).[39] Für den Empfang von E-Mails stehen mit dem Internet Message Access Protocol (IMAP) und Post Office Protocol (POP) zwei verschiedene

33 Die Bezeichnung Internet, auch teils „Clear Web" genannt, wird sehr häufig nicht in Bezug auf die technische Infrastruktur, sondern als Synonym für das Web verwendet, wie zum Beispiel bei der umgangssprachlichen Formulierung, „im Internet suchen". In der Entscheidung des LG Mannheim Urteil – 8.3.1996 - 7 O 60/96 CR 1996, 353 (354) wird das Web korrekt als Teilbereich des Internets beschrieben. Als Deep Web bezeichnete Netzwerke sind hingegen Teile des World Wide Webs, die mit allen Browsern ohne Proxy-Dienste erreichbar, aber als abgeschlossenes Netzwerk nur für autorisierte Benutzer oder Endgeräte zugänglich sind, u.a. zum Beispiel Firmen- oder Banknetzwerke. Aus diesem Grund sind Inhalte des Deep Webs auch nicht indexierbar für Suchmaschinen. Laut BSI „handelt es sich dabei um „90 % des gesamten Internets". Webseiten im Darknet stellen einen eher kleineren Teil des Deep Web dar. Deren Adressen werden nicht über den DNS-Server verwaltet, weshalb sie nur durch spezifische Suchmaschinen und Zugangspunkte des jeweiligen Overlay-Netzwerks oder Darknets auffindbar sind.

34 S. Moritz/Dreier E-Commerce-HdB/Federrath/Pfitzmann Teil A Rn. 42 ff.

35 Mittlerweile ist das Erstellen – zumindest einer professionellen – Webseite allerdings sehr komplex geworden. Eine Domain kann noch relativ einfach erworben werden, sofern die Wunschdomain noch nicht belegt ist. Im Web stehen zahlreiche, auch kostenlose Programme für das Webdesign zur Verfügung, um u.a. Layoutvorlagen, Kontaktformulare und Suchfunktionen sowie Tools um Fotos, Videos, Hyperlinks usw einzubinden. Um die Auffindbarkeit der Webseite zu gewährleisten, empfiehlt sich die Suchmaschinenoptimierung und die Webseite muss rechtliche Anforderungen, wie zum Beispiel die Impressumspflicht, erfüllen.

36 Vereinzelt wird im Folgenden auch die Kurzbezeichnung Browser verwendet.

37 Regelmäßig ist bei jedem Browser eine Suchmaschine vorausgewählt. Diese kann aber vom Nutzer beliebig konfiguriert werden.

38 S. Moritz/Dreier E-Commerce-HdB/Federrath/Pfitzmann Teil A Rn. 38 ff.

39 Die Übertragung im Internet erfolgt ebenfalls nach dem Store-and-Forward-Prinzip.

Protokolle zur Verfügung. Mittels einer E-Mail kann über das Internet eine Nachricht von einem Absender an einen oder mehrere Empfänger übermittelt werden. E-Mail-Dienste werden von E-Mail-Providern (oder auch E-Mail-Service-Providern) angeboten. Diese verwalten und veröffentlichen Mail Exchange Resource Records (MX-RR) der für die E-Mail-Konten genutzten Domains und verfügen über einen Mailserver, auf dem die E-Mail-Konten (oder auch E-Mail-Postfächer) der Nutzer gespeichert werden.[40] Jedes E-Mail-Konto wird durch eine E-Mail-Adresse, die dem Nutzer eindeutig zugewiesen wird, repräsentiert. Die E-Mail-Adresse, die für den Informationsaustausch benötigt wird, ist weder an eine bestimmte Örtlichkeit noch an einen bestimmten Rechner gebunden. Über die von den E-Mail-Providern angebotenen Webseiten können die einer E-Mail-Adresse zugeordneten Nachrichten von überall und mit beliebigen Endgeräten, insbesondere Desktops, Notebooks und Smartphones, die an das Internet angeschlossen sind, gelesen werden. Weitere Beispiele für Internetdienste sind Chat, Dateiübertragung, Internettelefonie und Internetrundfunk.

Durch den **Europäischen Kodex für elektronische Kommunikation** (**EKEK**)[41] wurde eine neue Unterkategorie von Internetdiensten definiert, die entsprechend in die deutsche Definition der Telekommunikationsdienste übernommen worden ist.[42] Die Definition der elektronischen Kommunikationsdienste gemäß Art. 2 Nr. 4 EKEK umfasst nurmehr neben der Unterkategorie „Internetzugangsdienste", die Unterkategorie „**interpersonelle Kommunikationsdienste**".[43] Die interpersonellen Kommunikationsdienste werden häufig auch als **Over-the-Top-Kommunikationsdienste** (**OTT-Kommunikationsdienste**) (→ V. Rn. 292 ff.) bezeichnet. Diese Bezeichnung macht ihre Zwitterstellung zwischen den Internet- und den Webdiensten deutlich. OTT-Kommunikationsdienste sind zu herkömmlichen Übermittlungsdiensten funktional gleichwertige Online-Dienste, die eine interpersonelle (Individual-)Kommunikation ermöglichen.[44] Beispielhaft genannt werden regelmäßig Vo**IP-Telefonie, Nachrichtenübermittlung** (**Messaging**) **und webgestützte E-Mail-Dienste**. Mobile Instant Messaging-Dienste wie Signal, WhatsApp und Threema haben zu einem sehr starken Rückgang von SMS und MMS geführt und dienen teilweise als Äquivalent für E-Mails. Vor allem haben sie aber insgesamt einen starken Anstieg von Kommunikationsvorgängen bewirkt, insbesondere da unterschiedliche Nachrichtenformen – Bild-, Text-, Video- und Sprachnachrichten möglich und kombinierbar sind. Spätestens seit der Corona-Pandemie und dem ersten „Lockdown" in Deutschland im März 2020 haben zudem **Videokonferenzdienste** eine große Bedeutung erlangt und werden in Unternehmen, Behörden, Schulen, Universitäten und sogar Gerichten als Ersatz für Präsenzveranstaltungen oder Telefonate eingesetzt. Um die Einordnung von Videokonferenzdiensten als individuelle Kommuni- 25

40 IdR bieten E-Mail-Provider weitere Zusatzdienste wie insbesondere den Schutz vor Spam-E-Mails und Computerviren an.

41 RL (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11.12.2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung)Text von Bedeutung für den EWR, s. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018L1972.

42 S. ausführlich zur Ausweitung der rechtlichen Definition der Telekommunikationsdienste, → IV. Rn. 5.

43 Eine dritte Unterkategorie bilden die an dieser Stelle nicht relevanten „Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für die Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden".

44 S. Engeler/Felber ZD 2017, 251 (254).

kationsdienste hat sich allerdings – anscheinend ausschließlich – in Deutschland eine neue rechtliche Diskussion entfacht.[45]

26 Charakteristisch für das Internet sind noch weitere, ergänzende Dienstleistungen, die für die Realisierung der Internetnutzung erforderlich und in diese eingebunden sind. Der **DNS-Service** wandelt den als Internetadresse bezeichneten Domain-Namen in die generische IP-Adresse um, die für den technischen Zugriff auf einen Server notwendig sind.[46] Im Web besteht die Internetadresse oder genauer gesagt der **Uniform Resource Locator** (**URL**) aus der Domain gegebenenfalls ergänzt um weitere Verzeichnisse und Dateibezeichnungen.[47] Die URL dient der Vereinheitlichung der Bezeichnung der Dokumente im Internet. Bei der E-Mail-Kommunikation ist jede individuelle E-Mail-Adresse einer Domain zugeordnet. Auf einer dem Aufruf der Internetseite über die URL oder der Übermittlung der E-Mail an den Empfänger vorgelagerten abstrakten Ebene „entscheidet" der DNS-Service, ob der durch den Domain-Namen bezeichnete Server der Internetseite oder des E-Mail-Providers tatsächlich dem Nutzer angezeigt oder Daten an ihn übermittelt werden. Fehler oder gezielte Veränderungen bei der Zuordnung einer Domain zu der korrekten IP-Adresse hätten zur Folge, dass der Zugriff auf bestimmte Server über den Domain-Namen nicht realisiert wird. Sofern IP-Adressen nicht mehrfach genutzt werden, wie zum Beispiel beim Shared Hosting, können Internetseiten im Web in der Regel auch durch die direkte Eingabe der IP-Adresse im Browser aufgerufen werden. Dann erfolgt der Aufruf der Internetseite unmittelbar und ohne den technischen Zwischenschritt über den DNS-Server.

27 Während der Begriff Internet das technische System beschreibt, sind die Kategorien der **Internetdienste** die Grundlagen der Nutzung durch den Menschen. Sie decken im Wesentlichen jeweils eine oder mehrere von vier Funktionen ab, die einen gemeinsamen Nenner bilden. Dies sind im Einzelnen der Austausch von Informationen, die Kommunikation, die Interaktion sowie der Aufbau und die Pflege sozialer Beziehungen.

3. Webdienste

28 Eine weitere Konkretisierung der Beschreibung des „Internets" kann durch eine nähere Betrachtung der Inhaltsebene, insbesondere der **Webdienste** erreicht werden, indem erstens eine generelle Beschreibung eines Webdienstes vorgenommen wird und zweitens beispielhaft Kategorien von Webdiensten funktional und entsprechend ihrer Zweckbestimmung qualifiziert werden.

29 Das Web ist in seiner Gesamtheit eine Sammlung unzähliger Dokumente, die als **Webseiten** auf Webservern abgelegt sind und auf die über das Internet und den Webbrowser zugegriffen werden kann.[48] Das Aufrufen von Webseiten erfolgt als Datenübertragung

45 S. Roßnagel NJW 2023, 400 sowie → Rn. 77.
46 Moritz/Dreier E-Commerce-HdB/Federrath/Pfitzmann Teil A Rn. 25 ff.
47 Moritz/Dreier E-Commerce-HdB/Federrath/Pfitzmann Teil A Rn. 43. Auf der Domain der Universität Kassel (uni-kassel.de) findet sich zum Beispiel die Unterseite des Wissenschaftlichen Zentrums für Informationstechnikgestaltung durch die Ergänzung um die Verzeichnisse eecs, iteg und startseite, s. http://www.uni-kassel.de/eecs/iteg/startseite.html.
48 Hoeren/Sieber/Holznagel/ MMR-HdB/Sieber Teil 1 Rn. 80.

Stichwortverzeichnis

Die **fetten** Zahlen verweisen auf den Paragrafen (Beitrag), die mageren auf die Randnummer.