

# Kommunikative Gefahren im Online-Umfeld: Neue Herausforderungen des digitalen Raums für eine wehrhafte Demokratie

Jan-Ole Harfst, Hamburg\*

*Der Beitrag widmet sich der Frage nach der Wehrhaftigkeit der deutschen Demokratie gegenüber den neuen kommunikativen Gefahren des Internets, insbesondere der Online-Verbreitung von Desinformation und Hass. Nach einem Überblick über die historische Konzeption wird die wehrhafte Demokratie des Grundgesetzes den heutigen Herausforderungen des digitalen Raumes gegenübergestellt und eine diesbezüglich fehlende Passung erörtert. Erweitert man das Konzept jedoch um alle Normen, die dem Schutz des Diskurses und der demokratischen Institutionen dienen, stehen weitere Verteidigungsinstrumente des einfachen Rechts zur Verfügung, deren Effektivität auch in Bezug auf ein Mitwirken des Einzelnen diskutiert wird. Schließlich wird die Notwendigkeit einer Regulierung von Online-Plattformen betont, welche angesichts der globalen Bedrohungslage nicht durch einzelne Staaten allein erfolgen kann und in der Konsequenz einen Übergang vom nationalen zum supranationalen Demokratieschutz erfordert. Insbesondere der Digital Services Act als neue EU-Verordnung bietet dabei vielversprechende Ansätze für eine angemessen wehrhafte Demokratie im digitalen Raum.*

Der Schutz der Demokratie darf sich nicht auf bewährte Verteidigungsmechanismen verlassen, sondern erfordert kontinuierliche Modernisierungen, um auch nie zuvor dagewesenen Gefahren angemessen begegnen zu können. Die hohe Geschwindigkeit, mit der sich neue Bedrohungen realisieren können, hat in den letzten Jahren dabei wohl nichts so öffentlichkeitswirksam gezeigt wie die zunehmend als Gefahr wahrgenommenen Möglichkeiten der Verengung und Manipulation des Diskurses im digitalen Raum: Neben stetig neuen Anwendungsstrategien (Fake-News-Kampagnen, Hashtag-Hijacking etc.) ermöglicht auch der kontinuierliche technische Fortschritt, insbesondere in Bezug auf generative KI, eine fortwährende Anpassungsfähigkeit gegenüber möglichen Schutzmechanismen und stellt eine Verteidigung damit vor durchgehend präzedenzlose Situationen. In der Folge sind Desinformation und digitaler Hass zu einem ständigen Inhalt des undurchsichtigen, algorithmisch-kuratierten Feeds von Online-Plattformen wie Facebook, Instagram, X, TikTok und

Co. geworden.<sup>1</sup> Zwar ist in Deutschland das Prinzip einer „streitbaren“ bzw. „wehrhaften“ Demokratie<sup>2</sup> verfassungsrechtlich verankert<sup>3</sup> – aber kann das Verteidigungsarsenal des Grundgesetzes auch den heutigen kommunikativen Gefahren im Online-Umfeld gerecht werden? Um diese Frage zu beantworten, sollen zuerst die historische Grundidee der wehrhaften Demokratie und ihre Rezeption im Grundgesetz skizziert werden, um sie anschließend den heutigen Herausforderungen des digitalen Raumes gegenüberzustellen.

## A. Historische Konzeptionen

Dabei ist zunächst hervorzuheben, dass die wehrhafte Demokratie als umfassendes Konzept eine relativ junge Entwicklung darstellt – jedenfalls im Verhältnis zur beachtlichen Historie der Staatsform an sich: Auch wenn einzelne Aspekte bzw. Mittel der wehrhaften Demokratie eine längere Entwicklungsgeschichte aufweisen, fanden die ersten Entwicklungen eines ganzheitlichen Konzepts in der ersten Hälfte des 20. Jahrhunderts statt und werden dem Staatsrechtler *Karl Loewenstein* und im Deutschen begriffsprägend dem Soziologen *Karl Mannheim* zugeschrieben.<sup>4</sup> Angesichts der politischen Ereignisse jener Jahrzehnte lässt sich das Prinzip der wehrhaften Demokratie dabei als Konsequenz bzw. Produkt dieser Zeit deuten: Jeweils aus

<sup>1</sup> So gaben etwa insgesamt 78 % der Befragten einer Forsa-Studie 2024 an, schon persönlich Hate Speech bzw. Hasskommentare im Internet gesehen zu haben: 14 % „sehr häufig“, 28 % „häufig“, 36 % „weniger häufig“, vgl. *Landesanstalt für Medien NRW*, Hate Speech Forsa-Studie 2024 – Zentrale Untersuchungsergebnisse, medienanstalt-nrw.de, [https://www.medienanstalt-nrw.de/fileadmin/user\\_upload/Forschung/forsa\\_Hassrede/LFMNRW\\_Hatespeech\\_forsa\\_2024.pdf](https://www.medienanstalt-nrw.de/fileadmin/user_upload/Forschung/forsa_Hassrede/LFMNRW_Hatespeech_forsa_2024.pdf), Abruf v. 7.8.2025.

<sup>2</sup> Während das BVerfG anfänglich nur den Begriff der „streitbaren Demokratie“ nutzte, vgl. BVerfGE 5, 85 (139), verwendet es heutzutage gleichermaßen den Begriff der „wehrhaften Demokratie“, vgl. jüngst BVerfGE 144, 20; *BVerfG NJW* 2024, 645.

<sup>3</sup> Vgl. BVerfG NJW 2024, 645 (647 f.) m. w. N.

<sup>4</sup> Vgl. *Schliesky*, § 277 Die wehrhafte Demokratie des Grundgesetzes, in: *Isensee/Kirchhoff* (Hrsg.), *Handbuch des Staatsrechts der Bundesrepublik Deutschland* Bd. 12, 3. Aufl. 2014, S. 847 (850 f.); wie so oft bei derartigen Konzeptentwicklungen ist eine solche Zuschreibung nicht unumstritten, vgl. zu *Loewenstein* etwa *Schaefer AöR* 2021, 401 (407; 409, dort Fn. 29).

\* Der Autor ist wissenschaftlicher Mitarbeiter am Leibniz-Institut für Medienforschung | Hans-Bredow-Institut. Dieser Beitrag entstand im Rahmen des DSA-Forschungsnetzwerks, welches von der Stiftung Mercator gefördert wird.

Deutschland ins Exil gezwungen,<sup>5</sup> verbinden die beiden Vordenker ihre Erfahrungen mit dem Scheitern der Weimarer Republik und der Machtübernahme durch die Nationalsozialisten, die auch ihren Konzeptionen zugrunde gelegt wurden.<sup>6</sup> Gleichzeitig bedeutet der zeitliche Kontext, dass sich die historische Konzeption der wehrhaften Demokratie selbst als jüngere Entwicklung nur auf begrenzte Erfahrungen in Bezug zur Kommunikation durch (Massen-) Medien stützen konnte, beschränkt auf die Presse sowie den Rundfunk in Form des Radios – womit die öffentliche Kommunikation im Gegensatz zu den heutigen Partizipationsmöglichkeiten des Internets den Eliten vorbehalten sein sollte. Ferner war auch der weltweite Austausch von Staaten untereinander vergleichsweise reduziert – es fehlte noch an weltweiten Verknüpfungen und einer international zusammenarbeitenden Gemeinschaft, welche sich erst herauszubilden begann.

Seine Theorie einer „militant democracy“<sup>7</sup> veröffentlichte *Loewenstein* 1937 in einem zweiteiligen Beitrag in der *American Political Science Review*.<sup>8</sup> Zusammengefasst forderte er Demokratien – angesichts ihrer Bedrohung durch universale Bewegungen wie den Faschismus, welche Freiheiten und Toleranzen der Demokratie strategisch gegen sie einsetzen würden – dazu auf, „militant“ zu werden<sup>9</sup>: Sie müssten legislative Maßnahmen ergreifen, um ihre verwundbaren Stellen zu schützen<sup>10</sup> – auch dann, wenn der Selbsterhalt ihrer Freiheiten es erfordern sollte, elementare demokratische Prinzipien zeitweise einzuschränken und Grundrechte vorübergehend aufzuheben.<sup>11</sup> Da Feuer mit Feuer zu bekämpfen sei, benötige es eine „disciplined“ or even – let us not shy from the word – ‘authoritarian‘ democracy<sup>12</sup>, deren umfassendste und wirksamste Maßnahme *Loewenstein* gegen den Faschismus als „political technique“<sup>13</sup> darin sah, staatsfeindliche Bewegungen gänzlich zu verbieten.<sup>14</sup> Mit seinem Beitrag sollte *Loewenstein*

den Diskurs zur Frage des „Ob“ und „Wie“ demokratischer Selbstverteidigung nicht nur maßgeblich anstoßen, sondern auch prägen.<sup>15</sup> Der für das Konzept in Deutschland lange Zeit üblicherweise verwendete Begriff einer „streitbaren Demokratie“, den zunächst auch das Bundesverfassungsgericht übernehmen sollte<sup>16</sup>, geht jedoch auf *Mannheim* zurück,<sup>17</sup> welcher 1951 in der streitbaren Demokratie einen „dritten Weg“ zwischen Diktatur und „laissez-faire Liberalismus“ sah.<sup>18</sup>

## B. Die wehrhafte Demokratie des Grundgesetzes

In der Bundesrepublik Deutschland sollten die von *Loewenstein* und *Mannheim* entwickelten Konzeptionen großen Einfluss haben.<sup>19</sup> Die Mütter und Väter des Grundgesetzes hielten das Konzept einer wehrhaften Demokratie zwar nicht wörtlich, aber sinngemäß in der Verfassung fest – ausgeprägt in solchen Vorschriften, welche der Verteidigung einer „freiheitlichen demokratischen Grundordnung“<sup>20</sup> dienen.<sup>21</sup> Das Bundesverfassungsgericht zählt insbesondere die gegenüber Akteuren anwendbaren Instrumente, wie das Vereinsverbot des Art. 9 Abs. 2 GG, die Grundrechtsverwirkung des Art. 18 GG und das Parteiverbot des Art. 21 Abs. 2 GG als Ausdruck des verfassungsrechtlichen Prinzips der wehrhaften Demokratie, welches „gewährleisten soll, dass Verfassungsfeinde nicht unter Berufung auf die Freiheiten, die das Grundgesetz gewährt, und unter ihrem Schutz die Verfassungsordnung oder den Bestand des Staates gefährden, beeinträchtigen oder zerstören.“<sup>22</sup> Zusätzliche Schutzmechanismen bestehen im weiteren Sinne etwa im Widerstandsrecht (Art. 20 Abs. 4 GG), der Ewigkeitsgarantie (Art. 79 Abs. 3 GG) oder der Verfassungstreuepflicht von Beamten (Art. 33 Abs. 5 GG i. V. m. BeamtenR).<sup>23</sup>

In der Zusammenschau stellt das Grundgesetz somit ein beträchtliches Verteidigungsarsenal bereit, das in den letzten Jahren zusätzlich erweitert wurde: So schuf der Gesetzgeber als Reaktion auf das nicht erfolgte NPD-Verbot<sup>24</sup>

<sup>5</sup> Zu den Hintergründen vgl. *Loewenstein/Lepsius/Ooyen/Schale*, Des Lebens Überfluss: Erinnerungen eines ausgewanderten Juristen, 1. Aufl. 2023, S. 154 ff., insb. Fn. 456; *Woldring*, Karl Mannheim: the development of this thought, 1. Aufl. 1986, S. 36 ff.

<sup>6</sup> Vgl. *Loewenstein*, *American Political Science Review* Vol. 31 (1937), 417 (426 ff.); *Mannheim*, Diagnose unserer Zeit: Gedanken eines Soziologen, 1. Aufl. 1951, S. 9, 12, 14, 18.

<sup>7</sup> Während sich dieser eher kämpferische Begriff im Englischen durchsetzen sollte, sind die dt. Bezeichnungen vergleichsweise defensiv, vgl. Hinweis auf semantische Unterschiede bei *Klamt*, Militant Democracy and the Democratic Dilemma: Different Ways of Protecting Democratic Constitutions, in: *Bruinsma/Nelken* (Eds.), Explorations in Legal Cultures, 1. Aufl. 2007, S. 133 (133).

<sup>8</sup> Von einer Selbsterhaltungspflicht des Staates sprach er hingegen bereits 1931, vgl. *Papier/Dürner*, AöR 2003, 340 (345 f.).

<sup>9</sup> Vgl. *Loewenstein*, (Fn. 6), 417 (417 f., 423 f.).

<sup>10</sup> Vgl. *Loewenstein*, (Fn. 6), 417 (431).

<sup>11</sup> Vgl. *Loewenstein*, (Fn. 6), 417 (432).

<sup>12</sup> Vgl. *Loewenstein*, *American Political Science Review* Vol. 31 (1937), 638 (655 f.).

<sup>13</sup> Vgl. *Loewenstein*, (Fn. 6), 417 (423 ff.).

<sup>14</sup> Im Original: „The most comprehensive and effective measure against fascism consists in proscribing subversive movements altogether“, *Loewenstein*, (Fn. 12), 638 (645).

<sup>15</sup> Vgl. *Ellian/Rijpkema*, Militant Democracy – Political Science, Law and Philosophy, 1. Aufl. 2018, S. 2.

<sup>16</sup> Vgl. BVerfGE 5, 85 (139).

<sup>17</sup> Vgl. *Papier/Dürner*, (Fn. 8), 340 (347).

<sup>18</sup> Vgl. *Mannheim*, (Fn. 6), S. 13 ff. Das Buch erschien auf Englisch bereits einige Jahre zuvor (1943).

<sup>19</sup> Vgl. *Müller*, Militant Democracy, in: *Rosenfeld/Sajó* (Eds.), The Oxford Handbook of Comparative Constitutional Law, 1. Aufl. 2012, S. 1253 (1258); *Schaefer*, (Fn. 4), 401 (409, dort Fn. 29).

<sup>20</sup> Die wörtlich hingegen mehrfach im Grundgesetz vorkommt. Der Begriff wurde durch das BVerfG kontinuierlich weiterentwickelt, es zählt dazu im Kontext des Art. 21 Abs. 2 GG inzwischen ihre Verankerung in der Garantie der Menschenwürde sowie das Demokratiet- und Rechtsstaatsprinzip, vgl. BVerfGE 144, 20 (202 ff.); *Barczak*, JuS 2025, 97 (97 ff.).

<sup>21</sup> Vgl. *Vöbkuhle/Kaiser*, JuS 2019, 1154 (1154).

<sup>22</sup> Vgl. BVerfG NJW 2024, 645 (647 f.) m. w. N.

<sup>23</sup> Vgl. *Vöbkuhle/Flaig*, JuS 2024, 617 (626).

<sup>24</sup> Vgl. BVerfGE 144, 20 (20 ff.).

2017 in Art. 21 Abs. 3 GG die Möglichkeit des Ausschlusses von der Parteifinanzierung,<sup>25</sup> während Ende 2024 durch eine Reform der Art. 93, 94 GG die Resilienz des Bundesverfassungsgerichts gestärkt werden sollte.<sup>26</sup> Letzteres ist für die wehrhafte Demokratie sogar in mehrfacher Hinsicht von Bedeutung, da die skizzierten Instrumente des Grundgesetzes zur Freiheitseinschränkung ausschließlich bei einer entsprechenden Entscheidung des Bundesverfassungsgerichts eingesetzt werden können.

Der Rückblick auf die Ursprünge der wehrhaften Demokratie und ihre Ausprägung in der Verfassung verdeutlicht zweierlei: Das Grundgesetz stellt nicht nur allgemeine Schutzmechanismen, sondern auch konkrete Maßnahmen zur Anwendung im Rahmen der wehrhaften Demokratie bereit. Unter Berücksichtigung der Möglichkeit gesetzgeberischer Erweiterungen neben der ständigen Verfassungsrechtsprechung lässt sich außerdem feststellen, dass die wehrhafte Demokratie des Grundgesetzes nicht in ihrer ursprünglichen Konzeption als Anachronismus verharren muss, sondern Entwicklungsmöglichkeiten aufweist, durch welche neuen Gefährdungslagen begegnet werden kann.

### C. Gewappnet für die kommunikativen Online-Gefährdungen der Demokratie?

Der freie Meinungs- und Willensbildungsprozess des Einzelnen und die Möglichkeit eines anschließenden freien und vielfältigen Diskurses stellen in einer freiheitlichen Demokratie Kernvoraussetzungen dar, um den Willen des Volkes abbilden zu können.<sup>27</sup> Dabei ist es insbesondere im Kontext von Wahlen essenziell, dass alle Berechtigten die Möglichkeit haben, informierte Entscheidungen zu treffen.<sup>28</sup> Doch mit der besonderen Bedeutung des Internets für die heutige Kommunikation verhalten der digitale Raum und technische Fortschritt den Feinden der Demokratie zur Erweiterung ihres Arsenal und ermöglichten gänzlich neue Angriffsmethoden – welche gerade an diesen wesentlichen Demokratie voraussetzungen ansetzten. Als besonders relevante kommunikative Online-Gefahren für die Demokratie steht die Verbreitung von Desinformation und Hass im Fokus dieses Beitrags. Es sei aber ferner darauf hingewiesen, dass das Internet in seinen Möglichkeiten weitaus mehr Angriffspotential bietet – man denke in infrastruktureller Hinsicht etwa an Cyberangriffe auf Institu-

tionen wie solche des Staates oder der Presse<sup>29</sup>, Cyberspionage oder auch Fragen der digitalen Abhängigkeit von anderen Staaten, welche unter dem Stichwort der „digitalen Souveränität“ diskutiert werden<sup>30</sup>.

Auch wenn die Verbreitung von Desinformation und Hass schon vor der Teilverlagerung des Diskurses in den digitalen Raum eine Demokratiegefährdung mit unterschiedlichen Angriffsvektoren darstellten, erhöht das Internet ihr Zersetzungspotenzial deutlich – etwa indem ihre quantitative Verbreitung durch die technischen Möglichkeiten ein nie zuvor dagewesenes Ausmaß erreichen kann. Eine Analyse wird jedoch durch die Vielschichtigkeit der Dimensionen von Desinformation und Hassrede erschwert, welche je nach Ausprägung und Kontext unterschiedliche Rechtsgüter bedrohen können.<sup>31</sup> Jene Komplexität kann an dieser Stelle nicht angemessen abgebildet werden, daher soll stattdessen das jeweilige Gefährdungspotenzial für die Meinungsvielfalt und freie Meinungs- und Willensbildung hervorgehoben werden. Die Verbreitung von Desinformation, hier verstanden als „falsche, ungenaue oder irreführende Informationen, die erfunden, präsentiert und verbreitet werden, um Gewinne zu erzielen oder bewusst öffentlichen Schaden anzurichten“<sup>32</sup>, setzt an Diskursinhalten an – sie manipuliert, worüber gesprochen wird und kann gezielt das Vertrauen in die Demokratie und demokratische Institutionen beschädigen. Dabei können konkrete Fehlvorstellungen erzeugt werden, die nicht nur Personen, Ereignisse oder Entscheidungen betreffen, sondern es auch vermögen, das Vertrauen in hergebrachte Informationsquellen und ihren Wahrheitsgehalt zu erschüttern<sup>33</sup>. Quantitativ profitiert Desinformation sowohl von den Online-Möglichkeiten massenhafter, globaler Verbreitung als auch der stetig zunehmenden Bedeutung des Internets als Bezugsquelle für Nachrichten in Deutschland.<sup>34</sup> Doch auch

<sup>25</sup> Das Instrument wurde sogleich bei der NPD angewendet, BVerfG NJW 2024, 645 (647 ff.); mit Entscheidungsbesprechung von *Wischmeyer* JuS 2025, 568 (568 ff.); zu den vier benannten Instrumenten vgl. auch *Beaucamp*, JA 2021, 1 (1 ff.).

<sup>26</sup> Vgl. dazu *Suhr*, DÖV 2025, 557 (557 ff.).

<sup>27</sup> Vgl. *Kloepfer*, § 42 Öffentliche Meinung, Massenmedien, in: *Isensee/Kirchhoff* (Hrsg.), *Handbuch des Staatsrechts der Bundesrepublik Deutschland* Bd. 3, 3. Aufl. 2005, S. 389 (395 ff.).

<sup>28</sup> Vgl. auch *Dreier*, *Grundgesetz-Kommentar*, 3. Aufl. 2015, Art. 20 Rn. 76: „Wahlen ohne vorherige Diskussion von Personen und Programmen, Abstimmungen ohne Erörterungen des Für und Wider und sachlicher Alternativen sind bloße Farce oder Fassade.“

<sup>29</sup> So wurde etwa die taz am Tag der Bundestagswahl 2024 Opfer einer DDOS-Attacke, welche die Webseite für mehrere Stunden lahmlegte, vgl. *From/Baack*, Festnahme nach Cyberangriff auf die taz – Ungarischer Hacker „HANO“ gefasst, taz.de, <https://taz.de/Festnahme-nach-Cyberangriff-auf-die-taz!/6102366/>, Abruf v. 7.8.2025.

<sup>30</sup> Vgl. dazu UFITA 2024, Heft 1, welches sich dem Thema schwerpunktmäßig widmet.

<sup>31</sup> Vgl. etwa bzgl. Desinformation *Dreyer/Stanciu/Pothast/Schulz*, *Desinformation – Risiken, Regulierungslücken und adäquate Gegenmaßnahmen*, Landesanstalt für Medien NRW, [https://www.medienanstalt-nrw.de/fileadmin/user\\_upload/NeueWebsite\\_0120/Themen/Desinformation/Leibnitz-Institut\\_LFMNRW\\_GutachtenDesinformation.pdf](https://www.medienanstalt-nrw.de/fileadmin/user_upload/NeueWebsite_0120/Themen/Desinformation/Leibnitz-Institut_LFMNRW_GutachtenDesinformation.pdf), S. 28 ff., Abruf v. 7.8.2025.

<sup>32</sup> Definition übernommen von der Europäischen Kommission, *Bekämpfung der Desinformation im Internet: ein europäisches Konzept*, COM/2018/236 final.

<sup>33</sup> Eine besondere Rolle spielen dabei Imitationen bestehender Presse-Onlineauftritte, vgl. etwa im Vorfeld der Bundestagswahl 2025 *Früwirth/Simona*, Fortsetzung folgt: Die prorussische Desinformationskampagne Doppelgänger in Deutschland, CeMAS, <https://cemas.io/publikationen/fortsetzung-folgt-doppelgaenger/>, Abruf v. 7.8.2025.

<sup>34</sup> Vgl. *Newman/Arguedas/Robertson/Nielsen/Fletcher*, *Reuters Institute Digital News Report 2025*, Reuters Institute, [https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2025-06/Digital\\_News-Report\\_2025.pdf](https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2025-06/Digital_News-Report_2025.pdf), S. 85, Abruf v. 7.8.2025.

qualitativ bietet der stetige technische Fortschritt ihr weitere Vorteile, indem er ihre Überzeugungskraft fortschreitend erhöht – etwa durch mittels generativer KI erstellte Deep-Fakes, welche immer echter wirken. In der Konsequenz wurde die Online-Verbreitung von Desinformation zu einem der prominentesten Mittel antidemokratischer Bewegungen.<sup>35</sup> Digitaler Hass bzw. Hassrede hingegen ist mit abweichendem Angriffsziel personenbezogen und richtet sich gegen bestimmte Teilnehmende eines Diskurses – mit dem Ziel, sie aus diesem zu drängen. Darüber hinaus können durch die Einschüchterungen gesellschaftliche Abschreckungseffekte (silencing effects) entstehen, welche dazu führen, dass sich marginalisierte Gruppen aus Angst präventiv aus dem Diskurs zurückziehen<sup>36</sup> – eine Demokratie, die von einem offenen und partizipativen Diskurs lebt, wird hier gezielt weiterer Stimmen beraubt. Deutlich wird dies in einer Campact-Studie von 2019: Der Aussage „Hassbotschaften gefährden die Vielfalt im Internet, weil sie Menschen einschüchtern und verdrängen“ stimmten 75 % der Befragten zu – 54 % gaben ferner an, sie würden „sich in Reaktion auf Hassrede im Internet seltener zu ihrer politischen Meinung [...] bekennen.“<sup>37</sup> Ferner beeinflusst die Präsenz von digitalem Hass auch die Entscheidung von Nicht-Betroffenen, bestimmte Räume im digitalen Diskurs aufzusuchen: Die wahrgenommene Negativität bzw. das Risiko, selbst zum Betroffenen zu werden, können diesbezüglich zu Desinteresse oder weiteren Abschreckungseffekten führen.

Bereits in dieser vereinfachten Perspektive wird evident, dass eine wehrhafte Demokratie zum Schutz ihrer Fundamente gegenüber den kommunikativen Online-Gefahren des Internets reagieren sollte. Doch dabei steht sie zugleich vor einem Dilemma: In ihrer Entgegnung muss eine sehr feine und schwierig zu bestimmende Grenze zwischen demokratiefeindlichen Äußerungen und extremen Diskursbeiträgen gewahrt werden, um nicht selbst zu einer Gefahr für den gesellschaftlichen Austausch zu werden. Somit sind bei der Ausgestaltung der Selbstschutzmaßnahmen der wehrhaften Demokratie eine Reihe von verfassungsrechtlichen Fragestellungen zu berücksichtigen – etwa in Bezug auf das Spannungsverhältnis zu Grundrechten wie

der Meinungsfreiheit des Art. 5 Abs. 1 GG –, welche differenzierte Abwägungen erfordern und eine eingreifende Reaktion der wehrhaften Demokratie auf ein angemessenes Mindestmaß beschränken sollen. Gleichzeitig stellt sich vor diesem Hintergrund die Frage, inwieweit die Instrumente der wehrhaften Demokratie am Ende dieses Prozesses noch eine effektive Abwehr gewährleisten können: Obwohl das Grundgesetz wie dargestellt auch anwendbare Instrumente im Rahmen der Wehrhaftigkeit vorsieht, wird bei einer Betrachtung unter dem Blickwinkel der skizzierten kommunikativen Gefahren des digitalen Raumes für die Demokratie evident, dass ihr Anwendungsbereich nicht zur neuen Gefährdungslage passt.

Zurückhaltender als die Vorstellung einer bisweilen autokratischen Demokratie bei *Loewenstein* beinhalten die gegenüber Demokratiefeinden einzusetzenden Instrumente des Grundgesetzes in der Konsequenz zwar tiefste Grundrechtseingriffe – aber sind in der Konsequenz als *ultima-ratio* konzipiert und nur einsetzbar, sollte das ihren Gebrauch provozierende Verhalten eine entsprechend schwerwiegende und nachweisbare Intensität erreicht haben. Diese hohe Hürde wird im Bereich der Online-Verbreitung von Desinformation und Hass schwerlich nachweisbar erreicht werden. Durch die Verbreitungsmöglichkeiten des Internets erfolgen entsprechende Angriffe auf die Demokratie oft quantitativ breit gestreut, was in der Summe zwar eine beträchtliche Wirkung entfalten mag, die aber schwierig zu bestimmen und kaum auf einzelne Akteure zurückführbar sein wird. Nicht nur erschweren technische Möglichkeiten wie Bot-Netze eine Identifizierung, sondern es handelt sich bei der Verbreitung dieser Online-Gefahren auch häufig um transnationale Vorgänge, die eine Durchsetzung erschweren und sich dem tendenziell nach „innen“ gerichteten Konzept der wehrhaften Demokratie des Grundgesetzes<sup>38</sup> als Lehre aus Weimar eher entziehen. Außerdem richtet sich die Mehrheit der Verteidigungsinstrumente gegen Personenzusammenschlüsse (Vereine, Parteien), während auch Einzelpersonen aufgrund der technischen Möglichkeiten des Internets massenhaft demokratiefeindliche Kommunikationsinhalte verbreiten können: Zwar wäre in diesem Fall noch an die Grundrechtsverwirkung gem. Art. 18 GG zu denken, aber – neben den bereits skizzierten Hürden – ist in Bezug auf die drastischen Konsequenzen dieses Instruments eine derartige Zurückhaltung geboten, dass es noch nie zur erfolgreichen Anwendung kam. Schließlich muss auch der zeitliche Faktor berücksichtigt werden: Während das Internet eine sofortige Veröffentlichung von Inhalten erlaubt, sind die Instrumente des Grundgesetzes weitaus schwerfälliger, um im sorgfältigen Verfahren ihren Konsequenzen gerecht werden zu können. Zusammenfassend lässt sich feststellen, dass die Online-Verbreitung von Desinformation und Hass trotz ihrer

<sup>35</sup> So erkennt in Deutschland eine große Mehrheit in Desinformation eine Gefahr für die Demokratie und den gesellschaftlichen Zusammenhalt, vgl. die Studie „Verunsicherte Öffentlichkeiten“ der Bertelsmann Stiftung, bertelsmann-stiftung.de, <https://www.bertelsmann-stiftung.de/de/themen/aktuelle-meldungen/2024/februar/grosse-mehrheit-erkennt-in-desinformation-eine-gefahr-fuer-demokratie-und-zusammenhalt>, Abruf v. 7.8.2025; zu Wahlen vgl. *Schlömer/Kehrborg*, ZRP 2025, 2 (2 ff.).

<sup>36</sup> Vgl. *Markard/Bredler*, JZ 2021, 864 (864 ff.); *Hoven/Witting*, NJW 2021, 2397 (2398 f.); *Schulze/Rieger*, Diskussionsräume und Radikalisierungsprozesse in Sozialen Medien, Bundeszentrale für politische Bildung, <https://www.bpb.de/themen/parteien/rechtspopulismus/562042/diskussionsraeume-und-radikalisierungsprozesse-in-sozialen-medien/>, Abruf v. 7.8.2025.

<sup>37</sup> Vgl. *Geschke/Klaßen/Quent/Richter*, Executive Summary – #Hass im Netz: Der schleichende Angriff auf unsere Demokratie, Campact, [https://blog.campact.de/wp-content/uploads/2019/07/Hass\\_im\\_Netz\\_Executive\\_Summary.pdf](https://blog.campact.de/wp-content/uploads/2019/07/Hass_im_Netz_Executive_Summary.pdf), S. 2, Abruf v. 7.8.2025.

<sup>38</sup> Die Wehrhaftigkeit der Demokratie des Grundgesetzes nach „außen“ stützt sich auf wenige Regelungen militärischen Hintergrundes, vgl. *Schmahl*, Wie wehrhaft ist das Grundgesetz gegenüber Bedrohungen von außen?, in Hofmann (Hrsg.), *Zeiten der Bewährung – FS 75 Jahre GG*, 2024, S. 479 (479 ff.).

Auswirkungen auf demokratische Fundamente die Schutzmechanismen des Grundgesetzes im Regelfall unterlaufen wird – dies jedoch nicht, weil die wehrhafte Demokratie des Grundgesetzes der Möglichkeit einer Fortentwicklung beraubt wurde. Maßgeblich sind vielmehr eine fehlende umfassende Durchsetzungsmacht der deutschen Staatsgewalt im globalen Internet, der Zuschnitt der Wehrhaftigkeit des Grundgesetzes auf Extremfälle und ihr reaktives Verwaltungshandeln gegenüber konkreten Akteuren (Vereine, Parteien, Personen), welches einer systemischen Bedrohungslage im Internet – gekennzeichnet von unzähligen, schwer identifizierbaren Kräften – gegenübersteht.

#### D. Wehrhafte Demokratie als Aufgabe des Einzelnen?

Erweitert man das Konzept der wehrhaften Demokratie jedoch, sodass es die Summe der auf den Schutz des Diskurses und der demokratischen Institutionen gerichteten Normen umfasst, stehen in der Bundesrepublik erheblich mehr Instrumente zur Abwehr der skizzierten kommunikativen Gefahren im Online-Umfeld zur Verfügung – auch in Bezug auf die Anwendungshäufigkeit, da ihre im Vergleich zum Grundgesetz schwächeren Konsequenzen niedrigere Hürden vorsehen. Gleichzeitig lässt sich jedoch von keinem umfassenden Schutzkonzept sprechen: In Ermangelung speziell geschaffener Vorschriften handelt es sich stattdessen um fragmentarisch über das Recht verteilte Abwehrmöglichkeiten unterschiedlicher Kontexte,<sup>39</sup> die ferner vorrangig dem Individuum zum Schutz bestimmter Rechtsgüter dienen – und dadurch nur mittelbar der Demokratie selbst. So vermögen die zivilrechtlichen Unterlassungsansprüche der §§ 823, 1004 BGB zwar der individuellen Verletzung von Persönlichkeitsrechten aufgrund der Online-Verbreitung von Desinformation oder Hass abzuwehren – das jedoch effektiv nur *ex post*, bezogen auf wenige Konstellationen und insbesondere eine Breitenwirkung nur dann erzielend, sollte ein Großteil der Betroffenen konstant ihre Rechte durchsetzen. Beliebte es die Rechtsordnung bei solchen, von der Geltendmachung durch die Betroffenen abhängigen Rechtsinstrumenten, wäre die Wehrhaftigkeit jedoch dem Spiel der gesellschaftlichen Kräfte überantwortet; spezifische Sicherungs- und Abwehrmechanismen des Staates selbst fehlten gerade. Somit kann in diesem Kontext eine Demokratie, die sich nicht lediglich auf Kosten und der Verantwortung weniger verteidigt, nur wehrhaft sein, wenn sie zugleich ein angemessenes Tätigwerden des legitimierte Staates vorsieht. Dabei ist es insbesondere die Strafverfolgung als letztmögliches Einschreiten der Exekutive gegenüber gesellschaftlich-missbilligtem Verhalten, welche der wehrhaften Demokratie weitere Instrumente bieten kann: Schon *Loewenstein* erwog als Maßnahme der wehrhaften Demo-

kratie in Bezug zur Kommunikation die Durchsetzung von Straf- bzw. Gewohnheitsrecht, welches sich politische Anfeindungen und Aufstachelung zu Gewalt oder Hass gegenüber bestimmten Teilen der Bevölkerung annehme.<sup>40</sup> In Bezug auf die Online-Verbreitung von Hass und Desinformation bietet das StGB keine eigens geschaffenen und entsprechend umfassenden Straftatbestände, doch von einer strafrechtlichen Wehrlosigkeit gegenüber den kommunikativen Gefahren des digitalen Raums lässt sich nicht sprechen, da sie durch allgemeine, bestehende Vorschriften bereits erfasst werden können: So kommen – je nach Ausprägung – etwa bei der Verbreitung von digitalem Hass<sup>41</sup> neben den Straftatbeständen zum Schutz der persönlichen Ehre und Freiheit (§§ 185 ff., 192a, 240 f. StGB) auch solche der Gefährdung des Rechtsstaats (§§ 86, 86a StGB), des Widerstandes gegen die Staatsgewalt (§ 111 StGB) und Straftaten gegen die öffentliche Ordnung (§§ 126, 130 f., 140 StGB) sowie mit Bezug zur Religion bzw. Weltanschauung (§ 166 StGB) in Betracht.<sup>42</sup> Doch obwohl die Anwendung des Strafrechts auf den ersten Blick umfangreiche Möglichkeiten zum Demokratieschutz bieten mag – da es trotz *ultima-ratio*-Eigenschaft im Vergleich zum Grundgesetz weniger intensive Gefährdungen auch durch Einzelpersonen erfassen kann – kann in ihr allein kein Mittel gegen die demokratiegefährdende Online-Verbreitung von Hass und Desinformation gesehen werden. So weist das bestehende Strafrecht Schutzlücken auf,<sup>43</sup> erfordert bezüglich der Ehrschutzdelikte der §§ 185 ff. StGB im Regelfall einen Strafantrag der Betroffenen (§ 194 StGB) und bietet nebst Abschreckungseffekten keine präventiven Maßnahmen. Ferner kommt es durch die Besonderheiten des digitalen Raumes zu Problemen der Rechtsdurchsetzung, welchen in Bezug auf eine Verantwortlichkeit von Anbietenden sozialer Netzwerke 2017 durch das umstrittene und inzwischen größtenteils aufgehobene Netzwerk-Durchsetzungsgesetz begegnet werden sollte.

Insbesondere ist jedoch erforderlich, dass eine wehrhafte Demokratie im Kontext der Online-Verbreitung von Hass und Desinformation nicht nur die dahinterstehenden Akteure in den Blick nimmt, so wie es die bisherigen Vorschriften hauptsächlich taten. Auch flankierende Maßnahmen, wie etwa dem Entgegenwirken von Desinformation schädlicher Internetquellen durch einen starken öffent-

<sup>40</sup> Vgl. *Loewenstein*, (Fn. 12), 638 (651 ff.).

<sup>41</sup> Zu Verbreitung falscher Tatsachen und der Anwendung des Strafrechts vgl. *Beck/Nussbaum*, KriPoZ 04/2025; *Lammich*, Fake News als Herausforderung des deutschen Strafrechts, 1. Aufl. 2022, S. 145 ff.; *Hoven/Krause*, JuS 2017, 1167 (1167 ff.).

<sup>42</sup> Vgl. ausführlich *Bulut*, Strafbarkeit der Hassrede in Sozialen Netzwerken, 1. Aufl. 2025, S. 240 ff.

<sup>43</sup> Vgl. etwa zur Online-Verbreitung von Hassrede *Bulut*, (Fn. 42), S. 441 ff., welche auf ein fehlendes einheitliches Gruppenschutzkonzept hinweist; zu politischen "Fake News" *Schreiber*, Strafbarkeit politischer Fake News, 1. Aufl. 2022, S. 317 f., 185 ff., der eine fehlende tatbestandliche Erfassung von politisch instrumentalisierten Falschinformationen, welche persönliche Wahlentscheidungen manipulativ beeinflussen, feststellt.

<sup>39</sup> Vgl. zur Übersicht bei der Online-Verbreitung von Desinformation *Dreyer/Stanciu/Pothast/Schulz*, (Fn. 31), S. 32 ff.; bei Hassrede *Seifert*, Hassrede in sozialen Netzwerken, 1. Aufl. 2024, S. 92 ff.

lich-rechtlichen Rundfunk, auch im Digitalen, können nur bedingt helfen: So vermögen ARD, ZDF und Deutschlandradio nur als Korrektiv zu dienen, wenn ihnen die Gesellschaft als Nachrichtenquelle vertraut – weswegen Desinformation häufig gezielt an dieser Stelle ansetzt und versucht, ihre jeweilige Glaubwürdigkeit zu beschädigen.<sup>44</sup> Daher müssen stattdessen auch die Bedingungen des Diskurses, die jeweiligen Räume des Austausches, in den Blick genommen werden, damit nicht nur den Inhalten selbst, sondern insbesondere auch ihrer massenhaften Verbreitung entgegengewirkt werden kann. Es ist nicht nur der demokratiefeindliche Social-Media-Post, sondern auch die Möglichkeit einer Priorisierung in einem algorithmisch-kuratiertem Feed, durch welche sich seine Wirkung intensiviert. Es ist die Option, sich als ein offizieller Account zu tarnen, welche Desinformation glaubhaft erscheinen lässt. Es ist das Vorgehen, sich auf Online-Plattformen ohne Meldeverfahren bzw. Inhaltsmoderation zurückzuziehen, um Gegenmaßnahmen zu entgehen. Es sind somit auch die Online-Plattformen als Intermediäre, welche in einem breit verstandenen Konzept der Wehrhaftigkeit nicht außer Acht bleiben dürfen und eine Regulierung erfordern – denn wer ihre Gestaltungsmacht in Bezug auf digitale Kommunikation ignoriert, wird nur durch eine stetige Intensivierung von Löscho- und Sperrvorschriften der Veränderung des Online-Diskurses ansatzweise begegnen können und in diesem Zuge selbst zur Gefahr werden.

## E. Vom nationalen zum supranationalen Schutz der Demokratie

Ausweislich der transnationalen Eigenschaften internetbezogener Vorgänge und der weltweiten Macht der größten Online-Plattformen kann eine solche Regulierung nicht nationalstaatlich bewältigt werden: Wenn Demokratien auch im globalen Internet wehrhaft bleiben wollen, ist ein gemeinsames Vorgehen mit anderen Staaten unausweichlich. Prädestiniert für diese Art der Zusammenarbeit, nimmt die Europäische Union mit der Schaffung des Digital Services Act (DSA) als EU-Verordnung 2022 eine regulatorische Vorreiterrolle ein: Digitale Vermittlungsdienste unterliegen – je nach Art und Größe – unterschiedlichen Anforderungen bezüglich Transparenz, Inhaltsmoderation, AGB, Kontaktmöglichkeiten, Melde- und Abhilfep Verfahren, trusted flagger etc., welche in der Summe ein „sicheres, vorhersehbares und vertrauenswürdigen Online-Umfeld“ (Art. 1 Abs. 1 DSA) in der EU schaffen sollen. Dabei ist hervorzuheben, dass der DSA in Bezug auf rechtswidrige Inhalte keine eigenen materiell-rechtlichen Bestimmungen vornimmt und den Vermittlungsdiensten keine Verpflichtungen zur Überwachung oder aktiven Nachforschung auferlegt – die EU-Verordnung dient nicht einem europaweiten Vorgehen gegen bestimmte Inhalte, sondern

dem Schutz von Internet-Nutzenden, indem die Rahmenbedingungen des digitalen Raumes angepasst werden. Es zeigt sich, dass ausgerechnet jene überstaatlichen Strukturen wie die EU, in welche sich einzelne Staaten unter Abgabe eigener souveräner Gestaltungsmacht begeben haben, nun dazu beitragen, im Zeitalter des Internets die demokratischen Fundamente der Staaten zu bewahren.

Besonders relevant in Bezug auf den Diskurs und somit die Demokratie sind dabei die Art. 34, 35 DSA, welche das Herzstück darstellen: Sie sehen eine Bewertung und Minderung von systemischen Risiken seitens sehr großer Online-Plattformen vor, wobei nicht nur nachteilige Auswirkungen auf Grundrechte, sondern auch die gesellschaftliche Debatte sowie auf Wahlprozesse und die öffentliche Sicherheit wörtlich umfasst sind. Mithilfe dieser risikobasierten Regulierung soll sichergestellt werden, dass die Möglichkeit besteht, auch zukünftigen Ausprägungen kommunikativer Online-Gefahren für die Demokratie entgegenzuwirken.<sup>45</sup> Ob dies erfolgreich gelingt, wird sich in Zukunft zeigen müssen – der DSA trat erst 2024 vollständig in Kraft. Jedenfalls aber stellt die EU-Verordnung die erste umfassende, transnationale Plattform-Regulierung dar, welche sich des Diskurses im Digitalen nicht lediglich in Bezug auf schädliche Inhalte annimmt. Flankiert wird der DSA in Bezug auf eine wehrhafte Demokratie im Digitalen ferner von weiteren EU-Vorschriften, wie etwa Art. 18 EMFA, der DS-GVO<sup>46</sup> oder der Verordnung über politische Werbung, womit sich ein europäisches „Wehrhaftigkeitsrecht“ herauszubilden beginnt – welches zwar kompetenzielle Fragen aufwirft, jedoch angesichts der inzwischen globalen Bedrohungslagen gegenüber einzelstaatlichen Ansätzen eine bessere Eignung aufweisen kann. Freilich soll abschließend nicht unterschlagen werden, dass selbst sehr große Online-Plattformen von sich aus dazu beitragen, der Online-Verbreitung von Desinformation und Hass auch präventiv entgegenzuwirken: Sei es etwa durch ihre privatautonomen AGB zur späteren Inhaltsmoderation, Verifizierungsmaßnahmen für staatliche Kanäle oder den Beitritt zu freiwilligen codes of conduct, wie dem – inzwischen in den DSA integrierten – Verhaltenskodex zur Bekämpfung von Desinformation. Ferner lässt sich Rahmen eines ko-regulativen Ansatzes wie im DSA weiterhin an diesen Selbstregulierungspraktiken gewinnbringend anknüpfen: Während einzelne Staaten bzw. die EU etwa bei Desinformation ohne konkreten Drittbezug aufgrund ihrer rigiden Grundrechtsbindung nur beschränkt einschreiten können, ist es Online-Plattformen als private Unternehmen aufgrund ihrer Privatautonomie und andersgearteten Grundrechtsbindung hingegen einfacher möglich, diese zu regulieren.<sup>47</sup> Doch wie die politischen Ereignisse

<sup>44</sup> Vgl. etwa im Vorfeld der Bundestagswahl *Reveland*, tagesschau als Ziel von Deepfakes, Tagesschau, <https://www.tagesschau.de/faktenfinder/ki-fakes-tagesschau-100.html>, Abruf v. 7.8.2025.

<sup>45</sup> Vgl. in Bezug auf Wahlen *Harfst*, Wahlen in der wehrhaften Plattform-Demokratie, Verfassungsblog, <https://verfassungsblog.de/wahlen-in-der-wehrhaften-plattformdemokratie-dsa-bundestagswahl/>, Abruf v. 7.8.2025.

<sup>46</sup> Vgl. etwa zur Anwendung bei „deep-fakes“ *Kumkar/Rapp*, ZfDR 2022, 199 (212 ff.).

<sup>47</sup> Vgl. *Mast*, JZ 2023, 287 (295 f.).

nisse in der USA und ihre Auswirkungen auf die Inhaltsmoderation von sehr großen Online-Plattformen wie Facebook zeigen,<sup>48</sup> ist eine (unregulierte) Selbstregulierung im Plattformkapitalismus unternehmerischen Schwingungen unterworfen, die keinen verlässlichen, konstant gewährleisteten Schutz der Demokratie ermöglichen können.

## F. Fazit

Die Verbreitung von Hass und Desinformation gefährdet die Meinungsvielfalt und freie Meinungs- und Willensbildung und damit den Diskurs als Fundament der Demokratie. Durch die technischen Möglichkeiten des digitalen Raumes haben sie dabei erheblich an Potential dazugewonnen, womit eine angemessene Reaktion der wehrhaften Demokratie erforderlich ist. Doch die im Grundgesetz vorgesehenen Verteidigungsinstrumente weisen trotz Modernisierungen eine fehlende Passung auf. Versteht man das Konzept der wehrhaften Demokratie jedoch weit, ermöglicht eine Kombination aus nationalem Recht und Unionsrecht, insbesondere dem DSA, vielversprechende Vorgehensmöglichkeiten – auch wenn die Zukunft zeigen muss, ob sie den neuen Bedrohungen gerecht werden können.

---

<sup>48</sup> Vgl. *Thompson/Conger*, Meet the Next Fact-Checker, Debunker and Moderator: You, New York Times, <https://www.nytimes.com/2025/01/07/technology/meta-facebook-content-moderation.html>, Abruf v. 7.8.2025.