

Prof. Dr. Michael Denga,
LL.M. (London), Maître en Droit (Paris)
Tel.: +49 (0)30 766 83 75-100
Fax: +49 (0)30 766 83 75-119
E-Mail: michael.denga@businessschool-berlin.de



Business & Law School
Hochschule für Management und Recht

Campus Berlin
Siemens Villa
Calandrellistraße 1-9
12247 Berlin

Campus Hamburg
HafenCity
Am Kaiserkai 1
20457 Hamburg

Durchsetzung und Optimierung der Verantwortung von Social Media-Plattformen

Gutachten im Auftrag der HateAid gGmbH

Prof. Dr. Michael Denga, LL.M. (London), Maître en Droit (Paris)

9. September 2025

Inhalt:

A. Wesentliche Ergebnisse.....	3
B. Die aktuelle Gefährdungslage von Nutzern auf Online Plattformen	4
C. Untersuchungsfokus	5
D. Interpretationskontext – Europas Digitale Souveränität	6
E. Pflichten von Social Media Plattformen	7
I. Notice and Take-Down im Kontext der Melde- und Abhilfeverfahren des DSA ...	7
II. Pflichten systemrelevanter Plattformen	8
III. Einfluss der KI-Verordnung.....	9
F. Durchsetzung der Plattformpflichten	10
I. Haftung des Plattformanbieters.....	11
1. Aufsichtsrecht des DSA	11
2. Private Enforcement des DSA.....	13
a) Effet utile und Komplementarität von Privat- und Aufsichtsrecht.....	13
b) Voraussetzungen des Private Enforcement	14
c) Zivilrechtliche Anknüpfungspunkte	15
d) Aktiv- und Passivlegitimation	15
II. Persönliche Haftung des Personals	16
1. Gesellschaftsrechtliche Organhaftung.....	16
2. Unmittelbare Haftung des handelnden Personals.....	17
3. Anwendbarkeit deutschen Rechts und Zuständigkeit deutscher Gerichte	19
G. Effektivierung der Auskunftspflichten.....	20
I. Transparenzprogramm des DSA.....	20
II. Probleme, insbesondere des Forschungsdaten Zugangs	21
III. Aktuelle Maßnahmen der Europäischen Kommission.....	21
IV. Weitere Erwägungen	22
H. Zentrale rechtspolitische Maßnahmen zur Steigerung der Sicherheit von Social Media-Plattformen	23
I. Verbot von Social Bots	23
II. Nutzeridentifikation per Video-Ident	24
III. Recht auf Inhaftefilter.....	24
IV. Qualifikation der Geschäftsleitung.....	25
V. Transparenz und Rechtsbehelfe für Shadow-Banning	25
VI. Altersbeschränkung für Social Media	26
VII. Beweislastumkehr im Prozess	26

A. Wesentliche Ergebnisse

Der DSA ist im Kontext **Digitaler Souveränität der Europäischen Union** zu lesen und anzuwenden, die als teleologisches Prinzip eine praktische Wirksamkeit der Regelungen des DSA in materieller wie auch prozeduraler Hinsicht gebietet.

Die Vorgaben des DSA sind **gegenüber Vermittlungsdiensten** sowohl durch behördliche Aufsicht als auch durch private Geltendmachung deliktischer Ansprüche (Private Enforcement) durchsetzbar. Art. 54 DSA begründet ausdrücklich Schadensersatzansprüche der Nutzer. Angesichts der geopolitischen Spannungen und der daraus folgenden politischen Kontingenz der aufsichtsrechtlichen Durchsetzung des DSA gewinnt das Private Enforcement eine besondere Bedeutung für die Umsetzung der Ziele des DSA.

Die DSA-Pflichten treffen das verantwortliche Personal von Vermittlungsdiensten zwar nicht unmittelbar, konkretisieren jedoch seinen individuellen Sorgfaltsmaßstab und können bei Verletzung eine **unmittelbare deliktische Haftung** nach § 823 Abs. 1 BGB auslösen.

Der **Forschungsdatenzugang** nach Art. 40 DSA wird durch oberflächliche Compliance und "Information Overkill" unterlaufen. Die EU-Delegierte Verordnung vom Juli 2025 adressiert diese Probleme nur teilweise, so dass eine Pflichtennachschräpfung erforderlich ist.

Social Media sollte auch von der neueren KI-Regulierung erfasst werden. Art. 7 KI-VO ermöglicht der EU-Kommission die Einstufung von **Social Media-Algorithmen als Hochrisiko-KI-Systeme** durch delegierte Rechtsakte, wodurch umfassende Transparenz- und Daten-Governance-Pflichten aktiviert würden.

Der DSA ist unter dem Aspekt von **Safety by Design** fortzuentwickeln. Empfohlen werden u.a. ein vollständiges Social Bot-Verbot, Video-Ident-Nutzerverifikation, ein Recht auf konfigurierbare Inhaltsfilter, Altersbeschränkungen für Social Media (16 Jahre) und eine Beweislastumkehr bei Plattformschäden.

B. Die aktuelle Gefährdungslage von Nutzern¹ auf Online Plattformen

Nutzer von Online Plattformen, namentlich von Social Media, sind seit Aufkommen der Angebote sog. „schlechten“ Inhalten ausgesetzt, hierzu zählen u.a. Bedrohungen, sexuelle Belästigung oder Identitätstäuschung. Es handelt sich dabei in der Regel um nach deutschem Recht illegale Inhalte, jedoch auch um solche die gegen die internen Richtlinien der Plattformen verstoßen oder sich nachteilig auf einzelne Nutzende oder die öffentliche Debatte insgesamt auswirken. Die grundrechtliche Gemengelage, zwischen negativer und positiver Informations- und Kommunikationsfreiheit, zudem auch im Rahmen der unternehmerischen Freiheit der Plattformen ist komplex und stark einzelfallabhängig;² an dieser Stelle sind mit „schlechten“ Inhalten allein rechtswidrige gemeint, als solche, bei denen die Interessen der Informationsempfänger oder Informationsbetroffener gegenüber den Interessen der Informationssender und der Plattform überwiegen.

Die Problemlage verschärft sich zunehmend, wobei drei Vektoren hervorzuheben sind:

1. Kritisch ist immer noch **übergriffiges Nutzerverhalten**, welches am häufigsten unter pseudonymen Konten erfolgt. Diese verbreiten rechtsverletzende Inhalte in eigenen Beiträgen, sowie Kommentarspalten und Privatnachrichten. Hierzu zählen Beleidigungen, Bedrohungen, Volksverhetzungen, Verleumdungen, Doxxing oder auch das nicht einvernehmliche Zusenden pornografischer Inhalte.
2. Mit der Verbreitung **generativer KI** ist die Erstellung falscher Inhalte für jedermann einfach möglich. Dies wird auf Social Media Plattformen unter anderem dazu genutzt, gefälschte Bilder auch von Personen zu verbreiten. Als besonders kritisch zu nennen sind auch gefälschte, authentisch wirkende Profile auf Social Media Plattformen, zudem die Erstellung und Verbreitung falscher, beleidigender oder sexuell-expliziter Inhalte, gegenüber den Betroffenen oder auch Dritten. Hochproblematisch ist der Einsatz von KI für den autonomen Betrieb von Fake-Accounts oder die Gründung von Chatgruppen auf Social Media-Plattformen, die innerhalb einer Rahmenprogrammierung selbstständig am Plattformdiskurs teilnehmen und in hoher Frequenz falsche Tatsachen oder Beleidigungen („Fake News“ – oder schlicht: Propaganda) verbreiten.³
3. Auch plattformseitig sind weiterhin erhebliche Probleme zu beklagen. Plattformen genießen umfangreiche Haftungsprivilegien und sind grundsätzlich nicht für nutzergenerierte Inhalte verantwortlich (zum Regime des DSA sowie der hier zu beobachtenden kopernikanischen Wende noch ausführlicher unten, E.). Dies gilt, obwohl sie an vielen Stellen durch ihre Algorithmen, deren genaue Funktionsweise allein ihnen bekannt ist, auf den Verbreitungsgrad von Inhalten einwirken. So werden vor allem emotionalisierende Inhalte, die intensive Interaktion hervorrufen, mit einer besonders großen Reichweite und Sichtbarkeit belohnt – denn gerade so wird die geschäftsmodelltragende, geldwerte Verweildauer der Nutzer auf der Plattform erhöht. Dies wird insbesondere durch Akteure ausgenutzt, die mit zielgerichteter und orchesterter Interaktion, sowie dem Einsatz von Mehrfachprofilen bewusst den Eindruck erwecken wollen, eine Mehrheitsmeinung zu repräsentieren. Die Plattformen unterscheiden dabei nicht zwischen hasserfüllten und ggf. sogar strafbaren Inhalten und solchen, die konstruktive Interaktionen hervorrufen. Darüber hinaus moderieren Online-Plattformen Inhalte auf Grundlage ihrer *Community Standards*, den Allgemeinen Geschäftsbedingungen, häufig automatisiert durch Einsatz von KI und Wortfiltern. Die so gewonnene **Kuratierungsgewalt** nutzen Plattformen auch dazu, solche Inhalte zu löschen, die nicht mit der politischen Ansicht der Plattforminhaber übereinstimmen.

¹ Ausschließlich zum Zweck der besseren Lesbarkeit wird im vorliegenden Gutachten auf die geschlechtsspezifische Schreibweise verzichtet. Alle personenbezogenen Bezeichnungen sind geschlechtsneutral zu verstehen.

² Vgl. nur *Eifert* NJW 2017, 1450 (1451f.) ; *Klonick* Harvard L. Rev. 131 (2018), 1598 (1626ff.); *Denga* EuR 2021, 569 (572).

³ *Drolsbach/Pröllochs*, Characterizing AI-Generated Misinformation on Social Media, 2025, S. 1.

Zudem sind die Beschwerdemechanismen noch nicht hinreichend effektiv und wirken oft zu spät und können damit die Verbreitung „schlechter“ Inhalte nicht verhindern.

Social Media-Plattformen haben für die soziale Teilhabe längst essenzielle Debattenräume geschaffen. Gleichzeitig werden diese höchst intransparent durch die Regeln privater Unternehmen gesteuert. Diese haben kaum eine wirtschaftliche Inzentivierung, der Verbreitung schädlicher Inhalte entgegenzuwirken und begünstigen durch ihre aufmerksamkeitsgetriebene Funktionsweise sogar deren massenhafte Verbreitung. Nutzer, die schädliche und sogar rechtswidrige Inhalte verbreiten, haben u.a. wegen der weitreichenden Anonymität, die ihnen die Plattformen durch die Nutzung von Fake- und Mehrfachprofilen ermöglichen, kaum Konsequenzen zu befürchten. Hierdurch entsteht ein Klima, in dem Internetnutzende aus Furcht vor digitalen Angriffen nicht wagen, frei ihre Meinung zu äußern und an Debatten teilzunehmen.⁴

Diese kurze Darstellung ist ein nicht abschließender Überblick der Problemlage, der jedoch klarmacht, dass im Interesse des Individualrechtsgüterschutzes, allerdings auch der Meinungspluralität und der Funktionalität öffentlich zugänglicher, digitaler Diskursräume regulatorische Durchsetzungsmechanismen zu aktivieren und womöglich auch Korrekturen darin geboten sind.

C. Untersuchungsfokus

Auf diesem Hintergrund ist der regulatorische Rahmen für digitale Plattformen, namentlich der DSA kritisch zu prüfen, um Gestaltungs- sowie Reformmöglichkeiten zu identifizieren, sowohl auf Ebene materieller Pflichten von Plattformen, als auch ihrer Durchsetzung. Ausgangspunkt hierbei ist, dass Online Plattformen nicht neutral im Informationsaustausch stehen, sondern insbesondere auf Grund der bereits erwähnten Kuratierungsmacht, die zentralen Akteure der Informationsverbreitung sind.⁵ Der europäische Gesetzgeber hat dies im DSA für „systemrelevante Plattformen“ (nach den Art. 33 ff. DSA) unmissverständlich klargestellt und dabei eine kopernikanische Wende, weg vom „Intermediärsprivileg“, eingeleitet (dazu unter E. I.).⁶

Im Fokus stehen sollen hier zwei Aspekte:

1. Der DSA scheint noch nicht die *Prävention* schlechter Inhalte verbessert zu haben. Daher sollen hier **präventive Systemmaßnahmen** von Plattformen, ihre Durchsetzung sowie ihre Fortentwicklung im Sinne einer *Safety by Design*⁷ erörtert werden (dazu unter E., F. und H.).
2. Die vom DSA vorgegeben **Transparenzpflichten** wirken noch nicht effektiv, namentlich ist der materielle Gehalt der Mitteilungen von Plattformen häufig nicht aussagekräftig; zudem wird der Forschungsdatenzugang nach Art. 40 DSA noch regelmäßig vereitelt. Daher sollen hier Optionen zur Verbesserung des Informationsgewinns von Online Plattformen erörtert werden (dazu unter G.).

⁴ Dazu etwa die repräsentative Studie von Das NETTZ, Gesellschaft für Medienpädagogik und Kommunikationskultur, HateAid und Neue deutsche Medienmacher*innen als Teil des Kompetenznetzwerks gegen Hass im Netz (Hrsg.), *Lauter Hass – leiser Rückzug. Wie Hass im Netz den demokratischen Diskurs bedroht. Ergebnisse einer repräsentativen Befragung*, 2024, abrufbar unter: https://kompetenznetzwerk-hass-imnetz.de/download_lauterhass.php

⁵ Vgl. dazu nur Klonick Harvard L. Rev. 131 (2018), 1598 (1610); zum Paradigma der Internetregulierung über Intermediäre vgl. Goldsmith/Wu, *Who controls the internet?*, 2006, S. 65 ff.

⁶ Auch Art. 17 der DSM-Richtlinie ist in dieser Perspektive zu lesen, dazu Denga, *Zurechnung*, 2022, S. 330.

⁷ Der Begriff ist dem regulatorischen Diskurs in Australien und dem Vereinigten Königreich geläufig, dazu die Stellungnahme des australischen *eSafety Commissioners* von September 2024, abrufbar unter: <https://www.esafety.gov.au/industry/safety-by-design>; so auch Woods zum Online Safety Act, 2024, abrufbar unter: <https://www.onlinesafetyact.net/analysis/safety-by-design/>.

D. Interpretationskontext – Europas Digitale Souveränität

Die Anwendung des DSA erfolgt nicht in luftleerem Raum, sondern im Kontext der Beschlüsse von Europäischem Parlament und Rat über die Gestaltung des Digitalen Binnenmarkts. Dabei steht insbesondere die Geltung europäischer Werte im Fokus der europäischen Gesetzgeber. Unter dem Visum der Digitalen Souveränität sollen die Belange der EU Bürger im Digitalen Raum einen gehaltvollen Geltungsanspruch erlangen.

Beispielhaft heißt es dort:

“Die Strategie (für den digitalen Binnenmarkt) ist auf mehrere Jahre angelegt und konzentriert sich auf zentrale, miteinander verknüpfte Maßnahmen, die nur auf EU-Ebene ergriffen werden können”⁸

“Deshalb müssen wir einen echten europäischen Binnenmarkt für Daten, d. h. einen auf europäische Regeln und Werte gestützten europäischen Datenraum, schaffen.”⁹

“Die europäische digitale Agenda für 2020-2030 reagiert auf diese Veränderungen, indem sie sich um die Schaffung sicherer digitaler Räume [...] und die Stärkung der digitalen Souveränität Europas bemüht, im Einklang sowohl mit der digitalen als auch mit der grünen Wende.”¹⁰

„Die Wettbewerbspolitik allein kann jedoch nicht alle systemischen Probleme lösen, die in der Plattformwirtschaft auftreten können. Der Logik des Binnenmarktes folgend sind möglicherweise zusätzliche Vorschriften erforderlich, um Wettbewerbsfähigkeit, Fairness und Innovation sowie die Möglichkeit des Marktzutritts sicherzustellen und öffentliche Interessen zu wahren, die über den Wettbewerb oder wirtschaftliche Erwägungen hinausgehen.“¹¹

Digitale Souveränität mag ein neues Prinzip im Recht des Digitalen Binnenmarkts sein, das noch der weiteren Konkretisierung bedarf. Fest steht freilich bereits jetzt, dass es sich dabei keineswegs um bloße Rhetorik handelt. Beschlüsse der EU sind unmittelbar wirksam.¹² Methodisch kann der Topos digitaler Souveränität angesichts seiner zentralen Bedeutung für die EU dazu dienen, jedenfalls die unbestimmten Rechtsbegriffe der EU-Digitalregulierung aufzuladen und teleologisch in Richtung Nutzerschutz auszurichten.¹³ Souveränität ist dabei zu verstehen als Hoheitsanspruch,¹⁴ demnach im Digitalen Raum europäische Rechtsgüter genauso gelten und geschützt werden wie im analogen Raum. Daher muss ihre

⁸ Europäische Kommission, Strategie für einen digitalen Binnenmarkt für Europa, 06.05.2015, S. 3, abrufbar unter: <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52015DC0192>.

⁹ Europäische Kommission, Gestaltung der digitalen Zukunft Europas, 19.02.2020, S. 9, abrufbar unter: https://commission.europa.eu/document/download/84c05739-547a-4b86-9564-76e834dc7a49_de?file-name=communication-shaping-europes-digital-future-feb2020_de.pdf.

¹⁰ Europäische Kommission, Fact Sheet on the European Union: Digital agenda for Europe, April 2025, abrufbar unter: https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe?utm_source=chatgpt.com.

¹¹ KOM(2020) 67 endgültig, S. 10.

¹² Vgl. Art. 288 Abs. 3; dazu Grabitz/Hilf/Nettesheim/Nettesheim EUV/AEUV, 85. EL 2025, AEUV Art. 288 Rn. 38.

¹³ Deutlich zur Selbstbehauptung der EU durch Digitalregulierung bei Bradford, Digital Empires, 2023, S. 105 ff., 324 ff.; zum gleichzeitig geltenden Gebot der Staatsferne in der Medienregulierung Wischmeyer JZ 2024, 774 (779 ff.); zur Teleologischen Trinität des Rechts des Digitalen Binnenmarkts vgl. bereits Dengä ZfPW 2024, 427 (445 ff.).

¹⁴ Vgl. dazu Grabitz/Hilf/Nettesheim/Nettesheim EUV/AEUV, 85. EL 2025, AEUV Art. 288 Rn. 14; zur Geltung demokratischer Prinzipien im digitalen Raum auch Susskind, The Digital Republic, 2022, insbes. S. 135 ff.

Integrität in digitalen Gefährdungslagen effektiv sichergestellt werden, mit gehaltvollem Schutz auf materieller und prozeduraler Ebene. Dies soll im Folgenden für den DSA dargelegt werden.

E. Pflichten von Social Media Plattformen

Das Regelungsprogramm des DSA ist in Art. 1 Abs. 2 auf drei Achsen heruntergebrochen, die gleichzeitig die Kapitel des Rechtsakts bezeichnen – die Haftungsbeschränkung von Vermittlungsdiensten in Fortführung des Intermediärsprivilegs der E-Commerce-Richtlinie¹⁵ (Kapitel II), besondere, gestufte Sorgfaltspflichten (Kapitel III)¹⁶ und die Durchführung und Durchsetzung der Verordnung (Kapitel IV). Social Media Plattformen unterfallen dem Regime als Vermittlungsdienste iSd Art. 3 lit. g), in der besonderen Form der Online Plattform iSd Art. 3 lit. i).

I. Notice and Take-Down im Kontext der Melde- und Abhilfeverfahren des DSA

Für die Regulierung der Vermittlungsdienste wird auf das Regime der E-Commerce-Richtlinie (ECRL) aus dem Jahr 2000¹⁷ aufgesetzt, deren Modifikation denn auch Gegenstand von Kapitel II ist. Das darin enthaltene „Intermediärsprivileg“ besagt, dass bei Durchleitung, Caching und Hosting im Grundsatz keine Haftung für „rechtswidrige“¹⁸ Inhalte besteht, sofern der Anbieter keine Kenntnis von ihnen hat; Anbieter müssen allerdings behördlichen Weisungen in Bezug auf rechtswidrige Inhalte sowie Auskunftsanordnungen in Bezug auf bestimmte Nutzer Folge leisten, im Falle von Caching und Hosting rechtswidrige Inhalte ab Kenntniserlangung beseitigen. Eine generelle Überwachungspflicht der Anbieter für ihre Dienste ist ausgeschlossen, um die Überwachungsfreiheit privater Kommunikation im digitalen Raum sicherzustellen.¹⁹ Allerdings dürfen Vermittlungsdienste nach Art. 7 „auf Eigeninitiative nach Treu und Glauben und sorgfältig freiwillige Untersuchungen durchführen oder andere Maßnahmen zur Erkennung, Feststellung und Entfernung rechtswidriger Inhalte“ treffen, ohne dabei das Intermediärsprivileg zu verlieren.²⁰

Dieses sehr simpel gehaltene Regime sollte zu Beginn des neuen Jahrtausends die Entwicklung der Internetwirtschaft in Europa fördern²¹ und wurde in den DSA übertragen. Zentraler Unterschied ist zum einen der Verordnungscharakter, der nationale Umsetzungsvorschriften überflüssig macht. Auch waren unter der E-Commerce-Richtlinie behördliche Auskunftsbegehren zu Nutzern nicht vorgesehen, die jetzt

¹⁵ Richtlinie 2000/31/EG. Zu den anerkannten Einschränkungen des Intermediärsprivilegs vgl. allerdings *Spindler*, Zivilrechtliche Sperrverfügungen gegen Access Provider nach dem EuGH-Urteil „UPC Telekabel“, GRUR 2014, S. ? f.; zur deutschen Störerdogmatik *Volkman*, Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, § 1004 BGB, Rn. 34 ff., 826 f.; zur deutschen Störerdogmatik *Spindler/Schuster/Volkman*, Recht der elektronischen Medien, 4. Aufl. 2019, § 1004 BGB, Rn. 34 ff.

¹⁶ Damit wird das von *Specht-Riemenschneider/Hoffmann* empfohlene funktionszentrierte Pflichtenmodell zumindest im Ansatz verwirklicht, wenngleich *diese* zugleich für die Aufgabe des Intermediärsprivilegs und eine Generalklausel plädierten, Verantwortung von Online-Plattformen, 2021, etwa S. 101; ausf. *Steinrötter/Denga*, Europäische Plattformregulierung, 2023, § 6; *Kaesling*, Hofman/Raue, Digital Services Act, 2023, Vor. Art. 33 ff.

¹⁷ Richtlinie 2000/31/EG vom 8.6.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (Richtlinie über den elektronischen Geschäftsverkehr), ABl. 2000 L 178/1.

¹⁸ Nach Art. 3(h) handelt es sich dabei um „alle Informationen, die als solche oder durch ihre Bezugnahme auf eine Tätigkeit, einschließlich des Verkaufs von Produkten oder der Erbringung von Dienstleistungen, nicht im Einklang mit dem Unionsrecht oder dem Recht eines Mitgliedstaats stehen, ungeachtet des genauen Gegenstands oder der Art der betreffenden Rechtsvorschriften“.

¹⁹ Zu den anerkannten Einschränkungen des Intermediärsprivilegs vgl. allerdings *Spindler* Zivilrechtliche Sperrverfügungen gegen Access Provider nach dem EuGH-Urteil „UPC Telekabel“, GRUR 2014, 826 f.; zur deutschen Störerdogmatik *Spindler/Schuster/Volkman*, Recht der elektronischen Medien, 4. Aufl. 2019, § 1004 BGB, Rn. 34 ff.

²⁰ Vgl. auch Erwägungsgrund 26; kritisch *Ruffert/Denga*, Die Regulierung Digitaler Plattformen, 2023, S. 14 ff.

²¹ *Hofmann* GRUR 2018, 21, 27 f.

in Art. 10 enthalten sind, ebenso wenig wie die ausdrückliche Legitimation freiwilliger Untersuchungen auf Eigeninitiative unter Art. 7.

Art. 14 DSA etabliert grundlegende Transparenz- und Schutzpflichten für alle Anbieter von Vermittlungsdiensten, indem er verlangt, dass Inhaltebeschränkungen, Moderationsmechanismen und interne Beschwerdeverfahren in **klarer, benutzerfreundlicher und maschinenlesbarer Form** in ihren Allgemeinen Geschäftsbedingungen offengelegt werden – die Community Standards müssen also hinreichend vorhersehbar sein. Änderungen der Nutzungsbedingungen müssen Nutzer aktiv mitgeteilt werden. Wird ein Dienst vorrangig von Minderjährigen genutzt, ist eine altersgerechte Formulierung verpflichtend. Zudem müssen die Maßnahmen zur Durchsetzung dieser Regelungen sorgfältig, objektiv und verhältnismäßig sein sowie im Einklang mit den Grundrechten, insbesondere Meinungsfreiheit und Medienpluralität, stehen. Für besonders große Dienste – VLOPs und sehr große Suchmaschinen – gelten zusätzlich die Anforderungen einer prägnanten Zusammenfassung in allen relevanten EU-Sprachen.

Unter dem DSA müssen Hosting-Anbieter, einschließlich Online-Plattformen, zusätzlich ein Melde- und Beschwerdeverfahren für rechtswidrige Inhalte einrichten (Art. 16–18). Nutzungsbeschränkungen wegen rechtswidrigen Inhalten oder der Community Standards sind zu begründen (Art. 17). Das Meldesystem muss „leicht zugänglich und benutzerfreundlich sein. Nach Eingang einer Meldung müssen Plattformen diese „unverzüglich“ bearbeiten und begründete Entscheidungen treffen (Art. 16 Abs. 5), die „zeitnah, sorgfältig, frei von Willkür und objektiv“ sein müssen (Art. 16 Abs. 6); der Einsatz „automatisierter Mittel“ ist dabei zulässig, muss jedoch offengelegt werden (Art. 16 Abs. 6). Bei der Beschränkung von Inhalten ist der betroffene Nutzer nach Art. 17 zu informieren, wobei Online-Plattformen ein internes Beschwerdesystem für Abhilfemaßnahmen verfügbar machen müssen (Art. 20).

Teilweise wurde die Regelung von Art. 16 als gegenüber den durch rechtswidrige Inhalte betroffenen Nutzern zu schwach kritisiert.²² Richtig ist zwar, dass aus Art. 16 selbst keine unmittelbare Pflicht zur Sperrung von Inhalten folgt; die Norm ist jedoch mit dem Intermediärprivileg von Art. 6 für Hosting-Anbieter verzahnt, was Art. 16 Abs. 3 klar stellt: die Meldungen unter Art. 16 bewirken die Kenntnis unter Art. 6, welche die Haftung für gehostete rechtswidrige Inhalte auslöst, sofern diese sie nicht alsbald sperrt oder entfernt. Der DSA ordnet damit zwar insgesamt nicht selbst eine Löschung rechtswidriger Inhalte ab Kenntnis an, bietet jedoch mittels des Haftungsrechts (und auch des Strafrechts) einen klaren Anreiz dafür.²³

II. Pflichten systemrelevanter Plattformen

Für die Gefahrenabwehr in digitalen Räumen zentral ist das Kapitel III, welches so gut wie alle der bekannten Social Media Plattformen betrifft.²⁴

²² So spricht *Holznagel* lediglich von „Notice and Take-Action“, CRi 2024, 172, 178.

²³ Zur Verhaltenssteuerung durch Haftung grundlegend *Becker* Journal of Political Economy 1968, 76 (2); *Calabresi/Melamed*, Harvard Law Review 85 (1972), 1089; *Kötz* FS Steindorff, 1990, 643; *Arlen/Kraakmann*, NYU Law Review, Vol. 72, No. 1 (1997), 687; *Schäfer/Ott*, Lehrbuch der ökonomischen Analyse des Zivilrechts, 6. Aufl. 2020, S. 159 ff.; *Wagner AcP* 206 (2006), 352.

²⁴ Insoweit besteht auch eine weitgehende Kongruenz mit dem Konzept der Gatekeeper unter dem DMA, vgl. *Europäische Kommission*, Pressemitteilung vom 6. September 2023, IP/23/4328.

Für Anbieter „sehr großer Online-Plattformen“ und „sehr großer Online-Suchmaschinen“ werden in Kapitel III Abschnitt 5 verschärfte Verpflichtungen festgelegt. Wegen des spezifischen Bezuges zu systemischen Risiken soll hier von „systemrelevanten Plattformen“ die Rede sein;²⁵ diese haben mindestens 45 Millionen aktive Nutzer in der Europäischen Union (Art. 33 Abs. 1) und erreichen somit mehr als 10% der Verbraucher innerhalb der Union.²⁶ Die Verschärfung der Sorgfaltspflichten systemrelevanter Plattformen fügt sich in den gestuften Aufbau der Sorgfaltspflichten des DSA ein und ist damit letztlich Ausdruck des Verhältnismäßigkeitsgrundsatzes. Denn Art und Anzahl der Verpflichtungen werden so „unmittelbar mit der Reichweite eines Dienstes und seiner ökonomischen und gesellschaftlichen Bedeutung verknüpft“.²⁷

Anbieter systemrelevanter Plattformen sind nach Art. 34 zur Vornahme einer regelmäßigen Risikobewertung verpflichtet. Dabei sollen insbesondere „systemische Risiken“, etwa die Verbreitung rechtswidriger Inhalte oder die Auswirkungen auf Wahlen oder die psychische Gesundheit der Nutzer, in den Blick genommen werden, die aus der Konzeption oder dem Betrieb der Dienste ergeben können. In der Folge sind ermittelte Risiken von den Anbietern durch sachgerechte und effektive Maßnahmen zu mitigieren, Art. 35. Die Anbieter sind zudem im Falle einer gesellschaftlichen „Krise“ zu besonderen Maßnahmen verpflichtet, die über die gesteigerten Verpflichtungen des Abschnittes sogar noch hinausgehen, Art. 36. Sie müssen sich jährlich einer unabhängigen Prüfung zu unterziehen, Art. 37.

Art. 38 und 39 nehmen Empfehlungssysteme und Online-Werbung in den Blick, wobei eine Option ohne Profiling angeboten werden und Inhalt und Kriterien geschalteter Werbung unterhalten werden muss. Die betroffenen Akteure müssen sowohl dem Koordinator für digitale Dienste, als auch der Kommission Zugang zu ihren internen Daten gewähren; auch qualifizierte Forscher können so Datenzugang erlangen (Art. 40).

Art. 41 verpflichtet die betroffenen Anbieter zur Einrichtung einer angemessen ausgestatteten Compliance-Abteilung, um eine unabhängige interne Überprüfung der Einhaltung der Verordnung durch die Anbieter zu gewährleisten. Darüber hinaus werden Anbietern verschärfte Transparenzberichtspflichten auferlegt (Art. 42).

III. Einfluss der KI-Verordnung

Die Anwendung der KI-Verordnung (KI-VO)²⁸ auf Social-Media-Plattformen offenbart eine strukturelle Inkongruenz zwischen den erheblichen gesellschaftlichen Risiken algorithmischer Inhaltsmoderation und den tatsächlich greifenden Regulierungsmechanismen der KI-VO.²⁹

Social-Media-Plattformen fallen zwar regelmäßig unter die Definition des "Anbieters" nach Art. 3 Nr. 2 KI-VO, da sie KI-Systeme für die automatisierte Inhaltsmoderation, Empfehlungsalgorithmen und Nutzerinteraktionsanalyse entwickeln, bereitstellen oder jedenfalls unter eigenem einsetzen.³⁰ Soweit diese Systeme als "allgemeine KI-Systeme" im Sinne des Art. 3 Nr. 63 KI-VO zu qualifizieren sind, unterliegen sie jedoch lediglich den verhältnismäßig schwachen

²⁵ S. bereits Heinze/Steinrötter/Denga/Denga, EU Platform Law, 2025, § 6.

²⁶ Dabei wird maßgeblich an die „durchschnittliche monatliche Zahl aktiver Nutzer in der Union“ angeknüpft, die zukünftig als Durchschnitt über einen Zeitraum von sechs Monaten berechnet werden soll, vgl. Erwägungsgrund 6; s. auch Müller MMR 2022, 1007 (1008).

²⁷ Erwägungsgrund 75, 79; Müller MMR 2022, 1007 (1009); dazu auch Janal ZEuP 2021, 227 (232); mit einer Analogie zu „kritischer Infrastruktur“ Berberich/Seip GRUR-Prax 2021, 4 (7).

²⁸ EU-Verordnung (EU) 2024/1689.

²⁹ Vgl. zum Zusammenspiel von DSA und KI-VO Heinze/Steinrötter/Denga/Bastians, EU Platform Law, 2024, § 21.

³⁰ Zum weiten Anbieterbegriff vgl. Art. 3 Nr. 3 KI-VO.

Pflichten der Art. 53 ff. KI-VO. Diese beschränken sich im Wesentlichen auf Dokumentationspflichten und die Bereitstellung von Anwendungsinformationen nach Art. 53 Abs. 1 lit. a, b KI-VO, ohne substantielle Transparenz- oder Risikobeurteilungspflichten zu begründen (mit Ausnahme der IP-Compliance-Strategie unter Art. 53 lit. c KI-VO). Handelt es sich um besonders leistungsfähige KI-Modelle³¹, so unterliegen deren Anbieter den Pflichten von Art. 55 für „KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko“, welche namentlich eine dem Risikoüberwachungs- und Mitigierungskonzept der Art. 34 f. DSA vergleichbare Bewertungs- und Minderungspflicht für systemische Risiken enthalten (Art. 55 Abs. 1 lit. b)); zudem sind eine Modellbewertung, Kommunikation mit den Aufsichtsbehörden sowie ein angemessenes Maß an Cybersicherheit geschuldet.³²

Die algorithmischen Systeme von Social-Media-Plattformen erfüllen *materiell* die Kriterien für Hochrisiko-KI-Systeme nach Art. 6 Abs. 2 KI-VO, da sie erhebliche Risiken für die öffentliche Sicherheit und Grundrechte bergen. Empfehlungsalgorithmen auf Online-Plattformen beeinflussen politische Meinungsbildung, Radikalisierungsprozesse und gesellschaftliche Diskurse in einem Ausmaß, das den in Anhang III genannten Anwendungsbereichen vergleichbar ist. Dennoch fallen sie *formell* nicht unter die dort aufgeführten Kategorien, wodurch die weitreichenden Transparenz- und Governancepflichten der Art. 8 ff. KI-VO nicht greifen; insbesondere sind Anbieter von Social Media Plattformen nicht verpflichtet eine gehaltvolle, dem Regime des Art. 10 KI-VO vergleichbare,³³ Daten-Governance umzusetzen.

Art. 7 KI-VO eröffnet der Europäischen Kommission allerdings die Möglichkeit, Anhang III durch delegierte Rechtsakte zu erweitern, wenn KI-Systeme "ein Risiko von Schäden darstellen, das dem Risiko von Schäden vergleichbar oder größer ist als das Risiko von Schäden, das von den bereits in diesem Anhang aufgeführten Hochrisiko-KI-Systemen ausgeht". Diese Bestimmung sollte strategisch genutzt werden, um Social-Media-Algorithmen als Hochrisiko-Systeme zu klassifizieren und damit insbesondere die Datengovernance-Pflichten des Art. 10 KI-VO zu aktivieren. Art. 10 KI-VO würde Plattformen zu umfassender Dokumentation ihrer Trainingsdaten, Datenqualitätsprüfungen und Bias-Monitoring³⁴ verpflichten – Transparenzpflichten, die für die demokratische Kontrolle algorithmischer Meinungsbildung essentiell wären.

F. Durchsetzung der Plattformpflichten

Die Praxis der Plattformen zeigt (wie unter B. beschrieben) eine erhebliche Diskrepanz zum Idealzustand der Compliance mit dem Pflichtenprogramm auf. Akut ist daher die Frage nach der Durchsetzung der Plattformpflichten. Hier steht die Haftung der Plattform selbst im Fokus (I.), zudem auch die des Personals (II.).

³¹ Zur Definition vgl. Art. 51 KI-VO.

³² Die Pflichten für Anbieter allgemeiner KI-Systeme werden in KI-Verhaltenskodex sowie in Leitfäden der *Europäischen Kommission* präzisiert, abrufbar unter <https://digital-strategy.ec.europa.eu/de/policies/contents-code-gpai>.

³³ Dazu umfassend BeckOK KI-Recht/Kilian/Schefzig, 2. Ed. 1.5.2025, KI-VO Art. 10 Rn. 1-98.

³⁴ Dazu Wachter/ Mittelstadt/ Russell , Bias Preservation in Machine Learning: The Legality of Fairness Metrics Under EU Non-Discrimination Law, 2021 , S. 25; Legner RD 2024, 426.

I. Haftung des Plattformanbieters

Primärer Adressat des DSA sind die Anbieter von Vermittlungsdienstleistungen; der Anbieterbegriff ist dabei im Sinne einer wirtschaftlichen Einheit zu verstehen, so dass insbesondere durch Konzernierung keine Haftungsabschirmung erzeugt werden kann.³⁵ Anders als im deutschen Haftungsrecht wird im Anwendungsbereich europarechtlicher Regulierung Unternehmen Verhalten ihres Personals strikt zugerechnet, mit wenigen Ausnahmen für rein private Aktivitäten.³⁶ Zu unterscheiden ist bei der Haftung des Plattformanbieters zwischen der Aufsichtsrechtlichen Verantwortlichkeit (1.) und jener im Wege des Private Enforcement (2.).

1. Aufsichtsrecht des DSA

Das Recht des DSA ist als Aufsichtsrecht zu qualifizieren, da sein Pflichtenprogramm behördlich und im europäischen Verwaltungsverbund durchgesetzt wird.³⁷

In Deutschland fungiert die Bundesnetzagentur als zentraler Koordinator für digitale Dienste gemäß Art. 51 DSA, ergänzt durch Spezialzuständigkeiten der Bundeszentrale für Kinder- und Jugendmedienschutz (BzKJ) und des Bundesbeauftragten für Datenschutz und Informationsfreiheit.³⁸ Für die in Kapitel III Abschnitt 5 geregelten Pflichten systemrelevanter Plattformen (dazu bereits oben, E. II.) ist hingegen die EU-Kommission nach Art. 56 Abs. 2, 4 DSA ausschließlich zuständig; für die übrigen Pflichten systemrelevanter Plattformen sind auch die Mitgliedstaaten zuständig, sofern die Kommission nicht ein Verfahren eröffnet.

Die Durchsetzungsbefugnisse der mitgliedstaatlichen Koordinatoren für digitale Dienste nach Art. 51 DSA sind weitreichend und umfassen das Betreten von Geschäftsräumen während üblicher Geschäftszeiten, die Beschlagnahme von Beweismitteln sowie die Information der Öffentlichkeit über laufende Verfahren und getroffene Bußgeldentscheidungen. Diese Befugnisse ermöglichen es den Behörden, effektiv gegen Verstöße vorzugehen und Transparenz zu schaffen. Art. 51 Abs. 3 UA 1 lit. b) DSA sieht bei hartnäckigen Verstößen gegen den DSA sogar die Möglichkeit vor, Dienste vorübergehend einzuschränken.³⁹

Das Sanktionssystem des DSA sieht auch empfindliche Geldbußen vor. Grundsätzlich müssen alle Sanktionen nach Art. 52 Abs. 2 DSA "wirksam, verhältnismäßig und abschreckend" sein, um eine effektive Durchsetzung der digitalen Diensteverordnung zu gewährleisten.⁴⁰ Nach Art. 52 Abs. 3 DSA können bei Pflichtverletzungen Geldbußen bis zu 6% des weltweiten Jahresumsatzes im vorangegangenen Geschäftsjahr verhängt werden.⁴¹ Für spezielle Verstöße wie die Bereitstellung unrichtiger, unvollständiger oder irreführender Informationen oder die Nichtduldung von Nachprüfungen sind Geldbußen von bis zu 1% des weltweiten Jahresumsatzes vorgesehen. Zusätzlich können Zwangsgelder von bis zu

³⁵ Zur Geltung des kartellrechtlichen Konzepts wirtschaftlicher Einheit als Grundprinzip der Binnenmarktregulierung vgl. *Denga, Zurechnung*, 2022, S. 203 ff., 328 f.; spezifisch im Kontext der Digitalmarktregulierung *Bauermeister/Schwamberger/König, Private Enforcement im Digitalen Binnenmarkt*, 2025, S. 128 ff.

³⁶ Dazu *Denga, Zurechnung*, 2022, S. 329 ff.; spezifisch im Kontext der Digitalmarktregulierung *Bauermeister/Schwamberger/König, Private Enforcement im Digitalen Binnenmarkt*, 2025, S. 128 ff.

³⁷ Zum Begriff des Aufsichtsrechts im Kontext des Bankwesens vgl. *Kümpel/Mülberr/Früh/Seyfried/Früh, Bankrecht und Kapitalmarktrecht*, 7. Aufl. 2025, Rn. 1.53 f.

³⁸ Bundesnetzagentur, Bundesnetzagentur wird zentrale Plattformaufsicht für Deutschland, 14.05.2024, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2024/20240514_DSC.html; s. auch *Müller, MMR* 2022, 1007 (1010).

³⁹ Dazu § 29 Digitale Dienste Gesetz.

⁴⁰ Vgl. dazu *ErwGr* 117, 144 VO (EU) 2022/2065.

⁴¹ Der DSA definiert den Begriff des Anbieters nicht, es ist aber davon auszugehen, dass bei der Umsatzberechnung das kartellrechtliche Konzept der wirtschaftlichen Einheit greift, dazu *Denga, Zurechnung*, 2022, S. 203 ff.

5% des durchschnittlichen weltweiten Tagesumsatzes oder der Tageseinnahmen nach Art. 52 Abs. 4 DSA verhängt werden.

Für sehr große Online-Plattformen und Suchmaschinen gelten spezielle Bestimmungen mit Geldbußen von bis zu 6% des weltweiten Jahresumsatzes nach Art. 74 Abs. 1 DSA und Zwangsgeldern von bis zu 5% der tagesdurchschnittlichen Einnahmen gemäß Art. 76 Abs. 1 DSA.

Während sich dies in der Theorie als gehaltvoller Durchsetzungsrahmen darstellt, stellen sich in der Praxis erhebliche Zweifel, die schon bei der überlagerten Verfahrensdauer bei auch einfachen Anträgen der Betroffenen beginnen.

Die Durchsetzung des DSA ist allerdings insbesondere seit dem Amtsantritt *Donald Trumps* 2025 zu einer hoch- und geopolitischen Angelegenheit geworden. Am 21. Februar 2025 veröffentlichte die Trump-Administration ein Memorandum, das amerikanische Tech-Unternehmen vor "Erpressung und unfairen Geldbußen aus dem Ausland" schützen soll, wobei explizit Zölle als Gegenmittel genannt werden. Darin heißt es deutlich, dass amerikanische Unternehmen "gescheiterte ausländische Volkswirtschaften" nicht länger durch "erpresserische Geldbußen und Steuern" stützen würden.⁴²

Plattform-Unternehmer wie *Elon Musk*, *Mark Zuckerberg* und *Tim Cook* haben sich dabei demonstrativ an die Seite Trumps gestellt, um europäische Regulierungen, namentlich den DSA, zu bekämpfen. So drohte bereits während des Wahlkampfs US-Vizepräsident *Vance* damit, die amerikanische NATO-Unterstützung davon abhängig zu machen, dass die EU nicht gegen X vorgeht.⁴³

Im Handelsstreit zwischen den USA und der EU könnte die Durchsetzung auch des Digital Markets Act⁴⁴ für US-Unternehmen wie *Alphabet*, *Meta* oder *Apple* auf Eis gelegt werden, berichtet das Wall Street Journal.⁴⁵ Dem Bericht zufolge zirkuliert im Büro des US-Handelsbeauftragten der Entwurf eines "Abkommens über gegenseitigen Handel", das neben dem Digitalsektor auch CO₂-Grenzabgaben und andere Bereiche erfasst. Inzwischen wird der DSA in Arbeitsberichten des US House of Representatives unverhohlen als *Zensurgesetz* dargestellt.⁴⁶

Insgesamt scheint die Befürchtung begründet, dass die europäischen Digitalgesetze zur Verhandlungsmasse zwischen EU und Trump-Regierung werden könnten, um Zölle auf europäische Güter, etwa Weine, Stahl oder Kraftfahrzeuge zu verhindern – und damit aufsichtsrechtlich nicht durch die Europäische Kommission oder die mitgliedstaatlichen Stellen durchgesetzt werden. Dies stünde klar in Widerspruch zum Ziel der Digitalen Souveränität der Europäischen Union und ihrer Bürger (dazu bereits oben, D.). Rein ökonomische Erwägungen vermögen

⁴² *The White House*, Fact Sheet: President Donald J. Trump Issues Directive to Prevent the Unfair Exploitation of American Innovation, February 21, 2025, para. 1.

⁴³ *Gehrke SZ* 31.03.2025, abrufbar unter: <https://www.sz-dossier.de/tiefgaenge/2025-03-31-die-meinungsfreiheit-der-dsa-und-raum-fuer-verbesserung-ff27f597>.

⁴⁴ EU-Verordnung (EU) 2022/1925].

⁴⁵ *Hancock WSJ* 03.06.2025, abrufbar unter: <https://www.wsj.com/tech/meta-to-challenge-eu-tech-crackdown-on-platforms-8f10f1e6>.

⁴⁶ Interim Staff Report of the *Committee on the Judiciary of the U.S. House of Representatives*, THE FOREIGN CENSORSHIP THREAT: HOW THE EUROPEAN UNION'S DIGITAL SERVICES ACT COMPELS GLOBAL CENSORSHIP AND INFRINGES ON AMERICAN FREE SPEECH, July 25, 2025, abrufbar unter: chrome-extension://efaidnbmnnnibpcjpcglclefindmkaj/https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/2025-07/DSA_Report%26Appendix%2807.25.25%29.pdf.

nicht das Recht zu beugen, so dass die EU-Kommission und auch die Koordinatoren für digitale Dienste sich nicht pauschal auf ihr Einschreitermessen zurückziehen können. Vielmehr führt das Effektivitätsinteresse europäischer Digitaler Souveränität zu einer erheblichen Ermessensreduktion der beauftragten Behörden, potentiell bis hin zur Aufgreifpflicht.⁴⁷ Umso mehr jedoch kommt bei einem Ausfall der Aufsichtsmechanismen für die Effektivität der europäischen Digitalregulierungen, namentlich des DSA, auf die Möglichkeit eines Private Enforcement an:

2. Private Enforcement des DSA

a) Effet utile und Komplementarität von Privat- und Aufsichtsrecht

Die Idee des Private Enforcement europäischen Rechts im digitalen Binnenmarkt reflektiert eine paradigmatische Erweiterung traditioneller Durchsetzungsmechanismen des Unionsrechts. Während klassische Enforcement-Modelle primär auf staatliche Akteure und die Europäische Kommission als zentrale Durchsetzungsinstanzen setzen, ermöglicht Private Enforcement eine dezentrale Rechtsdurchsetzung durch private Akteure, insbesondere zivilgesellschaftliche Organisationen, Verbraucherverbände und betroffene Nutzer. Private Enforcement fungiert dabei sowohl als Komplement zur behördlichen Aufsicht als auch als demokratisches Korrektiv gegen potentielle Vollzugsdefizite staatlicher Stellen – Privatrecht und Aufsichtsrechts sind sich dieser Weise gegenseitig „Auffangordnungen“. ⁴⁸ Zentral ist der Gedanke des *effet utile* aus Art. 4 Abs. 3 EUV, ⁴⁹ gerade dort wo die öffentliche Durchsetzung fraglich erscheint.⁵⁰

Die rechtsdogmatische Herausforderung liegt in der Gewährleistung kohärenter Rechtsdurchsetzung bei gleichzeitiger Wahrung der institutionellen Balance zwischen supranationaler, nationaler und privater Enforcement-Ebene, wobei die Effektivität dieses hybriden Modells maßgeblich von der prozeduralen Ausgestaltung der Beschwerdemechanismen und der Koordination zwischen den verschiedenen Durchsetzungsakteuren abhängt.

Ein europarechtliches Spezifikum liegt in der kompetenziellen Trennung der Durchsetzungsebenen, der EuGH gibt den Mitgliedstaaten lediglich auf, dass privatrechtliche Sanktionen „wirksam, verhältnismäßig und abschreckend“ sein müssen.⁵¹ Das Haftungsrecht drängt sich hierbei als Schlüsselinstrument auf, sowohl wegen seiner Kompensations- als auch seiner Präventionsfunktion.⁵²

⁴⁷ Zur analogen Frage im Kartellrecht monographisch *Dogs*, Die Verpflichtung der EU-Kommission zum Einschreiten gegen unternehmerische Wettbewerbsverstöße, 2022; zum Unabhängigkeitsdefizit des Europäischen Gremiums für digitale Dienste, *Schnidrig* ZUM 2025, 584.

⁴⁸ Hoffmann-Riem/Schmidt-Aßmann/Hoffmann-Riem, Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen, 1996, S. 261, S. 290 f..

⁴⁹ Zentral hierfür EuGH v. 17.9.2002 – C-253/00, ECLI:EU:C:2002:497 – *Muñoz*, – Rn. 30; eingehend *Poelzig*, Normdurchsetzung durch Privatrecht, 2012, S. 77 ff., 208 ff.; mit einer historischen Einordnung bis hin zum Recht des digitalen Binnenmarkts vgl. Bauermeister/Schwamberger/Pauer, Private Enforcement im Digitalen Binnenmarkt, 2025, S. 1-9; zur Kritik im Schrifttum an einer zu pauschalen Anwendung s. nur *Schmolke* NZG 2016, 721 (728).

⁵⁰ Vgl. EuGH v. 20.9.2001 – C-453/99, ECLI:EU:C:2001:465 (Courage und Crehan) – Rn. 26; *Heinze*, Schadensersatz im Unionsprivatrecht, 2017, S. 521 ff.

⁵¹ EuGH v. 2.10.1991 – C-7/90, ECLI:EU:C:1991:363 (Paul Vandevenne) – Rn. 11; v.10.7.1990 – C-326/88, ECLI:EU:C:1990:291 (Anklagemyndigheden) – Rn. 17; *Poelzig*, Normdurchsetzung durch Privatrecht, 2012, S. 362.

⁵² S. nur *Heinze*, Schadensersatz im Unionsprivatrecht, 2017, S. 539 ff.; zu den ökonomischen Arbeiten bereits die Nachweise in Fn. 23; zu den Unterschieden in den mitgliedstaatlichen Schadensrechten vgl. Bauermeister/Schwamberger/Messner-Kreuzbauer, Private Enforcement im Digitalen Binnenmarkt, 2025, S. 59 ff.

b) Voraussetzungen des Private Enforcement

Während über die vorgenannten Prämissen weitgehend Einigkeit besteht, ist doch noch nicht genau geklärt, wann genau Private Enforcement im Wege des Schadensersatzrechts greifen kann. Außerhalb der geschriebenen Normen, wie etwa in der Kartellschadensersatzrichtlinie⁵³, ist dies dogmatisch ungesichertes Terrain.⁵⁴ Unangefochten dürfte noch das Erfordernis einer unmittelbaren Anwendung der Norm sein,⁵⁵ die jedoch bei dem überwiegenden Verordnungscharakter des Europäischen Digitalmarktrechts gegeben ist. Problematisch ist hingegen bereits das Erfordernis einer individuellen Anspruchsberechtigung,⁵⁶ die jedenfalls seit dem *Thermofenster*-Urteil des EuGH weit relativiert sein dürfte.⁵⁷ Dort hatte der EuGH, wohl auf Hintergrund der rechtspolitischen Aufladung des Verfahrens im Zusammenhang mit Dieselgate, eine an der deutschen Schutzgesetzdoktrin ausgerichtete Auslegung unternommen und den Individualschutz der Typengenehmigungsverordnung 715/2007 bejaht, obwohl diese ihrem Wortlaut nach auf ein hohes Umweltschutzniveau ausgerichtet ist. Wenn jedoch für die Qualifikation einer Norm für Private Enforcement auf ihre „grundlegende Bestimmung“⁵⁸ und ihre Bedeutung für die Wettbewerbsordnung in der Europäischen Union⁵⁹ abgestellt wird, so trifft dies auf Hintergrund der Digitalen Souveränität als zentralem Auslegungstopos (oben, D.) auf eine erhebliche Zahl von Normen des Europäischen Digitalrechts zu, namentlich auf die zentralen Präventions- und Garantiemechanismen des DSA. Eine Ausschluss des Private Enforcement im Wege des Haftungsrechts ist im DSA weder ausdrücklich erwähnt noch folgt dieser aus dem Vorrang anderer privatrechtlicher Instrumente;⁶⁰ ganz im Gegenteil ordnet der DSA das Private Enforcement in Art. 54 ausdrücklich an.⁶¹

„Nutzer haben das Recht, im Einklang mit dem EU-Recht und nationalen Recht Schadenersatz von Anbietern von Vermittlungsdiensten für etwaige Schäden oder Verluste zu fordern, die aufgrund eines Verstoßes dieser Anbieter gegen die Verpflichtungen gemäß dieser Verordnung entstanden sind.“

⁵³ EU-Richtlinie 2014/104/EU; dazu *Kersting/Preuß*, Umsetzung der Kartellschadensersatzrichtlinie (2014/104/EU) - Ein Gesetzgebungsvorschlag aus der Wissenschaft, 2015, S. 2, 156, 183 u.a.

⁵⁴ Dazu nur der Überblick bei *Heinze*, Schadensersatz im Unionsprivatrecht, 2017, S. 518 ff.; s. auch *Wagner JZ* 2018, 130 (132); *Mörsdorf RabelsZ* 83 (2019), 797 (817 ff.); *ähnlich Ebers, Rechte, Rechtsbehelfe und Sanktionen im Unionsprivatrecht*, 2016, S. 52; *Cless, Unionsrechtliche Vorgaben für eine zivilrechtliche Haftung bei Marktmissbrauch*, 2018, S. 76.

⁵⁵ S. nur *Wagner AcP* 206 (2006), 352 (418).

⁵⁶ Auch dazu *Heinze*, *ibid.*, S. 520 f.

⁵⁷ EuGH NJW 2023, 1111 Rn. 68 ff., 85; kritisch dazu *MüKoBGB/Wagner*, 9. Aufl. 2024, BGB § 823 Rn. 638: „beunruhigend unklar“.

⁵⁸ Vgl. EuGH 20.9.2001, Rs. C-453/99, Slg. 2001, I-6297 Rn. 20 – *Courage*; so auch *Weyer ZEuP* 2003, 318 (335): „Dies [Verweis in *Courage* auf den grundlegenden Charakter des Art. 101 AEUV] lässt die Möglichkeit offen, die Neukonzeption auf grundlegende Vorschriften des EG-Vertrages zu beschränken.“

⁵⁹ EuGH 20.9.2001, Rs. C-453/99, Slg. 2001, I-6297 Rn. 27 – *Courage*: „können Schadensersatzklagen vor den nationalen Gerichten wesentlich zur Aufrechterhaltung eines wirksamen Wettbewerbs in der Gemeinschaft beitragen“; EuGH 17.9.2002, Rs. C-253/00, Slg. 2002, I-7289 Rn. 31 – *Muñoz*: „sind Klagen von Konkurrenten vor nationalen Gerichten besonders geeignet, wesentlich zur Sicherung eines lauterer Handels und der Markttransparenz in der Gemeinschaft beizutragen“; vgl. auch *Riesenhuber*, Europäisches Vertragsrecht, 2006, Rn. 237, für kapitalmarktrechtliche Wohlverhaltenspflichten.

⁶⁰ Zu diesen Negativkriterien vgl. *Heinze*, *ibid.*, S. 524 ff.

⁶¹ Dazu etwa *Bauermeister/Schwamberger/Zurth*, Private Enforcement im Digitalen Binnenmarkt, 2025, S. 28 f.; s. auch *Weigl/Wittershagen BRZ* 2/2024, 106 ff.

c) Zivilrechtliche Anknüpfungspunkte

Bejaht man die Eignung der Normen des DSA für ein haftungsrechtliches Private Enforcement, so können sie über drei dogmatische Konstruktionen des deutschen Zivilrechts wirken,⁶² die Schutzgesetzdoktrin nach § 823 Abs. 2 BGB, die Sorgfaltspflichtendoktrin unter § 823 Abs. 1 BGB und die Nebenpflichtdoktrin nach § 241 Abs. 2 BGB. Während sich gerade in Folge der *Thermofenster*-Entscheidung des EuGH die Diskussion auf die Schutzgesetzqualität von Normen unmittelbar anwendbaren EU-Rechts konzentriert, wird zu oft übersehen, dass diese auch die Sorgfaltspflichten konkretisieren. Bei der Verletzung der in § 823 Abs. 1 BGB enumerierten Rechtsgüter kann deshalb auf die Schutzpflichten (im Unternehmenskontext auch: „Organisationspflichten“⁶³) abgestellt werden, wobei das Verhalten von Leitungspersonal und Repräsentanten iSd. § 31 BGB relevant ist;⁶⁴ der Umweg über § 823 Abs. 2 oder § 826 BGB bleibt nur bei reinen Vermögensschäden erforderlich.⁶⁵ Sofern eine vertragliche Beziehung zwischen der Plattform und dem geschädigten Nutzer besteht, in Form des Plattformnutzungsvertrags,⁶⁶ können die Normen des DSA zudem die geschuldeten Nebenpflichten konkretisieren.⁶⁷ Neben dem haftungsrechtlichen Enforcement kommt auch die Geltendmachung von Unterlassungsansprüchen analog § 1004 BGB in Betracht.⁶⁸ Bei der Aktivierung der deutschen Haftungsnormen wird es fraglos zu Beweisproblemen kommen; sie müssen indes im Lichte der Regulierungsziele des DSA ausgelegt werden, um diesem zu praktischer Wirksamkeit zu verhelfen (bereits oben, D.). Dies kann insbesondere bedeuten, dass die Grundsätze der Produzentenhaftung über die Beweislastumkehr greifen (dazu noch unten, H. VII.).

d) Aktiv- und Passivlegitimation

Das Private Enforcement wirft auch die Frage nach der Aktiv- und Passivlegitimation auf. Aktivlegitimiert können neben den Geschädigten selbst auch Verbände sein. Kollektive Rechtswahrnehmung wird durch das Verbraucherrechtgedurchsetzungsgesetz (VDuG), das Unterlassungsklagengesetz (UKlaG) und das Musterfeststellungsklagengesetz (MuFKG) ermöglicht. Die Aktivlegitimation von Verbänden setzt nach § 3 Abs. 1 UKlaG voraus, dass diese als rechtsfähige Vereine organisiert sind, deren satzungsgemäße Aufgaben die Förderung gewerblicher oder selbständiger beruflicher Interessen umfassen oder die nach § 4 UKlaG als qualifizierte Einrichtungen anerkannt sind. Zusätzlich müssen sie gemäß § 3 Abs. 3 UKlaG mindestens 75 Mitglieder oder mindestens einen Verband mit 75 Mitgliedern als Mitglied haben, wobei bei Verbraucherschutzverbänden nach § 4 UKlaG eine Eintragung in die Liste qualifizierter Einrichtungen beim Bundesamt für Justiz erforderlich ist. Art. 86 DSA bestätigt das Recht der

⁶² Zur Relevanz des nationalen Schadensrechts s. etwa bei Heinze/Steinrötter/Denga/Achleitner, EU Platform Law, 2024, S. 48 f.

⁶³ Dazu m.w.N. MüKoBGB/Wagner, 9. Aufl. 2024, BGB § 823 Rn. 111; Denga, Zurechnung, 2022, S. 91 ff.; grundlegend für das Konzept des Verbunddelikts Kleindiek, Deliktshaftung und juristische Person, 1997; dazu zuletzt auch König, Unternehmenshaftung, 2023.

⁶⁴ Sogar noch weiter, ohne Bezug zum Personal des Unternehmens, König, Unternehmenshaftung, 2023, S. 541 ff.

⁶⁵ So etwa im Kontext des „Dieselskandals“ der BGH, Urteil vom 25.5.2020 – VI ZR 252/19.

⁶⁶ Zu diesen Röhrich/Graf von Westphalen/Haas/Mock/Wöstmann HGB/Bernzen/Specht-Riemenschneider, 6. Aufl. 2023.

⁶⁷ Zum Sonderproblem der Durchsetzung von Community Standards aus AGB Holznaegel CR 2023, 539-545.

⁶⁸ Zum allgemeinen Persönlichkeitsrecht im Rahmen von § 1004 BGB s. MüKoBGB/Raff, 9. Aufl. 2023, BGB § 1004 Rn. 37f.

Nutzer, sich bei der Durchsetzung ihrer Rechte durch Verbände vertreten zu lassen – ein essentielles Instrument für die Verwirklichung digitaler Souveränität in asymmetrischen Machtlagen der Plattformökonomie.

Wenngleich Art. 54 DSA einen Entschädigungsanspruch dem Wortlaut nach gegenüber den Anbietern von Vermittlungsdiensten verbürgt, schließt dies eine unmittelbare Haftung des Personal nicht aus, die nachfolgend erörtert werden soll.

II. Persönliche Haftung des Personals

Die Effektuierung der Plattformpflichten erfolgt nicht alleine durch die aufsichtsrechtliche und privatrechtliche Haftung der Anbieter von Vermittlungsdiensten, sondern auch durch die persönliche Haftung ihres Personals. Hier liegt eines der grundsätzlichen Paradigmen der Intermediärsregulierung im Internet – die Diffusion von Unternehmen als geistige Konstrukte und die weltweite Verbreitung von Plattforminhalten wird durch die persönliche Lokalisierung ihres Personals kompensiert.⁶⁹ So haften auch für systemische Risiken sehr wohl Individuen persönlich.⁷⁰ Dargestellt wird hier schematisch⁷¹ die Haftung von Organen und handelndem Personal unter deutschem⁷² Privatrecht⁷³.

1. Gesellschaftsrechtliche Organhaftung

Die gesellschaftsrechtliche Organhaftung nach § 43 GmbHG und § 93 AktG konstituiert eine reine Innenhaftung der Geschäftsleitung gegenüber der Gesellschaft, die dem Schutz des Gesellschaftsvermögens dient. Zugleich erfolgt auch eine Konzentration der organschaftlichen Sorgfaltspflichten gegenüber der Gesellschaft, um einen Wettlauf der Geschädigten um die persönliche Haftung der Organe zu vermeiden;⁷⁴ stattdessen können Dritte aus Schäden, die sie durch organisationsbezogene Fehler des Leitungspersonals einer Gesellschaft erleiden, zunächst nur gegenüber der Gesellschaft liquidieren – zumindest sofern dem Leitungspersonal nicht ein eigenhändiges Delikt nachgewiesen werden kann (dazu noch ausf. unten, F. II. 2.).⁷⁵

Das Leitungspersonal hat bei seiner Geschäftsführung die „Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters“ walten zu lassen (vgl. § 43 GmbHG; § 93 AktG). Der Sorgfaltsmaßstab orientiert sich an der „Business-Judgment-Rule“,⁷⁶ dernach eine unternehmerische

⁶⁹ Siehe nur *Goldsmith/Wu*, Who controls the internet?, 2006, S. 79 ff.; ein allgemeines Prinzip der Haftungsbeschränkung von Leitungspersonal oder der Haftungskonzentration auf die Verbandsperson ist im Gesetz nicht zu erkennen und unter Effektivitätsgesichtspunkten auch nicht anzuerkennen. Zur beschränkten Reichweite der Haftungsbeschränkung von Körperschaften, vgl. *Pistor*, Code of Capital, 2019, S. 60 ff.; zur persönlichen Verantwortung als Grundlage der Marktwirtschaft vgl. etwa *Euken*, Grundsätze der Wirtschaftspolitik, 6. Aufl. 1990, S. 279 ff.; im Grundsatz auch *Friedman*, Free to choose: A personal statement, 1980, S. 138; zur Rechtslage in den USA, sogar mit Diskussion einer verschuldensunabhängigen Mithaftung des Leitungspersonals für Delikte des Unternehmens mit zahlreichen Nachweisen *Anderson/Gerding*, Directors' personal liability for corporate fault : a comparative analysis, 2008, S. 301 ff.

⁷⁰ Dies gerade entgegen der Diffusion von Verantwortung bei komplexen, systemischen Risikolagen, dazu etwa aus soziologischer Perspektive *Beck*, Gegengifte: Die Organisierte Unverantwortlichkeit, 1988, S. 218 f.; zur dogmatischen Haftungs begründung im Einzelnen noch unten, F. II. 2.

⁷¹ Eine Prüfung der Anspruchsgrundlagen im Einzelfall bleibt erforderlich.

⁷² Dazu hier unter 3.; eine international-privatrechtliche Einordnung im Einzelfall bleibt erforderlich.

⁷³ Die strafrechtliche Verantwortlichkeit, insbesondere aus Garantenstellung oder Beihilfe, bleibt hier unberücksichtigt.

⁷⁴ *Hopt/Hopt*, 44. Aufl. 2025, HGB Anh. § 179 Rn. 19; vgl. *MHLS/Ziemons*, 4. Aufl. 2023, GmbHG § 43 Rn. 368; *BeckOGK/Fleischer*, Stand: 01.06.2025, AktG § 93 Rn. 384.

⁷⁵ *MüKoBGB/Wagner*, 9. Aufl. 2024, BGB § 823 Rn. 155, 159.

⁷⁶ Grundlegend BGH II ZR 175/95 – ARAG/Garmenbeck; kodifiziert in § 93 Abs. 1 Satz 2 AktG.

Entscheidung von Leitungspersonal keiner gerichtlichen Prüfung zugänglich ist und damit keine Haftung begründen kann, wenn (1) kein eigenes relevantes Interesse an der Entscheidung vorliegt (disinterested judgement), (2) die Entscheidung hinreichend informiert vorbereitet ist (informed judgement) und (3) im besten Interesse des Unternehmens gehandelt wird (rational belief und good faith).⁷⁷

Die geschuldeten konkreten Maßnahmen der Leitungsorgane umfassen zunächst die allgemeine Legalitätspflicht zur Einhaltung aller Gesetze,⁷⁸ worunter natürlich auch die DSA-Bestimmungen fallen. Diese fundamentale Pflicht erstreckt sich auf die gesamte Unternehmenstätigkeit und erfordert eine kontinuierliche Überwachung der Rechtskonformität aller Geschäftsprozesse. Darüber hinaus ist die Einrichtung einer funktionsfähigen Compliance-Organisation (über Art. 40 DSA hinaus, als „Legalitätskontrollpflicht“) verpflichtend,⁷⁹ wobei insbesondere die Schulung in kritischen Rechtsmaterien wie der DSA-Compliance essentiell ist. Dabei muss die Geschäftsleitung eine an Legalität ausgerichteten Unternehmenskultur sicherstellen, die auf die Verhinderung von DSA-Verstößen und Persönlichkeitsverletzungen ausgerichtet ist. Diese kulturelle Dimension der Compliance erfordert nicht nur formale Regelwerke, sondern eine gelebte Rechtskultur, die alle Unternehmensebenen durchdringt, vom *tone from the top*⁸⁰ über die Einrichtung eines Whistle-Blowing-Systems⁸¹ bis hin zum sachgerechten Umgang mit konkreten Compliance-Verstößen im „Dreiklang“⁸² von *Aufklären – Abstellen – Ahnden*.

Nach der *ARAG/Garmenbeck*-Rechtsprechung des BGH gilt, dass der Aufsichtsrat aufgrund seiner Aufgabe, die Tätigkeit des Vorstands zu überwachen und zu kontrollieren, die Pflicht hat, das Bestehen von Schadensersatzansprüchen der AG gegenüber Vorstandsmitgliedern eigenverantwortlich zu prüfen, wobei im Rahmen der Prüfung der dem Vorstand zuzubilligende weite Handlungsspielraum zu berücksichtigen ist.⁸³ Diese Rechtsprechung ist auf andere Rechtsformen übertragbar.⁸⁴ In ultima ratio kann die Durchsetzung per *actio pro socio* erfolgen, wenn sowohl Vorstand als auch Aufsichtsrat ihre Pflichten vernachlässigen.

2. Unmittelbare Haftung des handelnden Personals

In Betracht kommt die Verwirklichung eines eigenhändigen Delikts durch Personal der Plattform, nach § 823 Abs. 1 BGB. Anknüpfungspunkt der Rechtsgutsverletzung kann das allgemeine Persönlichkeitsrecht sein,⁸⁵ welches etwa durch personenbezogene Diffamation in Nutzerbeiträgen, die auf einer Social Media Plattform veröffentlicht werden, verletzt wird.

⁷⁷ M.w.N. MüKoAktG/Spindler, 6. Aufl. 2023, AktG § 93 Rn. 44.

⁷⁸ M.w.N. MüKoAktG/Spindler, 6. Aufl. 2023, AktG § 93 Rn. 89 ff.

⁷⁹ LG München I 5HK O 1387/10 Rn. 93 – Siemens/Neubürger; BeckOGK/Fleischer, Stand: 01.06.2025, AktG § 91 Rn. 47.

⁸⁰ MüKoGmbHG/Fleischer, 4. Aufl. 2023, GmbHG § 43 Rn. 190-193

⁸¹ Dazu Forgó/Helfrich/Schneider Betr. Datenschutz-HdB/Chr. Schröder, 3. Aufl. 2019, Teil VI. Kap. 3 Rn. 48 ff.; s. auch Gerdemann, Europe's New Whistleblowing Laws, 2023, S. 7.

⁸² Dazu Moosmayer Compliance, 4. Aufl. 2021, Rn. 4.

⁸³ BGH II ZR 175/95.

⁸⁴ Lutter/Hommelhoff/Kleindiek GmbHG, 21. Auflage 2023, GmbHG § 43 Rn. 23; Scholz/Verse GmbHG, 13. Aufl. 2025, GmbHG § 43 Rn. 71.

⁸⁵ Dazu MüKoBGB/Wagner, 9. Aufl. 2024, BGB § 823 Rn. 220; s. auch Jauernig/Teichmann, 17. Aufl. 2018, BGB § 823 Rn. 65.; BVefG NJW 2006, 595.

Der Betrieb der Social Media Plattform ist haftungsbegründend kausal für eine derartige Persönlichkeitsverletzung; da im deutschen Haftungsrecht keine *causa proxima* erforderlich ist,⁸⁶ vgl. § 830 Abs. 1 BGB, reicht zunächst jeder Verursachungsbeitrag für den Plattformbetrieb hin.

Die zentrale Frage ist freilich, ob das betreffende Personal selbst ein Verschuldensvorwurf nach § 276 BGB trifft. Die Frage nach vorsätzlichem oder fahrlässigen Handeln geht dabei auf im Verstoß gegen Sorgfaltspflichten (auch: Verkehrssicherungspflichten); steht dieser fest, so ist zugleich auch ein fahrlässiges Verhalten gegeben.⁸⁷ Insbesondere können so auch mittelbare Rechtsgutsverletzungen in weit gespannten Kausalketten zugerechnet werden, so dass sich die für das Strafrecht prägende Unterscheidung zwischen Tun und Unterlassen erübrigt.⁸⁸

Die Sorgfaltspflicht ist eine generelle Verhaltensvorgabe, nach der jeder Teilnehmer im Rechtsverkehr die Rechtsgüter anderer wahren muss. Diese „Generalformel“ wird kontextspezifisch aufgeladen und konkretisiert.⁸⁹

Die Pflichten des DSA konkretisieren den Gehalt der allgemeinen Sorgfaltspflicht, selbst wenn sie unmittelbar an die Plattform und nicht an deren Personal adressiert sind. Die Sorgfaltspflicht des Personals ist nicht mit jener der Gesellschaft identisch; es bedarf – wie immer bei öffentlich-rechtlichen Vorgaben – vielmehr einer normativen Verdichtung des Aufsichtsprogramms hin zu einem spezifischen eigenen Pflichtengehalt für das Personal.⁹⁰ Eine *mittelbare* Wirkung gegenüber dem Personal kann gerade dem DSA jedoch durchaus zugeschrieben werden, da der Rechtsakt objektiv die Qualität der Vermittlungsdienstleistung definiert. Die besonders akuten öffentlichen Interessen der Digitalmarktregulierung (zu diesen unter D.) und insbesondere das sehr konkrete und daher vorhersehbare Pflichtenprogramm des DSA vermögen normativ eine nach außen wirkende Garantenpflicht des Personals eines Vermittlungsdienstes für die Einhaltung der Vorgaben des DSA zu begründen.

Dabei spricht auch das haftungsrechtliche Nutzen-Lasten-Paradigma für eine Bindung des Personals von Vermittlungsdiensten an das Pflichtenprogramm des DSA. Denn jeder, der bei einem Vermittlungsdienst angestellt ist, also die Nutzen aus dessen Geschäftstätigkeit zieht, hat auch für dessen Compliance einzustehen.⁹¹ Dies gilt freilich nur im Rahmen der eigenen Zuständigkeit, innerhalb der eigenen „Sphäre“, die ihre Grenze an der objektiven⁹² Erkennbarkeit von Gefahren findet.⁹³ Hier können sich im Einzelfall diffizile Abgrenzungsfragen ergeben, namentlich bei institutioneller Ressortbildung,⁹⁴ wobei es für die Geschäftsleitung bei einer Überwachungspflicht bleibt.⁹⁵ Die Delegation von Aufgaben auf

⁸⁶ MwN Denga, Zurechnung, 2022, S. 101.

⁸⁷ Grüneberg BGB, 83. Aufl. 2024, BGB § 823 Rn. 175; MüKoBGB/Wagner, 9. Aufl. 2024, BGB § 823 Rn. 497.

⁸⁸ Medicus/Petersen, Bürgerliches Recht, 30. Aufl. 2025, § 25.

⁸⁹ Zur Pflichtenbegründung als Zurechnungsoperation Denga, Zurechnung, 2022, S. 304 ff.

⁹⁰ Analog, zur persönlichen Haftung für die Verletzung kapitalmarktrechtlichen Pflichten s. etwa BGH III ZR 105/22 (= BKR 2024, 325 m.Anm. Denga); vgl. auch m.w.N. Kleindieck, Deliktshaftung und juristische Person, 1997, S. 391 f.

⁹¹ Zum Nutzen-Lasten-Paradigma als Haftungsgrund vgl. mwN Denga, Zurechnung, 2022, S. 79 f.; Verantwortung wird im Zuge der Corporate Social Responsibility (CSR) als Grundbedingung der Marktwirtschaft verstanden, vgl. etwa KOM (2011) 681 endg., S. 7; zum Begriff der CSR s. nur Fleischer/Kalls/Vogt/Fleischer, Corporate Social Responsibility, 2017, S. 1-38; s. auch Schnitker zfpf 2017, S. 246f.; grundlegend für den Rahmen der freiheitlichen Marktwirtschaft Eucken, Grundsätze der Wirtschaftspolitik, 6. Aufl. 1990, S. 279.

⁹² Zum objektiven Maßstab für Sorgfaltspflichtverletzungen: MüKoBGB/Grundmann, 9. Aufl. 2022, BGB § 276 Rn. 55 f.

⁹³ Zu diesem Grundgedanken zivilrechtlicher Verantwortung Canaris, Die Vertrauenshaftung im Deutschen Privatrecht, 1971, § 38 III; im Kontext der Lieferkettenhaftung auch MüKoBGB/Wagner, 9. Aufl. 2024, § 823 Rn. 123 ff.; im Kontext der KI Haftung Denga CR 2018, 69 (72); grundlegend für den Rahmen der freiheitlichen Marktwirtschaft Hayek, Die Verfassung der Freiheit, 3. Aufl. 1991, S. 102.

⁹⁴ Zur deliktsrechtlichen Relevanz der Ressortbildung vgl. Mascherini, Die Ressortverteilung als Instrument zur Enthaftung der GmbH-Geschäftsführung, 2021, S. 26f.; s. auch Wilhelmi, Risikoschutz durch Privatrecht, 2009, S. 219.

⁹⁵ S. nur Bachmann, Gutachten E für den 70. DJT, 2014, S. E 42.

nachgeordnete Ebenen entbindet nicht von der allgemeinen Legalitätskontrollpflicht, sondern verpflichtet auf die Überwachung des Delegationsempfängers.⁹⁶ Der Grundsatz bleibt also die Verantwortung der Leitungsorgane, die bei Verletzung ihrer Legalitätskontrollpflicht mit den unmittelbar Handelnden gesamtschuldnerisch haften, §§ 830, 840 BGB.

Wenngleich die Feststellung einer konkreten Sorgfaltspflichtverletzung stets Frage des Einzelfalls ist, sind als typische Anknüpfungspunkte bei einer Tätigkeit für Vermittlungsdienstleister denkbar:

- Die Nichtbeachtung oder Unterdrückung von Meldungen rechtswidriger Inhalte, wegen Art. 16 f. DSA.
- Unterlassen der Löschung rechtswidriger Inhalte, von denen Kenntnis genommen wird, wegen Art. 6 DSA.
- Manipulatives Design des Nutzerinterfaces, wegen Art. 25 DSA.
- Zulassung profilspezifischer Werbung gegenüber Minderjährigen, wegen Art. 28.
- Versäumnis der Einrichtung einer adäquaten Compliance-Abteilung, nach Art. 41 DSA.
- Unterlassen der Meldung rechtswidriger Aktivitäten innerhalb des Unternehmens, etwa gegenüber der Compliance-Abteilung

Grauzonen der Sorgfaltspflicht ergeben sich insbesondere bei der Fehleinschätzung von Inhalten, zumal diese einer komplexen grundrechtlichen Interessenlage unterliegen. Hier schuldet das befassete Personal in der Regel jedoch die Konsultation der Vorgesetzten oder der Compliance-Abteilung.

Während sich die Widerrechtlichkeit aus der Rechtsgutsverletzung als solcher ergibt,⁹⁷ und auch die haftungsausfüllende Kausalität keinen besonderen Problemen unterliegt, ergeben sich einzelfallabhängige Fragen bei der Schadensberechnung, wobei die nationale Schadensdogmatik unter dem Vorzeichen der Effektivität und Äquivalenz der Umsetzung von Europarecht zu lesen ist.⁹⁸

3. Anwendbarkeit deutschen Rechts und Zuständigkeit deutscher Gerichte

Sofern eine Person mit gewöhnlichem Aufenthaltsort in Deutschland durch Inhalte betroffen ist, die über eine Social Media Plattform verbreitet werden, ist sowohl deutsches Zivilrecht anwendbar, als auch die Zuständigkeit deutscher Gerichte eröffnet.

Maßgeblich für die Beurteilung der Frage, ob bei einer über eine Social-Media-Plattform verbreiteten Persönlichkeitsrechtsverletzung deutsches Zivilrecht anwendbar ist und deutsche Gerichte international zuständig sind, ist zunächst, ob ein hinreichender Inlandsbezug vorliegt. Dies ist dann der Fall, wenn eine Person mit gewöhnlichem Aufenthaltsort in Deutschland durch die beanstandeten Inhalte konkret betroffen ist. In einem solchen Fall realisiert sich der geltend gemachte Schaden – namentlich die Verletzung des allgemeinen Persönlichkeitsrechts – im Inland. Damit ist sowohl im Rahmen des internationalen Privatrechts als auch im Bereich des internationalen Zivilverfahrensrechts ein hinreichender Anknüpfungspunkt zum deutschen Rechtsraum gegeben.

Hinsichtlich des anwendbaren Rechts ist zunächst zu berücksichtigen, dass die Verordnung (EG) Nr. 864/2007 (Rom II-VO) gemäß Art. 1 Abs. 2 lit. g auf Verletzungen des Persönlichkeitsrechts ausdrücklich keine Anwendung findet. Damit bestimmt sich die Anknüpfung nicht nach der Rom II-VO, sondern

⁹⁶ Aus dem aktienrechtlichen Schrifttum Grigoleit/*Grigoleit* AktG, 2. Aufl. 2020, § 77 Rn. 3; Grigoleit/*Koch* AktG, 2. Aufl. 2020, § 76 Rn. 8; *Langenbucher* ZHR 2023, 187, (725 ff).

⁹⁷ MüKoBGB/*Wagner*, 9. Aufl. 2024, BGB § 823 Rn. 5.

⁹⁸ Zum autonomen Schadensbegriff Hofmann/*Raue/Raue*, 2023, DSA Art. 54 Rn. 10, 26, 4; näher dazu Bauermeister/*Schwamberger/Hornkohl*, Private Enforcement im Digitalen Binnenmarkt, 2025, S.

nach dem nationalen IPR unter Art. 40-42 EGBGB.⁹⁹ Nach dessen Maßgabe ist bei deliktischen Ansprüchen auf den Ort des Erfolgs abzustellen. In ständiger höchstrichterlicher Rechtsprechung wird bei Verletzungen des Persönlichkeitsrechts über das Internet der Erfolgsort auch dort verortet, wo der Eingriff in die Rechtsgüter des Betroffenen spürbar wird, d. h. wo sich die Persönlichkeitsrechtsverletzung konkret auswirkt.¹⁰⁰ Ist der gewöhnliche Aufenthalt der betroffenen Person in Deutschland, so tritt der Schaden regelmäßig auch dort ein. Somit ist deutsches Deliktsrecht, insbesondere § 823 Abs. 1 BGB in Verbindung mit dem durch Art. 1 Abs. 1 GG grundrechtlich geschützten allgemeinen Persönlichkeitsrecht, anwendbar.

Auch die internationale Zuständigkeit deutscher Gerichte ist in diesen Fällen eröffnet. Maßgeblich ist insoweit die Verordnung (EU) Nr. 1215/2012 (Brüssel Ia-VO), insbesondere Art. 7 Nr. 2. Danach kann eine Person in einem anderen Mitgliedstaat verklagt werden, wenn dort das schädigende Ereignis eingetreten ist oder eintreten droht. Der Begriff des "schädigenden Ereignisses" ist dabei nach ständiger Rechtsprechung des Europäischen Gerichtshofs sowohl auf den Handlungs- als auch auf den Erfolgsort bezogen. Im Falle einer Persönlichkeitsrechtsverletzung durch Online-Veröffentlichungen liegt der Erfolgsort dort, wo die betroffene Person den Mittelpunkt ihrer Interessen hat, was regelmäßig mit dem gewöhnlichen Aufenthalt zusammenfällt. Dies hat der EuGH in der wegweisenden Entscheidung **eDate Advertising** ausdrücklich klargestellt.¹⁰¹ Demnach ist für eine in Deutschland lebende Person deutsches Gericht zuständig, da sie dort in ihrer sozialen Wertgeltung und persönlichen Integrität betroffen ist.¹⁰²

G. Effektivierung der Auskunftspflichten

Der DSA knüpft an das Informationsmodell¹⁰³ an, indem er Plattformen weitreichende Informationspflichten auferlegt, die Nutzern und Behörden eine eigene Risikoabschätzung ermöglichen.

I. Transparenzprogramm des DSA

Der DSA ein umfassendes Transparenzregime, das verschiedene Akteure des digitalen Ökosystems erfasst. Für Vermittlungsdienste statuiert der DSA ein gestuftes System von Transparenzpflichten, das sich nach der Größe und gesellschaftlichen Bedeutung der Plattformen richtet. Die fundamentalen Transparenzpflichten des DSA umfassen zunächst die allgemeinen Berichtspflichten nach Art. 15 DSA, die alle Anbieter von Vermittlungsdiensten treffen. Diese beinhalten die Veröffentlichung von Transparenzberichten über Maßnahmen der Inhaltsmoderation und deren Auswirkungen.¹⁰⁴

Systemrelevante Plattformen (also sehr große Online-Plattformen (VLOPs) und sehr große Online-Suchmaschinen (VLOSEs)) unterliegen nach Art. 33 ff. DSA erweiterten Transparenzpflichten. Diese umfassen insbesondere systemische Risikoanalysen nach Art. 34 DSA, die eine

⁹⁹ MüKoBGB/Junker, 9. Aufl. 2025, Rom II-VO Art. 1 Rn. 59.

¹⁰⁰ Aus der umfassenden Rechtsprechung zu grenzüberschreitenden Persönlichkeitsverletzungen s. nur BGH VI ZR 489/16; mwN MüKoBGB/Junker, 9. Aufl. 2025, EGBGB Art. 40 Rn. 74 ff., 79 ff.

¹⁰¹ EuGH, Urt. v. 25.10.2011 – C-509/09 und C-161/10, *eDate Advertising* und *Martinez*, Slg. 2011, I-10269 = NJW 2012, 137, Rn. 45 ff.; zuletzt auch EuGH, Urt. v. 21.12.2021 – C 251/20, *Gtflix Tv* = GRUR-RS 2022, 39577.

¹⁰² MüKOZPO/Gottwald, 6. Aufl. 2022, Brüssel Ia-VO Art. 7 Rn. 61.

¹⁰³ Das Informationsmodell setzt auf Informationsbereitstellung als Mittel für die Erreichung eines Regulierungszwecks – dazu etwa *Fleischer*, Informationsasymmetrie im Vertragsrecht, 2001, S. 203–208, 570–572; *Kerton/Bo-dell* 29 Journal of Consumer Affairs 1995, 1, bes. 20–24; *Grundmann/Kerber/Weatherill*, Party Autonomy and the Role of Information in the Internal Market, 2001, dort insbes. die Einleitung. Zu den Einschränkungen des Modells, siehe etwa EuGH Urt. v. 16.5.1989, Rs. 382/87 – *Buet*; *Schön* FS Canaris, 2007, 1191.

¹⁰⁴ Dazu Müller-Terpitz/Köhler/Barudi, 2024, DSA Art. 15 Rn. 16ff.; Mast/Kettemann/Dreyer/Schulz/Seckelmann, 2025, DSA Art. 15 Rn. 31-34.

jährliche Bewertung systemischer Risiken vorschreiben, externe Audits nach Art. 37 DSA als unabhängige Compliance-Prüfungen sowie insbesondere den Datenzugang nach Art. 40 DSA, der dem Koordinator für digitale Dienste am Niederlassungsort oder der Kommission Zugang zu den Daten, die für die Überwachung und Bewertung der Einhaltung des DSA erforderlich sind, gewährt. Art. 40 Abs. 4 DSA normiert zudem die Bereitstellung von Daten für "vetted researchers". Das Transparenzprogramm des DSA zielt darauf ab, die demokratische Rechenschaftspflicht großer Plattformen zu stärken und deren gesellschaftliche Auswirkungen messbar zu machen.

II. Probleme, insbesondere des Forschungsdatenzugangs

Der Forschungsdatenzugang nach Art. 40 DSA steht vor erheblichen praktischen Herausforderungen, die dessen Wirksamkeit fundamental beeinträchtigen. Die bisherige Implementierung zeigt deutliche Schwächen in der Durchsetzung der Transparenzpflichten, wobei sich zwei gegensätzliche, aber gleichmaßen problematische Reaktionsmuster der Plattformen herauskristallisiert haben.

Einerseits verweigern Plattformen oft die Bereitstellung substantieller Daten durch generische, nichtsagende Antworten. Diese oberflächlichen Reaktionen umgehen systematisch die Intention des Art. 40 DSA, indem sie formal den Anforderungen zu entsprechen scheinen, tatsächlich aber keine wissenschaftlich verwertbaren Erkenntnisse ermöglichen. Plattformen nutzen dabei bewusst die Unbestimmtheit der rechtlichen Vorgaben aus und beschränken sich auf allgemeine Beschreibungen ihrer Systeme, ohne Zugang zu den eigentlichen Wirkungsmechanismen ihrer Algorithmen oder konkreten Nutzungsdaten zu gewähren. Diese Strategie der "compliance by form" untergräbt den Transparenzzweck des DSA erheblich.

Andererseits praktizieren manche Plattformen einen "Information Overkill", bei dem sie Forscher mit unstrukturierten Datenmengen überlasten, die zwar umfangreich, aber für wissenschaftliche Zwecke weitgehend unbrauchbar sind. Diese Datenflut ohne entsprechende Kontextualisierung, Dokumentation oder methodische Aufbereitung macht eine sinnvolle wissenschaftliche Auswertung praktisch unmöglich. Die Bereitstellung von Rohdaten ohne entsprechende Metadaten, Erläuterungen der Datenstrukturen oder Hinweise auf Datenqualität und -grenzen führt dazu, dass Forscher mehr Zeit mit der Datenaufbereitung als mit der eigentlichen Analyse verbringen müssen, wenn eine Auswertung überhaupt möglich ist.

Beide Problemfelder werden durch die unklare Datenabgrenzung in Art. 40 DSA verschärft. Die Definition dessen, welche Daten den Forschern bereitzustellen sind, bleibt rechtlich unbestimmt, wodurch Plattformen erheblichen Interpretationsspielraum erhalten. Die Implementierung sicherer Zugangsmodalitäten erweist sich als technisch komplex, während die 80-Arbeitstage-Frist für begründete Anträge häufig überschritten wird. Die Durchsetzung der Transparenzpflichten durch die Koordinatoren für digitale Dienste (in Deutschland die BNetzA) hat erhebliche Schwächen, insbesondere bei der Bewertung der Qualität und Verwertbarkeit bereitgestellter Daten. Die koordinierte Anwendung zwischen den Mitgliedstaaten dürfte sich schwierig gestalten, was zu inkonsistenten Standards führen und es den Plattformen ermöglichen könnte, die schwächsten regulatorischen Ansätze auszunutzen.

III. Aktuelle Maßnahmen der Europäischen Kommission

Die Europäische Kommission hat mit der Delegierten Verordnung vom 1. Juli 2025¹⁰⁵ konkrete technische Bedingungen und Verfahren für den Datenzugang normiert. Diese neue Regelung adressiert zentrale Implementierungsprobleme durch die Verfahrensstandardisierung mittels

¹⁰⁵ Noch ohne amtlichen Titel, C(2025) 4340 final.

Einrichtung des "DSA data access portal" als zentrale digitale Infrastruktur für den Datenaustausch zwischen Forschern, Datenanbietern und Digital Services Coordinators. Art. 9 der Delegierten Verordnung spezifiziert die Zugangsmodalitäten durch konkrete technische, rechtliche und organisatorische Maßnahmen, die Datenanbieter beim Datenzugang implementieren müssen. Dabei werden insbesondere sichere Verarbeitungsumgebungen ("secure processing environments") als Zugangsmodalität etabliert.

Art. 8 der Delegierten Verordnung präzisiert die Zugangsvoraussetzungen und konkretisiert die Voraussetzungen für begründete Anträge, einschließlich der Anforderungen an die Unabhängigkeit der Forscher von kommerziellen Interessen und die Offenlegung der Forschungsfinanzierung. Bemerkenswert ist auch die Einführung eines Mediationsverfahrens in Art. 13 der Delegierten Verordnung. Dieses ermöglicht es Datenanbietern, bei Meinungsverschiedenheiten über Änderungsanträge eine freiwillige Mediation zu beantragen, wodurch eine effizientere Streitbeilegung angestrebt wird.

Die Delegierte Verordnung zielt auf eine Harmonisierung der Aufsichtspraktiken ab und soll eine Vereinheitlichung der Verfahren zwischen den verschiedenen Behörden erreichen. Durch die Verpflichtung zur Nutzung des zentralen DSA-Datenportals und standardisierte Bewertungskriterien soll die bisher problematische Fragmentierung der Anwendungspraxis überwunden werden. Das European Board for Digital Services hat in seiner Stellungnahme vom 2. Juli 2025 die kritische Rolle der Forscher bei der Gewährleistung größerer Online-Transparenz anerkannt und die Delegierte Verordnung als "milestone innovation" für den DSA bezeichnet.¹⁰⁶

IV. Weitere Erwägungen

Ein bedeutsames Transparenzdefizit besteht beim Zugang zu den externen Audits nach Art. 37 DSA. Diese Audits, die jährlich von unabhängigen Auditoren durchgeführt werden müssen, bleiben weitgehend vertraulich, lediglich Abschlussberichte werden veröffentlicht.¹⁰⁷ Eine Erweiterung der Transparenzpflichten auf die vollständigen Auditprotokolle könnte die demokratische Kontrolle sehr großer Plattformen erheblich stärken. Die laufende Entwicklung von Guidelines durch die Kommission, insbesondere zu "trusted flaggers" und zum Schutz Minderjähriger, zeigt die kontinuierliche Weiterentwicklung des Transparenzregimes. Diese Guidelines konkretisieren die allgemeinen DSA-Bestimmungen und schaffen praktikable Standards für die Implementierung.

Ein kritischer Aspekt der DSA-Transparenz ist die "meaningful consultation" von Stakeholdern bei systemischen Risikoanalysen.¹⁰⁸ Die praktische Umsetzung dieser Konsultationspflicht zeigt erhebliche Qualitätsmängel. Oftmals beschränken sich Plattformen auf oberflächliche Anhörungen, ohne die Stakeholder-Eingaben substantiell in ihre Risikoanalysen einzubeziehen.

¹⁰⁶S. dazu Press statement of the *European Board for Digital Services*, 02.07.2025, abrufbar unter https://cdn.table.media/assets/press_statement_board_meeting_020725_adopted_sl70ejhpiq7xk3z1ziruimonbnk_117852.pdf

¹⁰⁷ Kritisch zum Prozedere *Holznaegel*, Shortcomings of the first DSA Audits — and how to do better, 2025, abrufbar unter: <https://dsa-observatory.eu/2025/06/11/shortcomings-of-the-first-dsa-audits-and-how-to-do-better/>; kritisch auch *Laux/Wachter/Mittelstadt*, Computer Law & Security Review, Volume 43, November 2021, 105613.

¹⁰⁸ Vgl. Art. 42 DSA.

Verbesserungsansätze sollten strukturierte Konsultationsverfahren, verbindliche Antwortpflichten der Plattformen auf Stakeholder-Eingaben und eine externe Überprüfung der Konsultationsqualität umfassen.

Die Transparenzpflichten des DSA fügen sich in den klassischen Ansatz des Informationsmodells ein.¹⁰⁹ Die Delegierte Verordnung vom Juli 2025 adressiert wichtige Implementierungsprobleme, insbesondere beim Forschungsdatenzugang. Dennoch bleiben erhebliche Herausforderungen bei der praktischen Durchsetzung bestehen. Eine erfolgreiche Umsetzung erfordert kontinuierliche Weiterentwicklung der regulatorischen Instrumente und eine konsequente Durchsetzung durch die zuständigen Behörden. Die langfristige Wirksamkeit des DSA-Transparenzregimes wird maßgeblich davon abhängen, ob es gelingt, die strukturellen Informationsasymmetrien zwischen Plattformen und gesellschaftlichen Akteuren nachhaltig zu reduzieren. Zentral ist dabei die Etablierung eines qualitativ hochwertigen Informationsstandards, der sich wohl aus der Einbeziehung der vollständigen Audit-Protokolle (Art. 37 DSA) unter das Regime von Art. 40 DSA ergeben würde.

H. Zentrale rechtspolitische Maßnahmen zur Steigerung der Sicherheit von Social Media-Plattformen

Die oben (unter B.) knapp dargestellte Gefahrenlage auf Social Media Plattformen für die Rechtsgüter des Allgemeinen Persönlichkeitsrechts und der öffentlichen Meinungsbildung wirft auch die akute Frage nach der weiteren Optimierung der Verantwortlichkeitsstrukturen auf. Folgende regulatorische Maßnahmen können die Situation verbessern, wobei sie selbstredend nur komplementär zur Durchsetzung der bisher bestehenden Pflichten wirken und an dieser Stelle nur skizziert werden können.¹¹⁰

I. Verbot von Social Bots

Einen wesentlichen Beitrag zur Erhöhung der Sicherheit auf Social Media Plattformen würde das Verbot von Social Bots darstellen. Die rechtspolitische Rechtfertigung eines solchen Verbots ergibt sich aus der Abwesenheit eines legitimen Interesses an automatisierten Meinungsäußerungen in sozialen Netzwerken. Social Bots manipulieren vielmehr systematisch den öffentlichen Diskurs, indem sie ein breites Stimmungsbild vortäuschen und dadurch die demokratische Willensbildung verzerren. Sie werden von Scammern, Terroristen und totalitären Regimen eingesetzt um Nutzer von Social Media Plattformen zu manipulieren.¹¹¹ Eine Identifikation von Social Bots ist technisch umsetzbar, da diese häufig auffällige Aktivitätsmuster aufweisen und zudem das Anlegen eines Nutzerkontos an eine Nutzeridentifikation gekoppelt sein kann (dazu unter II.). Die dabei in Rede stehenden Grundrechte der Bot-Betreiber - unternehmerische Freiheit und Meinungsfreiheit - wiegen deutlich geringer als die beeinträchtigte Informationsfreiheit aller anderen Nutzer.¹¹² Daher vermögen auch Restzweifel an der tatsächli-

¹⁰⁹ Denga ZfPW 2024, 427 (450).

¹¹⁰ Eine an demokratischen Grundsätzen ausgerichtete Konzeption für die Regulierung digitaler Technologien, insbesondere von Social Media Plattformen, findet sich bei Susskind, *The Digital Republic*, 2022, insbes. S. 267 ff. (Part Ten).

¹¹¹ Vgl. dazu etwa die Studie von *Büro für Technikfolgenabschätzung beim Deutschen Bundestag*, *Social Bots*, TA-Vorstudie, 2017; s. auch von Ungern-Sternberg RW 2022, 94.

¹¹² Mit einer umfassenden Abwägung, im Ergebnis jedoch gegen ein Verbot Dürr, *Social Bots*, 2024.

chen Durchschlagskraft von Social Bots nichts zu ändern – Nutzer von Social Media Plattformen haben einen verfassungsrechtlich geschützten Anspruch darauf, von künstlich generierten Meinungsäußerungen verschont zu bleiben.¹¹³ Ein Social Bot-Verbot würde die Authentizität des digitalen Diskurses wiederherstellen und die informationelle Selbstbestimmung der Nutzer stärken, indem es ihnen ermöglicht, ihre Meinungsbildung auf der Grundlage genuiner menschlicher Äußerungen zu treffen. Eine reine Kennzeichnungspflicht, wie sie bereits unter der KI-VO¹¹⁴ und dem Medienstaatsvertrag¹¹⁵ vorgesehen ist, vermag angesichts der akuten Gefährdungslage im digitalen Raum nicht hinreichenden Schutz zu bieten.

II. Nutzeridentifikation per Video-Ident

Eine deutliche Stärkung der Sicherheit auf Social Media Plattformen böte die Einführung einer Klarnamenpflicht für Nutzer gegenüber der Plattform bei gleichzeitiger Wahrung der Pseudonymität im öffentlichen Plattformverkehr.¹¹⁶ Eine solche Registrierung kann durchaus analog zum Zugang zu Finanzdienstleistungen per Video-Ident-Verfahren erfolgen, welches mittlerweile standardisiert und nutzerfreundlich über mobile Endgeräte in etwa zehn Minuten durchführbar ist.¹¹⁷ Dieses System schafft einen ausgewogenen Kompromiss zwischen effektiver Rechtsdurchsetzung und der Freiheit des digitalen Diskurses. Während die Plattformen bei Rechtsverstößen die wahre Identität ihrer Nutzer ermitteln können, bleibt die anonyme und pseudonyme Meinungsäußerung im öffentlichen Raum gewährleistet. Dies entspricht dem verfassungsrechtlichen Gebot, dass Grundrechtseingriffe verhältnismäßig sein müssen und den mildesten verfügbaren Mitteln entsprechen sollten. Die Video-Ident-Lösung würde die Vorteile verlässlicher Identitätsfeststellung mit dem Schutz der anonymen Rede als wesentlichem Element demokratischer Partizipation kombinieren. Eine solche Lösung müsste selbstverständlich mit hinreichenden Garantien gegen unbefugten Zugriff auf die Nutzeridentitäten ausgestattet werden.¹¹⁸

III. Recht auf Inhaltefilter

Die Verpflichtung zu Echtzeit-Inhaltsfilterung durch Plattformen mit automatischer Blockade problematischer Inhalte wäre grundrechtlich höchst bedenklich, da sie faktisch einer Vorzensur gleichkäme.¹¹⁹ Rechtspolitisch vorzugswürdig ist stattdessen die Einführung eines Rechts auf Inhaltefilter, welches Plattformen zur Bereitstellung konfigurierbarer Filteroptionen verpflichtet, deren Nutzung jedoch den Nutzern selbst überlassen bleibt.¹²⁰ Diese Filter sollten verschiedene Schärfegrade aufweisen und es den Nutzern ermöglichen, ihre Inhaltswahrnehmung entsprechend ihren individuellen Präferenzen zu gestalten. Ergänzend sollte die technische Verunmöglichung von Screenshots – zumindest als optionales Recht der Nutzer – erwogen werden,

¹¹³ Zur negativen Informationsfreiheit vgl. etwa BeckOK InfoMedienR/Kühling, 48. Ed. 01.05.2025, GG Art. 5 Rn. 44.

¹¹⁴ Vgl. Art. 50 Abs. 1 KI-VO.

¹¹⁵ Vgl. §§ 18 Abs. 3, 93 Abs. 4 MStV.

¹¹⁶ So im Ergebnis auch die Studie von G'sell, Has the time come to end anonymity on social media?, 2023.

¹¹⁷ Dazu nur Moosmayer/Lösler/Diergarten Corporate Compliance, 4. Aufl. 2024, 3. Kap. Rn. 749 ff.

¹¹⁸ Zu den Risiken einer Identifikationspflicht am Beispiel Chinas s. nur Lee/Liu, 25 Wash. Int'l L.J. 1 (2016).

¹¹⁹ Dem steht auch Art. 8 DSA entgegen, dazu nur Müller-Terpitz/Köhler/Köhler, 2024, DSA Art. 8 Rn. 49.

¹²⁰ S. dazu European Parliament, The impact of algorithms for online content filtering or moderation, 2020, abrufbar unter: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/657101/IPOL_STU\(2020\)657101_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/657101/IPOL_STU(2020)657101_EN.pdf).

um die unbefugte Verbreitung privater Inhalte zu erschweren, wobei hier selbstredend der Vorbehalt praktischer Umsetzbarkeit und mögliche Umgehungsstrategien zu berücksichtigen sind. Zudem müsste sehr gut abgewogen werden, ob die Erschwerung der Dokumentation von Straftaten nicht ein zu schwerer Kollateralschaden wäre.

IV. Qualifikation der Geschäftsleitung

Analog zu den "Fit & Proper"-Anforderungen im Kapitalmarktrecht¹²¹ sollten für Führungskräfte von Social Media-Plattformen sowie deren lokale Repräsentanten spezifische Qualifikationsanforderungen etabliert werden, um sicherzustellen, dass diese den Herausforderungen digitaler Meinungsräume gerecht werden. Bereits *de lege lata* müssen KI-Kompetenzen im Sinne des Art. 4 der KI-Verordnung erworben werden, da moderne Plattformen in erheblichem Umfang auf algorithmische Systeme angewiesen sind.¹²² Die Einführung einer darüber hinausgehenden, öffentlich organisierten, oder zumindest zertifizierten Ausbildung oder Zertifizierung wäre dabei wünschenswert.

V. Transparenz und Rechtsbehelfe für Shadow-Banning

Das Phänomen des Shadow-Banning, bei dem Inhalte oder Nutzer algorithmisch unterdrückt werden, ohne dass die Betroffenen davon Kenntnis erlangen, stellt eine erhebliche Herausforderung für die Meinungsfreiheit und Funktionalität digitaler Meinungsräume dar. Während Art. 38 DSA nur personalisierte Empfehlungssysteme erfasst und eine Profiling-freie Option vorschreibt,¹²³ bleibt die umfassendere Kuratierungsgewalt der Plattformen inhaltlich weitgehend unreguliert. Der BGH hat in seiner Facebook-Entscheidung die Notwendigkeit der Anpassung von AGB an die tatsächlichen Moderationspraktiken betont,¹²⁴ doch sind konkrete Kriterien für Shadow-Banning-Maßnahmen bislang nicht etabliert, geschweige denn durchgesetzt. Art. 14 Abs. 1 und 4 DSA, die Sorgfalt, Objektivität, Verhältnismäßigkeit und Grundrechtsrespekt bei der Inholdemoderation verlangen, sind noch wenig konkretisiert.

Damit ist derzeit auch die Begründungspflicht nach Art. 17 Abs. 1 lit. a) DSA kein effektives Steuerungsinstrument, denn Plattformen können stets die Unvereinbarkeit eines Postings mit ihren Nutzungsbedingungen behaupten (mit generativen Angaben unter Art. 17 Abs. 3 DSA), wenn diese selbst (noch) unkontrolliert sind.

Das Problem liegt freilich auch darin, dass die Plattform die Kuratierung schlicht nicht mitteilt und den Nutzenden dann nichts von der Unterdrückung ihrer Inhalte erfahren, und daher auch nicht eine Begründung unter Art. 17 DSA einfordern können. Ebenso wenig kann die Kommission die Vollständigkeit der Meldungen zu Inhaltesperren nach Art. 24 Abs. 5 DSA kontrollie-

¹²¹ Vgl. Art. 9 Abs. 1, 6 MiFID II-RL 2014/65/EU; Art. 8-12 Delegierte RL (EU) 2017/593; Art. 8 Abs. 1 lit. b AIFM-RL 2011/61/EU; Art. 7 UCITS-RL 2009/65/EG; ergänzend CRD V-RL 2019/878/EU und CRR II-VO (EU) 2019/876 für Kreditinstitute mit Wertpapierdienstleistungen.

¹²² Dazu BeckOK KI-Recht/Kaufmann, 2. Ed. 1.5.2025, KI-VO Art. 4 Rn. 30ff.

¹²³ Dazu Müller-Terpitz/Köhler/Beyerbach/Seyer, 2024, DSA Art. 38 Rn. 7; zur Bezahlösung „pay or okay“ s. *D'Amico* Technology and Regulation 2024.

¹²⁴ BGH III ZR 179/20 und III ZR 192/20 = ZIP 2021, 1955-1956 (m.Anm. Denga).

ren. Das Einsichtsrecht in die Kalibrierung der Plattformmoderation nach Art. 40 DAS unterliegt den bereits oben genannten Problemen (oben, G.); empfehlenswert erscheint auch hier die Erweiterung der Zugangsrechte nach Art. 40 DSA auf die Audit-Protokolle.

Empfehlenswert ist hier auch ein effektives Widerspruchsrecht analog zu Art. 16 ff. DAS, mit der Verpflichtung zur Wiederherstellung der Sichtbarkeit bei fehlenden sachlichen Gründen. Art. 21 DSA schafft hier bislang keine Abhilfe, da er nur Entscheidungen nach Art. 20 DSA erfasst, also Sperrungen nach Meldungseingang zu rechtswidrigen Inhalten. Durch ein eigenes Widerspruchsrecht gegen AGB-Bedingte Sperrungen könnten Nutzer die Wahrung ihrer Kommunikationsfreiheiten, die in Art. 14 Abs. 4 DSA explizit den Plattformen aufgetragen ist, selbst durchsetzen, ggf. im Wege des Private Enforcement unter Art. 54 DSA (dazu oben, F. 2.).

VI. Altersbeschränkung für Social Media

Die Einführung eines Mindestalters von 16 Jahren für die Nutzung sozialer Medien entspricht den neuesten psychiatrischen Erkenntnissen über die medizinischen und sozialen Auswirkungen digitaler Medien auf die Gehirnentwicklung.¹²⁵ Diese Altersgrenze korrespondiert mit anderen gesellschaftlichen Altersbeschränkungen, etwa dem Konsum leichten Alkohols, und reflektiert die vergleichbare Wirkung digitaler Stimulation auf das sich entwickelnde Gehirn. Länder wie Frankreich und Australien haben bereits entsprechende Maßnahmen implementiert;¹²⁶ Auch die Leopoldina empfiehlt wegen der psychischen Gefahren der Apps eine Reglementierung von Social Media nach Altersstufen.¹²⁷ Die Europäische Kommission hat mit ihren Guidelines zur Altersverifikation und dem App-Prototyp für einen sichereren Online-Raum für Kinder erste Schritte unternommen.¹²⁸ Der Minderjährigenschutz im DSA, der sich bislang auf Art. 28 und die allgemeinen Sorgfaltspflichten beschränkt, bedarf einer substanziellen Erweiterung, da Plattformen durch ihr Design gerade die Vulnerabilität Jugendlicher ausnutzen.¹²⁹ Die Identifikation sollte analog zu Finanzdienstleistungen erfolgen, um die Wirksamkeit der Altersverifikation zu gewährleisten (dazu auch H. II.).

VII. Beweislastumkehr im Prozess

Nach dem Vorbild der novellierten Produkthaftungsrichtlinie¹³⁰ sollte eine Beweislastumkehr für Haftungsfälle im Zusammenhang mit Plattformschäden ausdrücklich geregelt werden. Diese würde der strukturellen Informationsasymmetrie zwischen Plattformbetreibern und geschädigten Nutzern Rechnung tragen.¹³¹ Plattformen verfügen über umfassende Daten zu ihren

¹²⁵ Dazu nur die Studie des *Center for Countering Digital Hate*, Youtube's Anorexia Algorithm, 2025; vgl. dazu auch die am 16. November 2023 in Kalifornien von 42 US-Generalstaatsanwälten eingereichte Klage gegen Facebook (4:23-cv-05448); dazu *Denga*, NJW-aktuell 3/2024, 15.

¹²⁶ Dazu *Schmid/Feld*, Social Media in der EU bald erst ab 16?, Tagesschau 07.06.2025, abrufbar unter: <https://www.tagesschau.de/ausland/europa/social-media-alter-eu-100.html>.

¹²⁷ *Leopoldina*, Soziale Medien und die psychische Gesundheit von Kindern und Jugendlichen, Juli 2025 (insbes. S. 36 ff.).

¹²⁸ S. hierzu Pressemitteilung der Europäischen Kommission vom 14.07.2025, abrufbar unter: <https://digital-strategy.ec.europa.eu/de/news/commission-presents-guidelines-and-age-verification-app-prototype-safer-online-space-children>.

¹²⁹ Dazu bereits die Nachweise in Fn. 125.

¹³⁰ Vgl. Art. 9 10 EU-Produkthaftungsrichtlinie 2024/2853; s. auch Art. 3, 4 der letztendlich nicht weiterverfolgten KI-Haftungsrichtlinie (COM(2022) 496).

¹³¹ Tragend schon für die Beweislastumkehr der Produzentenhaftung, BGHZ 51, 91 (104 ff.) – Hühnerpest; zum Verständnis des Plattformrechts als Produktrecht vgl. *Denga/Jungblut* ZfPC 2025 (i.E.).

algorithmischen Systemen, Moderationspraktiken und Nutzerverhalten, während Geschädigte kaum Einblick in die internen Prozesse erhalten. Eine Beweislastumkehr würde Plattformen dazu verpflichten, die Rechtmäßigkeit ihrer Praktiken und die Abwesenheit kausaler Zusammenhänge zu potentiellen Schäden zu belegen. Eine Klarstellung der Beweislastumkehr würde nicht nur die Rechtsdurchsetzung für Betroffene erleichtern, sondern auch präventive Anreize für Plattformen schaffen, ihre Systeme sicherer und transparenter zu gestalten. Schon de lege lata kann sich eine solche Beweislastumkehr aus den Grundsätzen der Produzentenhaftung ergeben,¹³² eine Klarstellung würde freilich Rechtssicherheit und Präventionswirkungen fördern.

9. September 2025

A handwritten signature in black ink, appearing to read 'Michael Denga', with a stylized flourish at the end.

Prof. Dr. Michael Denga

¹³² Erman/Wilhelmi BGB, 17. Auflage 2023, BGB § 823, Rn.112.