



ANALYSE DES STAATLICHEN REAKTIONS- GEFÜGES GEGEN MANIPULATIONEN DES ÖFFENTLICHEN INFORMATIONSRRAUMS

Rechtswissenschaftliches Gutachten

Prof. Dr. iur. Ralf Müller-Terpitz, September 2026

INHALT

§ 1 GEGENSTAND UND AUFBAU DER UNTERSUCHUNG	4
A. Gegenstand der Untersuchung	4
B. Aufbau der Untersuchung	5
C. Methodik der Untersuchung	5
§ 2 RECHTSWISSENSCHAFTLICHE UNTERSUCHUNG	7
A. Begriff und Verfahren der Manipulation des öffentlichen Informationsraums	7
I. Begriff der Manipulation des öffentlichen Informationsraums	7
1. Konkretisierung des Begriffskerns	7
2. Abgrenzung zu anderen Begriffen	8
a) Desinformation	8
b) Misinformation	10
c) Fake News	10
d) Propaganda	10
3. Vorteile des inhaltsneutralen Begriffsverständnisses	11
II. Verfahren der Manipulation des öffentlichen Informationsraums	14
1. Technische Aspekte	14
a) Technische Manipulation der Reichweite	14
b) Verschleierung des Absenders	15
2. Inhaltliche Aspekte	16
3. Gestalterische Aspekte	16
B. Fallstudien	17
I. Nutzung von Online-Plattformen zur technischen Manipulation der Reichweite	17
II. Nutzung von Online-Plattformen zur Verschleierung des Absenders	19
III. Nutzung von Künstlicher Intelligenz (Deepfakes)	20
IV. Nutzung journalistisch-redaktionell gestalt. Medien zur Manipulation des öffentl. Informationsraums	21
C. Rechtlicher Rahmen zur Bekämpfung von Manipulationen des öffentlichen Informationsraums	23
I. Kompetenzgefüge zur Bekämpfung von Manipulationen des öffentlichen Informationsraums	23
1. Europäische Union	23
a) Ausschließliche Zuständigkeiten	23
b) Geteilte Zuständigkeiten	26
2. Bundesrepublik Deutschland	26
a) Bund	27
b) Länder	27
II. Grundrechtliche Grenzen der Bekämpfung von Manipulationen des öffentlichen Informationsraums	28
1. Anwendbare Grundrechtsregime	29
a) Völkerrechtlicher Grundrechtsschutz (EMRK)	29
b) Nationaler Grundrechtsschutz (GG)	29
c) Unionaler Grundrechtsschutz (EUGRC)	30
2. Grundrechtliche Gewährleistungsgehalte im Detail	31
a) Vorbemerkungen	31
b) Grundrechtlicher Schutz von Manipulationen des öffentlichen Informationsraums	33
c) Schranken der Meinungs- und Medienfreiheit	43
3. Zwischenfazit	47

D. Status quo des Reaktionsgefüges zur Bekämpfung von Manipulationen des öffentl. Kommunikationsraums	48
I. Legislativer Status quo	48
1. Unionales Recht	48
a) Digital Services Act	48
b) European Media Freedom Act	59
c) KI-Verordnung	59
d) AVMD-Richtlinie	61
2. Nationales Recht	63
a) Zivilrecht	63
b) Strafrecht	64
c) Öffentliches Recht	66
II. Exekutiver Status Quo	69
1. Unionales Recht	69
a) Digital Services Act	69
b) Sonstige Zuständigkeiten	72
2. Nationales Recht	73
a) Bundesrecht	73
b) Landesrecht	74
III. Anwendung des rechtlichen Status quo auf die Fallstudien	74
1. Nutzung von Online-Plattformen zur technischen Manipulation der Reichweite	74
2. Nutzung von Online-Plattformen zur Verschleierung des Absenders	77
3. Nutzung von Künstlicher Intelligenz (Deepfakes)	79
4. Nutzung journ.-redaktionell gestalt. Medien zur Manipulation des öffentl. Informationsraums	81
E. Identifikation von Regelungs- und Zuständigkeitsdefiziten	84
I. Regelungsdefizite	84
II. Zuständigkeits- und Vollzugsdefizite	85
F. Entwicklung von Lösungsansätzen	87
I. Legislative Lösungsansätze	87
1. Verbesserung von Transparenz	87
2. Inhaltebezogene Regelungen	87
a) Repressive Maßnahmen	88
b) Präventive Maßnahmen	89
3. Plattformbezogene Regelungen	91
4. KI-bezogene Regelungen	92
5. Stärkung der Nutzerautonomie	92
II. Exekutive Lösungsansätze	93
§ 3 ZUSAMMENFASSUNG	94
ANHANG	98
LITERATUR	99
IMPRESSUM	105

§ 1 GEGENSTAND UND AUFBAU DER UNTERSUCHUNG

A. GEGENSTAND DER UNTERSUCHUNG

Ziel dieses rechtswissenschaftlichen Gutachtens ist es, das staatliche Reaktionsgefüge gegen Manipulationen des öffentlichen Informationsraums umfassend zu analysieren, Lücken zu identifizieren und insoweit Lösungsansätze zu präsentieren.

Ausgangspunkt hierfür ist die Erwägung, dass die gezielte Manipulation des öffentlichen Informationsraums die democratisierende Funktion freiheitlicher Kommunikation und damit des Staates und der Gesellschaft insgesamt zu untergraben vermag. Entsprechend besteht, wie eine Forsa-Befragung der LFM NRW aus dem Jahre 2024 ergeben hat¹, in der Bevölkerung die Wahrnehmung, dass solche Manipulationen und die hierdurch bedingte Verbreitung von Desinformation oder Verzerrung des öffentlichen Diskurses ein Bedrohungstatbestand für unsere freiheitlich-demokratische Grundordnung darstellt. Ursächlich hierfür ist, dass die vernetzte sowie medial und kommunikativ fragmentierte Gesellschaft ein ideales Einfallstor für Manipulations- und Desinformationsprozesse bildet. So wird vermutet, dass sechsmal mehr „Fakes News“ pro Tag veröffentlicht und verbreitet werden als wahrhaftige Nachrichten und Informationen.² Der „Global Risk Report 2026“ des World Economic Forum listet Mis- und Desinformation auf Platz 5 der gegenwärtigen globalen Risiken.³ Zutreffend führt Ladeur hierzu aus, dass es sich bei Desinformation

„um eine internetspezifische Kommunikationsstrategie (handelt), die es schwer identifizierbaren Kräften erlaubt, nicht nur in Krisensituationen an den etablierten und öffentlich bekannten Providern von Medieninhalten vorbei vor allem kampagnenartig mit großem, aber vielfach nicht erkennbarem Aufwand bestimmte Medieninhalte zu verbreiten, die eine erhebliche, ihrerseits nicht leicht erkennbare Unsicherheit unter Internetnutzern hervorrufen können. Diese Unsicherheit ist zunächst selbst ein medienspezifisches Phänomen, das es immer schon gegeben hat und das die Rationalität der öffentlichen Kommunikation nicht außer Kraft setzt. Allerdings verliefen die Verbreitungswege der klassischen Medien eher linear von den Medien als Sendern zu den Lesern/Zuschauern als Empfängern. Zugleich bildeten sich schwer durchschaubare Netzwerke mündlicher Kommunikation außerhalb dieser Verbreitungswege. Falschinformationen von einer gewissen Relevanz wurden zwischen Medien beobachtet und bewertet. Die Wissensbestände, an denen sich die Bürger orientiert haben, waren früher auch von relativ stabilen Gruppenzugehörigkeiten, stabilen gesellschaftlichen Richtungsannahmen und kulturellen Traditionen bestimmt, die es verhindert haben, dass sich außerhalb von Zeiten großer politischer Spannungen in der politischen Öffentlichkeit eindeutig falsche Behauptungen leicht verbreiten konnten.“⁴

1 Abrufbar unter https://www.medienanstalt-nrw.de/fileadmin/LFMNRW_Desinformation_forsa_2024.pdf (letzter Abruf: 30.4.2026).

2 Vgl. Müller, NJ 2024, 216 (217).

3 World Economic Forum, The Global Risk Report 2026, 21st Edition, 2026, S. 8, abrufbar unter: <https://www.weforum.org/publications/global-risks-report-2026/> (letzter Abruf: 30.4.2026).

4 Ladeur, K&R 2024, 477 (480).

Vor diesem Hintergrund geht die Auftraggeberin des Rechtsgutachtens davon aus, dass die Ordnungspolitik angesichts dieser immer größer werdenden Herausforderung in der Pflicht steht, einen holistischen sowie kollaborativen Ansatz zur Bekämpfung von Manipulationen des öffentlichen Informationsraums zu schaffen. Dieser soll in einer verhältnismäßigen Art und Weise einerseits die Meinungsfreiheit garantieren sowie andererseits die Bedrohungen für offene Gesellschaften effektiv reduzieren. Die Auftraggeberin leitet hieraus ab, dass aufgrund ihrer vielschichtigen Natur kein Allheilmittel gegen solche Manipulationen existiere, sondern der Handlungsrahmen – sei er regulatorisch präventiv oder repressiv – aus unterschiedlichen Maßnahmen und Instrumenten bestehen müsse. Damit gingen in Europa verschiedene Zuständigkeiten staatlicher sowie nicht-staatlicher Akteure einher.

Mit Blick auf diese Gegenstandsbeschreibung kann sich das vorliegende Rechtsgutachten nicht auf den Kompetenzbereich der Auftraggeberin (Vollzug des bundes- und landesweit gültigen Medienrechts) beschränken. Vielmehr muss seine Analyse in einer umfassenden deskriptiven und normativen Betrachtung des für Manipulationen des öffentlichen Informationsraums maßgeblichen Rechtsrahmens im Mehrebenensystem mit seinen unterschiedlichen Regelungsansätzen und Vollzugsinstanzen bestehen. In den Blick zu nehmen ist folglich das Unionsrecht sowie das Bundes- und Landesrecht mit all seinen Teilrechtsgebieten (Öffentliches Recht, Strafrecht und Zivilrecht). Dieser holistische Ansatz einer rechtlichen Analyse der Regelungs- und Durchsetzungsstrukturen gegen Desinformation resultiert im Übrigen auch aus der Zielgruppe des Gutachtens, das sich laut Auftragsbeschreibung an die Politik als Gestalterin des Ordnungsrahmens, andere europäische sowie nationale (Regulierungs-)Behörden sowie an die Auftraggeberin selbst in ihrer Funktion als staatsferne Medienaufsicht zur Ermöglichung von Meinungsfreiheit richten soll.

B. AUFBAU DER UNTERSUCHUNG

Die rechtswissenschaftliche Untersuchung erfolgt in sechs Arbeitsschritten (§ 2 A. – F.), die sich ihrerseits – jedenfalls partiell – in Teilschritte untergliedern. Diese Arbeitsschritte weisen einen teils deskriptiven, teils analytischen und teils normativen Charakter auf. Die Untersuchung ist im Übrigen so angelegt und umgesetzt, dass ein Arbeitsschritt auf dem anderen aufbaut. Freilich resultiert hieraus kein streng linearer, sondern ein interdependenter Arbeitsprozess. Aufgrund ihrer Wechselbezüglichkeit haben die Arbeitsschritte der späteren Stufen bei der Erstellung des Rechtsgutachtens dazu beigetragen, die Arbeitsschritte der vorangegangenen Untersuchungsstufen nachzuschärfen und zu verfeinern.

C. METHODIK DER UNTERSUCHUNG

Die Analyse stützt sich einerseits auf einschlägige veröffentlichte Quellen in Gestalt von amtlichen Dokumenten (EU, Bund, Länder) sowie andererseits auf rechtswissenschaftliche und kommunikationswissenschaftliche Studien⁵ und Literatur. Ergänzt wird dieser Quellenfundus durch Experteninterviews mit Personen aus dem behördlichen und zivilgesellschaftlichen Bereich (Verbände, Non-Governmental Organisations [NGOs]). Eine Liste der insoweit geführten Interviews nebst Interviewpartnern findet sich im Anhang.

Hinzu kommt eine sachverhaltsbasierte Entwicklung von Fallstudien mit beispielhaft umrissenen Szenarien, die teils quellenbasiert auf der Grundlage realer Sachverhalte (wie z. B. die Geschehnisse um „Russia Today“ [RT] oder „Compact“), amtlicher Dokumente, des rechtswissenschaftlichen und kommunikationswissenschaftlichen Schrifttums sowie auf der Grundlage von Expertengesprächen entwickelt wurden. Die durch diesen Prozess erarbeiteten Fallstudien bilden einen Sachverhaltsfundus, der im Rahmen der nachfolgenden Arbeitsschritte herangezogen wurde, um die dortigen Analysen zu veranschaulichen und die damit zusammenhängenden Rechtsfragen greifbarer zu machen.

⁵ Neben der bereits erwähnten Forsa-Befragung der LFM NRW (Fn. 1) sind hierfür die 2024 von der Friedrich-Nau-
mann-Stiftung und von der Bertelsmann-Stiftung in Auftrag gegebene Umfragen zu Desinformationskampagnen von
Relevanz; vgl. hierzu Waegner, MMR-Aktuell 2025, 01147.

§ 2 RECHTSWISSENSCHAFTLICHE UNTERSUCHUNG

A. BEGRIFF UND VERFAHREN DER MANIPULATION DES ÖFFENTLICHEN INFORMATIONSRAUMS

I. BEGRIFF DER MANIPULATION DES ÖFFENTLICHEN INFORMATIONSRAUMS

1. KONKRETISIERUNG DES BEGRIFFSKERNS

Die Formulierung „Manipulation des öffentlichen Informationsraums“ ist eine noch junge, die von den Landesmedienanstalten in den öffentlichen Diskurs eingebracht wurde.⁶ Ihr Zweck ist es, für die manipulative (dolose) Verzerrung von Kommunikationsprozessen eine inhaltsneutrale Umschreibung zu finden, die am Ziel des Vorgangs – der verdeckten und mit unredlicher Absicht erfolgenden Beeinflussung des individuellen und öffentlichen Meinungsbildungsprozesses – und nicht am Gegenstand – etwa einer bewusst unwahren Information – ansetzt.

Diese Manipulation kann in zwei Formen auftreten:

1. Durch eine Manipulation der Reichweite eines bestimmten Inhalts und/oder
2. durch die Manipulation (Verschleierung) des Absenders.

Im ersten Fall ist es das Ziel der Manipulation, für eine bestimmte meinungsrelevante Information oder meinungsbildende Position eine vermeintlich höhere Relevanz im gesellschaftlichen Diskurs bzw. eine höhere Zustimmung/Ablehnung zu erzeugen. Hierbei verwendet der Manipulator zumeist automatisierte Techniken, etwa in Gestalt einer bot-gesteuerten Verstärkung gefälschter oder gekaufter Interaktionen⁷ bzw. durch ein koordiniertes unauthentisches Verhalten (Coordinated Inauthentic Behaviour – CIB).⁸

⁶ S. hierzu die Informationsvorlage für die 353. Sitzung der DLM am 23.9.2025 in Leipzig, Top 6.3.2.

⁷ Bei einem Bot (als Kurzform für „Roboter“) handelt es sich um ein automatisiertes Softwareprogramm, das Aufgaben im Internet selbstständig und wiederkehrend ausführen kann, ohne dass ein Mensch eingreifen oder tätig werden muss.

⁸ Als Bsp. kann hier auf die Präsidentschaftswahl 2024 in Rumänien verwiesen werden. So verfügte der spätere Wahlsieger Călin Georgescu weder über die Unterstützung einer etablierten Partei noch über nennenswerte Umfragewerte oder finanzielle Mittel für seine Kampagne. Dennoch erzielten seine TikTok-Videos eine außergewöhnlich hohe Reichweite: Hunderttausende Aufrufe pro Video und Dutzende Millionen Ansichten ließen seinen Kanal von 120 Followern auf mehr als eine halbe Million anwachsen. Nach Angaben des rumänischen Nachrichtendienstes wurden vor dem Wahlgang über 25.000 neue TikTok-Konten erstellt. Die Wahl wurde im weiteren Verlauf aufgrund dieser und weiterer Auffälligkeiten annulliert. Die Europäische Kommission hat als Reaktion auf diese Vorfälle eine auf den Digital Services Act (DSA) gestützte Untersuchung eingeleitet (vgl. Pressemitteilung v. 17.12.2024: Kommission leitet förmliches Verfahren

Über den Einsatz dieser Techniken werden die Rezipienten jedoch im Unklaren gelassen.

Im zweiten Fall geht es um eine Manipulation, die versucht, von der Autorität oder dem Vertrauen, das der eigentlichen Identität entgegengebracht wird, zu profitieren. Es geht mithin um einen „Identitätsdiebstahl“, etwa in Gestalt gefälschter Social-Media-Accounts bekannter Persönlichkeiten und Institutionen oder gefälschter Medienangebote, gefälschter Webseiten oder Deep-fakes von Medienangeboten.⁹ Derartige Maßnahmen, die – wie die erste Fallgruppe – auf Manipulationen i.S. von Täuschungen bzw. Verschleierungen beruhen, sind häufig Instrumente der sog. „Doppelgänger“-Kampagne. Auch hier soll folglich bei den Rezipienten eine Fehlvorstellung über die Richtigkeit oder das Gewicht einer den Meinungsbildungsprozess prägenden Information oder Position hervorgerufen werden.

2. ABGRENZUNG ZU ANDEREN BEGRIFFEN

Mit diesem im Ausgangspunkt inhaltsneutralen Verständnis grenzt sich die Formulierung „Manipulation des öffentlichen Informationsraums“ bewusst von anderen, inhaltsbezogenen Begriffen ab, auch wenn sie Berührungspunkte zu diesen aufweisen kann.

Zu diesen anderen Begriffen zählen diejenigen der Desinformation (a)), der Misinformation (b)), der „Fake News“ (c)) und der Propaganda (d)). Allen drei Begriffen ist gemein, dass sie – zumindest vordergründig – an Informationen (News) anknüpfen. Informationen beziehen sich auf ein Realgeschehen, das – im Unterschied zu Meinungen, die durch Elemente der Stellungnahme und des Dafürhaltens gekennzeichnet sind – grundsätzlich dem Beweis zugänglich ist, d.h. als richtig oder falsch qualifiziert zu werden vermag.¹⁰

A) DESINFORMATION

Soweit ersichtlich, wird der Begriff „Desinformation“ in keinem nationalen oder unionalen Gesetz legaldefiniert. Auch der Digital Services Act (DSA)¹¹, der auf die Schaffung eines sicheren und vertrauenswürdigen Online-Umfelds abzielt (Art. 1 Abs. 1 S. 1 DSA), verwendet den Begriff der Desinformation lediglich in seinen Erwägungsgründen (ErwG)¹², nicht aber in seinen Rechtstexten. In den Erwägungsgründen findet der Begriff indes keine Erläuterung oder Definition, sondern wird nur durch Verweise auf unrichtige oder irreführende/täuschende Inhalte, damit

gegen TikTok wegen Wahlrisiken nach dem Gesetz über digitale Dienste ein; abrufbar unter: <https://digital-strategy.ec.europa.eu/de/news/commission-opens-formal-proceedings-against-tiktok-election-risks-under-digital-services-act> [letzter Abruf: 30.4.2026]). Sie prüft nun, ob eine Manipulation des TikTok-Empfehlungsalgorithmus auf der Plattform erkennbar ist; so Schlömer/Kehrberg, ZRP 2025, 2.

9 Siehe hierzu die Informationsvorlage für die 353. Sitzung der DLM am 23.9.2025 in Leipzig, Top 6.3.2, S. 3. Als Bsp. für solche Manipulationen des Absenders kann auf gefälschte Online-Auftritte des Spiegels oder der Washington Post verwiesen werden.

10 Zu dieser Differenzierung vgl. etwa BVerfGE 124, 300 (320). Eine Meinung kann demgegenüber ihrerseits nur subjektiv als „vertretbar/unvertretbar“ oder als „vernünftig/unvernünftig“ bewertet werden.

11 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates v. 19.10.2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), ABL EU Nr. L 277/1.

12 Vgl. insoweit DSA ErwG Nr. 2, 9, 69 S. 2, 83 S. 2, 84, 88, 95 S. 2, 104 S. 3, 106 und 108.

einhergehende gesellschaftliche Risiken sowie koordinierte Manipulationen wie die unauthentic Nutzung eines Diensts (CIB), die Einrichtung von Scheinkonten und den Einsatz von Bots umschrieben.¹³

Das Fehlen einer gesetzlichen Definition des Begriffs „Desinformation“ hat zur Folge, dass insoweit auf nichtstaatliche Normen zurückgegriffen werden muss. So bezeichnet das Konzept der EU-Kommission zur Bekämpfung von Desinformation im Internet aus dem Jahr 2018 und dem folgend der EU-Verhaltenskodex zur Bekämpfung von Desinformation aus demselben Jahr Desinformation als „nachweislich falsche oder irreführende Informationen, die mit dem Ziel des wirtschaftlichen Gewinns oder der vorsätzlichen Täuschung der Öffentlichkeit konzipiert, vorgelegt und verbreitet werden und öffentlichen Schaden anrichten können“.¹⁴ Der Begriff des öffentlichen Schadens soll dabei weit zu verstehen sein und u. a. Bedrohungen für die demokratischen Prozesse sowie für Güter wie die Gesundheit der Unionsbürger, die Umwelt und Sicherheit umfassen.¹⁵ Auch das Untergraben des Vertrauens in die Funktionsfähigkeit der staatlichen Ordnung wird man dazu zählen können.

Nach dieser Definition muss es sich also um einen bewussten, vorsätzlichen Vorgang handeln, in dem nachweislich falsche oder jedenfalls bewusst irreführende Informationen mit Schädigungseignung verbreitet werden. Das Zusammenwirken dieser drei Komponenten – Gegenstand: nachweislich falsche oder irreführende Information, Ziel: vorsätzliche Täuschung der Öffentlichkeit, Wirkung: Schadenspotenzial – ist geeignet, den Begriff der Desinformation für juristische Zwecke einzugrenzen und von kommunikativ unbedenklichen Prozessen abzugrenzen: So kann etwa die Verbreitung der bewusst falschen Behauptung, die Bundestagswahl 2025 sei zu Gunsten oder Ungunsten einer bestimmten Partei manipuliert worden – etwa über gefälschte Briefwahlunterlagen oder durch Manipulationen seitens angeblicher Wahlhelfer in den Wahlbüros¹⁶ –, das Vertrauen in die Funktionsfähigkeit der demokratischen Ordnung untergraben und damit kurz-, mittel- und langfristig einen Schaden verursachen (etwa durch die Abwendung der Bürger vom Staat, durch falsch informierte künftige Wahlentscheidungen oder sogar durch so ausgelöste Gewaltakte); eine Desinformation mit Schädigungspotenzial sollte deshalb staatliche Reaktionen ermöglichen und nach sich ziehen. Der bewusst falschen Behauptung, die Erde sei eine Scheibe, fehlt ein solches Schädigungspotenzial indes im Regelfall, weshalb eine staatliche Reaktion hier nicht geboten erscheint.¹⁷

13 So die treffende Analyse von Peukert, JZ 2023, 278 (279).

14 Europäische Kommission COM(2018) 236, S. 4; EU-Verhaltenskodex zur Bekämpfung von Desinformation, 2022, Präambel I. lit. a). S. ferner European Commission, Final Report of the High Level Expert Group on Fake News and Online Disinformation v. 12.3.2018, S. 10; EU-Kommission, Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Europäischer Aktionsplan für Demokratie, COM(2020), 790 final, S. 22; DSA ErwG Nr. 104 S. 3, wo Desinformation in den Zusammenhang mit vorsätzlich unrichtige Informationen gestellt wird; Peukert, JZ 2023, 278 (279 f.); bitkom, Policy Brief, S. 1. Durch die Inbezugnahme des Verhaltenskodexes in DSA ErwG Nr. 106 wird diese Definition für den DSA mit einer gewissen normativen Verbindlichkeit eingeführt; so auch Peukert, a.a.O.

15 Europäische Kommission/Hohe Vertreterin der Union für Außen- und Sicherheitspolitik, Gemeinsame Mitteilung an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Aktionsplan gegen Desinformation, JOIN(2018) 36 final v. 5.12.2018, S. 1. S. ferner DSA ErwG Nr. 95, wo auf reale und absehbare negative Auswirkungen auf die öffentliche Gesundheit oder Sicherheit, den gesellschaftlichen Diskurs, die politische Teilhabe und die Gleichbehandlung abgestellt wird.

16 Speziell zur Nutzung von Desinformation bei Wahlen Schlömer/Kehrberg, ZRP 2025, 2.

17 Ggf. glaubt die Person sogar an diese Behauptung. Dann läge noch nicht einmal eine Desinformation vor, sondern eine Meinungsäußerung oder ein Glaubenssatz. Wie hier als hinreichend präzise qualifiziert den Begriff der Desinformation

Das vorstehend skizzierte Begriffsverständnis ist von den interviewten Experten im Regelfall zugrunde gelegt und nicht kritisch bewertet worden.

B) MISINFORMATION

Misinformation (Fehlinformation) hingegen bezeichnet eine Information, die inhaltlich falsch oder irreführend ist, vom Äußernden aber nicht mit der Absicht zur Täuschung der Rezipienten verbreitet wird. Folglich ist sich der Äußernde der Unrichtigkeit der von ihm verbreiteten Information nicht bewusst. Dennoch kann auch eine solche Fehlinformationen schädliche Folgen haben.¹⁸

Bei derartigen Misinformationen handelt es sich um einen alltäglichen Vorgang, wie er ständig in Kommunikationsprozessen auftritt, etwa durch eine ungewollt fehlerhafte Pressemitteilung oder mediale Berichterstattung. In der Regel lösen derartige Informationen nur begrenzte rechtliche Reaktionsmöglichkeiten (etwa in Gestalt eines Anspruchs auf Richtigstellung, Gegendarstellung oder Unterlassung) aus. Wie noch zu zeigen sein wird, sind sie deshalb rechtlich anders zu bewerten als Desinformationen im vorbeschriebenen Sinne und bilden im Rahmen dieser Untersuchung keinen Analyseschwerpunkt.

C) FAKE NEWS

Der seit der US-Präsidentenwahl 2016 stark verbreitete Begriff „Fake News“ wurde aufgrund des Vorschlags einer Expertengruppe der EU-Kommission in ihrem Bericht vom März 2018 durch den Begriff „Desinformation“ ersetzt, weil er einschränkend und irreführend sei.¹⁹ Tatsächlich umfasst der Begriff in einer unscharfen Art und Weise eine weite Spanne von Kommunikationsinhalten – von der Desinformation i.e.S. (a)), über die Misinformation (b)) bis hin zu einer abweichenden und vom Äußernden als inakzeptabel angesehen Meinung. So wird man etwa die Äußerung von *Alice Weidel*, Adolf Hitler sei ein Kommunist gewesen, als Beispiel für eine „Fake News“ diskutieren können, bei der eine unrichtige Tatsachenbehauptung (*Adolf Hitler* war Gründer der NSDAP, nicht aber Mitglied der KPD) mit einer Meinungsäußerung (*Adolf Hitler* habe eine als kommunistisch zu qualifizierende Politik betrieben) verschmilzt. Der Begriff ist deshalb als ein (vor allem in den USA geläufiger) politischer Kampfbegriff zu qualifizieren²⁰, der infolge seiner Weite und Unschärfe nicht für eine juristische Analyse taugt. Die interviewten Experten sprachen sich ebenfalls klar gegen eine Nutzung dieses Begriffs aus.

ebenfalls Peukert, JZ 2023, 278 (279). Anders demgegenüber Ladeur, KR 2024, 477 (480), dem zufolge es schon schwierig zu beschreiben ist, was unter Desinformation zu verstehen sei oder gar Desinformation so zu definieren, dass damit Begriffsmerkmale für eine rechtliche Aufgabenbestimmung zu gewinnen wären.

18 Peukert, JZ 2023, 278 (280).

19 European Commission, Final Report of the High Level Expert Group on Fake News and Online Disinformation, 12.3.2018, S. 10; Brauneck, EuR 2020, 89 (90).

20 Vgl. insoweit auch Brauneck, EuR 2020, 89 (90 f.).

D) PROPAGANDA

Der Begriff „Propaganda“ ist ähnlich unscharf wie der Begriff „Fake News“ und deshalb mit diesem wesensverwandt. Propaganda versucht, die Einstellungen und Verhaltensweisen von Menschen zu beeinflussen. Dabei ist sie durch ein instrumentelles Verhältnis zur Wahrheit gekennzeichnet, weshalb sie sowohl falsche als auch wahre Informationen für ihre Zwecke nutzt.

Eine besondere Form der Propaganda ist die Kriegspropaganda. Diese ist gemäß Art. 20 Abs. 1 des Internationalen Pakts über Bürgerliche und Politische Recht (IPBPR) vom 19. Dezember 1966²¹ verboten. Da nahezu alle Staaten der Erde diesen sog. Zivilpakt ratifiziert haben, wird das Verbot auch als Völkergewohnheitsrecht angesehen und bindet damit die Mitgliedstaaten der EU, aber auch die EU als internationale Organisation selbst. Zudem kann dieses Verbot als ein allgemeiner Grundsatz des EU-Rechts qualifiziert werden.²²

Unter Kriegspropaganda ist das Werben für einen völkerrechtswidrigen Angriffskrieg zu verstehen, wie ihn Russland derzeit gegen die Ukraine führt. Als Rechtsbegriff spielt diese Form der Kommunikation vorliegend eine Rolle, auf die noch zurückzukommen sein wird.²³

3. VORTEILE DES INHALTSNEUTRALEN BEGRIFFSVERSTÄNDNISSES

Es liegt auf der Hand, dass zwischen dem unter 1. dargestellten Begriff der Manipulation des öffentlichen Informationsraums und den vorstehend skizzierten inhaltlichen Informationsbegriffen Überschneidungsbereiche existieren: So zielen die unter 1. dargestellten technischen Manipulationen des öffentlichen Informationsraums insbesondere darauf ab, kampagnenartig Desinformationen zu verbreiten.²⁴ Aber auch eine Verbreitung von Misinformationen, „Fake News“ oder Propaganda ist vorstellbar. Die Begrifflichkeiten stehen deshalb in einem Verhältnis von Mittel (Instrument der technischen Manipulation) und Gegenstand (Desinformation etc.) zueinander.

Der Vorteil einer Anknüpfung an die sub a) dargestellte inhaltsneutrale Formulierung liegt indessen darin, dass hierdurch einerseits vermieden werden kann, dass eine Information als richtig oder falsch oder als Bestandteil einer Meinungsäußerung, also inhaltlich, zu bewerten ist. Dies kann im Einzelfall schwierig und aufwändig sein, zu Unrecht staatliche Maßnahmen in einem demokratiesensiblen Bereich auslösen und zudem den Vorwurf der privaten oder hoheitlichen Meinungsmanipulation oder gar Zensur hervorrufen.²⁵ An einem solchen inhaltsbezogenen Vorgehen entzündeten sich deshalb immer wieder Kritik und Missverständnisse, gerade im internationalen Kontext mit seinen unterschiedlichen Auffassungen zur Reichweite der Meinungsfrei-

21 BGBl. 1973 II S. 1534. Namentlich heißt es dort: „Jede Kriegspropaganda wird durch Gesetz verboten.“

22 Baade, EuR 2020, 653 (654 ff.); ders., verfassungsblog v. 8.3.2022.

23 S. dazu unten § 2 C. I. 1. a).

24 S. hierzu DSA EwG Nr. 104, wo im Zusammenhang mit Desinformation auf Bots und Scheinkonten Bezug genommen wird. Zwingend ist dies freilich nicht. Man denke etwa an einen durch Manipulation gepushten Tweet, der keine Falschinformation, sondern lediglich eine bestimmte Meinungsäußerung enthält.

25 Entgegen der Informationsvorlage für die 353. Sitzung der DLM am 23.9.2025 in Leipzig, Top 6.3.2, S. S. 3 ist eine solche Bewertung der in Rede stehenden Information aber nicht per se unzulässig.

heit.²⁶ Schnell steht dann der kritische oder bewusst destruktive Vorwurf²⁷ einer privaten oder staatlichen Zensur im Raum, die vermeintlich darauf abziele, bestimmte, als politisch nicht korrekt oder unliebsam empfundene Meinungsäußerungen zu unterdrücken. Die Diskussion um den Koalitionsvertrag von CDU und SPD mit seinem Hinweis zur Bekämpfung von Desinformation²⁸ und die sich hieran entzündende mediale Diskussion²⁹ liefert ein anschauliches Beispiel hierfür. Auch wenn diese Zensurvorfälle *de jure* zumeist völlig unbegründet sind³⁰, beinhalten sie doch unbestreitbar das Potenzial, die rechtspolitische Diskussion um das Phänomen „Desinformation“ und die von ihr ausgehenden Gefahren politisch und gesellschaftlich zu desavouieren und Widerstände hervorzurufen sowie neue Des- und Misinformation zu generieren. Hinzu kommt, dass Desinformationen, Misinformationen und Fake News mitunter schwer von Meinungsäußerungen zu trennen sind: Bei der bereits beispielhaft erwähnten Äußerung von *Alice Weidel* etwa bedarf es einer Interpretation, ob es sich hierbei um eine Meinungsäußerung oder um eine Tatsachenbehauptung handelt. Zum Teil verschwimmen die Grenzen hin zur Satire oder es wird geltend gemacht, dass etwas satirisch zu verstehen gewesen sein soll.³¹ Teils dürfte es auch schwer zu begründen und bewerten sein, ob von einer Desinformation tatsächlich eine schädigende Wirkung für den Kommunikationsprozess ausgeht.³² Von daher empfiehlt sich eine Herangehensweise, die den Begriff der Desinformation vermeidet oder jedenfalls nicht in das Zentrum ihrer Betrachtung stellt.

Andererseits legt die inhaltsneutrale Formulierung den Fokus der Beobachtung und des Reaktionsgeschehens auf den eigentlich als problematisch empfundenen Umstand, dass der öffentliche Informationsraum durch manipulative Techniken verfälscht wird oder verfälscht zu werden droht. Diese Beobachtung lässt sich von der zutreffenden Erwägung leiten, dass nicht die einzelne Desinformation, sondern die gezielte massenhafte, kampagnenartige Verbreitung desinformativer oder propagandistischer Inhalte mit Schädigungsabsicht den Meinungsbildungsprozess illegitim verzerren und den eigentlichen Anknüpfungspunkt für gesetzgeberische und rechtliche Maßnahmen bilden sollten. Dieses Vorgehen hat nicht nur den Vorteil, dass es meinungsneutral

26 Instrukтив hierzu Möller, Meinungsfreiheit, S. 320 ff., der darauf hinweist, dass der Schutzbereich der Meinungsfreiheit in den USA teils weiter und teils enger als in Deutschland sei und sich die wesentlichen Unterschiede zwischen dem Grundrechtsschutz erst aus dem effektiven Garantiebereich der Grundrechte (also der Einschränkung durch den einfachen Gesetzgeber) ergäbe. Für den hier relevanten Kontext ist allerdings hervorzuheben, dass in den USA auch unwahre Tatsachenbehauptungen geschützt sein können und die amerikanische Grundrechtsdoktrin eine „mittelbare Drittwirkung“ der Meinungsfreiheit nicht kennt.

27 Eingehend hierzu Andree, Krieg der Medien, S. 36 f.

28 Namentlich heißt es im Koalitionsvertrag zwischen CDU, CSU und SPD zur 21. Legislaturperiode, Verantwortung für Deutschland, S. 123: „Gezielte Einflussnahme auf Wahlen sowie inzwischen alltägliche Desinformation und Fake News sind ernste Bedrohungen für unsere Demokratie, ihre Institutionen und den gesellschaftlichen Zusammenhalt. Die bewusste Verbreitung falscher Tatsachenbehauptungen ist durch die Meinungsfreiheit nicht gedeckt. Deshalb muss die staatsferne Medienaufsicht unter Wahrung der Meinungsfreiheit auf der Basis klarer gesetzlicher Vorgaben gegen Informationsmanipulation sowie Hass und Hetze vorgehen können.“

29 Vgl. hierzu etwa Karin König, Meinungsfreiheit durch Koalitionsvertrag gefährdet?, tagesschau v. 17.4.2025, abrufbar unter: <https://www.tagesschau.de/faktenfinder/kontext/meinungsfreiheit-koalitionsvertrag-100.html> (letzter Abruf: 30.4.2026).

30 Dazu noch nachstehend § 2 II. 2. c).

31 Z. B. mit Blick auf einen Video-Spot, wonach Bundeskanzler *Friedrich Merz* angeblich eine Kilometer-Steuer durchsetzen will; vgl. hierzu <https://correctiv.org/faktencheck/hintergrund/2025/12/23/welche-narrative-und-falschbehauptungen-2025-praegten/> (letzter Abruf: 30.4.2026).

32 Als Bsp. mag insoweit auf die Behauptung, die EU wolle das Bauen von Schneemännern verbieten, Bezug genommen werden. Die Mehrzahl der Rezipienten wird diese Äußerung, so sie nicht satirisch gemeint war, sofort als Desinformation erkannt haben. Dennoch ist nicht auszuschließen, dass die Meldung Wut und Verstörung über die EU hervorzurufen und zu bekräftigen im Stande ist. Jedenfalls bedarf die Wirkung dieser Behauptung einer schwierigen Bewertung.

erfolgt und hierdurch die Akzeptanz für solche Maßnahmen bei den am Kommunikationsprozess Teilnehmenden gesteigert wird. Es hat zugleich den Vorteil, dass diese Art des Vorgehens einen sehr effektiven Hebel bietet, um gegen derartige Manipulationen der öffentlichen Meinungsbildung einzuschreiten, da nicht einzelne Inhalte, sondern meinungsverzerrende Kampagnen und Praktiken „bekämpft“ werden können. Der Begriff bezeichnet deshalb inhalts- und wertneutral sowie präzise, worum es beim Kampf gegen Desinformation, Misinformation, Fake News oder Propaganda eigentlich geht, nämlich um die illegitime Einflussnahme auf einen fairen und offenen Meinungsbildungsprozess. In den Experteninterviews schimmerte denn auch eine starke Sympathie für diese neue Umschreibung durch, so vor allem bei den Experten aus der Aufsichtssphäre, da die Verhinderung technischer Manipulationen des Informationsraums nach dem institutionellen Selbstverständnis im Zentrum ihrer Arbeit stehe und nicht der Kampf um die Richtigkeit oder Unrichtigkeit einzelner Informationen.³³

Dieses inhaltsneutrale Begriffsverständnis spiegelt sich denn auch in den Regelungen und Dokumenten zur Bekämpfung von Desinformation wider: Die Desinformation wird dort nicht selten in einem Atemzug mit manipulativen oder missbräuchlichen Tätigkeiten (wie etwa koordinierte Tätigkeiten zur Verstärkung bestimmter Informationen durch Bots oder Scheinkonten) genannt.³⁴ Letztlich liegt dieses Begriffsverständnis auch den bisherigen Strategien der EU-Kommission im Kampf gegen Desinformation zugrunde, die dementsprechend von einem weiten Desinformationsbegriff ausgehen, der neben der vorstehend dargestellten Desinformation i.e.S. auch Misinformationen sowie Einflussoperationen inländischer und ausländischer Akteure durch technische und sonstige Maßnahmen umfasst.³⁵ Der Kampf gegen Desinformation ist deshalb schon immer auch als ein Kampf gegen manipulative (technische) Einflussnahmen aus dem In- und Ausland begriffen worden, weshalb die weitere Untersuchung unter dem Oberbegriff der „Manipulation des öffentlichen Informationsraums“ erfolgt.

Allerdings ist nicht zu leugnen, dass mit dieser inhaltsneutralen Formulierung andere klärungsbedürftige Unschärfen einhergehen können. So ist insbesondere zu klären, was eine unzulässige Manipulation des öffentlichen Kommunikationsraums ausmacht. Denn nicht jede Verbreitung einer Information unter geschickter Inanspruchnahme technischer Konfigurationen (Algorithmen) wird zugleich als eine rechtlich problematische Manipulation des öffentlichen Informationsraums zu bewerten sein können.³⁶ Von daher wird zu klären sein, wann eine Manipulation tatsächlich rechtlich problematisch ist und deshalb einen legitimen Gegenstand legislativer oder exekutiver Maßnahmen darzustellen vermag.

33 So wurde explizit betont, dass man kein „Wahrheitsministerium“ sein wolle. Vereinzelt wurde die Formulierung „Manipulation des öffentlichen Informationsraums“ allerdings auch kritisiert, da sie von dem im nationalen und internationalen Diskurs etablierten Begriff der Desinformation ablenke und einen als unnötig empfundenen neuen Begriff in die Debatte einführe. Andere Gesprächspartner wiesen darauf hin, dass die Formulierung der „technischen Manipulation des öffentlichen Informationsraums“ enger sei als der Begriff der Desinformation und diesen deshalb nicht vollständig substituieren könne.

34 Beispielhaft kann insoweit erneut auf DSA ErWG Nr. 104 S. 2 u. 3 verwiesen werden. S. ferner DSA ErWG Nr. 95.

35 Vgl. EU-Kommission, Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Europäischer Aktionsplan für Demokratie, COM(2020), 790 final, S. 22; EU-Verhaltenskodex zur Bekämpfung von Desinformation, 2022, Präambel I. lit. a mit Fn. 5 – 10. Vgl. ferner Peukert, JZ 2023, 278 (280) sowie DSA ErWG Nr. 5 und 68, die insoweit neben rechtswidrigen Inhalten auch von „anderweitig schädliche(n) Informationen und Tätigkeiten“ sprechen.

36 Vgl. auch Peukert, JZ 2023, 278 (280): „Lanciert ein einzelner Twitter-Nutzer, der einen #Hashtag vorschlägt, eine koordinierte Einflussoperation?“

II. VERFAHREN DER MANIPULATION DES ÖFFENTLICHEN INFORMATIONSRAUMS

Dies leitet zu der Untersuchung über, was unter manipulativen Taktiken und Mechaniken zur Verbreitung bestimmter Inhalte (wie insbesondere Desinformation) zu verstehen ist. Insoweit kann beobachtet werden, dass sich derartige Taktiken immer stärker professionalisieren, sprich mit immer raffinierteren Methoden darauf abzielen, das Vertrauen in Medien, Politik sowie demokratische Institutionen und Werte zu erschüttern.

Bei der Manipulation des öffentlichen Informationsraums können technische und gestalterische Aspekte unterschieden werden:

1. TECHNISCHE ASPEKTE

Die Manipulation des öffentlichen Informationsraums kann zum einen technisch erfolgen. Als solche technische Manipulation ist vor allem die Manipulation der Reichweite (a)) und die Verschleierung des Absenders (b)) zu identifizieren. Beide Vorgehensweisen können dabei auch miteinander verknüpft sein, um ihren manipulativen Charakter zu verstärken.³⁷

A) TECHNISCHE MANIPULATION DER REICHWEITE

Die technische Manipulation der Reichweite zielt – wie gesehen – darauf ab, einem bestimmten Inhalt (wie z. B. einer Desinformation) eine höhere Relevanz im gesellschaftlichen Diskurs bzw. eine höhere Zustimmung/Ablehnung zu einer Position zu verleihen. Dies erfolgt insbesondere durch eine bot-gesteuerte Verstärkung gefälschter oder gekaufter Interaktionen (etwa in Form von Likes, Kommentaren und Links) oder durch ein koordiniertes unauthentisches Verhalten (Coordinated Inauthentic Behaviour – CIB), das seinerseits bot-gesteuert (etwa durch automatisierte Accounts) umgesetzt werden kann. Diese technische Manipulation der Reichweite kann dabei über unterschiedliche Verbreitungswege ausgespielt werden: In Betracht kommt eine Verbreitung als Post in Messenger-Diensten und sozialen Netzwerken, über E-Mail-Dienste, in Form von Webseiten oder als politische Werbung auf Plattformen.

Diesen Vorgehensweisen ist gemein, dass sie mit einer bewussten Informationsasymmetrie arbeiten, weshalb der Empfänger eines bestimmten Inhalts (Nutzer) sich über den Einsatz technischer Hilfsmittel (etwa eines Chatbots, der in Form von Kommentaren oder Likes auf bestimmte Tweets oder Fragen automatisiert reagiert³⁸) oder bestimmter anderer Aspekte (wie

³⁷ Streng genommen, handelt es sich bei der Verschleierung des Absenders nicht um eine technische Manipulation, sondern um die Täuschung über einen Absender und damit um eine inhaltliche Manipulation. Da hierzu aber im Regelfall ein gewisser technischer Aufwand erforderlich ist (Einrichten von Konten, Bauen einer Webseite etc.) und diese Manipulation mit einer technischen Manipulation der Reichweite verknüpft sein kann, soll diese Vorgehensweise nachstehend unter dem Rubrum „technische Manipulation des öffentlichen Informationsraums“ behandelt werden.

³⁸ Laut Roth-Isigkeit, DVBl. 2025, 1059 (1061) m.w.N. sollen bereits 20% der Online-Kommunikation von (Social) Bots stammen.

dem Kauf von Likes und Kommentaren oder einer unauthentisch-automatisierten Koordinierung von Likes und Kommentaren) nicht im Klaren ist. Durch Intransparenz täuscht der Verwender solcher technischen Manipulationen mithin den Nutzer, indem er ihm eine wesentliche Information (technische Manipulation) mit Relevanz für dessen individuelle Meinungsbildung vorenthält. Der Nutzer ist infolgedessen nicht mehr in der Lage, den Stellenwert und die Authentizität bestimmter Handlungen (Kommentare, Antworten, Likes etc.) zu bewerten, da der Absender sein Vorgehen verschleiert.

Insoweit unterscheidet sich dieser Vorgang der technischen Manipulation der Reichweite von anderen Vorgängen, bei denen unter Ausnutzung bestimmter (algorithmischer) Verbreitungstechniken (wie z. B. die Search Engine Optimization – SEO – oder das authentische Liken und Kommentieren von Beiträgen) lediglich versucht wird, der eigenen oder fremden Information und Meinungsäußerung im öffentlichen Diskurs mehr Gewicht durch höhere Reichweite zu verleihen. Hier verschleiern die Nutzer ihr Vorgehen nicht, da sie die von den Plattformen und Suchmaschinen zugelassenen und jedermann zur Verfügung stehenden Möglichkeiten einsetzen, um ihrem Handeln im Internet mehr Sichtbarkeit und Relevanz zu verleihen.

B) VERSCHLEIERUNG DES ABSENDERS

Eine technische Manipulation des öffentlichen Informationsraums kann auch durch eine Verschleierung des Absenders erfolgen. Wie gesehen, zielt diese darauf ab, von der Autorität oder dem Ausnutzen des Vertrauens, das der eigentlichen Identität entgegengebracht wird, zu profitieren. Dies kann etwa durch gefälschte Accounts bekannter Persönlichkeiten (Politiker) oder durch gefälschte Medienangebote (unter Einschluss von Rundfunk- und Pressediensten), gefälschte Webseiten oder Deepfakes von Medienangeboten erfolgen. Die Fälschungen werden im Rahmen der „Doppelgänger“-Kampagne genutzt, d.h. als Kopie von Webauftritten behördlicher oder privater Institutionen (wie z. B. einem Printmedium)³⁹ bezeichnet.⁴⁰

Auch diese Vorgehensweise, der eine technische Manipulation des öffentlichen Informationsraums durch die Fälschung eines Internetauftritts zugrunde liegt, bedient sich mithin einer Verschleierung, d.h. einer bewussten Täuschung der anderen Kommunikationsteilnehmer. Insoweit unterscheidet sie sich klar von anderen Vorgängen der offenen Kommunikation durch die wahren Absender oder Kommunikatoren.

In einer erweiterten Sicht können hierunter auch Rundfunk-, Presse- oder Post-Beiträge gefasst werden, hinter denen bestimmte Institutionen (z. B. ausländische Staaten) stehen, die diesen Zusammenhang nicht offenlegen oder bewusst verschleiern. Hier fehlt es zwar an einer technischen Manipulation im eigentlichen Sinne (automatisierte Erhöhung der Reichweite oder Bau von Deepfake-Webseiten). Indes bedient sich diese Art der Einflussnahme auf den Kommunika-

39 Als weiteres Bsp. neben denjenigen in Fn. 9 kann hier auf die gefälschte Nachrichtenseiten der Süddeutschen Zeitung verwiesen werden; vgl. insoweit Jörg Schmitt, Süddeutsche Zeitung v. 12.8.2024, abrufbar unter: <https://www.sueddeutsche.de/projekte/artikel/politik/russland-fake-news-deutschland-nachrichtenseiten-bayern-e545166/?reduced=true> (letzter Abruf: 30.4.2026).

40 Näher dazu Schlömer/Kehrberg, ZRP 2025, 2 (3).

tionsprozess ebenfalls einer Verschleierung und kann ggf. mit Maßnahmen zur technischen Manipulation der Reichweite verknüpft sein.

2. INHALTLICHE ASPEKTE

Eine Manipulation des öffentlichen Informationsraums erfolgt indessen nicht nur über technische Manipulationen. Auch die Verbreitung von Desinformation oder Propaganda soll dazu beitragen, den öffentlichen Informationsraum und damit den Meinungsbildungsprozess zu manipulieren. Die Absender solcher Inhalte verschleiern hier nicht ihr technisches Vorgehen oder ihre Identität. Vielmehr treten sie offen auf (z. B. als Rundfunkveranstalter oder Webseitenbetreiber „Russia Today“ [RT]) und nutzen diesen Auftritt, um durch Desinformation und Propaganda den öffentlichen Kommunikationsprozess zu beeinflussen.

Die Formulierung „Manipulation des öffentlichen Informationsraums“ wird im Rahmen der vorliegenden Untersuchung deshalb weit verstanden: Er umfasst sowohl die technische als auch die inhaltliche Manipulation dieses Raums. Dort, wo es speziell um den einen (technische Manipulation) oder anderen (inhaltliche Manipulation) Aspekt geht, wird dies gesondert hervorgehoben. Ansonsten verwendet die Untersuchung die Formulierung „Manipulation des öffentlichen Informationsraums“, die sich auf beide Sachverhalte bezieht.

3. GESTALTERISCHE ASPEKTE

Aus dem vorstehend Ausgeführten erhellt zugleich, in welcher Gestalt eine Manipulation des öffentlichen Informationsraums erfolgt: Sie kann in Form von Textbeiträgen, Bildern, Memes⁴¹, audiovisuellen Beiträgen, Audio-Beiträgen oder Podcasts Verbreitung finden. Sie kann sich linearer oder nichtlinearer Medien bedienen. Für die Erzeugung der manipulativ verbreiteten Inhalte wird zudem verstärkt sog. Künstliche Intelligenz (KI) eingesetzt, etwa um manipulierte Bilder oder Videosequenzen zu produzieren (Deepfakes).⁴²

41 Hierbei handelt es sich um humorvolle Bilder, Videos oder Texte, die über das Internet und dort vor allem über soziale Netzwerke verbreitet werden.

42 Zum Begriff der Deepfakes s. Art. 3 Ziff. 60 KI-VO, der diese als „einen durch KI erzeugten oder manipulierten Bild-, Ton- oder Videoinhalt, der wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähnelt und einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheinen würde“ definiert. Laut bitkom, Policy Brief, S. 16 lassen sich als Arten von Deepfakes „Face Swapping“ (Manipulation von Bildern und Videos), „Body Puppetry“ (Manipulation von Bewegungen) und „Voice Swapping“ (Manipulation von Audioinhalten) unterscheiden, wobei diese Arten regelmäßig miteinander kombiniert würden.

B. FALLSTUDIEN

Zweck der Fallstudien ist es zum einen, als tatsachenbasierte Sachverhaltsschilderungen die im Gutachten zu analysierenden Rechtsfragen zu veranschaulichen. Zum anderen tragen die Fallstudien dazu bei, den Blick für die zu untersuchenden Rechtsfragen zu schärfen, sprich einen Beitrag dazu zu leisten, die für den Untersuchungsgegenstand relevanten Rechtsgrundlagen, die für den Vollzug dieser Rechtsgrundlagen zuständigen Behörden, die Interaktion zwischen parallel zuständigen Behörden sowie eventuelle exekutive Übergabepunkte zu identifizieren. Dies soll es ermöglichen, fallbaumartig Eskalationsstrukturen der Umsetzung des Regelungsgefüges gegen technische Manipulationen subsumtiv durchzuexerzieren. Schließlich können durch diese fallbasierte Herangehensweise Regelungs- oder Zuständigkeitslücken sowie Defizite bei der exekutiven Kooperation oder Übergabe von Manipulationssachverhalten aufgedeckt und die Entwicklung von Lösungsansätzen zum Umgang mit diesen Lücken und Defiziten erleichtert werden. Diese Lösungsansätze könnten etwa in der Erkenntnis bestehen, welche weiteren Akteure zur effektiven Bekämpfung von technischen Manipulationen einbezogen werden sollten.

Infolge der Vielgestaltigkeit von Manipulationssachverhalten werden die zu untersuchenden Fallstudien anhand von Themenstellungen auf einer mittleren Abstraktionsebene kategorisiert. Diese Themenstellungen orientieren sich an dem oben (A.) herausgearbeiteten Begriff der Manipulation des öffentlichen Informationsraums als dem Kern des Untersuchungsgegenstands. Neben der Identifikation und Verfeinerung dieser Fallgruppen durch eine Analyse amtlicher Dokumente sowie der rechts- und kommunikationswissenschaftlichen Literatur haben auch die Experteninterviews mit Vertretern von Behörden und zivilgesellschaftlichen Organisationen zu einer Gestaltung dieser Fallstudien beigetragen.

I. NUTZUNG VON ONLINE-PLATTFORMEN ZUR TECHNISCHEN MANIPULATION DER REICHWEITE

In diesem Fallszenario manipulieren Personen über Online-Plattformen (soziale Netzwerke)⁴³ mit Sitz im Inland, im EU-Ausland oder in Drittstaaten den öffentlichen Kommunikationsraum. Sie tun dies durch eine bot-gesteuerte Verstärkung gefälschter oder gekaufter Interaktionen (unter Einschluss von Werbung) bzw. durch ein automatisiert-koordiniertes unauthentisches Verhalten (CIB). Wie gesehen, spielen automatisierte Accounts und Bots eine zentrale Rolle bei der technischen Manipulation des öffentlichen Kommunikationsraums, da sie u. a. in der Lage sind, große Mengen bestimmter Inhalte zu disseminieren oder gezielt bestimmte Inhalte zu „ liken“ oder zu kommentieren, um infolge dieser verschleierte Interaktionen deren algorithmische Verbreitung zu fördern.⁴⁴ Nicht selten gehen solche Verhaltensweisen von im Ausland sitzenden „Troll-Fa-

43 Der Begriff „Online-Plattform“ wird hier i.S.d. Art. 3 lit. i) i.V.m. lit. g) iii) DSA verstanden und bezeichnet einen Hosting-Dienst, der im Auftrag eines Nutzers Informationen speichert und öffentlich verbreitet. In der öffentlichen Diskussion werden derartige Dienste häufig als „soziale Netzwerke“ qualifiziert. Typische Beispiele hierfür sind Facebook, Instagram, TikTok und YouTube oder Messenger-Dienste wie Signal, Telegram, WhatsApp und X.

44 Vgl. Gehringer, NJ 2024, B 18 (B 19) sowie oben § 2 A. II. 1. a).

briken“ aus. Die für solche „Fabriken“ handelnden Personen („Trolle“) verbreiten durch derartige Manipulationen – meist konzertiert, d.h. kampagnenartig – Desinformation in großem Stil, um den öffentlichen Willensbildungsprozess zu Gunsten ihrer Auftraggeber zu beeinflussen.⁴⁵ Umgekehrt können solche technischen Manipulationen auch genutzt werden, um Melde- und Beschwerdeverfahren zur Beeinträchtigung seriöser Inhalte zu missbrauchen.⁴⁶ Stets ist es das Ziel dieser Manipulationen, für eine vermeintlich höhere Relevanz im gesellschaftlichen Diskurs bzw. eine höhere Zustimmung/Ablehnung zu einer bestimmten Position zu erzeugen. Die Personen operieren dabei als Privatpersonen, im Auftrag von inländischen Organisationen (wie z. B. Parteien) oder im Auftrag ausländischer Staaten aus der EU⁴⁷ oder einem Drittstaat (wie z. B. China oder Russland).

Aufsichtsbehörden stellen sich vor diesem Hintergrund die Frage,

- wie sie präventiv bzw. repressiv gegen manipulierende Personen bzw. ihre Verhaltensweisen (Verschleierung) vorgehen können, d.h. unter welchen Voraussetzungen dies möglich ist und wie sich das Verfahren gestaltet, insbesondere, wenn diese Personen in einem anderen EU-Mitgliedstaat oder in einem Drittstaat leben. Auch fragen sie sich, ob und wie es effektiv verhindert werden können, dass diese Personen ggf. gesperrte Plattform-Accounts unter anderen, leicht modifizierten Namen oder Titeln, schnell wieder eröffnen, um ihre technischen Manipulationen fortzusetzen;⁴⁸
- welche rechtlichen Verpflichtungen und Möglichkeiten (wie z. B. Sperren, Löschen oder Kennzeichnen) die Online-Plattformen in Bezug auf das geschilderte Verhalten haben. Auch fragen sie sich, welche rechtlichen Verpflichtungen und Möglichkeiten die Plattformen haben, um einem gezielten Missbrauch von Melde- bzw. Beschwerdesystemen durch eine automatisierte Überfrachtung zu begegnen. Zudem fragen sie sich, ob eine unzulässige unauthentische Koordination (CIB) unter Influencern oder sonstigen Personen auch dann vorliegt, wenn diese als Gegenstand einer Absprache die Reichweite ihrer Inhalte durch wechselseitiges Kommentieren, Liken, Teilen und Verlinken steigern;⁴⁹
- welche rechtlichen Möglichkeiten sie selbst haben, um Plattformen zur Einhaltung dieser Verpflichtungen und Möglichkeiten anzuhalten, wer insoweit zuständig ist, wie die Interaktion zwischen den öffentlichen Aufsichtsbehörden bei grenzüberschreitenden Sachverhalten erfolgt und ob die bestehenden rechtlichen Möglichkeiten zur Bekämpfung einer technischen Reichweitenmanipulation ausreichen. Insbesondere stellen sie sich die Frage, welche Faktoren die Reichweite von Posts beeinflussen⁵⁰ und was sie rechtlich mit Blick auf die

45 Vgl. Gehringer, NJ 2024, B 18 (B 19). Als Bsp. mag insoweit die Kampagne zur angeblichen Affäre der deutschen Außenministerin Annalena Baerbock mit einem afrikanischen Gigolo dienen.

46 Ein solches Vorgehen wird schlagwortartig als „Operation Overload“ bezeichnet.

47 Zu letzterem vgl. Mehlan, MMR-Aktuell 2024, 01416, die über eine Werbekampagne des Kabinettsbüros des früheren ungarischen Premiers Viktor Orbán auf YouTube zu den vermeintlichen Gefahren illegaler Migration berichtet, die in sieben EU-Ländern (darunter Polen, die Slowakei, Deutschland und Italien) im Zusammenhang mit Wahlen verbreitet und millionenfach geklickt wurden.

48 Vgl. hierzu Thilo Komma-Pöllath/Stefan Herwig, Bei Youtube tummeln sich die Verschwörungsprediger, FAZ v. 26.11.2024.

49 Vgl. hierzu erneut Thilo Komma-Pöllath/Stefan Herwig, Bei Youtube tummeln sich die Verschwörungsprediger, FAZ v. 26.11.2024.

50 Bekannt ist bspw., dass u. a. die Gestaltung von Posts (Versalien, Farbwahl – rot; Wortwahl: Signalwörter, die zuspitzen bzw. den Ausnahmezustand, ja die Apokalypse beschreiben wie bspw. „zerstört“, „demütig“, „zerlegt“) und die Nutzungszahlen bzw. hohe Nutzer-Interaktionszahlen die Verbreitung sensationallyer und oft falscher Information begünstigen. Durch den Einsatz von Troll-Fabriken, Bots oder gekauften Kommentaren und Likes bietet dies die Möglichkeit, zu einer gezielten technischen Manipulation der Reichweite. Zum Vorstehenden vgl. Gehringer, NJ 2024, B 18 (B 19); Thilo

- Gestaltung der von den Plattformen eingesetzten Algorithmen unternehmen können;
- ob Personen bzw. zivilgesellschaftliche Institutionen, die auf technische Manipulationen aufmerksam machen wollen, ihrerseits ausreichende und effektive Möglichkeiten haben, dies zu tun und sich gegen ein Verhalten der Plattformen zu wehren vermögen, durch das sie gesperrt und (wie z. B. aus dem YouTube-Partnerprogramm) „entmonetarisiert“ werden sollen.⁵¹

II. NUTZUNG VON ONLINE-PLATTFORMEN ZUR VERSCHLEIERUNG DES ABSENDERS

In diesem Szenario bedienen sich Personen mit Sitz im Inland, im EU-Ausland oder in Drittstaaten gefälschter Konten bekannter Persönlichkeiten, gefälschter Medienangebote, gefälschter Webseiten oder Deepfakes von Medienangeboten. Ziel dieser Verschleierung ist es, von der Autorität oder vom Ausnutzen des Vertrauens zu profitieren, das den eigentlichen Identitäten entgegengebracht wird.⁵² Hierin unterscheidet sich dieses Szenario i.Ü. von der Manipulation der Reichweite, wo zwar ebenfalls mit Verschleierung (automatisierte Interaktionen) gearbeitet wird, aber nicht die Inanspruchnahme eines besonderen Autoritäts- oder Vertrauensverhältnisses im Vordergrund steht.

Aufsichtsbehörden stellen sich vor diesem Hintergrund die Frage,

- wie sie präventiv und repressiv gegen diese Personen bzw. ihre Verhaltensweisen (Verschleierung) vorgehen können, sprich unter welchen Voraussetzungen dies möglich ist und wie sich das Verfahren gestaltet, insbesondere, wenn diese Personen in einem anderen EU-Mitgliedstaat oder in einem Drittstaat leben. Auch fragen sie sich, ob und wie effektiv verhindert werden kann, dass diese Personen ggf. gesperrte Accounts unter anderen, leicht modifizierten Namen oder Titeln, schnell wieder eröffnen können, um ihre technischen Manipulationen fortzusetzen;⁵³
- welche Möglichkeiten die betroffenen Personen und Institutionen haben, sich gegen Instrumente der „Doppelgänger“-Kampagne zur Wehr zu setzen;
- welche rechtlichen Verpflichtungen und Möglichkeiten die Online-Plattformen in Bezug auf das geschilderte Verhalten haben;
- welche rechtlichen Möglichkeiten sie als Aufsichtsbehörden haben, um die Plattformen zur Einhaltung dieser Verpflichtungen anzuhalten, wer insoweit zuständig ist, wie die Interaktion zwischen den öffentlichen Aufsichtsbehörden bei grenzüberschreitenden Sachverhalten aussieht und ob die bestehenden Möglichkeiten ausreichen;

Komma-Pöllath/Stefan Herwig, Bei Youtube tummeln sich die Verschwörungsprediger, FAZ v. 26.11.2024.

51 Vgl. Thilo Komma-Pöllath/Stefan Herwig, Bei Youtube tummeln sich die Verschwörungsprediger, FAZ v. 26.11.2024.

52 Vgl. insoweit die vom Bayerischen Verfassungsschutz untersuchten „Doppelgänger“-Kampagnen, <https://www.stmi.bayern.de/media/presse-und-medien/news/2024/240812-baylfv-management-summary-doppelgaenger.pdf> (letzter Abruf: 30.4.2026).

53 Vgl. Thilo Komma-Pöllath/Stefan Herwig, Bei Youtube tummeln sich die Verschwörungsprediger, FAZ v. 26.11.2024.

- ob Personen oder zivilgesellschaftliche Institutionen, die auf eine Verschleierung des Absenders aufmerksam machen, ihrerseits ausreichende und effektive Möglichkeiten haben, um dies zu tun und sich gegen ein Verhalten der Plattformen zu wehren, durch das sie beispielsweise gesperrt und (wie z. B. aus dem YouTube-Partnerprogramm) „entmonetarisiert“ werden.

III. NUTZUNG VON KÜNSTLICHER INTELLIGENZ (DEEPAKES)

Zwar setzen Personen zur Verwirklichung der beiden ersten Fallstudien (I. und II.) regelmäßig KI ein, um ihre Ziele der Manipulation des öffentlichen Informationsraums zu erreichen, etwa durch die Gestaltung von Deepfakes, die Angst und Schrecken (Zugunglücke, Terrorfahrten, einstürzende Wahrzeichen, Anschläge auf Weihnachtsmärkte etc.) verbreiten, bzw. gefälschte Mitteilungen (wie z. B. audiovisuelle Statements hochrangiger Politikern⁵⁴) oder sonstige Video-Berichte⁵⁵ enthalten.⁵⁶

In dem sub III. zu erörternden Szenarien soll allerdings analysiert werden, welche besonderen rechtlichen Anforderungen bestehen, wenn KI für die Erzeugung von Deepfakes eingesetzt wird. Solche Techniken können im Übrigen auch als Gegeninstrument zur Erkennung und Bekämpfung manipulativer Verhaltensweisen genutzt werden.

Die Aufsichtsbehörden fragen sich vor diesem Hintergrund,

- wie sie präventiv und repressiv gegen diese Personen bzw. ihre Verhaltensweisen (Einsatz von Deepfakes) vorgehen können, d.h. unter welchen Voraussetzungen dies möglich ist und wie sich das Verfahren gestaltet (insbesondere, wenn die Person in einem anderen EU-Mitgliedstaat oder in einem Drittstaat lebt);
- welche rechtlichen Verpflichtungen oder Möglichkeiten die Online-Plattformen in Bezug auf das geschilderte Verhalten haben;
- welche rechtlichen Möglichkeiten die Aufsichtsbehörden selbst haben, die Online-Plattformen zur Einhaltung dieser Verpflichtungen anzuhalten, wer insoweit zuständig ist, wie die Interaktion zwischen den öffentlichen Aufsichtsbehörden bei grenzüberschreitenden Sachverhalten aussieht und ob die bestehenden Möglichkeiten ausreichen;
- in welchem Umfang es rechtlich zulässig oder sogar geboten ist, dass die Anwender von KI-Technologien (wie insbesondere Online-Plattformen, Suchmaschinen oder Large Language Models [LLMs]) softwarebasierte Instrumente einsetzen, die der Manipulation des öffentlichen Informationsraums entgegenwirken sollen. Auch fragen sie sich, wer zur Über-

54 Plakatives Beispiel: Friedrich Merz, dem durch eine Sprach-KI ein fremder Text („Die Rentner sollten aus diesem Land verschwinden!“) unterlegt wurde; vgl. dazu <https://correctiv.org/faktencheck/2025/12/12/die-rentner-sollten-aus-diesem-land-verschwinden-fake-merz-zitat-kursiert-seit-monaten/> (letzter Abruf: 30.4.2026).

55 Plakative Beispiele: Unzutreffender Bericht über die mit der Einführung des Euro verbundene Wirkungen auf die Inflation in Rumänien; Deep Fake-Video über eine muslimische Familie, die angeblich 6.000 €/Monat Sozialhilfe beziehe; vgl. erneut <https://correctiv.org/faktencheck/hintergrund/2025/12/23/welche-narrative-und-falschbehauptungen-2025-praegten/> (letzter Abruf: 30.4.2026).

56 Instrukтив dazu Tageschau, Mithilfe von KI gefälschte Videos: Das Ende der Wirklichkeit? v. 6.6.2025 (Interview m. Anna K. Bernzen), abrufbar unter: <https://www.tagesschau.de/faktenfinder/kontext/ki-fake-videos-100.html> (letzter Abruf: 30.4.2026). Allg. zur Nutzung von Deepfakes als Teil von Desinformationskampagnen Gehringer, NJ 2024, B 18 (B 19).

wachung dieser Instrumente zuständig ist;

- welche rechtlichen Möglichkeiten und Grenzen für einen KI-Einsatz durch die Aufsichtsbehörden selbst zwecks Bekämpfung von Manipulationen des öffentlichen Kommunikationsraums bestehen. Insbesondere fragen sie sich, ob dafür neue Rechtsgrundlagen geschaffen werden müssen;
- welche rechtlichen Möglichkeiten sie haben, um zu verhindern, dass Institutionen (wie insbesondere feindlich gesonnene ausländische Staaten) durch gezielte (Des-)Informationskampagnen LLMs, die zunehmend anstelle klassischer Online-Suchmaschinen für die Nachrichtensuche genutzt werden, gezielt dort beeinflussen, wo die LLM-Suche auf ein Material-Defizit aus seriösen Informationsquellen stößt (sog. „LLM-Grooming“), um hierdurch falsche oder missverständliche Narrative zu generieren.⁵⁷

IV. NUTZUNG JOURNALISTISCH-REDAKTIONELL GESTALTETER MEDIEN ZUR MANIPULATION DES ÖFFENTLICHEN INFORMATIONSRAUMS

Auch journalistisch-redaktionell gestaltete Medien, wie z. B. Fernsehsender, die (Online-)Presse oder sog. Influencer, werden dazu genutzt, um den öffentlichen Informationsraum zu manipulieren.⁵⁸ Prominente Beispiele hierfür sind „Russia Today“⁵⁹ und „Compact“.⁶⁰ Nicht selten planen diese Medien das Aufgreifen ihrer Meldungen durch andere Kanäle oder Plattformen in ihre Strategie mit ein, insbesondere um das vorstehend (III.) erwähnte „LLM Grooming“ zu ermöglichen. Hier steht nicht die technische, sondern die inhaltliche Manipulation⁶¹ – etwa durch klassische Desinformation oder sonst durch Verbreitung einseitig-verzerrender Narrative – im Vordergrund. Als Teil der Manipulation des öffentlichen Informationsraums soll dieses Verhalten deshalb in die Analyse miteinbezogen werden.

Aufsichtsbehörden fragen sich vor diesem Hintergrund,

- welche Möglichkeiten bestehen, die journalistisch-redaktionelle Tätigkeit eines linearen Rundfunksenders, eines nichtlinearen Online-Mediums bzw. eines Influencers aus Gründen der Wirtschaftssanktionierung zu unterbinden oder die Verbreitung eines Programms oder Kanals zu beschränken und wo insoweit rechtliche Grenzen verlaufen;
- welche Möglichkeiten bestehen, die journalistisch-redaktionelle Tätigkeit eines linearen Rundfunksenders, eines nichtlinearen Online-Mediums bzw. eines Influencers aus Gründen der Desinformation, Misinformation oder Propaganda zu beschränken oder die Verbreitung eines Programms oder Kanals zu unterbinden und wo insoweit rechtliche Grenzen verlaufen;

57 Vgl. hierzu Pablo Maristany de las Casas, Institute for Strategic Dialogue (ISD), Investigation/Talking Points: When chatbots surface Russian state media, 27.10.2025, abrufbar unter: https://www.isdglobal.org/digital_dispatches/talking-points-when-chatbots-surface-russian-state-media/ (letzter Abruf: 30.4.2026).

58 Vgl. Gehringer, NJ 2024, B 18 (B 20). S. ferner Schlömer/Kehrberg, ZRP 2025, 2 (5 f.).

59 Näher hierzu Setz/Seyda, ZD-Aktuell 2022, 01167 m.w.N.

60 Vgl. insoweit BVerwG, NVwZ 2024, 1764 ff. und BVerwG, Urt. v. 24.6.2025 – 6 A 4.24 = NJW 2025, 3650 ff. Für weitere Bsp. aus dem russischen und chinesischen Raum s. Gehringer, NJ 2024, B 18 (B 20).

61 S. oben § 2 A. II. 2.

- welche Möglichkeiten bestehen, den Trägerverein bzw. das Trägerunternehmen eines Mediendiensteanbieters mit vereins- oder gesellschaftsrechtlichen Mitteln zu verbieten und wo insoweit rechtliche Grenzen verlaufen („Compact-Fall“);
- welchen journalistischen Sorgfaltsstandards Influencer unterliegen und inwieweit diese rechtlich nutzbar gemacht werden können, um gegen Desinformation, Misinformation oder Propaganda vorzugehen. Zudem fragen sie sich, welche Möglichkeiten insoweit bestehen, wenn der Influencer im (EU-)Ausland oder in einem Drittstaat sitzt;
- wann tendenziöse Beiträge in unzulässige (kostenlose) politische Werbung umschlagen, etwa die eines Influencers auf seinem Social-Media-Account zugunsten einer politischen Partei oder eines ausländischen Staates und welche rechtlichen Konsequenzen dies nach sich zieht;
- welche rechtlichen Reaktionsmöglichkeiten bestehen, wenn in einem EU- oder in einem Drittstaat (wie z. B. den USA) ein Unternehmen (wie z.B. „Tenet Media“), hinter dem ein bekannter Desinformant (wie z. B. ein RT-Mitarbeiter) steht, Influencer mit Millionenbudgets anwirbt, um vor bestimmten Ereignissen (etwa Wahlen) Desinformationen und Propaganda zu verbreiten.

C. RECHTLICHER RAHMEN ZUR BEKÄMPFUNG VON MANIPULATIONEN DES ÖFFENTLICHEN INFORMATIONSRAUMS

Den rechtlichen Rahmen zur Bekämpfung von Manipulationen des öffentlichen Kommunikationsraums bilden die legislativen und exekutiven Handlungszuständigkeiten im Mehrebenensystem (EU, Bund, Länder) (I.). Zudem wird er durch die Grundrechte – seien sie unionalen oder nationalen Ursprungs – eingegrenzt, die einer staatlichen und privaten Bekämpfung (Online-Plattformen) von technischen Manipulationen des öffentlichen Informationsraums Grenzen setzen (II.). Sowohl Handlungszuständigkeiten als auch Grundrechte bilden gleichsam die Steuerungsvorgaben für hoheitliche Maßnahmen zur Bekämpfung kommunikationsbezogener Manipulationen und sollen deshalb „vor der Klammer“ erörtert werden.

I. KOMPETENZGEFÜGE ZUR BEKÄMPFUNG VON MANIPULATIONEN DES ÖFFENTLICHEN INFORMATIONSRAUMS

1. EUROPÄISCHE UNION

Das kompetenzielle Handeln der Europäischen Union (EU) basiert auf dem Prinzip der begrenzten Einzelermächtigung (Art. 5 Abs. 1 S. 1, Abs. 2 EUV). Entsprechend müssen unionale Maßnahmen zur Bekämpfung von Manipulationen des öffentlichen Informationsraums durch eine primärrechtlich zugewiesene Kompetenz unterlegt sein. Als solche kommen ausschließliche (a)) sowie geteilte Zuständigkeiten (b)) der EU in Betracht.

A) AUSSCHLIESSLICHE ZUSTÄNDIGKEITEN

Die Verträge weisen der EU keine umfassende ausschließliche (Gesetzgebungs-)Kompetenz i.S.d. Art. 2 Abs. 1 AEUV zur Bekämpfung von Manipulationen des öffentlichen Informationsraums zu.

Eine Ausnahme hiervon bildet lediglich Art. 215 AEUV, der im fünften Teil des AEUV über das auswärtige Handeln der Union unter Titel IV als sog. restriktive Maßnahme die Einstellung der Wirtschafts- und Finanzbeziehungen zu Drittstaaten ermöglicht.⁶² Die Bestimmung setzt einen nach Titel V Kapitel 2 EUV im Regelfall einstimmig zu erlassenden EU-Beschluss über die Aussetzung, Einschränkung oder vollständige Einstellung der Wirtschafts- und Finanzbeziehungen zu einem oder mehreren Drittländern (Art. 215 Abs. 1 AEUV) oder zu natürlichen oder juristi-

62 Zum ausschließlichen Charakter dieser Unionskompetenz Schneider/Terhechte, in: Grabitz/Hilf/Nettesheim, Art. 215 AEUV Rn. 3 m.w.N.

schen Personen sowie zu Gruppierungen oder nichtstaatlichen Einheiten (Art. 215 Abs. 2 AEUV) voraus. Die in Bezug genommenen Bestimmungen des EUV regeln in ihren Art. 23 ff. besondere Bestimmungen über die Gemeinsame Außen- und Sicherheitspolitik (GASP), die u. a. sämtliche Fragen der Sicherheit der Union umfassen.⁶³ Die Union verfolgt ihre GASP-Ziele u. a. durch Beschlüsse zur Festlegung der von der Union durchzuführenden Aktionen einschließlich von Einzelheiten zu ihrer Durchführung.⁶⁴ Soweit diese Beschlüsse ein „operatives Vorgehen“ zum Gegenstand haben, werden sie durch den Rat⁶⁵ gefasst. Auf Art. 215 AEUV gestützte restriktive Maßnahmen gegen Drittstaaten umfassen Wirtschaftssanktionen aller Art in den Bereichen der Warenverkehrs-, Dienstleistungs-, Niederlassungs- und Kapitalfreiheit; Gleiches gilt nach Abs. 2 für Sanktionsmaßnahmen gegen nichtstaatliche Akteure. Diese Wirtschaftsbezogenheit folgt aus dem Kontext der Unionspolitiken, da Art. 4 Abs. 2 S. 2 EUV allgemeine Maßnahmen zur Aufrechterhaltung der öffentlichen Ordnung prinzipiell den Mitgliedstaaten vorbehält.⁶⁶

Auf der Grundlage dieser Bestimmung wurde u. a. die VO (EU) 2022/350⁶⁷ zum Sende- und Verbreitungsverbot der russisch kontrollierten Medien RT und Sputnik gestützt.⁶⁸ Zudem sieht die Verordnung eine Aussetzung aller Rundfunklizenzen und -genehmigungen vor.⁶⁹ Die Maßnahmen sollen nur so lange beibehalten werden, bis die Aggression gegen die Ukraine beendet wird und bis die Russische Föderation und die mit ihr verbundenen Medien die Durchführung von Propagandaaktionen gegen die Union und deren Mitgliedstaaten einstellen.⁷⁰ Begründet wurden diese GASP-Maßnahmen mit einer erheblichen und unmittelbaren Bedrohung der öffentlichen Ordnung und Sicherheit der Union, da von diesen russisch kontrollierten Medien ein propagandistisches, desinformatives und destabilisierendes Verhalten als Bestandteil einer hybriden Bedrohung der EU ausginge.⁷¹

Bei den ergriffenen Maßnahmen handelt es sich um ein „sanktionsrechtliches Novum“⁷², das erwartungsgemäß nicht kritiklos geblieben ist: So wurde mit Blick auf die in Anspruch genommene Kompetenz thematisiert, ob die nach innen gerichtete Sanktionsmaßnahme eines Medienverbots über das erforderliche außenpolitische Beugepotenzial verfüge.⁷³ Denn der primärrechtlich

63 Vgl. Art. 24 Abs. 1 UAbs. 1 EUV.

64 Art. 25 lit. b) i) und iii) EUV.

65 Vgl. Art. 16 EUV.

66 Cremer, in: Calliess/Ruffert, EUV/AEUV, Art. 215 Rn. 19 u. 21.

67 Verordnung (EU) 2022/350 des Rates v. 1.3.2022 zur Änderung der Verordnung (EU) Nr. 833/2014 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren, ABl.EU Nr. L 65/1. Die Verordnung stützt sich ihrerseits auf den Beschluss (GASP) 2022/351 des Rates v. 1.3.2022 zur Änderung des Beschlusses 2014/512/GASP über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren. Eine von RT France gegen die Verordnung eingereichte Klage blieb erfolglos; vgl. EuG, Beschl. v. 30.3.2022 u. Urte. v. 27.7.2022 – T-125/22 (rechtskräftig – das Rechtsmittel zum EuGH wurde zurückgenommen – C-620/22 P).

68 Zur Reichweite dieses Sende- und Verbreitungsverbot Baade, verfassungsblog v. 8.3.2022; Ferreau, verfassungsblog v. 10.3.2022.

69 Art. 2f Abs. 1 und 2 der Verordnung.

70 ErwG Nr. 10 S. 2 der Verordnung.

71 ErwG. Nr. 5 ff. der Verordnung. Instruktiv zur Historie russischer Propaganda- und Desinformationskampagnen seit der Annexion der Krim im Jahre 2014 und zum Begriff der (Kriegs-)Propaganda Setz/Seyda, ZD-Aktuell 2022, 01167 (sub 2. und 3 a) und b)). Zum Begriff der Desinformation als Teil einer hybriden Bedrohung, die durch falsche oder irreführende Informationen fremder Staaten und nichtstaatlicher Akteure gezielt auf eine Destabilisierung abzielt, um das Vertrauen in die Demokratie und ihre Institutionen zu untergraben, die öffentliche Meinungsbildung zu beeinflussen und den gesellschaftlichen Zusammenhalt zu schwächen, s. BT-Drs. 20/13880, S. 3.

72 Setz/Seyda, ZD-Aktuell 2022, 01167 (sub. 1.). Ähnlich Ferreau, verfassungsblog v. 10.3.2022.

73 Ferreau, verfassungsblog v. 10.3.2022.

nicht definierte Sanktionsbegriff sei gemeinhin als außenpolitisch motiviertes nichtmilitärisches Zwangsmittel zu verstehen, das ein Völkerrechtssubjekt wie einen Staat zu völkerrechtskonformem Verhalten anhalten solle, indem auf seine wirtschaftliche Position eingewirkt werde.⁷⁴ Hieraus wurde geschlussfolgert, dass die Verhinderung der Dissemination russischer Propaganda zum Schutz der öffentlichen Sicherheit und Ordnung innerhalb der EU nicht eine wirtschaftspolitische Sanktionierung, sondern eine inhaltliche Regulierung von Medien betreffe.⁷⁵

Im Ergebnis erscheinen diese Zweifel jedoch unbegründet: Ob eine Maßnahme „nach innen gerichtet“ ist, spielt für die Anwendbarkeit des Art. 215 AEUV keine maßgebliche Rolle. Die Norm dient der Umsetzung von GASP-Maßnahmen, die – wie gesehen – allgemein Fragen der Sicherheit der Union betreffen können. Sie umfasst neben außengerichteten Maßnahmen deshalb auch solche mit innengerichteter Natur. Vorliegend geht es der Union um die Abwehr hybrider Bedrohungen in Gestalt russischer Propaganda und desinformativer Medienkampagnen mit dem Ziel der Destabilisierung einzelner EU-Mitgliedstaaten und der Union als Ganzes. Dieses russische Verhalten stellt zweifelsohne eine Bedrohung der Sicherheit der Union und damit ein zulässiges Ziel von GASP-Maßnahmen dar. Zudem besteht die völkerrechtliche Verpflichtung der EU und ihrer Mitgliedstaaten, der Verbreitung von Kriegspropaganda entgegenzutreten⁷⁶, was durch die skizzierten Maßnahmen erreicht werden soll. Dem kann auch nicht der Achtungsanspruch aus Art. 4 Abs. 2 S. 2 EUV entgegengehalten werden. Denn die beschlossenen GASP-Maßnahmen zielen auf die Bekämpfung einer Bedrohung der EU als Ganzes, weshalb sie nicht als eine Missachtung der nationalen Zuständigkeit für die Aufrechterhaltung der öffentlichen Ordnung im jeweiligen Mitgliedstaat qualifiziert werden können. Der regulative Zugriff auf bestimmte Medien (RT, Sputnik) ist insoweit nur ein Mittel, um das von den EU-Verträgen angestrebte Ziel (Sicherheit der Union) zu erreichen. Des Weiteren ist zu berücksichtigen, dass die Sanktionsmaßnahmen ihrer Natur nach immer einen zeitlich befristeten Charakter aufweisen und deshalb lediglich als ein nationale Maßnahmen ergänzendes, nicht aber als ein solche Maßnahmen verdrängendes Instrument zu qualifizieren sind. Auch können nach der Regelungssystematik EU-Sanktionen im Regelfall nur auf der Grundlage eines einstimmigen GASP-Beschlusses des Rates ergriffen werden. Die Verordnung trifft schließlich auch Maßnahmen wirtschaftsbezogener Natur, da sie unmittelbar die Dienstleistungsfreiheit der betroffenen Mediendiensteanbieter mit Blick auf die Verbreitung ihrer Inhalte beschränkt, auch wenn sie dadurch mittelbar ein nachgelagertes Ziel – die Bekämpfung von Propaganda und Desinformation – verfolgt.⁷⁷

Die auf Art. 215 AEUV gestützten Maßnahmen sind deshalb als kompetenzgerecht zu bewerten. Hieraus folgt freilich nicht, dass dieser Realbereich künftig nicht einer anderen Form der rechtlichen Behandlung zugeführt werden sollte, auch um die Unabhängigkeit und Staatsferne der Medien sachgerechter zu schützen. Hierauf wird noch zurückzukommen sein.

⁷⁴ Schneider/Terhechte, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, Art. 215 Rn. 7.

⁷⁵ Ferreau, verfassungsblog v. 10.3.2022.

⁷⁶ Hierzu und zum Begriff s. oben § 2 A. I. 2. d).

⁷⁷ Allg. zum doppelfunktionalen Charakter der Medien als kulturelles und wirtschaftliches Phänomen EuGH, Urt. v. 30.4.1974, Rs. 155/73, Slg. 74, 409 Rn. 6 – Sacchi; Urt. v. 18.3.1980, Rs. 52/79, Slg. 1980, 834 Rn. 8 – Debauve; Wagner, in: Bitburger Gespräche, S. 41 (44 f.).

B) GETEILTE ZUSTÄNDIGKEITEN

Da sich die ausschließliche Kompetenz aus Art. 215 AEUV auf den Ausnahmefall einer internationalen Spannungslage bezieht, liegt der kompetenzielle Schwerpunkt von EU-Maßnahmen zur Bekämpfung von Manipulationen des öffentlichen Informationsraums jedoch auf dem Gebiet der geteilten Zuständigkeiten i.S.d. Art. 2 Abs. 2 AEUV.

Insoweit hervorzuheben ist die Binnenmarktkompetenz aus Art. 114 Abs. 1 AEUV. Diese setzt allerdings voraus, dass die Angleichung mitgliedstaatlicher Regelungen zur Verwirklichung des Binnenmarkts i.S.d. Art. 26 Abs. 2 AEUV erforderlich ist. Grundsätzlich umfasst dies auch dienstleistungsbezogene Regelungen zum Kommunikations- und Medienrecht.⁷⁸ Zu fordern ist allerdings, dass – subjektiv – die unionsgesetzgeberische Tätigkeit auf das Errichten und Funktionieren des Binnenmarkts abzielen muss und – objektiv – der Rechtsakt tatsächlich den Zweck haben muss, die Voraussetzungen hierfür zu verbessern.⁷⁹ Art. 114 Abs. 1 AEUV gewährt mithin keine umfassende, blankettartige Norm⁸⁰, sondern lediglich eine begrenzte Kompetenz zur Bekämpfung von Manipulationen des öffentlichen Informationsraums. Keinesfalls steht der EU deshalb das Recht zu, losgelöst von den vorstehend beschriebenen Harmonisierungsgrenzen allgemeine kommunikationsbezogene Maßnahmen zur Bekämpfung von Manipulationen des Informationsraums als Bedrohung ihrer demokratischen Grundstruktur (vgl. Art. 2 EUV) zu ergreifen.

Das wichtigste unionsrechtliche Gesetz, welches eine Bekämpfung von Manipulationen des öffentlichen Informationsraums ermöglicht, der DSA, ist auf dieser Kompetenzgrundlage erlassen.⁸¹ Gleiches gilt für den European Media Freedom Act (EMFA)⁸² und die KI-Verordnung (KI-VO).⁸³

2. BUNDESREPUBLIK DEUTSCHLAND

Soweit der EU nach dem Prinzip der begrenzten Einzelermächtigung kein Gesetzgebungsrecht zusteht oder sie von einer geteilten Gesetzgebungskompetenz keinen (umfassenden) Gebrauch gemacht hat, liegt die legislative Zuständigkeit bei den Mitgliedstaaten. In der Bundesrepublik Deutschland sind diese auf Bund (a)) und Länder (b)) verteilt.

78 Ausführlich dazu Nielsen, Medienvielfalt, S. 51 ff.

79 Wagner, in: Bitburger Gespräche, S. 41 (46) m. Nachw. zur Rspr. des EuGH.

80 Letzteres wäre nach der BVerfG-Rspr. auch mit Art. 79 Abs. 3 GG als unionaler Integrationsschranke der Bundesrepublik Deutschland (vgl. Art. 23 Abs. 1 S. 3 GG) nicht zu vereinbaren; vgl. BVerfGE 58, 1 (37); 89, 155 (183 f., 187), 123, 267 (351).

81 Zur Kompetenzgerechtigkeit des DSA ausführlich Flamme, Meinungsmacht der Algorithmen, S. 250 ff. m. w. N.; Schumacher, AfP 2024, 480 ff. Skeptisch demgegenüber Gersdorf, 74. dJt I/G 49 f.

82 Verordnung (EU) 2024/1083 des Europäischen Parlaments und des Rates v. 11.4.2024 zur Schaffung eines gemeinsamen Rahmens für Mediendienste im Binnenmarkt und zur Änderung der Richtlinie 2010/13/EU (Europäisches Medienfreiheitsgesetz), ABL EU Nr. L v. 17.4.2024. Zum Streit über die Kompetenzgerechtigkeit dieser Verordnung s. Müller-Terpitz, (Un-)Level Playing Field im Medienbereich, S. 21 m.w.N.

83 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates v. 13.6.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828, ABL EU Nr. L v. 12.7.2024.

A) BUND

Der Bund verfügt über einige Kompetenzen zum Kampf gegen Manipulationen des öffentlichen Informationsraums. Er kann sich sowohl auf ausschließliche als auch auf konkurrierende Gesetzgebungskompetenzen stützen:

So verfügt der Bund über die ausschließliche Kompetenz (Art. 71, 73 GG) zur Abwehr von Gefahren des internationalen Terrorismus (Art. 73 Abs. 1 Nr. 9a GG) sowie zur Regelung der Zusammenarbeit des Bundes und der Länder in der Kriminalpolizei und im Verfassungsschutz (Art. 73 Abs. 1 Nr. 10 GG). Auch steht dem Bund die fakultative Kompetenz zur Einrichtung des Bundesverfassungsschutzes sowie der Bundesnetzagentur als Aufsichtsbehörden zu (Art. 87 Abs. 3 GG).

Im Bereich der konkurrierenden Gesetzgebungskompetenz steht ihm das Gesetzgebungsrecht für das Strafrecht und das Ordnungswidrigkeitenrecht sowie für das Bürgerliche Recht zu (Art. 74 Abs. 1 Nr. 1 GG). Zudem verfügt er über die konkurrierende Gesetzgebungskompetenz für das Vereinsrecht (Art. 74 Abs. 1 Nr. 3 GG). Für letztere hat das Bundesverwaltungsgericht im Rahmen des Compact-Verfahrens festgestellt, dass diese Kompetenz kraft historischer Herleitung auch das vereinigungsrechtliche Verbot eines Unternehmens⁸⁴ zu rechtfertigen vermag, das Medieninhalte produziert und verbreitet.⁸⁵

B) LÄNDER

Gemäß Art. 70 Abs. 1 GG und Art. 83 GG fällt außerhalb dieser Zuständigkeitsbereiche des Bundes die Kompetenz zur Gesetzgebung und zum Gesetzesvollzug den Ländern zu. Dies umfasst insbesondere den weiten Bereich der Mediengesetzgebung, welcher sich auf organisatorische und inhaltliche Fragen des Angebots von Mediendienstleistungen bezieht.⁸⁶ Hierauf gestützt dürfen die Länder auch gesetzliche Maßnahmen zur Bekämpfung von Manipulationen des öffentlichen Informationsraums ergreifen, etwa durch Anforderungen an journalistische Sorgfaltspflichten, durch Vorgaben zur Kennzeichnung bestimmter Inhalte (vgl. § 18 Abs. 3 MStV) sowie durch algorithmenbezogene Maßnahmen zur Sicherung des Meinungsbildungsprozesses und der Meinungsvielfalt (vgl. §§ 93 f. MStV).

Da sich diese gesetzlichen Regelungen zum Teil auf Online-Plattformen beziehen, können sie jedoch in Konkurrenz zu den Bestimmungen des DSA stehen.⁸⁷ Momentan ist deshalb unklar, welcher nationale Handlungsspielraum insoweit (noch) besteht und inwieweit nationale Regelungen zur Manipulationsbekämpfung nach dem Marktortprinzip (Bestimmungslandprinzip) auch auf solche Unternehmen erstreckt werden können, die ihren Sitz in einem anderen EU-Mit-

84 Vgl. §§ 1 – 3 des Vereinsgesetz (VereinsG) v. 5.8.1964 (BGBl. I S. 593), zuletzt geändert durch Art. 5 des Gesetzes v. 30.11.2020 (BGBl. I S. 2600)

85 BVerwG, Urt. v. 24.6.2025 – 6 A 4.24 = NJW 2025, 3650, Rn. 23 ff.

86 Vgl. BVerfGE 12, 205 (225 ff.); Kluth/Schulz, Konvergenz und regulatorische Folgen, S. 58.

87 Zum DSA noch ausführlich nachfolgend § 2 D. I. 1. a).

gliedstaat haben.⁸⁸ Das Verwaltungsgericht Berlin hat diese Fragen im Wege eines Vorabentscheidungsverfahrens (Art. 267 AEUV) dem EuGH vorgelegt.⁸⁹ Bis zu einer eventuellen Klärung dieser Rechtsunsicherheiten können die mitgliedstaatlichen Aufsichtsinstanzen jedoch mit guten Gründen von einer Anwendbarkeit der nationalen Normen zum Schutz des Informations- und Meinungsbildungsprozesses ausgehen. Mediendiensteanbietern ist deshalb zu raten, sowohl den unionalen als auch den nationalen Vorgaben zu entsprechen.⁹⁰

II. GRUNDRECHTLICHE GRENZEN DER BEKÄMPFUNG VON MANIPULATIONEN DES ÖFFENTLICHEN INFORMATIONSRAUMS

Für die Bewertung der grundrechtlichen Grenzen ist das delicate Spannungsverhältnis zwischen den individuellen Kommunikationsfreiheiten und dem Schutz der freiheitlich-demokratischen Grundordnung vor Manipulationen des öffentlichen Informationsraums in den Blick zu nehmen. Diese Untersuchung ist von der Erkenntnis geleitet, dass der Staat und der Staatenverbund EU dem „demokratiezersetzenden Gift“ solcher Manipulationen nicht schutzlos ausgeliefert sein kann. Gerade das Grundgesetz wurde in Reaktion auf die nationalsozialistische Willkür- und Schreckensherrschaft als „wehrhafte Verfassung“⁹¹ konzipiert, die sich einem Missbrauch der Kommunikationsfreiheiten zur Verfälschung öffentlicher Kommunikationsprozesses und einer hierdurch beabsichtigten Erschütterung der freiheitlich-demokratischen Grundordnung entgegenzustellen vermag.⁹² Es erlaubt deshalb Maßnahmen gegen Bestrebungen, die – wie die Manipulation des öffentlichen Informationsraums – auf eine Unterminierung oder gar Zerstörung der grundgesetzlich konstituierten individuellen Freiheiten sowie demokratischen Institutionen und Verfahren zielen. Und auch die EU gründet auf den Werten der Menschenrechte (unter Einschluss der Menschenwürde), der Demokratie und des Rechtsstaats.⁹³

Vor dieser Folie sind die exakten Grenzverläufe des europäischen und nationalen Grundrechtsschutzes herauszuarbeiten, um staatlich sanktionierbare Manipulationen der Informationsprozesse von staatlich nicht oder nur sehr eingeschränkt zu sanktionierenden Vorgängen (wie etwa die Verbreitung von Misinformationen oder unethischen, aber rechtmäßigen Meinungsäußerungen [„awful, but lawful“]) abzugrenzen. Diese Grenzverläufe markieren zugleich die grundrechtlich bestehenden legislativen, exekutiven und judikativen Handlungsspielräume für eine Bekämpfung von Manipulationen des öffentlichen Informationsraums. Die Untersuchung beschränkt sich dabei auf diejenigen Akteure, die manipulative Handlungen vornehmen oder verbreiten und *deshalb* zu Adressaten hoheitlicher Eingriffe werden sollen. Die Einbeziehung weite-

88 Ausführlich hierzu m.w.N. Müller-Terpitz, (Un-)Level Playing Field im Medienbereich, S. 29 ff.

89 VG Berlin v. 17.12.2024 – VG 32 L 221/24, MMR 2025, 761 ff. Das Verfahren ist beim EuGH unter dem Az. C-474/25 anhängig. Zum Vorstehenden s. des Weiteren VG Schleswig v. 30.6.2025 – 10 B 185/24, MMR 2025, 837 ff.

90 In diesem Sinne auch Grisse, in: Hofmann/Raue, DSA, Art. 27 Rn. 49.

91 Vgl. insoweit Art. 9 Abs. 2, Art. 18, Art. 20 Abs. 4, Art. 21 Abs. 2 bis 4 oder Art. 79 Abs. 3 GG.

92 So kann einem Grundrechtsberechtigten gemäß Art. 18 GG „die Freiheit der Meinungsäußerung, insbesondere die Pressefreiheit (Artikel 5 Abs. 1)“ aberkannt werden, wenn er diese Freiheiten „zum Kampf gegen die freiheitlich demokratische Grundordnung mißbraucht“. Die beispielhafte Erwähnung der Pressefreiheit führt zu dem Schluss, dass diese Sanktionsmöglichkeit weit zu verstehen ist und sich auf jede Form „aktiver Berichterstattung“ (Barczak, in: Dreier, GG, Art. 18 Rn. 38), sprich auf die Medienfreiheiten insgesamt, d.h. unter Einschluss der Rundfunkfreiheit und der Freiheit der Online-Medien, bezieht.

93 Vgl. Art. 2 EUV.

rer grundrechtlicher Perspektiven – etwa der Nutzer als Adressaten von Manipulationen – ließe die Analyse uferlos werden. Auf diese Perspektiven wird deshalb nur punktuell eingegangen.

1. ANWENDBARE GRUNDRECHTSREGIME

Regelungen zur Bekämpfung von Manipulationen des öffentlichen Informationsraums finden sich – wie noch zu zeigen sein wird – in verschiedenen unionalen und nationalen Gesetzen, etwa im DSA und im Medienstaatsvertrag (MStV). Aufgrund ihrer Qualität als unionales bzw. nationales Recht unterliegen sie den unterschiedlichen Grundrechtsregimen des Mehrebenensystems, das aus drei – allerdings miteinander verzahnten – Grundrechtsschichten besteht.⁹⁴

A) VÖLKERRECHTLICHER GRUNDRECHTSSCHUTZ (EMRK)

Die – zumindest formal betrachtet – unterste Schicht dieses Grundrechtsregimes bilden die Grundrechte der Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK)⁹⁵ in ihrer Interpretation durch den Europäischen Gerichtshof für Menschenrechte (EGMR).⁹⁶ Als völkerrechtlicher Vertrag hat die Konvention durch ein auf der Grundlage des Art. 59 Abs. 2 GG ergangenes Zustimmungsgesetz des Bundes Geltungskraft in Deutschland erlangt.⁹⁷ Entsprechend gilt sie innerstaatlich mit dem Rang eines Bundesgesetzes.

Wie das Bundesverfassungsgericht jedoch in seiner Görgülü-Entscheidung hervorgehoben hat, gehört zur Bindung an Gesetz und Recht (Art. 20 Abs. 3 GG) im Rahmen methodisch vertretbarer Gesetzesauslegung auch die Berücksichtigung der EMRK-Gewährleistungen einschließlich der hierzu ergangenen Entscheidungen des EGMR.⁹⁸ Zur Wahrung des verfassungsrechtlichen Prinzips der Völkerrechtsfreundlichkeit des Grundgesetzes⁹⁹ kommt der EMRK deshalb trotz ihres nur einfachrechtlichen Geltungsgrads bis zur Grenze der tragenden Verfassungsprinzipien¹⁰⁰ eine rechtlich sehr starke und ggf. dem nationalen Grundrechtsschutz sogar vorrangige Grundrechtswirkung zu. Über die Konvergenzklausel in Art. 52 Abs. 3 EUGRC strahlt die EMRK zudem als Rechtserkenntnisquelle¹⁰¹ auf die Interpretation der EU-Grundrechte aus.

94 So auch Masing, JZ 2015, 477 (483), der von einer „dreifach vertikalen Schichtung im Bereich des konkurrierenden Grundrechtsschutzes“ spricht.

95 Vom 4.11.1950 i.d.F. der Neubekanntmachung v. 22.10.2010, BGBl. II S. 1198.

96 Vgl. Art. 19 ff. EMRK.

97 BGBl. 1952 II S. 685, 686, 953.

98 BVerfGE 111, 307 (323 ff.).

99 BVerfGE 111, 307 (317 ff.). Diese Völkerrechtsfreundlichkeit manifestiert sich u. a. in Bestimmungen wie Art. 1 Abs. 2, Art. 24, 25, 26 GG und seiner Präambel.

100 BVerfGE 111, 307 (319).

101 Zum (umstrittenen) EU-rechtlichen Bedeutungsgehalt dieser Regelung instruktiv Kingreen, in: Calliess/Ruffert, EUV/AEU, Art. 52 Rn. 31 ff. m.w.N.

B) NATIONALER GRUNDRECHTSSCHUTZ (GG)

Auf der mittleren Grundrechtsschicht des Mehrebenensystems liegen die nationalen Grundrechte, die uneingeschränkte Anwendung auf die Ausübung nationaler Hoheitsgewalt, auch soweit deren Wirkungen im Ausland eintreten¹⁰², finden. Wie vorstehend (a)) bereits ausgeführt, kann es im Rahmen der Auslegung und Anwendung nationaler Grundrechte jedoch erforderlich werden, den Grundrechtsgehalten der EMRK in ihrer Interpretation durch den EGMR Rechnung zu tragen, um einen Widerspruch (und damit einen Völkerrechtsbruch) des nationalen Grundrechtsschutzes zum EMRK-Grundrechtsschutz zu vermeiden.

C) UNIONALER GRUNDRECHTSSCHUTZ (EUGRC)

Die höchste Schicht des Grundrechtsschutzes im Mehrebenensystem besteht aus den unionalen Grundrechten. Als Primärrecht konstituieren sich diese einerseits aus den allgemeinen Grundsätzen des Unionsrechts, wie sie sich aus den Rechtserkenntnisquellen der EMRK und den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben (Art. 6 Abs. 3 EUV), sowie andererseits aus der Charta der Grundrechte der Europäischen Union (EUGRC) vom 7. Dezember 2000¹⁰³ (Art. 6 Abs. 1 EUV). Als genuin unionsrechtlicher Grundrechtsquelle kommt letzterer eine überragende Bedeutung für die Interpretation und Anwendung der unionalen Grundrechte zu; sie soll deshalb nachfolgend im Zentrum der Analyse des EU-Rechts stehen.

Nach Art. 51 Abs. 1 S. 1 EUGRC definiert die Charta ihren Anwendungsbereich wie folgt:

„Diese Charta gilt für die Organe, Einrichtungen und sonstigen Stellen der Union unter Wahrung des Subsidiaritätsprinzips und für die Mitgliedstaaten ausschließlich bei der Durchführung des Rechts der Union.“

Zum einen folgt aus dieser Regelung, dass der europäische Gesetzgeber (Rat und Europäisches Parlament), die Kommission und der Gerichtshof der Europäischen Union (EuGH) als Organe der Union¹⁰⁴ an die EU-Grundrechte gebunden sind. Zum anderen unterliegen aber auch die Mitgliedstaaten einer Bindung an die EU-Grundrechte, wenn sie Unionsrecht „durchführen“, d.h. unmittelbar geltendes Unionsrecht umsetzen – sei es in Gestalt der gesetzgeberischen Umsetzung einer EU-Richtlinie in nationales Recht oder durch den Vollzug unmittelbar anwendbaren Verordnungsrechts. Soweit hierbei mitgliedstaatliche Handlungsspielräume – etwa für den nationalen Gesetzgeber bei der Umsetzung einer Richtlinie oder für die Exekutive beim Vollzug von unionsrechtlich nicht vollständig determiniertem Recht – bestehen, können die Mitgliedstaaten indes zugleich der Bindung an nationale Grundrechtssysteme, in Deutschland also den

102 Vgl. Art. 1 Abs. 3 GG sowie BVerfGE 154, (215 ff., Rn. 87 ff.) – BND-Ausland-Ausland-Fernmeldeaufklärung, wonach die Bindung der deutschen Staatsgewalt an die Grundrechte (Art. 1 Abs. 3 GG) nicht auf das deutsche Hoheitsgebiet beschränkt ist und „jedenfalls“ der Schutz des Art. 5 Abs. 1 S. 2 GG und des Art. 10 Abs. 1 GG als Abwehrrecht auch auf Ausländer mit Sitz im Ausland zu erstrecken ist.

103 ABl.EU Nr. C 364/1.

104 Zu diesen s. Art. 13 Abs. 2 EUV.

Grundrechten des Grundgesetzes und der EMRK, unterfallen.¹⁰⁵ Bei der Anwendung des Grundrechtsschutzes im Mehrebenensystem resultiert hieraus eine komplexe normative Gemengelage. Wie noch zu zeigen sein wird (nachstehend 2.), stimmt der Gewährleistungsgehalt des Grundrechtsschutzes auf nationaler (GG) und europäischer (EMRK, EUGRC) Ebene jedoch weitgehend überein. Im Regelfall kann deshalb die vom Bundesverfassungsgericht in der „Recht auf Vergessen II“-Entscheidung aufgestellte widerlegliche Vermutung zugrundegelegt werden, dass die Reichweite des nationalen Grundrechtsschutzes die Reichweite des Grundrechtsschutzes durch die Unionscharta abbildet.¹⁰⁶ Um diese Vermutung zu verifizieren, bedarf es jedoch einer Analyse aller drei Grundrechtsebenen. Soweit die Grundrechte des Grundgesetzes infolge einer EU-rechtlichen Vollharmonisierung (wie etwa in Gestalt zahlreicher Regelungen des DSA oder EMFA) durch den Anwendungsvorrang des Unionsrechts verdrängt werden, findet im Übrigen allein der Maßstab der Unionsgrundrechte Anwendung.¹⁰⁷

2. GRUNDRECHTLICHE GEWÄHRLEISTUNGSGEHALTE IM DETAIL

Die Untersuchung des konkreten grundrechtlichen Gewährleistungsgehalts erfolgt in drei Schritten: Nach allgemeinen Vorbemerkungen (a)) geht sie zunächst der Frage nach, inwieweit die rechtsgutachtlich zu untersuchenden Manipulationen des öffentlichen Informationsraums überhaupt unter den Schutzbereich eines Grundrechts fallen (b)). Soweit dies der Fall ist, stellt sich im Weiteren die Frage, unter welchen Voraussetzungen derartige Manipulationen durch staatliches Handeln beschränkt werden dürfen und wo die Grenzen dieser Schrankenziehungen verlaufen (c)). Erst aus der Summe dieser schrittweisen Analyse ergibt sich der effektive grundrechtliche Gewährleistungsgehalt von Manipulationen des öffentlichen Informationsraums.

A) VORBEMERKUNGEN

aa) Einschlägige Grundrechtstatbestände

Im Mehrebenensystem werden kommunikationsbezogene Handlungen durch unterschiedliche Grundrechte geschützt: Auf nationaler Ebene erfolgt ein Schutz über Art. 5 Abs. 1 GG. Dieses Grundrecht umfasst die Meinungs- und Informationsfreiheit (Art. 5 Abs. 1 S. 1 GG) sowie die Presse- und Rundfunkfreiheit (Art. 5 Abs. 1 S. 2 GG). Auf unionaler Ebene schützt Art. 11 Abs. 1 EUGRC die Meinungs- und Informationsfreiheit; der Schutz der Medienfreiheiten wird durch Art. 11 Abs. 2 EUGRC verbürgt. In der EMRK findet sich eine Art. 5 Abs. 1 S. 1 GG und Art. 11 Abs. 1 EUGRC vergleichbare Gewährleistung der Meinungs- und Informationsfreiheit, welche vom EGMR in ständiger Rechtsprechung über individualkommunikative Prozesse hinaus auch auf journalistisch-redaktionelles Handeln extendiert wird.¹⁰⁸ Da der EuGH noch keine detaillierte Rechtsprechung zur Reichweite der Meinungsfreiheit entwickelt hat, ist insofern auf die

¹⁰⁵ Näher dazu BVerfGE 152, 152 (169 ff., Rn. 42 ff.).

¹⁰⁶ BVerfGE 152, 152 (171 ff., Rn. 49 ff.). Ausführlich hierzu Roß, JZ 2025, 651 ff.

¹⁰⁷ Vgl. insoweit BVerfGE 152, 216 (236, Rn. 50) – Recht auf Vergessen II.

¹⁰⁸ Vgl. EGMR, Ur. v. 17.9.2009, Nr. 13936/02, Rn. 96 – Manole u. a./Moldau; Grabenwarter/Pabel, Europäische Menschenrechtskonvention, § 23 Rn. 2 ff.

Judikatur des EGMR zu rekurrieren, die – wie gesehen¹⁰⁹ – gemäß Art. 6 Abs. 3 EUV und Art. 52 Abs. 3 EUGRC als Interpretationsleitlinie für das Unionsrecht fungiert.¹¹⁰

bb) Grundrechtswirkungen

Den vorstehend skizzierten Grundrechtsgewährleistungen ist gemein, dass sie als Abwehrrechte des Bürgers gegen staatliche oder quasi-staatliche¹¹¹ Hoheitsgewalt konzipiert sind und deshalb prinzipiell nur das Handeln von Privaten (natürliche oder juristische Personen) schützen. Für die nationalen Grundrechte folgt dies aus Art. 1 Abs. 3 GG, der die staatliche Gewalt an Grundrechte bindet und damit im Umkehrschluss von einer Grundrechtsberechtigung prinzipiell ausschließt. Gleiches gilt für die normstrukturell ähnlich gestalteten Art. 1 EMRK¹¹² und Art. 51 Abs. 1 EUGRC.¹¹³

Ist das Handeln von Personen, die den öffentlichen Informationsraum manipulieren, indes einem Staat zuzurechnen, können sich diese Personen schon *a limine* nicht auf Grundrechtsschutz für ihre Tätigkeiten berufen. Eine solche Zurechnung hat insbesondere dann zu erfolgen, wenn Personen als Agenten im Auftrag oder auf Weisung eines Staates handeln. Eine solche Konstellation liegt regelmäßig vor, wenn ausländische Akteure über staatlich beauftragte bzw. finanzierte Trolle, Blogger oder Influencer – sei es mit Sitz im Inland, EU-Ausland oder in einem Drittstaat – durch manipulative Verhaltensweisen und Kampagnen den öffentlichen Informationsraum zu beeinträchtigen versuchen. Eine solche „Foreign Information Manipulation and Interference“ (FIMI), die einen Großteil der Manipulationen des öffentlichen Informationsraums ausmachen, genießen deshalb regelmäßig keinen grundrechtlichen Schutz durch nationale oder europäische Grundrechte. Gleiches gilt für journalistisch-redaktionell gestaltete Mediendienste, die keine hinreichende Unabhängigkeit von einem Staat oder staatlich kontrollierten Institutionen aufweisen.¹¹⁴ Entsprechend bedürfen insoweit ergriffene staatliche Gegenmaßnahmen auch keiner grundrechtlichen Rechtfertigung.

Nur dort, wo rein private Akteure (etwa Anhänger einer politischen Partei oder rein private Blogger und Influencer) manipulative Handlungen vornehmen, stellt sich deshalb die Frage, inwieweit dieses Handeln grundrechtlichen Schutz genießt und welche staatlichen Maßnahmen dagegen gerechtfertigt sein können. In dieser Konstellation ist es auch ohne Relevanz, ob sich diese Personen im In- oder Ausland befinden. Ausreichend ist vielmehr, dass sie mit ihren Handlungen auf das Territorium der Bundesrepublik Deutschland einwirken und hierdurch einen „genuine link“ zur deutschen Hoheitsgewalt begründen, welcher das Ergreifen staatlicher Gegenmaß-

109 S. oben § 2 C. II. 1. a).

110 Wie hier Cornils, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, EU-GRCharta, Art. 11 Rn. 32.

111 Gemeint ist das Handeln der EU.

112 Die Bestimmung lautet: „Die Hohen Vertragsparteien sichern allen ihrer Hoheitsgewalt unterstehenden Personen die in Abschnitt 1 bestimmten Rechte und Freiheiten zu.“

113 Zu letzterer Bestimmung s. bereits oben § 2 C. II. 1. c).

114 Vgl. insoweit EGMR, Entsch. v. 7.12.2006, Nr. 35841/02, Rn. 46 ff. – Österreichischer Rundfunk/Austria; Ferreau, verfassungsblog v. 10.3.2022, der zu Recht darauf hinweist, dass über Art. 52 Abs. 3 EUGRC diese Rspr. auch für Art. 11 EUGRC maßgeblich ist. Nicht überzeugend deshalb Setz/Seyda, ZD-Aktuell 2022, 01167 (sub 3. c.), die unter Berufung auf Lehofer, verfassungsblog v. 21.3.2022 auch für das Betätigungsverbot von RT und Sputnik die Möglichkeit eines Grundrechtsschutzes aus Art. 11 EUGRC und eines Rechtsmissbrauchs nach Art. 54 EUGRC erörtern.

nahmen – seien sie legislativer, exekutiver oder judikativer Natur – rechtfertigt. Als Adressaten deutscher Hoheitsgewalt (*status subjectionis*) genießen sie dann allerdings im Gegenzug den Schutz der deutschen Grundrechte.¹¹⁵

Das vorstehend Ausgeführte gilt auch für die Grundrechte der EMRK. Für diese orientiert sich der EGMR am Kriterium der effektiven Kontrolle („effective control“) über das Handeln auf fremdem Territorium; folgerichtig hat er auf dieser Grundlage in vielen Fällen eine Auslandsgeltung der Konventionsgrundrechte anerkannt.¹¹⁶ Und auch die Grundrechte der EUGRC erfassen in ihre Abwehrfunktion Hoheitsakte der Grundrechtsverpflichteten dann, wenn sie außerhalb des räumlichen Geltungsbereichs des EU (Art. 52 EUV, Art. 355 AEUV) Wirkung entfalten.¹¹⁷

B) GRUNDRECHTLICHER SCHUTZ VON MANIPULATIONEN DES ÖFFENTLICHEN INFORMATIONSRAUMS

Soweit nach dem vorstehend Dargelegten ein Grundrechtsschutz nicht *a limine* ausscheidet, stellt sich im nächsten Schritt die Frage, durch welche Grundrechte die Manipulation des öffentlichen Informationsraums geschützt sein könnte.

aa) Meinungsfreiheit

Aufgrund unterschiedlicher Tatbestandsdogmatiken des nationalen und europäischen Schutzes der Meinungsfreiheit soll zum besseren Verständnis zunächst die nationale Grundrechtsebene untersucht werden. Die Analyse differenziert zwischen dem Äußern von Meinungen und Tatsachen und dem Verbreiten von Meinungen und Tatsachen.

(1) Nationaler Grundrechtsschutz (GG)

Äußern von Meinungen und Tatsachen

Das Grundgesetz schützt die Meinungsfreiheit – oder besser gesagt: die Meinungsäußerungsfreiheit¹¹⁸ – in Art. 5 Abs. 1 S. 1 Var. 1 GG. Das Bundesverfassungsgericht versteht unter Meinungen in ständiger Rechtsprechung Werturteile, die durch das Element der Stellungnahme, des Dahaltens bzw. des Meinens im Rahmen einer geistigen Auseinandersetzung gekennzeichnet sind. Insofern lassen sie sich auch nicht als wahr oder unwahr erweisen.¹¹⁹ Ob die geäußerte Meinung wertvoll oder wertlos, „richtig“ oder „falsch“, emotional oder rational begründet ist, ob sie abs-

¹¹⁵ S. hierzu bereits oben Fn. 102.

¹¹⁶ Vgl. insoweit EGMR (GK), Urte. v. 7.7.2011, Nr. 55721/07, §§ 132 ff. m.w.N. – Al-Skeini and others/United Kingdom. S. ferner Aust, AVR 52 (2014), 375 (394 ff.). m.w.N.

¹¹⁷ Jarass, in: Jarass, Charta der Grundrechte der EU, Art. 51 Rn. 44.

¹¹⁸ Frei nach dem deutschen Volkslied „Die Gedanken sind frei“ kann jeder jederzeit unbehelligt von staatlicher Ingerenz eine Meinung haben. Die Meinungsfreiheit schützt deshalb nicht primär das Haben von Meinungen, sondern deren Äußerung und Verbreitung; so mit Recht Gröpl, NVwZ 2025, 281. Dennoch werden die Begriffe „Meinungsfreiheit“ und „Meinungsäußerungsfreiheit“ als Synonyme verstanden, so auch hier.

¹¹⁹ BVerfGE 124, 300 (320).

trus oder töricht erscheint und den sich Äußernden blamiert, ist für das Eingreifen des grundrechtlichen Schutzes deshalb grundsätzlich ohne Belang.¹²⁰ Die Bürger sind auch nicht gehalten, die der Verfassung zugrunde liegenden Wertsetzungen persönlich zu teilen. Das Grundgesetz baut zwar auf der Erwartung auf, dass die Bürger die allgemeinen Werte der Verfassung akzeptieren und verwirklichen, erzwingt eine dahingehende Werteloyalität aber nicht. Geschützt sind deshalb auch Meinungen, die auf eine grundlegende Änderung der politischen Ordnung zielen, und zwar unabhängig davon, ob und wie weit sie im Rahmen der grundgesetzlichen Ordnung durchsetzbar ist. Dementsprechend fällt nach Auffassung des Bundesverfassungsgerichts selbst die Verbreitung nationalsozialistischen Gedankenguts als radikale Infragestellung der freiheitlich-demokratischen Grundordnung nicht *a priori* aus dem Schutzbereich der Meinungsfreiheit heraus. Den hierin begründeten Gefahren entgegenzutreten, weist die freiheitliche Ordnung des Grundgesetzes primär bürgerschaftlichem Engagement im freien politischen Diskurs sowie der staatlichen Aufklärung und Erziehung in den Schulen (Art. 7 GG) zu. Es vertraut mithin auf die Kraft der freien Auseinandersetzung als wirksamste Waffe auch gegen die Verbreitung totalitärer und menschenverachtender Ideologien.¹²¹

Von diesem wertenden, einschätzenden und subjektiv-dafürhaltenden Charakter des „Meinens“ grenzt das Bundesverfassungsgericht in ständiger Rechtsprechung Tatsachenbehauptungen (Informationen) ab. Diese zeichnen sich durch den Umstand aus, dass sie – anders als Meinungen – dem Wahrheitsbeweis zugänglich sind.¹²² Die Mitteilung einer reinen Tatsache (etwa die Außentemperatur an einem bestimmten Ort zu einer bestimmten Zeit) ist deshalb *per se* keine grundrechtlich geschützte Äußerung einer Meinung, weil ihr die für eine Meinungsäußerung charakteristischen subjektiven Merkmale fehlen. Tatsachenbehauptungen fallen deshalb allerdings nicht *a limine* aus dem Schutzbereich des Art. 5 Abs. 1 S. 1 Var. 1 GG heraus. Vielmehr werden sie durch das Grundrecht der Meinungsäußerungsfreiheit geschützt, wenn ihre Mitteilung zugleich die Grundlage der geäußerten Meinung bildet.¹²³ Im Einzelfall ist eine Trennung der tatsächlichen und wertenden Bestandteile einer Äußerung deshalb nur zulässig, wenn dadurch der Äußerungssinn nicht verfälscht wird. Wo dies nicht möglich ist, muss die Äußerung im Interesse eines wirksamen Grundrechtsschutzes insgesamt als Meinungsäußerung angesehen werden, weil andernfalls eine wesentliche Verkürzung des Grundrechtsschutzes droht.¹²⁴

Tatsachenbehauptungen sind vom Schutz des Art. 5 Abs. 1 S. 1 Var. 1 GG im Übrigen auch dann erfasst, wenn sie sich später als falsch erweisen.¹²⁵ Dementsprechend kann sich der Schutz des Art. 5 Abs. 1 S. 1 GG prinzipiell auch auf unwahre Tatsachenbehauptungen beziehen.¹²⁶ Hierunter fallen typischerweise die oben (§ 2 A. I. 2. b)) erwähnten Misinformationen.

120 BVerfGE 61, 1 (7); 65, 1 (41); 90, 241 (247); 93, 266 (289); 124, 300 (320); Bethge, in: Sachs, GG, Art. 5 Rn. 25.

121 BVerfGE 124, 300 (320 f.). So zuvor bereits BVerfG-K, NJW 2001, 2069 (2070); NJW 2009, 908 (909).

122 Vgl. BVerfGE 33, 1 (14); 124, 300 (320); Grimm, NJW 1995, 1697 (1698); Schemmer, in: Epping/Hillgruber, BeckOK-GG, Art. 5 Rn. 5.

123 Vgl. BVerfGE 54, 208 (219); 61, 1 (8); 71, 162 (179); 85, 1 (15 f.); 90, 241 (247); 94, 1 (7); 114, 339 (352 f.); Bethge, in: Sachs, GG, Art. 5 Rn. 27; Grimm, NJW 1995, 1697 (1699).

124 BVerfGE 61, 1 (9); 90, 1 (15 f.); 90, 241 (248); BVerfG-K, NJW 2012, 1498 (1499).

125 Vgl. BVerfG-K, NJW-RR 2000, 1209 (1210).

126 BVerfGE 61, 1 (8); 90, 241 (254); 99, 185 (197); Mafi-Gudarzi, ZRP 2019, 65 (67) m.w.N.

Die Grenze des Schutzes unwahrer Tatsachenbehauptungen ist nach der ständigen Rechtsprechung des Bundesverfassungsgerichts jedoch dort erreicht, wo es sich um bewusst unwahre Tatsachenbehauptungen handelt oder um solche, deren Unwahrheit schon im Moment der Entäußerung unzweifelhaft feststeht.¹²⁷ Das Bundesverfassungsgericht begründet diese ungeschriebene Schutzbereichsbeschränkung mit dem Telos der Äußerungsfreiheiten – der individuellen und öffentlichen Meinungsbildung; eine feststehend unwahre Tatsachenbehauptung könne indes nicht zu einer „richtigen“ Meinungsbildung beitragen.¹²⁸ Ein „Recht zur Lüge“ schützt das Grundgesetz folglich nicht – weder durch Art. 5 Abs. 1 S. 1 Var. 1 GG¹²⁹ noch – aufgrund des engen Tatbestandsbezugs von Informationen zu Art. 5 Abs. 1 GG – durch das subsidiäre Auffanggrundrecht der allgemeinen Handlungsfreiheit (Art. 2 Abs. 1 GG).¹³⁰ Im Unterschied zur Desinformation¹³¹ kommt es für diese verfassungsgerichtliche Schutzbereichsbeschränkung auch nicht auf eine schädigende Absicht oder Wirkung der erwiesenen unwahren Tatsachenbehauptung an.

An die Schwelle für die Unwahrheit einer Tatsachenbehauptung sind jedoch hohe Anforderungen zu stellen. Aussagen, deren Unwahrheit nicht gesichert feststeht, bleiben deshalb vom Schutzbereich der Äußerungsfreiheiten grundsätzlich umfasst. Knüpfte man den grundrechtlichen Schutz solcher Informationen an unzweifelhaft wahre Gegebenheiten, verkürzte dies den Schutzbereich der Meinungsäußerungsfreiheit auf inakzeptable Weise.¹³² Zu hohe Anforderungen an die Richtigkeit von Tatsachenbehauptungen bergen die Gefahr, dass aus Angst vor staatlichen Sanktionen tatsachenbasierte Äußerungen unterbleiben; dies wiederum führte zu einer problematischen „Selbstzensur“ des demokratischen Kommunikationsprozesses.¹³³

Derartige abschreckende Effekte („Chilling effects“) müssen bei der Beurteilung der Anforderung an die Richtigkeit von Tatsachenbehauptungen deshalb Berücksichtigung finden.¹³⁴ Im Zweifel ist von der Zulässigkeit einer Äußerung auszugehen.¹³⁵

127 BVerfGE 90, 1 (15); 94, 1 (8); 99, 185 (197); Grote/Wenzel, in: Dörr/Grote/Marauhn, GG/EMRK, Kap. 18 Rn. 29. Näher zu dieser verfassungsrechtlichen Grenzziehung zwischen Kommunikationsfreiheit und Desinformation auch Ferreau, AfP 2021, 204 (205 f., Rn. 4 ff.); Löber/Roßnagel, in: Steinebach et al., Desinformation, S. 149 ff.; Mafi-Gudarzi, ZRP 2019, 65 (67).

128 So BVerfGE 54, 208 (219); 61, 1 (8); ähnlich BVerfGE 90, 241 (247); BVerfG-K, NJW 2005, 3271 (3272). S. ferner Bethge, in: Sachs, GG, Art. 5 Rn. 28; Grote/Wenzel, in: Dörr/Grote/Marauhn, GG/EMRK, Kap. 18 Rn. 29. Kritisch zu dieser Schutzbereichsbegrenzung Ferreau, AfP 2021, 204 (205, Rn. 5), der den rechtsprinzipiellen Charakter von Grundrechten hervorhebt und deshalb eine Einschränkung erst über die abwägungsoffene Rechtfertigungsebene zulassen will. Dem lässt sich jedoch entgegenhalten, dass es sich bei den Grundrechten historisch betrachtet primär um Abwehrrechte des Bürgers gegen den Staat und erst sekundär um Prinzipien handelt; entsprechend nehmen letztere an den Grenzen des abwehrrechtlichen Gehalts der Grundrechte teil. Kritisch ferner Schulz, in: Paschke/Berlit/Meyer/Kröner, Gesamtes Medienrecht, 5. Abschnitt Rn. 21 m.w.N., der den diskursiven Charakter der Wahrheitsfeststellung betont und eine gerichtliche Bewertung von Wahrheit deshalb als problematisch erachtet. Wiederum anders Cremer, NVwZ 2023, 1463 ff., der auch menschenwürdevidrige, formalbeleidigende und schmähekritische Äußerungen aus dem Schutzbereich des Art. 5 Abs. 1 S. 1 GG (und nicht erst auf der Rechtfertigungsebene) ausscheiden will.

129 Bethge, in: Sachs, GG, Art. 5 Rn. 28.

130 Allg. zur Subsidiarität des Art. 2 Abs. 1 GG im Verhältnis zu anderen grundrechtlichen Gewährleistungen Di Fabio, in: Dürig/Herzog/Scholz, GG, Art. 2 Rn. 21 ff. Anders wohl Schulz, in: Paschke/Berlit/Meyer/Kröner, Gesamtes Medienrecht, 5. Abschnitt Rn. 21, wonach die Holocaust-Leugnung zwar nicht unter Art. 5 Abs. 1 S. 1 Var. 1 GG, wohl aber unter Art. 2 Abs. 1 GG fallen könne.

131 S. oben § 2 A. I. 2. a).

132 Grimm, NJW 1995, 1697 (1699); Warg, DÖV 2018, 473 (481).

133 Vgl. BVerfGE 90, 241 (248) unter Bezugnahme auf BVerfGE 54, 208 (219 f.); 61, 1 (8); 85, 1 (22).

134 Ähnlich Holznagel, MMR 2018, 18 (20).

135 Vgl. u. a. BVerfGE 7, 198 (208); 20, 162 (177); 93, 266 (294 f.).

Dies gilt auch für sog. „misinformative Verhaltensweisen“. Diese sind dadurch gekennzeichnet, dass sie absichtlich oder unabsichtlich richtige Tatsachenbehauptungen (Informationen) falsch „framen“ und dadurch die Gefahr falscher Schlussfolgerungen bei den Adressaten solcher Mitteilungen hervorrufen.¹³⁶ Dennoch bleiben sie grundsätzlich von der Meinungsäußerungsfreiheit geschützt.

Art. 5 Abs. 1 S. 1 Var. 1 GG dürfte schließlich auch solche Äußerungen schützen, die infolge einer Programmierung Meinungsäußerungen automatisiert zum Ausdruck bringen. Hierunter fallen etwa automatisierte Kommentare oder Likes, mit denen Einfluss auf den öffentlichen Willensbildungsprozess genommen werden soll – sei es durch eine inhaltliche Reaktion (Kommentare) oder durch eine Reichweitenverstärkung (Likes, Links und Teilen). Solange und soweit diese technischen Reaktionen auf ein bewusstes und zielgerichtetes menschliches Handeln in Form einer Programmierung zurückzuführen sind, fallen sie grundsätzlich in den Schutzbereich der Meinungsäußerungsfreiheit.¹³⁷

Verbreiten von Meinungen und Tatsachen

Art. 5 Abs. 1 S. 1 Var. 1 GG schützt allerdings nicht nur das Recht, in den Grenzen des vorstehend skizzierten Meinungen und hierauf bezogene Tatsachen zu äußern, sondern auch die Verbreitung solcher Inhalte.¹³⁸ Denn ohne das Recht zur Verbreitung einer Meinungsäußerung verlöre das Grundrecht mangels eines Schutzes geistiger Einwirkungen auf Dritte an Relevanz.

Welche Verbreitungshandlungen konkret durch Art. 5 Abs. 1 S. 1 Var. 1 GG geschützt werden, wird im rechtswissenschaftlichen Schrifttum indes kaum erörtert. Für den vorliegenden Untersuchungsgegenstand von Relevanz ist, dass dieser Verbreitungsschutz alle Tätigkeiten umfasst, die der Übermittlung einer grundrechtlich geschützten Meinungsäußerung dienen, einschließlich bloß untergeordneter begleitender Tätigkeiten, die als Mittel des geistigen Meinungskampfs die Wirkung und Reichweite der Äußerung verstärken sollen.¹³⁹ Unter derartigen begleitenden Tätigkeiten wird man auch den Einsatz technischer Hilfsmittel wie etwa Bot-Accounts, Chatbots oder Maßnahmen zur SEO-Optimierung subsumieren müssen, sofern sie darauf abzielen, einen bestimmten geistigen Inhalt im „Ozean der Meinungen und Mitteilungen“ für andere besser auffindbar oder prominenter sichtbar zu machen. Da Art. 5 Abs. 1 S. 1 GG grundsätzlich auch das pseudonyme und anonyme Äußern von Meinungen schützt¹⁴⁰, dürfte dies auch für solche

136 Baade, verfassungsblog v. 8.3.2022, benennt als Beispiel hierfür einen RT DE-Post, der bezogen auf den Ukraine-Krieg in der Überschrift die Unterstützung Russlands durch China zum Ausdruck brachte („China bei UN-Versammlung: Blockmentalität aufgeben und Russlands Sicherheitsinteressen ernstnehmen“) und erst ganz am Ende des Posts darauf hinwies, dass die UN-Vollversammlung mit großer Mehrheit Russland aufgefordert hatte, den Krieg gegen die Ukraine zu beenden; abrufbar unter: <https://web.archive.org/web/20220306091312/https://de.rt.com/kurzclips/video/133218-china-bei-un-versammlung-blockmentalitat/> (letzter Aufruf: 30.4.2026).

137 In diesem Sinne wohl auch Schulz, in: Paschke/Berlit/Meyer/Kröner, *Gesamtes Medienrecht*, 5. Abschnitt Rn. 20, der ebenfalls „algorithmisch erzeugte Kommunikate“ als vom Schutzbereich des Art. 5 Abs. 1 S. 1 GG umfasst ansieht.

138 S. Art. 5 Abs. 1 S. 1 GG, wo es heißt: „Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten (...)“ (Hervorhebung nur hier).

139 BVerfGE 97, 391 (398 f., Rn. 29); Jarass, in: Jarass/Pieroth, GG, Art. 5 Rn. 9; Krieger, in: Dreier, GG, Art. 5 Rn. 66.

140 BGH, NJW 2009, 2888 (2892, Rn. 38); Jarass, in: Jarass/Pieroth, GG, Art. 5 Rn. 13; Grabenwarter, in: Dürig/Herzog/Scholz, GG, Art. 5 Abs. 1 Rn. 86; Schulz, in: Paschke/Berlit/Meyer/Kröner, *Gesamtes Medienrecht*, 5. Abschnitt Rn. 19; Wendt, in: v. Münch/Kung, GG, Art. 5 Rn. 4. Einfachgesetzlich wird dieses Recht durch § 19 Abs. 2 des Gesetzes über

unterstützenden Verbreitungshandlungen gelten, die dem Adressaten einer Äußerung im Kommunikationsprozess nicht offengelegt werden. Hierzu zählen etwa automatisiert generierte Kommentare oder Likes, solange diese in Form einer Programmierung auf konkretes menschliches Handeln zurückzuführen sind. Gleiches gilt für Äußerungen unter Inanspruchnahme einer falschen Identität. Hieraus folgt freilich nicht, dass insoweit keine gesetzlichen Vorgaben oder Einschränkungen zulässig wären.¹⁴¹

Die tatbestandliche Grenze eines grundrechtlichen Schutzes wird erst dann erreicht, wenn es um die Verbreitung nicht geschützter Inhalte, also um bewusst oder erwiesen unwahrer Tatsachenbehauptungen, geht. Da – wie vorstehend ausgeführt – diese Mitteilungen schon nicht durch das Äußerungsrecht geschützt sind, gilt dies logischerweise auch für eine darauf bezogene automatisierte oder nicht-automatisierte Verbreitungshandlung. Der Gesetzgeber kann derartige Handlungen deshalb ohne grundrechtlichen Rechtfertigungsdruck verbieten, muss dies aber nicht.

(2) Völkerrechtlicher Grundrechtsschutz (EMRK)

Äußern von Meinungen und Tatsachen

Art. 10 Abs. 1 EMRK schützt das „Recht auf freie Meinungsäußerung“. Dieses Recht schließt insbesondere die Meinungsfreiheit – also das Bilden und Haben von Meinungen – sowie das Recht mit ein, „Informationen und Ideen“ (Art. 10 Abs. 1 S. 2 EMRK) „weiterzugeben“. Schon durch diesen Normtext wird deutlich, dass die Meinungsäußerungsfreiheit der EMRK nicht nur das Bilden, Haben und Äußern einer Meinung und Idee, also eines Werturteils, sondern auch die Weitergabe von Informationen, also von Tatsachen, schützt. Ebenso wie die deutsche Grundrechtsdogmatik unterscheidet der EGMR deshalb zwischen „value judgments“ und „statements of facts“.¹⁴² Anders als nach Art. 5 Abs. 1 S. 1 GG sind aber beide Inhalte vom Schutzbereich des Art. 10 Abs. 1 EMRK umfasst – und zwar grundsätzlich losgelöst von ihrem Wahrheitsgehalt.¹⁴³ Eine Unterscheidung zwischen „Meinungen“ und bloßen „Tatsachen“ erfolgt sodann auf der Ebene der Eingriffsrechtfertigung.¹⁴⁴

Mit Blick auf erwiesen unwahre Tatsachenbehauptungen war in der Rechtsprechung des EGMR lange unklar, ob das Gericht diesen Umstand – wie das Bundesverfassungsgericht – schon auf der Schutzbereichs- oder erst auf der Rechtfertigungsebene berücksichtigt.¹⁴⁵ In der Rechtspre-

den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz – TDDDG) v. 23.6.2021 (BGBl. I S. 1982; 2022 I S. 1045), zuletzt geändert durch Art. 3 des Gesetzes v. 10.3.2026 (BGBl. 2026 I Nr. 64), geschützt.

141 Dazu noch nachstehend § 2 C. II. 2. c).

142 EGMR, Urt. v. 23.6.2009 – 17089/883, § 29 – Sorguc/Türkei; Urt. v. 8.7.1986 – 9815/82, §§ 22, 46 – Lingens/Österreich; Cornils, in: Gersdorf/Paal, BeckOK-InfoMedienR, EMRK, Art. 10 Rn. 15.

143 Grabenwarter/Pabel, EMRK, § 23 Rn. 5; Mensching, in: Karpenstein/Mayer, EMRK, Art. 10 Rn. 9.

144 Vgl. EGMR, Urt. v. 8.7.1986 – 9815/82, §§ 22, 46 – Lingens/Österreich; Urt. v. 23.5.1991 – 11662/85, § 63 – Oberschlick/Österreich; Urt. v. 12.7.2001 – 29032/95, § 85 – Feldek/Slowakei; Grote/Wenzel, in: Dörr/Grote/Marauhn, GG/EMRK Konkordanzkommentar, Kap. 18 Rn. 28.

145 Hong, ZaöRV 2010, 73 (83 f.).

chung des EGMR finden sich Beispiele für beide Lösungsansätze.¹⁴⁶ Während etwa in den Entscheidungen „Witzsch“ und „Schimanek“ im Endeffekt noch die Rechtfertigungslösung bevorzugt wurde¹⁴⁷, löste sich der EGMR in späteren Entscheidungen von dieser Sichtweise und entschied unter Berufung auf Art. 17 EMRK (Verbot des Rechtsmissbrauchs¹⁴⁸), dass eine Leugnung geschichtlicher Tatsachen zu revisionistischen Zwecken *a limine* nicht unter den Schutz des Art. 10 Abs. 1 EMRK falle.¹⁴⁹ Der EGMR hat diese Einschränkung für die „Kategorie klar etablierter historischer Tatsachen“ – zu denen etwa der Holocaust gehört – entwickelt, deren „Leugnen oder Revision“ einen Missbrauch des Grundrechts i.S.d. Art. 17 EMRK darstelle und deshalb nicht durch die Meinungsfreiheit geschützt werde. In Folgeentscheidungen wurde dies vom Gerichtshof bestätigt¹⁵⁰ und dort um bestimmte antisemitische, extremistische und islamistische Äußerungen in Gestalt von Hassaufrufen sowie rassistischen Beleidigungen ergänzt.¹⁵¹ In anderen Fällen hat er das Vorliegen dieser Fallgruppen abgelehnt und den Schutz durch Art. 10 Abs. 1 EMRK für eröffnet erklärt.¹⁵²

Allerdings nähert sich diese Unterscheidung des EGMR nur partiell der Schutzbereichsrestriktion des Bundesverfassungsgerichts für bewusst oder erwiesen unwahre Tatsachenbehauptungen an. Der Gerichtshof hat vielmehr betont, dass Art. 17 EMRK nur ausnahmsweise in extremen Fällen anzuwenden sei und er in Fällen, die Art. 10 der Konvention betreffen, nur dann herangezogen werden sollte, wenn unmittelbar erkennbar sei, dass dieser Artikel durch die beanstandeten Äußerungen von seinem eigentlichen Ziel entfernt werden solle, indem das Recht auf freie Meinungsäußerung zu Zwecken genutzt werde, die den Werten der Konvention eindeutig zuwiderliefen.¹⁵³ Bei der Prüfung, ob verbale oder non-verbale Äußerungen aufgrund des Art. 17 EMRK dem Schutz des Art. 10 Abs. 1 EMRK *a limine* entzogen sind, kommt es nach Auffassung des EGMR deshalb entscheidend darauf an, ob sich diese Äußerungen gegen die der Konvention zugrundeliegende Werte richteten, etwa indem sie Hass oder Gewalt schürten, bzw. ob ihr Urheber durch das Tätigen dieser Äußerungen versucht habe, sich auf die Konvention zu berufen, um eine Tätigkeit auszuüben oder eine Handlung vorzunehmen, die darauf abziele, die in der Konvention festgelegten Rechte und Freiheiten zunichte zu machen.¹⁵⁴ In Fällen, in denen es um die Leugnung des Holocaust geht, entscheidet der EGMR deshalb im Einzelfall und in Abhängigkeit der Gesamtumstände darüber, ob er Art. 17 EMRK unmittelbar anwendet und die betroffene Äußerung für mit der Konvention unvereinbar erklärt oder ob er stattdessen Art. 10 EMRK für anwendbar hält und Art. 17 EMRK erst später bei der Prüfung der Notwendigkeit des

¹⁴⁶ Für eine Übersicht der Rechtsprechung bis 2010 s. Hong, ZaöRV 2010, 73 (77, 86 ff.).

¹⁴⁷ Vgl. EGMR, Entsch. v. 20.4.1999 – 41448/98, S.4 f. – Witzsch/Deutschland; Entsch. v. 1.2.2000 – 32307/96, S. 7 – Schimanek/Österreich: „In these circumstances, the Court concludes that it derives from Article 17 that the applicant's conviction was necessary in a democratic society within the meaning of the second paragraph of Article 10.“

¹⁴⁸ Die Bestimmung lautet: „Diese Konvention ist nicht so auszulegen, als begründe sie für einen Staat, eine Gruppe oder eine Person das Recht, eine Tätigkeit auszuüben oder eine Handlung vorzunehmen, die darauf abzielt, die in der Konvention festgelegten Rechte und Freiheiten abzuschaffen oder sie stärker einzuschränken, als es in der Konvention vorgesehen ist.“

¹⁴⁹ Vgl. EGMR, Entsch. v. 24.6.2003 – 65831/01 = NJW 2004, 3691 (3692 f.) – Garaudy/Frankreich. Ausführlich hierzu Hong, ZaöRV 2010, 73 (90 ff.).

¹⁵⁰ U. a. in EGMR, Entsch. v. 13.12.2005 – 7485/03 – Witzsch/Deutschland.

¹⁵¹ Vgl. hierzu und zu den Rechtsprechungsnachweisen Mensching, in: Karpenstein/Mayer, EMRK, Art. 10 Rn. 10. S. ferner Cornils, in: Gersdorf/Paal, BeckOK-InfoMedienR, EMRK, Art. 11 Rn. 15.

¹⁵² Vgl. etwa EGMR, Urt. v. 23.9.1998 – 24662/94 – Lehieux u. a./Frankreich zur Bewertung der Rolle von Philippe Pétain im Zweiten Weltkrieg.

¹⁵³ EGMR (GK), Urt. v. 15.10.2015 – 27510/08, § 114 – Perinçek/Schweiz.

¹⁵⁴ EGMR (GK), Urt. v. 15.10.2015 – 27510/08, § 115 – Perinçek/Schweiz.

behaupteten Eingriffs – also im Rahmen der Rechtfertigungsprüfung – heranzieht.¹⁵⁵ Es bedarf mithin einer wertenden Betrachtung des jeweiligen Einzelfalls, ob von einer *A-priori*-Schutzbereichsbegrenzung oder von einer Rechtfertigungslösung auszugehen ist. Einige der vorstehend skizzierten manipulativen Maßnahmen (wie z. B. automatisierte Hasskommentare) könnten die Voraussetzung einer Schutzbereichsrestriktion erfüllen, andere (wie z. B. automatisierte Likes) wohl eher nicht.

Verbreiten von Meinungen und Tatsachen

Jenseits der klassischen Formen einer Verbreitung und Weitergabe von Informationen und Ideen durch Texte, Bilder oder gesprochene Worte lassen sich der Rechtsprechung und dem rechtswissenschaftlichen Schrifttum keine Konkretisierungen dieser Tätigkeiten entnehmen. Vor diesem Hintergrund können die obigen Ausführungen zu Art. 5 Abs. 1 S. 1 GG auf Art. 10 Abs. 1 EMRK übertragen werden. Auch dieses Grundrecht schützt mithin solche Handlungen, die vorliegend als Manipulationen des öffentlichen Informationsraums beschrieben werden. Hierzu gehören u. a. automatisierte Verbreitungsvorgänge, sofern diese einer konkreten natürlichen oder juristischen Person zugerechnet werden können. Gleiches gilt für die Täuschung über die Identität des Äußernden. Im Übrigen gilt auch hier der Grundsatz, dass das, was nicht vom Schutzbereich der Meinungsäußerungsfreiheit umfasst ist, nicht den Schutz der Verbreitungsfreiheit (die bei Art. 10 Abs. 1 EMRK in der Äußerungsfreiheit enthalten ist) genießen kann.

(3) Unionaler Grundrechtsschutz (EUGRC)

Auf unionaler Ebene wird die Meinungsäußerungsfreiheit durch Art. 11 Abs. 1 S. 1 EUGRC geschützt. Laut Art. 11 Abs. 1 S. 2 EUGRC schließt dies die Meinungsfreiheit¹⁵⁶ und die Freiheit mit ein, „Informationen und Ideen“ ohne behördliche Eingriffe weiterzugeben. Der Wortlaut des Art. 11 Abs. 1 EUGRC stimmt folglich mit demjenigen des Art. 10 Abs. 1 EMRK überein. Folglich greift die Auslegungsregelung in Art. 53 Abs. 3 EUGRC. Mangels einer anderslautenden EuGH-Rechtsprechung kann deshalb auf die vorstehend zur EMRK und zur Rechtsprechung des EGMR herausgearbeiteten Grundsätze und Grenzen der Meinungsäußerungsfreiheit verwiesen werden, zumal Art. 54 EUGRC wortgleich Art. 17 EMRK wiederholt.¹⁵⁷ Gleiches gilt im Übrigen für das Verbreiten von Meinungen und Tatsachen.

bb) Medienfreiheit

Für den Untersuchungsgegenstand sind allerdings auch die Medienfreiheiten von Relevanz. Zu denken ist hier an die im Rahmen der Fallstudien erörterte Konstellation, dass ein privates Medium oder ein staatlich nicht gelenkter Influencer über Desinformation, Misinformation bzw.

¹⁵⁵ EGMR, Ur. v. 3.10.2019 – 55225/14, § 37 – Pastörs/Deutschland.

¹⁵⁶ S. hierzu bereits oben Fn. 118.

¹⁵⁷ Brings-Wiesen, in: Spindler/Schuster/Kaesling, Recht der elektronischen Medien, 1. Teil C Rn. 16; Jarass, Charta der Grundrechte der EU, Art. 11 Rn. 10; Grote/Wenzel, in: Dörr/Grote/Maruhn, GG/EMRK Konkordanzkommentar, Kap. 18 Rn. 28.

Propaganda auf den öffentlichen Informationsraum einwirkt. Auch ist die Frage zu erörtern, inwieweit sich Online-Plattformen auf den Schutz der Medienfreiheiten berufen können.

(1) Nationaler Grundrechtsschutz (GG)

Schutz journalistisch-redaktionell geschützter Mediendienste

Linear oder nichtlinear verbreitete digitale Mediendienste mit journalistisch-redaktionell gestalteten Inhalten können sich – je nach Konstellation – auf die durch Art. 5 Abs. 1 S. 2 GG verbürgte Presse- oder Rundfunkfreiheit berufen. Da beide Grundrechte dem Schutz des für eine Demokratie schlechthin konstitutiven Meinungsbildungsprozesses dienen, vermitteln sie einen starken Schutz gegen solche staatlichen Maßnahmen, die sich auf den journalistisch-redaktionell gestalteten Inhalt und dessen Verbreitung beziehen. Allerdings können Inhalte, die nicht dem Schutz der Meinungsfreiheit (vorstehend aa)) unterfallen, auch keinen Schutz durch die Medien Grundrechte genießen.¹⁵⁸

Für den grundrechtlichen Schutz von Manipulationen des öffentlichen Informationsraums von besonderem Interesse sind die Ausführungen des Bundesverwaltungsgerichts in seiner „Compact-Entscheidung“.¹⁵⁹ Das Gericht hat dort zwar anerkannt, dass auch Presse- und Medienunternehmen als Wirtschaftsvereinigungen auf der Grundlage des Vereinsgesetzes verboten werden können, wenn sie sich als verfassungsfeindlich i.S.d. Art. 9 Abs. 2 GG erweisen.¹⁶⁰ Das Gericht hat ferner anerkannt, dass die Verbotsbehörden und Gerichte zur Begründung eines Vereinsverbots auch bei einem Presse- und Medienunternehmen an Inhalte von Meinungsäußerungen, die Ausdruck des Bestrebens sind, die verfassungsmäßige Ordnung zu beseitigen, anknüpfen dürften. Dies gelte selbst dann, wenn diese Äußerungen weder rechtswidrig noch strafbar seien; sie könnten jedenfalls als Indizien für ein Vereinsverbot herangezogen werden.¹⁶¹ Allerdings müsse im Rahmen der Verhältnismäßigkeitsprüfung des Verbots eines Presse- und Medienunternehmens dem Zweck des Art. 5 Abs. 1 S. 2 GG angemessen Rechnung getragen werden. Die Pressefreiheit schütze eine freie, staatlich nicht gelenkte Presse als ein Wesenselement der freiheitlichen Demokratie. Aufgabe der Presse sei es deshalb, umfassend zu informieren, die Vielfalt der bestehenden Meinungen wiederzugeben und selbst Meinungen zu bilden und zu vertreten. Dies müsse in Unabhängigkeit vom Staat erfolgen, weshalb die Pressefreiheit vor staatlichen Einflussnahmen auf die mit Hilfe der Presse gestalteten und verbreiteten Informationen, insbesondere vor negativen oder positiven Sanktionen, schütze. Durch das Verbot eines Presse- und Medienunternehmens greife der Staat jedoch besonders massiv in die freie und öffentliche Meinungsbildung ein. Nach Ansicht des Bundesverwaltungsgerichts sei ein Vereinsverbot deshalb nicht mit den Anforderungen des Grundgesetzes zu vereinbaren, wenn es nur als Mittel

158 Dieser Gleichklang rechtfertigt sich aus der Erwägung heraus, dass laut BVerfG die Meinungsfreiheit auch dann Form und Inhalt von Meinungsäußerungen schützt, wenn sie im Rahmen der Ausübung der Medienfreiheiten erfolgen; vgl. BVerfGE 85, 1 (11 ff.); Schlemmer, in: Epping/Hillgruber, BeckOK Grundgesetz, Art. 5 Rn. 20.

159 BVerwG, Urt. v. 24.6.2025 – 6 A 4.24 = NJW 2025, 3650 ff. Zum vorangegangenen vorläufigen Rechtsschutzverfahren Brosius-Gersdorf/Gersdorf, NVwZ 2024, 1697 ff.; Ferreau, K&R 2024, 777 ff.

160 S. hierzu BVerwG, Urt. v. 24.6.2025 – 6 A 4.24 = NJW 2025, 3650, Rn. 21 ff. (dort auch m. Nachw. zur Gegenauffassung) sowie oben § 2 C. I. 2. a).

161 BVerwG, Urt. v. 24.6.2025 – 6 A 4.24 = NJW 2025, 3650, Rn. 38 ff.

fungierte, Meinungsäußerungen oder Publikationen zu untersagen, die für sich genommen den Schutz aus Art. 5 Abs. 1 GG genießen. Das Äußern und Verbreiten verfassungsfeindlicher Ideen in Presse- und Medienerzeugnissen überschritten als solche noch nicht die Grenze der freien politischen Auseinandersetzung. Vielmehr setze die Verfassung grundsätzlich auf die freie, öffentliche Kommunikation und die Kraft des Diskurses. Rechtsradikales Gedankengut sei hiervon nicht *per se* ausgenommen; erst recht gelte dies für bloße Geschmacklosigkeiten oder wissenschaftliche Halbwahrheiten.¹⁶² Abstrakte Gefahren, die mit der Verbreitung in Presse- und Medienprodukten verbunden seien, namentlich die hierdurch erzielte große Reichweite, nehme das Grundgesetz nach der normativen Wertung des Art. 5 Abs. 1 S. 2 GG deshalb bewusst hin.¹⁶³

Bei Zugrundelegung dieser Hürden dürfte zukünftig das vereinsrechtliche begründete Verbot eines Mediendiensteanbieter nahezu ausgeschlossen sein, soweit sich dieser auf das Äußern und Publizieren grundrechtlich geschützter Meinungen beschränkt. Erst, wenn er diesen Schutzbereich verließ, etwa in verfassungsfeindlicher Absicht erwiesen unwahre Tatsachenbehauptungen oder strafrechtlich untersagte Meinungen¹⁶⁴ verbreitete, käme eine vereinsrechtliche Verbotsmaßnahme in Betracht. Aber auch in diesem Fall wäre es nach der Rechtsprechung des Bundesverwaltungsgerichts erforderlich, dass solche nicht geschützten Inhalte dem Medienunternehmen zuzurechnen und für die Publikationstätigkeit dieses Unternehmens „prägend“ sind.¹⁶⁵

Schutz von Online-Plattformen

Welchen grundrechtlichen Schutz Online-Plattformen genießen, ist bislang nicht abschließend geklärt. Immerhin hat das Bundesverfassungsgericht für Online-Suchmaschinen (und damit für einen bedeutenden Teil der Medienintermediäre) in seiner „Recht auf Vergessen II“-Entscheidung mit Blick auf die EU-Grundrechte zu erkennen gegeben, dass es für reine Suchmaschinen nur von einem Schutz über die unternehmerische Betätigungsfreiheit und nicht von einem Schutz über die Kommunikationsgrundrechte, d. h. die Meinungs- oder gar Rundfunkfreiheit ausgeht. Namentlich hat es dort angenommen, dass der beklagte Suchmaschinenbetreiber in den persönlichen und sachlichen Schutzbereich des Art. 16 EUGRC (unternehmerische Freiheit) falle. Hingegen hat es seinen Schutz über die Freiheit der Meinungsäußerung aus Art. 11 Abs. 1 EUGRC explizit abgelehnt. Das Gericht erkannte zwar an, dass die angebotenen Suchdienste und die hierfür verwendeten Mittel zur Aufbereitung der Suchergebnisse nicht inhaltsneutral seien, sondern auf die Meinungsbildung der Nutzer erheblichen Einfluss ausüben könnten. Jedoch bezweckten diese Dienste nicht die Verbreitung bestimmter Meinungen. Vielmehr seien sie allein darauf ausgerichtet, potenzielle Interessen der Nutzerinnen und Nutzer unabhängig von bestimmten Meinungen möglichst weitgehend zu befriedigen und so eine Dienstleistung im wirt-

¹⁶² S. hierzu bereits oben § 2 C. II. 2. b) aa (1).

¹⁶³ BVerwG, Urt. v. 24.6.2025 – 6 A 4.24 = NJW 2025, 3650, Rn. 153 ff.

¹⁶⁴ Dazu noch unten § 2 D. I. 2. b).

¹⁶⁵ Vgl. BVerwG, Urt. v. 24.6.2025 – 6 A 4.24 = NJW 2025, 3650, Rn. 157 ff. An einer solchen Zurechnung fehlte es bei Online-Plattformen i.Ü. regelmäßig, da diese erst ab Kenntniserlangungen für die auf ihnen gespeicherten Online-Inhalte verantwortlich werden (vgl. Art. 6 DSA sowie unten § 2 D. I. 1. a) bb)).

schaftlichen Interesse des Unternehmens möglichst attraktiv zu gestalten.¹⁶⁶ Im Umkehrschluss folgt hieraus, dass den Suchmaschinenbetreibern ein geringerer Grundrechtsschutz zukommt, da sie nur über die Wirtschaftsgrundrechte (auf nationaler Ebene also die Art. 12 und 14 GG, auf EU-Ebene Art. 16 EUGRC), nicht aber über die Kommunikationsgrundrechte geschützt werden. Verhältnismäßige gesetzgeberische Maßnahmen zur Bekämpfung von Manipulationen des öffentlichen Kommunikationsraums werden sich in der Abwägung deshalb regelmäßig durchsetzen.

Unklar bleibt jedoch, ob diese Aussagen auch auf soziale Netzwerke erstreckt werden können. Im Unterschied zu Suchmaschinen bezwecken diese – um in der Diktion des Bundesverfassungsgerichts zu bleiben – gerade die Verbreitung meinungsbildender Angebote und Inhalte. In seiner Facebook-Entscheidung hat der Bundesgerichtshof einem sozialen Netzwerk deshalb nicht nur grundrechtlichen Schutz aus Art. 12 Abs. 1 GG, sondern auch aus Art. 5 Abs. 1 S. 1 GG (Meinungsfreiheit) zugestanden. Sie stellten sich als „unverzichtbare Mittlerperson“ für den Austausch von Meinungen dar und nähmen, anders als ein rein technischer Vermittler (wie z. B. ein Internet Access Provider), über ihre Gemeinschaftsstandards zudem Einfluss auf den Kommunikationsprozess.¹⁶⁷ Diese Auffassung findet in Teilen der Literatur Unterstützung.¹⁶⁸ Teils werden dort aber auch noch weitergehende Auffassungen (Schutz sozialer Netzwerke durch die Rundfunkfreiheit) vertreten¹⁶⁹, was mit Blick auf den fehlenden Darbietungscharakter der Medienintermediärsleistung jedoch als fraglich erscheint.¹⁷⁰

Diese schwierigen und nicht abschließend geklärten Schutzbereichsfragen brauchen an dieser Stelle nicht weiter vertieft zu werden. Jedenfalls kann der Staat unter Beachtung des Verhältnismäßigkeitsprinzips zum Schutz der grundrechtlichen Wertentscheidungen des Art. 5 Abs. 1 S. 1 und 2 GG (Schutz des Meinungsbildungsprozesses und der Vielfalt) sowie des Demokratieprinzips (Art. 20 Abs. 1 und 2 GG) vor Manipulationen des öffentlichen Informationsraums in die Grundrechtspositionen der Online-Plattformen eingreifen.

¹⁶⁶ BVerfGE 152, 216 (257 f., Rn. 104 f.). Das Gericht verweist an dieser Stelle verstärkend auf EuGH, Urt. v. 13.5.2014, Az. C-131/12, Rn. 85 – Google Spain, wo Suchmaschinenbetreibern die Berufung auf das datenschutzrechtliche Medienprivileg versagt wurde.

¹⁶⁷ BGH, NJW 2021, 3179 (3187, Rn. 74). Das Gericht nimmt damit auf eine Rechtsfigur Bezug, die das BVerfG in seiner Mephisto-Entscheidung zur Begründung der Grundrechtsträgerschaft von Buchverlagen entwickelt hat. Ähnlich wie der BGH sprach das Gericht dort von einer „unentbehrlichen Mittlerfunktion“ (BVerfGE 30, 173 [191]). Und auch für die selbstständige Vermittlungstätigkeit des Presse-Grossos bejahte das BVerfG einen Schutz durch die Pressefreiheit (Art. 5 Abs. 1 S. 2 GG), da sie „typischerweise pressebezogen ist, in enger organisatorischer Bindung an die Presse erfolgt, für das Funktionieren einer freien Presse notwendig ist und wenn sich die staatliche Regulierung dieser Tätigkeit zugleich einschränkend auf die Meinungsverbreitung auswirkt“ (BVerfGE 77, 346 [354]).

¹⁶⁸ Pille, Meinungsmacht sozialer Netzwerke, S. 177 ff., der einen Verbreitungsschutz nach Art. 5 Abs. 1 S. 1 GG für möglich hält, letztlich einen institutionellen Schutz der Internetintermediäre aber über ein aus Art. 5 Abs. 1 GG fließendes einheitliches Grundrecht der Kommunikationsfreiheit herleitet.

¹⁶⁹ Vgl. etwa Heidtke, Meinungsbildung und Medienintermediäre, 169 ff. m.w.N., der wegen des offenen Rundfunkbegriffs von einem Schutz der Medienintermediäre durch die Rundfunkfreiheit ausgeht und deshalb die Ausgestaltungsdogmatik des BVerfG für übertragbar hält. Ähnlich Gersdorf, 74. dJt I/G 12 ff., der je nach Gegenstand für einen Schutz über die Massenkommunikationsgrundrechte (Presse- oder Rundfunkfreiheit) plädiert.

¹⁷⁰ Skeptisch wie hier Pille, Meinungsmacht sozialer Netzwerke, S. 186.

Schutz KI-generierter Medieninhalte

Soweit die Manipulation des öffentlichen Informationsraums durch den Einsatz von KI-Systemen erfolgt, die – wie etwa ein Large Language Model (LLM) – autonom Inhalte generieren und verbreiten¹⁷¹, stellt sich des Weiteren die Frage, ob ein solcher KI-generierter Inhalt grundrechtlich durch die Medienfreiheiten (oder alternativ die Meinungsfreiheit) geschützt sein kann. Letztlich wird dies vom Grad der Autonomie des eingesetzten KI-Systems abhängen: Soweit Personen Einfluss auf die Arbeitsweise dieses Systems ausüben können, vermag ein solch manipulatives Verhalten in den vorstehend skizzierten Grenzen (unwahre Tatsachenbehauptungen) den Schutz der Kommunikationsgrundrechte für sich in Anspruch zu nehmen. Werden diese Kommunikationsinhalte jedoch völlig autonom generiert und verbreitet, fehlt es an einem Willensbildungsprozess durch eine natürliche oder juristische Person, die den maßgeblichen Anknüpfungspunkt für Grundrechtsschutz durch Art. 5 Abs. 1 GG darstellt.¹⁷² Hierzu bedarf es einer Bewertung des jeweils eingesetzten KI-Dienstes, ggf. unter Einschluss der für die Ergebniserzeugung erforderlichen Prompts.

(2) Europäischer Grundrechtsschutz (EMRK und EUGRC)

Für den europäischen Grundrechtsschutz (EMRK und EUGRC) gilt das vorstehend Ausgeführte sinngemäß. Für Suchmaschinen ist daran zu erinnern, dass das Bundesverfassungsgericht unter Rückgriff auf die datenschutzrechtliche Judikatur des EuGH einen Grundrechtsschutz dieser Intermediäre aus Art. 11 EUGRC verneint und stattdessen auf Art. 16 EUGRC rekurriert hat. Für die Online-Plattformen (soziale Netzwerke) wird man demgegenüber einen grundrechtlichen Schutz aus Art. 10 Abs. 1 EMRK bzw. Art. 11 Abs. 1 EMRK und – soweit die unternehmerischen Interessen der Plattformen betroffen sind – aus Art. 16 und 17 EUGRC bejahen können.¹⁷³

Auch ist zu betonen, dass – analog zum nationalen Grundrechtsschutz aus Art. 5 Abs. 1 S. 1 Var. 2 GG – weder aus Art. 10 Abs. 1 EMRK noch aus Art. 11 Abs. 1 S. 2 EUGRC eine Pflicht der EU oder der Mitgliedstaaten fließt, den Zugang zu Informationen zu gewährleisten; die dort normierte Informationsfreiheit beschränkt sich deshalb auf die Nutzung allgemein zugänglicher Quellen.¹⁷⁴ Unionale oder mitgliedstaatliche Maßnahmen gegen eine Manipulation des öffentlichen Informationsraums können deshalb die Meinungs- und Medienfreiheiten, nicht aber die Informationsfreiheit potenzieller Adressaten solcher Manipulationen beeinträchtigen.

¹⁷¹ S. dazu noch unten § 2 D. I. 1. c).

¹⁷² Vgl. hierzu auch Schwartmann, AfP 2024, 1 (5, Rn. 27 f.) m.w.N.

¹⁷³ Vgl. insoweit EGMR, Urt. v. 19.2.2013, 40397/12 – Neij u. a./Schweden mit dem Hinweis, dass die durch Art. 10 Abs. 1 EMRK geschützte Weitergabe nicht auf den Autor beschränkt sei, sondern sich auch auf Verleger und das Bereitstellen einer Internetplattform beziehe; Daiber, in: Meyer-Ladewig/Nettesheim/von Raumer, EMRK, Art. 10 Rn. 18. S. ferner Brauneck, EuR 2020, 89 (108 f.) m.w.N.

¹⁷⁴ Jarass, Charta der Grundrechte der EU, Art. 11 Rn. 15 m.w.N.

C) SCHRANKEN DER MEINUNGS- UND MEDIENFREIHEIT

aa) Schranken der Kommunikationsgrundrechte

Soweit nach dem vorstehend Ausgeführten ein kommunikatives Verhalten in den Schutzbereich der Meinungs- und Medienfreiheiten (Kommunikationsfreiheiten) fällt, kann dieses gemäß Art. 5 Abs. 2 GG durch ein „allgemeines Gesetz“ eingeschränkt werden.¹⁷⁵ Darunter sind Gesetze zu verstehen, die nicht eine Meinung als solche verbieten, die sich nicht gegen die Äußerung einer Meinung als solche richten, sondern dem Schutz eines schlechthin ohne Rücksicht auf eine bestimmte Meinung zu schützenden Rechtsguts dienen.¹⁷⁶

Einen solchen geschriebenen Schrankenvorbehalt statuiert auch Art. 10 EMRK, dessen Abs. 2 zunächst betont, dass die Ausübung der Kommunikationsfreiheiten „mit Pflichten und Verantwortung verbunden“ ist; „sie kann daher Formvorschriften, Bedingungen, Einschränkungen oder Strafdrohungen unterworfen werden, die gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sind für die nationale Sicherheit, die territoriale Unversehrtheit oder die öffentliche Sicherheit, zur Aufrechterhaltung der Ordnung oder zur Verhütung von Straftaten, zum Schutz der Gesundheit oder Moral, zum Schutz des guten Rufes oder der Rechte anderer, zur Verhinderung der Verbreitung vertraulicher Informationen oder zur Wahrung der Autorität und der Unparteilichkeit der Rechtsprechung.“ In bestechender Weise reflektiert dieser Schrankenvorbehalt die europäische Kommunikationsdogmatik in Gestalt der hierzu als nötig empfundenen rechtskulturellen Grenzen. Mit seiner expliziten Bezugnahme auf die nationale Sicherheit und territoriale Unversehrtheit ist die Bestimmung im Angesicht von FIMI-Maßnahmen durch feindselige Drittstaaten von erschreckender Aktualität.

Art. 11 EUGRC wiederum steht unter dem Vorbehalt der aus Art. 52 Abs. 1 EUGRC fließenden, für alle Charta-Rechte geltenden Grundrechtsschranke. Hiernach muss jede „Einschränkung oder Ausübung der in dieser Charta anerkannten Rechte und Freiheiten (...) gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie notwendig sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.“

Allen drei Schranken ist gemein, dass sie nach einer gesetzlichen Grundlage verlangen, die ihrerseits gewissen Schranken (den sog. Schranken-Schranken) unterworfen ist.¹⁷⁷

175 Zwar finden die Kommunikationsfreiheiten ihre Schranken auch in den gesetzlichen Bestimmungen zum Schutz der Jugend und in dem Recht der persönlichen Ehre. Wie bereits dargelegt, bewertet die vorliegende Untersuchung grundrechtliche Fragen indes aus der Perspektive einer manipulativen Verbreitung von Inhalten und nicht aus der Rezipientenperspektive; zudem fordert das BVerfG auch für den Jugend- und Ehrenschatz ein allgemeines Gesetz i.S.d. Art. 5 Abs. 2 GG; vgl. BVerfGE 124, 300 (326).

176 Locus classicus: BVerfGE 7, 198 (209 f.) – Lüth. Präzisiert durch BVerfGE 124, 300 (321 ff.) – Rudolf Heß-Gedenkkundgebung.

177 Dazu sogleich nachfolgend bb).

bb) Schranken-Schranken der Kommunikationsgrundrechte

Für den vorliegenden Kontext bestehen diese Schranken-Schranken aus dem abwägungsoffenen, d.h. nur relativ wirkenden Verhältnismäßigkeitsprinzip ((1)) sowie aus dem absolut wirkenden Zensurverbot ((2)).

(1) Relative Schranken-Schranke (Verhältnismäßigkeitsprinzip)

Als wichtigste materiellrechtliche Schranken-Schranke für die Beschränkung von Grundrechten fungiert das Verhältnismäßigkeitsprinzip. Für die nationalen Grundrechte fließt es aus Art. 19 Abs. 2 GG (Wesensgehaltssperre) sowie aus dem Rechtsstaatsprinzip (Art. 20 Abs. 3 GG) und wurde durch die Rechtsprechung des Bundesverfassungsgerichts für die einzelnen Grundrechte verfeinert. Nach diesem Prinzip muss der hoheitliche Eingriff in ein Grundrecht einen legitimen Zweck verfolgen und geeignet sein, diesen Zweck zu erreichen. Zudem muss er erforderlich sein, d.h. es darf kein gleich geeignetes, aber milderer Mittel zur Erreichung des Eingriffszwecks zu Verfügung stehen. Und schließlich muss der Zweck der Beschränkung in Relation zur Tiefe der Beschränkung des Grundrechts in einem angemessenen Verhältnis stehen. Insoweit hat das Bundesverfassungsgericht speziell für die Kommunikationsfreiheiten das Angemessenheitskriterium in Gestalt der Wechselwirkungslehre sowohl für die Rechtsetzung als auch für die Rechtsanwendung weiter konkretisiert: Hiernach findet zwischen dem Grundrechtsschutz und den Grundrechtsschranken eine Wechselwirkung in dem Sinne statt, dass die allgemeinen Gesetze zwar Schranken setzen, diese aber ihrerseits im Licht dieser Grundrechtsverbürgungen bestimmt werden müssen. Die Schranken der Kommunikationsfreiheit dürfen deren substanziellen Gehalt mithin nicht in Frage stellen. Folglich ist bei Einschränkungen der besonderen Bedeutung des Kommunikationsprozesses Rechnung zu tragen, weshalb Beschränkungen nur aus überragend wichtigen Allgemein- oder Individualwohlgründen in Betracht kommen können.¹⁷⁸

Auch in Art. 10 Abs. 2 EMRK kommt das Verhältnismäßigkeitsprinzip deutlich zum Ausdruck. Dieses zählt nicht nur die legitimen Ziele für eine hoheitliche Beschränkung der Kommunikationsfreiheiten auf, sondern fordert zugleich, dass die Beschränkung „in einer demokratischen Gesellschaft notwendig sein muss“. Nach der Rechtsprechung des EGMR ist ein hoheitlicher Eingriff „notwendig“, wenn er einem „dringenden sozialen Bedürfnis“ („pressing social need“) entspricht.¹⁷⁹ Dies wiederum setzt voraus, dass die von den hoheitlichen Stellen zur Rechtfertigung des Eingriffs angeführten Gründe relevant und ausreichend („relevant and sufficient“) sein müssen und der Eingriff verhältnismäßig zu den verfolgten legitimen Zielen („proportionate to the legitimate aims pursued“) ist.¹⁸⁰ Diese Voraussetzungen stimmen mithin mit denjenigen des nationalen Rechts überein. Letzteres trifft auch auf Art. 11 i.V.m. Art. 52 Abs. 1 EUGRC zu, der explizit auf das Verhältnismäßigkeitsprinzip Bezug nimmt und zudem – wie das deutsche Recht – die Achtung des Wesensgehalts der Grundrechte einfordert.

178 Vgl. BVerfGE 7, 198 (208 f.); 94, 1 (8); 107, 299 (331); 124, 300 (331 f.).

179 Vgl. EGMR, Ur. v. 26. 9. 1995, Nr. 7851/91 Rn. 52 – Vogt = NJW 1996, 375 ff.; Mensching, in: Karpenstein/Mayer, EMRK, Art. 10 Rn. 52.

180 Vgl. EGMR (GK), Ur. v. 17.12.2004, Nr. 33348/96 Rn. 88 ff. – Cumpănaă u. Mazăre; Mensching, in: Karpenstein/Mayer, EMRK, Art. 10 Rn. 52.

Für den vorliegenden Untersuchungsgegenstand folgt aus alledem, dass Manipulationen des öffentlichen Informationsraums Gegenstand hoheitlicher Einschränkungen sein können. Art. 10 Abs. 2 EMRK benennt hierzu die legitimen Gründe, die über diese Bestimmung auf das nationale und unionale Recht ausstrahlen und von diesem folglich als legitime Gründe anerkannt werden. Ob eine gesetzliche Beschränkung von Manipulationen des öffentlichen Informationsraums und deren Vollzug dem Verhältnismäßigkeitsprinzip genügt, muss sodann gesondert für den jeweiligen Einzelfall untersucht und festgestellt werden. Dabei ist allerdings in Rechnung zu stellen, dass falsche Tatsachenbehauptungen, so sie nicht ohnehin vom Schutz der Kommunikationsfreiheiten ausgeklammert sind, im Regelfall einen geringeren Grundrechtsschutz genießen als der Schutz des öffentlichen Kommunikationsprozesses. Auch ist zu berücksichtigen, dass technische Manipulationen, die darauf abzielen, den Kommunikationsprozess in täuschender Absicht zu manipulieren und zu verzerren, ebenfalls im Regelfall als nicht schutzwürdig erscheinen; sie konterkarieren das durch die Kommunikationsgrundrechte geschützte Bestreben eines gleichberechtigten und offenen Ringens um das bessere Argument.¹⁸¹ Vielmehr ist von einer Gewährleistungspflicht des Gesetzgebers für den freien Meinungsbildungsprozess auszugehen, welche ihn auch dazu verpflichtet, diesen Prozess vor Verfälschungen, Verzerrungen und Verschleierungen zu bewahren.¹⁸² Art. 10 Abs. 2 Hs. 1 EMRK hebt diesen Aspekt der Kommunikationsfreiheiten explizit hervor, wenn er einleitend zum Schrankenvorbehalt die „Pflichten und Verantwortung“ einer Grundrechtsausübung betont.

(2) Absolute Schranken-Schranke (Zensurverbot)

Das Zensurverbot des Grundgesetzes (Art. 5 Abs. 1 S. 3 GG¹⁸³) stellt eine absolute Schranken-Schranke für hoheitliche Beeinträchtigungen der Kommunikationsfreiheiten dar. Das Grundgesetz folgt dabei einem engen Zensurbegriff. Es versteht unter Zensur lediglich die formelle staatliche Vorzensur in Gestalt eines präventiven Verfahrens der Inhaltskontrolle, von dessen Ausgang die Erlaubnis zur Verbreitung eines bestimmten Inhalts (Meinungsäußerung, journalistisch-redaktionelle Beiträge etc.) abhängt.¹⁸⁴ Adressat dieses Zensurverbots ist einerseits die Hoheitsgewalt, andererseits der Private (wie beispielsweise eine Plattform), soweit sein Handeln dem Staat – etwa durch gesetzlich auferlegte Pflichten – zuzurechnen ist. Darüber hinaus vermag das Zensurverbot eine abwägungsoffene Ausstrahlwirkung zu entfalten, soweit es um Maßnahmen geht, die zwar keine Zensur im vorbeschriebenen Sinne darstellen, dieser aber in ihrer Wirkung (Unterdrückung von meinungsbildenden Beiträgen) ähneln.¹⁸⁵

Das Recht der Europäischen Union kennt zwar kein explizites Zensurverbot. Dennoch stellt eine formelle staatliche Vorzensur auch im Unionsrecht einen Verstoß gegen den Wesensgehalt¹⁸⁶

181 Vgl. hierzu bereits oben bei Fn. 163.

182 So mit Recht Ferreau, AfP 2021, 204 (205, Rn. 7), der allerdings bemängelt, dass diese Pflicht bislang nur bereichsspezifisch (etwa für den Rundfunk) ausgeformt worden sei. Nimmt man jedoch die mittlerweile zahlreichen Regelungen auf unionaler (DSA) und nationaler Ebene (§§ 91 ff. MStV) in den Blick (dazu noch nachstehend § 2 D. I.), dürfte diese aus dem Jahre 2021 stammende Einschätzung zumindest graduell an Gültigkeit verloren haben.

183 Die Bestimmung lautet: „Eine Zensur findet nicht statt.“

184 Vgl. BVerfGE 33, 52 (72); Bethge, in: Sachs, GG, Art. 5 Rn. 131.

185 Ausführlich zu Letzterem Schmidt, Uploadfilter, S. 180 f.

186 Vgl. erneut Art. 52 Abs. 1 EUGRC.

der Kommunikationsfreiheiten dar und ist deshalb unzulässig. Dementsprechend ist das Zensurverbot als allgemeiner Grundsatz des Unionsrechts anzusehen. Eine entsprechende Wertung ergibt sich auch aus dem Vergleich der Verfassungsüberlieferungen der Mitgliedstaaten, die bei- nahe ausnahmslos ein präventives staatliches Verfahren der Inhaltskontrolle verbieten. Zudem findet dieses Verbot im Wortlaut des Art. 11 Abs. 1 S. 2 EUGRC („ohne behördliche Eingriffe“) einen Anklang.¹⁸⁷

Für den vorliegenden Untersuchungsgegenstand folgt hieraus, dass das absolut wirkende Zensurverbot keine oder eine nur marginale Rolle im Kampf gegen Manipulationen des öffent- lichen Informationsraums spielt. Soweit hoheitliche Maßnahmen gegenüber den unmittelbar Handelnden oder gegenüber Online-Plattformen darauf abzielen, einer technischen Manipulation (CIB, Verschleierung des Absenders) entgegenzuwirken, richten sich diese Maßnahmen lediglich gegen die Art und Weise, nicht aber gegen den Inhalt dieser Kommunikation.

Aber auch in ihrer abwägungsoffenen Ausstrahlungswirkung kommt dem Zensurverbot mit Blick auf hoheitliche Maßnahmen keine Relevanz zu, da diese gerade darauf abzielen, den Kommuni- kationsprozess offen und vielfältig zu gestalten. Manipulative Vorgehensweisen genießen dem- gegenüber keinen hervorzuhebenden Grundrechtsschutz. Soweit sich hoheitliche Maßnahmen gegen inhaltliche Manipulationen des öffentlichen Informationsraums (in Gestalt von Desinfor- mation oder Propaganda) wenden, ist daran zu erinnern, dass diese Verhaltensweisen im Regel- fall nicht unter den personellen oder materiellen Schutzbereich der Kommunikationsfreiheiten fallen. Maßnahmen gegen entsprechende Mediendienstanbieter können deshalb ebenfalls *a limine* nicht als Zensur qualifiziert werden.

3. ZWISCHENFAZIT

Als Fazit für die grundrechtlichen Grenzen der Bekämpfung von Manipulationen des öffentlichen Informationsraums lässt sich deshalb festhalten, dass ein großer normativer Gleichlauf der Grundrechtsregime im Mehrebenensystem besteht. Dies betrifft schon die Frage, ob der Schutz- bereich eines Kommunikationsgrundrechts überhaupt eröffnet ist; jedenfalls aber bezieht sich dieser Gleichlauf auf den effektiven Gewährleistungsgehalt dieser Grundrechte. Mit grundrecht- lichen Wertungskonflikten in Bezug auf hoheitliche Maßnahmen zur Bekämpfung von Manipu- lationen des öffentlichen Informationsraums ist deshalb nicht zu rechnen.

Die Untersuchung hat des Weiteren gezeigt, dass sowohl nach dem nationalen als auch nach dem europäischen Grundrechtsschutz manipulative Verhaltensweisen im hier verstandenen Sinne zumeist keinen Schutz durch die Kommunikationsgrundrechte erfahren. Entweder fehlt es an der Eröffnung des personellen Schutzbereichs, da grundrechtlich nicht geschützte staatliche oder staatlich gelenkte Akteure am Werke sind. Oder der materielle Schutzbereich lässt sich nicht auf manipulative Verhaltensweisen erstrecken, so wie im Fall von Desinformation.

¹⁸⁷ Ausführlich zur Herleitung und Reichweite des unionalen Zensurverbots Schmidt, Uploadfilter, S. 184 ff.

Dort, wo manipulative Maßnahmen ausnahmsweise Schutz genießen, verbleiben dem nationalen und unionalen Gesetzgeber bei ihrer Bekämpfung große Gestaltungsspielräume. Der Schutz eines offenen, unverzerrten Kommunikationsprozesses rechtfertigt weitreichende Einschränkungen.

Diese sind im Wesentlichen nur dem Verhältnismäßigkeitsprinzip unterworfen. Ob diese Schranken-Schranke beachtet wird, bedarf indes einer Betrachtung des Einzelfalls.

D. STATUS QUO DES REAKTIONSGEFÜGES ZUR BEKÄMPFUNG VON MANIPULATIONEN DES ÖFFENTLICHEN KOMMUNIKATIONSRAUMS

Im Lichte dieser rahmenrechtlichen Einordnung es das Ziel der weiteren Untersuchung, den Status quo des derzeitigen Reaktionsgefüges zur Bekämpfung von Manipulationen des öffentlichen Informationsraums zu beschreiben und zu analysieren. Diese Analyse bildet zugleich die Grundlage für eine Identifikation möglicher regulatorischer Defizite (E.) sowie neuer Lösungsansätze (F.).

Entsprechend der oben dargelegten Reichweite des Untersuchungsgegenstands (§ 1 A.) ist diese Status-quo-Analyse umfassend angelegt. In vertikaler Hinsicht erstreckt sie sich auf alle Regelungsebenen (EU, Bund, Länder), in horizontaler Hinsicht auf legislative (I.) und exekutive Maßnahmen (II.). Am Schluss sollen die gefundenen Ergebnisse auf die herausgearbeiteten Fallstudien (§ 2 B.) angewandt werden (III.).

I. LEGISLATIVER STATUS QUO

Das Recht beinhaltet ein Reaktionsgefüge zum Kampf gegen Manipulationen des öffentlichen Informationsraums sowohl auf unionaler (1.) als auch auf nationaler Ebene (2.). Insoweit einschlägige Normen finden sich in allen Teilrechtsgebieten (Öffentliches Recht, Strafrecht und Zivilrecht) und weisen dementsprechend einen präventiven oder repressiven Charakter auf.

1. UNIONALES RECHT

A) DIGITAL SERVICES ACT

Eine der wichtigsten Rechtsquellen zur Bekämpfung von Manipulationen des öffentlichen Informationsraums ist der DSA. Die Verordnung aus dem Jahre 2022 gilt für Vermittlungsdienste, über die – wie beschrieben (§ 2 B.) – die Mehrzahl solcher Manipulationen erfolgt.

Die Verordnung beinhaltet unionsweit harmonisierte sowie auf unterschiedliche Vermittlungsdienste abgestimmte Regelungen, durch die für Nutzer ein sicheres und vertrauenswürdiges Online-Umfeld geschaffen werden soll.¹⁸⁸

aa) Anwendbarkeit auf Online-Plattformen

Art. 3 lit. g) DSA definiert Vermittlungsdienste als eine Dienstleistung der Informationsgesellschaft¹⁸⁹, die in einer „reinen Durchleitung“ (Access Provider), einer „Caching“-Leistung (Caching Provider) oder einen „Hosting“-Dienst (Host Provider) besteht. Für den hier interessierenden Untersuchungsgegenstand sind vor allem letztere von Relevanz. Laut der Definitionsnorm in Art. 3 lit. g) iii) DSA besteht ihr Dienst darin, von einem Nutzer bereitgestellte Informationen in dessen Auftrag zu speichern. Da diese von Dritten bereitgestellten Informationen auf den Kommunikationsraum einwirken sollen, werden sie im Regelfall öffentlich verbreitet. Diese Form des Host Providers qualifiziert Art. 3 lit. i) DSA als „Online-Plattform“. Für sie gelten strengere Anforderungen als für einen nicht auf die öffentliche Verbreitung von Informationen ausgerichteten Vermittlungsdienst wie etwa ein reiner Cloud Service. Die nachstehende Analyse des DSA fokussiert sich deshalb auf die für Online-Plattformen geltenden Regelungen.¹⁹⁰

bb) Haftung der Online-Plattformen

Gemäß Art. 4 bis 10 DSA unterfallen Vermittlungsdienste unter Einschluss der Online-Plattformen bestimmten Haftungsregelungen und -privilegierungen. Für diese gilt Art. 6 DSA, der Online-Plattformen unter bestimmten Voraussetzungen von einer Haftung freistellt. So haftet die Plattform nicht für die im Auftrag der Nutzer gespeicherten und verbreiteten Informationen, wenn die Plattform keine tatsächliche Kenntnis von der rechtswidrigen Tätigkeit oder den rechtswidrigen Inhalten hat (Art. 6 Abs. 1 lit. a) DSA) oder sobald der Host Provider ab Kenntniserlangung zügig tätig wird, um den Zugang zu den rechtswidrigen Inhalten zu sperren oder diese zu entfernen (Art. 6 Abs. 1 lit. b) DSA).¹⁹¹ Von diesem sog. „Notice-and-take-Action-Prinzip“

¹⁸⁸ Vgl. Art. 1 Abs. 1 und 2 DSA.

¹⁸⁹ Gem. Art. 3 lit. a) DSA handelt es sich hierbei um einen Dienst i.S.d. Art. 1 Abs. 1 lit. b) der RL (EU) 2015/1535, d.h. um eine i.d.R. gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung. Diese Voraussetzung trifft auf die hier relevanten Online-Plattformen zu.

¹⁹⁰ Laut Kuhlmann/Trute, GSZ 2022, 115 gehören zu diesen Hosting-Diensten auch offen zugängliche Messengerdienste (Kanäle) wie Signal, Telegram und WhatsApp.

¹⁹¹ Infolge einer neuen Entscheidung des EuGH zum österreichischen Russmedia-Konzern könnte sich eine Verantwortlichkeit der Plattform für gehostete Informationen auch ohne Kenntniserlangung indes aus dem Datenschutzrecht (Art. 26 DSGVO) ergeben. Dies setzt freilich das Hosting personenbezogener Daten voraus, an denen es im vorliegenden

lässt Art. 6 Abs. 4 DSA ausdrücklich die Möglichkeit unberührt, dass eine Justiz- oder Verwaltungsbehörde nach dem Rechtssystem eines Mitgliedstaats vom Hosting-Dienst auf der Grundlage des geltenden Unionsrechts oder des nationalen Rechts im Einklang mit dem Unionsrecht verlangt, eine Zuwiderhandlung abzustellen oder zu verhindern. Prozedurale Einzelheiten hierzu regelt Art. 9 DSA.

Freiwillige Maßnahmen der Online-Plattformen (etwa in Gestalt KI-basierter Filter) zur Erkennung, Entfernung oder Sperrung rechtswidriger Inhalte führen nicht zu einem Verlust des Haftungsprivilegs (Art. 7 DSA¹⁹²). Zudem obliegt den Plattformen keine allgemeine Verpflichtung zur Überwachung der ihnen übermittelten Informationen oder zu einer aktiven Nachforschung nach rechtswidrigen Tätigkeiten (Art. 8 DSA). Die Bestimmung ist nicht nur auf Informationen und Inhalte (wie z. B. strafbare Äußerungen) bezogen¹⁹³, sondern bezieht sich allgemein auf Tätigkeiten rechtswidriger Art. Hierunter können insbesondere technische Manipulationen des öffentlichen Informationsraums (CIB, Verschleierung des Absenders) fallen, sofern diese Verhaltensweisen als rechtswidrig zu erachten sind.

cc) Sorgfaltspflichten der Online-Plattformen

Kapitel III des DSA ist den Sorgfaltspflichten der Vermittlungsdienste unter Einschluss der Online-Plattformen gewidmet. Es bildet den Schwerpunkt der Verordnung.

(1) Allgemeine Geschäftsbedingungen (Art. 14 DSA)

Art. 14 DSA statuiert eine für alle Arten von Vermittlungsdiensten geltende Bestimmung zur Verwendung Allgemeiner Geschäftsbedingungen (AGB). Nach seinem Abs. 1 S. 1 müssen die Anbieter von Vermittlungsdiensten in ihren AGB Angaben zu etwaigen Beschränkungen in Bezug auf die von den Nutzern bereitgestellten Informationen machen. Diese Beschränkungen können sowohl einen inhaltlichen als auch einen technischen Ursprung haben: So machen Online-Plattformen ihren Nutzern in Gestalt von Gemeinschaftsstandards (Community Standards) Vorgaben zu erlaubten und nicht-erlaubten Inhalten.¹⁹⁴ Auch können diese Standards Verhaltensweisen untersagen, die als Manipulation des öffentlichen Informationsraums zu qualifizieren sind.¹⁹⁵

Die untersagten Verhaltensweisen müssen dabei nicht die Schwelle einer gesetzlich definierten Rechtswidrigkeit überschreiten. Vielmehr ist es den Plattformen als Ausdruck ihrer grundrecht-

Kontext der Manipulation des öffentlichen Kommunikationsraums nicht selten fehlen dürfte; vgl. insoweit EuGH, Urt. v. 2.12.2025, C-492/23 = NJW 2026, 893 ff.

192 Köhler, in: Müller-Terpitz/Köhler, DSA, Art. 7 Rn. 2 m.w.N. qualifiziert diese Norm als „Gutes-Samariter-Privileg“.

193 Der DSA verwendet die Begriffe der Information und der Inhalte synonym; vgl. nur Art. 3 lit. h) DSA, wo rechtswidrige Inhalte als „alle Informationen“ definiert werden.

194 Vgl. hierzu etwa die Vorgaben von Meta, das hasserfüllte Äußerungen auf seinen Plattformen (Facebook, Instagram, WhatsApp) untersagt und sich Maßnahmen gegen Fehlinformationen vorbehält. Aktuelles Bsp. aus der Rspr.: OLG Frankfurt a.M., ZUM 2025, 361 ff. zur rechtmäßigen Löschung ungesicherter Tatsachenäußerungen über die angeblich fehlende Wirksamkeit und die Gefährlichkeit von Impfstoffen, die gegen die AGB-rechtlichen Kommunikationsstandards der Plattform, nicht aber gegen geltendes Recht verstießen.

195 Vgl. erneut die Vorgaben von Meta, die CIB und Identitätstäuschungen verbieten. DSA ErwG Nr. 5 und 68 sprechen in diesem Zusammenhang von „anderweitig schädlichen Informationen und Tätigkeiten“.

lich geschützten unternehmerischen Betätigungsfreiheit (Art. 16 EUGRC)¹⁹⁶ prinzipiell gestattet, über ihr AGB-Recht derartige Verhaltensweisen auch unterhalb dieser Schwelle zu verbieten

Art. 14 Abs. 4 DSA ergänzt diese Regelung dahingehend, dass die Anbieter von Vermittlungsdiensten bei der Anwendung und Durchsetzung der in Abs. 1 genannten Beschränkungen sorgfältig, objektiv und verhältnismäßig vorgehen und dabei die Rechte und berechtigten Interessen aller Beteiligten sowie die Grundrechte der Nutzer (wie insbesondere das Recht auf freie Meinungsäußerung, die Freiheit und den Pluralismus der Medien) berücksichtigen müssen. Die Regelung ist Ausdruck einer mittelbaren Drittwirkung von Grundrechten, die über die Anwendung und Durchsetzung der AGB letztlich auch Rückwirkungen auf deren Gestaltung zu entfalten vermag.¹⁹⁷ Im Extremfall könnte sich daraus deshalb eine Pflicht der Online-Plattformen zum Einschreiten gegen Manipulationen des öffentlichen Informationsraums ergeben, wenn nur dadurch der Pluralismus und die Offenheit des Kommunikationsprozesses gewährleistet zu werden vermag. Einen normativen Anknüpfungspunkt hierfür bieten die Risikobewertung und Risikominderung nach Art. 34 und 35 DSA.¹⁹⁸

(2) Melde- und Abhilfeverfahren (Art. 16 DSA)

Gemäß Art. 16 Abs. 1 DSA müssen Hosting-Dienste unter Einschluss von Online-Plattformen Verfahren bereitstellen, mit denen ihnen Personen oder Einrichtungen (wie z. B. Vereine oder Stiftungen) Einzelinformationen melden können, die die Meldenden als rechtswidrig ansehen. Unter „rechtswidrigen Informationen“ versteht der DSA Inhalte, die als solche oder durch ihre Bezugnahme auf eine Tätigkeit nicht im Einklang mit dem Unionsrecht oder dem Recht eines Mitgliedstaats stehen, ungeachtet des genauen Gegenstands oder der Art der betreffenden Rechtsvorschriften (Art. 3 lit. h) DSA). Es geht mithin um Verstöße gegen gesetzliche Regelungen und nicht bloß um Verstöße gegen die vertraglichen Vereinbarungen der Plattformen i.S.d. Art. 14 Abs. 1 DSA. Durch eine solche Meldung erlangt die Plattform Kenntnis i.S.d. Art. 6 Abs. 1 DSA, was das „Notice-And-Take-Action“-Verfahren in Gang setzt.¹⁹⁹

Soweit die gemeldeten Inhalte rechtswidrig sind, also gegen Gesetze verstoßen²⁰⁰, muss der Hosting-Dienst gemäß Art. 16 Abs. 6 DSA zeitnah, sorgfältig, frei von Willkür und objektiv über das weitere Vorgehen entscheiden. Die Vorschrift ergänzt mithin die bereits aus Art. 6 Abs. 1 DSA fließende Verpflichtung zum Tätigwerden ab Kenntniserlangung. Der Begriff der Information ist dabei weit zu verstehen und umfasst neben Inhalten (wie Äußerungen oder journalistisch-gestalteten Beiträgen) auch solche über bestimmte Verhaltensweisen (wie z. B. über ein ClB oder die Verschleierung eines Absenders).

Art. 16 Abs. 1 DSA verpflichtet allerdings nicht zur Einrichtung eines Verfahrens zur Meldung von Verstößen gegen die Nutzer-AGB (Gemeinschaftsstandards). AGB-rechtliche Verbote nicht-

196 S. dazu bereits oben § 2 C. II. 2. b) bb) (1).

197 In diese Richtung ebenfalls Barudi, in: Müller-Terpitz/Köhler, DSA, Art. 14 Rn. 23.

198 S. dazu noch nachfolgend § 2 D. I. 1. a) cc) (10).

199 S. dazu bereits oben § 2 D. I. 1. a) bb).

200 Zu den in Betracht kommenden Gesetzesverstößen noch unten § 2 D. I. 2.

rechtswidriger Inhalte (hasserfüllte Sprache, Desinformation, Propaganda etc.) oder nicht-rechtswidriger technischer Manipulationen des öffentlichen Informationsraums gehören deshalb nicht zum Kreis der nach Art. 16 Abs. 1 DSA meldefähigen Informationen. Die Meldung derartiger Inhalte und Verhaltensweisen kann von den Plattformen allerdings auf freiwilliger Basis ermöglicht werden.²⁰¹

Eine Handhabe gegen Personen oder Institutionen, die Meldeverfahren dazu missbrauchen, um andere Nutzer in Misskredit zu bringen oder die Arbeit der Plattformen durch Überlastung („Overload“) zu konterkarieren bietet Art. 23 Abs. 2 DSA. Hiernach dürfen die Anbieter von Online-Plattformen „die Bearbeitung von Meldungen und Beschwerden, die über die in den Artikeln 16 und 20 genannten Melde- und Abhilfeverfahren bzw. über interne Beschwerdemanagementsysteme von Personen oder Stellen oder von Beschwerdeführern eingehen, die häufig offensichtlich unbegründete Meldungen oder Beschwerden einreichen, für einen angemessenen Zeitraum nach vorheriger Warnung aus(setzen)“. Solche Verhaltensweisen können zudem AGB-rechtlich untersagt und verfahrensrechtlich näher ausgestaltet sein.²⁰²

(3) Meldung von Straftaten (Art. 18 DSA)

Gemäß Art. 18 Abs. 1 DSA müssen Hosting-Dienste, die „Kenntnis von Informationen erhalten, die den Verdacht begründen, dass eine Straftat, die eine Gefahr für das Leben oder die Sicherheit einer Person oder von Personen darstellt, begangen wurde, begangen wird oder begangen werden könnte“, diesen Verdacht unverzüglich den jeweils zuständigen Strafverfolgungs- oder Justizbehörden mitteilen.

Im zu untersuchenden Kontext dürfte diese Verpflichtung von eher untergeordneter Bedeutung sein. Es ist aber nicht auszuschließen, dass Manipulationen des öffentlichen Informationsraums – etwa in Gestalt einer durch CIB verstärkten Verbreitung von Desinformation über eine bestimmte Person – zu einer Gefahr für deren körperliche Unversehrtheit oder Sicherheit werden könnte. Dies ist eine Frage des Einzelfalls.

(4) Internes Beschwerdemanagementsystem und außergerichtliche Streitbeilegung (Art. 20 und 21 DSA)

Art. 20 und 21 DSA enthalten Regelungen, die sich speziell an Hosting-Dienste in Gestalt von Online-Plattformen richten. Diese müssen den Nutzern sowie den meldenden Personen und Einrichtungen i.S.d. Art. 16 Abs. 1 DSA für mindestens sechs Monate Zugang zu einem wirksamen internen Beschwerdemanagementsystem gewähren (Art. 20 DSA). Zudem müssen sie diesem Personenkreis die Möglichkeit eröffnen, eine zertifizierte außergerichtliche, nicht bindende

201 So i. Erg. auch Barudi, in: Müller-Terpitz/Köhler, DSA, Art. 16 Rn. 12, dem zufolge das vorzuhaltende Verfahren für die Meldung bloßer Verstöße gegen die AGB des Hosting-Dienstes vorgehalten werden „kann“, aber nicht vorgehalten werden „muss“.

202 Vgl. Meta-Nutzungsbedingungen v. 1.1.2025, Nr. 3.2. Ziff. 6, abrufbar über: https://www.facebook.com/terms/?locale=de_DE (letzter Abruf: 30.4.2026).

Streitbeilegungsstelle anzurufen (Art. 21 DSA). Wird also ein Nutzer aufgrund von Manipulationen des öffentlichen Informationsraums zum Adressaten einer plattformseitigen Überprüfung seines Handelns, kann er gegen die hierzu getroffene Entscheidung intern Beschwerde einlegen und – soweit aus seiner Sicht erforderlich – sodann eine außergerichtliche Streitbeilegung in Anspruch nehmen. Dieselben Möglichkeiten stehen den meldenden Personen oder Einrichtungen zu. Interessant an dieser Bestimmung ist, dass sie eine interne und externe Streitbeilegung auch in Bezug Verstöße gegen die Plattform-AGB ermöglicht, obschon diese nach Art. 16 Abs. 1 DSA nicht meldefähig sind.

(5) Vertrauenswürdige Hinweisgeber (Art. 22 DSA)

Die Anbieter von Online-Plattformen sind gemäß Art. 22 DSA des Weiteren dazu verpflichtet, Maßnahmen zu ergreifen, um Meldungen, die durch vertrauenswürdige Hinweisgeber („Trusted Flagger“) erfolgen, vorrangig zu behandeln und unverzüglich zu bearbeiten. Die Regelung nimmt insoweit auf Art. 16 DSA Bezug und beschränkt ihren Anwendungsbereich entsprechend auf rechtswidrige Inhalte. Meldungen von Verstößen gegen die Gemeinschaftsstandards der Plattformen werden durch Art. 22 DSA mithin nicht privilegiert.²⁰³

Der Status eines vertrauenswürdigen Hinweisgebers wird unter den in Art. 22 Abs. 2 DSA genannten Voraussetzungen (Sachkenntnis, Unabhängigkeit Sorgfalt und Objektivität) auf Antrag durch den Koordinator für digitale Dienste (Digital Services Coordinator – DSC) verliehen.²⁰⁴ Eine Organisation, die sich speziell gegen Desinformation im Netz richtet (wie etwa *Correctiv*), ist mangels Antrags noch nicht als vertrauenswürdiger Hinweisgeber eingestuft.

(6) Missbräuchliche Verwendung (Art. 23 DSA)

Nach Art. 23 Abs. 1 DSA sind Online-Plattformen zudem verpflichtet, die Erbringung ihrer Dienste für Nutzer, die häufig und offensichtlich rechtswidrige Inhalte bereitstellen, für einen angemessenen Zeitraum nach vorheriger Warnung auszusetzen.

Die Regelung bezieht sich abermals nur auf rechtswidrige Inhalte und nicht auf reine Verstöße gegen die Gemeinschaftsstandards der Online-Plattformen. Dennoch könnte diese Regelung auch auf solche Nutzer zur Anwendung kommen, die in rechtswidriger Weise den öffentlichen Informationsraum manipulieren, etwa durch die Nutzung falscher Identitäten.

(7) Gestaltung und Organisation der Online-Schnittstelle (Art. 25 DSA)

Eine für die Bekämpfung von Manipulationen des öffentlichen Kommunikationsraums interessante Bestimmung beinhaltet ferner Art. 25 DSA. Nach dieser Regelung dürfen „Anbieter von

²⁰³ So auch Raue, in: Hofmann/Raue, DSA, Art. 22 Rn. 16.

²⁰⁴ Eine Liste der bislang anerkannten vier Institutionen findet sich unter https://www.dsc.bund.de/DE/Fachthemen/DSC/1_Themen/TrustedFlagger/start.html (letzter Abruf: 30.4.2026).

Online-Plattformen (...) ihre Online-Schnittstellen nicht so konzipieren, organisieren oder betreiben, dass Nutzer getäuscht, manipuliert oder anderweitig in ihrer Fähigkeit, freie und informierte Entscheidungen zu treffen, maßgeblich beeinträchtigt oder behindert werden.“ Unter einer Online-Schnittstelle versteht Art. 3 lit. m) DSA „eine Software, darunter auch Websites oder Teile davon sowie Anwendungen, einschließlich Mobil-Apps“.

U. a. auf der Grundlage dieser Bestimmung ist von der Kommission erst unlängst (und erstmalig) eine Geldbuße in Höhe von 120 Mio € gegen die Online-Plattform X verhängt worden.²⁰⁵ Grund hierfür ist Xs Verwendung des „blauen Häkchens“ für „verifizierte Konten“, in der die Kommission eine Täuschung der Nutzer sieht. Denn – so die Kommission – auf X könne jeder bezahlen, um den Status „verifiziert“ zu erhalten, ohne dass die Plattform wirklich überprüfe, wer hinter dem Konto stecke. Dies erschwere es den Nutzern, die Authentizität der Konten und Inhalte, mit denen sie interagierten, zu beurteilen. Diese Täuschung setze Nutzer u. a. der Gefahr von Imitationen („Doppelgänger“) sowie anderen Formen der Manipulation durch böswillige Akteure (Konten mit automatisierten Inhalten in Form von Beiträgen, Kommentaren oder Likes) aus. Zwar schreibe der DSA keine Nutzerverifizierung vor; er verbiete es Online-Plattformen allerdings, fälschlicherweise zu behaupten, Nutzer seien verifiziert worden, ohne dass eine solche Verifizierung tatsächlich stattgefunden habe.²⁰⁶ Es handelt sich hierbei mithin um eine Kommissionsmaßnahme, die technischen Manipulationen i.S.d. Untersuchungsgegenstands entgegenwirken soll.

(8) Transparenz der Empfehlungssysteme (Art. 27 DSA)

Art. 27 DSA verpflichtet Online-Plattformen dazu, über die wichtigsten Parameter der Wirkweise der von ihnen verwendeten Empfehlungssystemen²⁰⁷ einschließlich der Möglichkeiten für die Nutzer, diese Parameter zu ändern oder zu beeinflussen, in ihren AGB aufzuklären. Für den Einsatz solcher Empfehlungsalgorithmen konkretisiert die Bestimmung die nach Art. 14 Abs. 1 DSA zu leistenden Angaben.²⁰⁸ Die verordnungsrechtlich vorgeschriebene Transparenz kann von Nutzern dazu genutzt werden, Schutzmaßnahmen gegen Manipulationen des öffentlichen Informationsraums zu ergreifen. Sie kann solche Manipulationen allerdings auch erleichtern.

(9) Online-Schutz Minderjähriger (Art. 28 DSA)

Auch Art. 28 DSA kommt für den Untersuchungsgegenstand Bedeutung zu. Nach dieser Regelung müssen Anbieter von Online-Plattformen, die für Minderjährige zugänglich sind, geeignete und verhältnismäßige Maßnahmen ergreifen, um insbesondere für ein hohes Maß an Sicherheit

205 S. Pressemitteilung der Kommission v. 5.12.2025, abrufbar unter: <https://digital-strategy.ec.europa.eu/en/news/commission-fines-x-eu120-million-under-digital-services-act> (letzter Abruf: 30.4.2026).

206 Pressemitteilung der Kommission v. 5.12.2025, wie vor.

207 Der Begriff „Empfehlungssystem“ wird von Art. 3 lit. s) DSA definiert als „ein vollständig oder teilweise automatisiertes System, das von einer Online-Plattform verwendet wird, um auf ihrer Online-Schnittstelle den Nutzern bestimmte Informationen vorzuschlagen oder diese Informationen zu priorisieren, auch infolge einer vom Nutzer veranlassten Suche, oder das auf andere Weise die relative Reihenfolge oder Hervorhebung der angezeigten Informationen bestimmt“.

208 S. dazu bereits oben § 2 D. I. 1. a) cc) (1).

und Schutz der Minderjährigen innerhalb ihres Dienstes zu sorgen.

Solche Maßnahmen können sich auch gegen Manipulationen des öffentlichen Informationsraums richten. Denn durch manipulierte Reichweiten oder Verschleierungstaktiken, über die Desinformation oder Propaganda speziell an Minderjährige verbreitet werden, kann deren grundrechtlich geschützte Persönlichkeitsentwicklung erheblich beeinträchtigt werden.²⁰⁹ Die Leitlinien der Kommission für Maßnahmen zur Gewährleistung eines hohen Maßes an Privatsphäre, Sicherheit und Schutz von Minderjährigen im Internet gemäß Art. 28 Abs. 4 der Verordnung (EU) 2022/2065 vom 10. Oktober 2025²¹⁰ enthalten hierzu erste Ansätze. So schreiben sie unter Ziff. 6.3.1. lt. b) vii) unter der Überschrift „Kontoeinstellungen“ zum Thema „Standardeinstellungen“ vor, dass wenn ein minderjährige Nutzer „willentlich Push-Benachrichtigungen aktiviert, (...) diese den Nutzer nur über Interaktionen informieren (sollten), die sich aus den direkten Kontakten des Nutzers und aus Inhalten von Konten oder Kanälen ergeben, denen der Nutzer aktiv folgt oder mit denen er interagiert (z. B. sollten Push-Benachrichtigungen niemals unauthentisch sein und stets die genaue Angabe des Nutzers oder Erstellers enthalten, von dem die Benachrichtigung kommt).“²¹¹ Hierin kann eine Schutzmaßnahme sowohl vor CIB als auch vor einer Verschleierung des Absenders gesehen werden.

(10) Risikobewertung und Risikominderung (Art. 34 und 35 DSA)

Einen besonders wichtigen Ansatzpunkt zur Bekämpfung von Manipulationen des öffentlichen Informationsraums bieten die Art. 34 und 35 DSA. Diese verpflichten VLOPs und sehr große Online-Suchmaschinen (VLOSEs)²¹² zu Maßnahmen der Risikobewertung (Art. 34 DSA) und Risikominderung (Art. 35 DSA). Diese Maßnahmen können Überschneidungen zu den oben bereits vorgestellten Verpflichtungen (etwa zum Meldeverfahren oder zum Minderjährigenschutz) aufweisen.

Nach dem in den genannten Bestimmungen implementierten selbstregulatorischen Ansatz der Risikobewertung und Risikominderung haben VLOPs und VLOSEs mindestens einmal jährlich oder bei Einführung neuer, risikogeneigter Funktionen eine Bewertung systemischer Risiken durchzuführen. Diese Risikobewertung hat sich u. a. auf etwaige tatsächliche oder vorhersehbare Auswirkungen der Plattform-Dienste auf die in Art. 11 GRC verankerte Meinungs- und Informationsfreiheit einschließlich der Medienfreiheit und des Medienpluralismus sowie auf alle tatsächlichen oder absehbaren nachteiligen Auswirkungen auf gesellschaftliche Debatten, Wahlprozesse und die öffentliche Sicherheit (Art. 34 Abs. 1 lit. b) und c) DSA) zu erstrecken. Innerhalb dieses Bewertungsprozesses ist insbesondere die Gestaltung der algorithmischen Empfehlungssysteme (Art. 34 Abs. 2 lit. a) und Art. 35 Abs. 1 lit. d) DSA) und der anwendbaren AGB nebst

209 Für das nationale Recht folgt dieser Persönlichkeitsschutz aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, für das europäische Recht aus Art. 8 Abs. 1 EMRK sowie aus Art. 7 EUGRC. Einen Nexus zu diesen Grundrechten der Betroffenen stellt im Allgemeinen ebenfalls her bitkom, Policy Brief, S. 7.

210 ABl.EU C/2025/5519.

211 Hervorhebung nur hier.

212 Zur Definition und Festlegung dieser Diensteanbieter s. Art. 33 DSA. Hiernach handelt es sich bei VLOPs und VLOSEs um Online-Plattformen, die durchschnittlich von mindestens 45 Mio. aktiven Nutzern in der Union genutzt werden und von der Kommission als solche benannt wurden. Eine Liste der derzeit benannten VLOPs und VLOSEs findet sich unter <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses> (letzter Abruf: 30.4.2026). Der Begriff der Online-Suchmaschine wird durch Art. 3 lit. j) DSA definiert.

ihrer Durchsetzung (Art. 34 Abs. 2 lit. c) und Art. 35 Abs. 1 lit. b) DSA) zu berücksichtigen. Mit diesen Vorgaben verarbeitet der europäische Gesetzgeber die Erkenntnis, dass algorithmische Empfehlungssysteme zentralen Einfluss auf die Sichtbarkeit kommunikativer Inhalte haben. Plattformalgorithmen strukturieren im großen Stil digitale Kommunikationsprozesse. Wie Beobachtungen dieser Strukturierungsprozesse zeigen, bevorteilen Empfehlungsalgorithmen dabei die Verbreitung stark emotionalisierender oder skandalisierender Inhalte – auch, weil derartige Inhalte von Nutzern häufiger kommentiert, geteilt oder „gelikt“ werden. An diesem Punkt setzen automatisierte CIB-Prozesse an, indem sie algorithmische Effekte durch automatisiert erstellte Inhalte und Kommentare mit Skandalwirkung, automatisiertes Teilen oder Liken dazu nutzen, Kommunikationsprozesse zu manipulieren und durch Desinformation oder Propaganda zulasten sorgfältig recherchierter Informationen und rational begründeter Meinungen zu verzerren.²¹³

Einem solchen Mechanismus der „regulierten Selbstregulierung“ ist jedoch eine zurückgenommene normative Steuerungswirkung immanent. Denn primär überlässt er es den Plattformen, die Schwere und Wahrscheinlichkeit der systemischen Risiken ihrer algorithmischen Systeme für den unionsrechtlich geschützten Kommunikationsprozess zu bewerten. Auch obliegt es primär ihnen, adäquate Maßnahmen zur Minderung festgestellter Risiken zu ergreifen. Zudem bleiben die gesetzlich umschriebenen Voraussetzungen für eine Bewertung der Plattform-Risiken und darauf gestützte Abhilfemaßnahmen sehr abstrakt. Der Mechanismus entfaltet deshalb nur eine geringe normative Steuerungswirkung (i.S. einer konditionalen „Wenn-Dann-Logik“) und dürfte der Kommission deshalb nur bei offensichtlichen Verstößen die Anordnung konkreter Abhilfemaßnahmen gestatten.²¹⁴ Vor diesem Hintergrund ist es wahrscheinlicher, dass die Kommission im Verhandlungswege versuchen wird, von den Online-Plattformen kompromissbasierte Verpflichtungszusagen (Art. 71 DSA) zu erlangen.

Freilich wird diese normative Offenheit durch den Umstand moderiert, dass die Kommission in Zusammenarbeit mit den DSCs sowie nach Durchführung einer öffentlichen Konsultation (unverbindliche) Leitlinien zur Konkretisierung der Risikominderungsmaßnahmen erlassen kann (Art. 35 Abs. 3 DSA). Auch sollen die Kommission und das Europäische Gremium für digitale Dienste (Art. 61 DSA) die Ausarbeitung freiwilliger Verhaltenskodizes – wie etwa dem Verhaltenskodex zur Bekämpfung von Desinformation (der u. a. eine Demonetarisierung von Desinformation und Beschwerdemöglichkeit für Nutzer)²¹⁵ oder die im April 2024 erlassene EU-Kommissionsleitlinien für VLOPs und VLOSEs zur Minderung systemischer Risiken für Wahlprozesse („Election Guidelines“)²¹⁶ – befördern (Art. 45 Abs. 1 und 2 DSA). Diese Leitlinien identifizieren u. a. die Manipu-

213 I. Erg. ähnlich Kastor/Püschel, K&R 2023, 20 (21 ff.) mit dem zutreffenden Hinweis, dass Desinformation in Art. 34 f. DSA nicht explizit erwähnt, aber dennoch geregelt werde; Kuhlmann/Trute, GSZ 2022, 115 (119 f.), die zu Recht betonen, dass das Risikomanagementsystem der Art. 34 f. DSA nicht auf rechtswidrige Inhalte beschränkt ist.

214 Zu diesem Bild passt, dass die oben bei Fn. 205 erwähnte Geldbuße wegen eines Verstoßes gegen den konkreten gefassten Art. 25 DSA und nicht wegen eines Verstoßes gegen die Art. 34 f. DSA verhängt wurde. Für die rumänische Präsidentschaftswahl vom November 2024, die u. a. aufgrund des Vorwurfs einer Manipulation des öffentlichen Informationsraums über die Plattform TikTok annulliert wurde, hat die Kommission gegenüber dieser Plattform ein „Einfrieren“ der hierfür relevanten Plattformdaten angeordnet und kurze Zeit später ein Verfahren eröffnet. Eine Entscheidung in der Sache ist bislang jedoch nicht ergangen. Vgl. insoweit die Pressemitteilungen v. 5.12.2024 und 17.12.2024, abrufbar unter: <https://digital-strategy.ec.europa.eu/en/news/commission-online-platforms-and-civil-society-increase-monitoring-during-romanian-elections> und <https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-tiktok-election-risks-under-digital-services-act> (letzter Abruf: 30.4.2026).

215 Zu diesem etwa Mafi-Gudarzi, ZRP 2019, 65 (66).

216 Leitlinien der Kommission für Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen zur

lation von Informationen und die Einmischung aus dem Ausland (FIMI), die Verbreitung (gewalt) extremistischer Inhalte sowie die Verbreitung massenhafter illegaler Hetze als Erscheinungen, die ein erhöhtes Risiko für die Integrität von Wahlen bergen. Die Leitlinien enthalten u. a. folgende Empfehlungen für VLOPs und VLOSEs: Erleichterung des Zugangs zu amtlichen Informationen über den Wahlprozess für Nutzerinnen und Nutzer; Anpassung der Empfehlungssysteme, um die Nutzerinnen und Nutzer bei ihrer Suche nach seriöser Information zu unterstützen; Verringerung der Monetarisierung und Viralität von Inhalten; Sperrung von CIB-Konten, die die Integrität von Wahlprozessen gefährden könnten; klare Kennzeichnung politischer Werbung und Zusammenarbeit mit den nationalen (Wahl-)Behörden. Der selbstregulative Mechanismus wird so durch eine softlaw-basierte kooperativ-dialogische Facette ergänzt. An diesem Mechanismus beteiligen sich allerdings nicht alle Unternehmen; X beispielsweise ist dem Verhaltenskodex zur Bekämpfung von Desinformation nicht beigetreten. Und auch diese Leitlinien und Verhaltenskodizes leiden an dem vorstehend bereits hervorgehobenen Umstand, dass die Mechanismen zur Bewältigung von Systemrisiken sehr abstrakt formuliert und deshalb auf eine freiwillige Beachtung durch die jeweiligen Plattformen angewiesen sind.²¹⁷

Mangels hinreichender praktischer Erfahrungswerte bleibt vor diesem Hintergrund abzuwarten, welche Durchschlagskraft diesem koregulatorischen und kooperativen Risikomanagementsystem für die Bekämpfung von Manipulationen des öffentlichen Informationsraums zukommen wird. Es erscheint zwar prinzipiell geeignet, zu einer besseren Strukturierung des öffentlichen Kommunikations- und Meinungsbildungsprozesses beizutragen. Der bisherige praktische Vollzug dieses Instruments deutet jedoch an, dass es sich um einen eher schwerfälligen Mechanismus handelt. Soweit die Kommission gegen VLOPs Verfahren wegen DSA-Verstößen eröffnet hat, betrafen diese mehrheitlich nicht die Gestaltung der eingesetzten Empfehlungsalgorithmen, sondern Verstöße gegen ordnungsrechtliche Bestimmungen des DSA (wie z. B. Art. 25, 27, 39 oder 40 DSA). Zudem dauerten diese Verfahren allein für die vorläufige Feststellung von Verstößen zumeist bis zu zwei Jahren. Kommt es i.Ü. nicht zu einer einvernehmlichen Beendigung des Verfahrens²¹⁸, drohen weitere Verzögerung durch den Rechtsweg.

(11) Krisenreaktionsmechanismus (Art. 36 DSA)

Art. 36 DSA statuiert einen Krisenreaktionsmechanismus. Nach dieser Regelung kann die Kommission auf Empfehlung des Gremiums VLOPs und VLOSEs auffordern, eine Bewertung ihrer Plattformen mit Blick auf schwerwiegende Bedrohungen (Art. 36 Abs. 1 lit. a) DSA) sowie Maßnahmen zur Verhinderung oder Beseitigung dieser Bedrohungen (Art. 36 Abs. 1 lit. b) DSA) zu ergreifen. Unter einer schwerwiegenden Bedrohung versteht die Bestimmung eingetretene außergewöhnliche Umstände mit schwerwiegendem Bedrohungscharakter für die öffentliche Sicherheit und Gesundheit in der Union (Art. 36 Abs. 2 DSA).

Minderung systemischer Risiken in Wahlprozessen gemäß Art. 35 Abs. 3 der Verordnung (EU) 2022/2065, ABl.EU C/2024/3014 = EUR-Lex - 52024XC03014 - EN - EUR-Lex.

217 Zurückhaltend mit Blick auf die Wirksamkeit des Risikomanagementsystems wie hier auch Kuhlmann/Trute, GSZ 2022, 115 (120 f.) – „ohne Ausarbeitung weiterer Leitlinien (...) wenig operationabel“; ferner fehlten klare Maßgaben deren Bewertung zudem im Ermessen der profitorientierten Anbieter lägen; Schlömer/Kehrberg, ZRP 2025, 2 (4).

218 Erneut sei insoweit auf das Instrument der Verpflichtungszusage aus Art. 71 DAS hingewiesen.

Als solche außergewöhnlichen Umstände können auch Manipulationen des öffentlichen Informationsraums im Rahmen einer FIMI gelten, wenn diese darauf abzielen, die Union als Ganzes oder einzelne EU-Mitgliedstaaten zu destabilisieren.²¹⁹ Da die Regelung auf Art. 35 Abs. 1 DSA zurückverweist, gelten die vorstehenden Ausführungen ((10)) entsprechend.

(12) Zusätzliche Transparenz der Online-Werbung (Art. 39 DSA)

Art. 39 verpflichtet VLOPs und VLOSEs, die Werbung auf ihren Online-Schnittstellen (wie z. B. Webseiten oder Newsfeeds) anzeigen, bestimmte Angaben (wie insbesondere über den Werbeerhalt, den Beworbenen und den Sponsor) in einem Anzeigenarchiv („Ads Repository“) öffentlich zugänglich zu machen. Durch diese Transparenz und Zugänglichkeit sollen Wissenschaftler und Institutionen der Zivilgesellschaft u. a. in die Lage versetzt werden, hybride Desinformations- und Propagandakampagnen, koordinierte Informationsoperationen und gefälschte Werbung zu erkennen. Der Bestimmung kommt mithin Relevanz für den hiesigen Untersuchungsgegenstand zu.

Aufgrund von behindernden Designmerkmalen der Anzeigenarchivs, Zugriffsbarrieren und des Fehlens wichtiger Informationen hat die Kommission einen Verstoß von X gegen diese Regelung bejaht und das Unternehmen mit der bereits erwähnten Geldbuße in Höhe von 120 Mio. € belegt.²²⁰

(13) Datenzugang und Kontrolle (Art. 40 DSA)

Abschließend hervorzuheben ist Art. 40 Abs. 4 DSA, der eine Regelung zum Datenzugang und zur Kontrolle vorsieht. Nach dieser Bestimmung müssen VLOPs und VLOSEs Wissenschaftlern einen Datenzugang zu Forschungszwecken gewähren, der es u. a. ermöglichen könnte, Manipulationen des öffentlichen Informationsraums besser zu verstehen und insoweit Gegenmaßnahmen zu entwickeln.

Dieser Forschungsdatenzugang, der über den DSC am Niederlassungsort des Anbieters zu administrieren ist, verläuft in der Praxis schleppend. Erst unlängst hat die Kommission im Rahmen des bereits mehrfach erwähnten Geldbußverfahrens einen Verstoß des Anbieters X gegen diese verordnungsrechtliche Verpflichtung festgestellt. So verböten die Nutzungsbedingungen von X berechtigten Forschern, unabhängig auf öffentliche Daten – etwa durch das sog. „Scraping“²²¹ – zuzugreifen.

Darüber hinaus errichteten die Prozesse von X für den Zugang von Forschern zu öffentlichen Da-

219 So auch die Einschätzung von Kuhlmann/Trute, GSZ 2022, 115 (121), die die Regelung explizit in einen Zusammenhang mit Corona und dem Ukraine-Krieg stellen.

220 Pressemitteilung der Kommission v. 5.12.2025, abrufbar unter: <https://digital-strategy.ec.europa.eu/en/news/commission-fines-x-eu120-million-under-digital-services-act> (letzter Abruf: 30.4.2026).

221 = automatisiertes Auslesen, Extrahieren und Speichern von Webseiten-Daten mittels einer speziellen Software.

ten unnötige Barrieren, welche die Forschung zu systemischen Risiken effektiv untergraben.²²²

dd) Zwischenfazit

Die vorstehende Untersuchung hat gezeigt, dass der DSA zahlreiche rechtliche Anknüpfungspunkte für die Bekämpfung von Manipulationen des öffentlichen Informationsraums bereitstellt. Diese beziehen sich teils auf rechtswidrige Inhalte und Verhaltensweisen; teils erfassen sie aber – wie die AGB-Gestaltung oder das Risikomanagementsystem – auch Inhalte und Verhaltensweisen unterhalb der Rechtswidrigkeitsschwelle. Teils beinhalten die Regelungen klare ordnungsrechtliche Vorgaben (wie etwa die Pflicht zur Einrichtung eines Meldesystems oder zur Herstellung von Transparenz über die eingesetzten Empfehlungsalgorithmen), teils aber auch nur Vorgaben in Gestalt einer regulierten Selbstregulierung, um losgelöst von Einzelfällen abstrakt-generelle Lösungen für komplexe Risikoszenarien zu finden. Die Kommission hat bislang nur vereinzelt Verstöße gegen die skizzierten Vorgaben angenommen. Da der DSA aber erst seit knapp zwei Jahren in der Anwendung ist, darf mit weiterer Vollzugserfahrung (und darauf bezogener Judikatur) gerechnet werden.

B) EUROPEAN MEDIA FREEDOM ACT

Der EMFA statuiert Vorschriften für das Funktionieren von Mediendiensten (Art. 1 Abs. 1 EMFA), also für redaktionell verantwortete Inhalteanbieter gleich welcher Art (Art. 2 Ziff. 1 EMFA). Zu diesen Regelungen gehört Art. 18 EMFA, der VLOPs zu einem besonderen verfahrensrechtlichen Schutz von Public-Value-Mediendienstanbietern verpflichtet. Hierdurch soll sichergestellt werden, dass die Sichtbarkeit solcher Medien nicht vorschnell und ohne faires Verfahren eingeschränkt werden kann. Auch dies stellt eine Maßnahme zur Bekämpfung von Manipulationen des öffentlichen Informationsraums dar, da die erhöhten verfahrensrechtlichen Hürden zum Schutz von Public-Value-Inhalten einen Beitrag zum Kampf gegen Desinformation und Propaganda zu leisten vermag. Mangels Erfahrungswerte bleibt die Wirksamkeit der Regelung sowie ihr Beitrag zur Gewährleistung eines offenen und vielfältigen Kommunikationsprozesses abzuwarten.

C) KI-VERORDNUNG

Auch die KI-Verordnung ist vorliegend von Relevanz. Gemäß Art. 2 Abs. 1 lit. c) KI-VO gilt diese u. a. für KI aus Drittstaaten. Nach Art. 99 Abs. 4 lit. g) KI-VO können zudem wirksame Sanktionen (bis zu 15 Mio. €) für Verstöße gegen die skizzierten Transparenzpflichten verhängt werden. Eine Umsetzung dieser Bestimmung soll durch § 16 des Gesetzes zur Marktüberwachung und Innovationsförderung von künstlicher Intelligenz (KI-Marktüberwachungs-und-Innovationsförderungsgesetz – KI-MIG) erfolgen, der auf das nationale Ordnungswidrigkeitengesetz verweist.²²³

222 Pressemitteilung der Kommission v. 5.12.2025, abrufbar unter: <https://digital-strategy.ec.europa.eu/en/news/commission-fines-x-eu120-million-under-digital-services-act> (letzter Abruf: 30.4.2026).

223 Vgl. BT-Drs. 21/4594, S. 18.

aa) Verbot von manipulativen oder täuschenden Techniken (Art. 5 KI-VO)

So verbietet Art. 5 Abs. 1 lit. a) KI-VO die Verwendung eines KI-Systems, „das Techniken der unterschwelligen Beeinflussung außerhalb des Bewusstseins einer Person oder absichtlich manipulative oder täuschende Techniken mit dem Ziel oder der Wirkung einsetzt, das Verhalten einer Person oder einer Gruppe von Personen wesentlich zu verändern, indem ihre Fähigkeit, eine fundierte Entscheidung zu treffen, deutlich beeinträchtigt wird, wodurch sie veranlasst wird, eine Entscheidung zu treffen, die sie andernfalls nicht getroffen hätte, und zwar in einer Weise, die dieser Person, einer anderen Person oder einer Gruppe von Personen erheblichen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit zufügen wird.“²²⁴ Auch durch die Manipulation des öffentlichen Informationsraums kann ein solcher erheblicher Schaden angerichtet werden. Namentlich werden im rechtswissenschaftlichen Schrifttum als Schadenspositionen „kultureller Schäden“ oder kollektive und gesellschaftliche Schäden wie die Beeinflussung von Wahlscheidungen genannt.²²⁵

bb) Transparenzpflichten (Art. 50 KI-VO)

Zudem müssen die Anbieter von KI-Systemen, „die für die direkte Interaktion mit natürlichen Personen bestimmt sind, so konzipiert und entwickelt werden, dass die betreffenden natürlichen Personen informiert werden, dass sie mit einem KI-System interagieren, es sei denn, dies ist aus Sicht einer angemessen informierten, aufmerksamen und verständigen natürlichen Person aufgrund der Umstände und des Kontexts der Nutzung offensichtlich“ (Art. 50 Abs. 1 S. 1 KI-VO).

Ferner müssen „Anbieter von KI-Systemen, einschließlich KI-Systemen mit allgemeinem Verwendungszweck²²⁶, die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen, (...) sicher(stellen), dass die Ausgaben des KI-Systems in einem maschinenlesbaren Format gekennzeichnet und als künstlich erzeugt oder manipuliert erkennbar sind“ (Art. 50 Abs. 2 S. 1 KI-VO). Das Gleiche gilt für „Betreiber eines KI-Systems, das Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert, die ein Deepfake sind, (die offenlegen müssen), dass die Inhalte künstlich erzeugt oder manipuliert wurden. (...) Ist der Inhalt Teil eines offensichtlich künstlerischen, kreativen, satirischen, fiktionalen oder analogen Werks oder Programms, so beschränken sich die in diesem Absatz festgelegten Transparenzpflichten darauf, das Vorhandensein solcher erzeugten oder manipulierten Inhalte in geeigneter Weise offenzulegen, die die Darstellung oder den Genuss des Werks nicht beeinträchtigt.“ Entsprechende Techniken einer solchen „Transparency by Design“ sind etwa sog. digitale Wasserzeichen, Metadatenidentifizierungen, kryptografische

224 Zum Verhältnis dieser Norm zu der Dark-Pattern-Regelung in Art. 25 DSA (oben § 2 D. I. 1. a) cc) (7)) s. Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of Art. 33 of Regulation (EU) 2022/2065 and the interaction of that Regulation with other legal acts v. 17.11.2025, COM(2025) 708 final, S. 14 u. 19, wo von einer parallelen Anwendbarkeit beider Bestimmungen ausgegangen wird.

225 Raue, in: Schefzig/Kilian, BeckOK KI-Recht, Art. 5 Rn. 40 m.w.N. Auch die Leitlinien der Kommission zu verbotenen Praktiken der künstlichen Intelligenz (KI), C(2025) 884 final, Rn. 86, erwähnen „gesellschaftliche Schäden“ als berücksichtigungswert.

226 Hierbei handelt es sich um LLMs.

Methoden zum Nachweis der Herkunft und Authentizität eines Inhalts, Protokollierungsmethoden, „Fingerabdrücke“ oder eine Kombination solcher Techniken.²²⁷

Des Weiteren müssen „Betreiber eines KI-Systems, das Text erzeugt oder manipuliert, der veröffentlicht wird, um die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren, (...) offenlegen, dass der Text künstlich erzeugt oder manipuliert wurde. Diese Pflicht gilt nicht, wenn (...) die durch KI erzeugten Inhalte einem Verfahren der menschlichen Überprüfung oder redaktionellen Kontrolle unterzogen wurden und wenn eine natürliche oder juristische Person die redaktionelle Verantwortung für die Veröffentlichung der Inhalte trägt“ (Art. 50 Abs. 4 KI-VO).²²⁸

cc) Existenz eines KI-Systems (Art. 3 KI-VO)

Die Anwendbarkeit der vorstehend skizzierten Manipulationsverbote und Transparenzverpflichtungen setzt allerdings voraus, dass es sich bei dem eingesetzten Medium um ein KI-System handelt. Als solches definiert Art. 3 Ziff. 1 KI-VO „ein maschinengestütztes System, das für einen in unterschiedlichem Grad autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können“.

Hieraus folgt, dass nicht alle Formen einer technischen Manipulation von Informationsprozessen und -räumen auf KI-Systemen beruhen. Denn ein KI-System im Sinne der KI-VO ist ein autonomes, anpassungsfähiges sowie daten- und modellgestütztes Gesamtsystem mit regelungsbedürftigen Auswirkungen auf Menschen oder deren Umgebungen. Das automatisierte Kommentieren, Teilen oder Liken demokratiezersetzender Inhalten durch (Social) Bots wird diesen Grad der Autonomie und selbstlernenden Anpassungsfähigkeit häufig nicht erreichen.²²⁹ Am ehesten werden KI-Systeme deshalb bei der Erstellung komplexer Inhalte (Deepfakes von kombinierten oder nicht kombinierten Bildern und Videos, Bewegungen und Audioinhalten²³⁰) zum Einsatz kommen, aber weniger (oder überhaupt nicht) bei bloßen technischen Manipulation des öffentlichen Informationsraums (etwa durch Bots oder die Ausnutzung der Wirkungsweise von Empfehlungsalgorithmen) zur Erhöhung der Reichweite durch CIB.²³¹

D) AVMD-RICHTLINIE

Die AVMD-Richtlinie kann für den Untersuchungsgegenstand auf verschiedene Art und Weise Relevanz erlangen:

- 227 Oster, AfP 2024, 285 (286 f., Rn. 7) m.w.N., der zudem darauf hinweist, dass durch diese Transparenzvorgabe das „Cheapest Cost Avoider“-Prinzip umgesetzt werden soll.
- 228 Zur Kennzeichnungspflicht von Deepfakes vgl. bitkom, Policy Brief, S. 17 f. Zu Inkonsistenzen des Anwendungsbereichs dieser Regelung s. Oster, AfP 2024, 285 (286, Rn. 6).
- 229 Insofern etwas undifferenziert Kalbhenn, ZRP 2025, 111 (112), der Chatbots pauschal dem Anwendungsbereich des Art. 50 Abs. 1 KI-VO unterstellt.
- 230 S. hierzu bereits oben Fn. 42.
- 231 So i. Erg. denn auch Kalbhenn, ZRP 2025, 111 (112): „Nicht adressiert wird in der KI-VO (...) der massenhafte und koordinierte Einsatz von Bots, um künstlich Relevanz und Reichweite zu erzeugen.“

aa) Beschränkung des freien Empfangs von audiovisuellen Mediendiensten (Art. 3 AVMD-RL)

Zunächst eröffnet die AVMD-Richtlinie die Möglichkeit, den Empfang und die Weiterverbreitung solcher linearen bzw. nichtlinearen audiovisuellen Mediendienste²³² einzuschränken, die durch Desinformation und (Kriegs-)Propaganda zu Gewalt oder Hass gegen Gruppen bzw. Personen aufstacheln, öffentlich zur Begehung terroristischer Straftaten auffordern oder die körperliche, geistige und sittliche Entwicklung von Minderjährigen beeinträchtigen. Als Vorbild für solche Manipulationen des öffentlichen Informationsraums kann auf die Beschränkungen von RT und Sputnik verwiesen werden, welche vom EuGH als rechtmäßig bewertet wurden. So haben seit 2015 Lettland und Litauen die russischsprachige Ausstrahlung des Fernsehkanals „RTR Planeta“ mehrfach ausgesetzt. Diese Entscheidungen basierten auf Art. 3 Abs. 2 und 3 AVMD-RL i.V.m. Art. 6 AVMD-RL, welche die Aussetzung von Fernsehsendungen erlauben, wenn sie Hass schüren. Die Kommission bestätigte insoweit, dass Lettland und Litauen das Recht hätten, Fernsehsendungen, die zur Besetzung und „Vernichtung“ verschiedener Staaten aufriefen, als rechtswidrige Kriegspropaganda auszusetzen.²³³ Auch der EuGH erkannte in der Rechtssache *Baltic Media Alliance* an, dass die Bekämpfung einer kriegspropagandistischen Anstiftung zum Hass aufgrund von Nationalität ein legitimes Ziel der öffentlichen Ordnung darstelle.²³⁴

Diese genuin medienrechtlichen Beschränkungsmöglichkeiten treten neben die bereits oben²³⁵ skizzierte, von anderen Voraussetzungen abhängige Option, durch Wirtschaftssanktionen gegen bestimmte feindselige Mediendiensteanbieter vorzugehen.

bb) Schutz vor bestimmten Inhalten und Meldeverfahren (Art. 28b AVMD-RL)

Zudem statuiert Art. 28b AVMD-RL für Video-Sharing-Dienste²³⁶ Regelungen, die über den Schutz vor bestimmten Inhalten und Meldeverfahren einen Beitrag zum Kampf gegen Manipulationen des öffentlichen Kommunikationsraums zu leisten vermögen.

So haben nach Art. 28b Abs. 1 AVMD-RL die Mitgliedstaaten sicherzustellen, dass die ihrer Rechtshoheit unterliegenden Video-Sharing-Plattform-Anbieter angemessene Maßnahmen zum Schutz von Minderjährigen vor entwicklungsbeeinträchtigenden Inhalten (lit. a) und der Allgemeinheit vor gewalt- oder hassbezogenen Inhalten (lit. b) treffen. Zudem müssen Video-Sharing-Dienste für ihre Nutzer gemäß Art. 28b Abs. 3 UAbs. 3 lit. d) AVMD-RL geeignete Meldeverfahren zur Meldung derartiger Inhalte bereitstellen. Das interessante an dieser Bestimmung ist, dass sich – anders als nach dem DSA²³⁷ – diese Meldungen auch auf nicht-rechtswidrige Inhalte beziehen können. Von daher ist es gerechtfertigt, diese Bestimmung parallel zu Art. 16 DSA anzuwenden.²³⁸

²³² Vgl. Art. 1 lit. a) i) AVMD-RL.

²³³ Beschlüsse der Kommission v. 19.7.2015, 17.2.2017, 4.5.2018 u. 3.5.2019 – RTR Planeta I – IV.

²³⁴ EuGH, Urt. v. 4.7.2019 – C-622/17 = ZUM 2019, 923 ff. m. Anm. Brings-Wiesen, ZUM 2019, 933 ff. Näher zum Ganzen m.w.N. Baade, verfassungsblog v. 8.3.2022; ders., EuR 2020, 653 (654 f.); Ferreau, verfassungsblog v. 10.3.2022; Setz/Seyda, ZD-Aktuell 2022, 01167 (sub 2.).

²³⁵ § 2 C. I. 1. a).

²³⁶ Zum Begriff s. Art. 1 lit. a) ii) (aa) AVMD-RL.

²³⁷ S. hierzu oben § 2 D. I. 1. a) cc) (2).

²³⁸ S. hierzu auch Report from the Commission to the European Parliament, the Council and the European Economic and

2. NATIONALES RECHT

A) ZIVILRECHT

aa) Vertragliche Möglichkeiten

Das Zivilrecht eröffnet zunächst die Möglichkeit einer AGB-Kontrolle der Gemeinschaftsstandards nach den §§ 307 ff. BGB i.V.m. Art. 14 DSA sowie von vertragsrechtlichen Streitigkeiten, die sich aus dem Nutzervertrag mit Blick auf die Möglichkeiten zur Sperrung oder Löschung von Inhalten ergeben können. Dies setzt allerdings ein Tätigwerden der Plattform voraus, gegen das sich ein Nutzer – ggf. nach Ausschöpfung der vom DSA vorgesehenen Beschwerde- und Streit-schlichtungsverfahren²³⁹ – gerichtlich zur Wehr setzt.²⁴⁰

bb) Deliktische Möglichkeiten

In Gestalt des § 823 BGB i.V.m. § 1004 BGB (Unterlassungs- und Beseitigungsanspruch) bzw. §§ 823 Abs. 1 und 2, 826 BGB (Schadensersatz) bietet das Zivilrecht zudem die Möglichkeit, deliktisch gegen Persönlichkeitsverletzungen vorzugehen. Solche Persönlichkeitsverletzungen können insbesondere in einem „Identitätsdiebstahl“ bestehen, der zur Verschleierung der wahren Identität eines Kommunizierenden begangen wird (sog. Doppelgänger-Kampagne). Anknüpfungspunkt hierfür kann der unbefugte Gebrauch eines Namens (§ 12 BGB), ein Markenrechtsverstoß (§ 14 MarkenG) oder sonst eine Persönlichkeitsbeeinträchtigung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) sein. Aber auch Desinformationen oder Deepfakes mit persönlichkeitsverletzendem Charakter kommen als Anknüpfungspunkte für einen solchen deliktischen Unterlassungs- oder Schadensersatzanspruch in Betracht.²⁴¹

Erfolgt eine solche Beeinträchtigung durch ein Handeln von außerhalb der Bundesrepublik Deutschland oder der EU (etwa aus China oder Russland), greift nicht die Brüssel-Ia-Verordnung.²⁴² Maßgeblich ist dann das deutsche internationale Zivilprozessrecht in Gestalt des § 32 ZPO. Ein deutsches Gericht ist hiernach zuständig, wenn der Handlungsort oder der Erfolgsort in Deutschland liegt (§ 32 ZPO); Letzteres trifft typischerweise auf Online-Delikte in Gestalt von Persönlichkeitsrechtsverletzungen oder der Verletzung von Namensrechten und gewerblichen Schutzrechten (Markenrechten) zu.

Social Committee on the application of Art. 33 of Regulation (EU) 2022/2065 and the interaction of that Regulation with other legal acts v. 17.11.2025, COM(2025) 708 final, S. 20 f. Als unklar bezeichnet das Verhältnis zwischen Art. 28b AVMD-RL und Art. 16 DSA indes Barudi, in: Müller-Terpitz/Köhler, DSA, Art. 16 Rn. 11. Eine explizite Kollisionsnorm zu Art. 28b AVMD-RL statuiert i.Ü. Art. 18 Abs. 4 UAbs. 3 EMFA.

239 S. hierzu bereits oben § 2 D. I. 1. a) cc) (4).

240 Aktuelles Beispiel: Die Löschung von Nutzer-Äußerungen über angebliche Impfschäden (Desinformation) als Verstoß gegen die Plattform-Gemeinschaftsstandards; s. hierzu oben Fn. 194.

241 Vgl. insoweit bitkom, Policy Brief, S. 18, dort auch mit dem zutreffenden Hinweis, dass in all diesen Maßnahmen zugleich ein nicht gerechtfertigter datenschutzrechtlicher Eingriff i.S.d. DSGVO liegen kann.

242 Verordnung (EU) Nr. 1215/2012 des Europäischen Parlaments und des Rates v. 12.12.2012 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen.

Jenseits dieser Gerichtsstandsfragen ist zudem zu klären, welches Recht zur Anwendung kommt. Insoweit greift die Rom-II-Verordnung, die auch für schädigende Handlungen aus Drittstaaten (wie China oder Russland) gilt.²⁴³ Sie sieht in Art. 4 Abs. 1 Rom-II-VO die Grundregel vor, dass das Recht desjenigen Staates Anwendung findet, in dem der Schaden eintritt (vorliegend also §§ 823 ff. BGB), und zwar auch dann, wenn der Schädiger im Ausland sitzt.

Trotz dieser eindeutigen Rechtslage wird in der Praxis jedoch häufig die Anspruchsdurchsetzung Schwierigkeiten bereiten, da die bei einem deutschen Gericht eingereichte Klage über das Haager Zustellungsübereinkommen (HZÜ) im Ausland zugestellt werden muss. Zwar sind China und Russland Vertragspartner dieses Übereinkommens. Dennoch dürfte bei FIMI-Maßnahmen in der Praxis eine Zustellung mehr als ungewiss sein. Selbst wenn es zu einer Zustellung und zu einem Urteil käme, bedürfte das Urteil der Anerkennung durch den Drittstaat, was in der zu untersuchenden Konstellation ebenfalls mehr als fraglich erscheint. Aus diesem Grund dürfte auch eine Klage direkt im Ausland faktisch keinen Erfolg versprechen. An diesem Rechtsschutzdefizit wird sich kurzfristig nichts ändern.

Da FIMI-Maßnahmen zudem staatlich initiiert sind, müssen sie streng genommen als sog. „*acta iure imperii*“, d.h. als juristische Handlungen hoheitlicher Natur betrachtet werden. Nach diesem völkerrechtlichen Prinzip genießen derartige Handlungen und die Personen, die sie umsetzen, staatliche Immunität mit der Folge, dass sie ausschließlich an den gesetzlichen Regeln des Ausgangsstaats zu messen sind. Freilich werden Staaten, die FIMI-Maßnahmen durchführen, im Regelfall nicht bereit sein, hierfür offiziell die Verantwortung zu übernehmen, da es sich um verdeckte Operationen handeln dürfte.

B) STRAFRECHT

Auch strafrechtliche Bestimmungen können vorliegend von Relevanz sein. Insoweit kommen, je nach Lebenssachverhalt, zahlreiche Bestimmungen in Betracht. Die nachfolgende Untersuchung konzentriert sich deshalb auf diejenigen Strafrechtsnormen, die einen spezifischen Bezug zur Manipulation des öffentlichen Informationsraums aufweisen. Vorab ist insoweit festzustellen, dass derartige Manipulationen *per se* im Regelfall nicht rechtswidrig oder gar strafbar sind.²⁴⁴ Dies gilt vor allem für Desinformationen als einer Form der Manipulation des öffentlichen Informationsraums.

aa) Materielle Straftatbestände

Desinformation kann nur im Einzelfall, d.h. wenn ihr ein persönlichkeitsverletzender Charakter zukommt, als üble Nachrede strafbar sein (§ 186 StGB). Gleiches gilt für die bewusst unwahre Tatsachenbehauptung, die ggf. als Verleumdung (§ 187 StGB) strafbar ist. Sind Personen des

²⁴³ Verordnung (EG) Nr. 864/2007 des Europäischen Parlaments und des Rates v. 11.7.2007 über das auf außervertragliche Schuldverhältnisse anzuwendende Recht.

²⁴⁴ So auch Kastor/Püschel, K&R 2023, 20; Schlömer/Kehrberg, ZRP 2025, 2 (4).

politischen Lebens betroffen, erhöht sich unter den Voraussetzungen des § 188 Abs. 2 StGB die Strafandrohung für derartige Taten. Im Regelfall handelt es sich dabei um Antragsdelikte (§ 194 Abs. 1 S. 1 StGB).²⁴⁵ In diesem Kontext ist auch § 90 StGB zu erwähnen, der die Verunglimpfung des Bundespräsidenten, welche durch eine Ehrkränkung i.S.d. §§ 185 ff. StGB erfolgen muss²⁴⁶, unter Strafe stellt. Auch kommt insoweit eine Strafbarkeit nach § 90a StGB (Verunglimpfung des Staates und seiner Symbole), § 90b StGB (verfassungsfeindliche Verunglimpfung von Verfassungsorganen) und § 90c StGB (Verunglimpfung von Symbolen der Europäischen Union) in Betracht, die ebenfalls durch falsche Tatsachenbehauptungen erfolgen kann.²⁴⁷ Zu erwähnen ist ferner die landesverräterische Fälschung (§ 100a StGB).

Auch § 107 StGB (Wahlbehinderung) und § 107a StGB (Wahlfälschung) können vorliegend von Relevanz sein, haben aber mit ihrer unmittelbaren Anknüpfung an die Wahlakte als solche einen nur sehr eingeschränkten Anwendungsbereich. Gleiches gilt für die §§ 108 und 108a StGB, welche die Wählernötigung und Wählertäuschung unter Strafe stellen.

§ 80a StGB (Aufstacheln zum Verbrechen der Aggression) stellt die Kriegspropaganda unter Strafe.²⁴⁸ § 85 StGB bestraft denjenigen, der den organisatorischen Zusammenhalt einer verbotenen Vereinigung fortführt; dies kann mit Blick auf verbotene Mediendiensteanbieter Relevanz erlangen. Des Weiteren stellt § 86 StGB die Verbreitung von Propagandamitteln verfassungswidriger und terroristischer Organisationen unter Strafe. Schließlich kann auch die Volksverhetzung (§ 130 StGB) bei Manipulationen des öffentlichen Informationsraums einschlägig sein. Häufig beziehen sich falsche Tatsachenbehauptungen jedoch nicht unmittelbar auf eine konkrete andere Person oder es fehlt ihnen der nötige Gruppenbezug. Auch kann ihnen wegen vorgespiegelter Neutralität der ehrverletzende Charakter oder sonst ein erforderliches Tatbestandselement (wie die Aufstachelung zum Hass oder zur Gewalt) fehlen.²⁴⁹

bb) Strafprozessuale und sonstige Verfolgungsaspekte

Gemäß § 4 i.V.m. § 9 Abs. 1 StGB können strafbare Manipulationen des öffentlichen Informationsraums auch vom Ausland aus begangen werden, solange ihr Erfolg im Inland eintritt. Allerdings setzt die Strafverfolgung dann eine Auslieferung des Täters voraus. Während dies in der EU auf der Grundlage eines Europäischen Haftbefehls im Regelfall möglich ist, kann mit Drittstaaten wie Russland eine Auslieferung nur auf der Grundlage des Europäischen Auslieferungsabkommens erfolgen. Letzteres wird von Russland derzeit aber nicht angewendet.

Falls Manipulationen des öffentlichen Informationsraums eine Strafbarkeit im vorbeschriebenen Sinne nach sich ziehen, ergeben sich hieraus trotz der skizzierten Strafverfolgungshemmnisse interessante rechtliche Effekte für die Bekämpfung derartiger Einwirkungen auf den Kommu-

245 S. hierzu auch Kuhlmann/Trute, GSZ 2022, 115 (119), die berechtigterweise darauf hinweisen, dass sich diese Regelungen nicht nur gegen Falschinformationen wenden, sondern darüber hinaus dem Rechtsgüterschutz dienen.

246 Valerius, in: v. Heintschel-Heinegg/Kudlich, BeckOK StGB, § 90 Rn. 3.

247 Vgl. Valerius, in: v. Heintschel-Heinegg/Kudlich, BeckOK StGB, § 90a Rn. 4.

248 Die Bestimmung setzt Art. 26 Abs. 1 S. 2 GG um.

249 Mafi-Gudarzi, ZRP 2019, 65 (67) m.w.N.; Schlömer/Kehrberg, ZRP 2025, 2 (5).

nikationsprozess. Denn die Strafbarkeit hat zur Folge, dass diese Manipulationshandlungen als rechtswidrige Inhalte oder Tätigkeiten i.S.d. Art. 3 lit. h) DSA zu qualifizieren sind. Erlangt eine Online-Plattform – etwa über das Meldeverfahren nach Art. 16 DSA – von ihnen Kenntnis, muss sie gemäß Art. 6 DSA im Regelfall tätig werden, um eine zivilrechtliche oder strafrechtliche Verantwortlichkeit für sich bzw. ihrer Mitarbeiter abzuwenden. Gleiches gilt, wenn zur Durchsetzung dieser Straftatbestände die Anordnung einer Justiz- und Verwaltungsbehörde i.S.d. Art. 9 DSA gegen die Plattform ergeht. Von daher bildet das Strafrecht zugleich einen Hebel zur Bekämpfung rechtswidriger Inhalte auf Plattformen, auch wenn der eigentliche Täter für sein Verhalten nicht zur Verantwortung gezogen werden kann. Gleiches gilt im Übrigen bei Verstößen gegen zivilrechtliche Normen.²⁵⁰

C) ÖFFENTLICHES RECHT

aa) Vereinsrecht

Wie das Bundesverwaltungsgericht in seiner bereits des Öfteren erwähnten Compact-Entscheidung²⁵¹ festgestellt hat, umfasst das Vereinsrecht kompetenziell die Möglichkeit, unter den Voraussetzungen des Art. 9 Abs. 2 GG i.V.m. § 3 Abs. 1 Nr. 1 VereinsG gegen einen Mediendiensteanbieter mit Sitz in Deutschland ein Vereinsverbot auszusprechen, sprich diese Vereinigung aufzulösen. Mit Blick auf die Kommunikationsfreiheiten hat das Gericht diese Möglichkeit allerdings dahingehend eingeschränkt, dass verfassungsfeindliche Inhalte dem Medium ein Gesamtgepräge geben müssen und nicht von der Meinungsäußerungsfreiheit (Art. 5 Abs. 1 S. 1 Var. 1 GG) gedeckt sein dürfen. In der Praxis erweist sich dies als eine so hohe Hürde, dass dem Instrument für die Zukunft keine Bedeutung zukommen dürfte.

bb) Medienrecht

Zudem hält das Medienrecht der Länder zahlreiche Bestimmungen mit Relevanz für den vorliegenden Untersuchungsgegenstand bereit. Hier spielen vor allem Bestimmungen aus dem Medienstaatsvertrag (MStV) eine zentrale Rolle. Als solche sind hervorzuheben:

(1) Journalistische Sorgfaltspflichten (§§ 6, 19 MStV)

Rundfunkanbieter und Telemedien²⁵² mit journalistisch-redaktionell gestalteten Angeboten haben nach §§ 6, 19 MStV den anerkannten journalistischen Grundsätzen zu entsprechen. Hierzu gehört insbesondere, dass Nachrichten (also Informationen) vor ihrer Verbreitung mit der nach den Umständen gebotenen Sorgfalt auf Inhalt, Herkunft und Wahrheit zu prüfen sind. Die Verbreitung von Desinformation verstößt mithin gegen diese gesetzliche Vorgabe.

²⁵⁰ S. dazu bereits vorstehend § 2 D. I. 2. a).

²⁵¹ S. hierzu oben § 2 C. I. 2. a) und § 2 C. II. 2. b) bb) (1).

²⁵² Zur Definition s. § 2 Abs. 1 MStV.

(2) Kennzeichnungspflicht für Social Bots (§ 18 MStV)

Des Weiteren sind gemäß § 18 Abs. 3 MStV Anbieter in sozialen Netzwerken verpflichtet, bei mittels eines Computerprogramms automatisiert erstellten Inhalten oder Mitteilungen (sog. Chatbots oder Social Bots) den Umstand der Automatisierung kenntlich zu machen, sofern das hierfür verwandte Nutzerkonto seinem äußeren Erscheinungsbild nach für die Nutzung durch natürliche Personen bereitgestellt wurde. Unter Social Bots sind grundsätzlich alle Softwareprogramme zu verstehen, die menschliche Verhaltensweisen in sozialen Netzwerken imitieren, indem sie z. B. Beiträge automatisiert verfassen, kommentieren, liken oder teilen.²⁵³

Die Bestimmung ist für den Kampf gegen technische Manipulationen des Informationsraums von großer Bedeutung. Sie zielt darauf ab, durch Transparenz die Offenheit und Vielfalt des Kommunikationsprozesses zu schützen.²⁵⁴ Da es sich bei diesen Social Bots im Regelfall nicht um KI-Anwendungen handelt²⁵⁵, bleibt § 18 Abs. 3 MStV in vielen Fällen neben der KI-Verordnung anwendbar.²⁵⁶ Ein Verstoß gegen diese Transparenzvorgabe macht den Social Bot zudem zu einem illegalen Inhalt i.S.d. DSA.²⁵⁷ Der Anbieter des Bots muss hierfür allerdings seinen Sitz in Deutschland haben (§ 1 Abs. 7 MStV)²⁵⁸, was auf viele Verwender solcher Programme nicht zutreffen dürfte.

(3) Medienintermediärsregulierung (§§ 93 und 94 MStV)

Von Relevanz ist ferner die Transparenzvorschrift in § 93 MStV für Anbieter von Medienintermediären²⁵⁹, zu denen insbesondere soziale Netzwerke und Suchmaschinen gehören. Er verpflichtet diese Online-Plattformen dazu, zwecks Sicherung der Meinungsvielfalt über die zentralen Kriterien der Aggregation, Selektion und Präsentation von eingesetzten Empfehlungsalgorithmen aufzuklären. Dies erlaubt auch Einblicke in die Wirkungsweise von Algorithmen bei der Verbreitung von Desinformation und Propaganda oder für die technische Manipulation der Reichweite solcher Inhalte.²⁶⁰ Inwiefern diese Regelung neben Art. 27 DSA anwendbar ist, ist allerdings sehr umstritten.²⁶¹

Daran anknüpfend gewährleistet § 94 MStV zur Sicherung der Meinungsvielfalt ein Diskriminierungsverbot. Es verbietet Medienintermediären, mit Blick auf journalistisch-redaktionell gestaltete Angebote ohne sachlich gerechtfertigten Grund von den nach § 93 MStV zu veröffentlichen-

253 Lent, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, § 18 Rn. 13 mw.N.

254 Vgl. Held/Ingold, in: Binder/Vesting, Beck'scher Kommentar zum Rundfunkrecht, § 18 Rn. 89, dort auch zur Verfassungsmäßigkeit der Regelung.

255 S. hierzu bereits oben § 2 D. I. 1. c) cc).

256 Gleiches gilt i.Ü. für das Verhältnis dieser Regelung zum DSA, da letzterer jenseits des Art. 16 Abs. 6 S. 2 DSA (automatisierte Bearbeitungen von Meldungen rechtswidriger Inhalte nach Art. 16 Abs. 1 DSA) keine allgemeine Kennzeichnungspflicht für automatisierte Inhalte vorschreibt.

257 Kalbhenn, ZUM 2021, 663 (669 ff., 673), der zu Recht darauf hinweist, dass dies natürlich auch bei einem Verstoß gegen die Transparenzpflichten der KI-VO gilt.

258 Held/Ingold, in: Binder/Vesting, Beck'scher Kommentar zum Rundfunkrecht, § 18 Rn. 89.

259 Zur Definition s. § 2 Abs. 2 Nr. 16 u. 21 MStV.

260 Zu diesem Regelungsgegenstand s. bereits oben § 2 D. I. 1. a) cc) (8).

261 Ausführlich hierzu Müller-Terpitz, (Un-)Level Playing Field im Medienbereich, S. 39 ff. m.w.N. S. ferner die oben Fn. 89 genannten Fundstellen.

den Kriterien zugunsten oder zulasten eines bestimmten Angebots systematisch abzuweichen oder durch diese Kriterien solche Angebote unmittelbar oder mittelbar systematisch unbillig zu behindern (§ 94 Abs. 1 und 2 MStV).

Da dieser Diskriminierungsschutz auf eine Sicherung der Meinungsvielfalt zielt, ließe sich unter eine solche unbillige Behinderung auch eine Gestaltung des Empfehlungsalgorithmus subsumieren, die Manipulationen des öffentlichen Informationsraums erleichtert oder sogar bevorteilt. Die Regelung könnte deshalb als ein Anknüpfungspunkt für die Bekämpfung solcher Manipulationen fungieren. Ob die Bestimmung neben dem Risikomanagementsystem des Art. 34 f. DSA anwendbar ist, ist zwar umstritten, im Ergebnis aber wegen des unterschiedlichen Anwendungsbereichs (vgl. § 91 MStV vs. Art. 33 DSA), der unterschiedlichen Zielsetzung (§ 94 MStV dient speziell der Sicherung der Meinungsvielfalt) und der unterschiedlichen Normstruktur der Bestimmung (ordnungsrechtliche vs. privatautonom-selbstregulative Regelung) zu bejahen. Ob die Norm über § 1 Abs. 8 MStV auch auf Online-Plattformen im EU-Ausland erstreckt werden darf, ist mit Blick auf das in der E-Commerce-Richtlinie geregelte Herkunftslandprinzip (Art. 3 Abs. 1 EC-RL) allerdings ebenfalls hoch umstritten.²⁶²

(4) Präventive Maßnahmen bei Rechtsverstößen (§ 109 MStV)

§ 109 Abs. 1 und 3 MStV eröffnet den Landesmedienanstalten ein wichtiges Instrumentarium bei Rechtsverstößen gegen Bestimmungen des Medienstaatsvertrags. Diese Maßnahmen können sich einerseits gegen den unmittelbar Verantwortlichen, d.h. gegen den Rundfunkveranstalter, Telemedienanbieter oder Verwender eines Social Bots richten (Abs. 1). Bei mangelnder Erfolgsaussicht ist es den Landesmedienanstalten andererseits jedoch auch erlaubt, gegen Dritte, also insbesondere gegen die Online-Plattformen, vorzugehen. Hierbei ist allerdings das Digitale-Dienste-Gesetz (und damit das Herkunftslandprinzip der E-Commerce-Richtlinie) und der DSA zu beachten. Konkret bedeutet dies, dass unter den in § 109 Abs. 3 MStV normierten Voraussetzungen Maßnahmen i.S.d. Art. 9 DSA auch gegen die Plattformen gerichtet werden können. Dies ist deshalb von Relevanz, weil – wie gesehen – die eigentlich Verantwortlichen häufig unerreichbar im Ausland (China oder Russland) sitzen. Maßnahmen zur Bekämpfung von Manipulation des öffentlichen Informationsraums, die auf Verstöße gegen den MStV gestützt werden, können dann immerhin an die mittelbar verantwortlichen Plattformen, die zumeist über eine EU-Niederlassung verfügen, adressiert werden.

Zu beachten ist allerdings, dass es den Landesmedienanstalten verwehrt ist, Maßnahmen wegen eines Verstoßes gegen § 17 MStV zu ergreifen. Die Norm ist explizit vom Anwendungsbereich des § 109 Abs. 1 MStV ausgenommen. Ein Verstoß gegen die verfassungsmäßige Ordnung (= Summe aller Normen der Rechtsordnung) reicht für ein Tätigwerden der Landesmedienanstalten mithin nicht aus.²⁶³ Auch sind die Einschränkungen in § 109 Abs. 1 S. 4 MStV mit Blick auf § 19 MStV (journalistische Sorgfaltspflichten von Telemedien) zu beachten.

²⁶² Vgl. hierzu erneut die vorstehend genannten Nachweise.

²⁶³ So jedenfalls die nicht unumstrittene herrschende Sichtweise; vgl. Müller-Terpitz, (Un-)Level Playing Field im Medienbereich, S. 57 Fn. 295 m.w.N.

(5) Repressive Maßnahmen bei Rechtsverstößen (§ 115 MStV)

Verstöße gegen etliche der vorstehend skizzierten Bestimmungen können zudem mit einer Geldbuße geahndet werden. Dies gilt insbesondere für Verstöße gegen das Kennzeichnungsgebot aus § 18 Abs. 3 MStV (§ 115 Abs. 1 S. 2 Nr. 2 MStV) und gegen die §§ 93 und 94 MStV (§ 115 Abs. 1 S. 2 Nr. 41-46 MStV). Die Höhe der Geldbuße kann bis zu 500.000 €/Verstoß betragen (§ 115 Abs. 2 MStV).

Verstöße gegen die journalistischen Standards können demgegenüber nicht repressiv, sondern nur präventiv (durch eine Beanstandung) geahndet werden; der Gesetzgeber sichert hierdurch die Meinungs- und Medienfreiheiten vor hoheitlichen Eingriffen mit hohem Abschreckungspotenzial ab.

II. EXEKUTIVER STATUS QUO

Aus Sicht des Gesetzesvollzugs sind hoheitliche (EU-Kommission, Bundesregierung und Bundesministerien²⁶⁴, BND, Bundes- bzw. Landesverfassungsschutzämter, Staatsanwaltschaften, Polizeibehörden), staatsferne (Landesmedienanstalten) und nichtstaatliche Akteure (Online-Plattformen) auf verschiedenen Ebenen (unional, national, föderal) für das Ergreifen und die Durchsetzung von Maßnahmen zum Kampf gegen Manipulationen des öffentlichen Informationsraums zuständig. Insoweit stellt sich die Frage, wie diese Zuständigkeiten im Mehrebenensystem verteilt sind und an welchen Stellen sich aufsichts- und vollzugsrechtliche Übergabepunkte ergeben.

1. UNIONALES RECHT

A) DIGITAL SERVICES ACT

Dem DSA kommt insoweit die größte Bedeutung für die exekutive Zuständigkeitsordnung und das Zusammenspiel der einzelnen Behörden zu.

aa) Europäische Kommission

So begründet der DSA für VLOPs und VLOSEs als den wichtigsten Plattformen im Rahmen des hiesigen Untersuchungsgegenstands gemäß Art. 56 Abs. 2 und 4 DSA eine ausschließliche Zuständigkeit zugunsten der Kommission, soweit Verstöße gegen die Art. 33 ff. DSA (Risikomanagementsystem) in Rede stehen. Ihr stehen hierzu die Befugnisse aus Art. 64 ff. DSA zur Verfügung. Die Kommission arbeitet dabei eng mit den DSCs der Mitgliedstaaten zusammen.

²⁶⁴ Vgl. insoweit BT-Drs. 20/13880 v. 21.11.2024, S. 1 f.

Bei festgestellten Verstößen gegen die Verordnung kann sie gestützt auf Art. 72 DSA hohe Geldbußen (bis zu 6% des Gesamtjahresumsatzes) verhängen.²⁶⁵

Auch für sonstige Verstöße gegen den DSA verfügt die Kommission mit Blick auf diese Plattformen über eine konkurrierende Kompetenz im Verhältnis zum Mitgliedstaat des Niederlassungsorts (Art. 56 Abs. 3 und 4 DSA). An dieser Stelle besteht mithin ein aufsichtsrechtlicher Übergabepunkt von der Kommission auf die jeweils zuständige Behörde des Mitgliedstaats²⁶⁶, der jedoch von einem Unterlassen der Kommission (fehlende Verfahrenseinleitung) abhängt.

bb) Behörden der Mitgliedstaaten

Besteht keine ausschließliche oder konkurrierende Zuständigkeit zugunsten der Kommission, sind die Mitgliedstaaten für die Durchsetzung des DSA zuständig. Gemäß Art. 49 DSA können sie hierfür mehrere nationale Stellen benennen, von denen allerdings eine Behörde als DSC zu bestellen ist. In Deutschland ist diese Stelle bei der Bundesnetzagentur angesiedelt.²⁶⁷

(1) Mitgliedstaatliche Behörden am Niederlassungsort

Für die Beaufsichtigung der Vermittlungsdienste sind die mitgliedstaatlichen Behörden nach dem Herkunftslandprinzip zuständig (Art. 56 Abs. 1 DSA). Deutsche Behörden können deshalb nur solche Vermittlungsdienste beaufsichtigen, die ihre Hauptniederlassung in der Bundesrepublik Deutschland haben. Für den hier interessierenden Untersuchungsgegenstand fallen deutsche Exekutivinstitutionen als unmittelbar zuständige Aufsichtsbehörden damit praktisch aus.

Zudem kann der DSC am Niederlassungsort gemeinsame Untersuchungen mit den DSCs am Bestimmungsort durchführen, wenn die vermuteten Verstöße gegen den DSA mehrere Mitgliedstaaten betreffen. Eine solche gemeinsame Untersuchung kann auch durch eine Empfehlung des Gremiums oder auf Verlangen eines DSC am Bestimmungsort initiiert werden (Art. 60 Abs. 1 und 2 DSA).

(2) Mitgliedstaatliche Behörden am Bestimmungsort

Die zuletzt genannte Regelung deutet an, dass die zuständigen Behörden am Bestimmungsort (also im Empfangsstaat einer Vermittlungsdienstleistung) nach dem DSA nicht zur Untätigkeit verpflichtet sind. Der DSA räumt ihnen vielmehr verschiedene Reaktionsmöglichkeiten ein, aus denen sich unterschiedliche aufsichtsrechtliche Übergabepunkte ergeben:

²⁶⁵ Erster Anwendungsfall hierfür ist die bereits erwähnte Geldbuße i.H.v. 120 Mio. € gegen X; vgl. <https://digital-strategy.ec.europa.eu/en/news/commission-fines-x-eu120-million-under-digital-services-act> (letzter Abruf: 30.4.2026).

²⁶⁶ Vgl. hierzu Art. 49 DSA.

²⁶⁷ Näher hierzu § 12 DDG.

Beschwerderechte (Art. 53 DSA)

So statuiert Art. 53 DSA ein Beschwerderecht für Nutzer sowie für jegliche Einrichtungen, Organisationen oder Vereinigungen, die mit der Wahrnehmung von Rechten unter dem DSA betraut sind (wie z. B. die „Trusted Flagger“), welches diese gegenüber dem DSC des Mitgliedstaats, in dem die Beschwerdeführer ihren Aufenthalt haben, ausüben können. Der DSC ist sodann verpflichtet, diese Beschwerde zu prüfen und ggf. an den DSC des Niederlassungsorts weiterzuleiten. Ggf. hat er die Beschwerde an eine andere zuständige Behörde in seinem Mitgliedstaat abzugeben. Die Norm statuiert folglich einen Übergabepunkt von Einrichtungen an den DSC des Bestimmungsorts und von dort an den DSC des Niederlassungsorts, nicht aber unmittelbar an die EU-Kommission.

Man wird den Wortlaut dieser Norm weit zu verstehen haben und unter die Begriffe „Einrichtungen“ oder „Organisationen“ auch andere zuständige Behörden des Bestimmungsorts – wie etwa die Landesmedienanstalten – subsumieren können. Denn auch diese sind über Art. 49 DSA i.V.m. § 12 DDG mit der Wahrnehmung von Ordnungsrechten beauftragt. Die Beschwerde muss sich dabei nach dem Wortlaut des Art. 53 DSA nicht auf den Kompetenzbereich dieser Einrichtung beschränken.

Eine Remonstrationsmöglichkeit gegen die Nichtweiterleitung einer Beschwerde existiert indes nicht. Allerdings kann sich gerade im Bundesstaat aus dem ungeschriebenen verfassungsrechtlichen Prinzip der Bundestreue eine Pflicht des nationalen DSC ergeben, Beschwerden der Landesmedienanstalten über Verstöße gegen den DSA, welche bei innerstaatlicher Betrachtung den Legislativbereich der Länder betreffen, weiterzugeben, es sei denn, der DSC kann diese Weitergabe mit sachlichen Argumenten verweigern.²⁶⁸ Gerichtlich wäre die Weiterleitung einer Beschwerde im Wege einer verwaltungsrechtlichen Leistungsklage durchzusetzen.

Zusammenarbeit der DSCs (Art. 58 DSA)

Art. 58 Abs. 1 DSA gibt dem DSC des Bestimmungsorts unter den dort genannten Voraussetzungen ferner die Möglichkeit, ein Verfahren durch den DSC des Niederlassungsorts anzustoßen. Diese Möglichkeit wird in Art. 58 Abs. 2 DSA zudem auf das Gremium erstreckt, welches unter den dort genannten Voraussetzungen durch entsprechenden Beschluss ein Prüfverfahren im Niederlassungsstaat erzwingen kann. Dieses Verfahren kann auch in eine Befassung der Kommission münden, welche den DSC am Niederlassungsort dann zu einer weitgehenden Berücksichtigung der Rechtsauffassung der Kommission verpflichtet (Art. 59 DSA). Es bestehen hier also mehrere aufsichtsrechtliche Übergabepunkte mit einem inhärenten Eskalationspotential, um der grenzüberschreitenden Zusammenarbeit zwischen den DSCs Nachdruck zu verleihen. Letztlich bleibt der DSC am Niederlassungsort jedoch in seiner Entscheidung frei.

268 Allg. zur Bedeutung der Bundestreue im europäischen Mehrebenensystem BVerfGE 92, 203 ff. – EG-Fernsehrichtlinie.

Auch hier kann aus dem Prinzip der Bundestreue eine Pflicht des deutschen DSC folgen, im Interesse der Landesmedienanstalten von den Möglichkeiten eines Verfahrens nach Art. 58 DSA Gebrauch zu machen. Insoweit gelten die vorstehenden Ausführungen entsprechend.

Zusammenarbeit mit der Kommission (Art. 65 DSA)

Mit Blick auf VLOPs und VLOSEs können die DSCs am Niederlassungs- oder Bestimmungsort schließlich unter den in Art. 65 Abs. 2 und 3 DSA genannten Voraussetzungen die Kommission auffordern, eine Prüfung gegen diese Online-Plattformen einzuleiten. Der deutsche DSC könnte auch hier nach dem Prinzip der Bundestreue verpflichtet sein, eine solche Aufforderung auf Verlangen der Landesmedienanstalten auszusprechen. Kommt die Kommission der Aufforderung nicht nach, bliebe der Bundesrepublik Deutschland nur die Möglichkeit, gemäß Art. 265 AEUV eine Untätigkeitsklage zum EuGH zu erheben. Eine solche Klage könnte unter den Voraussetzungen des § 7 Abs. 1 EUZBLG vom Bundesrat als Repräsentationsorgan der Länder in EU-Angelegenheiten erzwungen werden.

B) SONSTIGE ZUSTÄNDIGKEITEN

Ansonsten sind für den Vollzug des EMFA und der AVMD-Richtlinie die jeweiligen nationalen Behörden zuständig, in Deutschland also im Regelfall die Landesmedienanstalten.²⁶⁹

Für den Vollzug der KI-Verordnung steht die Bestimmung der innerstaatlich zuständigen Aufsichtsbehörden noch aus. Zu einer solchen wird aller Voraussicht nach die BNetzA erklärt werden.²⁷⁰ Ergänzend dazu soll durch den 1. Teil des Digitale Medien-Staatsvertrags (DMStV) für die Durchführung des Art. 5 Abs. 1 lit. a) und b) sowie des Art. 50 Abs. 1, 2, 4 und 5 KI-VO²⁷¹ die nach § 106 zuständige Landesmedienanstalt für zuständig erklärt werden, soweit Rundfunkveranstalter und Anbieter von Telemedien betroffen sind und die Aufsichtsmaßnahmen dem Schutz der Meinungsfreiheit oder Meinungsvielfalt dienen. Zudem sollen die Landesmedienanstalten für die Zusammenarbeit mit den anderen Marktüberwachungsbehörde und notifizierenden Behörde nach dem KI-MIG-E, der Europäischen Kommission und anderen Behörden im Anwendungsbereich der KI-Verordnung einen gemeinsamen Beauftragten benennen. Soweit der öffentlich-rechtliche Rundfunk betroffen ist, bezieht der nach Satz 2 benannte Beauftragte die jeweils betroffene Rundfunkanstalt in das Verfahren ein.²⁷²

269 Für den EMFA vgl. insoweit § 113a Abs. 1 7. MÄStV-E, für die AVMD-RL, die im MStV und im JSMStV umgesetzt ist, §§ 106 ff. MStV.

270 Vgl. § 2 Abs. 1 KI-MIG-E (BT-Drs. 21/4594, S. 7).

271 S. dazu bereits oben § 2 D. I. 1. c) aa) und bb).

272 So § 111 Abs. 5 des Diskussionsentwurfs für einen DMStV – Teil 1 (Stand: Juni 2025), abrufbar unter: https://rundfunkkommission.rlp.de/fileadmin/rundfunkkommission/Dokumente/DMStV_1/DMStV_Synopsen/Diskussionsentwurf_Synopse_Anhoerung_9_MAEStV.pdf (letzter Abruf: 30.4.2026). § 2 Abs. 8 S. 1 KI-MIG-E ergänzt diese Regelung aus bundesrechtlicher Perspektive.

2. NATIONALES RECHT

Im nationalen Recht ist erneut die Bundes- von der Landesebene zu trennen. Zwischen beiden Ebenen erfolgt eine Zusammenarbeit, die entsprechende Übergabepunkte kreiert.

A) BUNDESRECHT

Auf bundesrechtlicher Ebene bestehen unterschiedliche sachliche Zuständigkeiten im Umgang mit Bedrohungslagen durch Manipulationen des öffentlichen Informationsraums. Erfolgen diese Manipulationen von außen, werden sie zum Gegenstand einer Aufklärung durch den BND. Erfolgen diese Maßnahmen im Inneren, ist dies eine Zuständigkeit für den Bundesverfassungsschutz, soweit es sich um bundesweite Bedrohungslagen handelt. Die Bundes- und Landespolizeien leisten dabei ggf. Amtshilfe, falls konkrete Maßnahmen gegenüber Individuen durchgesetzt werden müssen. Die Staatsanwaltschaften der Länder schließlich sind gehalten, die seltenen Fälle von strafrechtlich relevanten Manipulationshandlungen aufzuklären und – soweit möglich – strafprozessual zu verfolgen. Zu erwähnen ist ferner die Task Force gegen Desinformation und weitere hybride Bedrohungen unter Leitung des Bundesministeriums des Innern, welche ressortübergreifend den Informationsaustausch zwischen den unterschiedlichen Behörden auf Bundes- und Landesebene organisieren und befördern soll.²⁷³

Eine besonders wichtige Stellung kommt dabei dem DSC zu, der als eine Art Bindeglied bzw. Koordinierungsstelle zwischen den nationalen Behörden (unter Einschluss der Landesmedienanstalten), der Kommission und dem Gremium fungiert. Er leitet Informationen an die EU-Kommission und/oder den zuständigen DSC innerhalb der EU weiter (z. B. Anordnungen zur Löschung rechtswidriger Inhalte gegenüber Plattformen, Beschwerden oder Hinweise zu möglichen systemischen Verstößen an die EU-Kommission und an andere nationale DSCs). Er ist zuständig für die Aufsicht und Durchsetzung des DSA gegenüber Anbietern mit Sitz oder gesetzlichem Vertreter in Deutschland sowie zentrale Beschwerdestelle für Nutzende in Deutschland.²⁷⁴

Zu betonen ist allerdings, dass der DSC keine Anordnungen zur Entfernung illegaler Inhalte erlassen kann; er übt mithin keine Inhaltskontrolle aus. Hierfür zuständig sind v.a. die Landesmedienanstalten mit Blick auf jugendgefährdende oder sonst rechtswidrige Inhalte sowie das Bundeskriminalamt mit Blick auf terroristische Online-Inhalte. Zudem bemüht sich der DSC um eine intensive Vernetzung mit allen relevanten nationalen Behörden. Auch sucht er den Austausch mit der Forschung und Zivilgesellschaft (etwa für Fragen des Datenzugangs und des Faktenchecks) und organisiert Roundtable-Gespräche (etwa zu bevorstehenden Wahlen) bzw. entwickelt „Toolboxen“, um Handreichungen für bevorstehende Bedrohungslagen zur Verfügung zu stellen. Der Aufsichtsmechanismus ist mithin durch einen stark dialogischen Ansatz geprägt, was an zumeist fehlenden eigenen Kompetenzen des DSC liegt.

²⁷³ Vgl. BfV, Gefährdung durch russische Spionage und Desinformation, MMR-Aktuell 2025, 01273.

²⁷⁴ S. hierzu bereits oben § 2 D. II. 1. a) bb).

B) LANDESRECHT

Auf der landesrechtlichen Ebene sind im Regelfall die Landesmedienanstalten gegenüber den Inhalteproduzenten bzw. Plattformen aufsichts- und handlungsbefugt. In Ausübung dieser Zuständigkeit können sie Maßnahmen bei Verstößen gegen Transparenzpflichten (§§ 18 Abs. 3, 93 MStV), journalistische Sorgfaltspflichten (§§ 6, 19 MStV) oder das algorithmische Diskriminierungsverbot ergreifen.²⁷⁵ Hierzu können sie Maßnahmen nach § 109 MStV i.V.m. Art. 6 und 9 DSA anordnen.²⁷⁶

III. ANWENDUNG DES RECHTLICHEN STATUS QUO AUF DIE FALLSTUDIEN

1. NUTZUNG VON ONLINE-PLATTFORMEN ZUR TECHNISCHEN MANIPULATION DER REICHWEITE

In diesem Fallszenario²⁷⁷ stellen sich die Aufsichtsbehörden die Frage,

- wie sie präventiv bzw. repressiv gegen manipulierende Personen bzw. ihre Verhaltensweisen (Verschleierung) vorgehen können, d.h. unter welchen Voraussetzungen dies möglich ist und wie sich das Verfahren gestaltet, insbesondere, wenn diese Personen in einem anderen EU-Mitgliedstaat oder in einem Drittstaat leben. Auch fragen sie sich, ob und wie es effektiv verhindert werden kann, dass diese Personen ggf. gesperrte Plattform-Accounts unter anderen, leicht modifizierten Namen oder Titeln, schnell wieder eröffnen können, um ihre technischen Manipulationen fortzusetzen.
 - Gegen diese Personen kann vorgegangen werden, wenn sie gegen rechtliche Verpflichtungen verstoßen. Diese Verstöße können in der Missachtung von Transparenzanforderungen (§§ 8 Abs. 3 und 7, 22 Abs. 1, 18 Abs. 3 MStV, Art. 26 DSA, Art. 50 KI-VO) liegen. Insoweit sind die Landesmedienanstalten zuständig. Gestützt auf § 109 Abs. 1 MStV könnten sie eine Beanstandungs- und Untersagungsverfügung gegenüber den manipulativ tätigen Personen erlassen. Die präventive, d.h. zukunftsgerichtete Untersagungsverfügung könnte dabei auf vergleichbare Handlungen (Einrichtung von Ersatzaccounts) erstreckt werden. Repressiv könnte das manipulative Verhalten als Ordnungswidrigkeit (§ 115 MStV) geahndet werden.
- Die Durchsetzung dieser präventiven und repressiven Maßnahmen wäre innerhalb der Bundesrepublik Deutschland oder der EU problemlos möglich. Sollten die Verursacher der manipulativen Handlungen – wie im Regelfall – ihren Sitz in Drittstaaten (China, Russland) haben, gestaltete sich ihre Durchsetzung jedoch als äußerst schwierig, wenn nicht gar unmöglich. Hier käme indes ein Vorgehen nach § 109 MStV gegen die Online-Plattformen in Betracht (dazu nachstehend).

²⁷⁵ S. hierzu bereits oben § 2 D. I. 2. c) aa).

²⁷⁶ So auch Kuhlmann/Trute, GSZ 2022, 115 (118). Räumlich ist diese Anordnung im Regelfall auf das Territorium der Bundesrepublik Deutschland beschränkt.

²⁷⁷ S. oben § 2 B. I.

- welche rechtlichen Verpflichtungen und Möglichkeiten (wie z. B. Sperren, Löschen oder Kennzeichnung) die Online-Plattformen in Bezug auf das geschilderte Verhalten haben. Auch fragen sie sich, welche rechtlichen Verpflichtungen und Möglichkeiten die Plattformen haben, um einem gezielten Missbrauch von Melde- bzw. Beschwerdesystemen durch eine automatisierte Überfrachtung zu begegnen. Zudem fragen sie sich, ob eine unzulässige unauthentische Koordination (CIB) unter Influencern oder sonstigen Personen auch dann vorliegt, wenn diese als Gegenstand einer Absprache die Reichweite ihrer Inhalte durch wechselseitiges Kommentieren, Liken, Teilen und Verlinken steigern.
 - Eine unmittelbare gesetzliche Verpflichtung zum Sperren, Löschen oder Kennzeichnen manipulierter Kommentare, Likes oder Links haben Online-Plattformen nicht. Eine Handlungsbefugnis könnte jedoch aus ihren AGB resultieren. Die Durchsetzung dieser Befugnis kann von Dritten (Privatpersonen, Aufsichtsbehörden) indes nicht unmittelbar erzwungen werden. Inhalte oder Handlungen, die lediglich gegen die AGB verstoßen, sind insbesondere keine rechtswidrigen Inhalte i.S.d. DSA.
 - Einer manipulativen Steigerung der Reichweite bestimmter (desinformativer) Inhalte kann die Plattform jedoch im Rahmen ihres Risikomanagementsystems nach Art. 34 und 35 DSA begegnen. Eine derartige Maßnahme hat tatsächliche nachteilige Auswirkungen auf gesellschaftliche Debatten und Wahlprozesse (Art. 34 Abs. 1 lit. c) DSA). Von daher sind die VLOPs und VLOSEs zur Anpassung ihrer Inholdemoderation sowie ihrer algorithmischen Systeme verpflichtet und müssen dies ggf. auch zum Gegenstand ihrer AGB machen (Art. 35 Abs. 1 lit. b) – d) DSA). Derartige Anpassungen könnten – im Rahmen des technisch Möglichen – darin bestehen, dass nicht gekennzeichnete automatisierte Kommentare, Likes oder Links von automatisierten Accounts nicht weitergeleitet oder in ihrer Reichweite reduziert werden. Bei wiederholten Verstößen gegen die Transparenzanforderungen könnte zudem eine Sperrung oder Löschung der automatisierten Accounts, von denen aus operiert wird, in Betracht kommen. Zudem bestünde die Möglichkeit, eine Kennzeichnung solcher Inhalte (etwa als automatisiert oder als Desinformation) durch andere (institutionalisierte) Nutzer zuzulassen. Da der DSA auf dem Marktortprinzip (Art. 2 Abs. 1 DSA) basiert, müssen Plattformen derartige Maßnahmen auch gegenüber solchen Personen ergreifen, die ihren Sitz außerhalb der EU haben. Den Plattformen steht bei der Wahl der Maßnahmen jedoch ein Ermessensspielraum zu, der durch das Verhältnismäßigkeitsprinzip gesteuert wird. Hierbei kommt dem Kriterium der Eignung von ergriffenen Gegenmaßnahmen besondere Relevanz zu.
 - Einem Missbrauch der Meldeverfahren durch bestimmte Personen oder Einrichtungen müssen die Plattformen nach Art. 23 Abs. 2 DSA begegnen, indem sie unter den dort genannten Voraussetzungen die Bearbeitungen von Meldungen durch die Personen oder Einrichtungen für einen angemessenen Zeitraum aussetzen. Für missbräuchlich agierende „Trusted Flagger“ gilt Vergleichbares. Zudem kann sich aus den Plattform-AGB zumindest eine Handlungsbefugnis zum Ergreifen von Maßnahmen ergeben.
 - Nutzen Influencer die transparent zu machenden algorithmischen Wirkmechanismen zur Erhöhung ihrer eigenen Reichweite, etwa indem sie verabredungsgemäß Inhalte anderer Influencer liken, teilen, verlinken oder unentgeltlich positiv kommentieren, ist hierin keine manipulative Steigerung der Reichweite zu sehen. Dies gilt auch dann, wenn sie sich hierfür automatisierter Mechanismen bedienen, solange dieses Verhalten transparent erfolgt.

- welche rechtlichen Möglichkeiten sie selbst haben, um Plattformen zur Einhaltung dieser Verpflichtungen und Möglichkeiten anzuhalten, wer insoweit zuständig ist, wie die Interaktion zwischen den öffentlichen Aufsichtsbehörden bei grenzüberschreitenden Sachverhalten erfolgt und ob die bestehenden rechtlichen Möglichkeiten zur Bekämpfung einer technischen Reichweitenmanipulation ausreichen. Insbesondere stellen sie sich die Frage, welche Faktoren die Reichweite von Posts beeinflussen und was sie rechtlich mit Blick auf die Gestaltung der von den Plattformen eingesetzten Algorithmen unternehmen können;
 - Da AGB-Verstöße (Gemeinschaftsstandards), welche ggf. eine manipulative Erhöhung der Reichweite verbieten, aufsichtsrechtlich nicht unmittelbar durchgesetzt werden können, verbleibt zunächst die Möglichkeit einer Anknüpfung an die selbstregulatorischen Verpflichtungen aus Art. 34 und 35 DSA. Für deren Einhaltung und Umsetzung ist ausschließlich die Kommission zuständig. Sie kann und muss auf entsprechende Hinweise der nationalen DSCs durch Einleitung eines Prüfverfahrens reagieren. Allerdings könnte es im Einzelfall schwierig sein, einen Verstoß der VLOPs und VLOSEs gegen das Risikomanagementsystem festzustellen, da den Plattformen – wie gesehen – sowohl bei der Risikobewertung als auch bei Risikominderung ein (weiter) Ermessensspielraum zusteht. Verbindliche aufsichtsrechtliche Maßnahmen dürften deshalb nur bei einer vollständigen bzw. teilweisen Untätigkeit oder bei einer offensichtlich fehlenden Eignung der ergriffenen Maßnahmen in Betracht kommen. Es ist deshalb damit zu rechnen, dass derartige Verfahren durch eine Verpflichtungszusage abgeschlossen werden. Momentan fehlt es indes an einer hinreichenden Vollzugspraxis, um dies abschließend beurteilen zu können.
 - Bei Verstößen gegen Transparenzvorgaben können die Plattformen, wie gesehen, nach Maßgabe der Art. 6 und 9 DSA zum Adressaten von Verfügungen durch nationale Aufsichtsbehörden werden. In Deutschland wird diese Möglichkeit über § 109 MStV eröffnet.
- ob Personen bzw. zivilgesellschaftliche Institutionen, die auf technische Manipulationen aufmerksam machen wollen, ihrerseits ausreichende und effektive Möglichkeiten haben, dies zu tun und sich gegen ein Verhalten der Plattformen zu wehren vermögen, durch das sie gesperrt und (wie z. B. aus dem YouTube-Partnerprogramm) „entmonetarisiert“ werden sollen.
 - Soweit die technische Manipulation dazu führt, dass die verbreiteten Informationen gesetzlichen Transparenzvorgaben nicht genügen, handelt es sich um rechtswidrige Inhalte. Diese sind melde- und beschwerdefähig, wobei Meldungen von privilegierten Institutionen („Trusted Flagger“) bevorzugt behandelt werden müssen. Nicht von Gesetzes wegen melde- und beschwerdefähig sind bloße Verstöße gegen die Plattform-AGB.
 - Da eine Aussetzung der Meldebefugnis eine vorherige Warnung bzw. Anhörung voraussetzt, sind meldende Personen bzw. zivilgesellschaftliche Institutionen gesetzlich ausreichend geschützt. Eine missbräuchliche Vollzugspraxis der Plattformen könnte – je nach ihrer Größe – durch die Kommission oder die nationale Behörde des Niederlassungsorts mit hinreichend scharfen Sanktionen geahndet werden. Der DSC des Bestimmungsorts kann dabei die Kommission oder die nationale Behörde des Niederlassungsorts zur Einleitung eines Prüfverfahrens auffordern; im letzteren Fall kann diese Einleitung durch das Gremium auch erzwungen werden (Art. 58 Abs. 2 DSA).

2. NUTZUNG VON ONLINE-PLATTFORMEN ZUR VERSCHLEIERUNG DES ABSENDERS

In diesem Fallszenario²⁷⁸ stellen sich die Aufsichtsbehörden die Frage,

- wie sie präventiv und repressiv gegen diese Personen bzw. ihre Verhaltensweisen (Verschleierung) vorgehen können, sprich unter welchen Voraussetzungen dies möglich ist und wie sich das Verfahren gestaltet, insbesondere, wenn diese Person in einem anderen EU-Mitgliedstaat oder in einem Drittstaat leben. Auch fragen sie sich, ob und wie effektiv verhindert werden kann, dass diese Personen ggf. gesperrte Accounts unter anderen, leicht modifizierten Namen oder Titeln, schnell wieder eröffnen können, um ihre technischen Manipulationen fortzusetzen.
 - Soweit der „Identitätsdiebstahl nicht strafbar ist, kann gegen die Missachtung der Persönlichkeits-, Namens- und Markenrechten privater Personen oder Institutionen nur zivilrechtlich vorgegangen werden. Eine Ahndung von zivilrechtlichen Verstößen wäre der Landesmedienanstalt mit Blick auf § 109 Abs. 1 MStV, der § 17 MStV (verfassungsmäßige Ordnung) explizit aus der Aufsichtsbefugnis der Landesmedienanstalten ausklammert, hingegen verwehrt. Hier müssten die Betroffenen folglich selbst den Zivilrechtsweg (Unterlassungs- und ggf. Schadensersatzklage) beschreiten.
 - Soweit sich die „Identitätsdiebe“ nicht innerhalb der Bundesrepublik Deutschland oder der EU aufhalten, dürfte sich die Durchsetzung der zivilrechtlichen Ansprüche als äußerst schwierig, wenn nicht gar unmöglich gestalten. Jedoch könnten die Betroffenen in Erwägung ziehen, die Online-Plattformen gemäß Art. 6 Abs. 1 DSA im Wege der sog. Störerhaftung auf Unterlassung in Anspruch zu nehmen. Dieser Unterlassungsanspruch bezöge sich auch auf gleichgelagerte „Identitätsdiebstähle“ in der Zukunft.
- welche Möglichkeiten die betroffenen Personen und Institutionen haben, sich gegen Instrumente der „Doppelgänger“-Kampagne zur Wehr zu setzen.
 - Insoweit kann auf die vorstehenden Ausführungen verwiesen werden.
- welche rechtlichen Verpflichtungen und Möglichkeiten die Online-Plattformen in Bezug auf das geschilderte Verhalten haben;
 - Möglicherweise erwächst den Betroffenen aus den Plattform-AGB ein vertraglicher Anspruch (ggf. als Vertrag zugunsten Dritter) zur Beseitigung und Verhinderung eines solchen „Identitätsdiebstahls“. Dieser vertragliche Anspruch müsste von den Betroffenen im Zivilrechtsweg geltend werden.
 - Der Verstoß gegen die AGB macht den „Identitätsdiebstahl“ allerdings nicht zu einem rechtswidrigen Inhalt, weshalb insoweit keine Melde- und Beschwerdeverfahren einzureichen sind. Ab Kenntniserlangung könnte die Plattform indes nach den Grundsätzen der Störerhaftung für den „Identitätsdiebstahl“ verantwortlich und dementsprechend zur Beseitigung und Unterlassung verpflichtet sein.
 - Bei einem systematischen Auftreten solcher „Identitätsdiebstähle“ griffen zudem die Verpflichtungen aus dem Risikomanagementsystem (Art. 34 und 35 DSA). Insoweit kann auf die Ausführungen sub 1. Verwiesen werden.

278 S. oben § 2 B. II.

- welche rechtlichen Möglichkeiten sie als Aufsichtsbehörden haben, um die Plattformen zur Einhaltung dieser Verpflichtungen anzuhalten, wer insoweit zuständig ist, wie die Interaktion zwischen den öffentlichen Aufsichtsbehörden bei grenzüberschreitenden Sachverhalten aussieht und ob die bestehenden Möglichkeiten ausreichen;
 - Wie gesehen, scheiden Aufsichtsmaßnahmen wegen eines „Identitätsdiebstahls“ aus. Insbesondere die Landesmedienanstalten sind hieran wegen § 109 Abs. 1 MStV, der einen Verstoß gegen § 17 MStV aus dem Spektrum zulässiger Aufsichtsmaßnahmen ausklammert, gehindert.
 - Anders könnte dies zu beurteilen sein, wenn der „Doppelgänger“ durch seine Tätigkeit gegen die Informationspflichten aus § 18 Abs. 1 und 2 MStV verstieße. Insoweit könnten die Landesmedien präventive wie repressive Maßnahmen ergreifen, wobei dieser „Anbieter“ allerdings seinen Sitz in Deutschland haben müsste. Für EU-ausländische Anbieter müsste das Verfahren nach Art. 3 Abs. 4 EC-RL bzw. Art. 3 Abs. 2 AVMD-RL eingeleitet werden. Allerdings dürfte ein solches Verfahren auf Grundlage der unionsrechtlichen Abweichungsbefugnisse nur in extremen Ausnahmefällen möglich sein. Denn die Ausnahmevorschriften der Art. 3 Abs. 4 EC-RL und Art. 3 Abs. 2 bzw. 3 AVMD-RL sind restriktiv formuliert und entsprechend restriktiv auszulegen (vgl. Erwgr. 36 und 43 AVMD-RL). Sie sind daher keine Lösung für den aufsichtsrechtlichen Alltag, sondern auf Ausnahmekonstellationen beschränkt.
 - Ansonsten muss nach den Vorgaben des DSA vorgegangen werden, wenn der „Identitätsdiebstahl“ nach dem Recht eines Mitgliedstaats rechtswidrig ist und die Plattform nicht tätig wird, um diesen Rechtsbruch zu unterlassen.
- ob Personen oder zivilgesellschaftliche Institutionen, die auf eine Verschleierung des Absenders aufmerksam machen, ihrerseits ausreichende und effektive Möglichkeiten haben, um dies zu tun und sich gegen ein Verhalten der Plattformen zu wehren, durch das sie beispielsweise gesperrt und (wie z. B. aus dem YouTube-Partnerprogramm) „entmonetarisiert“ werden;
 - Da die Verschleierung des Absenders nicht zwingend zu einem Rechtsverstoß führen muss, greifen die Melde- und Beschwerdeverfahren des DSA nicht. Die Möglichkeit, derartige Meldungen vorzunehmen, hängt deshalb von der AGB-rechtlichen Gestaltung der Plattformen ab.
 - Die Schutzmechanismen gegen Sperrungen beziehen sich ebenfalls nur auf die gesetzlich vorgeschriebenen Melde- und Beschwerdeverfahren. Insoweit könnte allerdings ein AGB-rechtlicher Schutz greifen. In diesem Kontext ist zu beachten, dass sich ggf. aus der AGB-Rechtsprechung der nationalen Zivilgerichte eine Verpflichtung ergeben könnte, meldende Personen bzw. Institutionen vor oder jedenfalls nach einer Einschränkung ihrer Meldemöglichkeiten anzuhören. Allerdings bezieht sich die bisherige Rechtsprechung lediglich auf die Sperrung bzw. Löschung von Konten²⁷⁹ und nicht auf die Einschränkung von Meldemöglichkeiten.

279 Vgl. insoweit BGH, NJW 2021, 3179 ff.

3. NUTZUNG VON KÜNSTLICHER INTELLIGENZ (DEEPPAKES)

In diesem Fallszenario²⁸⁰ stellen sich die Aufsichtsbehörden die Frage,

- wie sie präventiv und repressiv gegen diese Personen bzw. ihre Verhaltensweisen (Einsatz von Deepfakes) vorgehen können, d.h. unter welchen Voraussetzungen dies möglich ist und wie sich das Verfahren gestaltet (insbesondere, wenn die Person in einem anderen EU-Mitgliedstaat oder in einem Drittstaat lebt);
 - Sowohl der Einsatz manipulativer KI als auch die fehlende Kennzeichnung des Einsatzes von KI-Tools ist nach der KI-Verordnung verboten. Die jeweils zuständige nationale Behörde (BNetzA/Landesmedienanstalt) kann hiergegen sowohl präventiv (Untersagung) als auch repressiv (Geldbuße) vorgehen. Dabei gilt das Marktortprinzip.
 - Sitzen die Personen, welche KI-Tools nutzen, in Drittstaaten (China, Russland), ist es schwierig, wenn nicht gar unmöglich, gegen die Anbieter oder Verwender dieser Tools vorzugehen. Da es sich bei der Verwendung verbotener KI-Tools oder der fehlenden oder unrichtigen Kennzeichnung des Einsatzes solcher Tools um eine rechtswidrige Tätigkeit i.S.d. DSA handelt, können derartige Handlungsweisen gemeldet werden. Die Plattform ist dann ab Kenntniserlangung (Art. 6 DSA) zur Unterbindung dieser Verhaltensweise (etwa durch Sperrung eines Kontos oder KI-generierten Inhalts) verpflichtet. Bei nicht freiwilliger Beachtung dieser Unterlassungspflicht können – je nach Fallgestaltung – die Kommission oder die nationalen Behörden des Niederlassungsorts der Plattform aufsichtsrechtliche Maßnahmen nach dem DSA ergreifen bzw. hierzu durch die DSCs der anderen Mitgliedstaaten angehalten werden.
- welche rechtlichen Verpflichtungen oder Möglichkeiten die Online-Plattformen in Bezug auf das geschilderte Verhalten haben;
 - Die Verwendung verbotener oder nicht ordnungsgemäßer KI-Tools kann zunächst gemäß den Plattform-AGB unzulässig sein.
 - Ab Kenntniserlangung haften die Plattformen zudem nach den Grundsätzen der Störerhaftung auf Unterlassung.
 - Zudem besteht auch hier die Pflicht der VLOPs und VLOSEs, nach den Vorgaben der Art. 34 und 35 DSA eine Bewertung systemischer Risiken für den öffentlichen Diskurs durch den Einsatz von KI-Tools vorzunehmen und insoweit Risikominderungsmaßnahmen (z. B. – soweit technisch umsetzbar – in Gestalt der algorithmischen Entfernung KI-generierter Inhalte, die gegen die KI-Verordnung verstoßen) vorzuschlagen. Auf die Grenzen dieses Mechanismus wurde oben sub1. bereits hingewiesen.
- welche rechtlichen Möglichkeiten die Aufsichtsbehörden selbst haben, die Online-Plattformen zur Einhaltung dieser Verpflichtungen anzuhalten, wer insoweit zuständig ist, wie die Interaktion zwischen den öffentlichen Aufsichtsbehörden bei grenzüberschreitenden Sachverhalten aussieht und ob die bestehenden Möglichkeiten ausreichen;
 - Insoweit kann auf die Ausführungen sub 1. verwiesen werden.
 - Die Medienanstalten können unter Beachtung der Grenzen des § 109 MStV gegen die Plattformen vorgehen, wenn der KI-Einsatz zugleich § 18 Abs. 3 MStV verstößt.

280 S. oben § 2 B. III.

- in welchem Umfang es rechtlich zulässig oder sogar geboten ist, dass die Anwender von KI-Technologien (wie insbesondere Online-Plattformen, Suchmaschinen oder Large Language Models [LLMs]) softwarebasierte Instrumente einsetzen, die der Manipulation des öffentlichen Informationsraums entgegenwirken sollen. Auch fragen sie sich, wer zur Überwachung dieser Instrumente zuständig ist;
 - Der Einsatz solcher Instrumente kann nach Art. 35 DSA gerechtfertigt und sogar geboten sein, um einem von KI ausgehenden systemischen Risiko nach Art. 34 DSA entgegenzuwirken. Gemäß Art. 8 DSA müssen die Plattformen mittels KI-Tools allerdings grundsätzlich nicht proaktiv nach solchen Inhalten suchen. Diese Norm müsste aber ggf. hinter den insoweit spezielleren Art. 35 DSA zurücktreten. Gemäß Art. 7 DSA bleiben die Plattformen zudem zu freiwilligen Maßnahmen zur Bekämpfung rechtswidriger Deepfakes berechtigt. Infolge dieser Regelungssystematik aus Art. 8 und Art. 35 DSA erscheint es im Übrigen fraglich, ob der nationale Gesetzgeber den Einsatz von KI-Tools zur Bekämpfung manipulativer Einflussnahmen auf den Informationsraum verbindlich vorschreiben darf.
 - Dass die Plattformen zum Einsatz solcher Tools berechtigt sind, lässt neben Art. 7 DSA auch Art. 16 Abs. 6 S. 2 DSA erkennen, der den Einsatz automatisierter Mittel zur Bearbeitung von Beschwerden erlaubt und insoweit lediglich eine Kenntlichmachung einfordert.
- welche rechtlichen Möglichkeiten und Grenzen für einen KI-Einsatz durch die Aufsichtsbehörden selbst zwecks Bekämpfung von Manipulationen des öffentlichen Kommunikationsraums bestehen. Insbesondere fragen sie sich, ob dafür neue Rechtsgrundlagen geschaffen werden müssen;
 - Zwar erscheint eine solche Rechtsgrundlage nicht zwingend erforderlich, da die Aufsichtsbehörden im öffentlich zugänglichen Informationsraum operieren und hiervon im Regelfall keine Eingriffswirkung ausgeht.
 - Da aber nicht vollständig ausgeschlossen zu werden vermag, dass auch der rechtmäßige Einsatz von KI (etwa zur Erstellung satirischer Deepfakes) durch eine Aufsichts-KI in den Fokus behördlicher Maßnahmen geraten könnte, empfiehlt sich aus Gründen der Rechtssicherheit die Schaffung einer Rechtsgrundlage.
- welche rechtlichen Möglichkeiten sie haben, um zu verhindern, dass Institutionen (wie insbesondere feindlich gesonnene ausländische Staaten) durch gezielte (Des-)Informationskampagnen LLMs, die zunehmend anstelle klassischer Online-Suchmaschinen für die Nachrichtensuche genutzt werden, gezielt dort beeinflussen, wo die LLM-Suche auf ein Material-Defizit aus seriösen Informationsquellen stößt (sog. „LLM-Grooming“), um hierdurch falsche oder missverständliche Narrative zu generieren;
 - Insoweit bestehen nur mittelbare Möglichkeiten, etwa durch Beachtung der Anforderungen, welche die KI-Verordnung an den Einsatz von Trainings-, Validierungs- und Testdatensätze stellt (vgl. Art. 10 KI-VO). Diese könnten marktaufsichtsrechtliche Konsequenzen nach der KI-Verordnung zur Folge haben.
 - Aufgrund der Black-Box-Problematik in Bezug auf den Einsatz von Trainings-, Validierungs- und Testdatensätzen dürfte es jedoch effektiver sein, für eine plurale und ausgewogene Nachrichtengenerierung durch KI Sorge zu tragen. Hierauf wird noch zurückzukommen sein.²⁸¹

281 S. dazu nachstehend F. I. 4.

4. NUTZUNG JOURNALISTISCH-REDAKTIONELL GESTALTETER MEDIEN ZUR MANIPULATION DES ÖFFENTLICHEN INFORMATIONSRAUMS

In diesem Fallszenario²⁸² stellen sich die Aufsichtsbehörden die Frage,

- welche Möglichkeiten bestehen, die journalistisch-redaktionelle Tätigkeit eines linearen Rundfunksenders, eines nichtlinearen Online-Mediums bzw. eines Influencers aus Gründen der Wirtschaftssanktionierung zu unterbinden oder die Verbreitung eines Programms oder Kanals zu beschränken und wo insoweit rechtliche Grenzen verlaufen;
 - Eine Möglichkeit hierzu eröffnet Art. 215 AEUV, der allerdings einen einstimmigen GASP-Beschluss voraussetzt. Die Norm erlaubt zudem nur befristete Maßnahmen.
 - Grundrechtliche Grenzen dürften in dieser Konstellation zumeist keine Rolle spielen, da es um eine Sanktionierung staatlich gelenkter Medien geht.
- welche Möglichkeiten bestehen, die journalistisch-redaktionelle Tätigkeit eines linearen Rundfunksenders, eines nichtlinearen Online-Mediums bzw. eines Influencers aus Gründen der Desinformation, Misinformation oder Propaganda zu beschränken oder die Verbreitung eines Programms oder Kanals zu unterbinden und wo insoweit rechtliche Grenzen verlaufen;
 - Eine solche von außenwirtschaftsrechtlichen Sanktionen losgelöste Möglichkeit eröffnet Art. 3 Abs. 2 i.V.m. Art. 6 AVMD-RL. Da die Abweichungsbefugnisse nach Art. 3 Abs. 2 AVMD-RL infolge ihrer restriktiven tatbestandlichen Voraussetzungen und ihrer hierdurch bedingten restriktiven Interpretation jedoch auf extreme Ausnahmefälle beschränkt sind, stellt diese Rechtsgrundlage keine Lösung für den aufsichtsrechtlichen Alltag dar. Insbesondere gilt die Abweichungsbefugnis nach Art. 3 Abs. 2 und 3 i.V.m. Art. 6 AVMD-RL nur für Desinformation, Misinformation oder Propaganda, die eine ernsthafte und schwerwiegende Gefahr der Beeinträchtigung für die öffentliche Sicherheit sowie für die Wahrung nationaler Sicherheits- und Verteidigungsinteressen darstellt. Die Hürden sind mithin vergleichsweise hoch und dürften nur in seltenen Fällen überschritten werden.
 - Soweit diese Medien durch Art. 11 Abs. 2 EUGRC grundrechtlich geschützt sind, müssen diese Maßnahmen indes verhältnismäßig sein. Die wiederholte und langanhaltende Manipulation des öffentlichen Informationsraums durch demokratiezersetzende Desinformation und Propaganda dürfte sich jedoch als Abwägungsbelang zugunsten eines vorübergehenden Verbots oder einer sonstigen Tätigkeitsbeschränkung im Regelfall durchsetzen.
- welche Möglichkeiten bestehen, den Trägerverein bzw. das Trägerunternehmen eines Mediendiensteanbieters mit vereins- oder gesellschaftsrechtlichen Mitteln zu verbieten und wo insoweit rechtliche Grenzen verlaufen („Compact-Fall“);
 - Ein vereinsrechtliches Verbot durch das Bundesinnenministerium oder ein Landesministerium setzt voraus, dass sich der Trägerverein des Mediums gegen die freiheitlich-demokratische Grundordnung wendet (Art. 9 Abs. 2 GG). Dies kann auch in Form medialer Inhalte erfolgen.

282 S. oben § 2 B. IV.

- Allerdings dürfen diese Inhalte nicht durch die Meinungs- und Medienfreiheiten geschützt sein. Soweit dies nicht der Fall ist, müssen sie zudem dem Unternehmen zuzurechnen sein und die Tätigkeit des Unternehmens prägen.
 - Die Verbotsvoraussetzungen sind damit sehr streng und dürften deshalb im Regelfall kaum erfüllt werden – zumal sie durch das von einem Verbot bedrohte Medium durch eine Verhaltensanpassung leicht umgangen werden können.
- welchen journalistischen Sorgfaltsstandards Influencer unterliegen und inwieweit diese rechtlich nutzbar gemacht werden können, um gegen Desinformation, Misinformation oder Propaganda vorzugehen. Zudem fragen sie sich, welche Möglichkeiten insoweit bestehen, wenn der Influencer im (EU-)Ausland oder in einem Drittstaat sitzt;
- Influencer mit Sitz im Inland unterliegen den Anforderungen des § 19 MStV. Im Rahmen des Art. 109 Abs. 1 MStV können gegen sie deshalb aufsichtsrechtliche Maßnahmen ergriffen werden. Grundsätzlich könnte auf dieser Grundlage auch ein (vorübergehendes) Betätigungsverbot gegen einen Influencer ergehen, wenn dieser gröblich, wiederholt und langandauernd gegen die Grundsätze journalistischer Sorgfalt verstieße.
 - Für Maßnahmen gegen Influencer mit Sitz im EU-Ausland ist erneut auf die Möglichkeiten nach Art. 3 Abs. 2 bzw. 3 i.V.m. Art. 6 und Art. 6a AVMD-RL zu verweisen. Allerdings sind derartige Maßnahmen – wie vorstehend bereits ausgeführt – nur in Ausnahmekonstellationen möglich.
 - Soweit Influencer unerreichbar von einem Drittstaat aus operieren, bleibt nur die Möglichkeit, unter den Voraussetzungen des § 109 Abs. 3 MStV i.V.m. den Bestimmungen des DDG, d.h. unter Beachtung des Art. 3 E-Commerce-RL, gegen die Verbreitungsplattform mit Sitz in der EU vorzugehen.
- wann tendenziöse Beiträge in unzulässige (kostenlose) politische Werbung umschlagen, etwa die eines Influencers auf seinem Social-Media-Account zugunsten einer politischen Partei oder eines ausländischen Staates und welche rechtlichen Konsequenzen dies nach sich zieht;
- Nach den Vorgaben in § 8 Abs. 7 und Art. 1 Abs. 2 TTPW-VO ist von einer politischen (Schleich-)Werbung auszugehen, wenn dem Influencer für seine Tätigkeit ein Entgelt gezahlt oder sonst ein wirtschaftlicher oder rechtlicher Vorteil gewährt wurde.
 - Wird dies nicht offengelegt, verstößt der Influencer gegen die Kennzeichnungspflichten des Medienstaatsvertrags und der TTPW-VO. Dies kann entsprechende aufsichtsrechtliche Maßnahmen nach sich ziehen, deren Grundlage sich je danach unterscheiden, wo der Influencer seinen Sitz hat.
- welche rechtlichen Reaktionsmöglichkeiten bestehen, wenn in einem EU- oder in einem Drittstaat (wie z. B. den USA) ein Unternehmen (wie z. B. „Tenet Media“), hinter dem ein bekannter Desinformant (wie z. B. ein RT-Mitarbeiter) steht, Influencer mit Millionenbudgets anwirbt, um vor bestimmten Ereignissen (etwa Wahlen) Desinformationen und Propaganda zu verbreiten;
- Medienrechtlich handelte es sich hierbei um Schleichwerbung, die für im Inland ansässige Influencer gemäß § 8 Abs. 7 S. 1 MStV und § 22 Abs. 1 S. 1 MStV unzulässig ist. Insoweit können gestützt auf § 109 Abs. 1 MStV Beanstandungs- und Untersagungsverfügungen der jeweils zuständigen Landesmedienanstalten ergehen.

- Gemäß Art. 1 Abs. 2 TTPW-VO kann dieser Inhalt aber auch als politische Werbung i.S.d. dieser Verordnung qualifiziert werden. Die Verordnung findet unabhängig vom Sitz des Influencers nach dem Markttortprinzip Anwendung (Art. 2 Abs. 1 TTVO). Dies hat zur Folge, dass derartige Inhalte gemäß Art. 11 Abs. 1 TTPW-VO kennzeichnungspflichtig wären. Verstöße können dann von der jeweils zuständigen nationalen Behörde gerügt und mit einer Geldbuße sanktioniert werden (Art. 22 Abs. 5 lit. c) und d) TTPW-VO). Aufgrund des Erfordernisses einer medieninhaltebezogenen Prüfung sind die Landesmedienanstalten für die Durchsetzung dieser Transparenzvorgaben zuständig.²⁸³
- Befindet sich die Person im EU-Ausland, müssen sich die Landesmedienanstalt an die ausländische Vollzugsbehörde wenden.
- Für ein Agieren aus einem Drittstaat (USA, Russland, China) gilt das vorstehend zu § 109 Abs. 3 MStV Gesagte.

283 BR-Drs. 766/25, S. 25.

E. IDENTIFIKATION VON REGELUNGS- UND ZU- STÄNDIGKEITSDEFIZITEN

An diese deskriptiv-analytische Beschreibung des rechtlichen Status quo schließt sich nun eine kurze Analyse der Frage an, wo normative Regelungsdefizite und Defizite beim Vollzug bzw. der Kooperation zwischen den Vollzugsinstanzen bestehen. Diese Analyse schließt die Frage mit ein, wo zwar gesetzliche Regelungen bestehen, sich diese allerdings aus normativen oder vollzugspraktischen Gründen als nicht hinreichend wirksam erweisen. Die Untersuchung beschränkt sich dabei auf zentrale Aspekte.

I. REGELUNGSDEFIZITE

Für die normative Ebene hat die Untersuchung des Status quo folgende Regelungsdefizite identifiziert:

- Im nationalen Recht bestehen wenige tatbestandliche Anknüpfungspunkte, die eine Rechtswidrigkeit von Manipulation des öffentlichen Informationsraums begründen. Hier liegt im Verhältnis zum DSA mit seinen primär plattformbezogenen Anforderungen ein mitgliedstaatlicher Hebel zur Begründung von Rechtswidrigkeitsbeständen und dadurch bedingter Reaktionen seitens der Plattformen.
- Das Beschwerdeverfahren des Art. 16 DSA ist auf rechtswidrige Inhalte beschränkt. Rechtmäßige Inhalte, die gegen gesellschaftliche Interessen (systemische Risiken) oder gegen die Plattform-AGB (Gemeinschaftsstandards) verstoßen, können nur im Rahmen eines freiwilligen Angebots der Plattformen oder ggf. als Ergebnis einer Risikomanagementanalyse Berücksichtigung finden.
- Das System der Risikobewertung und -minderung (Art. 34 und 35 DSA), das losgelöst von einem Einzelfall in privatautonomer Verantwortung durchzuführen ist, erweist sich als eher schwerfällig und unbestimmt. Vor diesem Hintergrund ist über flankierende ordnungsrechtliche Regelungen im DSA nachzudenken.
- Zudem erscheint § 94 MStV als zu eng. Er bezieht sich lediglich auf eine algorithmische Diskriminierung journalistisch-redaktionell gestalteter Inhalte, nicht aber auf sonstige Diskriminierungen von Informations- und Meinungsbeiträgen im Kommunikationsprozess. Eine solche Diskriminierung kann aber auch durch eine Algorithmengestaltung erfolgen, die manipulativ-automatisiert „gepushte“ Inhalte begünstigt.
- KI-generierte Nachrichten unterliegen gegenwärtig keinen substanziellen inhaltlichen Anforderungen an ihre Generierung.
- Den Bundes- und Landeswahlleitern fehlt die Möglichkeit, auf Wahlen bezogene Desinformation zu untersagen bzw. die Löschung gegenüber Plattformen anzuordnen.²⁸⁴

284 Hierbei handelt es sich um einen Hinweis aus dem Interview mit der BNetzA/DSC.

- Das nationale Verwaltungsverfahrenrecht ist mit Blick auf Drittstaaten nicht hinreichend effizient, um eine Zustellung und Vollstreckung nationaler Beanstandungs- und Untersagungsverfügungen zu gewährleisten.²⁸⁵

II. ZUSTÄNDIGKEITS- UND VOLLZUGSDEFIZITE

Für die aufsichtsrechtliche Ebene lassen sich nach der Status-quo-Betrachtung folgende Zuständigkeits- und Vollzugsdefizite identifizieren:

- Die Landesmedienanstalten können in vielen Fällen Maßnahmen zur Auffindbarkeit von Public-Value-Inhalten als einem Beitrag zur Bekämpfung von Manipulationen des öffentlichen Informationsraums nicht effektiv umsetzen. Dies liegt zum einen daran, dass die Auffindbarkeitsregulierung auf Medienplattformen beschränkt ist und zum anderen an dem Umstand, dass für Regelungen wie die §§ 84 und 94 MStV zwar das Marktortprinzip (Bestimmungslandprinzip) gilt, dieses aber mit dem Herkunftslandprinzip der E-Commerce-Richtlinie im Widerspruch steht. Ob über Art. 1 Abs. 6 EC-RL diese Regelungen legitimiert werden können, ist derzeit Gegenstand eines Vorlageverfahrens beim EuGH.²⁸⁶ Für Maßnahmen der Vielfaltssicherung ist das Herkunftslandprinzip deshalb zugunsten des Marktortprinzips (Bestimmungslandprinzip) zurückzudrängen.
- Dies gilt auch für die Beaufsichtigung von Verstößen gegen den DSA. Es ist zu erwägen, das aufsichtsrechtliche Herkunftslandprinzip zugunsten des Bestimmungslandprinzips zurückzudrängen. Der DSA sollte insoweit an die Aufsichtspraxis anderer Verordnungen (wie etwa der DSGVO) angeglichen werden. Hierdurch könnten die langwierigen und komplexen behördlichen Abstimmungsverfahren im Rahmen des durch den DSA etablierten Verwaltungsverbunds vereinfacht werden. Zudem ermöglichte dies eine effektive Etablierung von Best-Practice-Beispielen.
- Bei Anträgen auf einen Forschungsdatenzugang (Art. 40 DSA) bestehen Probleme in der Umsetzung (lange Bearbeitungsdauer, unterschiedliche Ausgestaltung der Zugangsregeln durch die Plattformen, unvollständiger Datenzugang etc.). Auch die Werbearchive („Ads Repositories“) sind für Wissenschaftler teilweise schlecht zugänglich. Vor diesem Hintergrund empfiehlt sich die Prüfung, inwieweit die Durchsetzung des DSA mit Blick auf den Zugang zu Plattform- und Werbedaten optimiert werden kann, um einen schnelleren, transparenteren sowie umfassenderen Zugang zu ermöglichen und zu verhindern, dass schlecht umgesetzte Datenschnittstellen, Archive und Repositorien dringend benötigte Forschung in diesem Bereich behindern.
- Durch europäisches Wirtschaftssanktionsrecht wurde zwar unionsweit ein Betätigungsverbot gegenüber RT ausgesprochen. Allerdings fehlt es an einer zentralen Stelle (wie etwa der Kommission), die dieses Verbot unionseinheitlich durchsetzt und eine Weiterverbreitung verbotener Inhalte über Plattformen (wie z. B. X) effektiv sanktioniert.²⁸⁷

²⁸⁵ Es gilt das in der vorstehenden Fußnote Gesagte.

²⁸⁶ Vgl. hierzu m.w.N. Müller-Terpitz, AfP 2026, 99 (102, Rn. 15). Für eine solche Legitimation spricht, dass der EuGH seit neuestem in einer ähnlichen Bestimmung (Art. 1 Abs. 4 der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12.12.2006 über Dienstleistungen im Binnenmarkt) eine Bereichsausnahme zugunsten der Mitgliedstaaten sieht und diese Interpretation explizit auch auf Art. 1 Abs. 6 EC-RL erstreckt hat; vgl. EuGH, Urt. v. 18.12.2025 – C-366/24 = GRUR 2026, 252 (253 f., Rn. 29 ff., 43).

²⁸⁷ Hierbei handelt es sich erneut um einen Hinweis aus dem Interview mit der BNetzA/DSC.

F. ENTWICKLUNG VON LÖSUNGSANSÄTZEN

Lösungsansätze für die vorstehend beschriebenen Defizite lassen sich sowohl für die legislative (I.) als auch für die exekutiven Ebene (II.) formulieren.

I. LEGISLATIVE LÖSUNGSANSÄTZE

1. VERBESSERUNG VON TRANSPARENZ

Transparenz ist eine wichtige Voraussetzung, um Manipulationen des öffentlichen Informationsraums zu begegnen. Sie ermöglicht es, die Generierung und Herkunft von Informationen zuzuordnen und dies bei der individuellen Informationsverarbeitung und Meinungsbildung entsprechend zu würdigen.

Mit Blick auf die zur Manipulation von technischer Reichweite eingesetzten Social Bots genügt die gegenwärtige Fassung des § 18 Abs. 3 MStV allerdings nicht den insoweit erforderlichen Transparenzanforderungen: So bleibt nach dieser Regelung unklar, inwieweit sie für bestimmte manipulative Verhaltensweisen zur Reichweitenerhöhung (wie z. B. durch „Paid Likes“ oder „Paid Followers“) Anwendung findet.²⁸⁸ Entsprechend sollte die Regelung an die bekannten ClB-Vorgehensweisen angepasst werden. Dies böte die Möglichkeit, bei Verstößen gegen diese neugeschaffene Offenlegungspflicht präventiv und repressiv gegen die unmittelbaren Verursacher und – im Falle ihrer Nichterreichbarkeit – unter Beachtung der E-Commerce-Richtlinie und des DSA gegen die Plattformen vorzugehen. Die Länder könnten hierdurch zugleich einen Regelungsimpuls für eine unionseinheitliche Umsetzung solcher Transparenzpflichten im Rahmen des DSA setzen.

2. INHALTEBEZOGENE REGELUNGEN

Der DSA überlässt den Mitgliedstaaten bewusst die Definition dessen, was als rechtswidriger Inhalt anzusehen ist, gegen die Plattformen Maßnahmen zur Eindämmung zu ergreifen haben und die Anknüpfungspunkt aufsichtsrechtlicher Maßnahmen sein können.

Solche rechtswidrigen Inhalte können als repressive (a)) und präventive Verbote (b)) ausgestaltet werden. Wie oben²⁸⁹ bereits ausgeführt, ist das deutsche Recht mit Blick auf Manipulationen des öffentlichen Informationsraums „arm“ an solchen Verboten.

²⁸⁸ Vgl. hierzu den Vorschlag für einen § 18a MStV in der Informationsvorlage für die 353. Sitzung der DLM am 23.9.2025 in Leipzig, Anlage zu TOP 6.3.2 – Technische Manipulation des öffentlichen Informationsraums – Weiterentwicklung des Positionspapiers Desinformation – Änderungsbedarf im MStV.

²⁸⁹ § 2 E. I.

A) REPRESSIVE MASSNAHMEN

Unter repressiven Maßnahmen sind solche straf- oder ordnungswidrigkeitenrechtlicher Natur zu verstehen. Insoweit werden in der rechtswissenschaftlichen Literatur verschiedene Möglichkeiten diskutiert:

aa) Äußerungsrechtliche Verbote

Vorgeschlagen wird, Desinformation, also die bewusst oder erwiesen unwahre Tatsachenbehauptung, unter der Voraussetzung unter Strafe zu stellen, dass sie den öffentlichen Frieden zu stören geeignet ist. Dies erinnert an den auf EU-Ebene vertretenen Desinformationsbegriff.²⁹⁰ So wird etwa eine Regelung nach dem Vorbild und in Ergänzung des § 130 Abs. 3 StGB empfohlen, der schon heute mit der Billigung und Verharmlosung des NS-Unrechts einen Desinformationsstrafatbestand enthält.²⁹¹

Da – wie gesehen²⁹² – Desinformation grundrechtlich nicht geschützt ist, wäre ein solcher Straftatbestand prinzipiell zulässig. Auch verfügt die Rechtsprechung über genug Erfahrung, um einen solchen Straftatbestand grundrechtskonform im Lichte der Meinungsfreiheit oder anderer Grundrechte (wie Art. 2 Abs. 2 S. 2 GG) auszulegen. Zudem hätte diese Strafbarkeit den Vorteil, als Anknüpfungspunkt für Maßnahmen zur Entfernung rechtswidriger Inhalte auf Plattformen dienen zu können.

Diesen Vorteilen stehen allerdings auch gewichtige Nachteile gegenüber: So sind Tatsachenäußerungen – wie gesehen – häufig von Meinungsäußerungen kaum zu trennen und fallen deshalb durchaus in den Schutz der Meinungsfreiheit. Dies hinwiederum wirft schwierige Abgrenzungsfragen dahingehend auf, ob ein strafbares Verhalten vorliegt oder nicht. Zudem ist die Strafandrohung durch eine geschickte Wortwahl leicht zu umgehen.²⁹³ Auch würde so ein erheblicher Verfolgungsaufwand für die Strafverfolgungsorgane bewirkt, der ein ohnehin schon überlastetes System endgültig überfordern könnte – von bewussten Maßnahmen der Überforderung („Overload“) ganz zu schweigen. Des Weiteren dürften von einer solchen Strafandrohung „Chilling effects“ ausgehen, da schon eine unbedachte Äußerung das Risiko staatsanwaltlicher Ermittlungen oder gar einer Strafverfolgung in sich trägt. Dies wiederum widerspräche dem Ziel der Meinungsäußerungsfreiheit, sich frei und wertelloyal äußern zu können und dürfte in der Bevölkerung das Gefühl von Meinungsrepression weiter verstärken. Von diesem Instrument ist daher abzuraten.

290 S. oben § 2 A. I. 2. a).

291 Vgl. Mafi-Gudarzi, ZRP 2019, 65 (67) m.w.N. S. ferner Schlömer/Kehrberg, ZRP 2025, 2 (5).

292 S. oben § 2 C. II. 2.

293 Der Äußernde sagt nicht: „Corona existiert nicht. Geht raus, trifft Leute und habt Spaß.“, sondern er formuliert: „Es wird behauptet, Corona existiere. Ich kann das nach wie vor nicht glauben. Geht raus und habt trotzdem Spaß.“

bb) Wahlrechtliche Verbote

Anstelle des Schutzes des öffentlichen Meinungsbildungsprozesses (über einen § 130 StGB n.F.) kommt demgegenüber ein Schutz des demokratischen Willensbildungsprozesses in Betracht. So könnte § 108a StGB (Wählertäuschung) ergänzt oder ein neuer Straftatbestand geschaffen werden, der in Bezug auf die Verbreitung falscher Tatsachen, die geeignet sind, den Wählerwillen zu beeinflussen, eine Strafbarkeit vorsieht. Als Vorbild hierfür könnte der österreichische § 264 StGB dienen.²⁹⁴

Ein solcher Straftatbestand verwirklichte einen konkreten Rechtsgüterschutz – den Schutz von Wahlen als wichtigstem Element demokratischer Willensbildung –, hätte einen zeitlich eingeschränkten Anwendungsbereich (Wahlkampfzeit) und ließe sich hinreichend konkret fassen, ohne den Meinungsäußerungsprozess im Rahmen von Wahlkämpfen zu beschneiden. Ein solches Verbot wäre deshalb vorzugswürdig; es müsste aber ebenfalls rechtspolitisch gut erwogen werden. Gesetzgebungsbefugt hierfür wäre der Bundesgesetzgeber.

cc) Identitätsrechtliche Verbote

Schließlich ist mit Blick auf die Fallgruppe der Verschleierung des Absenders zu konstatieren, dass ein „Identitätsdiebstahl“ als solcher in Deutschland nicht strafbar ist, da hierfür kein eigener, spezifischer Straftatbestand existiert. Täter können lediglich über Delikte wie den Betrug (§ 263 StGB), den Computerbetrug (§ 263a StGB), das Ausspähen von Daten (§ 202a StGB) oder die Urkundenfälschung (§ 267 StGB) strafrechtlich verfolgt werden. Diese Konstellationen liegen bei „Identitätsdiebstählen“ der hier relevanten Art allerdings im Regelfall nicht vor.

Von daher könnte über einen Tatbestand nachgedacht werden, der es unter Strafe stellte, die Identität einer anderen Person oder Institution dazu zu verwenden, Kommunikationsprozesse in Täuschungsabsicht zu manipulieren, um hierdurch den öffentlichen Frieden zu stören. Das Vorgehen böte einen Anknüpfungspunkt für gefahrenabwehrende Beanstandungs- und Untersagungsmaßnahmen; eine Strafverfolgung dürfte indessen zumeist an der fehlenden Möglichkeit des Zugriffs auf die vom Ausland aus operierenden Täter scheitern.

B) PRÄVENTIVE MASSNAHMEN

aa) Allgemeines Verbot der Verbreitung von Desinformationen und der Identitätstäuschung

Ein Mittelweg gegenüber einem strafrechtlichen Verbot von Desinformation könnte darin bestehen, für Telemedien einen Tatbestand (etwa in § 17 MStV) aufzunehmen, der es diesen untersagt, schädliche Desinformation zu verbreiten. Dieser Tatbestand müsste nicht zwingend bußgeldbewehrt sein, um den Kommunikationsprozess nicht zu stark zu beeinträchtigen – eine

²⁹⁴ Vgl. Mafi-Gudarzi, ZRP 2019, 65 (68), dort auch mit weiteren strafrechtlichen Folgefragen. S. ferner Schlömer/Kehrbach, ZRP 2025, 2 (5).

Regelungstechnik, die etwa für §§ 3, 6 und 19 MStV angewandt wird. Die Landesmedienanstalten hätten dann einen Hebel, um gegen Desinformation in Form von Beanstandungs- und Unterlassungsverfügungen vorzugehen (§ 109 Abs. 1 MStV). Allerdings wäre dies zunächst auf Anbieter mit Sitz im Inland beschränkt, es sei denn, man würde über Art. 1 Abs. 6 EC-RL auch für diesen Regelungskontext eine Norm wie in § 1 Abs. 8 MStV für möglich erachten.

Zudem könnte statt eines strafrechtlichen Verbots der Identitätstäuschung auch hier über ein rein öffentlich-rechtliches Verbot (erneut ohne repressive Sanktionierung) nachgedacht werden. So könnte es etwa in § 17 MStV oder in § 18 Abs. 1 MStV verboten werden, beim Angebot eines Telemediums über die wahre Identität der Person durch Verwendung einer falschen Identität eines Dritten zu täuschen. Damit wäre auch eine Abgrenzung zur Verwendung von Pseudonymen oder einer anonymen Kommunikation gewährleistet: Bei diesen täuscht der Äußernde nicht darüber, dass er eine andere reale natürliche oder juristische Person ist, sondern gibt offen zu erkennen, dass er unerkannt bleiben möchte. Bei der Täuschung über die wahre Identität suggeriert der Handelnde indes, ein Dritter – also ein anderer – zu sein.

bb) Erweiterung des Befugnispektrums der Landesmedienanstalten

Ergänzend dazu muss das Befugnispektrum der Landesmedienanstalten erweitert werden. So ist in § 109 Abs. 1 MStV die Ausnahme für § 17 MStV zu streichen.²⁹⁵ Dies gäbe den Landesmedienanstalten die Möglichkeit, gegen Rechtsverstöße („verfassungsmäßige Ordnung“) von Telemedien mit ihrem medienrechtlichen Instrumentarium vorzugehen.

Inwieweit eine Regelung wie § 17 MStV auch auf Plattformen i.S.d. DSA erstreckt werden könnte, ist – wie gesehen – indes streitig. Da der DSA eine solche allgemeine Verpflichtung auf die verfassungsmäßige Ordnung nicht kennt, dürfte er in dieser Hinsicht einer nationalen Regelung allerdings nicht im Wege stehen. Zudem ist der Begriff des „rechtswidrigen Inhalts“ nicht zwingend auf Inhalte Dritter (wie Influencer, Social Bot-Anwender etc.) zu begrenzen. Verstöße gegen eine solche nationale Norm könnten allerdings nur im Rahmen des Kompetenzgefüges des DSA (Kommission, Behörde des Niederlassungsorts) geltend gemacht werden.

cc) Erstreckung des Staatsfernegebots auf Telemedien mit journalistisch-redaktionellem Inhalt

Darüber hinaus sind weitere Maßnahmen vorstellbar, um die Rechtswidrigkeit bestimmter Inhalte bzw. Verhaltensweisen auf mitgliedstaatlicher Ebene festzustellen und diese zum Anknüpfungspunkt (medien-)aufsichtlicher Maßnahmen zu machen. Eine solche Maßnahme könnte in der Erweiterung des Staatsfernegebots auf alle Formen digitaler Mediendienste liegen. Hierdurch würde es bspw. möglich, auch staatlich finanzierte und gelenkte Influencer oder Telemedienangebote zu untersagen. Daneben wäre darüber nachzudenken, die allgemeinen Grund-

²⁹⁵ So auch der Vorschlag der DLM in der Informationsvorlage für ihre 353. Sitzung am 23.9.2025 in Leipzig, Anlage zu TOP 6.3.2 – Technische Manipulation des öffentlichen Informationsraums – Weiterentwicklung des Positionspapiers Desinformation – Änderungsbedarf im MStV für einen neuen § 109 MStV, der zugleich ein Aufgreifermessen explizit regeln soll.

sätze nach § 3 MStV auch auf Telemedien mit journalistisch-redaktionellem Inhalt zu erstrecken, sekundiert um die materiellen Anforderungen nach § 53 MStV.²⁹⁶ Dies böte die Möglichkeit, bei groben und persistenten Rechtsverstößen derartige Telemedien in Zukunft zu untersagen („Compact-Konstellation“).²⁹⁷

Auch könnte darüber nachgedacht werden, die Regelung in Art. 6 AVMD-RL um ein europäisches Gebot der Staatsferne zu ergänzen, um effektiver gegen staatliche Propaganda vorgehen zu können. In vielen europäischen EU-Mitgliedstaaten fehlt ein solches Gebot. Für eine solche Ergänzung böte sich die laufende Evaluierung und Revision der AVMD-Richtlinie an.²⁹⁸ Ein solches Vorgehen stünde der deutschen Regelungstradition näher als der französische Ansatz, der zur Eindämmung des Phänomens staatlich gelenkter Influencer die Einführung eines Transparenzregisters vorsieht.²⁹⁹ In diesem Kontext ist auch auf die Verhandlungen um die Richtlinie zur Transparenz bei Lobbyarbeit aus Drittstaaten hinzuweisen, die sich gleichfalls auf Kommunikationskampagnen (auch über Social-Media-Influencer) erstreckt.³⁰⁰

3. PLATTFORMBEZOGENE REGELUNGEN

Zwar bietet der DSA Möglichkeiten zum Umgang mit technischen Reichweitenmanipulationen und Identitätstäuschungen. Diese Möglichkeiten erscheinen aber – wie gesehen – eher indirekt (regulierte Selbstregulierung) und schwerfällig.

Von daher wird empfohlen, den DSA nach dem Vorbild des DMA durch unmittelbar anwendbare ordnungsrechtliche Vorgaben zu ergänzen. So könnten insbesondere Verpflichtungen statuiert werden, die VLOPs und VLOSEs auch losgelöst von diagnostizierten systemischen Risiken dazu anhalten, gegen manipulative Verhaltensweisen, die von der Plattform erkannt oder dieser gemeldet wurden (CIB, Nutzung von automatisierten und nicht gekennzeichneten Bots zur Generierung von Desinformationen oder zum Setzen von Likes, Paid Likes oder Links etc.), vorzugehen. Zahlreiche Verpflichtungen aus dem Verhaltenskodex gegen Desinformation könnten so in direkte DSA-Ge- und Verbote transponiert und damit verbindlich gemacht werden. Dies hätte den Vorteil, dass aus dem reaktiv-privatautonen Risikomanagementsystem des DSA eine proaktiv-verbindliche Regulierung würde. Mit Blick auf die Bedeutung eines offenen Kommuni-

296 Vgl. hierzu den Vorschlag für einen § 2a MStV durch DLM, Anlage zu TOP 6.3.2 – Technische Manipulation des öffentlichen Informationsraums – Weiterentwicklung des Positionspapiers Desinformation – Änderungsbedarf im MStV.

297 Das derzeitige Diskussionspapier der Rundfunkkommission zum 2. Teil des DMStV (Stand: 22.10.2025), abrufbar unter: https://rundfunkkommission.rlp.de/fileadmin/rundfunkkommission/Dokumente/Beschluesse/2025_10_22_Anlage_Eckpunkte_Gesamtmatrix_DMStV_Teil_2.pdf (letzter Abruf: 30.4.2026), sieht in Ziff. 18 insoweit lediglich die Prüfung für eine Ergänzung des Bundesrechts durch Landesmedienrecht vor, um effektiv verhindern zu können, dass digitale Angebote von verbotenen Vereinigungen online abrufbar sind. Ein eigenständiger Verbotstatbestand, der kompetenzrechtlich zulässig sein dürfte, wird dort nicht erörtert.

298 In diese Richtung auch schon Ferreau, *verfassungsblog* v. 10.3.2022.

299 Näher hierzu m.w.N. Schlömer/Kehrberg, *ZRP* 2025, 2 (5 f.).

300 Vgl. hierzu den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Anforderungen im Binnenmarkt an die Transparenz der Interessenvertretung im Auftrag von Drittländern und zur Änderung der Richtlinie (EU) 2019/1937 (COM/2023/637 final) und dort ErwG Nr. 18. Da Art. 4 des Vorschlags eine Vollharmonisierung vorschreibt, ist unklar, inwieweit ein medienrechtliches Staatsfernegebot daneben Bestand haben könnte. Da die „Organisation von Kommunikations- und Werbekampagnen“ jedoch nicht als journalistisch-redaktionelle Tätigkeit aufzufassen sei dürfte, sollten sich diese Unklarheit i. Erg. ausräumen lassen.

kationsprozesses für den demokratischen Meinungsbildungsprozess wären solche Regelungen zur Bekämpfung abstrakter Gefahren grundrechtlich auch unproblematisch. Schon in der gegenwärtigen Vollzugspraxis zeigt sich deutlich (zuletzt etwa in der Verfügung gegenüber X vom Dezember 2025), dass die Kommission vor allem Verstöße gegen klar definierte DSA-Vorgaben (etwa zu den Meldesystemen, zum Datenzugang oder zur Anlage von Werbearchiven) sanktioniert, weniger indes Verstöße gegen Art. 34 und 35 DSA. Für ein solches Vorgehen wäre freilich eine Änderung des DSA von Nöten.

Bei einer solchen Änderung des DSA sollte zudem in Betracht gezogen werden, die Melde- und Beschwerdeverfahren konsequent auf Verstöße gegen die Plattform-AGB zu erweitern.

4. KI-BEZOGENE REGELUNGEN

Um zu verhindern, dass Nutzer über KI-generierte Informationen mit Relevanz für den politischen Meinungsbildungsprozess in die Irre geführt werden, sollte auf nationaler Ebene über eine Ergänzung des MStV nachgedacht werden. Diese Ergänzung könnte dergestalt konzipiert sein, dass nachrichtliche KI-Inhalte die verwendeten Quellen offenlegen müssen. Alternativ könnte erwogen werden, dass solche Inhalte nur aus behördlich anerkannten Public-Value-Inhalten generiert werden dürfen. Als Anerkennungsbehörde fungierten dann – wie auch schon bislang in Public-Value-Verfahren – die Landesmedienanstalten.³⁰¹

Ein solches Vorgehen hätte den Vorteil, dass inhaltliche Anforderungen an bestimmte KI-Produkte formuliert würden, die grundsätzlich in die Zuständigkeit der Mitgliedstaaten fallen. Sollte es sich bei dem eingesetzten KI-Dienst zugleich um eine Online-Plattform i.S.d. DSA handeln, läge bei Verstößen gegen die nationale Kennzeichnungspflicht ein rechtswidriger Inhalt i.S. dieser Verordnung vor. Dies wiederum löste den dort niedergelegten sowie bereits dargestellten aufsichtsrechtlichen Mechanismus aus.

5. STÄRKUNG DER NUTZERAUTONOMIE

Und schließlich sollte eine Stärkung der Nutzerautonomie erwogen werden. So könnten VLOPs verpflichtet werden, den Nutzern das Recht zuzugestehen, selbst darüber zu entscheiden, welche Art von Inhalten sie ausgespielt bekommen wollen. Insofern sind Design-Einstellungen vorstellbar, die es Nutzern ermöglichen, das Zuspielen bestimmter Inhalte (wie etwa nicht gekennzeichnete und automatisiert erstellte Inhalte oder adäquat gekennzeichnete Desinformation) zu unterbinden.³⁰² Eine solche Stärkung könnte auf der Grundlage des bereits existenten Risikomanagementsystems (Art. 34 und 35 DSA) erfolgen.

³⁰¹ Für weitere Vorschläge vgl. das Diskussionspapier der Rundfunkkommission zum 2. Teil des DMStV, Ziff. 4 (Stand: 22.10.2025), abrufbar über: https://rundfunkkommission.rlp.de/fileadmin/rundfunkkommission/Dokumente/Beschlusse/2025_10_22_Anlage_Eckpunkte_Gesamtmatrix_DMStV_Teil_2.pdf (letzter Abruf: 30.4.2026).

³⁰² So insbesondere eine Forderung aus den Interviews mit Correctiv und der BNetzA/DSC.

Vorstellbar wäre aber auch, entsprechend der obigen Empfehlung³⁰³ eine dahingehende Verpflichtung zur Gestaltung des Empfehlungsalgorithmus als unmittelbar wirkendes Gebot neu in den DSA aufzunehmen.

II. EXEKUTIVE LÖSUNGSANSÄTZE

Für manche der vorstehend skizzierten Defizite bietet sich schon heute eine intensivere Nutzung bereits existenter Mechanismen an – vor allem dort, wo die gesetzlichen Grundlagen (wie beim DSA oder der KI-VO) noch relativ jung sind. Hierzu zählt etwa die Verbesserung der Kooperation und des Informationsaustauschs zwischen der Kommission und den mitgliedstaatlichen Behörden sowie die Verbesserung der Kooperation und des Informationsaustauschs zwischen den DSCs und innerhalb der Aufsichtsinstanzen der Bundesrepublik Deutschland (Bund/Länder). Zudem sind die nationalen Behörden sowohl auf der Bundes- (DSC) als der Länder (Landesmedienanstalten) ausreichend mit Personal auszustatten, um eine effektive Umsetzung des bereits existenten Aufsichtsinstrumentariums zu gewährleisten.³⁰⁴

Daneben ist grundsätzlich zu erwägen, ob – jedenfalls mit Blick auf die Sicherung der Kommunikationsordnung – den Mitgliedstaaten wieder mehr eigene Vollzugskompetenzen zugestanden werden. Das derzeitige System des DSA, welches die Aufsicht bei der EU-Kommission und der nationalen Behörde des Niederlassungsorts konzentriert, ist zu hinterfragen. Andere Verordnung (wie insbesondere die DSGVO) folgen nicht nur für die materiellen Regelungen, sondern auch für die Aufsicht dem Bestimmungsortprinzip. Dies würde den Kampf gegen Manipulationen des öffentlichen Informationsraums dorthin zurückverlagern, wo er hingehörte: auf die Ebene der jeweils betroffenen Mitgliedstaaten. Ein solches System könnte durch die gremiumseitige Auferlegung von Prüfpflichten durch die nationalen Behörden sekundiert werden, um zu verhindern, dass Mitgliedstaaten ihrer Vollzugskompetenz nicht adäquat nachkommen. Für die VLOPs und VLOSEs ist nach dem Vorbild des DMA, des Wettbewerbsrechts und des Art. 56 Abs. 4 DSA eine konkurrierende Zuständigkeit zwischen der Kommission und den Behörden des Bestimmungslands in Erwägung zu ziehen mit einem „Erst-Zugriffsrecht“ der Kommission.

303 S. § 2 F. I. 3.

304 So die Forderung von bitkom im Experteninterview (allerdings beschränkt auf den DSC).

§ 3 ZUSAMMENFASSUNG

1. Das Gutachten untersucht das staatliche Reaktionsgefüge gegen Manipulationen des öffentlichen Informationsraums. Ausgangspunkt ist die These, dass gezielte Manipulationen des öffentlichen Informationsraums demokratische Meinungsbildungsprozesse untergraben und damit eine erhebliche Bedrohung für die freiheitlich-demokratische Grundordnung darstellen können. Ziel der Untersuchung ist es, bestehende rechtliche Regelungen und Zuständigkeiten im europäischen Mehrebenensystem zu analysieren, Regelungs- und Vollzugslücken zu identifizieren und darauf aufbauend Lösungsansätze zu entwickeln.
2. Der öffentliche Informationsraum wird als ein zentraler Ort gesellschaftlicher und politischer Willensbildung verstanden. Aufgrund der digitalen Vernetzung, algorithmischer Verbreitungslogiken und einer zunehmenden Fragmentierung der Medienlandschaft ist dieser Raum besonders anfällig für gezielte Einflussnahmen. Empirische Befunde und internationale Risikoanalysen belegen, dass Des- und Misinformationen sowie manipulative Kommunikationsstrategien als relevante gesellschaftliche Risiken wahrgenommen werden.
3. Das Gutachten verfolgt einen holistischen Ansatz, der unionsrechtliche, bundesrechtliche und landesrechtliche Regelungen einbezieht. Es beschränkt sich nicht auf medienrechtliche Fragestellungen, sondern berücksichtigt auch strafrechtliche, zivilrechtliche und sicherheitsrechtliche Aspekte. Diese Breite ist erforderlich, da Manipulationen des öffentlichen Informationsraums regelmäßig mehrere Rechtsgebiete und Zuständigkeiten berühren.
4. Methodisch stützt sich die Untersuchung auf eine Auswertung amtlicher Dokumente, rechts- und kommunikationswissenschaftlicher Literatur sowie auf Experteninterviews mit Vertretern von Behörden und zivilgesellschaftlichen Organisationen. Ergänzend werden realitätsnahe Fallstudien entwickelt, die typische Manipulationsszenarien abbilden und als Grundlage für die rechtliche Analyse dienen.
5. Zentraler begrifflicher Ausgangspunkt ist die „Manipulation des öffentlichen Informationsraums“. Dieser von den Landesmedienanstalten geprägte Begriff ist bewusst inhaltsneutral angelegt und fokussiert nicht auf die Wahrheit oder Unwahrheit einzelner Inhalte, sondern auf die verdeckte und unredliche Verzerrung von Kommunikationsprozessen mit dem Ziel der Beeinflussung individueller und kollektiver Meinungsbildung.
6. Manipulationen können dabei insbesondere in zwei Grundformen auftreten: erstens durch die technische Manipulation der Reichweite bestimmter Inhalte und zweitens durch die Verschleierung oder Täuschung über die Identität des Absenders. Beide Formen zielen darauf ab, bei den Rezipienten eine falsche Vorstellung über Relevanz, Zustimmung oder Autorität von Informationen zu erzeugen.
7. Die Reichweitenmanipulation erfolgt häufig durch automatisierte Verfahren wie Bots, durch gekaufte Interaktionen und/oder durch ein koordiniertes unauthentisches Verhalten (Coordinated Inauthentic Behavior – CIB). Nutzer können dabei regelmäßig nicht erkennen, dass die wahrgenommene Popularität eines Inhalts technisch erzeugt wurde. Diese Intransparenz stellt eine wesentliche Täuschung dar, da sie die Fähigkeit der Rezipienten zur eigenständigen Bewertung der Relevanz von Informationen beeinträchtigt.

8. Die Verschleierung des Absenders nutzt gezielt das Vertrauen in bekannte Personen, Institutionen oder Medienmarken aus. Typische Erscheinungsformen sind gefälschte Social-Media-Accounts, imitierte Medienangebote, manipulierte Webseiten oder Deepfakes (z. B. „Doppelgänger“-Kampagne). Auch diese Praktiken beruhen auf Täuschung und unterscheiden sich grundlegend von offener, authentischer Kommunikation.
9. Der Begriff der Manipulation grenzt sich bewusst von inhaltsbezogenen Begriffen wie Desinformation, Misinformation, „Fake News“ oder Propaganda ab. Diese Begriffe knüpfen an den Wahrheitsgehalt von Informationen an und sind juristisch häufig unscharf oder politisch aufgeladen. Insbesondere der Begriff „Fake News“ erweist sich als ungeeignet für eine rechtliche Analyse.
10. Desinformation wird als vorsätzliche Verbreitung nachweislich falscher oder irreführender Informationen mit Schädigungspotenzial verstanden. Misinformation bezeichnet demgegenüber unbeabsichtigte Falschinformationen ohne Täuschungsabsicht. Propaganda ist durch ein instrumentelles Verhältnis zur Wahrheit gekennzeichnet und kann sowohl wahre als auch falsche Informationen umfassen.
11. Der Vorteil des inhaltsneutralen Manipulationsbegriffs liegt darin, dass staatliche Maßnahmen nicht an der Bewertung einzelner Inhalte ansetzen müssen. Dadurch lassen sich Zensurvorfälle vermeiden und die Akzeptanz regulatorischer Eingriffe erhöhen. Zugleich ermöglicht dieser Ansatz ein effektiveres Vorgehen gegen kampagnenartige, systematische Verzerrungen des Diskurses.
12. Neben technischen Manipulationen berücksichtigt das Gutachten auch inhaltliche und gestalterische Aspekte. Manipulationen können durch Texte, Bilder, Videos, Memes oder Audioformate erfolgen und zunehmend unter Einsatz Künstlicher Intelligenz (KI) produziert werden. Deepfakes nehmen dabei eine besondere Stellung ein, da sie Authentizität vortäuschen und schwer zu erkennen sind.
13. Zur Konkretisierung der Problemlagen entwickelt das Gutachten vier Fallstudien: die Nutzung von Online-Plattformen zur technischen Manipulation der Reichweite, die Nutzung von Online-Plattformen zur Verschleierung des Absenders, die Nutzung von KI (Deepfakes) sowie die Nutzung journalistisch-redaktioneller Medien zur Manipulation des öffentlichen Informationsraums. Diese Fallstudien verdeutlichen typische rechtliche und institutionelle Herausforderungen.
14. Die Fallstudien zeigen, dass Manipulationen häufig grenzüberschreitend erfolgen und Akteure aus Drittstaaten involviert sind. Dadurch entstehen komplexe Zuständigkeitsfragen, insbesondere im Verhältnis zwischen nationalen Behörden, EU-Institutionen und Plattformbetreibern. Auch der Missbrauch von Melde- und Beschwerdesystemen wird als relevantes Problem identifiziert.
15. Der rechtliche Rahmen zur Bekämpfung von Manipulationen des öffentlichen Informationsraums ist durch ein Mehrebenensystem geprägt. Auf EU-Ebene bestehen keine umfassenden ausschließlichen oder geteilten Kompetenzen zur Wahrnehmung dieser Aufgabe, wohl aber begrenzte Zuständigkeiten wie im Bereich der Gemeinsamen Außen- und Sicherheitspolitik und des Binnenmarkts.
16. Eine besondere Rolle spielt Art. 215 AEUV, der als Grundlage für wirtschaftliche Sanktionen gegen Drittstaaten und Akteure dient. Auf dieser Basis wurden unter anderem Verbreitungsverbote für russische Staatsmedien wie „Russia Today“ erlassen. Diese Maßnahmen sind kompetenzrechtlich zulässig, bleiben jedoch auf Ausnahmekonstellationen (Konflikt mit einem Drittstaat) beschränkt und sind zeitlich begrenzt.

17. Der Schwerpunkt der unionsrechtlichen Regulierung liegt deshalb auf den geteilten Zuständigkeiten, und dort insbesondere auf der Binnenmarktkompetenz aus Art. 114 AEUV. Auf dieser Grundlage wurde der Digital Services Act (DSA) erlassen, der für Online-Plattformen zentrale Pflichten zur Bekämpfung illegaler und manipulativer Inhalte vorschreibt.
18. Auf nationaler Ebene ist die Gesetzgebungskompetenz zwischen Bund und Ländern verteilt. Der Bund verfügt über Zuständigkeiten im Straf-, Vereins- und Sicherheitsrecht, während die Länder insbesondere für das Medienrecht und die Medienaufsicht zuständig sind. Diese Kompetenzverteilung führt zu Abgrenzungs- und Koordinationserfordernissen.
19. Die Länder können medienrechtliche Vorgaben zu journalistischen Sorgfaltspflichten, Transparenz- und Kennzeichnungspflichten sowie für die Gestaltung algorithmischer Systeme erlassen. Allerdings bestehen Unsicherheiten hinsichtlich der Vereinbarkeit nationaler Regelungen mit dem DSA, die einer gerichtlichen Klärung harren.
20. Die Bekämpfung von Manipulationen des öffentlichen Kommunikationsraums unterliegt strengen grundrechtlichen Grenzen. Meinungs- und Medienfreiheit sind sowohl nach dem Grundgesetz, nach der Europäischen Menschenrechtskonvention (EMRK) als auch nach der EU-Grundrechtecharta geschützt. Gleichzeitig ist anzuerkennen, dass der Staat im Sinne einer „wehrhaften Demokratie“ nicht verpflichtet ist, manipulative Angriffe schutzlos hinzunehmen.
21. Die grundrechtlichen Grenzen der Bekämpfung von Manipulationen des öffentlichen Informationsraums sind durch einen normativen Gleichlauf dieser Grundrechtsregime im Mehrebenensystem gekennzeichnet. Dies betrifft schon die Frage, ob der Schutzbereich eines Kommunikationsgrundrechts überhaupt eröffnet ist; jedenfalls aber bezieht sich dieser Gleichlauf auf den effektiven Gewährleistungsgehalt dieser Grundrechte. Mit grundrechtlichen Wertungskonflikten in Bezug auf hoheitliche Maßnahmen zur Bekämpfung von Manipulationen des öffentlichen Informationsraums ist deshalb nicht zu rechnen.
22. Die Untersuchung zeigt des Weiteren, dass sowohl nach dem nationalen als auch nach dem europäischen Grundrechtsschutz manipulative Verhaltensweisen im hier verstandenen Sinne zumeist keinen Schutz durch die Kommunikationsgrundrechte erfahren. Entweder fehlt es an der Eröffnung des personellen Schutzbereichs, da grundrechtlich nicht geschützte staatliche oder staatlich gelenkte Akteure am Werke sind. Oder der materielle Schutzbereich lässt sich nicht auf manipulative Verhaltensweisen erstrecken, so wie insbesondere im Fall von Desinformation.
23. Dort, wo manipulative Maßnahmen ausnahmsweise Schutz genießen, verbleiben dem nationalen und unionalen Gesetzgeber bei ihrer Bekämpfung große Gestaltungsspielräume. Der Schutz eines offenen, unverzerrten Kommunikationsprozesses rechtfertigt weitreichende Einschränkungen. Diese sind im Wesentlichen nur dem Verhältnismäßigkeitsprinzip unterworfen. Ob diese Schranken-Schranke beachtet wird, bedarf einer Betrachtung des Einzelfalls.
24. Die ausführliche Analyse des einfachrechtlichen Status quo zeigt, dass mit dem DSA, der KI-Verordnung, dem European Media Freedom Act (EMFA) und den nationalen Regelungen ein breites rechtliches Handlungsinstrumentarium existiert. Insbesondere der DSA stellt zahlreiche rechtliche Anknüpfungspunkte für die Bekämpfung von Manipulationen des öffentlichen Informationsraums bereit. Diese beziehen sich teils auf rechtswidrige Inhalte und Verhaltensweisen; teils erfassen sie aber – wie die AGB-Gestaltung oder das

Risikomanagementsystem – auch Inhalte und Verhaltensweisen unterhalb der Rechtswidrigkeitsschwelle. Teils beinhalten die Regelungen klare ordnungsrechtliche Vorgaben (wie etwa die Pflicht zur Einrichtung eines Meldesystems oder zur Herstellung von Transparenz über die eingesetzten Empfehlungsalgorithmen), teils aber auch nur Vorgaben in Gestalt einer regulierten Selbstregulierung, um losgelöst von Einzelfällen abstrakt-generelle Lösungen für komplexe Risikoszenarien zu finden.

25. Gleichwohl bestehen erhebliche Regelungs- und Vollzugslücken, so insbesondere bei der Durchsetzung von Pflichten gegenüber ausländischen Akteuren, die nicht in einem EU-Staat ansässig sind, sowie gegenüber sehr großen Online-Plattformen. Insoweit hat die Kommission bislang nur vereinzelt Verstöße gegen die skizzierten Vorgaben angenommen. Da der DSA aber erst seit knapp zwei Jahren in der Anwendung ist, darf mit weiterer Vollzugserfahrung (und darauf bezogener Judikatur) gerechnet werden.
26. Defizite zeigen sich zudem in der Koordination zwischen Behörden sowie in der praktischen Durchsetzung bestehender Pflichten. Unterschiedliche Zuständigkeiten und begrenzte Ressourcen erschweren ein effektives Vorgehen gegen systematische Manipulationen des öffentlichen Informationsraums.
27. Als legislative Lösungsansätze schlägt das Gutachten deshalb unter anderem eine Stärkung von Transparenzpflichten beim Einsatz von Social Bots, gezielte inhaltsbezogene Verbote mit klaren Tatbeständen, die den Schutz des demokratischen Willensbildungsprozesses verbessern sollen, eine Erweiterung der Befugnisse der Landesmedienanstalten sowie eine Erstreckung des Staatsfernegebots auf alle Formen digitaler Mediendienste vor. Plattformbezogene Regelungen, die das derzeitige System der regulierten Selbstregulierung zu klaren Ge- und Verboten fortschreiben, sowie eine regulatorische Stärkung der Nutzerautonomie werden ebenfalls als zentrale Hebel identifiziert.
28. Für die exekutive Ebene empfiehlt das Gutachten eine intensivere Kooperation zwischen nationalen und europäischen Behörden, den Ausbau technischer Kompetenzen sowie klarere Eskalations- und Übergabestrukturen. Nur durch ein koordiniertes Vorgehen lässt sich die Manipulation des öffentlichen Informationsraums wirksam eindämmen.
29. Zusammenfassend kommt das Gutachten zu dem Ergebnis, dass Manipulationen des öffentlichen Informationsraums eine reale und wachsende Gefahr für demokratische Gesellschaften darstellen. Die bestehenden rechtlichen Instrumente bilden eine wichtige Grundlage, reichen ohne gezielte Weiterentwicklung und effektivere Durchsetzung aber nicht aus, um dieser Herausforderung nachhaltig zu begegnen.

ANHANG*

INSTITUTION	DATUM
Correctiv	04.09.2025
EU-Kommission (DG Connect)	08.09.2025
BITKOM	16.09.2025
CeMas	29.09.2025
BNetzA/DSC	29.09.2025
BMI/Task Force Desinformation	11.11.2025

* Unternehmen aus der Plattformökonomie, die zu den VL0Ps und VL0SEs zählen, würde ebenfalls Gelegenheit für ein Interview gegeben. Solche Interviews kamen allerdings nicht zustande.

LITERATUR

- Andree, Martin*, Krieg der Medien. Dark Tech und Populisten übernehmen die Macht, 2025.
- Aust, Helmut*, Spionage im Zeitalter von Big Data: Globale Überwachung und der Schutz der Privatsphäre im Völkerrecht, Archiv des Völkerrechts (AVR), Bd. 52, 2014, 375 ff.
- Baade, Björnstjern*, Das Verbot der Kriegspropaganda im Recht der Europäischen Union, EuR 2020, 653 ff.
- Baade, Björnstjern*, The EU's "Ban" of RT and Sputnik, verfassungsblog v. 8.3.2022.
- Binder, Reinhart/Vesting, Thomas* (Hrsg.), Beck'scher Kommentar zum Rundfunkrecht. Medienstaatsvertrag, Jugendmedienschutz-Staatsvertrag, Rundfunkbeitragsstaatsvertrag, Rundfunkfinanzierungsstaatsvertrag, 5. Aufl. 2024 (zitiert: *Bearbeiter*, in: *Binder/Vesting, Beck'scher Kommentar zum Rundfunkrecht*).
- bitkom*, Policy Brief. Maßnahmen gegen Desinformation & Deepfakes im Superwahljahr 2024.
- Brauneck, Jens*, EU-Desinformationsbekämpfung durch Google, Facebook u. a. unter Androhung von Gesetzen, EU-Außenpolitik durch Gegenpropaganda in Drittstaaten?, EuR 2020, 89 ff.
- Brosius-Gersdorf, Frauke/Gersdorf, Hubertus*, Medienverbote nach dem Vereinsgesetz. Zum COMPACT-Beschluss des BVerwG, NVwZ 2024, 1697 ff. *Calliess, Christian/Ruffert, Matthias* (Hrsg.), EUV/AEUV. Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, 6. Aufl. 2022 (zitiert: *Bearbeiter*, in: *Calliess/Ruffert, EUV/AEUV*).
- Cremer, Wolfram*, Der Schutzbereich der grundgesetzlichen Meinungsfreiheit. Zur Konzeptionierung einer dogmatisch fundierten Neuausrichtung, NVwZ 2023, 1463 ff.
- Dörr, Oliver/Grote, Rainer/Marauhn, Thilo* (Hrsg.), GG/EMRK, Konkordanzkommentar zum europäischen und deutschen Grundrechtsschutz In zwei Bänden, 3. Aufl., 2022 (zitiert: *Bearbeiter*, in: *Dörr/Grote/Marauhn, GG/EMRK*).
- Dreier, Horst* (Hrsg.), Grundgesetz, Bd. I, 4. Aufl. 2023 (zitiert: *Bearbeiter*, in: *Dreier, GG*).
- Dürig, Günter/Herzog, Roman/Scholz, Rupert* (Hrsg.), Grundgesetz, 108. EL August 2025 (zitiert: *Bearbeiter*, in: *Dürig/Herzog/Scholz, GG*).
- Epping, Volker/Hillgruber, Christian* (Hrsg.), BeckOK Grundgesetz, 64. Edition, Stand: 15.11.2025 (zitiert: *Bearbeiter*, in: *Epping/Hillgruber, BeckOK-GG*).
- Ferreau, Frederik*, Desinformation als Herausforderung für die Medienregulierung, AfP 2021, 204 ff.
- Ferreau, Frederik*, Präventiver Verfassungsschutz durch Verbote von Medien? Zugleich Kommentar zu BVerwG, Beschluss vom 14. 8. 2024 – 6 VR 1.24, K&R 2024, 777 ff.
- Flamme, Florian*, Erneuter Vorwurf der Begünstigung von Desinformation gegen YouTube, MMR-Aktuell 2022, 444970.

- Gehring, Ferdinand*, Einblicke in globale Desinformations- und Propagandastrategien, NJ-Beilage 2024, B-18 ff.
- Gersdorf, Hubertus/Paal, Boris* (Hrsg.), BeckOK Informations- und Medienrecht, 50. Edition, Stand: 1.11.2025 (zitiert: *Bearbeiter*, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht).
- Grabenwarter, Christoph/Pabel, Katharina*, Europäische Menschenrechtskonvention, 7. Aufl. 2021.
- Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin* (Hrsg.), Das Recht der Europäischen Union, Werkstand: 86. EL September 2025 (zitiert: *Bearbeiter*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union).
- Grimm, Dieter*, Die Meinungsfreiheit in der Rechtsprechung des Bundesverfassungsgerichts, NJW 1995, 1697 ff.
- Heidtke, Aron*, Meinungsbildung und Medienintermediäre. Vielfaltssichernde Regulierung zur Gewährleistung der Funktionsbedingungen freier Meinungsbildung im Zeitalter der Digitalisierung, 2020.
- Heintschel-Heinegg von, Bernd/Kudlich, Hans* (Hrsg.), BeckOK StGB, 67. Edition Stand: 1.11.2025 (zitiert: *Bearbeiter*, in: von Heintschel-Heinegg/Kudlich, BeckOK StGB).
- Hofmann, Franz/Raue, Benjamin* (Hrsg.), Digital Services Act. Gesetz über digitale Dienste, 2023 (zitiert: *Bearbeiter*, in: Hofmann/Raue, DSA).
- Holznagel, Bernd*, Phänomen „Fake News“ – Was ist zu tun? Ausmaß und Durchschlagskraft von Desinformationskampagnen, MMR 2018, 18 ff.
- Hong, Mathias*, Hassrede und extremistische Meinungsäußerungen in der Rechtsprechung des EGMR und nach dem Wunsiedel-Beschluss des BVerfG, ZaöRV 2010, 73 ff.
- Jarass, Hans D.*, Charta der Grundrechte der Europäischen Union unter Einbeziehung der sonstigen Grundrechtsregelungen des Primärrechts und der EMRK, 4. Aufl. 2021.
- Kalbhenn, Jan Christopher*, Designvorgaben für Chatbots, Deepfakes und Emotionserkennungssysteme: Der Vorschlag der Europäischen Kommission zu einer KI-VO als Erweiterung der medienrechtlichen Plattformregulierung, ZUM 2021, 663 ff.
- Kalbhenn, Jan Christopher*, Plattformregulierung als politische Aufgabe der Zeit. Sicherung der Medienvielfalt durch Public Open Space, ZRP 2025, 111 ff.
- Karpenstein, Ulrich/Mayer, Franz C.* (Hrsg.), Konvention zum Schutz der Menschenrechte und Grundfreiheiten, 3. Aufl. 2022 (zitiert: *Bearbeiter*, in: Karpenstein/Mayer, EMRK).
- Kastor, Niklas E./Püschel, Hanna*, Faktenchecker vor dem Hintergrund des Digital Services Act. Eine rechtliche Einordnung, K&R 2023, 20 ff.
- Kuhlmann, Simone/Trute, Hans-Heinrich*, Die Regulierung von Desinformationen und rechtswidrigen Inhalten nach dem neuen Digital Services Act, GSZ 2022, 115 ff.

- Köster, Niklas E./Püschel, Hanna, Faktenchecker vor dem Hintergrund des Digital Services Act, K&R 2023, 20 ff.
- Kluth, Winfried/Schulz, Wolfgang, Konvergenz und regulatorische Folgen. Gutachten im Auftrag der Rundfunkkommission der Länder, 2014.
- Ladeur, Karl-Heinz, Netzwerkgerechte Regulierung: Exempel „Kuratieren“ von Medieninhalten und Kampf gegen „Desinformation“, K&R 2024, 477 ff.
- Löbig, Lena Isabell/Roßnagel, Alexander, in: Steinebach/Bader/Rinsdorf/Krämer/Roßnagel (Hrsg.), Desinformation aufdecken und bekämpfen. Interdisziplinäre Ansätze gegen Desinformationskampagnen und für Meinungspluralität, 2020, S. 149 ff.
- Mafi-Gudarzi, Nima, Desinformation: Herausforderung für die wehrhafte Demokratie, ZRP 2019, 65 ff.
- Masing, Johannes, Einheit und Vielfalt des Europäischen Grundrechtsschutzes, JZ 2015, 477 ff.
- Mehlan, Amelie, Online-Werbung – Wie Victor Orban Desinformation über YouTube in Europa verbreitet, MMR-Aktuell 2024, 01416.
- Meyer-Ladewig, Jens/Nettesheim, Martin/Raumer von, Stefan (Hrsg.), EMRK. Europäische Menschenrechtskonvention, 5. Aufl. 2023 (zitiert: *Bearbeiter*, in: Meyer-Ladewig/Nettesheim/Raumer, EMRK).
- Möller, Thomas, Der grundrechtliche Schutzbereich der Meinungsfreiheit in Deutschland, England und den USA, 2016.
- Müller, Stephan, 20. Frankfurter Medienrechtstage 2024 – Strategien gegen Desinformation und Propaganda, NJ 2024, 216 ff.
- Müller-Terpitz, Ralf, (Un-)Level Playing Field im Medienbereich, Juristisches Gutachten im Auftrag der Landesanstalt für Medien NRW, Juni 2025.
- Müller-Terpitz, Ralf, (A-)Symmetrie der Regulierung von Plattformen und Medien – Augenhöhe oder David gegen Goliath?, AfP 2026, 99 ff.
- Müller-Terpitz, Ralf/Köhler, Markus (Hrsg.), Digital Services Act, 2024 (zitiert: *Bearbeiter*, in: Müller-Terpitz/Köhler, DSA).
- Münch von, Ingo/Kunik, Philip (Hrsg.), Grundgesetz, Bd. 1, 8. Aufl. 2024 (zitiert: *Bearbeiter*, in: von Münch/Kunig, GG).
- Nielsen, Jan, Die Medienvielfalt als Aspekt der Wertesicherung der EU, 2019.
- Oster, Jan, Künstliche Intelligenz und Vielfaltssicherung, AfP 2024, 285 ff.
- Peukert, Alexander, Desinformationsregulierung in der EU – Überblick und offene Fragen, JZ 2023, 278 ff.
- Pille, Jens-Ullrich, Meinungsmacht sozialer Netzwerke, 2016.
- Roß, Leo, Grundrechtsschutz im Kooperationsverhältnis von BVerfG und EuGH, JZ 2025, 651 ff.

- Roth-Isigkeit, David*, Ordnung von Kommunikationsräumen und Medien, DVBl. 2025, 1059 ff.
- Sachs, Michael* (Begr.), Grundgesetz, 10. Aufl. 2024 (zitiert: Bearbeiter, in: *Sachs, GG.*)
- Schefzig, Jens/Kilian, Robert* (Hrsg.), BeckOK KI-Recht, 4. Edition Stand: 1.11.2025 (zitiert: *Bearbeiter*, in: *Schefzig/Kilian, BeckOK KI-Recht*).
- Schlömer, Jan/Kehrberg, Stefan*, Demokratien unter Druck: Wie Desinformation Wahlen beeinflusst, ZRP 2025, 2 ff.
- Schmidt, Maximilian Mike Joshua*, Uploadfilter: Zensur im 21. Jahrhundert?, 2026.
- Setz, Tahireh/Seyda, Linda*, Der Umgang der EU mit Propaganda und Desinformation russischer Staatsmedien in Zeiten des Ukrainekriegs, ZD-Aktuell 2022, 01167.
- Spindler, Gerald/Schuster, Fabian/Kaesling, Katharina* (Hrsg.), Recht der elektronischen Medien, 5. Aufl. 2026 (zitiert: *Bearbeiter*, in: *Spindler/Schuster/Kaesling, Recht der elektronischen Medien*).
- Schwartmann, Rolf*, Anwendungsszenarien und Rechtsrahmen für den Einsatz künstlicher Intelligenz im Journalismus, AfP 2024, 1 ff.
- Waegner, Hannah*, Umfrage zu Desinformation: Junge Menschen und TikTok-Nutzer besonders empfänglich, MMR-Aktuell 2025, 01147.
- Wagner, Eva Ellen*, Die unionsrechtlichen Vorgaben für die Reform des öffentlich-rechtlichen Rundfunks in Deutschland, in: Stiftung Gesellschaft für Rechtspolitik/Institut für Rechtspolitik (Hrsg.), Bitburger Gespräche, Jahrbuch 2024, S. 41 ff.
- Warg, Gunter*, Meinungsfreiheit zwischen Zensur und Selbstzensur, DÖV 218, 473 ff.

IMPRESSUM

Herausgeberin

Landesanstalt für Medien NRW
Zollhof 2
40221 Düsseldorf

T +49 211 77007-0

F +49 211 727170

info@medienanstalt-nrw.de

www.medienanstalt-nrw.de

Direktor: Dr. Tobias Schmid

Verantwortlich

Marie-Franca Hesse (Leiterin Kommunikation)

Dr. Meike Isenberg (Leiterin Intermediäre und Forschung)

Durchführende Person

Prof. Dr. iur. Ralf Müller-Terpitz